

Closed Circuit Television System Guide

By Wal Brewer

Introduction

This brief is not a specification but aims to set out guidelines for specifying and/or selecting CCTV surveillance systems.

A CCTV system has limitations in the security sense. However an effective CCTV system could be expected to:

- ⊕ Provide a deterrent to those considering attacks on the facility;
- ⊕ Increase the probability of detecting behaviour that may be precursory to a criminal attack; and
- ⊕ Providing evidence to assist in any post incident investigation.

Why Use CCTV

Deterrent Value of Cameras

In the main, CCTV coverage of areas where criminal activity occurs, CCTV systems have reduced crime. The deterrent value is in the increased probability that offenders will be identified and eventually brought before the courts.

Increasing the Likelihood of Detecting Criminal Planning

CCTV cameras have the potential to observe images of activities that indicate criminal planning may be in progress. However, a considerable amount of legitimate activities in public places could also appear suspicious. A competent CCTV system with the ability to store images for analysis by appropriately trained people could assist in the detection of a criminal plan when considered with other available intelligence.

Evidence for Post Event Analysis

CCTV cameras have the potential to provide images just prior to, during and possibly just after a criminal attack. These images could provide critical evidence in the search for perpetrators after an event. To be effective, the cameras need to be located where the potential to be damaged by the incident is minimal. If the images are to be used as irrefutable evidence, then the images must be captured and stored in a manner that is acceptable in the courts. Further, there needs to be a process that ensures that potentially critical images are not over-written or corrupted.

CCTV as a Substitute for Human Surveillance

CCTV cameras do have many benefits over direct human surveillance. They include:

- ⊕ Having a much reduced operating cost;
- ⊕ Having the ability to cover an area on a 24 hour basis and many points simultaneously by using many cameras from a range of vantage points including vantage points that could be inaccessible or hazardous to humans; and
- ⊕ Having the ability to record images of activity for storage and analysis by others;

The down side is that:

- ⊕ A human must still determine what images are to be kept because the ability to store images is finite and the usual methods commence over-writing the oldest data once the data medium is full;
- ⊕ Images can be missed because of poor light, an obstruction or the system may be following a pattern of surveillance based on a specific 'guard tour' which could happen to be aimed at another field of view at the time of the incident; and
- ⊕ Humans are able to follow up on a greater range of indicators based on what is observed than a CCTV system could even with the best of video activation and trigger inputs available.

Used intelligently and monitored by appropriately trained and briefed operators the CCTV system has the potential to cover many critical points far more economically than humans on-site.

Recording Entry and Exit at Critical Points

CCTV systems have proven very capable in this regard particularly since the advent of digital recording systems. Cameras recording pedestrian and vehicle entry and exit needs to be organised so that images can be retrieved based on date, time and place. Normally a human needs to oversight the procedure releasing the entry/exit barrier when a satisfactory identification is made. It is usual to link the person or the vehicle to an access control card or PIN before entry, in particular, or exit is granted.

CCTV Coverage Aims

CCTV coverage should aim to provide surveillance and coverage that will:

- ⊕ Act as a deterrent to people seeking to harm the facility, its clients and staff;
- ⊕ Help identify suspicious people and vehicles;
- ⊕ Help identify suspicious behaviour;
- ⊕ Assist in the identification of possible points of attack based on public assembly;
- ⊕ Provide a record of activity at critical points for security analysis and criminal evidence; and
- ⊕ Providing evidence to assist in any post incident investigation.

NB: The general principle should be to cover the point/s of security interest or the pathway/s to the point/s of interest or both.

Camera Positioning

Widespread CCTV camera coverage is not considered essential. What is essential is a means of identifying suspicious behaviour in areas where criminals are likely to strike.

However, the points that should be covered include:

- ⊕ The vehicle entrances to the facility;
- ⊕ The pedestrian entrances to the facility; and
- ⊕ The perimeter or other place attractive to criminals.

NB: Camera positioning must consider the light available and its intensity and the potential to cause glare or back-light subjects of interest. The position of the sun over the course of a day at various times of the year must also be considered.

Camera Control

The cameras should normally be fixed. In circumstances where there is an operator monitoring the system, or where cameras are required to sweep large areas, remote control cameras should be considered. Camera controls should include:

- ⊕ Pan - movement in azimuth;
- ⊕ Tilt - movement in elevation;

- ⊕ Zoom - the ability to alter the effective focal length of the lens to view close up or from afar;
- ⊕ Automatic iris control;
- ⊕ Automatic (electronic) shutter speed control;
- ⊕ Light filters in difficult light conditions; and
- ⊕ Automatic or remote switching from colour to black and white to gain better image performance in poor light conditions.

NB: movement activated cameras will record continuously when set to continually sweep areas - the movement activation detection mechanism/software doesn't know if the subject is moving or if the camera is moving.

The Cameras

The cameras are of little interest in terms of specification. It is the camera performance that needs to be the driving consideration. The following characteristics should be considered:

- ⊕ Image resolution expressed in terms of pixels where 720 x 486 (effective pixels) resolution would be the minimum acceptable in these applications if the identification of individuals and vehicle number plates is desirable. If resolution is expressed in TV (horizontal) lines (TVL) then 470 TVL would be an acceptable minimum in PAL video format - the standard used in Australia;
- ⊕ The ability to provide clearly defined images in all available light conditions;
- ⊕ The ability to capture acceptable images where the subject is back lit (eg. from the rising or setting sun);
- ⊕ The ability to be TCP/IP addressable; and
- ⊕ The ability to capture images utilising video motion detection and on alarm input;

A camera fitted with a zoom lens must be able to capture clear bright images in areas of security interest in the worst light conditions at the focal length required to capture the required images which could be at maximum zoom where lens light transmission performance is at its poorest .

It may be necessary for example to specify cameras with features to enhance image definition, clarity and brightness of objects that are backlit.

Cameras claiming to operate in 0.5 or 1.0 lux light levels need to be treated with caution. The light available for image capture is the light reflected from the subject, in low lux light levels the reflected light could be one fifth of the ambient level. Further, zoom lenses reduce the amount of light reaching the image plane where the image sensitive surface (or CCD element is located).

All endeavours should be made to select the right camera for each location. The practice of one camera model fits all situations usually does not result in optimum performance or an economical installation. No camera should be accepted until a full field test/demonstration is conducted in all possible light conditions and at all likely lenses focal length settings. Field testing must also include assessment of the images produced in the worst expected light conditions.

Camera Mountings and Enclosures

The mounting points must be stable, provide the required coverage and avoid direct light into the lens. The higher the camera can be located the less likely they are to be affected by glare from the sun or artificial light sources. Of course, greater height means greater

cost, or less stable mountings, and images from downward aimed cameras may be less useful in identifying people's faces and vehicle number plates.

Cameras located outdoors will almost certainly require mountings and enclosures for protection from the elements, tampering and vermin and possibly shades and/or filters to reduce glare from the sun or flood lights.

Cameras that are to be generally static but may need to be re-aimed from time to time should be remotely controlled for focus, pan, tilt and zoom.

Camera mountings that are difficult to reach without the aid of long ladders or special human elevating equipment (cherry pickers) should be avoided.

Location and mounting considerations:

- ⊕ Coverage needed;
- ⊕ Lighting available and its coincident angle/s - natural and artificial;
- ⊕ Aiming and alignment;
- ⊕ Problems with low sun - morning, evening and winter;
- ⊕ Mounting stability;
- ⊕ Limitations on mounting on heritage buildings/structures;
- ⊕ Out of reach of vandals and risk of being accidentally misaligned;
- ⊕ Weather conditions and need for environmental protection;
- ⊕ Protection for installation, including cabling, from vermin and insects; and
- ⊕ Do not interfere with the normal activities of the facility.

It goes without saying that east and west facing cameras will have difficulty handling early morning and late afternoon sun. North facing (southern hemisphere) or south facing (northern hemisphere) cameras may have similar difficulties in winter. Some of these effects can be managed by using careful camera aiming, camera lens hoods, cameras tolerant to back lit subjects and cameras that use automatic shutter speed control instead of auto iris.

Data (Image) Capture Options

Data can be captured based on a number of conditions using CCTV. Capturing data based on one or more conditions can maximise the likelihood of capturing images of interest and reduce data file size which in turn relieves data transmission, data processing and storage requirements. Data can be captured based on one or more of the following parameters:

- ⊕ Time interval - recording a set number of images per second;
- ⊕ Event activated - where an input from a trigger device, such as a movement detection device, causes the system to record images from specified cameras for a specified period of time;
- ⊕ Movement activated - where a relatively simple signal processor inside the camera detects movement within its field of view and causes the system to record images from that camera for a specified period of time;
- ⊕ Movement activated - where a relatively sophisticated device connected to the camera detects a particular form of movement within nominated areas of the field of view of the connected camera and causes the system to record images from that camera for a specified period of time;
- ⊕ Movement activation followed by tracking - where a relatively sophisticated device connected to the camera detects a particular form of movement within the field of view of the camera and causes the system to record images from that camera for a specified period of time whilst the camera follows the subject that triggered the action.

- ⊕ Time activated - where the system records images from specified cameras at specified times;
- ⊕ Guard tour - where a camera with pan, tilt and zoom capabilities sweeps a predetermined area in a predetermined sequence with the ability to aim on predetermined areas in the event of an input from a trigger device; and
- ⊕ Command activated - where the operator commands the system to record images from specified cameras on command.

CCTV Monitoring

CCTV systems are of greatest value when an operator is deployed to monitor them at all times that the identified risks are assessed to exist. A combination of monitoring and movement activated image recording for later review is probably the best compromise solution. To minimise the review effort the system should be configured to record images and sequences of images based on time, alarm type activation or video motion within the camera field of view.

Recording based on events is usually restricted to recording when movement is detected in a camera field of view or movement is triggered by some other device or means such as:

- ⊕ Operator command;
- ⊕ The opening of a gate, boom gate or door fitted with triggering switch;
- ⊕ The switching on of a light; and/or
- ⊕ The tripping of an intrusion or movement detector.

Digital CCTV recording systems can be set up to record everything then over-write images not associated with a predetermined event thus discarding images of no consequence. This process allows the system to record some images immediately before the triggering event and some immediately after for better event analysis.

If images are to be used for more than security analysis, for example evidence in criminal prosecutions, they must be capable of being authenticated and proof from alteration.

The System

The CCTV system should be of the digital video recording type where images or sequences of images are stored digitally on random access media for random retrieval and review.

Images should be a minimum of 720x486 (effective pixels) but more importantly should provide sufficient clarity and definition in all light (natural and artificial) conditions, to be able to identify, the following:

- ⊕ The registration number plate of a vehicle at a distance of 20 metres and up to 15 degrees oblique to the camera where the vehicle frontage fills half of the field of view; and
- ⊕ A person facing the camera at a distance of 20 metres where the person fills the height of the field of view.

The system should be capable of handling the required number of cameras with capacity to expand by 25% or other nominated amount based on projected future needs.

The system should be capable of controlling pan, tilt, and zoom cameras remotely.

Back-up and Archive

Backing up of images of interest and archiving of same needs to be considered. For the type of events that could indicate a possible future criminal attack some images and image sequences may need to be kept for up to 3 months and occasionally even more. Adequate archiving facilities for this requirement should be allowed for. All archiving should be random access storage with a simple to use cataloguing system for easy and fast retrieval.

It should also be possible to extract images and copy them to removal media such as CD ROM or DVD CD for forwarding to other authorities for information.

Power Requirements

Most modern CCTV systems, and the peripherals required to make them effective, have a low voltage power requirement that can be provided at low cost providing that there is articulated mains power of the 110 Volts AC or 240 Volts AC to the site. Most components have built in rectifiers, regulators and devices to allow them to be connected directly to a mains power supply outlet. Others require a separate power supply. Battery back-up is recommended to ensure continuous operation in the event of mains power interruptions. The duration of the standby power supply would depend upon the time it would normally take to rectify a typical power outage in the area of the installation. In most cases, one to two hours is all that is necessary. If the facility already has an uninterruptible power supply, there may be capacity to provide the CCTV system power requirements from it.

CCTV System Options

Stand-alone Systems with Local Monitoring and Data Recording

This option offers a quick and simple solution but would need an operator on-site to be effective.

This option does not provide any off-site data recording, backup or monitoring. If the on-site system components were attacked, any data recorded could be stolen or destroyed. In summary, such a system could have:

- ⊕ On-site monitoring at prescribed times.
- ⊕ Automated 'guard tour" monitoring, that is, cameras automatically scan the area under surveillance in a preset pattern.
- ⊕ On-site storage of recorded images - first recorded to be first over-written.
- ⊕ On-site archiving (eg. using DVD CD ROM) of incidents of interest identified by the operator.
- ⊕ CCTV communication requirements - nil.

Networked System with Local Data Recording and Off-site Monitoring

This system allows for off-site monitoring and control but to reduce communications bandwidth requirements has on-site data recording with the capacity for the operator to archive images and sequences of interest on command.

This option provides for off-site monitoring and limited off-site data recording. If the on-site system components were attacked, data recorded off-site could be retrieved. This option would be less vulnerable to deliberate interference with data than Option 1. In summary, such a system would have:

- ⊕ On-site monitoring.
- ⊕ Automated 'guard tour" monitoring at all other times, that is, cameras automatically scan the area under surveillance in a preset pattern and viewed by operators at a central monitoring facility who have the capacity to command cameras to switch between several preset scanning patterns or take direct control of the camera/s
- ⊕ Off-site monitoring at prescribed times
- ⊕ On-site storage of recorded images - first recorded to be first over-written
- ⊕ Off-site archiving of sequence recorded images and incidents of interest identified by either an on-site or off-site operator.

- ⊕ CCTV communication requirements - eg. Wireless, ADSL (asymmetrical digital subscriber line) telephone communications, fibre optic or a combination of these allowing images to be recorded off-site also.

Networked System with Local and Off-site Data Recording and Off-site Monitoring

This system allows for off-site monitoring, control and data recording. It requires considerable communications media bandwidth and depending upon the number of cameras may not perform satisfactory unless very high speed communications are provided.

This option provides for full off-site monitoring and data recording. If the on-site system components were attacked all data recorded could be retrieved. This option would be less vulnerable to deliberate interference with data than Option 1. In summary, such a system would have:

- ⊕ Automated 'guard tour" monitoring at prescribed times, that is, cameras automatically scan the area under surveillance in a preset pattern and viewed by operators at a central monitoring facility who have the capacity to command cameras to switch between several preset scanning patterns or take direct control of the camera/s
- ⊕ Off-site monitoring at prescribed times
- ⊕ On-site and off-site (as specified) storage of sequence recorded images - first recorded to be first over-written
- ⊕ Off-site archiving of sequence recorded images and incidents of interest identified by the operator or triggered by a interfaced triggering device such as an intrusion detection device
- ⊕ CCTV communication requirements - Wireless, Fibre optical cable, ADSL or a combination of all three.

Network Options

The options that should be considered are those that can provide communications over a wide area at a satisfactory bandwidth. Network options include those outlined below.

Dial-up Network

Advantages

Third party infrastructure is already there.
 Low capital cost.
 Can be monitored from anywhere there is a telephone line.
 Multiple dial-up lines are possible.

Disadvantages

Very low bandwidth which equals very poor image quality and/or slow image transmissions - 56Kbits/sec (using normal telephone line) to 128Kbits/sec (using ISDN) at best.

Virtual Private Network Using ADSL

Advantages

Third party infrastructure is already there.
 Low capital cost.
 Can be monitored from anywhere ADSL service is available.
 Asymmetrical transmission of data provides a bandwidth of up to 256 Kbits/sec upstream and 1.5Mbits/sec downstream.

Disadvantages

Ongoing communications connection costs.
 Moderate bandwidth if symmetrical system needed - some systems do not work well on asymmetrical digital subscriber line communications preferring the slower symmetrical digital subscriber line instead.
 Reliance on service provider for security

Several lines can be used to achieve system redundancy and a higher level of data transmission required.

unless encrypted.

Vulnerable to attacks on the network infrastructure.

Wireless Network

Advantages

Infrastructure easier to install and maintain than cables.

Can be redeployed if required with relative ease.

Faster than any available telephone subscriber network.

Can offer bandwidths from 250Kb/sec to 54Mb/sec.

Disadvantages

High capital costs.

Can suffer from RF interference.

Poor security unless encrypted.

Affected by extreme weather conditions, for example, high winds and lightning strikes.

Could be affected by EW or radio jamming equipment.

Licensing may be required for high powered (long range) RF communications systems.

Fibre Optic Cable Network

Advantages

Faster than any other available form of communications providing bandwidths up to 2Gb/sec.

Disadvantages

Very high capital costs considering the wide area to be covered and the communication distances.

Regular maintenance required.

Cable network in public places prone to damage or deliberate interference

The Ideal Network

The ideal network for the overseas environment would be one that used a combination of communication technologies. For short runs between cameras and digital video controllers, twisted pair, Category 5 cabling or even co-axial cable would appear to be suitable. For communications between the various on site digital video controllers and the central monitoring facility the choice could be made based on the number of cameras x images/sec x image size or in other words the bandwidth required. Simply choose the best communications for each link - the same means of communications would not be necessary be needed for all.

Other Considerations

It is possible to obtain software that can be used to view images and sequences of images on personal computers that do not form part of the CCTV system. Preference should be given to systems that produce image formats that do not require special software for viewing as it may be necessary to send images to agencies, that may remotely located, quickly for analysis.

If difficult lighting conditions or long distances between camera and subject exist, and high resolution images are needed, consideration should be given to using B-W (black and white) cameras.

Explosive resistant camera enclosures are available and consideration should be given to using them in situations where the need to glean evidence, before, during and after an explosion is a high priority.

In a system where movement or other input initiates recording of images, missed images are assumed to be because no movement took place. Images taken in sequence from each camera provides a means of verifying that no one has interfered with the system to prevent images being recorded - a break in the sequence indicates that something has prevented images being recorded. Another way of verifying that there has been no break in the sequence of images is to place a clock in the field of view of critical cameras. The clock should be positioned where the time can be readily discerned but far enough away so that the movement of the hands or the changing of the display does not set off any movement activated recording. The time on the clock should be synchronised and kept within a few seconds of the CCTV system clock so that verification by comparing the time of the two is possible.

Developing Specifications

The specifications form part of a statement of requirement or similar instrument. Specifications should set out the performance required of the system. The specification should demand what is known as a 'turn key' system, that is, on completion it will function without anything more than operator actions from the client or the client's agents. Even the best of cameras and equipment can fail to provide the level of performance required if they are not selected, installed and configured correctly.

The statement of requirement should provide for a demonstration of performance in similar conditions to those that prevail at the facility. Be wary of bench tests or showroom demonstrations. Demonstrations using a few cameras could disguise the performance of networks; accordingly a basic understanding of data traffic needs to be understood. Data traffic is a product of:

- ⊕ Image file size - notwithstanding data compression techniques, the greater the resolution the greater the file size - a typical image file size ranges from 3Kbytes to 30Kbytes;
- ⊕ The number of cameras on the system;
- ⊕ The number of images required per second; and
- ⊕ Multiplying the above elements will give the amount of data to be transmitted per second - multiply this by 60 (for data per minute) and again by 60 (for data per hour) and again by 24 (for data per day).

Data storage is based on the above multiplied by the number of day's data that is to be kept on the system.

Data storage is normally expressed in bytes and transmission speeds are expressed in bits. There are eight bits to each byte.

By stating the performance required it is much easier to verify that the installation meets expectations.

Sometimes it is prudent to specify the tests, together with a minimum objective pass standard, that are to be conducted on the installed system at commissioning. It is normal to request details of proposed tests during the installation phase well before the commissioning phase is reached.

Technical equipment details should only be specified if it is reliably known that the specification will result in the desired system performance or a desired operating procedure for the system.

Technical specification may need to be specified when it is difficult to objectively measure performance. For example, a high resolution camera is difficult to define. Specifying 470 HTVL (Horizontal Television Lines) is clear and is not open to interpretation.

Maintenance Requirements

Most new equipment comes with some form of guarantee. This should be in favour of the system owner - not the installer. It is usual to have a defects liability period that should commence following successful commissioning even though use of the system may be possible before that date. Avoid defect liability periods that commence on 'practical completion' because 'practical completion' can be vague. To protect against shoddy workmanship, avoid contracts that require money to be paid before commissioning. It is good practice to withhold monies until the end of the defects liability period.

Ask tenderers to quote for maintenance at the time of tendering. Maintenance may be required during the defects liability period - ensure that this is defined. The amounts quoted for ongoing maintenance can give clues to the level of workmanship the contractor proposes to maintain during installation. A reluctance to quote for say five years maintenance or a high maintenance quote could indicate shoddy workmanship can be expected - the contractor should know how much ongoing care his installation will need. Always have a clause to allow you to obtain maintenance elsewhere. For this reason avoid being locked into proprietary equipment that can only be expanded, serviced and maintained by the original contractor, supplier or agents.

It is usual to enter into a comprehensive maintenance contract where all failures or defects are rectified under the terms of the contract. The maintenance contract should place the onus on the contractor to take the responsibility for the entire system including systems supplied by others such as telecommunications, that is, make good or initiate action to make good any failure or defects. The maintenance contract should include performance parameters including time to respond - usually two hours during business hours and four hours outside these times and a mean time to repair.

Project Management

General

Project management is a major consideration in a project of this complexity. Project management will be easier for a non-technical person if the specifications are based on performance. The main phases of the project are as follows:

- ⊕ Project definition - where the client establishes needs and parameters to be met;
- ⊕ Tender documentation - where requests for tender are prepared together with system and equipment parameters (specifications) are documented;
- ⊕ Tender evaluation - where competing tenders are evaluated against a prescribed criteria including compliance and value for money, tender evaluation should include references from existing users of similar equipment/installations and the observation of the proposed equipment in a operating under realistic conditions;
- ⊕ Awarding of tenders and signing of contracts;
- ⊕ Detailed design by the successful tenderer to be reviewed by the client/project manager before installation commences - the contract should allow the client to discontinue after this phase for any reason the client chooses;
- ⊕ Installation plan - where the contractor sets out how the system is to be installed, at what times (including day and night) he/she will require access to sites, what form of trenching will be required and where, what machinery is required on site and what damage might it do or interruption (noise) it might cause, what form mountings including poles etc., will be required and where, when testing will be conducted and what form and level of involvement is required from the client and parties on whose property installation elements are to be placed;

- ⊕ Installation - where the system and equipment is installed, configured and adjusted;
- ⊕ Training - training should occur at this point, prior to commissioning to ensure that operators are ready when the system comes on line;
- ⊕ Commissioning - where the system and equipment is proven to function and perform to the client's satisfaction (in accordance with what was specified) for acceptance;
- ⊕ Payment - part payment should occur here with agreed amounts withheld until after the defects liability period;
- ⊕ Defects liability period - where all defects are rectified and all latent defects are noted for rectification at the installer's expense should failure occur soon after the defects liability period.
- ⊕ Ongoing maintenance - where the system is maintained in accordance with original equipment suppliers' and the installer's recommendations.

Two areas that require considerable supervision are system design and cabling installation. Design is the basis for the system installation and if not sound will result in an inferior system. Cabling is critical because it is normally out of view and performed by people with limited skills. Cabling discipline is paramount particularly when there are other system cables in the vicinity. All cable runs should be tested during installation and the test results for continuity, signal strength, signal noise ratio, etc., made available to the client for scrutiny by an expert before the system is accepted. Cables must be adequately supported and protected from accidental (including from vermin) and deliberate damage.

Project cost control

Project cost control is an essential element of project management. A fixed price contract is fundamental to this end. It is important to be sure of system requirements before contracts are signed to avoid variations which can attract higher than expected costs. Variation costs can be controlled better if the contract is written in a manner that specifies how variations are to be costed. The contractor should be asked to provide a breakdown quote costing all significant components and assemblies on a per unit basis installed and cabling on a per metre basis installed. The contract should then stipulate what amounts shall be deducted if the component, assembly etc is not installed and conversely, the cost of extra components, assemblies etc.

Proprietary equipment, that is, equipment that is available to one or a few installers or needs special training or equipment to install or maintain, should be avoided. It is far better to insist on equipment that is available to many different installers that can be maintained by many also.

Limiting access to sites where components of the system are to be installed comes at a cost. The contractor should be able to work a normal business day around your scheduled events and activities, To avoid disputes over delays and claims for extra payments, known scheduled events which must be worked around and site access restrictions should be provided to the tenderers with the tender documentation.

Be wary of any works supplied on an hourly rate unless the total time is capped or has some other satisfactory constraining clause.

Be wary of any quotes for trenching, cabling and structural works that leave costs open ended. Examples include allowances for unknown rock in trenching or extra foundations because the ground may be *discovered* to be unstable.

Identify the level and competency of project supervision for installation quality and works safety by the contractor and insist that it is provided.

Never enter into a payment agreement that provides for equipment to be paid for on invoice. All components should be installed and operational before being paid for.