Surveillance Use Cases: Focus on Video Analytics

ERNCIP Thematic Group Video Analytics and Surveillance

Jeroen van Rest, MSc., TNO

2015

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.

EUR 27851 EN

Surveillance Use Cases: Focus on Video Analytics

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

JRC100401

EUR 27851 EN

ISBN 978-92-79-57770-3

ISSN 1831-9424

doi:10.2788/236268

Contents

Acknowledgements

The author gratefully acknowledges the contributions, suggestions and reviews of the other members of the ERNCIP Thematic Group Video Analytics and Surveillance, the ERNCIP office and of TNO colleagues.

Abstract

This report describes surveillance use cases in the context of protection of critical infrastructure. The focus in this report is on video analytics. This report is created as part of the work of the ERNCIP Thematic Group on Video Analytics and Surveillance.

The broad purpose of the Thematic Group on Video Analytics and Surveillance is:

- to develop a more common approach to the testing and evaluation of video analytics systems;
- to encourage the development of innovative video analytics technologies.

In order to accomplish this, interaction is required with several communities:

1. Critical infrastructure (CI) operators and other end-users;
2. Suppliers of surveillance products and services;
3. National and European policymakers;
4. Research and technology organisations.

The aim of this report is to facilitate the interaction with the relevant communities by providing a limited set of surveillance-use cases which are clustered around several surveillance application areas. This helps make discussions as specific as possible, and to make the results of this thematic group (TG) as relevant as possible for these communities. This first report provides a starting point for this set.

In order to accomplish these goals, common understanding must be obtained and supported among the aforementioned target groups. This is complicated because many factors influence the performance of surveillance and video analytics systems. The usefulness and performance of these systems also depend on the particular context and environment in which they are to be used.

Obviously, surveillance measures cost money, both OPEX and CAPEX. However, depending on their use, security investments can save money, and sometimes also indirectly generate new income. Surveillance has led in practice to:

- less costs due to less incidents;
- less costs due to less impact from incidents;
- more business transactions because customers experience less friction from security measures;
- more business transactions because customers perceive less risk;
- less costs because the liability can be shifted to another party;
- less costs because security can be organised more efficiently;
- less costs because security has less indirect incidental costs (e.g. stress-related absence).

The added value of video analytics is as diverse as the added value of surveillance in general. In a very generic sense, it can help to reduce the amount of footage that must be analysed by humans. This is however too narrow a view, because it suggests that video analytics is only about efficiency gains. For example, video analytics can help to prevent and stop threats, such as terrorist attacks, by deterring adversaries from hardened targets. It can help in the case of a crisis to prevent further damage and to assist in response by increasing the situational awareness. Video analytics can also help by taking over dull, dangerous or 'dirty' tasks. These are gains in effectiveness.

The scope of this report is contemporary surveillance (i.e. around the year 2016) in the physical domain for the protection of CI against security incidents. Protection includes the prevention, disturbance, containment, response and investigation of security incidents. The specific use cases are based on the needs of CI operators and respective law enforcement agencies tasked with this protection throughout the EU. The main criterion for inclusion of a use case in this report is therefore whether end-users have expressed interest in a use case.

A surveillance use case is technology-agnostic: it is defined by the capability it provides in a certain context and environment. The use cases are grouped per type of environment where they typically occur. But, use cases may be relevant in multiple contexts and environments. For example, left luggage is relevant at large international airports, but also at public offices. Use cases are described once, but in such a manner that they can also be used in different environments. Thus, in this chapter, the description of the environment serves as an example, not as a limiting factor.

For each environment a short impression is given of the assets that must be protected, why they are vulnerable and typical threats that may occur.

Surveillance is used in every phase of every security mission. Whether for prevention, protection, response, investigation or for recovery purposes, the capability of creating and maintaining accurate and actual situational awareness is instrumental. This explains the amount of resources that operators of CIs put into surveillance and related capabilities such as identification of persons (biometrics) and detection of hazardous materials (CBRNE).

Developing and harmonising effective surveillance capabilities is relevant for the policies of DG Migration and Home Affairs and DG Justice and Consumers, but also for other European policy areas such as Customs, Migration, Humanitarian aid and civil protection, and Transport.

Most of these European policies also have national variants in the Member States. Surveillance is instrumental for critical infrastructure protection (CIP) and many other security policies. In addition, private organisations and home owners are also allowed to use surveillance capabilities. Because of this wide applicability, there is no separate market of surveillance products for CIP. Surveillance products are in such wide use that harmonising the surveillance market for CIP is only effective if other application domains are also taken into account.

The relevance of surveillance is also illustrated with a brief analysis of the European Security Research and Innovation Agenda (ESRIA). The European Security Research and Innovation Forum (ESRIF) explicitly includes surveillance or situational awareness in each of the five clusters of the ESRIA. Based on such research, a lot of new products and services based on video analytics will enter the EU security market in the coming years.

What exactly constitutes a CI varies in each Member State. CI supports essential functions for Member States and for Europe as a whole. These functions are built upon capabilities and resources of a varied nature: physical assets like buildings, staff and vehicles, but also ICT systems and more abstract assets like networks of trust. Surveillance therefore takes place not only in the physical domain (air, maritime and land), but also in the cyber domain and in online communities. Some of these domains are the focus of other TGs of ERNCIP. The work of this TG currently focuses on surveillance in the physical domain (especially land and sea), with a focus on video analytics. Even with this limitation in scope, there are a lot of (types of) assets to be protected, with a high variety surveillance use cases.

From the perspective of physical security measures, many types of physical objects share a lot of similarities. Many laboratories are basically offices. A factory that is part of the defence industrial base shares a lot of similarities with a factory that produces dangerous chemicals. This is also reflected in the way EU research calls are formulated. Based on this insight, seven classes of physical objects are defined: public transport hub, public building, long infrastructure, industrial site, mobile asset, secured location and office.

The camera (visible light and infrared) is one of the most dominant sensors for the security of CI and urban environments. Cameras work in a very wide range of CI scenarios. Video footage is directly interpretable by humans, and it is accepted as legal evidence. There is a wide range of commercial products and services available for cameras and a large international research infrastructure. As a consequence, law

enforcement agencies, owners of CI and owners of objects in urban environments have invested significantly in video surveillance systems (VSS), and this trend continuous with new developments such as bodycams, unmanned autonomous vehicles and wearable technologies.

Several contemporary video analytics use cases are described in this report which are considered 'not solved'. These use cases have been described in such a way as to be 'technology-agnostic', which makes them invariant to technological developments, and therefore suited to compare different technological approaches on an equal footing. Using the ERNCIP organisation and the framework described in this report, it can easily be extended and/or actualised.

Currently, only some use cases are described. There are some placeholders and summaries for candidates for other use cases and capabilities. Future work of the TG includes extending these use cases. Owners of critical infrastructure and law enforcement agencies are invited to suggest more relevant use cases and desired capabilities.

The next steps are to:

- extend the set of relevant use cases and desired capabilities;
- disclose and develop test data sets for relevant video analytics use cases;
- apply joint innovation early in the case of innovative use of video analytics;
- describe coherent innovation roadmaps for the introduction of video analytics in operations;
- prevent and stop crises with dynamically deployed surveillance capabilities;
- develop large-scale auto calibration in order to make video analytics robust and (ad hoc) scalable;
- develop metadata standards to cover relevant factors influencing video analytics.

1 Introduction

This report describes surveillance use cases in the context of protection of critical infrastructure. The focus of this report is on video analytics. This report is created as part of the work of the ERNCIP Thematic Group on Video Analytics and Surveillance.

The availability of relevant test data sets is very important for all domains that video analytics is used in. For law enforcement agencies (LEA), they are a means to help focus the development of technologies towards actual relevant use cases. For critical infrastructure owners, test data sets help narrow the gap between expected and real value. These interests align with those of citizens, industry and scientists [1].

While the relevance of good data sets is clear in general, it is not likely that one type of stakeholders will consistently create and maintain good relevant data sets, with the incidental exception of some scientists (e.g. PETS). But, since technology, threats and society constantly change, this is for scientists not sustainable. When scientists and emergency services cooperate, a larger set of benefits can be aligned, creating a more sustainable solution (e.g. i-LIDS). However, without a clear chain to business (monetary) benefits, the sustainability of that solution is not high enough in times of budget cuts and austerity. This will not improve in the foreseeable future. So, it is necessary to cooperate with more types of partners, especially those that actually earn money with VA: CI end-users and/or industry. The EU has — within the ERNCIP project TG VAS — recognised this challenge and is willing to give organisational support. The vision of the TG VAS is that communities of CI end-users, or of industrial branch organisations (have) develop repositories of — for them — relevant data sets because this will give them clear business continuity and monetary benefits, if only they can acquire the knowledge to do so.

1.1 Purpose

The broad purpose of the Thematic Group on Video Analytics and Surveillance is:

- to develop a more common approach to the testing and evaluation of video analytics systems;
- to encourage the development of innovative video analytics technologies.

In order to accomplish this, interaction is required with several communities:

1. Critical infrastructure operators and other end-users;
2. Suppliers of surveillance products and services;
3. National and European policymakers;
4. Research and technology organisations.

The aim of this report is to facilitate the interaction with the relevant communities by providing a limited set of surveillance use cases which are clustered around the application areas of the previous sections. This helps make discussions as specific as possible, and to make the results of this TG as relevant as possible for these communities.

Specifically, in this introduction and in [1] the relevance of high quality test data sets for video analytics has been described. This requires a specification of those relevant use cases, of which a first proposal can be found in this report.

1.2 Common understanding

In order to accomplish these goals, common understanding must be obtained and supported among the aforementioned target groups. This is complicated because many factors influence the performance of surveillance and video analytics systems. The usefulness and performance of these systems also depend on the particular context and

environment in which they are to be used. For example, intruder detection in an indoor office at night is very different from 24 hours per day intruder detection in an outdoor woodland area. The factors that influence the (perceived) performance of surveillance and video analytics have been described in [1]. In that report, we give a comprehensive method and model that can be used to describe incidents, security measures, projects, data sets, products, R & D outcomes, use cases and the relations between them. In addition, we identify several myths, partial truths and misconceptions which are repeated here because they are essential for proper understanding and appreciation of this report:

'There are no limits to what video analytics can do.' The consequence of this misconception is that the public has unrealistic expectations of what video analytics can do. This is also known as the CSI effect, because in such television series images can be enhanced indefinitely, and during the investigation, the viewpoint on the scene can still be changed. It is true that with modern technologies such as super-resolution and various forms of sensor fusion it is possible to generate new **views** on existing, combined data, but it is against the laws of nature to generate new **data** out of thin air.

'A camera has never caught a criminal.' But neither has a police car or a uniform. This statement suggests that cameras do not contribute to security. This is a misleading statement because the security function of cameras is to contribute to situational awareness and to deter. Both of which they have been shown to do, if used properly.

'Crime displacement is the Achilles heel of situational security measures.' Crime displacement is an effect on the target selection phase of a criminal. Depending on the purpose of the security measures, this can be a very desirable effect.

'Security only costs money.' A **security department** does not generate income for a business, nor should a police organisation generate net income for a state. But an investment in security measures can reduce costs, and sometimes even help generate more income.

'Video analytics is not fulfilling its promise.' There can be a significant difference between expected performance and the realised performance. Video analytics are being applied successfully in a growing number of scenarios. At the same time, there is a lot of active research, so the 'promise' is continually expanded.

'Security through obscurity is bad.' Obscurity hampers peer review, which may lead to prolonged existence of weaknesses in the security mechanism and hinders accountability. On the other hand, obscurity represents a cost factor in the preparation of adversaries, and as such contributes to deterrence.

'Video analytics is an add-on.' Video analytics is indeed a separate capability. However, it can make or break a business case, and it requires significant attention to the way it is incorporated in work processes, the user interface, IT infrastructure, etc. If the use of video analytics is bolted on at the end of a system engineering process, then the chance of it contributing to the desired impact is substantially minimised. In other words, the use of video analytics should be incorporated from the beginning, not only at the end. Other ways to formulate this is 'video analytics is plug-and-play'.

1.3 Approach

The challenge which is addressed in this report is:

1. to describe surveillance use cases which are relevant for the target communities of this TG; and
2. to describe them in such a way that they are encouraging innovation;
3. while still allowing the provision of clear direction on the actual performance and future potential in operational use.

The approach is to use the methodology introduced in [1] to scope and describe surveillance use cases. Per use case an assessment is made on whether there is an active market, and on whether there is active R & D.

1.4 Scope

The scope of this report is contemporary surveillance in the physical domain for the protection of CI against security incidents. Protection includes the prevention, disturbance, containment response to, and investigation of security incidents. The specific use cases are based on the needs of CI operators and respective law enforcement agencies tasked with this protection throughout the EU. The main criterion for inclusion of a use case in this report is therefore whether end users have expressed interest in a use case.

Examples of application domains (and use cases) that are out of scope, are therefore:

- the protection of crowds at festivals and sporting events, because they are not CI;
- specialised forensic instruments, unrelated to CI;
- workplace safety monitoring, because the scope is on security.

1.5 Terminology

The terminology and abbreviations are described at the end of this report, and described in more detail in [1].

2 Surveillance in the EU context

Surveillance is used in every phase of every security mission. Whether for prevention, protection, response, investigation or for recovery purposes, the capability of creating and maintaining accurate and actual situational awareness is instrumental. This explains the amount of resources that operators of CI put into surveillance and related capabilities such as identification (e.g. biometrics) and detection (e.g. CBRNE).

2.1 The relevance of surveillance for EU policies

Developing and harmonising effective surveillance capabilities is relevant for the policies of DG Migration and Home Affairs and DG Justice and Consumers, but also for other European policy areas such as Customs, Migration, Humanitarian aid and civil protection, and Transport (Table 1, Table 2, Table 3).

Table 1 European policy areas which rely on surveillance

European policy area	Respective policies which rely on surveillance
Customs	Facilitating trusted traders
Humanitarian aid and civil protection	Protection; Capacity building; Resilience; Forest fires; Monitoring tools
Justice and home affairs	See separate tables for DG Migration and Home Affairs and DG Justice and Consumers
Research and innovation	See separate table for FP7 Main Security Missions
Transport	Security and safety; Infrastructure

This table excludes defence policies.

Table 2 DG Migration and Home Affairs policy areas which rely on surveillance

DG Migration and Home Affairs policy area	Respective policies which rely on surveillance
Common European Asylum System	Temporary protection; Reception conditions; Asylum procedures
Organised crime and human trafficking	Crime prevention; Trafficking in human beings; Trafficking in firearms; Child sexual abuse; Money laundering; Corruption; Counterfeiting; Confiscation and asset recovery
Crisis and terrorism	EU Counter Terrorism Strategy; Prevention and protection; Radicalisation and recruitment; Explosives; Critical infrastructure (See CIP Areas, Table 5); Security research (See FP7 Main Security Missions); Crisis management, Terrorist Financial Tracking Programme

DG Migration and Home Affairs policy area	Respective policies which rely on surveillance
Police cooperation	Law enforcement; Prüm Decision; Passenger name record
Immigration	Curbing irregular immigration; Organising legal immigration better
Schengen, borders and VISA	Smart borders; Border crossing; Schengen Area
Internal security	Internal Security Strategy; Harmony Process; Standing Committee On Operational Cooperation On Internal Security (COSI)

Table 3 DG Justice policy areas which rely on surveillance

DG Justice and Consumers policy area	Respective policies which rely on surveillance
Fundamental rights	Rights of the child; Racism and xenophobia; Homophobia
Criminal justice	Judicial cooperation; Recognition of decisions between EU countries
Data protection	All topics
Gender equality	Ending gender-based violence
Tackling discrimination	All topics
Drugs control policy	Drugs situation in the EU; EU response to drugs

Most of these European policies also have national variants in the Member States. In addition, private organisations and home owners are also allowed to use surveillance capabilities.

Surveillance is instrumental for CIP and many other security policies.

Because of this wide applicability, there is no separate market of surveillance products for CIP.

Surveillance products are in such wide use, that harmonising the surveillance market for CIP is only effective if other application domains are also taken into account.

2.2 Surveillance in EU research

The relevance of surveillance is also illustrated with a brief analysis of the European Security Research and Innovation Agenda (ESRIA) [2]. The European Security Research and Innovation Forum (ESRIF) explicitly includes surveillance or situational awareness in each of the five clusters of the ESRIA (Table 4).

Table 4 FP7 Main Security Research Missions all relate to surveillance

EU Main Security Research Mission	Research areas which include surveillance
Security of citizens	Organised crime; Intelligence against terrorism; Explosives; Ordinary crime and forensics; CBRN protection; Information gathering
Security of infrastructures and utilities	Surveillance
Intelligent surveillance and border security	Sea borders; Land borders; Air borders; Border checks; Intelligent border surveillance
Restoring security and safety in case of crisis	Preparedness, prevention, mitigation and planning; Response; CBRN Response

Besides these explicit mentions, surveillance is also typically mentioned in the context of higher level research capabilities such as protection, intelligence, preparedness, response, investigation, and recovery. As a consequence, the ESRIA expresses a wide range of research needs in areas such as land, maritime, air, space, financial and online surveillance, sensors and sensor integration, positioning and localisation technologies, behaviour analysis and analytics.

The FP7 and Horizon 2020 working programmes operationalise these needs into research calls. The FP7-SECURITY programme alone has funded 49 projects related to surveillance, and more have been funded in FP7-TRANSPORT, FP7-ICT, FP7-INFRASTRUCTURES, FP7-PEOPLE, FP6-IST and PASR. In the Horizon 2020 Work Programme 2014-2015 this expression of demand is continued.

Figure 1 shows the current ([1]) planned and realised EU research effort for projects related to surveillance ([2]), and related to video analytics, based on an extract of the EU Cordis database ([3]) and the ITEA and ARTEMIS R & D programmes. If we assume a time-to-market of 2-5 years of this kind of research, then a lot of new products and services based on video analytics will enter the EU security market in the coming years. Appendix A contains a list of these video analytics projects, and the ERNCIP website for the TG VAS also contains a webpage with more information.

([1]) The stagnation in 2013 is probably due to the gap year between FP7 and H2020.
([2]) This data includes projects about surveillance sensors, surveillance and command rooms, surveillance data interoperability and surveillance and privacy. It excludes projects which are about other domains, e.g. healthcare, or are only about niches, e.g. biometrics, CBRNE, maritime surveillance, cyber, safety of transport and logistics or money laundering.
([3]) The Cordis database is not very up to date. Sometimes projects that have started in January have not been registered until October of that year.

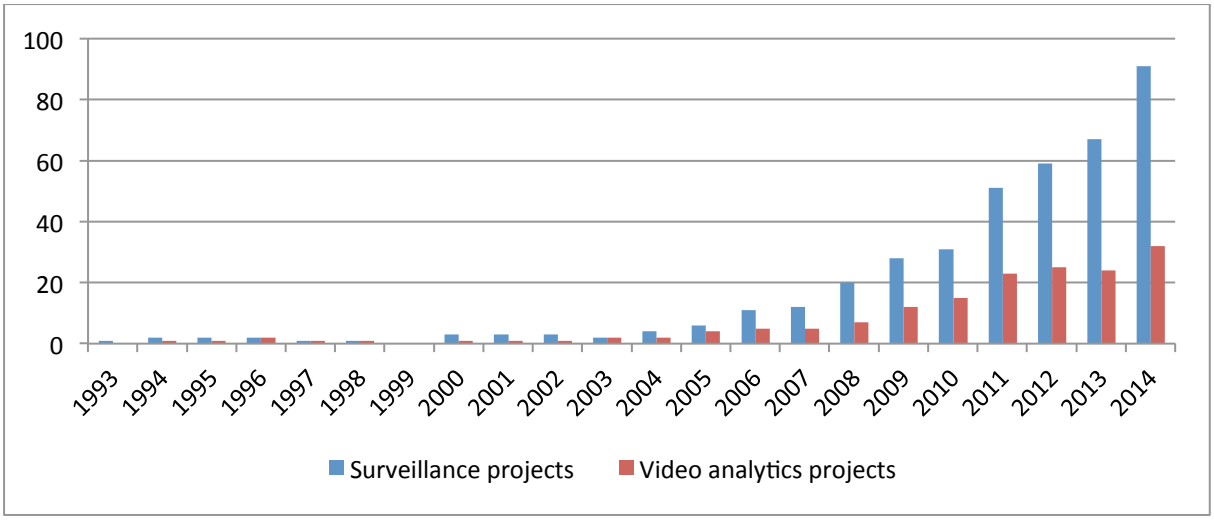

Figure 1 The effort in EU projects per year from surveillance-related projects and for video analytics projects (EU Cordis database).

2.3 Surveillance for critical infrastructures

What exactly constitutes a CI varies per Member State [3]. CI supports essential functions for Member States and for Europe as a whole. These functions are built upon capabilities and resources of a varied nature: physical assets like buildings, staff and vehicles, but also ICT systems and more abstract assets like networks of trust. Surveillance therefore takes place not only in the physical domain (air, maritime and land), but also in the cyber domain and in online communities. Some of these domains are the focus of other TGs of ERNCIP.

The work of this TG currently focusses on surveillance in the land domain. Even with this limitation in scope, there are a lot of assets to be protected, with a large variety (Table 5).

Table 5 Physical objects to be protected as part of a critical infrastructure

Critical infrastructure	Typical objects to be protected
Energy (including nuclear)	Energy plants, pipes, offices, storage depots
ICT	Data centres, offices, communication cables, radio transmitters, distribution centres
Finance	National banks, offices, high value transports
Healthcare	Hospitals, laboratories, offices
Food	Distribution centres
Water	Dikes, sluices, water barriers, water basins, pipes
Transport	Train stations, roads, railroads, airports, offices, ports, mobile assets, bridges, tunnels
Safety	Prisons, police and fire stations, offices

Critical infrastructure	Typical objects to be protected
Government	Offices, embassies, parliaments, individuals, homes, palaces, military compounds
Chemicals	Industrial plants, factories, storage depots, chemical transport, offices
Defence industrial base	Industrial plants, storage depots, factories, weapon transport, offices
Legal/judicial	Courtrooms, prisoner transport
Space and research facilities	Laboratories, launch pads, offices, mobile assets

In practice, CIP involves not just the prevention of incidents, or the containment of the consequences, but also the investigation after an incident (e.g. by law enforcement) and the preparation before (e.g. assessing the pattern of life, i.e. creating and maintaining a model of what is normal). This is further described in section 2.1 of [1].

Security measures have to be adapted to the desired level of resistance, e.g. if the critical infrastructure is highly redundant, then individual objects do not need a lot of protection. So, only specific elements of a CI need protection. For example, within the CI healthcare, certain laboratories, large hospitals and storage depots of vital vaccines may need physical security measures, but not every individual medical post.

2.3.1 Classes of physical objects

From the perspective of physical security measures, many types of physical objects share a lot of similarities. Laboratories are often basically offices. A factory that is part of the defence industrial base shares a lot of similarities with a factory that produces essential chemicals. This is also reflected in the way EU research calls are formulated ([4]). Based on this insight, seven classes of physical objects are defined: public transport hub, public building, long infrastructure, industrial site, mobile asset, secured location and office. Table 6 describes how all types of physical objects map to one or more of these classes. The remainder of this report is structured according to these classes.

([4]) EU Research calls formulate generic application areas, e.g. topic SEC-2010.2.3-3 of the 2010 FP7 Security call: Automatic detection and recognition of threats to critical assets in large unpredictable environment: 'The task consists (1) to develop tools that integrate smart surveillance information system and (2) to improve relevant sensors in terms of affordability, autonomy, robustness and display from heterogeneous critical assets (e.g. mobile assets and/or temporary sites/plants).'

Table 6 Examples of physical objects that may need protection.

Critical infra	Public transport hubs	Public buildings	Long infrastructure	Industrial sites	Mobile assets	Secured location	Office
Energy (including nuclear)			Pipe	Energy plant, Storage depot			Office
ICT			Network cable	Data centre, Radio transmitter, Distribution centre			Office
Finance					High value transport	National bank	Office
Healthcare		Hospital		Lab			Lab, Office
Food				Distribution centre			
Water			Dike, Sluice, Water barrier, Pipe	Water basin			
Transport	Airport, Train station	Train station	Road, Railroad, Bridge, Tunnel	Port	Vehicles, Boats, Airplanes		Office
Safety		Police station			Emergency vehicle, Mobile command post	Prison, Police and fire station	Office
Government		Embassy, Parliament, Hotel, Monument		Military compound	Individual	Military compound, Home, Palace, Embassy	Office
Chemicals				Industrial plant, Factory, Storage depot	Chemical transport		Office
Defence industrial base				Industrial plant, Storage depot, Factory	Weapon transport		Office
Legal/ judicial					Prisoner transport	Courthouse	
Space and research facilities				Lab, Launch pad	Transport of space infra		Lab, Office

The threat can also vary considerably: infiltrators, angry mobs, weather events, lone wolfs or work accidents all require different measures. Several (sub)sectors have therefore created elaborate design basis threats (see section 3.3.4 of [1]).

2.4 Monetary perspective on risk management measures for CIP

A surveillance measure for security, such as video analytics, is an example of a risk management measure. As such, investments in such measures should be based on a

generic cost-effectiveness analysis, where the effectiveness relates to the contribution to risk management. For CIP, this is complicated due to the fact that CI should by definition be considered from a networked perspective due to the effect of cascading risk. This potentially complicates the cost-effectiveness analysis, as it should also weigh the benefits for services depending on the respective infrastructure.

As part of the generic cost-effectiveness analysis, it may also make sense to make a more specific cost–benefit analysis, i.e. strictly confined to the monetary perspective on the investment. Obviously, surveillance measures cost money, both OPEX and CAPEX. However, depending on their use, security investments can save money, and sometimes also indirectly generate new income.

The following positive monetary effects have been observed in practice ([5]):

- Less costs due to less incidents;
- Less costs due to less impact from incidents;
- More business transactions because customers experience less friction from security measures;
- More business transactions because customers perceive less risk;
- Less costs because the liability can be shifted to another party;
- Less costs because security can be organised more efficiently;
- Less costs because security has less indirect incidental costs (e.g. stress-related absence).

2.5 The relevance of video analytics for EU policies

The camera (visible light and infrared) is one of the most dominant sensors for the security of CI and urban environments. Cameras work in a very wide range of CI scenarios. Video footage is directly interpretable by humans, and it is accepted as legal evidence. There is a wide range of commercial products and services available and a large international research infrastructure. As a consequence, LEAs, owners of CI and owners of objects in urban environments have invested significantly in video surveillance systems (VSS), and this trend continues with new developments such as bodycams, UAVs and wearables.

The added value of video analytics is as diverse as the added value of surveillance in general (section 2.1 in [1]). In a very generic sense, it can help to reduce the amount of footage that must be analysed by humans. This is however a too narrow view, because it suggests that video analytics is only about efficiency gains. The next three paragraphs contain three examples of different kinds of benefits of the introduction of video analytics.

Certain kinds of human behaviour are indicative of hostile intent [1]. The analysis of these kinds of patterns of behaviour is very difficult for humans, so in practice it is rarely done. Video analytics can help find such patterns. As such they can help 'predict' future events. This helps to prevent and stop incidents.

([5]) In the preparation of this report, it appeared to be impossible to find a clear and complete model that lists these potential monetary benefits (and costs) of investments in risk management measures. Existing models such as ROSI and ALE are limited to only the first two elements of this list, and the outcome of more generic methods, such as ROI and the aforementioned generic cost-effectiveness analysis appears to depend mainly on the expertise of the participants, rather than a concrete and explicit checklist. If such a model is indeed absent, then risk management investment decisions will have often been made on incomplete information, in such cases underestimating the monetary benefits of investments in risk management measures [12].

In the case of a crisis in CI or urban environments, such as a terrorist attack, LEAs suddenly gain (legal) access to many more surveillance cameras which can help to prevent further damage and assist in response by increasing the situational awareness. These are extra cameras that are not worked with under normal circumstances. Those cameras are under normal circumstances used to sustain a certain type of capability and therefore they may be equipped with different types of analytics — or none at all — than are required during a crisis. Auto calibration can help to scale up video analytics deployments while still achieving reliable performance. As such it can help to manage crises, e.g. terrorist attacks.

Certain kinds of incidents generate emotionally disturbing information, including video footage. This can include human trafficking, child pornography, terrorist incidents, etc. Analysing this footage 'by hand' leads to severe cognitive and emotional loads and/or suboptimal workloads for human operators. Video analytics can help to take over these dull, dangerous or 'dirty' tasks, thereby preventing absenteeism.

3 Surveillance use cases

This chapter describes several contemporary surveillance use cases in a structured manner. A surveillance use cases is technology-agnostic: it is defined by the capability it provides in a certain context and environment. The use cases are grouped per type of environment where they typically occur. But use cases may be relevant in multiple contexts and environments. For example, left luggage is relevant at large international airports, but also at public offices. Use cases are described once, but in such a manner that they can also be used in different environments. Thus, in this chapter, the description of the environment serves as an example, not as a limiting factor.

For each environment a short impression is given of the assets that must be protected, why they are vulnerable and typical threats that may occur.

The structure of each section is:

- Environment of a physical critical infrastructure:
  - Use case (includes threats)
    - Capability (to mitigate the threat)

> Currently, only some use cases are described. There are some placeholders and summaries for candidates for other use cases and capabilities. Future work of the TG includes extending these use cases. Owners of critical infrastructure and law enforcement agencies are invited to suggest more relevant use cases and desired capabilities.

The environments and use cases are described using the morphological analysis of the surveillance domain (MAS). The capabilities are described using a morphological analysis of the video analytics subdomain. Both methods are introduced and described in [1]. The benefit of using these methods here is that a lot of information can be given in a short manner, while still being very specific. The drawback is the learning curve involved.

> The cursory reader may want to skip the descriptions of the use cases and capabilities, and just focus on their heading titles.

3.1 Public transport hub

There are several significant interests at stake at public transport hubs, e.g. airports and train stations. These are usually of a symbolic, economic, defensive and logistical nature. Additionally, the nature of operating a public transport hub is vulnerable in several aspects. The gathering of large amounts of people, high value goods, planes during take-off and landing, but also a plane at cruising height or a high speed train are interesting targets — or even weapons. Because of their highly connected nature, a small local accident can have global consequences. So, there are also less tangible vulnerabilities such as the continuity of the operation, both on the hub itself, in local logistical chains and in connecting hubs. There is a wide variety of threats directed at such hubs coming from accidents, petty crimes, organised crime and terrorism.

MAS: Privacy awareness: medium, high; Relation: the same; Type of environment: built-high rise, built low-rise, road, rural, water, coast, closed indoor, open indoor; Type of object: long infrastructure, public transport hub, street; Existing infrastructure: high; Compartments present: observation area, perimeter, access gate, outdoor, door, indoor room; Closed compartments: perimeter, access gate, outdoor, door, indoor room; Asset to protect: public order, the wellbeing of a crowd, the continuation of a process, the integrity of an object; Target: individual, building, crowd, small object, industrial infrastructure, vehicle, security system; Threat direction: accident, nature, media, illness, activist, criminal, extremist, terrorist;

3.1.1 Use case left luggage

Left luggage at crowded locations can be a sign of an attack with a bomb, or of a criminal transaction (e.g. selling of drugs). Even if the luggage was just forgotten without any bad intentions, the owner will at some point miss his luggage which may cause frustration of the airport operation and discomfort for this passenger, his travel group and other passengers.

MAS: People density: low, medium, high; Asset to protect: public order, the wellbeing of a crowd, the continuation of a process, the integrity of an object; Threat direction: accident, criminal, extremist, terrorist; Frequency: multiple and persistent, fact; Number of attackers: none, individual; Capabilities: none, weapons; Physical angle of attack: ground; Modus operandi: negligence, bombing; Equipment: none, explosive, dirty bomb; Incident phase: during, after; Vulnerability: false alarms, security awareness; Chance: high; Impact: low, medium, high; Responsibility: private industry;

A contemporary intelligent CCTV surveillance system that would help mitigate this risk, could be described as follows:

MAS: Modality: visible light, smell; Sensor type: camera, human, animal; Active: passive, visible light; Invasiveness: not significant, slight; Array form: single, wide baseline; Platform: fixed, rotating; Amount of sensors: 100; Distance sensor object: 10m; Type of object: individual, container; Type of material to be observed: biological, metal, plastic, cloth; Amount of objects to be observed: 1, 2, 10, 100; Function: detect; Surveillance pattern: bag of words, scenario view; Aspect: presence; Security process: in-the-act; Threat assessment: threatening objects or persons, incident phase; Development phase: use; Subcomponents: sensor, storage, network, processing unit, viewing station, human operator, human on the floor;

Within this use case, there are several tasks which could be solved with video analytics. For these tasks more specific descriptions are given.

3.1.1.1 Capability: indoor detection of left luggage

MAVA: Cover: indoor; Light: lamp; Amount of objects: 1, 5, 10, 100; Distance to object: 10m; Orientation: skim; Modality: visible light; Array form: single; Platform: fixed, rotating; Function: detection; Object type: baggage; Aspect: presence;

3.1.1.2 Capability: indoor determining owner

MAVA: Cover: indoor; Light: lamp; Amount of objects: 1; Distance to object: 10m, 100m; Orientation: skim; Modality: visible light; Array form: single; Platform: fixed, rotating; Function: detection; Object type: person; Aspect: presence, behaviour; Relation: temporal, spatial, interaction;

3.1.1.3 Capability: indoor locating owner

MAVA: Cover: indoor; Light: none, lamp; Amount of objects: 1, 5, 10, 100, 1000; Distance to object: 10m; Orientation: skim; Modality: visible light; Array form: single; Platform: fixed, rotating; Function: recognition; Object type: person; Aspect: location;

3.1.1.4 Capability: indoor following owner

MAVA: Cover: indoor; Light: lamp; Amount of objects: 1, 5, 10, 100; Distance to object: 10m; Orientation: skim; Modality: visible light; Array form: single, wide baseline; Platform: fixed, rotating; Function: tracking, recognition; Object type: person; Aspect: location;

3.1.2 Use case breach of secured indoor area

On airports, airside and landside are two different compartments with a strictly governed security filter in between. There are also many other secured areas where critical

functions of the airport are housed. When unauthorised people enter such compartments, this can have far-reaching consequences, e.g. the evacuation of the airside compartment. For safety reasons, certain doors may not be locked, which creates a vulnerability.

MAS: Type of environment: closed indoor, open indoor; Type of object: public transport hub; Existing infrastructure: high; Compartments present: access door / gate, secured area (ring 2), observation area (ring 3); Closed compartments: access door / gate, perimeter, secured area (ring 2); People density: low, medium; Asset to protect: the integrity of an object; Target: none, building; Threat direction: accident, media, activist, criminal, extremist, terrorist; Frequency: multiple and persistent; Number of attackers: none, individual; Capabilities: none; Physical angle of attack: ground; Modus operandi: negligence, burglary; Equipment: none; Incident phase: during; Vulnerability: false alarms, access control, security awareness; Chance: medium, high, fact; Impact: low, medium; Responsibility: private industry;

A contemporary intelligent CCTV surveillance system that would help mitigate this risk, could be described as follows:

MAS: Modality: visible light; Sensor type: camera; Active: visible light; Invasiveness: slight; Array form: single, wide baseline; Platform: fixed; Amount of sensors: 1, 2; Distance sensor object: 10m; Type of object: individual; Type of material to be observed: biological, cloth; Behaviour to be observed: tailgating, trespassing; Amount of objects to be observed: 1, 2, 10; Function: detect; Surveillance pattern: threshold alarm, concentric circles of protection; Aspect: presence, behaviour; Security process: in-the-act; Threat assessment: threatening objects or persons; Development phase: use; Subcomponents: sensor, processing unit;

Within this use case, there are several tasks which could be solved with video analytics. For these tasks more specific descriptions are given.

3.1.2.1 Capability: indoor detection of loitering

MAVA: Cover: indoor; Light: lamp; Amount of objects: 1, 5, 10; Distance to object: 10m; Orientation: skim; Modality: visible light; Array form: single; Platform: fixed; Function: detection; Object type: person; Aspect: behaviour;

3.1.2.2 Capability: indoor detection of tailgating

MAVA: Cover: indoor; Light: lamp; Amount of objects: 2; Distance to object: 1m; Orientation: top down, skim, side; Modality: visible light; Array form: single; Platform: fixed; Function: detection; Object type: person; Aspect: behaviour; Relation: temporal, spatial;

3.1.2.3 Capability: indoor detection of walking against the mandatory flow

MAVA: Cover: indoor; Light: lamp; Amount of objects: 1, 5, 10, 100; Distance to object: 1m, 10m; Orientation: top down, skim; Modality: visible light; Array form: single, stereo, wide baseline; Platform: fixed; Function: detection; Object type: person, crowd; Aspect: flow;

3.1.2.4 Capability: indoor detection of passing through a door

MAVA: Cover: indoor; Light: lamp; Amount of objects: 1; Distance to object: 1m, 10m; Orientation: skim, side; Modality: visible light; Array form: single; Platform: fixed; Function: detection; Object type: person; Aspect: behaviour;

3.1.2.5 Capability: indoor sterile zone detection

MAVA: Cover: indoor; Light: lamp; Amount of objects: 1; Distance to object: 10m, 100m; Orientation: skim; Modality: visible light, heat; Array form: single; Platform: fixed; Function: observation, detection; Object type: person; Aspect: presence;

3.1.2.6 Capability: indoor following intruder

This is identical to 'Capability: indoor following owner' described in section 3.1.1.4.

3.1.3 Use case public order management

Within public transport, police officers patrol transport hubs. They rely on cooperation with centralised CCTV operators. In addition, the bodycam is emerging [4] as a surveillance platform in such scenarios.

This is the MAS for a police officer with a bodycam out of the reach of fixed CCTV.

MAS: Type of environment: built-high rise, built low-rise, closed indoor, open indoor; Type of object: public transport hub, street, vehicle; Existing infrastructure: high; People density: low, medium, high; Physical angle of attack: ground; Modus operandi: demonstration, molest, vandalism; Chance: low, medium, high, fact; Impact: low, medium, high; Responsibility: individual, private industry, regional, public; Modality: visible light, sound, heat; Sensor type: camera, IR-detector, microphone, human, GPS; Active: passive, visible light; Invasiveness: not significant, slight; Array form: single, stereo, movement; Platform: free moving; Amount of sensors: 1; Distance sensor object: 1m, 10m; Type of object: individual, group, bicycle, motorcycle, car, van, bus, tractor, lorry, train/tram, public service vehicle; Amount of objects to be observed: 100 and 10000; Function: observe, detect, classify, identify; Aspect: presence, number plate, face, behaviour, identity; Security process: preparation, intelligence, prevent, in-the-act, investigation; Development phase: use;

3.1.3.1 Capability: aggression detection against bodycam user

MAVA: Light: none; Amount of objects: 1, 5; Distance to object: 0m, 1m, 10m; Orientation: side; Modality: visible light, heat; Array form: single; Platform: free moving; Image improvement: stabilisation; Object type: person; Aspect: behaviour;

3.1.4 Use case maintenance

For large video analytics deployments, maintenance becomes a separate use case (section 6.3.3 of [1]). In such large deployments, the environment is always changing, which requires maintenance on the camera deployment.

3.1.4.1 Capability: auto calibration of large VSS deployments

MAVA: Amount of objects: 1000; Function: calibration; Object type: camera; Aspect: location, orientation;

3.1.5 Use case crisis management

In the case of a crisis, many more cameras become available.

3.1.5.1 Capability: auto calibration of heterogeneous VSS deployments

The capability is identical to the 'Capability: auto calibration of large VSS deployments' described in section 3.1.4.1. But in this case it is applied in an ad hoc setting. More information is described in sections 6.3.3. and 6.3.4 of [1].

3.2 Public building

A public building is a building without access control, i.e. the general public can enter freely. The reason is typically because of the nature of their function, or because of their symbolic value. Examples are a hospital, a parliament or a monument. These are therefore vulnerable objects.

3.2.1 Use case crowd control

A crowd can be(come) a threat as part of a protest or demonstration, or if the capacity of the building is simply too small for the amount of people that want to use it. Typical tasks include people counting, density estimation, flow estimation, detecting the mood and level of intoxication and the detection of specific groups in the crowd.

3.2.2 Use case bomb threat

An explicit bomb threat (i.e. not just lost luggage) threatens integrity and use of the building. Typical tasks include evacuation monitoring, detection of suspicious behaviour and the detection of left luggage. This may have similarities to the 'Use case crisis management' in section 3.1.5.

3.3 Long infrastructure

Long infrastructure is infrastructure that connects remote objects, usually for purposes of transport (rail, highway), transport of energy (oil, gas), or for telecommunication (internet, phone). Long infrastructure is vulnerable because a local interruption may hinder the capacity of the entire object. It is also difficult to protect because it is spread out over a large area.

Effects in long infrastructure often cascade to a lot of other critical infrastructures, such as healthcare, government, food, safety and legal/justice.

Typical use cases are sabotage, e.g. from environmental activists and stealing, e.g. from energy pipelines.

3.4 Mobile asset

There are many kinds of mobile assets, ranging from individuals to cars, trucks, trains, ships and aircraft.

3.4.1 Use case cargo theft at highway

A single cargo theft should not have a serious impact on a critical infrastructure. But if certain routes have to be avoided because of frequent, or particular violent attacks, or when specific types of cargo are particularly at risk, then the infrastructures starts to lose its function. Cargo is particularly vulnerable at parking lots.

3.5 Secured location

Secured locations such as courthouses, palaces, national banks and police stations have several perimeters. Only a small part of the location may be open to the public, if any at all.

3.5.1 Use case intrusion

Intrusion can happen in many different manners. One manner is to transport illicit material into the facility (e.g. drugs into a prison) by a small radio-controlled helicopter. Another is for someone to sneak over a fence.

3.6 Industrial site

Large industrial environments are inherently very complex systems to be monitored and controlled, given the presence of machines, vehicles, people and industrial or commercial plants. There are many people working in the facility and there are guided persons visiting the facility. Such facilities have several perimeters. The entrance to the facility is guarded and all passages in and out are checked regarding identity and for illicit material.

3.7 Offices

This concerns offices with high respect for integrity. Assume a public office to which the public have access with right to remain anonymous. Still there is a need for surveillance to detect illegal threats to official servants and to the public visiting the premises.

3.7.1 Use case visitor threats

There is a need for surveillance to detect threats while not revealing the identity of the visitors except when there is a crime on going or suspected to be imminent.

4 Conclusions and next steps

Several contemporary video analytics use cases are described which are considered 'not solved'. These use cases have been described in such a way as to be 'technology-agnostic', which makes them invariant to technological developments, and therefore suited to compare different technological approaches on an equal footing. Using the ERNCIP organisation and the framework described in this report and in [1], it can easily be extended and/or actualised.

Currently, only some use cases are described. There are some placeholders and summaries for candidates for other use cases and capabilities. Future work of the TG includes extending these use cases. Owners of critical infrastructure and law enforcement agencies are invited to suggest more relevant use cases and desired capabilities.

The next subsection gives more detail about the next steps in the line of disclosing and developing test data sets for video analytics. It is followed by the description of more generic next steps as were already introduced in [1].

4.1 Disclose and develop test data sets for video analytics

The use cases described in this report can be used to specify the disclosure and development of test data sets for video analytics, as per the first recommendation of [1]. It is recommended to proceed with the other steps:

(1) To write a clear argument as to why data sets matter in the boardroom of CI end users and industry;
(2) To create an ICT infrastructure that helps disclose existing test data sets;
(3) To write a manual for creating high quality relevant data sets;
(4) To write a manual for maintaining and creating a repository of data sets to be used by scientists, industry and CI end users, validated by emergency services and CI end users.
(5) To describe a procurement framework to be used by CI end users when procuring VA, making use of these data sets and repositories.

4.2 Joint innovation

At a certain maturity level, test data sets are not sufficient anymore. Therefore, the pitfall of using test data sets is to also use them too late in the innovation process. The impact of using video analytics on the business can be substantial, and there is a learning curve involved. If the respective parties (CI and LEAs) do not have substantial experience with video analytics already, then it is wise to introduce video analytics gradually in the working environment. This allows the business to adapt in their own tempo, and this gives time to industry and R & D to adapt and improve the capabilities as required. This is called joint innovation.

In real working conditions, the threat that the new capability should address may not manifest itself frequently. But, obviously, representative data should be generated to test, develop and adapt the capability. It may therefore be required to start using red teams during this gradual introduction.

4.3 Develop large-scale auto calibration

Auto calibration is an accelerator — and sometimes even an enabler — for the development, deployment and scalability of video analytics in many types of CI [1]. As such it is relevant for all use cases, but in practice it is often 'hidden' within them. In this report, this use case has been made explicit, for example in sections 3.1.4.1 and 3.1.5.1, but this use case should be part of every large-scale or ad hoc scenario.

Auto calibration is currently emerging from research laboratories [5]. It is recommended to start a dedicated effort to develop large-scale auto calibration for large-scale operational use in the context of urban environments and CI. This is described in more detail in section 6.3.4 and Appendix F, both in [1].

4.4 Roadmap for the innovation, development and procurement strategies of video analytics

This report describes a set of use cases for surveillance for CIP. The readiness level of respective technologies to be used in these use cases varies (per our selection) from TRL = 5 to 9 ([6]). Technologies within one use case and within one context, e.g. left luggage at an airport, can be combined to form a roadmap. An example of such a roadmap has been submitted for finding and tracking people at a large airport [6]. This helps owners of CI and LEAs to manage the risk involved in the respective innovation, development and procurement strategies. It is recommended to develop such roadmaps for coherent, relevant clusters of use cases that contribute to the missions and goals of CI and LEA's.

([6]) TRL levels may not be the best manner to describe the maturity of technology. See section 3.3.6 of [1].

References

[1] ERNCIP Thematic Group Video Analytics & Surveillance, "Surveillance and video analytics: Factors Influencing the Performance," JRC, Ispra, 2015.

[2] ESRIF, "ESRIF Final Report," 2009.

[3] B. M. Hämmerli and A. Renda, "Protecting critical infrastructure in the EU," Centre for European Policy Studies, Brussels, 2010.

[4] H. Bouma, J. Baan, F. Ter Haar, P. Eendebak, R. Den Hollander, G. Burghouts, R. Wijn, S. Van den Broek and J. Van Rest, "Video content analysis on body-worn cameras for retrospective investigation," *Proc. SPIE, vol. 9652,* 2015.

[5] R. Den Hollander, H. Bouma, J. Baan, P. Eendebak and J. Van Rest, "Automatic inference of geometric camera parameters and inter-camera topology in uncalibrated disjoint surveillance cameras," *Proc. SPIE, vol. 9652,* 2015.

[6] H. Bouma, J. Van Rest, K. Van Buul-Besseling, J. d. Jong and A. Havekes, "Integrated roadmap towards fast finding and tracking people at large airports (submitted)," *International Journal of Critical Infrastructure Protection,* 2015.

[7] J. Burgoon, R. Parrott, B. Le Poire, D. Kelley, J. Walther and D. Perry, "Maintaining and restoring privacy through communication in different types of relationships.," *Journal of Social and Personal Relationships 6.2,* pp. 131-158, 1989.

[8] S. Gutwirth, Privacy and the information age., Rowman & Littlefield, 2002.

[9] M. Langheinrich, "Privacy by design—principles of privacy-aware ubiquitous systems.," *Ubicomp 2001: Ubiquitous Computing. Springer Berlin Heidelberg,* 2001.

[10] J. Van Rest, M. Roelofs and A. Van Nunen, "Deviant behaviour - Socially accepted observation of behaviour for security - Summary," TNO, 2014.

[11] D. Lyon, Surveillance studies: An overview., Polity, 2007.

[12] INCOSE, "A Consensus of the INCOSE Fellows," [Online]. Available: http://www.incose.org/practice/fellowsconsensus.aspx. [Accessed 8 November 2014].

[13] J. Van Rest, "Monetary benefits of investments in risk management (in preparation)," TNO, 2016.

List of abbreviations and definitions

Term	Definition
Agent	An agent is an autonomous entity such as a human, an animal and an automated self-controlled system (a robot). In this report it means a person in the role of victim, witness, perpetrator or supervisor.
Asset (to be protected)	The object, person, situation or the process of which the continuity must be protected. This can be e.g. the life and wellbeing of a VIP, the democratic order or public order in general.
Behaviour	The reaction of a cognitive agent to a stimulus, expressed in elements of his environment.
Behaviour profiling	The extrapolation of information about an agent or a group of agents, based on its behaviour.
Cognition	The ability to solve problems.
Compartment	A compartment is a conceptual subsection of a physical space. In the context of object security, it is typically enforced with security measures.
Context	The context of a surveillance system consists of the factors that influence the system and necessarily includes the environment, including people in the environment. Typical examples of surveillance context are the local culture, the level of threat, and the weather conditions. Additionally, world knowledge as prior probability, and known correlations between events and actions, are also a part of a surveillance system's context.
Effectiveness	The degree to which a desired effect is obtained.
Environment	(1) The environment of a system is the system's surrounding that could interact with the system. The typical environment for a surveillance system is the area under surveillance including the people under surveillance and the location(s) of the system components (including storage, data transport, monitoring room, etc.). (2) The environment of a subject is those factors that have direct interaction with it.
Intent	The state of mind of a cognitive agent (a person) which is directed towards an object or situation in his environment.
Invasiveness/ intrusiveness/ obtrusiveness	The type of, and degree to which the integrity of a person is breached. This has both an objective and a subjective component. However, there is no common definition of the invasiveness of a surveillance capability. This frustrates answering questions such as 'how invasive is a particular surveillance capability?', or 'which is the least invasive manner of detecting a specific modus operandi?'. See section 2.4 in [1].
Object	(6) Object to be secured;

Term	Definition
	(7) Object to be observed; (8) The internal (in a surveillance system) representation of an object.
Privacy	The definition of privacy is not settled. Privacy is the ability to control and limit physical, social, psychological and informational access to the self or one's group [7]. Gutwirth writes that privacy is the safeguard of personal freedom — the safeguard of the individual's freedom to decide who she or he is, what she or he does, and who knows about it [8]. Langheinrich gives a short history of the concept of privacy by design [9], and illustrates as part of that history the origination of five specific categories of privacy that together appear to encapsulate all previous definitions: 1. Privacy of personal behaviour (media privacy); 2. Privacy of territory (territorial privacy); 3. Privacy of the person (bodily privacy); 4. Privacy of personal communications (interception privacy), and 5. Privacy of personal data (data or information privacy).
Profiling	The extrapolation of information about something, based on known qualities. It leads to the identification of patterns in data of the past which can develop into probabilistic knowledge about individuals, groups and situations in the present and in the future [10].
Risk	A risk is the combination of the chance on, and the impact of an undesirable situation. A risk is caused by the combination of an asset, a threat and a vulnerability.
Safety and security	Safety is the absence of risk. Security is the absence of risk intentionally caused by others.
Scene	The scene is what can be directly observed by the surveillance system.
Sensor	A device which converts one energy to another, usually an electric signal, e.g. microphone, CCTV camera, pressure sensor and also the human eye. There are several closely related concepts: • An **active sensor** sends a signal which is reflected by the subject, and/or which triggers a response from the subject, e.g. radar, sonar and lidar. • An **intelligent sensor** applies some form of knowledge to either improve the output signal or to interpret the signal to a higher level of abstraction, e.g. a face recognition system, video analytics and also a human. • A **probing sensor** is a sensor with a probing mechanism with the function of bringing a stimulus to the observed subject. The response to the stimulus is measured by the sensor. Human surveillance professionals do this, e.g. in security questioning. • A **virtual sensor** is a sensor in the digital domain, e.g. a sensor that detects a hacking attempt. This is formally not a sensor (i.e. not a transducer) but typically a software program.
Situation	Situation awareness is the perception of the environment with respect to time and/or space, and the comprehension of its meaning. It also

Term	Definition
awareness	includes the projection of the environment into the future or the past.
Stimulus	A stimulus is a detectable change (as perceived by the subject) in the environment (including the subject's own body). A stimulus can already be present in the environment (with the subject passing by), or it can be introduced directly or indirectly by the supervisor. Varying stimuli are used in security questioning and predictive behaviour profiling to trigger a tell-tale reaction.
Subject	(In this report) The person under surveillance.
Surveillance	The focused, systematic and routine attention to personal details for purpose of influence, management, protection or direction [11]. In the context of ERNCIP, surveillance is only covered when used for safety and security purposes.
System	A construct or collection of different elements that together produce results not obtainable by the elements alone [12].
Threat	(That which leads to) the potential occurrence of an undesirable situation. Security measures protect against threats.
Threat assessment	The threat assessment is the process which uses the situational awareness to estimate the concrete threat.
Video analytics	(Video content analysis) is processing of video to determine spatial and temporal aspects of and relations between objects in a scene. Threat assessment, i.e. generating alerts, is in this report considered to be a separate process.
Vulnerability	A weakness or hole in the security.

Abbreviation	Full text
ERNCIP	European Reference Network for Critical Infrastructure Protection
EU	European Union
i-LIDS	Image library for intelligent detection systems
MA	Morphological analysis
MAS	Morphological analysis on the surveillance domain
MAVA	Morphological analysis on the subdomain of video analytics
TACTICS	Tactical approach to counter terrorists in cities
TG (VAS)	Thematic group (video analytics and surveillance)
TRL	Technology readiness level

List of figures

List of tables

Appendix A ERNCIP and the Thematic Group on Video Analytics and Surveillance

The EU Joint Research Centre (JRC) is implementing a European Reference Network for Critical Infrastructure Protection project (ERNCIP). The mission of ERNCIP is to foster the emergence of innovative, qualified, efficient and competitive security solutions, through the networking of European experimental capabilities.

ERNCIP aims at providing a framework within which experimental facilities and laboratories will share knowledge and expertise in order to harmonise test protocols throughout Europe, leading to better protection of critical infrastructures against all types of threats and hazards.

ERNCIP is a direct response to the lack of harmonised EU-wide testing or certification for CIP products and services, which is a barrier to future development and market acceptance of security solutions.

What is equally important, ERNCIP Inventory was established under the umbrella of the European Programme for Critical Infrastructure Protection. The ERNCIP Inventory is a free-to-use search tool for open source information on European security experimental and testing facilities.

Work is carried out within eight thematic groups. One of them is the Thematic Group on Video Analytics and Surveillance. Each group has — for their thematic area — the following aims and objectives:

Identification of products/solutions

Given the generality with which the ERNCIP sponsors propose the thematic areas, it is left to the Thematic Group to identify and prioritise the security products/solutions that need to be dealt with, within the scope of its thematic area.

Common test protocols

The establishment of common test protocols will gradually create an EU common market for security products, strengthening the competitiveness of Europe internationally in that field. Detailed aims and objectives are:

1. Recommend common test methodologies and protocols for testing of security solutions at EU level. Any aspect of security product design or operation relevant to critical infrastructure protection issues could be considered;
2. Develop new test methodologies and/or harmonise existing ones as needed;
3. Promote standardisation of test methods via CEN, CENELEC and other standardisation bodies;
4. Investigate the possibility of drafting EU-wide recommendations for products/ solutions that may improve the protection/resilience of critical assets or mitigate the risk.

Metrology

5. Propose methodologies for measurement, quality assurance, calibration and metrology for qualified labs;
6. Define characteristics of reference materials and calibration objects required.

Certification

7. Investigate the possibility and the conditions of promoting a common certification or labelling procedure;
    - 7a. recommend an EU-wide evaluation/certification/labelling procedure for such products/solutions based on the agreed requirements or standards and assess impact;
    - 7b. recommend an EU-wide qualification scheme for labs which wish to evaluate such products/solutions.

Research and investments

8. Investigate new and innovative products/solutions and exchange good practice and recommend EU research topics;
9. Identify experimental capability and expertise lacks in Europe.

Appendix B EU research on video analytics

Based on a search in the EU Cordis database and other repositories a list of EU projects that somehow incorporate video analytics and security can be created. The list is ordered by start year of the project, and thus gives a historical perspective.

Name (URL)	Description	Start	End	Funding (Call)	Topic
PASSWORDS	Parallel and Real-Time Advanced Surveillance System with Operator Assistance for Revealing Dangerous Situations	1994	1996	FP3-ESPRIT 3	
CROMATICA	Crowd management with telematic imaging and communication assistance	1996	1998	FP4-TELEMATICS 2C	A.2
ADVISOR	Annotated Digital Video for Surveillance and Optimised Retrieval	2000	2002	FP5-IST	1.1.2.-1.6.1
AMI	Augmented Multi-party Interaction	2003	2009	FP6-IST	IST-2002-2.3.1.6
CANDELA	Content Analysis and Networked DELivery Architectures towards Intelligent Video	2003	2005	ITEA	Call 5
ISCAPS	Integrated surveillance of crowded areas for public security	2005	2007	PASR 2004	
MUSCLE	Research project exploring the full potential of statistical learning and cross-modal interaction for the (semi-) automatic generation of semantic meta-data for multi-media.	2005	2008	FP6-IST	IST-2002-2.3.1.7
AMIDA	Augmented Multi-party Interaction with Distance Access	2006	2009	FP6-IST	IST-2005-2.5.7
CANTATA	Content Aware Networked systems Towards Advanced and Tailored Assistance	2006	2009	ITEA	Call 8
IDETECT 4ALL	Novel intruder detection & authentication optical sensing technology	2008	2011	FP7-SECURITY	SEC-2007-2.3-04
PROMETHEUS	Prediction and interpretation of human behaviour based on probabilistic structures and heterogeneous sensors	2008	2010	FP7-ICT	ICT-2007.2.1
SAMURAI	Suspicious and abnormal behaviour monitoring using a network of cameras & sensors for situation awareness enhancement	2008	2011	FP7-SECURITY	SEC-2007-2.3-04,SEC-2007-2.3-03
ADABTS	Address the European need for increased security against deliberate threat (terror, crime, riots) by advancing the capability for automatic detection of abnormal, potentially threatening behaviour of crowds or individuals in crowds while respecting privacy and civil liberties.	2009	2013	FP7-SECURITY	SEC-2007-2.3-03

IMSK	The Integrated Mobile Security Kit (IMSK) project will combine technologies for area surveillance; checkpoint control; CBRNE detection and support for VIP protection into a mobile system for rapid deployment at venues and sites (hotels, sport/festival arenas, etc) which temporarily need enhanced security.	2009	2013	FP7-SECURITY	SEC-2007-1.2-02
INDECT	Intelligent information system supporting observation, searching and detection for security of citizens in urban environment	2009	2014	FP7-SECURITY	SEC-2007-1.2-01
PRONTO	PRONTO emphasises the role of event recognition in intelligent resource management.	2009	2012	FP7-ICT	ICT-2007.4.4
SUBITO	Surveillance of Unattended Baggage and the Identification and Tracking of the Owner	2009	2011	FP7-SECURITY	SEC-2007-2.3-01
ViCoMo	Visual Context Modelling	2009	2012	ITEA 2	Call 3
OPARUS	The goal of this project is to elaborate an open architecture for the operation of unmanned air-to-ground wide area land and sea border surveillance platforms in Europe.	2010	2012	FP7-SECURITY	SEC-2009-3.4-01
PROTECTRAIL	The PROTECTRAIL objective is to provide a viable integrated set of railway security solution.	2010	2014	FP7-SECURITY	SEC-2009-2.2-01
SPY	SPY project will create a new automated, intelligent surveillance and rescue framework adapted for mobile environments.	2010	2013	ITEA 2	Call 4
TASS	TASS is a multi-segment, multi-level intelligence and surveillance system, aimed at creating an entire airport security monitoring solution providing real-time accurate situational awareness to airport authorities.	2010	2014	FP7-SECURITY	SEC-2009-2.2-02
VANAHEIM	Integration of innovative audio/video analysis tools within a CCTV surveillance platforms typically in use in urban transport environments (metro and railway stations).	2010	2013	FP7-ICT	ICT-2009.2.1
VIRTUOSO	Virtuoso aims to provide the security authorities with an advanced integrated toolkit, developed around an "open" architecture to exploit open source information for decision support .	2010	2013	FP7-SECURITY	SEC-2009-3.2-03
ADDPRIV	Platform for automatic semantic content discrimination within video surveillance data.	2011	2014	FP7-SECURITY	SEC-2010.6.5-2

ARENA	Architecture for the Recognition of thrEats to mobile assets using Networks of multiple Affordable sensors	2011	2014	FP7-SECURITY	SEC-2010.2.3-3
BASYLIS	The BASYLIS project aims to address issues by developing a low-cost smart sensing platform that can automatically and effectively detect a range of security threats in complex environments.	2011	2013	FP7-SECURITY	SEC-2010-2.3-3
CUBRIK	Human-enhanced time-aware multimedia search	2011	2014	FP7-ICT	ICT-2011.1.5
DESURBS	DESURBS focuses on the DESigning of safer URBan Spaces and addresses the issues of planning, (re)design, and (re)engineering of urban areas to make them less vulnerable and more resilient to security threats	2011	2014	FP7-SECURITY	SEC-2010.2.3-1
MOSAIC	Multi-modal data intelligence capture and analytics including video and text collaterals.	2011	2014	FP7-SECURITY	SEC-2010.2.3-3
SAFECITY	SafeCity deals with smart Public safety and security in cities.	2011	2013	FP7-ICT	FI.ICT-2011.1.8
SAVASA	Standards Based Approach to Video Archive Search and Analysis	2011	2014	FP7-SECURITY	SEC-2011.5.3-4
SECUR-ED	The SECUR-ED Project is a demonstration project with an objective to provide a set of tools to improve urban transport security.	2011	2014	FP7-SECURITY	SEC-2010.2.1-1
SV3D	Surveillance platform based on multi-source video analytics, localized data and cognitive interfaces.	2011	2013	FP7-SME	SME-2011-1
ADVISE	Focus on design and development of a unification framework for surveillance-footage archive systems.	2012	2015	FP7-SECURITY	SEC-2011.5.3-4
AVERT	The Autonomous Vehicle Emergency Recovery Tool (AVERT) provides a capability rapidly to deploy, extract and remove both blocking and suspect vehicles from vulnerable positions and confined spaces	2012	2015	FP7-SECURITY	SEC-2011.1.3-1
IMPART	Intelligent Management Platform for Advanced Real-Time media processes.	2012	2015	FP7-ICT	ICT-2011.4.4
PROACTIVE	PRedictive reasOning and multi-source fusion empowering AntiCipation of attacks and Terrorist actions In Urban EnVironmEnts	2012	2015	FP7-SECURITY	SEC-2011.1.2-1

TACTICS	TACTICS seamlessly integrates new research results in the area of behaviour analysis, characteristics of the possible urban-based targets and situational awareness into a decision making framework comprising of a coherent set of tools and related processes, supporting security forces in responding more efficiently and effective to a given threat in order to actually prevent the attack or to limit its consequences.	2012	2015	FP7-SECURITY	SEC-2011.1.2-1
COPCAMS	The COPCAMS (COgnitive & Perceptive CAMeraS) project aims at a new, many-core programmable accelerator platform for smart cameras and gateways, able to extract relevant information and autonomously react to the environment, operating on a large, distributed scale	2013	2016	ARTEMIS	Call 2012
SAWSOC	SAWSOC aims at bringing a significant advancement in the convergence of physical and logical security, meaning effective cooperation (i.e. a coordinated and results-oriented effort to work together) among previously disjointed functions.	2013	2016	FP7-SECURITY	SEC-2012.2.5-1
APPS	Advance the surveillance technology by enabling the development of plug & play solutions, enhancing intelligent decision making capabilities, and developing robust communication mechanisms.	2014	2018	ITEA 2	Call 8
C2-SENSE	Interoperability Profiles for Command/Control Systems and Sensor Systems in Emergency Management	2014	2017	FP7-SECURITY	SEC-2013.5.3-1
CRIM-TRACK	Sensor system for detection of criminal chemical substances	2014	2016	FP7-SECURITY	SEC-2012.1.6-1
EWISA	Early warning for increased situational awareness	2014	2018	FP7-SECURITY	SEC-2013.3.2-1
INSIST	The goal of the INSIST project is to increase comfort and safety of public spaces by linking video surveillance and light management technology into a smart connected platform and ecosystem.	2014	2018	ITEA 2	Call 8
ISIS	Integrated intelligent sensor system for improved security of water supply	2014	2016	FP7-SECURITY	SEC-2012.1.5-2
POP-ALERT	Population Alerting: Linking Emergencies, Resilience and Training	2014	2016	FP7-SECURITY	SEC-2013.4.1-5

P-REACT	This project will design and develop a low cost surveillance platform that will detect Petty Crime incidents.	2014	2016	FP7-SECURITY	SEC-2013.7.2-1
SMARTPREVENT	Smart Video-Surveillance System to Detect and Prevent Local Crimes in Urban Areas	2014	2016	FP7-SECURITY	SEC-2013.7.2.1
SUPER	Social sensors for secUrity Assessments and Proactive EmeRgencies management	2014	2017	FP7-SECURITY	SEC-2013.6.1-1
SURVEIRON	Advanced surveillance system for the protection of urban soft targets and urban critical infrastructures	2014	2015	H2020-DRS-2014	DRS-17-2014-1
VALCRI	Visual Analytics for Sense-making in CRiminal Intelligence analysis	2014	2017	FP7-SECURITY	SEC-2013-1.6-4
VASCO	The concentration of government buildings within urban environments has become a source of serious security vulnerability.	2014	2017	FP7-SECURITY	SEC-2013.2.1-1
ZONESEC	ZONeSEC delivers an innovative and cost-effective approach to the protection of critical widezone areas across the European Union.	2014	2018	FP7-SECURITY	SEC-2013-1.6-3
ICT4COP	Community-based policing and post-conflict police reform	2015	2020	H2020-FCT-2014	FCT-14-2014
Invest	INtelligent Video analytics to analyse complex scenes and Enhance Security of critical infrastructure and urban soft Targets	2015	2015	H2020-DRS-2014	DRS-17-2014-1
NOSY	New Operational Sensing System	2015	2018	H2020-FCT-2014	FCT-05-2014
TRILLION	Trusted Citizens - LEA coLlaboratIon over sOcial Networks	2015	2018	H2020-FCT-2014	FCT-14-2014

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

Free publications:

- one copy:
  via EU Bookshop (http://bookshop.europa.eu);
- more than one copy or posters/maps:
  from the European Union's representations (http://ec.europa.eu/represent_en.htm);
  from the delegations in non-EU countries (http://eeas.europa.eu/delegations/index_en.htm);
  by contacting the Europe Direct service (http://europa.eu/europedirect/index_en.htm) or calling 00 800 6 7 8 9 10 11 (freephone number from anywhere in the EU) (*).

(*) The information given is free, as are most calls (though some operators, phone boxes or hotels may charge you).

Priced publications:

- via EU Bookshop (http://bookshop.europa.eu).

LB-NA-27851-EN-N

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

Publications Office

doi:10.2788/236268

ISBN 978-92-79-57770-3