TAPA FSR CCTV Systems Guidance V1

A TAPA Facility Security Requirements Guidance Document for users of TAPA Standards

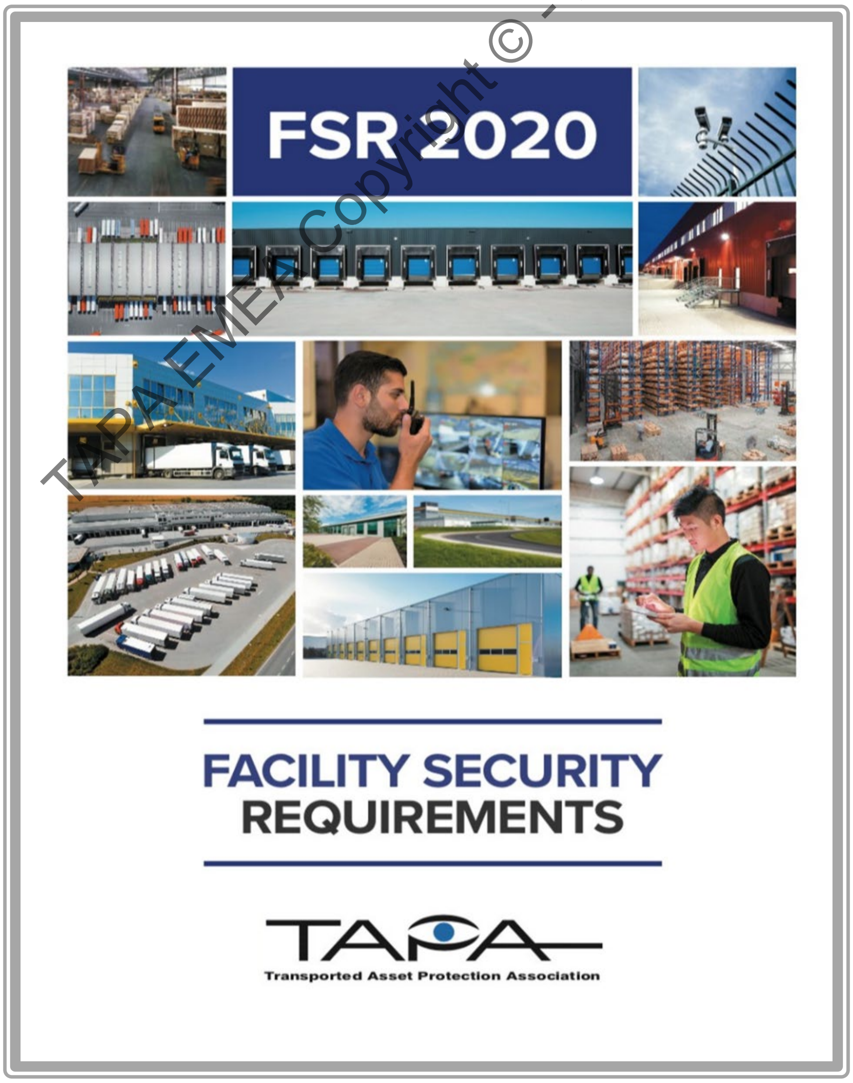
www.tapaemea.org

TAPA EMEA
Pastoor Ohllaan 39
3451 CB Vleuten
The Netherlands

info@tapaemea.org
Tel. +31 619 573 461

TAPA does not represent nor warrant that the information contained in this document will prevent any loss, damage or injury to a person or property, because of burglary, theft, hold-up, fire or other cause, or that the information will in all cases provide the protection for which it is intended. If the reader chooses to use any information in this document, they assume all risk and liability for doing so.

CONTENTS



FSR 2020

FACILITY SECURITY
REQUIREMENTS

TAPA
Transported Asset Protection Association

1. Introduction

CCTV is not only a constantly evolving arena with new innovations leading to continued product development and emerging technology, CCTV is also a recognised component of security systems deployed to protect logistic facilities against criminal activity, and as such CCTV Systems are an integral part of the TAPA Facility Security Requirements (FSR) Standard.

TAPA has produced this CCTV Systems Guidance (CSG) to provide helpfully supporting information on CCTV systems for users of the TAPA Facility Security Requirements (FSR) Standard.

The purpose of this document is to:

- Provide guidance on how existing and emerging CCTV system technology can be used to meet FSR and wider operational requirements
- Provide additional detailed information on CCTV system solutions not covered in the FSR
- Provide users with CCTV system categories that will help in the selection and identification of suitable products.
- Provide examples of CCTV systems and their intended use

TAPA acknowledges CCTV technology is an area of continued innovation and as such this document will be reviewed and updated as necessary, providing FSR users with up-to-date information on CCTV systems. The latest version will be available to download from the standards section of the TAPA website.

TAPA has included images and information on products in the CSG. These commercially available products are considered examples of products that help protect workers, facilities, and their cargoes. Other products are available. TAPA does not endorse any of the products included in this document.
TAPA cannot specify which product is appropriate for a TAPA FSR security level.

2. About TAPA

Cargo crime is one of the biggest supply chain challenges for manufacturers of valuable and high-risk products and their logistics service suppliers.
The threat is no longer only from opportunist criminals. Today, organized crime rings are operating globally and using increasingly sophisticated attacks on vehicles, premises, and personnel to achieve their aims.

TAPA is a unique forum that unites global manufacturers, logistics suppliers, freight carriers, law enforcement agencies, and other stakeholders with the common aim of reducing losses from international supply chains. TAPA's primary focus is theft prevention using real-time intelligence andthe latest preventative measures.

TAPA's Mission:

TAPA EMEA

The leading industry association for supply chain resilience & security professionals

TAPA's mission is to help protect members' assets by minimizing cargo losses from the supply chain. TAPA achieves this through the development and application of global security standards, recognized industry practices, technology, education, benchmarking, regulatory collaboration, and the proactive identification of crime trends and supply chain security threats.

3. Facility Threats and Risk Assessment

Understanding the threat to supply chain facilities is fundamental to designing security systems and countermeasures.
TAPA acknowledge each member will have their own risk assessment process and as such TAPA is not specifying any approach but suggests areas that should be considered for inclusion.

Risk assessment

Most security practitioners will advise the use of a risk assessment process to help/select the countermeasures that can help mitigate the threat of theft to an acceptable level.

A risk assessment process should seek to understand.

- The threat faced – who, how or what will impact the facility, its employees and assets.
- The likelihood of an incident occurring.
- Crime Intelligence Data – Review cargo and local crime statistics available from LEA's and other local sources.
- The consequence or impact of an incident occurring.
- Impact on employees or security guards – personal injury or mental health
- Financial losses. Cargo value; loss of revenue
- Supply chain disruption.

Risk assessments should be:

- Revisited annually.
- Following a change in facility usage or assets held at the facility.
- As a result of an incident.

The selection of a suitable CCTV system should be aided bythe risk assessment process.

- What features/protection the CCTV system must provide.
- The consequences of the CCTV system being defeated.
- Does the CCTV system complement the measures that support the protection of the facility and assets?
- Supporting procedures that allow for incident management and emergency response.

And in terms of the technical part of CCTV Systems:

- Camera field of view: Do they reflect changes to the physical/threat environment?
- Data: Does the image quality being captured meet the needs and support risk reduction?
- Changes to local laws or data privacy guidelines: Is the system compliant?
- Giving each camera a job description to ensure that each camera specification is in line with the function it is required to fulfill.

Facility Threats

The threat to a facility can come from a person or group who intentionally causes harm or chooses to act with malice.

This threat can include theft, but also disruption to the facility or supply chain. Action from protesters or activist groups can have a significant impact on a facility but the measures employed to minimise the threat would be similar to that of deterring theft.

The external threat.

Just as security professionals complete risk assessments to protect cargo. Criminals are also carrying out their risk assessment and hostile reconnaissance of a planned target.

Is the risk of being caught worth the potential reward?

When it comes to attacking facilities, criminals do not like to be spotted, take too long to access their target cargo, or be interrupted. In most incidents, organized criminals will have the knowledge to:

- Attack the facility when it is at its most vulnerable.
- Access the facility by defeating or avoiding the physicalmeasures in place.
- Have a plan for neutralizing or ignoring any electronic sensors they knowwill be in place.
- Calculate how much time they need to complete their operation and make their escape with their targeted cargo.

The opportunist threat.
Security systems and processes are subject to human error or system faults, where this occurs opportunists can take advantage of the situation and commit crimes. Security systems and physical security measures should be maintained and tested regularly to minimise the risk

The internal threat
Often underestimated, the insider is a person from within the Logistic Service Supplier who uses their legitimate access to commit a malicious act or provide the information required by criminals to gain access to the facility or assets.

As the insider is aware of the security measures at the facility, identification of an insider is difficult, and it is an unfortunate fact that employees' collaboration with criminals is still a common risk.

Regular audit of security system data such as access logs is important to identify misuse or trends. Scheduled changing of access pin codes and physical key audits can help deter insider activity. Procedures that control shipping information or access to the cargo are also important factors to consider in protecting the cargo from an internal threat.

Suitable and sufficient management systems
Management commitment to support security policy and procedures that enforce the mitigation options selection should be in place as standard practice.

4. CCTV Systems

The context of this section is to overview what a CCTV system is and the principal considerations of what it can do for a logistics asset. CCTV innovation has greatly advanced in recent times, and it is important to understand what the basic principles are and what they can do.

CCTV systems - Designing out the risks or: Why do we use CCTV systems in our facilities?

There are 4 main reasons for using CCTV as a security risk mitigation measure in our facilities:

- To deter criminal activity such as theft
- To monitor suspicious activities (either in real-time or offline)
- To record evidence for post-incident investigations
- To keep a tab on activities and identify potential security risks

CCTV systems should be designed to assist in supporting the basic security principles of deterring, detect, delay, respond and when used in conjunction with additional security measures such as Perimeter Protection; Lighting; Intrusion Detection and Access Control it can provide a high level of confidence in the security design.

Poorly designed or maintained security systems will invite the attention of criminals. It is through good design and planning that a deterrent can be introduced that helps prevent or minimise impacts of cargo loss.

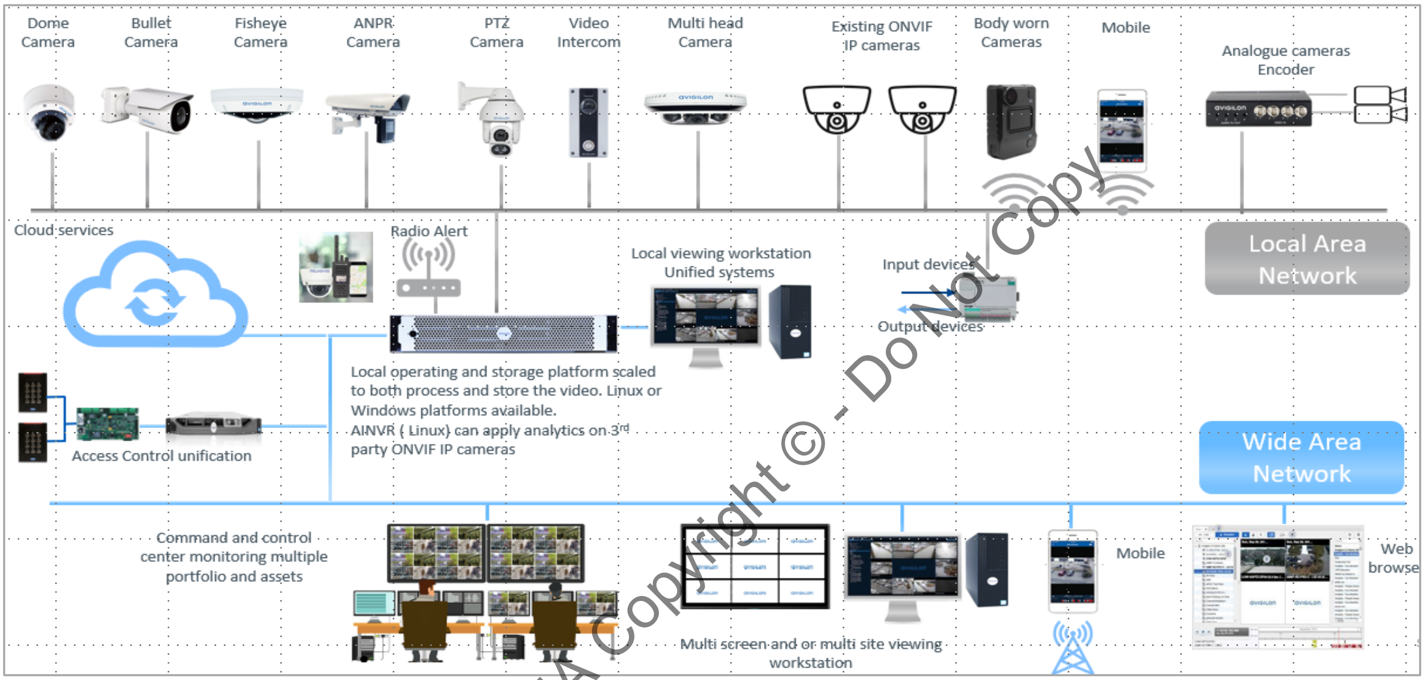
Organised criminal groups adapt and change their approach to counter any security systems they face. Reviewing risk assessments; the effectiveness of the systems and processes deployed when completing the annual FSR audit helps stay ahead of the criminals.

What is CCTV, or closed-circuit television?

In general, it's a system that allows you to keep an eye on whatever is ongoing in and around your business. The cameras, monitors and recording devices you had installed for such a system will allow you to view events, live or later via the recorded footage.

Within a CCTV system, multiple sorts of cameras and other equipment can be used.

The below figure shows a sample of how a professional CCTV system can be set up. In reality, CCTV systems for logistic providers can look less complicated but with most of the same sort of elements used as cameras, recording devices and monitoring

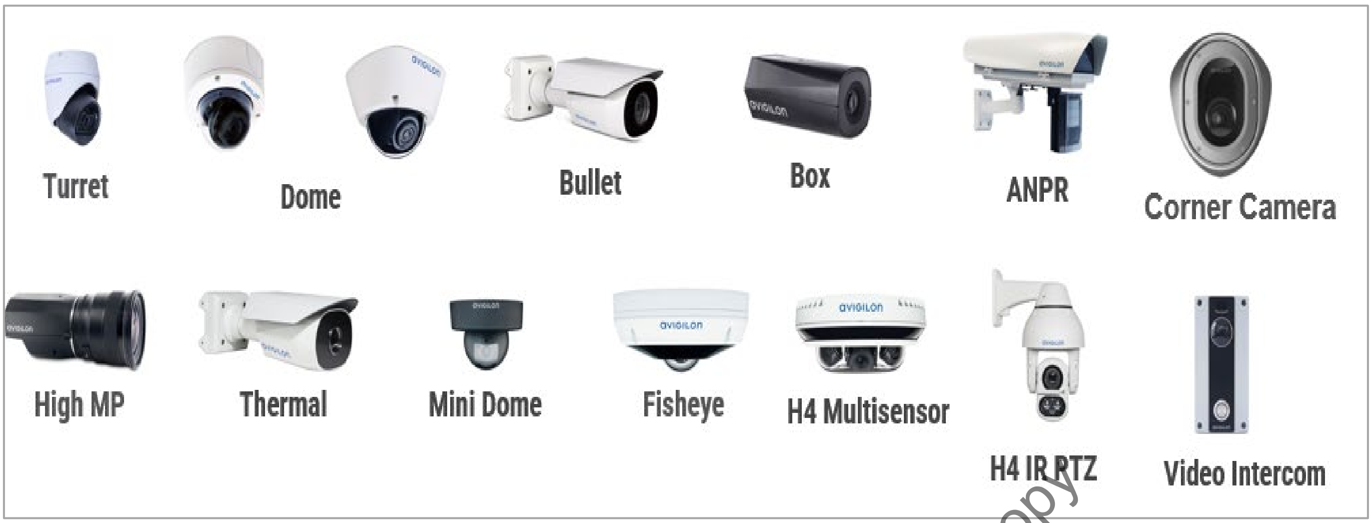

Dome Camera
Bullet Camera
Fisheye Camera
ANPR Camera
PTZ Camera
Video Intercom
Multi head Camera
Existing ONVIF IP cameras
Body worn Cameras
Mobile
Analogue cameras Encoder
Cloud services
Radio Alert
Local viewing workstation Unified systems
Input devices
Output devices
Local Area Network
Local operating and storage platform scaled to both process and store the video. Linux or Windows platforms available.
AINVR (Linux) can apply analytics on 3rd party ONVIF IP cameras
Access Control unification
Wide Area Network
Command and control center monitoring multiple portfolio and assets
Multi screen and or multi site viewing workstation
Mobile
Web browse

Camera form factors

A logistic centre is a challenging environment for cameras, considerations will include physical protection of devices, space and access considerations or available lighting. HD Cameras are integrated units with compact profiles with a powerful MP range that doesn't need the physical size to increase to address Logistics sites range generally.

The form factors of cameras are a variation on the key types below.

Most cameras will come with built-in IR (Infrared) options, and these should be taken in most instances to account for local lighting failure, other elements such as Wide dynamic range (WDR) are a consideration to assure backlighting does not affect the image in areas of wide light change (door openings /shutter areas etc).



Analog cameras:
Have been around for years and are still the most common type of CCTV camera installed today. They have basic functionality and store video onsite. However, the trend shows that IP cameras are becoming a more popular option in new installations.

IP (Internet protocol) cameras:
Carry out the same functions as their Analog counterparts, but with vastly greater capabilities. IP cameras boast sharper, higher resolution images and more flexible features like remote zoom and repositioning. They also give you the option to view footage on a web browser or mobile device.

Cabling:
All CCTV systems require some amount of cabling, even those with wireless cameras. Cables link different pieces of equipment together, including monitors, recorders, modems, and wired cameras. When using analogue cameras, it is good practice to keep the coax cable running less than 300m and 80m or less in IP installations. The cable run can also effect the power to the camera so cable runs that are too long can cause power losses to the camera.

Video recorders:
CCTV systems store image data captured on a dedicated recording system, or in some cases hold the images on a storage device embedded within the camera itself.
Cameras can be set up to record all images captured, but this will take up a lot of storage space particularly if you are retaining data for long periods.
Cameras can also be programmed to record only during certain times of the day or when they detect movement. Video recording options include **DVR** and **NVR.**

DVRs, or digital video recorders, are the modern replacement for analogue recorders that use videotapes. DVRs capture footage from analogue cameras in a digital format at the desired resolution and frames per second. When the hard disk gets full, new images will record over the oldest footage first.

NVRs, or network video recorders, work similarly to DVRs, but they're compatible with IP cameras. Your cameras and NVR connect via a network switch or router. You can easily access footage on an NVR through a web browser or mobile app.

Display unit:
CCTV images can be viewed on single or multiple screens depending on your requirement. If you have IP cameras, you can also view footage remotely from a smartphone or computer.

But installing a CCTV camera doesn't mean you're automatically safe; Within the FSR requirements, TAPA will explain what the performance should be from such a system to be compliant with TAPA FSR. FSR provides a minimum requirement for CCTV so it is important to consider other operational requirements such as safety considerations within your solution design.

- **Deciding how you'll be monitoring the system:**
  If you decide to monitor your system using the Internet, getting an IP Address for your Digital Video Recorder (DVR) or NVR will equip it to survey and record easily; an Ethernet cable carries all information via the Ethernet switch.

- **Determining the number of Cameras required:**
  Depending upon the nature of your requirement and the expanse of the area you want to protect, (in line with the TAPA FSR standards), decide on the number of cameras required to ensure complete security.

- **Positioning the CCTV cameras:**
  TAPA FSR requirements dictate areas CCTV cameras must be present to comply with the standard however it is important to remember factors that could impact the camera and images being viewed/recorded
  - Exposure to extreme weather conditions such as rain, glare from sunlight etc.
  - Glare from lighting
  - Landscaping such as trees

- **CCTV System Protection:**
  It is paramount to secure the digital video recorder (DVR) or the network video recorder (NVR) ensuring image data is secured.

- **Deciding on power backup of CCTV Camera:**
  - The CCTV system requires a constant power supply
  - Ensure power cannot be tampered with or switched off unintentionally
  - Consider a UPS backup (uninterrupted power supply) for the security system in the event of a localised power failure
  - would ensure incessant surveillance. Thus, make sure you have both a constant power supply and a reliable power backup in case of power cuts to ensure security at all times.

- **Post Installation Testing:**
  After you’re done with the installation process, it is very important to fully test the system.
  - Has the installer delivered on the brief?
  - Are the CCTV images as expected day and night?
  - Are the cameras focused correctly and recording images?

  - Do the cameras meet local data protection laws and if not, can they be moved, or images redacted to meet the requirement of the laws?
  - Are the cameras and the cables safe from tampering?

- **Maintaining the CCTV cameras:**
  Best practice
  - Daily system functionality checks
  - Regular camera cleaning removing dirt or cobwebs
  - Annual (FSR minimum requirement) maintenance inspection of the CCTV System
  - Agree supplier call-out response time and service schedule

Quality in cameras: how to choose the right security camera?

Although often such advice is given by the installation company used, it's important to understand what makes any camera the best for your facility. Choosing the right camera or cameras is the most complex decision in any video surveillance project.

There are different types of cameras that can be classified by various technical aspects, such as whether they are motorized or not, or whether they allow night vision or not. On this occasion, we are going to focus on another fundamental aspect that directly refers to the quality of the captured image. By knowing what each camera is supposed to do and giving it a job description will make it easier to ensure the correct camera is selected. The location of the camera can also determine what specification the camera must have for example sunrise and sunset times. There are cameras that automatically compensate for the light change (WDR).

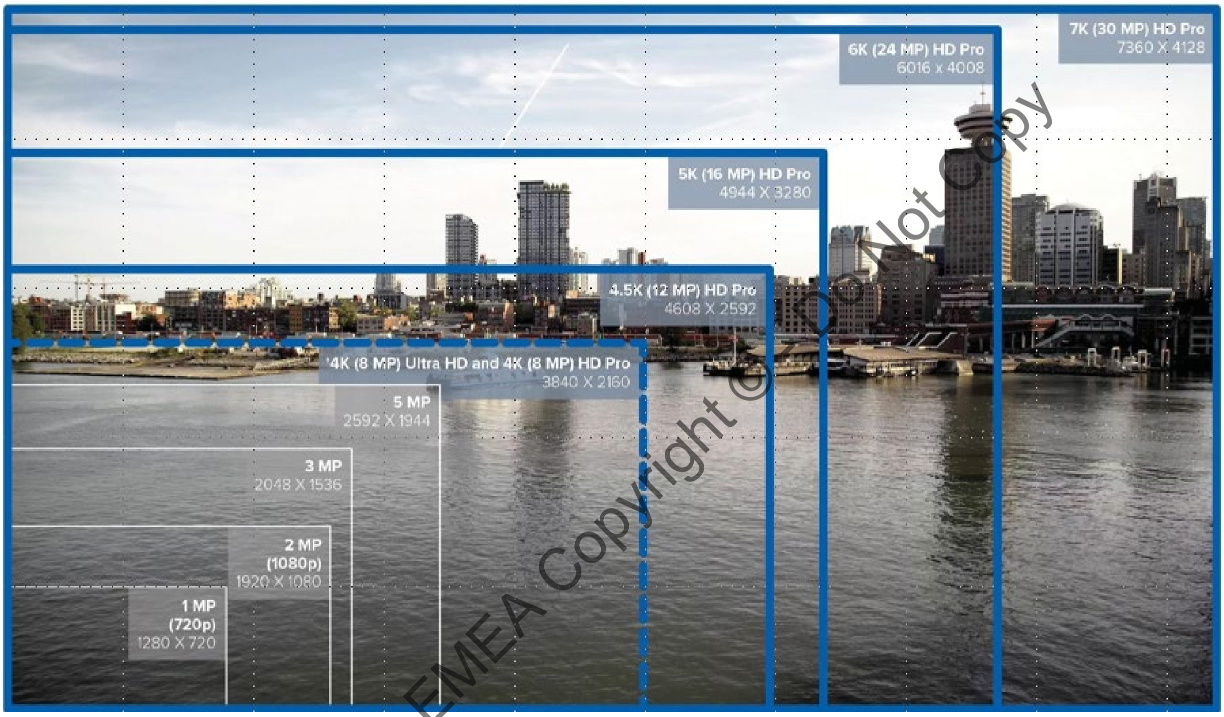
What is image resolution?

The resolution of an image indicates the level of detail that can be observed in it.

Resolution is measured in pixels, specifically in columns of pixels (the width of the image) and rows of pixels (the height of the image). The greater the number of columns and rows of pixels, the higher resolution said image will have, the greater the level of detail it will be able to offer us.

When we multiply that number of pixel columns by the number of pixel rows, we get the unit of measurement in millions (mega) of pixels. So, for example, suppose we have an image 1500 pixels wide by 1200 pixels high. We would have an image with a total size, a resolution, of 1,800,000 pixels, which if we go to a million, would be 1.80 megapixels.

Megapixel (MP) Comparisons



In the image above, the contrasted viewing coverage can be seen ranging from a small area with a 1Megapixel camera to a vast area with 30MP. The context for logistic sites is that high positions can often be achieved on buildings and lighting columns. This enables greater area coverage (internally and externally) to be achieved and with fewer cameras.

IP cameras need little manual servicing as camera setup can be done at the camera, column base, at the operator control position or remotely (subject to IT security parameters) so optimum and ideal coverage is now achievable with less compromise due to camera access concerns.

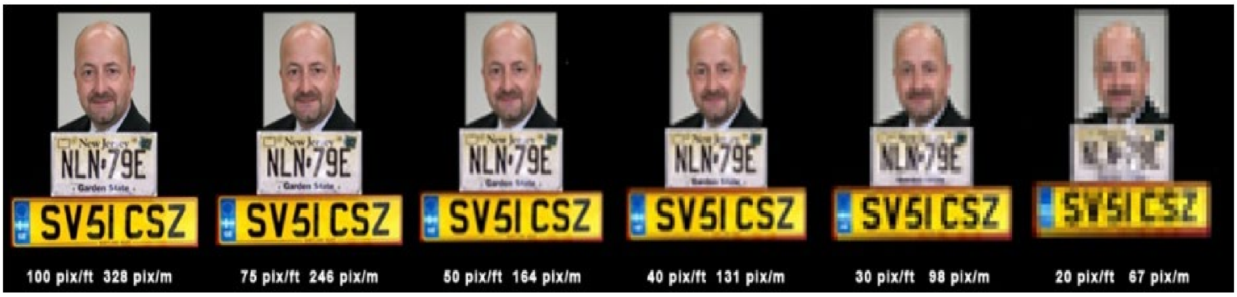
Typically, this reduces busy camera count, with camera location intensity now limited to areas with reduced line of site (internal hallways etc)
IP cameras capture video images, compress, and transmit them in digital format over the network. The recorder is programmed with IP addresses to receive these video streams and record them to NVR (network video recorder). Typically, HD Cameras range from 2mp, with advanced manufacturers having currently up to 61 MP units. These have revolutionised Video observation with the ability to do more with less camera. Typically, IP cameras are PoE (Power over Ethernet) so reducing infrastructure cost versus mains requirement on previous camera types.

Megapixel density now prescribes camera relationship to the target, so the distance and definition of target outcomes can now be clearly prescribed, and it would be recommended that any solution offered has a design tool plot to assure the level of coverage and fixed camera viewing zoom for both live and recorded images.

It is also important to assure that appropriate ambient area lighting is available in the camera’s view. It would be anticipated that with good quality cameras aligned with site lighting as a health and safety requirement for logistics sites general site coverage is enough with ancillary lighting at the edge or shadowed areas.

Consideration should also be given to vegetation management particularly on perimeter lines to assure cameras are not obscured. Thermal imaging cameras could be a consideration for areas where lighting would be problematic (light pollution adjacent to private housing). Similarly, overshoot into other premises must be avoided where deploying longer-range camera views.

The example below defines the context of megapixel density, however, note, that the relevant density of say could be achieved with a 2-3 megapixel at a short range, raising the camera megapixel spec for longer ranges



Change Management

Internal change controls are an important part of an organisation's risk management programme, especially where changes to the operating environment, facility layout, usage, asset value and desirability create additional security risks.

From the outset, supply chain risks, likelihood and impact are factors that most warehouse, transport and logistics providers want to assess. In doing so, they seek to minimize the risks associated with supply chain disruptions, security incidents, the unavailability of goods through theft or other malicious acts, and potential damage to an organisation's brand or reputation.

The methodology employed, typically referred to as a risk assessment examines both general and specific threats, vulnerabilities, asset criticality, likelihood, frequency, and impact. Ultimately, the aim of an organisation's assessment programme is to mitigate its known security risks to a level commensurate with its risk appetite.

Facility buildings support many different types of operations and workplaces. The definition of a workspace varies widely according to its function and may range from offices to warehouses, loading bays and product storage areas. Depending on its use, each area offers different levels of inherent risk, both for the organisation and its employees.

Understanding the functionality of a building, how and where organisational assets are stored, handled, and transported forms an integral part of the facility risk and change control assessments. Facility buildings may also be multi-occupancy, consisting of private and common access areas, which equally need to be managed.

Asset criticality or value is often determined by a range of factors including:

- The cost of purchasing or replacing the asset.
- The commercial impact of an unavailable asset when it is stolen.
- The effects of harm to the asset.
- The length of time required to manufacture and/or replace the asset.
- The impact on an organisation's reputation or brand, where the asset can't be delivered to a customer.

Whilst many certified businesses correctly apply TAPA's Facility Security Requirements to their facilities, over time operational changes outlined above may impact its ability to protect its critical assets. One example might be where critical assets monitored by the facility CCTV system have been moved to an area without camera coverage. Similarly, a newly constructed internal wall might now block the view of existing CCTV cameras monitoring a high-value storage area. In both cases, the effectiveness of the security protection has been reduced, thereby increasing the likelihood of a successful targeted attack against the asset.

Most organisations employ some sort of change management process. The facility CCTV system needs to be an integral part of this process because as we've just seen, new vulnerabilities may be introduced because of systems or environmental change. Wherever possible the security responsible person should identify the organisation's change management controls and establish a notification process when a change impacts security. A regular programme of security testing will also help to ensure the site's CCTV camera systems are necessary, relevant and proportionate to the level of assessed risk.

5. FSR Overview

CCTV systems are an important layer for protecting facilities, the people in and around the facilities and the cargo being stored or moved through the facilities. However, it should be clear that they are just one of many countermeasures to be considered when selecting the deterrents and physical security measures to protect employees, vehicles, facilities and stored cargo. Therefore, TAPA recommends to its members and the industry to adopt TAPA FSR as the standard for logistic facilities. Achieving TAPA FSR certification means that the facility has been approved by an accredited certification body (IAB) for FSR Level A-C or via a self-audit by authorised auditors (AA) by TAPA LSP/Applicant for FSR Level C.

The FSR requires a layered approach to protecting facilities and includes:

- Scalable security levels to assist the facility owner in the selection of riskmitigation countermeasures.
- FSR Level C provides basic countermeasures and procedures that help to provide deterrents and protection for facilities from criminal interest.
- FSR Levels A and B provide more robust countermeasures and procedures and are more suited to protect high-value and/or vulnerable cargo.
- Where the facility is deemed to be at high risk then FSR can also be used for additional enhancements to cover IT/Cyber threat measures

TAPA FSR – CCTV systems and the FSR standard.

TAPA is not a testing and compliance organisation and therefore cannot certify, confirm, or reject any security products that are used to help facility owners meet the requirements of TAPA security standards.

Despite claims by some providers of CCTV systems, no CCTV systems have been certified by TAPA to meet TAPA standards.

This does not mean that suitable CCTV systems are not available, it just means TAPA cannot certify or endorse them.

Identifying CCTV that meets or exceeds TAPA FSR requirements can sometimes be a challenge for auditors and end users. This section will seek to explain the features and capabilities that a CCTV system is required to meet as part of the FSR certification audit.

TAPA CCTV FSR Guidance

Why?

Applying the 'defence in depth' principles (deter, detect, delay, mitigate, respond), CCTV cameras when used in conjunction with other security systems form a vital part of the location's overall security protection measures.

CCTV coverage to provide general oversight of open space. This will enhance the site's situational awareness and help detect potential issues before they occur.

- Monitor pedestrian and vehicle movement routes.
- Tracking people, vehicles, and assets around the site.

Deter

The presence of CCTV camera systems is likely to deter intruders by making the facility perimeter appear too physically/technically difficult to breach, thereby increasing the probability of the attacker's detection, failure and/or capture.

Visual deterrents may include the display of signage on the outer perimeter fence line highlighting the use of CCTV cameras and security lighting.

Detect

Using CCTV cameras to identify suspicious activities within the facility's external cargo handling, shipping, and receiving areas include:

- The early detection of intruders as they cross the outer perimeter boundary.
- Visual verification of perimeter intrusion alarms and alerts.
- To raise the alarm and to initiate further investigations and/or escalation.
- Initiation of an appropriate response to the perceived threat.

- Most systems now have the ability to detect movement and/or in specific directions and alert controllers or remotely.

Delay

The presence of CCTV camera systems in conjunction with other physical barriers, including secure access, loading bay and driver reception doors maximise the time taken for an attacker to breach the building's security once detection has occurred.

Where intruders have already breached the outer perimeter and gained access to the facility's cargo handling, shipping, and receiving areas, CCTV cameras provide visual verification of the attack force, including information about their numbers, the use of a getaway vehicle, possession of any weapons, prohibited articles or tools.

Mitigate

The use of perimeter protection measures, including CCTV to minimise the impact of an attack.
Maximize the protection provided to access points at the perimeter.
Facility warehouse external cargo handling, shipping, and receiving yard areas are generally located in a zone between the outer and inner (building) perimeter boundaries. Operational activities typically include the loading and unloading of products, shunting and vehicle marshaling. For this reason, they are busy workspace areas.
Threats may include the presence of onsite intruders, illegal migrants (from a trailer incursion), insider threats (rogue employees) or other unauthorised personnel in the area.

Response

Use of CCTV and other perimeter detection systems to determine where/if an attack is taking place.

- Allocation of resources to deal with the threat.
- Law enforcement response.
- It is important that the response time is less than the time of detection and the time of breach.

7.1.1 Warehouse External Cargo Handling, Shipping & Receiving Yard.

Warehouse External Cargo Handling, Shipping and Receiving Yard (General)	
7.1.1	CCTV able to view all traffic at external cargo handling, shipping, and receiving yard (including entry and exit point) ensuring all vehicles and individuals are recognisable at all times, unless temporary obstruction due to operational needs (i.e., truck loading and unloading in real time).

Why?

Even though not all TAPA FSR Certification levels mandate a physical perimeter, it is quite important for a facility operator to be able to view via CCTV the area surrounding the warehouse building and the handling areas, as well as to recognize approaching and leaving vehicles and individuals.

Risk

A lack of CCTV compliance in this key risk area may result in

- The undetected presence of a site intruder
- Unavailability of evidence to support claims or investigations.

External Dock Doors

External Dock Doors	
7.1.11	External dock areas covered via colour or "day/night" exterior cameras
7.1.12	Cameras mounted to be able to view all operations and movement around external dock areas at all times unless temporary obstruction due to operational needs (i.e., truck loading and unloading in real time).
7.1.13	All vehicles and individuals around dock areas clearly recognisable.
7.1.14	Vehicles and individuals around the external dock area are visible in most cases.

Why?

External dock doors are used to facilitate the delivery/collection of finished goods, product packaging and raw materials. For some facilities, the presence of external dock doors allows direct access into the warehouse, production, or storage areas, thereby increasing the likelihood of a successful targeted attack against its protected assets.

CCTV Cameras deployed in external dock areas shall be of sufficient quality to provide recognisable day/night images of vulnerable areas outlined within the TAPA FSR Standard.

An image is recognisable if the user can identify an individual by their demeanor, mannerisms, clothing or a vehicle by its registration plate number, model, color and branding.

CCTV images are important in the recognition of site intruders, the identification of suspicious or criminal behaviour and to prevent the loss of company property. Real-time images allow the security team to make dynamic risk decisions based on the events being viewed.

Gaps in camera coverage mean security incidents may be missed. Camera quality concerns also introduce question marks over evidential quality and image integrity.

Risk

Where CCTV cameras are not deployed within these critical areas to meet the required TAPA's Facility Security Requirements level,

- Risk of an undetected intrusion event, resulting in serious injury or harm to a company employee.
- Unauthorised access to a restricted area or asset
- Theft
- Product interference
- Safety violation
- Unavailability of images for post-incident investigation

Outside Walls, Roof and Doors

7.2	Outside Walls, Roof and Doors
Exterior sides of the facility: CCTV	
7.2.1	Colour or "day/night" exterior camera system in place covering all sides of the facility.
7.2.2	Colour or "day/night" exterior camera system in place covering exterior sides of facility doors, windows, or other openings
7.2.3	All views of exterior cameras clear at all times unless temporary obstruction due to operational needs (i.e. truck loading and unloading in real time).
7.2.4	All vehicles and individuals clearly recognisable at exterior camera system
7.2.5	Vehicles and individuals visible in most cases at exterior camera system

Why?

Applying the defense-in-depth principles, the exterior facility sides typically represent the inner perimeter boundary line. Within this inner perimeter are often located the businesses protected assets. At risk, areas include facility windows (ground & lower floor), walls, roof, and doors. Attackers will target these vulnerable areas, as they often represent the path of least resistance to achieving their goal.

The presence of CCTV cameras in these key areas allows for the:

- Early detection of intruders as they cross the inner perimeter boundary.
- Visual verification of perimeter intrusion alerts.
- To raise the alarm and to initiate further investigations and/or escalation.
- Initiation of an appropriate response to the perceived threat.

CCTV cameras deployed within these critical areas will both capture these events and mitigate the security risk down to acceptable levels. Gaps in camera coverage mean security incidents may be missed. Camera quality concerns also introduce question marks over CCTV evidential value and image integrity.

Risk

Where TAPA's Facility Security Requirements are not met at the required level, there is a risk of

- Undetected intrusion event,
- Unauthorised access to information or other protected assets,
- Theft,
- Safety violation.
- Unavailability of images for post-incident investigation

Office and Warehouse Entry and Exit points

Office area Visitor Entry Points (s)	
7.3.2	Office area visitor entry point (s) covered by CCTV; (color "day/night" cameras) individuals clearly recognisable at all times.

Why?

Office and warehouse entry/exits points are typically the main entry points through which company employees gain access to the site's protected assets. The deployment of CCTV cameras in conjunction with other security systems ensures building access is both controlled and monitored, thereby mitigating the risk of a successful targeted attack.
Additionally, the setup of a CCTV system according to the above requirement facilitates the recognition of visitors in real-time or at a later date.
CCTV cameras deployed within these critical areas will both capture these events and mitigate the security risk down to acceptable levels.
Gaps in camera coverage mean security incidents may be missed.
Camera quality concerns also introduce question marks over CCTV evidential value and image integrity.

Risk

Where TAPA's Facility Security Requirements are not met at the required level, there is a risk of

- Undetected intrusion event,
- Unauthorised access to information or other protected assets,
- Theft,
- Safety violation.
- Unavailability of images for post-incident investigation,

Workforce Entry Points

Workforce Entry Points	
7.3.10	Workforce entry point (s) covered by CCTV; (color or "day/night" cameras).

Why?

CCTV Cameras deployed at workforce entry points shall be of sufficient quality to provide recognisable day/night images. An image is recognisable if the user can identify an individual by their demeanor, mannerisms, and clothing.

CCTV images are important in the recognition of site intruders, the identification of suspicious or criminal behaviour, insider threat and theft. Real-time images allow the security team to make dynamic risk decisions.

Recorded images assist with the investigation and detection of crime. Additionally, the setup of a CCTV system according to the above requirement facilitates the recognition of drivers and employees in real-time or at a later date, in order to trace the entry and exit points. CCTV cameras deployed within these critical areas will both capture these events and mitigate the security risk down to acceptable levels. Gaps in camera coverage mean security incidents may be missed. Camera quality concerns also introduce question marks over CCTV evidential value and image integrity.

Risk

Where TAPA's Facility Security Requirements are not met at the required level, there is a risk of

- Undetected intrusion event,
- Unauthorised access to information or other protected assets,
- Theft,
- Safety violation.
- Unavailability of images for post-incident investigation

Driver and Vehicle Identification

Driver and Vehicle Identification	
7.3.17	Vehicle identifiers are logged manually (i.e. written) or with cameras. Include at a minimum licence plate and vehicle type.

Why?

The presence of CCTV cameras at vulnerable vehicle entry points ensures truck identifiers, such as the vehicle model, color, branding, and registration numbers are viewed both in real and recorded time. When combined with other security systems, such as barrier and access control, CCTV cameras provide a vital element of the facility's overall security protection systems.

Facilities are at risk from both petty (opportunistic) and organised crime activities, where attackers use a variety of fraud techniques including the use of false company, truck, and driver identities to steal from businesses.

The presence of effective entry controls combined with effective CCTV cameras and identity verification systems ensures the risks associated with a fraudulent collection are mitigated to acceptable levels.

Risk

The absence of CCTV cameras in this area, means vital evidence may be lost and/or missed. The resultant losses may be both financial (in terms of the value of the goods stolen) and reputational in respect of the impact on the company brand. Once stolen goods may also be sold on the 'black market' with consequential quality and consumer risks.

Internal Dock Doors and Dock Areas

Internal Dock Doors and Dock Areas	
7.4.4	All internal dock doors and dock areas covered by CCTV. (Color or "day/night" cameras).
7.4.5	Views of freight being loaded/unloaded at all internal dock doors and dock areas, clear at all times unless temporary obstruction due to operational needs (i.e. truck loading and unloading in real time).
7.4.6	Buyer assets under 100% CCTV surveillance in cargo movement or staging areas (i.e. pallet breakdown/build up areas, routes to and from storage racks, dock, transit corridors).

Why?

There are several reasons for this requirement, addressing both mal intended activities as well as identification of misplaced goods that might not reach their destinations and claims that might be initiated by customers.

If we take out the real-time or post-incident identification of intruders (i.e. with Video Content Analysis alarming functionality or with real-time CCTV monitoring), this requirement, if in place, might be proven very helpful:

- In case your customer raises a claim and you need to be able to prove that the sealing process has been applied correctly (you need to be very careful when you install your internal dock-doors cameras and also ensure that dock doors are closed after the sealing process is completed if you want to be able to take advantage of this functionality),

- Or that a specific pallet or package missing at the destination was actually loaded at the origin. Of course, you need to adapt the resolution of your CCTV system recordings if you want to take advantage of this capability, as well.

Risk

Where TAPA's Facility Security Requirements are not met at the required level, there is a risk of

- Undetected intrusion event,
- Unauthorised access to information or other protected assets,
- Theft,
- Safety violation.
- Unavailability of images to investigate
  - Undetected intrusion event
  - Vehicle loading/unloading & sealing processes
  - Customer claims

Inside Warehouse and Office

High Value Cage (HVC) /Area	
7.4.15	Complete CCTV (Color or "day/night" cameras) coverage on HVC entrance and internal area. *Note: If the HVC is too small to locate a camera inside, camera coverage of the entrance is sufficient.*
7.4.16	CCTV (Color or "day/night" cameras) coverage on HVC entrance.
7.4.18	HVC doors/gates are alarmed to detect forced entry. Alarms can be generated by door contacts and/or use of CCTV motion detection to detect unauthorized access.

Why?

As the High Value cage is the area whereby definition the most theft-targeted products are stored, it goes without saying that the entrances and the interior of the High Value cage need to be protected as best as possible.

In some cases, CCTV is also used with motion detection functionality to alarm these cages.

Risk

Where TAPA's Facility Security Requirements are not met at the required level, there is a risk of

- Undetected intrusion event to the HVC,
- Unauthorised access to the HVC,
- Theft,
- Unavailability of images for post-incident investigation

Inside Warehouse and Office

Trash Inspection from Warehouse	
7.4.21	Internal and/or external warehouse main trash collecting bins/ compacting areas are monitored by CCTV.

Why?

One common way to carry small-sized goods from the warehouse, out of it, is by using the trash bins, usually, by employees. Having effective CCTV coverage of these bins can both assist in preventing or identifying losses executed with this modus operandi.

Risk

Where TAPA's Facility Security Requirements are not met at the required level, there is a risk of

- Theft,
- Safety violation
- Unavailability of images for post-incident investigation

Internal fraud and pilferage incidents can be prevented if this requirement is applied effectively, otherwise, losses associated with this modus operandi might appear.

Inside Warehouse and Office

Cargo Integrity; Loading/Unloading Validation Process	
7.4.32	Robust procedures are in place ensuring that all Buyer assets shipped and received are validated at point of handover by conducting a manual and/or electronic piece count. Process must ensure abnormalities are consistently recognised, documented and reported to the LSP/Applicant and/or Buyer. Manual and/or electronic records must be of evidential quality. If drivers are not present to witness this activity, Buyer/LSP/Applicant must ensure alternative count verification such as scans and/or CCTV images, collected and retained specifically for this purpose. *Note: In addition to missing pieces, abnormalities may include damage, missing straps or tape, cuts, or other obvious openings, indicating a possible theft or pilferage.*

Why?

In this case CCTV supports cargo counting during loading or unloading as an alternative method. The records by CCTV should be kept for as long as your customers have the right to claim for missing goods, so even if the standard requirement is 30 days min, you might consider expanding this duration if your customers can claim missing goods for more than 30 days, provided of course that there are no operational or legal restrictions.

Risk

Where TAPA's Facility Security Requirements are not met at the required level, there is a risk of

- Not being able to collect post-incident evidence for losses and customers' claims.
- Not being able to collect evidence of missing items during cycling or wall-to-wall inventory counts.

Security Systems; Design, Monitoring and Responses

CCTV	
7.5.18	Digital recording of CCTV in place.
7.5.19	Recording speed for CCTV is set as a minimum for 8 frames per second (Fps) per camera *Note: Tapa will allow existing certificate holders without the capability to upgrade to 8 fps to continue with existing 3 fps until the 2023 revision. New certificate holders must meet the new requirement*
7.5.20	Digital recording functionality checked daily on operational days via procedure. Records available.
7.5.21	CCTV recordings stored for a minimum of 30 days where allowed by local law. LSP/Applicant must provide evidence of any local laws that prohibit the use of CCTV and/or limit the video data storage to less than 30 days.
7.5.22	Access tightly controlled to CCTV system, including hardware, software, and data/video storage.
7.5.23	CCTV images, for security purposes, are only viewed by authorized personnel.
7.5.24	Procedures in place detailing CCTV data protection policy regarding use of real time and archive images in accordance with local law

Why?
Manufacturers of CCTV equipment no longer support analogue recording systems, therefore the recommended recording platform for FSR compliance is digital.
Digital recording provides

- Superior image quality which meets data protection legislation
- Higher capacity for data storage of images

Frames per Second (FPS) set at a higher frame rate results in smoother image playback of recorded images.

8 fps does not only enhance the quality of the video but also gives the capability to the CCTV system to capture more frames during an incident. For example, if there is a suspicion about an employee carrying a small smart-phone box out of the facility, and the employee is captured in the CCTV for 15 seconds running from the warehouse exit door to his parked car (50 or 60m away from the door), then with 8 fps the system shall record 8x15=120 frames, whereas with 3fps the system shall record 3x15=45 frames. As usually, the employee tries to hide the box, it is more likely to have a frame recorded the box when you have 120 frames compared to 45 frames.

Daily check of recording is necessary to ensure the effectiveness of the system. It is very disappointing and frustrating to realize that recordings are not available after an incident has taken place and an investigation has been initiated.

30 days of CCTV records storage is a requirement addressing the need for evidence availability in case of claims or losses that are either identified not in real-time (i.e. cyclic inventory counts, or destination claims of missing goods). You might consider expanding this duration if your customers can claim missing goods for more than 30 days, provided of course that there are no operational or legal restrictions.

As destruction or alteration of evidence is a common way for criminals to escape from identification, it is very important to protect the access of the CCTV system, including hardware, software, and data/video storage. This protection is both physical and electronic i.e., both the data rooms need to be physically protected and alarmed, as well as the software access either locally or in the cloud should be adequately and effectively protected. Management of access rights and passwords should be in place to ensure the proper application of this requirement.

Finally, personal data protection requirements, both legal and ethical) should be considered to ensure CCTV images, for security purposes, are only viewed by authorized personnel and that documented procedures are in place detailing CCTV data protection policy regarding the use of real-time and archive images in accordance with local law.

Local legislation should always be analyzed to ensure understanding is identical to the legal requirements and that we do not interpret the law according to our intentions.

Risk

Where TAPA's Facility Security Requirements are not met at the required level, there is a risk of

- Lack of adequate CCTV records to support investigations
- Lack of evidential quality CCTV recordings
- Intentional or unintentional deletion or alteration of CCTV records
- Legal implications

Security Systems; Design, Monitoring and Responses

CCTV	
Exterior and Interior Lighting	
7.5.25	Exterior and interior lighting levels are sufficient to support CCTV images that allow investigation and evidential quality image recording.
7.5.26	Exterior and interior lighting levels are sufficient to clearly recognize all vehicles and individuals.

Why?

Even though current technology supports video recording in the dark, it is always desirable to enhance the video recording capability with ambient lighting. As day-night cameras switch from color to black and white recording when the lighting conditions are not sufficient, CCTV is able to record even in the dark.

A rule of thumb related to the quality of recording and lighting conditions is that lighting for CCTV should be based on the inverse square rule: **if you double the distance to the subject being lit, you will need FOUR times the original light**. Additional lighting can be used to create an evenly lit scene in the camera's field of view, as this will ensure captured images are not too dark or washed out.

Experts recommend (not required):

- External light levels at the sides of the building need minimum of 5 Lux
- Loading/unloading area needs minimum of 50 - 100 Lux
- Parking /handling area close to the dock area needs minimum of 20 Lux
- Gatehouse/vehicle entrance area needs minimum of 100 Lux
- In the warehouse min 150 Lux

A good reference for this topic is included in the link below: https://www.anixter.com/content/dam/Suppliers/Raytec/Complete%20Guide%20to%20CCTV%20Lighting.pdf

Risk

Where TAPA's Facility Security Requirements are not met at the required level, there is a risk of

- CCTV images are not evidential quality hindering both real-time or post-investigation situations.

Requirements vs Risk Matrix

Req/Security Risk	Internal Fraud and Pilferage	Not real-time intrusion detection and alarming	Unavailability of CCTV to support claims or investigations	Legal implications	Deletion or alteration of CCTV records	Non evidential quality records
7.1.1		X	X			X
7.1.11 7.1.12 7.1.13 7.1.14 7.1.15	X	X				X
7.2.1 7.2.2 7.2.3 7.2.4 7.2.5	X	X	X			X
7.3.2		X				
7.3.10	X	X	X			
7.3.17		X	X			
7.4.4 7.4.5 7.4.6	X	X	X	X		X
7.4.21	X					
7.4.32	X		X			X
7.5.18 7.5.19 7.5.20 7.5.21 7.5.22 7.5.23 7.5.24			X	X	X	X
7.5.25 7.5.26			X			

6. Frequently Asked Questions

What is an IP camera?

IP stands for Internet Protocol. An IP camera is a digital video system that can be connected and transmit data over a network. These cameras work can work be viewed both locally and remotely so that you can view your security feed from anywhere with an Internet connection. IP cameras can also be referred to as network cameras or webcams.

What is the difference between a DVR and NVR?

There are several differences between DVR and NVR, the most important are:

- NVR can be part of a computer network along with the IP cameras, therefore there is no need to run dedicated wires to support your CCTV system; you can use the existing network infrastructure.
- The NVR supports high-resolution megapixel cameras
- The DVR uses coaxial connections to each of the analogue cameras.
- The DVR supports only cameras with VGA resolution

Does lighting need to be on permanently?

Lighting only needs to be on only if it acts as a deterrent in itself; criminals prefer to work in dark environments. Energy efficient LED lighting significantly reduces the cost of permanently illuminating dark areas. As an alternative to permanent lighting in a CCTV monitored area, lights can be controlled by motion sensors, provided they respond immediately to catch fast action.

How many hours of video can the DVR/NVR store?

There are several parameters that may affect this answer. Some of them are:

- Number of cameras
- Resolution and Frames per second recorded
- Size/capacity of storage devices (hard drives)

How much does a CCTV system cost?

Price is always a relative figure. What is most important here is to find the best relationship between price and quality. Absolute prices of CCTV systems may vary significantly based on the components. For example, CCTV cameras range in price from about £100 to around £6,000.

The most important thing is to understand what you want to achieve with the system and then get one that brings together the right components that make it fit for the purpose you intend. Always describe your operational needs rather than technical specs. The supplier needs to "translate" your operational needs to technical specifications of the system that he has to design, install and commission.

Value rather than the lowest cost is the foremost objective of many buyers. Maintenance and support, as well as hardware, software and installation costs, should all be factored in when trying to determine the supplier that offers the best value.

IP CCTV supports a Lower Total Cost of Ownership (TCO) through remote monitoring of camera operation and reduced maintenance. HD cameras with up to 30-megapixel resolution, and remote control of zoom and direction of view, enable system consolidation by reducing the number of cameras required.

What are the basic components of a modern CCTV system?

For an IP surveillance system, you'll need:

- The actual IP cameras
- An NVR or other type of storage system
- Accessories such as microphones and speakers generally will come built into the cameras (if necessary) so additional parts will not be required.

How recording on motion detection work?

You can program your CCTV system to record motion detection. Usually, the programming supports also recording some seconds prior to motion detection (i.e. you can program your system to record 15 seconds prior to someone entering a room.)

But how the system knows that in 15 seconds someone will enter the room, so it can start recording 15 mins ahead?

The answer is simple: the system records continuously and if there is no entrance, it deletes the recorded video and over-writes the new one. In case motion is detected, the recorded video is stored and not deleted.

What is Lux?

Lux is the unit for measuring the quantity of lighting. One lux (Latin for "light") is the amount of illumination provided when one lumen is evenly distributed over an area of one square meter.

And what is lumen? Unfortunately, you need to go deep into your school physics books to find out this.

Note: Just for reference and not for information: a lumen is equal to the amount of light emitted per second in a unit solid angle of one steradian from a uniform source of one candela. Many unknown words, no need to go deeper!

What happens if there is a power outage?

Like any electrical component, DVRs and NVRs might be damaged by power surges and spikes (fluctuations of voltage), so they must be properly protected. DVR/NVRs will come back on as soon as power is restored. However, an uninterruptable power supply (UPS) that provides a short period of backup power and serves as a surge protection device is strongly recommended. This ensures your video surveillance will still be online in the event someone cuts the power to break in unnoticed.

If you decide to use a UPS for a short period of time, please note that CCTV records will not be available in case of longer power outages; a backup power connection to an existing diesel generator might be a good solution to ensure the continuity of CCTV operation.

Can I use a CCTV system to identify and report an alarm?

Yes, even older DVRs can transmit an alarm based on specific conditions (i.e., motion detection). Modern CCTV systems are equipped with alarm triggering conditions based on VCA (video content analysis) that can raise an alarm.

7. Useful links

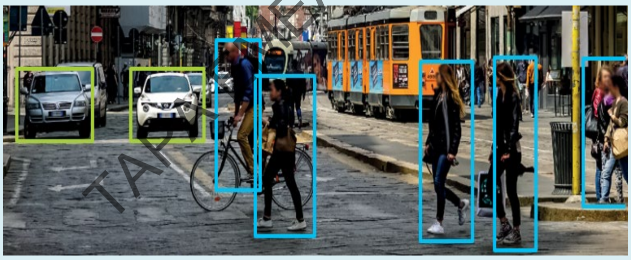
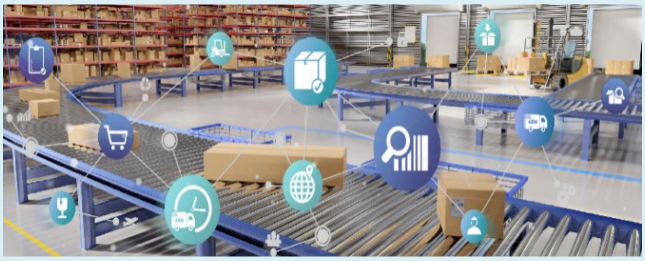
7.1. TAPA Members - Security Service Providers (CCTV systems)

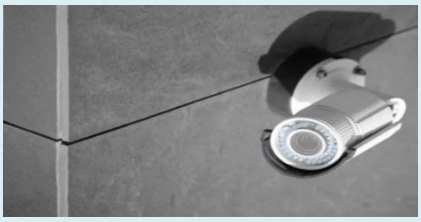
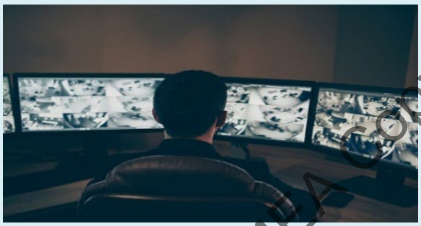
- https://www.bettinivideo.com/IT/index.php
- https://www.g4stelematix.com
- http://www.genetec.com
- http://www.geutebrueck.com
- http://www.johnsoncontrols.com
- https://sternkraft.com/en/
- http://www.multiprotexion.com/

7.2. Information on CCTV

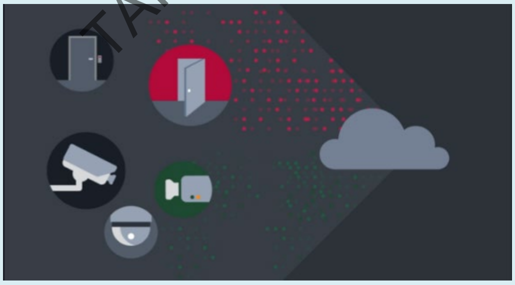
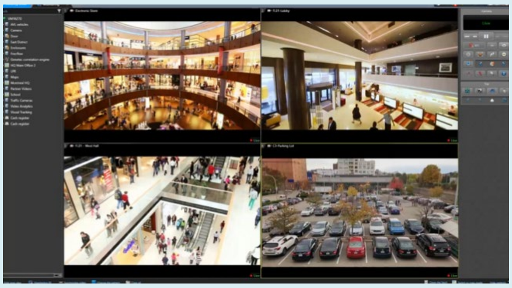
- https://www.motorolasolutions.com/en_xu/video-security-access-control.html
- https://www.gensecurity.com/blog/understanding-cctv-components-the-4-parts-every-system-requires
- https://www.techtarget.com/whatis/definition/CCTV-closed-circuit-television#:~:text=CCTV%20(closed%2Dcircuit%20television),for%20surveillance%20and%20security%20purposes.
- https://ellipsesecurity.com/2019/05/cctv-glossary-of-terms/
- http://www.pfn.ir/editor/uploadfiles/tabshow/pic/solutions/cctv_glossary.pdf
- https://www.cctvsecuritypros.com/hd-comparison-videos/
- https://www.caughtoncamera.net/news/different-types-of-cctv/
- https://www.its.com.au/comparison-cctv-technologies
- https://www.youtube.com/watch?v=kjUa0UjZBYQ
- https://www.anixter.com/content/dam/Suppliers/Hikvision/IPC-Comparison-Chart-Jan-2019.pdf
- https://www.securitysolutionsmedia.com/2019/02/26/understanding-cctv-storage-requirements/
- https://www.westerndigital.com/tools/surveillance-capacity-calculator
- https://reolink.com/blog/cctv-storage-calculation-formula/
- https://www.cpni.gov.uk/cctv
- 20200203 CCTV in the Workplace.pdf (cpni.gov.uk)
- https://www.cpni.gov.uk/system/files/documents/a9/3b/20200203%20CCTV%20within%20the%20Perimeter%20of%20a%20Site.pdf
- https://www.cpni.gov.uk/resources/cctv-cni-perimeter

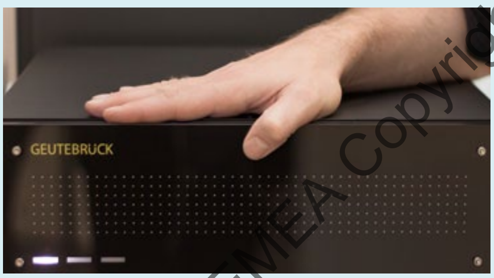
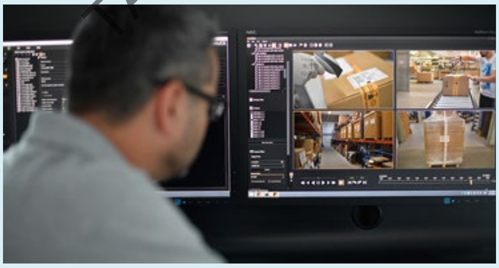
8. Appendix A: CCTV Systems Examples

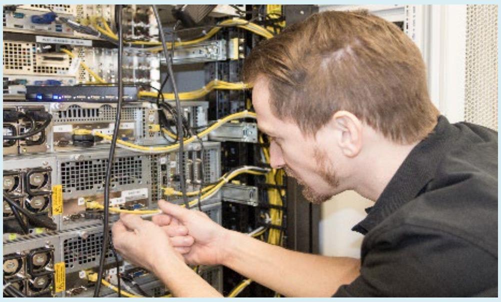
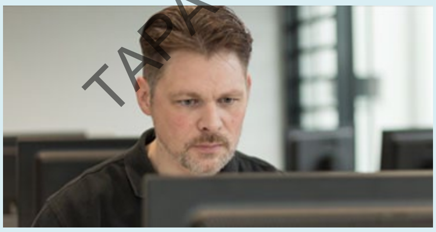
Ref	Product	Description
CSG-01.1	Video Surveillance Made in Italy	The product range consists of numerous cameras and recording units, ENCODER-DVR-NVR-SERVER complemented by centralization software solutions, Diagnostics Tool, Smart-App, VMS, smart video analysis and specific applications.
		Bettini S.r.l https://www.bettinivideo.com/EN/
CSG-01.2	DETECTA-MADE IN ITALY - AI	DETECTA AI enables the detection of events captured by newly or already installed cameras on the site using sophisticated algorithms. DETECTA AI is a flexible and ready-to-use solution that exploits video streams from TLC, NVR / DVR, Video Encoders and other video surveillance devices previously installed on the site. In this way, it's possible to optimize existing resources with consequent cost and time saving
		Bettini S.r.l https://www.bettinivideo.com/EN/
CSG-01.3	LOGISTICS - BVI	Business Video Intelligence systems are solutions that use video data from cameras to manage business processes (for example in Logistics, Finance, Retail, etc.). They are able to generate a new database by extracting the event data from the images of a video system and from information contained in management and ERP software's.
		Bettini S.r.l https://www.bettinivideo.com/EN/

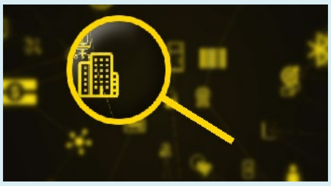
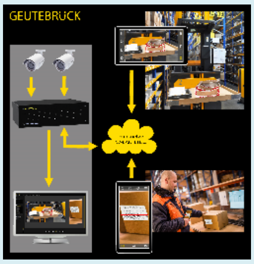
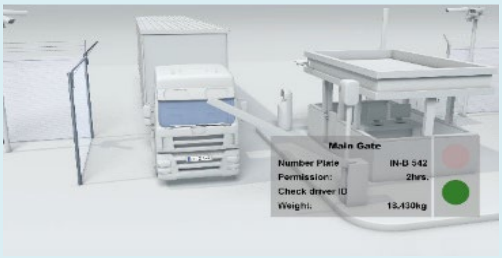
CSG-02.1	CCTV & SOFTWARE	Video Surveillance is at the heart of any integrated security programme. G4S has many years of experience in specifying, installing, and supporting commercial CCTV for high security applications.
		G4S Telematix S.A. https://www.g4stelematix.com
CSG-02.2	IP CAMERAS	IP cameras are the backbone of any modern video system. Using digital technology, they allow you to adopt a smarter approach to security by using analytics to evaluate video in real-time and alert to suspicious activity.
		**G4S Telematix S.A.** https://www.g4stelematix.com
CSG-02.3	REMOTE CCTV MONITORING	Real time video surveillance provides a permanent “eyes on your premises”. Ensuring the surveillance facility delivers an appropriate service and avoids wasted expenditure can be a real challenge.
		**G4S Telematix S.A.** https://www.g4stelematix.com
CSG-02.4	VIDEO ALARM VERIFICATION	False alarms are a real nuisance. They causing disruption to neighbouring properties and leave staff following up false alarms. A fast, efficient process for handling video surveillance alerts is critical to minimise disruption and identify the real emergencies.
		G4S Telematix S.A. https://www.g4stelematix.com
CSG-02.5	VIDEO ANALYTICS	Monitoring CCTV systems can be very time intensive and costly to ensure that alarms and escalating situations are not missed at any time. In addition, it can be very staff intensive due to the regular rotation of operators required on any shift.
		G4S Telematix S.A. https://www.g4stelematix.com

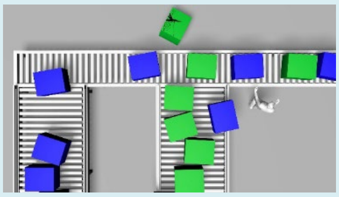
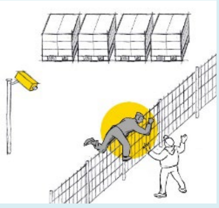
CSG-02.6	RAPID & TEMPORARY SURVEILLANCE	Securing sites left vacant at short notice and monitoring outdoor spaces round the clock are real challenges. Our range of rapid deployment CCTV Towers are available on a temporary basis at short notice and provide the platform for 24*7 surveillance.
		G4S Telematix S.A. https://www.g4stelematix.com Telematix
CSG-02.7	SURVEILLANCE	Automation and technology enhancements have made drone technology a reality. Whether it is perimeter or external inspections, a visible criminal deterrent or replacing physical patrols, drones have a role to play.
		G4S Telematix S.A. https://www.g4stelematix.com Telematix
CSG-02.8	ANPR SOLUTIONS	Automatic Number Plate Recognition can be an integral part of an integrated security system.
	ANPR SEND SIGNAL ARH 001	G4S Telematix S.A. https://www.g4stelematix.com Telematix
CSG-02.9	ADVANCED DRIVER ASSISTANCE SYSTEMS	Improve driver safety in real-time through optional in-cab coaching in high-risk situations such as yawning, smoking, distraction, phone call, no seatbelt, and more, helping drivers practice safe driving habits.
		G4S Telematix S.A. https://www.g4stelematix.com Telematix
CSG-02.10	VEHICLE CAMERAS	From vandal-proved cameras to anti-explosion cameras, from indoor cameras to outdoor cameras which are tested with up to IP68 protection level, they all provide the best image quality for choices of different requirements.
		G4S Telematix S.A. https://www.g4stelematix.com Telematix

CSG-02.11	CCTV MAINTENANCE	Our systems are only as good as we maintain them. Here is a case study on how we maintain 230 IP & legacy analogue CCTV cameras across 5 sites.
		G4S Telematix S.A. https://www.g4stelematix.com
CSG-02.12	TRANSITION FROM ANALOG TO IP CAMERAS	Migrating to an intelligent IP based platform whilst securing zero downtime is challenging. Here is a case study on how we migrated to new tech within the constraints of a demanding environment.
		G4S Telematix S.A. https://www.g4stelematix.com
CSG-02.13	CYBERSECURITY SERVICES	Physical security & cybersecurity come together in one service.
		G4S Telematix S.A. https://www.g4stelematix.com
CSG-03.01	Video Surveillance	Integrated Solutions
	 	**Genetec** https://www.genetec.com

CSG-04.1	CCTV cameras and accessories	Complete camera range of CCTV cameras for all types of applications, form factors, resolutions and mounting variants from indoor or outdoor to thermal imaging
		Geutebrück GmbH https://shop.geutebrueck.com/
CSG-04.2	CCTV lighting products	Range of outdoor IR and white light floodlights
		Geutebrück GmbH https://shop.geutebrueck.com/
CSG-04.3	CCTV servers and appliances	Complete range of stations and servers for CCTV application with configurable HDD capacity in six different form factors, with optional RAID and redundant power supply
		Geutebrück GmbH https://shop.geutebrueck.com/
CSG-04.4	G-Core Video Management Software	Enterprise type video management software for professional video management applications with a wide range of video analytics, third party interfaces and logistics specific options
		Geutebrück GmbH https://shop.geutebrueck.com/
CSG-04.5	G-SIM Security Management System	Specific Enterprise type information management software for intuitive and easy operation of medium to large Geutebrück CCTV systems including Video Track & Trace functionality
		Geutebrück GmbH https://shop.geutebrueck.com/

CSG-04.6	G-Tect Video Analytics Options	Specific Various video analytics options from classical to AI based algorithms for perimeter protection, logistics applications and other uses
		Geutebrück GmbH https://shop.geutebrueck.com/ GEUTEBRÜCK
CSG-04.7	CCTV Network products and accessories	Range of switches and other network accessories to build an IP based CCTV surveillance network
		**Geutebrück GmbH** https://shop.geutebrueck.com/ GEUTEBRÜCK
CSG-04.8	CCTV Monitors and operating console	Range of monitors and operating console for control rooms
		Geutebrück GmbH https://shop.geutebrueck.com/ GEUTEBRÜCK
CSG-04.9	Services and Support	Various services and support ranging from project design and commissioning to after sales hotline, patch management and more
		**Geutebrück GmbH** https://shop.geutebrueck.com/ GEUTEBRÜCK
CSG-04.10	VAM Vehicle Access Management	Video based vehicle access management solution for logistics premises including visual automatic number plate recognition, white list and black list access control and well time reports
		Geutebrück GmbH https://shop.geutebrueck.com/ GEUTEBRÜCK

CSG-04.11	Third party interface integration	Specific Service to integrate third-party your CCTV monitoring system, e.g. ERP or warehousing management systems to optimize logistics processes, including missing or damaged goods processing
		Geutebrück GmbH https://shop.geutebrueck.com/ GEUTEBRÜCK
CSG-04.12	Scanner Connect App for Zebra Scanners	App to connect Zebra scanners directly into the video management system including automatic position identification based on Geutebrück icons to visually document the complete scanning process of goods
		Geutebrück GmbH https://shop.geutebrueck.com/ GEUTEBRÜCK
CSG-04.13	SmartPhone Connect App including Scanner function	App for Android Smartphones converting them into surveillance cameras and logistics code scanners (EAN, QR and others)
		Geutebrück GmbH https://shop.geutebrueck.com/ GEUTEBRÜCK
CSG-04.14	Data protection & security	Specific image data will be handled in a way that complies with data protection laws (with masking, dual-control passwords and logging of video views/exports), this creates a sense of trust.
		Geutebrück GmbH https://shop.geutebrueck.com/ GEUTEBRÜCK
CSG-04.15	Automated Yard Management	All authorised numberplates can be assigned to the responsible loading bay. When the system detects an authorised numberplate on entry, the driver is shown details of their destination on a display or sent the information by text message.
	 Main Gate Number Plate IN-B 542 Permission: 2hrs. Check driver ID Weight: 13.430kg	Geutebrück GmbH https://shop.geutebrueck.com/ GEUTEBRÜCK

CSG-04.16	Video Track & Trace	Video recordings of all stations that a package goes through in the supply chain can be found and evaluated in a matter of seconds thanks to the barcode. Damage or incorrectly loaded items can be located immediately. Processes that contain errors are identified.
		Geutebrück GmbH https://shop.geutebrueck.com/ GEUTEBRÜCK
CSG-04.17	AI-based systems for object detection	AI-trained software identifies known objects and the number that are present in video images. Detection is based on previously learnt object characteristics, which are taught in via a training process based on photos and videos.
		Geutebrück GmbH https://shop.geutebrueck.com/ GEUTEBRÜCK
CSG-04.18	Perimeter protection	To gain entry, intruders have to get past a number of "boundaries": including the fence, garden, car park, doors and windows of the building. Video analysis detects all suspicious movement in video images at an early stage and warns staff accordingly.
		Geutebrück GmbH https://shop.geutebrueck.com/ GEUTEBRÜCK
CSG-04.19	Clear up attempted deception	The seamless video documentation of the status of the goods – from order picking through to final dispatch – provides court-enforceable evidence for any claims relating to incorrect deliveries, damaged or missing goods, or damaged packaging.
		Geutebrück GmbH https://shop.geutebrueck.com/ GEUTEBRÜCK
CSG-04.20	Prevent loss of items	The interface to the ERP system enables you to search for the order search number of a dispatch order. You can view the journey of each package in order in almost real-time. Incorrectly loaded items can be identified and corrected rapidly.
		Geutebrück GmbH https://shop.geutebrueck.com/ GEUTEBRÜCK

CSG-05.01	**CCTV Cameras** Axis, Avigilon, Arecont, American Dynamics, Bosch, Dahua, Dallmeier, Geutebrück, HIKVision, Honeywell, Panasonic, Samsung Sony, etc.	Video compression with H.264, H.265 and MJPE/MPEG, 30 FpS and more, multiple lens options, able to work with Ultra-Low-Light or Ultra-Backlight, HDTV 1080p or 4K, WDR Forensic Capture, up to 20 Privacy Masking Zones, from IP67, I68Ex to IP69, ONVIF Compliant, adaptive IR Beams, Audio Capabilities, Varios Layouts: 360 Deg, PTZ, Thermal, Domes, Box, Bullet,
		Johnson Controls http://www.johnsoncontrols.com
CSG-05.02	**Servers** Dell, HP, Fujitsu, Lenovo	up to 4 Sockets per Server Memory: (96 DIMMS): 8GB/16GB/32GB/64GB/128GB RDIMM, LRDIMM up to 2400 MT/s Storage: 2.5" SATA/SAS SSD, SAS HDD (15K, 10K), nearline SAS HDD (7.2K) 2.5" Dell PowerEdge NVMe Express Flash PCIe SSD
		Johnson Controls http://www.johnsoncontrols.com
CSG-05.03	**Switches** Cisco, NetGear, HP, Zyxel, Ubiquiti	32 x 100G QSFP28 ports Wire-speed, ultra-low latency switching Supports Open Network Install Environment (ONIE) for zero-touch installation of network OS SDN-enabled with OpenFlow 1.3 support Dual AC/DC hot-swappable power supply modules for 1+1 redundancy and load sharing
		Johnson Controls http://www.johnsoncontrols.com
CSG-05.04	**UPS** APC, BLueWalker,	Output Power Capacity: 1.0k Watts / 1.5 kVA Output Connections: (2) IEC Jumpers (Battery Backup) (8) IEC 320 C13 (Battery Backup) Nominal Output Voltage: 230 Volt Nominal Input Voltage: 230 Volt Cold-Start-Capability, Green Mode, Intelligent Card Slot, LCD Interface, Predictive replace battery date, Temperature-compensated battery charging,
		Johnson Controls http://www.johnsoncontrols.com
CSG-05.05	**Software** Axis, Avigilon, Bosch, Briefcam, Cisco Meraki, exacqVision, Genetec, Heitel, Honeywell, Milestone, Mirasys, OnSSI, Panasonic, Qognify, Salient, Softwarehouse, TrueVUE, Verint, Verkada, Xtralis (HW), 3VR	Parcel-Tracking, DWS-Integration (Dimensioning, Weighing, Scanning), Deep Barcode Scanner Integration, Conveyor-Belt-Connectivity, X-Ray Integration, RFID-Integration and Integration with Picking-Systems, Cloud-based solution available, Cyber-proof, AI-ready
		Johnson Controls http://www.johnsoncontrols.com

CSG-06.01	Safeway Cameras	The cameras of the SafeWay system cover the space around the vehicle, allowing both live view and development of recordings from the system memory.
		Sternkraft GmbH https://sternkraft.com/en/ STERNKRAFT VIDEO TELEMATICS
CSG-07.01	MULTI EYE	MULTI EYE is a project designed by Multiprotexion: it's a multilingual telematic totem that can recognize and verify the plate and the color of the vehicle, allow access to certain areas, scan personal documents, and measure body temperature. It's a good solution for companies in the control of logistic areas, usually subject to heavy vehicle traffic.
		Multiprotexion Srl http://www.multiprotexion.com/ MULTIPROTEXION
CSG-07.02	ET01 SOLAR TOWER	ET01 is a mobile station of active video surveillance completely autonomous, equipped with 4 thermal cameras with A.I. and a VOIP kit. Equipped with 3 integrated solar panels and an ingenious folding system, which allows the optimal absorption of solar energy, the system is combined with high-efficiency batteries that guarantee a long autonomy.
		Multiprotexion Srl http://www.multiprotexion.com/ MULTIPROTEXION