



# Video analytics adoption: Key considerations for the end-user

*ERNCIP Thematic Group  
Video surveillance for  
security of critical  
infrastructure*

Sarah Doyle, MSc., Kinesense

2016

The research leading to these results has received funding from the European Union as part of the European Reference Network for Critical Infrastructure Protection project.

Video analytics adoption:  
Key considerations for the end-user

This publication is a Technical report by the Joint Research Centre, the European Commission's in-house science service. It aims to provide evidence-based scientific support to the European policymaking process. The scientific output expressed does not imply a policy position of the European Commission. Neither the European Commission nor any person acting on behalf of the Commission is responsible for the use which might be made of this publication.

**JRC Science Hub**

<https://ec.europa.eu/jrc>

JRC102121

ISBN 978-92-79-60076-0

doi:10.2788/18092

© European Union, 2016

Reproduction is authorised provided the source is acknowledged.

All images are courtesy of Kinesense, except: *page 13*, figure 3 Photo credit: Quebec's Ministry for Transport.

## Contents

Acknowledgements .....	5
Abstract .....	6
1. Introduction .....	7
2. An overview of video analytics .....	8
2.1 What is video analytics? .....	8
2.2 What are the advantages of using video analytics? .....	8
2.3 How can video analytics be used? .....	8
2.4 What are the current prevalent video analytics functions? .....	9
2.5 Edge versus server analytics? .....	11
3. Selecting video content analytics (VCA) .....	12
3.1 Key considerations in selecting video analytics .....	12
3.1.1 What is the problem you are addressing? .....	12
3.1.2 What is the function of the video analytic? .....	12
3.1.3 What detection rate is acceptable? .....	12
3.1.4 What false alarm rate is acceptable? .....	12
3.1.5 Will your surveillance infrastructure affect your video analytic choice? .....	13
3.1.6 What frame rate will the video analytic work with? .....	13
3.1.7 Is the image quality of your footage sufficient for the video analytic? .....	13
3.1.8 Will the camera position be compatible with video analytics? .....	13
3.1.9 How complex is your environment? .....	14
3.1.10 How will lighting conditions affect video analytics? .....	15
3.1.11 How much configuration is required? .....	16
3.1.12 How do you want to be notified of alerts? .....	16
3.1.13 What is your budget? .....	16
3.1.14 What support and maintenance is required? .....	16
3.1.15 What are the legal restrictions which may exist in your country? .....	17
4. Video analytics use cases .....	18
4.1 Den Jyske Kontrolcentraal Case Study: Utilising video analytics in a remote monitoring service .....	18
4.2 Post-event investigation: the use of video analytics by law enforcement .....	19
4.3 P-REACT Research Case Study: Developing a video surveillance system using video analytics .....	19
5. Conclusion .....	20
References .....	21
List of abbreviations and definitions .....	22
List of figures .....	23
List of tables .....	23



## **Acknowledgements**

The author gratefully acknowledges the contributions and reviews of the other members of the Encip Thematic Group; Video Surveillance for security of critical infrastructure, the Encip office and case study contributors including Den Jyske Kontrolcentraal, the P-REACT project consortium and Greater Manchester Police.

## Abstract

This report has been generated by the Erncip Thematic Group Video Surveillance for security of critical infrastructure (TG VAS).

Video analytics is a technology that analyses the video content. The technology is increasingly being adopted by security managers, law enforcement and other users to address various security issues.

This report outlines the basics of the technology, how it is used and its advantages. It aims to draw end-users attention to the key factors which must be taken into account when considering its adoption. It is aimed at managers, security personnel, law enforcement officers and other end-users whose knowledge of video analytics is limited. This report should help the end-user engage initially with potential providers of video analytics.

General factors which affect video analytics are explored. For more in-depth analysis of factors affecting video analytics see *Surveillance and video analytics: Factors Influencing the Performance* (1). General comments are made in relation to video surveillance systems, however, for more in-depth CCTV deployment guides see *Home Office. CCTV Operational Requirements Manual 2009* (2).

Note that this report does not aim to define what analytics can or cannot do, as this is a constantly evolving area. Nor does this report imply any recommendations by the authors or the European Commission.

## 1. Introduction

Video security systems are used across cities, facilities and organisations to detect and deter crime and other security risks. Traditional video security systems provide the infrastructure only to capture, store and distribute video, leaving the task of threat detection to human operators. This task is time consuming, tedious and error prone due to human fatigue.

As camera numbers increase, the issue of managing and making use of video becomes increasingly prevalent. There are an estimated 2.1 billion cameras operating worldwide based on historical shipment information (3). Increasingly security managers and camera owners are looking for ways to automate security detection and make better use of their cameras.

Video analytics (VA) is one technology that can transform video surveillance and investigation from a manual, resource-intensive and error-prone process into an automated, efficient and accurate one. As a result, it can effectively deliver effective crime detection, prevention, and prosecution.

The purpose of this document is to provide an introduction to video analytics technology for end-users considering its adoption. This guide should enable end-users to understand the basic premise of the technology, its uses and considerations which should be taken into account in its adoption. It is not intended to be a technical in-depth deployment guide but an introductory guide. This guide is intended for those addressing security issues as opposed to adopting video analytics for operational purposes, such as shopper footfall analysis.

## 2. An overview of video analytics

### 2.1 What is video analytics?

The Erncip Thematic Group Video Surveillance for security of critical infrastructure (TG VAS) defines video analytics as:

'... the analysis of video content to generate a search index or to provide automatic alerts to specific events or activity, through the categorisation of objects or actions appearing in video.'

Traditionally, objects and content in video are identified by detecting pixel change and grouping these pixels into objects or 'blobs', distinguishing the background and foreground video content. The technology then seeks to further define objects based on their position, size, direction of motion, time and so on. Advanced algorithms will seek to extend classification to the type of object and the actions of that object such as loitering, crawling, etc. Essentially, video analytics is a mathematical function or algorithm that aims to classify objects based on pixels.

### 2.2 What are the advantages of using video analytics?

There is no doubt that video is an attractive surveillance mechanism. As the saying goes, 'a picture is worth a thousand words'. If this is true, video speaks volumes more. Essentially, video analytics helps you to get to the pertinent image or video clip less onerously, either in real time or post event. The technology can help improve security effectiveness and efficiency towards proactive security. A direct cost or monetary benefit can be obtained from using video analytics, including:

1. Incident prevention can save significant costs related to asset damage, theft and business continuity disturbance. For instance, detecting a perimeter breach quickly and automatically can enable security personnel to respond to the threat and prevent it taking place.
2. A reduction in the number of guards or personnel required. For example, automated remote video surveillance detecting perimeter intrusion as a service is a growing trend which eliminates the need for on-site guards. See Den Jyske Kontrolcentraal case study in section 3 for further insights on remote monitoring.
3. Video is a pertinent way to prove deniability or liability. Using video analytics to find key incidents as evidence eliminates manually sifting through video. This has a direct effect on legal, litigation and insurance costs, as well as saving time and money by not having to manually watch video. See Greater Manchester Police case study in section 3 to show how video analytics can be used in post-event analysis.
4. Using video analytics to reduce security risk can greatly affect customer and staff perceived risk and increase satisfaction.
5. Reduction in staff stress-related illnesses, particularly prevalent to those watching potentially disturbing video scenes.
6. Video analytics can support other operational systems. For example, video analytics can be used to detect motion which can control lighting levels, eliminating the need to have lighting running at full brightness.

### 2.3 How can video analytics be used?

Video analytics technology can be deployed in government, commercial, residential and industrial environments. Video analytics are predominantly used for two primary security functions; **real-time** event alert detection and **post-event** investigation.

There is a broad spectrum of real-time functions or modalities. The common video analytics functions include perimeter intrusion, left baggage detection, group detection, and person loitering. Others include smoke or fire detection, density analysis, etc. These analytic types can be used for a variety of security purposes such as crowd control, public safety, anti-theft or asset damage, etc.

When implementing an automated video surveillance system, predominantly the focus is on real-time detection of events. Often the post-event analysis requirements are not given significant consideration. If an incident takes place, will you have to trawl through hours of video to find out when it happened or can you use video analytics? Some analytics are designed for real-time alert detection and post event but not always. Furthermore, real-time alert analytics are normally specifically focused on a type of security threat and are not suitable for post-event investigation.

As a general note, typically video analytics are used as an aid to the monitoring personnel or investigators rather than replacing them.

## 2.4 What are the current prevalent video analytics functions?

Currently there are a broad range of video analytics functions or modalities that can be classified into general categories. Essentially, a VA function is looking at who, what, where and when (independently or in combination).

The most prominent functions are outlined in Table 1. The general level of reliability of these types of analytics cannot be concretely commented on, as their effectiveness depends on 1. the environment which they are deployed, 2. their purpose, 3. how much configuration is required and 4. how commercially advanced the analytic is. However, the Encip group has made some general comments on these generally available solutions taking into account their market maturity and required configuration.

VA type	Description	Comments
Object tracking	This detects an object and tracks its trajectory through the camera field of view.	This is distinct to tracking an object from one camera to another camera (known as multi-camera tracking) and is quite robust in non-crowded environments or when there is no occlusion of the object of interest
Object classification	Differentiates between a person, vehicle or other object. Shape, size and movement are key characteristics used to distinguish between objects.	This is typically combined with other analytics functions such as tripwire and can work well when configured. Size seems to be the most common way of distinguishing between objects at present.
Tripwire event detection	This detects when an object moves over a line (tripwire) which is drawn on the camera field of view.	This is one of the most common analytics types and works very well, especially in an indoor environment. However, configuration particularly in outdoor environments, to taken into account weather conditions, etc, may be required.

<b>VA type</b>	<b>Description</b>	<b>Comments</b>
Intrusion detection	This detects when an object enters an area of interest within the camera field of view.	This is similar in design and maturity to tripwire detection.
Left object detection	This detects when an object has been left behind or inserted in the camera field or view or a designated area of interest.	
Removal detection	This detects when an object has taken or removed in the camera field or view or a designated area of interest.	This works in a similar way to Left object detection.
Loitering detection	Detects when a person or vehicle remains in the full camera view or a designated area.	This type of algorithm is typically based on statistical analysis or dwell time of an object. It has been widely deployed in non-complex or crowded environments.
People counting	Detect and counts people as they cross a point of interest	This type of analytic is typically successful unless people are moving very close together or in groups.
Image change	Detects when there has been a major change in the camera view such as view obstruction, power cut or the camera has been moved	This is a common analytics typically used to check a camera is still functional. Also referred to as 'Health check'.
Object Multi-camera tracking	Tracking an object from one camera FOV to another	This is a highly desirable analytic function, however, it relies on tracking a characteristic such as colour which may differ from camera to camera and typically requires the camera network schematic. Overall, this function is difficult to deploy with good results.

Table 1 VA function overview

Commercially available video analytics solutions are able to robustly find the presence of persons, vehicles and objects and their movement in single camera views. Significant developments have been made to extend classification by analysis of their actions, interactions between objects and the environment, e.g. loitering detection, group detection.

At a research level, significant development work has taken place to extend the above functionality to deal with crowded environments or between cameras. Work is also focusing on extending behaviour classifications such as gait and gesture analysis. There are examples of such advanced implementations of video analytics but as they require significant configuration to the scene and may not work in all environments, their deployment levels have been low to date.

## **2.5 Edge versus server analytics?**

Video analytics algorithms can run on processors either embedded in or near the camera or on a server. The former is typically referred to as edge video analytics and the latter server analytics. Video analytics performed at the edge can have the advantage of accessing images prior to compression as a result of the transmission process and may help in minimising bandwidth and transmission speed but can require significant computational resources at the camera which may not be possible. Server based analytics can be more configurable, easier to maintain and are often more advanced, however, you do not get the bandwidth benefits attributable to edge analytics.

In recent years edge analytics have become increasingly popular. Wherever the algorithms run the process is similar, the video source gets fed into a processor where the video analytics analyse the content creating an alert which can be sent to a variety of locations such as a control centre system, personnel mobile device, etc.

### **3. Selecting video content analytics (VCA)**

#### **3.1. Key considerations in selecting video analytics**

As with any new security systems, there are a number of issues to be considered. This section aims to highlight the key questions or issues to consider, in relation to adopting video analytics. It also highlights some of the common pitfalls when using video analytics.

##### **3.1.1. What is the problem you are addressing?**

The first question to ask when considering video analytics is what is your operational security purpose? This needs considerable definition encompassing an extensive exploration of the problem (threats/assets/security issues), stakeholders, risk assessment and success criteria to determine the most appropriate solution. A complete assessment of the purpose will give rise to key requirements. The *CPNI guide to producing operational requirements for security measures* (2014) is a good reference for anyone carrying out this task (4).

##### **3.1.2. What is the function of the video analytic?**

It is important to clearly outline how the video analytics will function. Is the purpose to detect an object or track objects involved? Is the purpose to detect, observe, recognise or identify? The *Home Office CCTV Operational requirements Manual, 2009* (2) has a good outline of the screen height level of detail required to detect, observe, recognise, identify. Video analytics can be very useful at detecting a security breach. In fact, evidence suggests humans will often miss events due to fatigue. However, the cognitive abilities of video analytics are nowhere near human intelligence. For example, a fight may be detected by video analytics but it is unlikely that the perpetrator could be tracked through a busy scene as they escape. Therefore, video analytics is less likely to be useful to recognise and identify. A clear understanding of what the analytic was designed to do should be obtained and matched to the problem you are addressing.

##### **3.1.3. What detection rate is acceptable?**

The key thing to consider when examining video analytics is the detection rate (or the detection probability rate (Pd)). What detection rate is acceptable will be determined largely by the risk assessment. If the event is not detected would the repercussions be severe, moderate or minor? Some users will be happy with a 75 % detection rate, for others this will be unacceptable. It is also important to consider the detection rate under various conditions. The *CPNI guidance note: testing installed video analytic systems* (2015) has some useful examples of how to test perimeter intrusion under various conditions (5).

##### **3.1.4. What false alarm rate is acceptable?**

Related to the detection rate is the false alarm rate (FAR). A system may have a 99 % detection rate but the false alarm rate may be significant. As a general rule if the detection rate needs to be maximised, the sensitivity of the system will be increased which will typically leads to more false alarms. All video analytics are prone to false alarms so they need to be tolerated, but how many can be tolerated a day? Thought must also be given to the number of false alarms across a camera installation. If you have three false alarms a day across 100 cameras, that is 300 false alarms a day!

There are a large number of factors which will affect the false alarm rate (some of which are discussed below). Testing should be carried out in the environment that it will be used in and if outdoors, in a range of weather conditions.



### ***3.1.5 Will your surveillance infrastructure affect your video analytic choice?***

You will have a lot more scope in deploying video analytics in a greenfield site whereas you will be more restricted in an existing installation. When looking to deploy in an existing site, one of the key factors will be whether the video analytics supplier has integrated or can be deployed on your current cameras or video management system (VMS). Currently, only a small number of cameras support video analytics in the camera but it is a growing trend. Generally, there is a bit more scope in deploying server based analytics as more and more video management systems (VMS) support growing video analytics products.

Another common issue with video analytics is that they can typically not be used with non static cameras including PTZ cameras. There are research developments in this area but few of any common video analytics that can be used on moving video streams. Other considerations include video processing power (especially for 100s of cameras) and storage space. Overall, if you have an existing surveillance system, the choice of video analytic will be driven by what is supported.

### ***3.1.6 What frame rate will the video analytic work with?***

Typically, the frame rate of the video should be high, giving smooth motion flow through the video, as is required for most video analytics. Low frame is typically in the 1 to 6fps range, higher in the 12 to 25 fps range. The typical speed of objects moving through the scene should also be considered in terms of frame rate. If objects move quickly, a higher frame rate should be considered. A person running could easily be missed with low frame rates.

### ***3.1.7 Is the image quality of your footage sufficient for the video analytic?***

The quality of the image should be sharp enough, providing sufficient detail and without compression artefacts. It is worth noting, that images from high resolution cameras are often significantly compressed when they are streamed, thereby, the quality may not be sufficient for more complex server algorithms, as a lot of detail may be lost.

### ***3.1.8 Will the camera position be compatible with video analytics?***

The camera position or field of view (FOV) can have a significant impact on video analytics performance. Analytics will frequently be designed to work at a particular angle. For example, face recognition and licence plate recognition will typically not work from a higher position than the area under analysis, i.e. the number plate or face. Others will have a minimum angle which they work at. Furthermore, if objects are blocking a point of interest and an event takes place, the video analytics will typically not detect it. Video analytics like cameras cannot see through walls (unless it's a thermal imager!). Neither will video analytics work reliably through trees. So, remember that when you place a camera in winter take into account that foliage growth may block your camera view come spring, as per Figure 1. It may be required to move an existing camera or deploy a new one for the video analytics to work.



**Figure 1 Foliage blocking camera view**

### ***3.1.9 How complex is your environment?***

The complexity of a scene can refer to many environmental variables such as weather, lighting changes, etc. Altering camera position and lighting may greatly reduce the number of false alarms in video analytics. One of the key areas of complexity that can cause issues for video analytics is the number and density of objects in a scene. This is particularly relevant as objects may occlude each other. The density or number of objects does not simply refer to the objects you are interested in but all objects. Figure 2 shows a high density environment. A common issue in a maritime environment when using video analytics to detect boats, is triggering of false alarms caused by seagulls or as per Figure 3 highlights unexpected objects many include owls as caught on camera by Quebec Ministry of Transport.



**Figure 2 Example of high density environment**



**Figure 3 Unexpected objects**

Photo credit: Quebec's Ministry for Transport

### **3.1.10 How will lighting conditions affect VA?**

One of the key environmental conditions that affect VA is lighting so it warrants special comment. First of all, video analytics will require good lighting to work. It simply does not work at night without some illumination (excluding thermal imaging), so consider your requirements from day to night. See Figure 4 for an example of very bad lighting conditions. Rapidly changing light conditions may trigger false alarms. For example, vehicle headlights triggering false alarms or as per Figure 5, sun glare can obstruct a camera view at certain times of the day.



**Figure 4 Poorly lit field of view (FOV)**



**Figure 5 Sunlight obscuring camera view**

### **3.1.11 How much configuration is required?**

Video analytics are rule based and as such will often require configuration to the scene to provide the video analytics with perspective information such as the size of people, vehicles and other objects. Configuration can be critical to minimising false alarms and improving detection rates. The Den Jyske Kontrolcentraal case study in Section 3 highlights how using configuration can greatly affect false alarm rates. Manufacturers should outline what reliability issues the analytics are sensitive to and how much configuration is required. Configuration can greatly affect your budget. Figure 6 and 7 highlights the difference between motion detection and more advanced video analytics. As shown, the number of false alarms with motion detection is greater, due to moving trees.



**Figure 6 Motion detection algorithm**



**Figure 7 Video analytics algorithm**

### **3.1.12 How do you want to be notified of alerts?**

As previously noted, your existing surveillance system will affect your choice of video analytics. You will also need to consider how you want to be notified of alerts, which is often dependent on your existing infrastructure. Will the alert display in your video management software (VMS) client or a separate one? Do you need it sent to a mobile device or can you consider remote monitoring as a service? If false alarms are low and you are detecting intrusions, getting an email alert sent to a phone can be very effective. Larger organisations may have security personnel in a control room watching video live who will view and verify alerts. Other organisations may be satisfied with more remote alert creation via email, etc. or post event investigation of an incident.

### **3.1.13 What is your budget?**

Video analytics greatly differ in price from free to thousands of euro depending on function and sophistication and are typically priced on a per channel basis. If you have a large camera installation base, the cost can rapidly rise. Thought should be given to which cameras need analytics and which cameras might not, depending on risk assessment and performance. Furthermore, associated costs with analytics need to be considered. They often require substantial configuration to the scene to optimise performance and deal with environmental issues such as light, etc. Also, alterations to infrastructure may be required including altering camera positions, cabling, storage and integrations with other surveillance systems. This all has a cost and should be considered at the outset.

### **3.1.14 What support and maintenance is required?**

Support and ease of use should be taken into consideration. These factors should be considered for the various stages of the lifecycle of the solution. Who will perform the installation and how will it be configured? Can this be done remotely or on-site? How will updates be installed and what training is available? How will issues during deployment be dealt with? One area which is often overlooked is keeping the camera lens clean and

obstruction free. A build up of sea salt is common in maritime environments. Spiders are often keen to make a camera their home but in doing so create a web of issues for VA.

### ***3.1.15 What are the legal restrictions which may exist in your country?***

Legal, data protection and ethical considerations should always be considered when deploying CCTV in general. Although the legal status differs across Europe, anyone operating a system should seek to be compliant with the laws that exist in their country. typically there is a distinction between private or public locations and as a general rule, the usage of CCTV should be proportional to risk and seek to be open and fair.



## **4. Video analytics use cases**

Video analytics has been deployed in a variety of ways. Some implementations have been successful and others less so. The purpose of this section is to outline some examples of video analytics deployments, the benefits achieved and complexities encountered.

### **4.1 Den Jyske Kontrolcentsal Case Study: Utilising video analytics in a remote monitoring service**

Den Jyske Kontrolcentsal (see [www.djk.dk](http://www.djk.dk)) offers remote monitoring services to a large variety of customers in Denmark with over 560 cameras across 100 locations. The service they offer relies on the use of video analytics to provide alerts to prevalent events. The detection rate of the alarms is important. Every time they receive an alert, one of their operators has to manually verify it. The company estimates the cost of a false alert to be approximately 50 cents an alert. When you consider that for one of their installations, they had 769 alarms from 4 cameras over a period of 7 days, the cost of false alarms is high, nearly €400 euros. This is why Jakob Hansen says their company has been focusing on adopting more sophisticated video analytics solutions as opposed to simple motion detection. According to Jakob you can get 50 % false alarms with simple motion detection but it can be around 5 % with more sophisticated analytics. However, Jakob notes that the cost of more sophisticated video analytics can quickly ramp up the price, 'It can take anything from 30 minutes to 2.5 hours to calibrate video analytics to the scene. Sometimes this can be done remotely but providing a reference size in the scene is the typical starting point for configuration. So someone of a known height has to walk around.'

Jakob notes that the deployment of video analytics was a success for one of their customers, a Mink farm. The customer was essentially losing stock and wanted to be alerted when minks started to escape or when intruders were present. As this often happened at night, a thermal imaging camera in tandem with a normal camera was set up and analytics were configured to create an alert when objects of a small size (similar to a Mink) escaped. The analytics were also configured to count escaping Mink. Jakob notes that video analytics worked well in this case, as the solution was set up to address a specific requirement and calibrated for optimum results.

At another location they monitor approximately 140 shops each with an average of six cameras. They use cameras with inbuilt motion detection to alert them when someone might enter the grounds of the premises at night. They then filter events by watching them, so the analytics work by aiding monitoring personnel rather than replacing them. Monitoring personnel can then use an intercom voice as a deterrent.

When looking to deploy video analytics, Den Jyske Kontrolcentsal recommends that users do the following. First and foremost, planning is key. Jakob recommends taking the time to really look at the problem that you are trying to solve and mapping out the current and planned camera locations. Too often he sees cameras being erected without due consideration. As a result they often are not placed on the correct location or height and are essentially useless. When thinking about what video analytics to deploy Jakob recommends staying away from simple motion detection as a high number of alarms are created by simple things such as blowing leaves, light changes and so on. He also notes that it is really important to think about integration. Can the video analytics you want to be used be deployed on the edge with cameras that you want to use or already have in place or easily be integrated with your video management software (VMS)?

## **4.2 Post-event investigation: the use of video analytics by law enforcement**

Greater Manchester Police (GMP) is a large metropolitan police force in the United Kingdom. With an ever-increasing workload, GMP wanted to adopt video analytics in order to cut down the time spent watching CCTV during post-event investigation. Detective Chief Superintendent, Head of Crime, Russ Jackson oversees the VERA unit who support major investigation teams. They process over 800 CCTV jobs per year related to major investigations. CCTV is important as it helps verify witness and suspect statements and frequently provides the key evidence to convict perpetrators.

By using a video investigation platform which incorporates video analytics, the unit has been able to significantly reduce the amount of video that they have to sift through and more importantly it has enabled them to find events in video quicker which helps operationally. The average time saving from using video analytics is 79 %.

Once video for a case is recuperated, the VERA team start uploading into a case file in their video investigation platform. Video algorithms read the video, indexing objects and events by colour, location and direction of movement. When an investigator searches by creating a visual filter, the software calls up what has already been detected as it indexed the footage, and shows only the desired events. For example, only people coming and going from a particular door or cars of red colour, etc.

There are significant complexities for law enforcement when dealing with video. They do not have control over the video sources which they make use of. A large portion of video is obtained to third party sources, e.g. hotels, shops, etc. so the format is always different. The video is often of poor quality with low frame rates and poor resolution. It is important that video analytics can deal with such video. The most important thing is that events are detected. The production of false alarms is tolerable. Time and ease of use is important so calibrating video analytics to the scene is not typically possible.

Video analytics for post-event investigation in law enforcement is greatly increasing. It is key time saver but still requires manual interpretation. It aids the investigator rather than replacing one. The quest to be able to automatically find a particular person in video fully automatically from one camera scene to another is required by law enforcement but as yet video analytics cannot provide a significantly robust solution. However, video analytics can greatly expedite manual video investigation reviewing.

## **4.3 P-REACT Research Case Study: Developing a video surveillance system using video analytics**

The P-REACT project is a research project funded by the European Commission under the seventh framework programme (FP7). This project has undertaken to develop a surveillance platform to detect petty or volume crime like break-ins, assaults and general anti-social behaviour in urban and transport domains. At its core the project utilises video analytics as a method to detect such activities. According to project co-ordinator Juan Arraiza Irujo, 'We have developed video analytics to detect unauthorised entry, fighting, running, chasing and graffiti. When these types of behaviour are detected an alert will be

sent to a central monitoring station where they will be reviewed and the appropriate response taken.'

The project participants comprise of organisations specialising in video analytics development and end-users. The key issue to developing a successful solution is getting the right balance between end-user needs and what is technically feasible; notes Mr Arriaza, 'End-users want a system that detects crime events with a 100 % detection rate and as low as possible false alarms.' However, not all crime types can be detected by video analytics as least not without significant configuration to the scene. 'Take bike theft from bike stands', explains Mr Arriaza, 'initially we looked at this crime type as it was a big issue at transport hubs but when we reviewed footage of such crimes, it was very difficult to make out thieves from normal cyclists taking their bikes.'

Therefore, the project seeks to detect behaviours that are indicative of certain crimes For instance if a cashier in a small shop is held up; video analytics will be used to detect leaning over the counter and fighting. In order to improve detection rates, audio analytics to detect screaming and key words will also be used. Similarly, anti-social behaviour at bus stops in certain urban areas was an issue, so video analytics will be used to detect fighting and graffiti in key hot spots.

In order to keep the solution low cost and affordable for small shops a number of design choices were made. Firstly, the analytics will run on an embedded system near the camera which means only events triggered will be transmitted reducing bandwidth costs and potentially enabling the solution to be used with an existing installed camera. Secondly, the analytics have been extensively worked on in order to reduce the level of configuration required making it less costly to install the system. It is intended that the P-REACT system will help to reduce incidents of certain petty crimes by making security personnel and police more proactive in responding to it.

At the time of writing the P-REACT solution was 18 months in to a 24-month development timeline. See [p-react.eu](http://p-react.eu) for more detail.

## 5. Conclusion

Video analytics is an effective and useful technology when deployed appropriately. This document acts as an overview for the end-user and highlights the key factors to take into account when considering video analytics adoption. As outlined in this document there are numerous factors which affect performance, from lighting conditions, scene complexity and image quality to required usage and risk assessment. It is clear that there is a need to better understand the limitations and deployment considerations of video analytics by end-users. Some of the recommendations of this group include:

- appropriate requirement analysis and testing by end-users;
- clear deployment guides and scenarios should be outlined by manufacturers;
- CCTV and security manufacturers should consider the factors affecting video analytics when designing hardware and solutions;
- there is a requirement for performance standards for video analytics taking into account the wide variety of applications and levels of performance.



## References

### References

1. **Erncip Thematic Group Video Analytics & Surveillance**, *Surveillance and video analytics: Factors Influencing the Performance*, Ispra: JRC, 2015.
2. **Home Office**, *CCTV Operational Requirements Manual 2009*, Cohen, N., Gattuso, J. and MacLennan-Brown, K., Publication No 28/09. [Online]  
[https://www.gov.uk/government/uploads/system/uploads/attachment\\_data/file/378443/28\\_09\\_CCTV\\_OR\\_Manual2835.pdf](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/378443/28_09_CCTV_OR_Manual2835.pdf)
5. *Video Analytics: Opportunity or Spoof Story? The State of the Art of Intelligent Video Surveillance*, Massimiliano, A. and Fabio Bisogni, F. s.l. : IEEE, 2011, Intelligence and Security Informatics Conference (EISIC), 2011 European.
3. How many video surveillance cameras as there in this world?  
<https://storageservers.wordpress.com/>. [Online]  
<https://storageservers.wordpress.com/2014/07/30/how-many-video-surveillance-cameras-are-there-in-this-world/>.
4. **CPNI (2014)**, Guide to producing operational requirements for security measures (August 2013) [Online] [http://www.cpni.gov.uk/documents/publications/2010/2010001-op\\_reqs.pdf?epslanguage=en-gb](http://www.cpni.gov.uk/documents/publications/2010/2010001-op_reqs.pdf?epslanguage=en-gb)
5. **CPNI (2015)**, Guidance note: testing installed video analytic systems. [Online]  
<https://www.cpni.gov.uk/Documents/Publications/2015/18%20December%202015%20Guidance%20Note%20Testing%20installed%20video%20analytic%20systems.pdf>
6. **Home Office CAST**, *Image library for intelligent detection systems*, 2010.
7. **Erncip Thematic Group Video Analytics & Surveillance**, *Factors Which Influence the Performance of Surveillance Systems*, s.l.: JRC, 2014.
8. **BSIA, British Security Industry Association** (June 2009), An introduction to video content analysis industry guide, [Online]  
<http://www.bsia.co.uk/publications/publications-search-results/262-an-introduction-to-video-content-analysis-industry-guide.aspx>
9. **Association of Chief of Police Officers** (2011), Practice Advice on the use of CCTV in criminal investigations, [Online] <http://library.college.police.uk/docs/npia/cctv-final-locked-v21-2011.pdf>

## List of abbreviations and definitions

**CCTV** Closed circuit television

**FAR** False alarm rate

**FOV** Field of view

**Pd** Detection probability

**PTZ** Pan-tilt-zoom

**VA** Video analytics

**VCA** Video content analysis

**List of figures**

Figure 1 Foliage blocking camera view..... 14

Figure 3 Unexpected objects ..... 15

Figure 4 Poorly lit field of view (FOV) ..... 15

Figure 5 Sunlight obscuring camera view ..... 16

Figure 6 Motion detection algorithm      Figure 7 Video analytics algorithm ..... 16

**List of tables**

Table 1 VA function overview ..... 10



Europe Direct is a service to help you find answers to your questions about the European Union  
Free phone number (\*): 00 800 6 7 8 9 10 11  
(\*) Certain mobile telephone operators do not allow access to 00 800 numbers or these calls may be billed.

A great deal of additional information on the European Union is available on the internet.  
It can be accessed through the Europa server <http://europa.eu>

#### **How to obtain EU publications**

Our publications are available from EU Bookshop (<http://bookshop.europa.eu>),  
where you can place an order with the sales agent of your choice.

The Publications Office has a worldwide network of sales agents.  
You can obtain their contact details by sending a fax to (352) 29 29-42758.

## JRC mission

As the Commission's in-house science service, the Joint Research Centre's mission is to provide EU policies with independent, evidence-based scientific and technical support throughout the whole policy cycle.

Working in close cooperation with policy directorates-general, the JRC addresses key societal challenges while stimulating innovation through developing new methods, tools and standards, and sharing its know-how with the Member States, the scientific community and international partners.

*Serving society  
Stimulating innovation  
Supporting legislation*

