European Commission

JRC TECHNICAL REPORTS

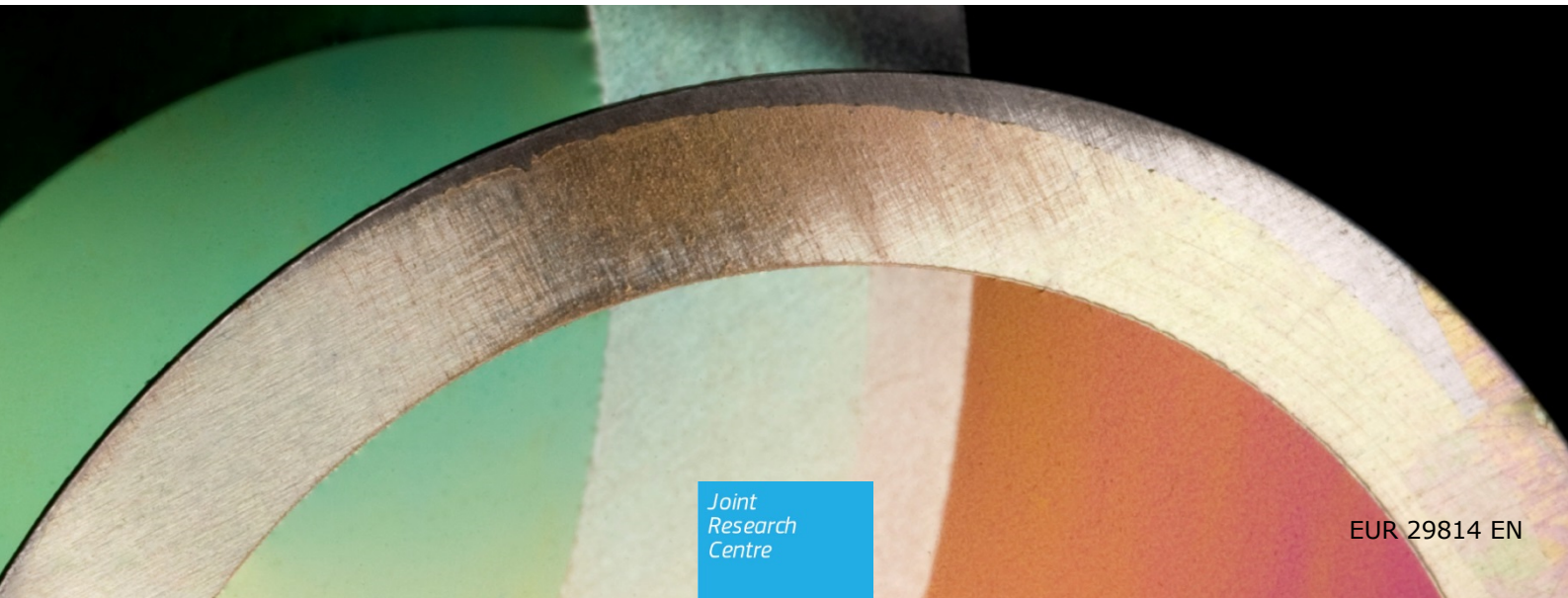
Technical and operational issues associated with early warning zones for critical infrastructure

ERNCIP Thematic Group on Early Warning Zones

Authors
Jeroen van Rest, Raul Sanchez-Reillo, Geoff Whittaker, James Ferryman, Stefano Leucci, Alessandro Ortalda, Peter Waggett

Editor
Georgios Marios Karagiannis

2019



Joint Research Centre

EUR 29814 EN

Contact information
Name: Georgios GIANNOPOULOS
Address: Via E. Fermi 2749, I-21027 Ispra, Italy
Email: georgios.giannopoulos@ec.europa.eu
Tel.: (+39) 0332-78-6211

JRC Science Hub
https://ec.europa.eu/jrc

JRC117253

EUR 29814 EN

PDF ISBN 978-92-76-08963-6 ISSN 1831-9424 doi:10.2760/806546

Luxembourg: Publications Office of the European Union, 2019

How to cite this report: van Rest, J., Sanchez-Reillo, R., Whittaker, G., Ferryman, J., Leucci, S., Ortalda, A., Waggett, P. and Karagiannis, G. M., *Technical and operational issues associated with early warning zones for critical infrastructure*, EUR 29814 EN, ISBN 978-92-76-08963-6, doi:10.2760/806546, Publications Office of the European Union, Luxembourg, 2019.

Contents

Acknowledgements

The authors acknowledge the information and wisdom provided by all of the participants of the meetings and other collaborators held during this phase of the Early Warning Zones (EWZ) Project. Their input has been incorporated into the following chapters. Each task leader has delivered their individual chapter and this final report contains these chapters as modified by the group discussions.

The authors also gratefully acknowledge the help and support of the JRC team in providing guidance, help and support in completing this project. We would especially like to thank the JRC project managers Alessandro Lazardi and Georgios Giannopoulos without whom the group would not have been able to complete its work.

Authors

Jeroen van Rest

Raul Sanchez-Reillo

Geoff Whittaker

James Ferryman

Stefano Leucci

Alessandro Ortalda

Peter Waggett

Editor

Georgios Marios Karagiannis

Abstract

This document captures the work performed during the current phase of the Early Warning Zones (EWZ) Project. The aim of the Early Warning Zones Project has been to explore the technical and operational issues associated with providing an early warning zone around critical infrastructures (CIs). Seven key areas of technical and operational issues have been explored and documented in this report. These are:

- EWZ use cases
- Biometric recognition for EWZ
- Standardisation challenges for EWZ
- Video and cognitive surveillance challenges for EWZ
- EWZ policy options and design requirements
- Data protection impact assessment and prototype development
- Guidance for implementing EWZ

It is noted that this subject is still at an early stage of investigation and the intention has been to make sure that all of the activity performed by the group has been captured in this report under the separate tasks. It is also apparent that there would be many fruitful areas of future research activity that could follow from a deeper and more integrated follow-on stage for this project.

1 Introduction

Recent security incidents directed at 'soft targets' ([1]), including those that have caused casualties and damage at (semi-)public spaces such as infrastructure access control points (Zaventem and Istanbul airports), have highlighted the need to receive early warnings of potential threats in certain zones in and around critical infrastructures. These zones can be located both outside and inside of security perimeters.

Situational awareness is a key concept in emergency and crisis management, where it describes the human perception of a complex and rapidly evolving situation that enables emergency managers to draw conclusions, build understanding and make decisions (Johnson et al., 2011). The lack of situational awareness has been identified as one of the major challenges of incident planning (Karagiannis and Synolakis, 2017).

Early indicators of threats can be found in the appearance of known high-threat persons, of potentially dangerous objects such as abandoned luggage, cars related to high-threat persons, or in the suspicious behaviour of persons, and any combinations of these.

Traditional security doctrine dictates that an additional perimeter with access control must be added around zones which may be vulnerable to attacks. However, in the case of terrorist threats this will simply result in the creation of an additional potential (soft) target: the queues of people waiting for that additional access control.

Due to such technological advancements in recognition technologies, there may now be an alternative approach: early detection of threats not at perimeters, but in the flow of people within 'early warning zones' (EWZ). Detecting threats in flow would not create new soft targets. Specifically, the automatic detection and recognition of persons of interest in the vicinity could provide alerts and allow for the timely deployment of measures to counter or reduce the impact of these threats. This is called biometric recognition surveillance in a person-of-interest-list scenario.

A number of organisations within Europe have deployed capabilities that provide early warning zones using recognition capabilities around biometric matching of faces (e.g. Davies et al., 2016). These organisations have reported anecdotal evidence of the benefits that can accrue from such deployments.

There is however, very little evidence available in the open press as to the performance of such systems. Possibly the most relevant information available comes from the tests run by NIST in 2018. Their Ongoing Face Recognition Vendor Test stated that:

> 'The major result of the evaluation is that massive gains in accuracy have been achieved in the last five years (2013-2018) and these far exceed improvements made in the prior period (2010-2013).' (Grother, 2018)

However, the performance of biometric (recognition) systems depends significantly on the quality of the images and specifics of the use case:

> '…, for at least 10 % of images — those with significant ageing or sub-standard quality — identification often succeeds but recognition confidence is diminished such that matches become indistinguishable from false positives, and human adjudication becomes necessary.' (Grother, 2018)

So, the question is open as to whether these kind of biometric person-of-interest list surveillance systems are currently already usable, and whether it should be expected that they ever will be. If they are, or will be, there will need to be a balance struck between the warning time, the flow-rate of persons, efficiency and ethical compliancy that any such capability will generate. This report aims to provide more clarity in this matter.

([1]) A soft target is a target that is not adequately protected against typical threats directed towards it. Among security specialists and in security policies, this term is typically used to describe a target where (many) unprotected people gather or move through, and that might (for that reason) be for terrorists an attractive target.

Other related capabilities are the detection of potentially dangerous objects such as lost luggage, drones or suspicious behaviour of people, including people in cars. This report focuses mainly on the detection of known attackers on foot, while giving a general overview of other relevant developments.

The themes for the ERNCIP thematic groups are proposed by the ERNCIP sponsors. The original proposed topic was 'Extended Virtual Fencing'. This name was changed into Early Warning Zones (EWZ) to reflect the following notions. First, any line-based solution would create practical challenges related to the integration with intervention capabilities. Second, a (biometric recognition) surveillance system does not have any stopping capability, only a revelatory capability. Hence, the word 'fence' was replaced with 'warning zone'. Third, the goal of this warning zone is not to extend the space where surveillance is carried out (this is merely a means to an end), but to increase the warning time before an attack. Hence, the word 'extended' is replaced with 'early'.

1.1 Problem statement

Modern video surveillance systems (VSS) can provide sets of images that can be analysed in real time and used for direct biometric recognition via automated face recognition (AFR) or through behavioural traits. These can enable the recognition and identification of individuals that potentially pose a threat at a relatively long range from the sensor, e.g. ahead of peripheries. Obtaining high-quality sensor data in a sustainable manner for people in flow is a major technological and organisational challenge, with many pitfalls.

Biometric technologies can be coupled with, and extended through, cognitive and analytical computing techniques ('narrow artificial intelligence') to deliver high confidence alerts which no single measure alone would provide. Among other functionalities, cognitive computing approaches would allow systems to learn and adapt to new behaviours to provide rapid updates to evolving threats that would update across networked systems automatically. However, the increasing use of such networked and cognitive systems will also present ethical, organisational and technical challenges.

Obviously, the use of this kind of technology raises questions with regard to privacy in relation to security in the context of dynamic threat levels. This requires the assessment of ongoing research into the societal impact of these technologies, such as privacy issues associated with the use and storage of biometric/video data and privacy enhancing technologies.

In addition, while the general idea of EWZ exists in popular culture through science fiction and action movies, the reality is that EWZ is not a clearly defined technology. As a consequence, expectations of the potential value of EWZ may be unrealistic ('CSI effect').

1.2 Intended audience, purpose and scope

The intended audience for this report includes EU-level policy authorities (especially the Directorate-General for Migration and Home Affairs), industry, end-users and other stakeholders that are interested in the deployment of video analytic and surveillance systems and methods. It will also be of interest to academics researching biometrics and surveillance and to standardisation bodies.

The purpose of this report is to inform this audience on the current and near-future (im)possibilities of using biometrics recognition and other detection technologies in 'early warning zones'.

The ERNCIP Thematic Group on EWZ (TG) focuses on the protection of critical infrastructure (CI) against threats that have the capacity to lead to cascading effects to society. Therefore, at the first meeting of the EWZ Technical Group a decision was made to focus on high-end threats in such early warning zones. This decision was guided by several terrorist attacks which had occurred in the months prior to the meeting. However, such threats can by their nature be very varied and complex, and go beyond

terrorist attacks, which were the immediate cause. They may also be related to organised crime, crowd control during riots, or espionage.

Low-risk threats such as shoplifting, pickpocketing and fare evading in public transport are explicitly out of scope because they do not affect the CI to a significant degree. The risk of scope and mission creep, i.e. the risk that EWZ are also used for disproportional low-risk situations, is acknowledged, but is not discussed in this report.

The TG focuses in depth on the capability to identify known threatening persons while they are moving freely, but in a broader sense, an overview will also be given of other relevant capabilities for EWZ.

1.3 Results

The ERNCIP Thematic Group on EWZ has produced this final report that outlines the issues and provides best practice guidance on measures needed to move from isolated short-range systems used for biometric recognition ([2]) to complete solutions that integrate the biometric elements with other information sources within a cognitive surveillance architecture. As part of that work, the group will also investigate realistic concepts of operations (ConOps) needed to provide extended virtual boundaries.

Chapter 2 describes the method we used for each chapter to obtain the respective results.

Chapter 3 describes the ConOps to be used to guiding the thinking of the TG.

Chapter 4 describes the available biometric recognition modes and their capabilities.

Chapter 5 describes the EWZ standardisation challenges.

Chapter 6 describes the video and cognitive surveillance landscape for EWZ.

Chapter 7 describes the issues around data privacy and protection to be considered by an implementer of EWZ systems.

Chapter 8 provides an overview of a data protection impact assessment prototype.

Chapter 9 describes the overall issues to be considered by implementers of EWZ systems.

Last, Chapter 10 presents the conclusions of the group and recommendations for future areas of study.

([2]) The term recognition is used to recognise someone from a set of people, e.g. from a watchlist. In that regard, identification is a special case of recognition where the set includes all people. In addition, identification is used to determine someone's identity, which is not the case in recognition. Depending on the use case, the privacy implications of using one versus the other are different. For EWZ, recognition is often sufficient.

2 Method

In this chapter, the method is described for each of the main activities of this TG. No operational tests involving real persons were done for this report. All information that is presented in this report is based on publications written in other studies.

2.1 Organising the thematic group

The themes for the ERNCIP thematic groups are proposed by the ERNCIP sponsors. A proposal for a group on the use of biometrics to generate early warnings of known threatening persons led to the creation of a new thematic group, with representatives of CI operators, experts on biometrics, video analytics and ethical, legal and societal aspects (ELSA). They are facilitated by experts from the ERNCIP office. This group is largely autonomous in the way they approach the challenge of EWZ. They identified amongst themselves tasks and task leaders. When additional expertise was needed then this was organised from the peer network of the initial group.

This approach stimulated independent and out-of-the-box thinking. However, there was no clear problem owner identified, which could have led to scope or mission creep. The group mitigated this risk by focusing on clear and agreed-upon use cases.

2.2 Questionnaire on state of the art

While the generic challenge was formulated as a result of the continuous interaction between ERNCIP office and DG Migration and Home Affairs, this did not provide sufficiently specific information regarding the state of the art of EWZ. With the help of the national contact points, a questionnaire was distributed regarding the needs and perceived barriers regarding EWZ with policymakers and end-users. The results of this questionnaire informed the TG and are available through the ERNCIP Project Office.

2.3 Identification and specification of use cases

The specification of use cases is done by the members of the TG. The use cases are based on contemporary ideas that the experts encountered in their professional work. The sources of these ideas are withheld in order to adhere to information security requirements. This also helped to focus the information and discussion on the proper abstract level, without getting lost in local details.

The method for obtaining the concept of operation and use cases consists of the following steps. First, a draft for the structure of a use case was described. This was done by starting with the dimensions of the morphological analysis for video surveillance systems (MAVAS) introduced by the ERNCIP TG on Video Analysis and Surveillance (ERNCIP, 2015). This helped to avoid biases (e.g. 'the recognition of known threatening persons will only work with face recognition') and served as a reminder to think of all relevant aspects (e.g. 'is the potential for active lighting of the scene also part of the use case description?'). Second, this draft was distributed among the members of the TG, with an invitation for comments on this draft. These comments were processed and followed up with a call for use cases. Third, the use cases were processed to make them of comparable depth and scope. Fourth, the results were presented to and discussed within the TG and feedback was obtained to improve the use cases on societal impact and functionality. Finally, the use cases and the information that was elicited with the help of the use cases were synthesised into a single comprehensive text for Chapter 3 of this report.

3 EWZ use cases

The purpose of this chapter is to provide the reader with a clear description of the issues associated with EWZ by describing potential use cases. The description contains a range of functional and non-functional requirements for EWZ, validated for selected use cases along with outlines of concepts of operation, including:

- Statement of the objectives in relation to a context and environment;
- Strategies, tactics, policies, and constraints affecting the system;
- Organisations, activities, and interactions among participants and stakeholders;
- Human–machine interaction, including task allocation to human and machine;
- Modes of deployment;
- Outline of the cost–benefit analysis issues.

There are several reasons to start the approach by specifying use cases. First, professional teams investigating solutions to the problem of attacks on soft targets near critical infrastructures will be comprised of professionals from different backgrounds and nationalities, and they may have different functional expectations of EWZ. In addition, it can be difficult to imagine how state-of-the-art or future technologies can solve existing or new problems. This is also the case for the members of this TG. Use cases help create common understanding and focus in such teams.

Second, this TG has the ambition to enhance the functionality and/or accuracy of EWZ through the coupling and extension of biometric technologies through cognitive and analytical computing techniques with other types of information. This requires a clear description of EWZ use cases to which these enhancements can be added.

Third, the work of this TG will generate questions regarding the societal impact (e.g. privacy and data protection). The TG intends to facilitate this discussion, which will also benefit from a clear description of EWZ in terms of use cases.

3.1 End-user perception of watchlist surveillance

A questionnaire was distributed to representatives of all EU Member States. Some representatives elected not to forward the questionnaire. Others forwarded it to multiple national agencies. In the end, responses were obtained from eight agencies in six EU Member States.

The questionnaire can be found in Annex B. Many questions were not answered by the respondents. This may have been due to overly complex questions, the classification of relevant information or other unknown factors. Because of the low response rate and the incompleteness of the responses, the representativeness of the answers may be low. An obvious bias that was not addressed in this study was that some Member states with EWZ surveillance watchlists may have withheld some relevant information for security reasons. Still, the answers guided the thematic group in focusing its attention and capacity.

One Member State indicated that they have an early warning zone, based on fingerprints. No other information was provided, so it was not possible to verify whether their definition of an early warning zone aligned with that of this report.

Five agencies indicated that EWZ are — for them — desirable. The other three agencies did not answer this question. This answer motivated the group to pursue this topic further. According to the respondents, the main inhibitors are in the legal domain, followed by cultural barriers, and then uncertainty about cost-effectiveness. The TG, and this report, focuses therefore in later chapters on the legal domain, and in this chapter on the cost-effectiveness.

3.2 Recognition of known threatening persons in early warning zones: watchlist surveillance

Early warning zones help generate alerts on known persons of interest in an area where persons are under surveillance, but where they are not yet claiming an identity. This implies that there is no incentive for persons to provide a biometric identifier (e.g. a face, fingerprint, etc.). The biometric identifier must thus be obtained from non-cooperative persons.

The attitude of persons under surveillance towards the biometric sensors has a great impact on operational performance. When (friendly) persons actively present their biometric identifier, the quality of the biometric image will improve.

But, when (hostile) persons actively attempt to hide their identifier, it may be impossible to obtain it from them, as this statement from NIST describes for faces:

> 'Deliberately uncooperative subjects can expend arbitrary effort to evade detection and recognition by avoiding the camera, either completely or by keeping their head down, or by altering the appearance of their face, for example by wearing (sun)glasses, hats, cosmetics, and masks. The likelihood that such techniques will be used — they have been ubiquitous in bank robberies since the advent of the CCTV camera — may well contraindicate the use of face recognition. Such techniques can be 100 % effective. Effective evasion is however predicated on knowledge on when cameras are present and face recognition may be in use. Without that knowledge, successful evasion would require continuous persistent effort.' (Grother, 2017)

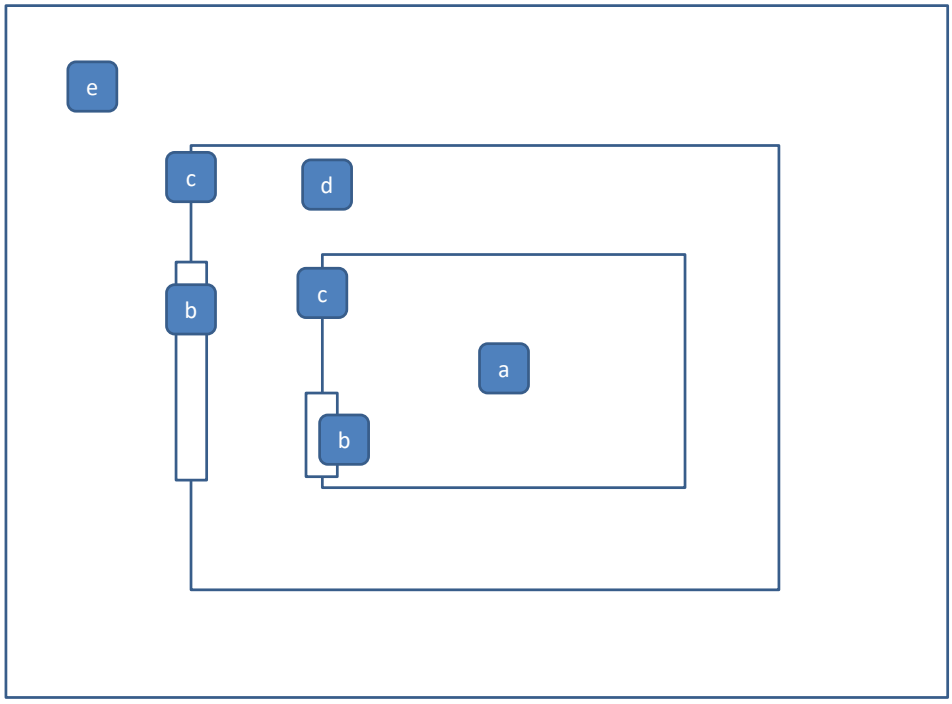
Even when persons are indifferent, there may be a very wide variety over time in the capture rate and in the quality of the captured biometric identifiers. A selection of other relevant factors includes the weather (e.g. hiding biometric identifiers under clothing), (dis)abilities (e.g. gait recognition does not work for people in wheelchairs) and the presence of factors that require attention from persons (which compete for this attention with the biometrics system).

A growing number of companies claim that their technologies can help build the capability to deliver recognition and identification of individuals (watchlist biometric surveillance) without the subjects' cooperation and without interfering with the flow of people. This capability requires more than just technology; it requires a holistic approach in terms of ethics and legal frameworks, functionality, work processes, staff and technology. In order to focus the work of the TG, we present in this section several examples what this capability might entail in the form of **use cases**.

3.2.1 Early warning zone

This report assumes a typical compartmentalisation of critical infrastructure and its environment in a simple ring model.

Figure 1. The ring model (security-in-depth) applied to a CI: a. vital area (ring 1); b. access door/gate; c. perimeter; d. secured area (ring 2); e. observation area (ring 3)



Source: JRC.

The early warning zone can be either in the secured area/ring 2d., or in the observation area/ring 3e. Ring a. would not be 'early' any more. Perimeters and access doors/gates can be included, but, if they become 'choke points', then they may become new (soft) targets.

3.2.2 Watchlist surveillance: generic capability description

A traditional biometrics-based access control system has only to compare a person with a biometric image of himself: this is a 1 to 1 comparison. If an EWZ system is to be used to stop 'n' known threatening persons ([3]), then this becomes a 1 to 'n' comparison, which has 'n' times as many opportunities to falsely recognise someone. So, an EWZ system requires a much better accuracy than a traditional access control system if a similar degree of false alarms is to be obtained.

Typically, increasing the accuracy of a biometrics system would be solved by requesting more cooperation from the subject and decreasing the distance between the sensor and the subject. However, in the case of EWZ, these options are not viable. In fact, it is imperative to decrease the level of required cooperation in order to avoid the creation of waiting lines which become de facto additional soft targets. And the distance between the sensor and the subject must be increased in order to help protect the EWZ against threats directed towards it.

If deterrence is also a function of an EWZ, then distance and a low degree of interaction become even more important as they help conceal the workings of the EWZ, which is a known factor in creating deterrence (besides actual effectiveness).

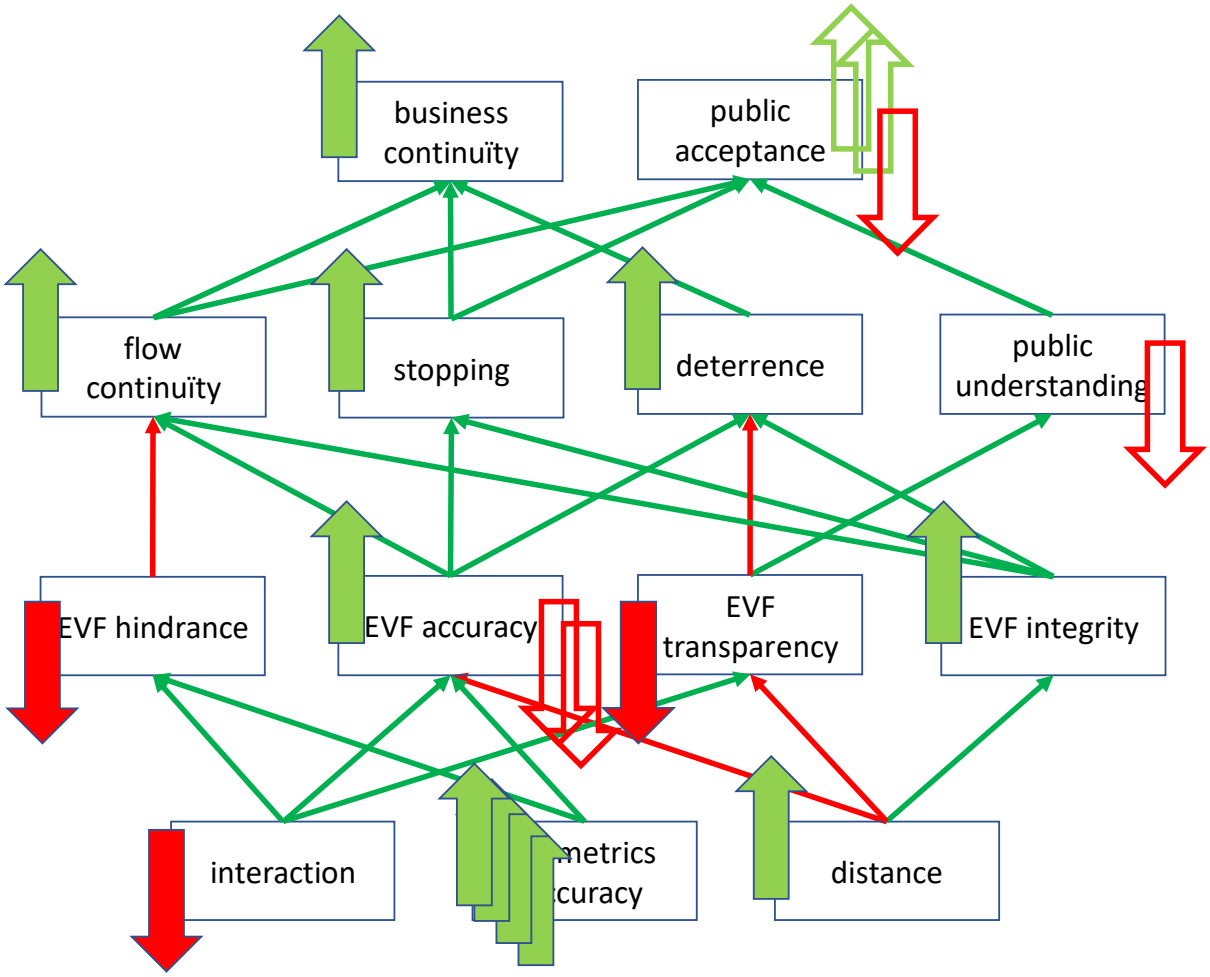
So, EWZ requires the use of biometric traits that can be obtained from a distance, such as those based on sound (e.g. voice, footsteps), light (e.g. face, iris, walking pattern or gait) and vibrations (perhaps heartbeat and footsteps), and that can be obtained with a

([3]) Other types of use cases can be imagined regarding missing persons, persons with a restraining order or fugitives. Depending on the use case and the actual operational parameters, the 1 to n comparison can scale down to a 1 to 1 comparison.

low degree of cooperation, in order not to disturb the flow of people. Section Chapter 4 goes into more detail about which biometrics modalities are relevant for EWZ.

The consequence of this combination of requirements is that the increase in the accuracy of the biometrics subsystem must not only compensate from the switch from a 1 to 1 comparison to a 1 to n comparison, but also for an increase in distance and for a decrease in the degree of cooperation. This is illustrated in **Figure 2**.

Figure 2. Goal tree of a generic biometrics access control system



Note: The goal tree of a generic biometrics access control system, annotated with the required changes to make it an EWZ system (including deterrence). The lines between the boxes represent effects (green for positive, red for negative). The big arrows on the left-hand side of each box represent the desired change (to be read top-down). The big hollow arrows on the right-hand side represent side effects — which sometimes must be compensated for.

Source: JRC.

Also illustrated in this figure (in the top right) is the effect that the way an EWZ works will have on the acceptance of an EWZ by the general public. In short, if it works (stopping power and deterrence go up) then for the support of the public, that could compensate for the reduction in transparency that an EWZ has over a regular biometrics-based access control system.

3.2.3 Watchlist surveillance: contribution to EWZ

The basic premise of watchlist biometric surveillance is that it provides warnings in a timely manner, i.e. before an attack takes place. The step from the detection of someone on a watchlist to a warning can be achieved in several ways. In order to distinguish these

ways Van Rest (2014, 2015) has described five **surveillance patterns**, inspired by architectural design patterns. In the next table, each of the five patterns are instantiated for early warning zones. We distinguish between high-risk and medium-risk persons. The distinction is that the presence of a high-risk person always warrants an intervention.

Table 1. Surveillance patterns for early warning zones

Name	**Generic function**	**Function of surveillance pattern for EWZ**
Threshold alarm	Alarm when the value of an attribute of an object crosses a threshold.	Alarm when the similarity of a biometric image — irrespective of the location of this person in the EWZ — resembles the biometric image of a person on the list above a certain threshold; i.e. when a high-risk person enters the EWZ. This is the basic function of a watchlist biometric surveillance system for an early warning zone.
Profiling of a person	Alarm when a combination of values of multiple attributes of an object indicates a threat posed by a person.	Alarm when the pattern of appearance of a person indicates suspicious behaviour. Such as visiting the observation area of a CI multiple times in a limited period, but never engaging in the use of the CI. This could be indicative of scouting the object's defensive measures with the intention of attacking at a later moment.
Concentric circles of protection	Alarm when a threat attempts to breach a circle of protection.	Variant 1: Alarm when a known high-threat person attempts to pass access control to a secured zone. **In the context of a high threat, this pattern is considered a bad practice**: attackers may attack the queue before the access control. Variant 2: Everyone is captured and enrolled at the entrance of a secured zone. When, within that secured zone, someone is involved in an incident, they may be linked through tracking or through biometrics with their entrance, at which point they can be identified based on the other credentials they provided.
Bag of observations /profiling of a situation	Alarm when a combination of events indicates a threat posed by a combination of factors — not just one person — but without there being a clear narrative or causal link between those events.	Alarm when multiple events occur, one of them being the presence of a medium-threat person. E.g. the presence of multiple medium-threat persons, or a combination of a medium-threat person with deviant behaviour of other persons, suspicious objects being present, etc.
Scenario view	Alarm when a predefined modus operandi of multiple linked events enfolds.	Example: alarm when persons attract the attention of a significant amount of security resources in one area — creating a diversion, where a medium-risk person enters the EWZ in another area.

Source: Van Rest, 2014; 2015.

These surveillance patterns show the range of possibilities that watchlist surveillance can contribute to EWZ. While the 'threshold alarm' is the plainest variant of watchlist surveillance, others may be more cost-effective, depending on the specific context and purpose of the EWZ.

3.2.4 Watchlist surveillance: alarm resolution

Alarm resolution is the management of the alarm so that it becomes (more) usable. This typically includes additional checks to determine if an alarm was false or just, and to prepare the situation for follow-up action. In the context of watchlist surveillance for the purpose of obtaining early warnings of high-threat persons, this part is non-obvious, and critical for the overall security of the CI and everyone involved. For example, consider the fact also that high-threat persons may have completely innocuous and legitimate reasons to be near certain types of CI.

Assuming that the recognition itself is not disclosed to the suspect, the security staff have the advantages of superior information and of initiative. These advantages can be used to covertly obtain more information regarding the actual threat. For example, other surveillance and detection resources can be deployed on the subject in order to verify the identity, and to assess other threat indicators, such as hostile intent, or the possession of weapons or explosives.

It cannot be assumed that the resulting information position gives 100 % clarity regarding the justification of the alarm: despite all available information pointing in a different direction, the alarm can still be false.

Irrespective of whether the alarm is valid or false, it requires a short-term proportional response which may in itself create additional risk. For example, the person may not respond adequately to instructions from security staff, which may then resort to applying force. Other steps that can be taken are the verification of identity using overt means, such as the authentication of identity documents, the verification of the identity using more accurate types of biometrics, and security questioning.

Ultimately, if the alarm is valid, then we have a situation where a high-threat person has been recognised. Depending on the overall security plan, this will require one or more prompt reactions which may have a very large impact on the life and wellbeing of everyone involved, including innocent bystanders, and on the continuity of the CI. On the other hand, if the alarm was false, then we have a situation where someone is engaged as if they were a high-threat to the CI, but they know that they are not. This can easily lead to dangerous situations, e.g. if the person fails to comply with instructions from security staff. Further, such false alarms erode society's trust in the security management of the CI and the LEAs involved.

An EWZ with watchlist surveillance can also be used for intelligence purposes. For example, to inform intelligence services of the attention that watchlisted persons have for CI. In that case, there is not much of a warning function, so these kinds of purposes are out of scope for this report.

3.2.5 Watchlist surveillance: functional components

An EWZ system for the recognition of known high-threat persons (i.e. watchlist biometric surveillance) is composed of several (optional) functional components, described in Table **2** below. This table excludes the measures used for alarm resolution. In this table, the term 'biometric template' is used for all types of biometric modalities.

Table 2. Functional components of a watchlist surveillance system for early warning zones.

Functional component	Function
Biometric imaging for enrolment	[Optional] Capturing a biometric template from the subject for the enrolment process. An alternative for this component is to use biometric images from other systems, such as from identity documents, mugshots or surveillance systems.
Biometric capture subsystem in flow	This captures the biometric template from the subject when he is detected in a surveillance setting. It may include spoofing detection, active lighting and template enhancement (e.g. image enhancement). The sensors for this component may be provided by the CI operator, the local municipality or a law enforcement agency.
Biometric comparison	Comparing biometric templates from persons 'in flow' to the enrolment templates. This component typically produces ranked lists of similar persons for each person in flow.
Managed analytics	[Optional] Monitors and determines technical metadata parameters of sensors, sensor data and the subject, related to the performance of the EWZ system.
Alert and messaging	Generates alerts and messages based on the ranked lists and a set of business rules or other cognitive surveillance functions.
Detection and tracking	[Optional] Detects the presence of persons, so that it is also known when the biometric capture subsystem fails ('failure-to-capture') and keeps track of persons between moments of their detection, their recognition, and — if required — an intervention on them.
Other supporting functions	Other supporting functions include management reporting, system administration (monitoring system health and user authorisation), testing, training, secure storage and secure communication.

Source: JRC.

The EWZ functional components directly related to biometrics are described in more detail in Chapter 4. This includes the enrolment, biometric imaging (including spoofing) and biometric comparison.

The EWZ functional components that are also related to surveillance are described in Chapter 6. This includes template enhancement (e.g. image enhancement), managed analytics, and detection and tracking. Managed analytics, and detection and tracking are here marked as optional. Whether they are required depends on the use case and the required operational performance.

3.2.6 Watchlist surveillance: operational performance

Two recent studies can help describe operational performance. The first, published in 2017 by NIST is the *Face In Video Evaluation (FIVE) report* (Grother, 2017). This report presents the performance of 36 face recognition algorithms that were offered in December 2015. We focus on section 5.5 of the report, covering face recognition in the indoor access areas surrounding a sports arena. The second study was published in September 2018 by Cardiff University and covers the experiments done by the UK South Wales Police, which were outdoor during daylight (Davies, 2018). These experiments used two versions of face recognition technology from the same vendor, one from early

2017, and the second from late 2017. The vendor was one of the highest ranking algorithms from the earlier NIST study.

Neither report is clear about the ability of the algorithms to successfully capture a face. The NIST study describes how 'many' non-actors plus 480 enrolled subjects entered the area, and that algorithms detected between 27 544 (algorithm 'K33V') and 530 585 (algorithm 'A30V') instances of faces in the same set of videos. This wide variation can be explained by acknowledging that the same person can be recognised multiple times, but also that persons can be missed. The Cardiff study describes in section 7 a limited experiment on seven persons, but does not distinguish between failure-to-capture, and false non-match. The study does not provide any information about the total number of persons that passed the large-scale experiments. However, on page 17 it provides information about balancing the input of faces with the capacity of resources. This was done 'in the hope of reducing the load put on the computer hardware', and to 'not bombard the operators with alerts'. Restricting the input of faces to match available resources is a valid operational practice, if it is done within acceptable ethical and risk management parameters:

- If load balancing means that people of certain cultural or ethical backgrounds have a significantly different chance of being presented to a face recognition system, then this should raise ethical questions related to discrimination and other biases.
- And if load balancing means that it becomes easier for adversaries to avoid being presented to a face recognition system, then it can lead to unknown amount of risk, and/or to more than acceptable risk.

Both reports present information about the ability of a system to accurately recognise a person in the case that an image was successfully captured. However, without knowing how many people were missed, it is difficult to assess the meaning of those numbers. In theory, the face detection step of the tested algorithms could have rejected faces that the face recognition step would struggle with.

The best algorithm of the NIST study had a false non-identification rate (FNIR) of 0.129. This means that for every 10 known high-threat persons that visit a site and of which a facial image was made (see previous paragraph), roughly one known high-threat person will not be recognised. This performance may be acceptable for certain sites, especially when acknowledging that there may also be other security measures in place. However, this performance corresponded to — in the NIST evaluation — one false positive for every 11.7 minutes on average of video footage from one camera. That could imply for a site with 10 cameras, one false positive every 70 seconds. This may also have been experienced by the South Wales Police, as in the Cardiff study it is described how they tried various technical and operational configurations to find one that did not overwhelm their resources, including an upgrade of the algorithm by the supplier.

Even if the accuracy of face recognition improves significantly over what was witnessed in these two studies, there are very few situations where straightforward 'plain' watchlist surveillance in a high-threat scenario will be both cost-effective and with acceptably low hindrance to the well-meaning public. Which leads to the conclusion that more innovative approaches are required. NIST already suggested a form of fusion where multiple detections per person were combined to generate only one alert. Other suggestions were already presented in section 3.2.3 which describes the combination of different pieces of information in order to increase overall reliability of an alert; and in the next section technologies are discussed that may help monitor or even widen the operational conditions within which face recognition works reliably.

3.2.7 Managed analytics for watchlist surveillance

If CI operators and their LEAs are not content with the accuracy of a watchlist surveillance system, there is the possibility to apply managed analytics:

> 'Managed Analytics (MA) is analytics that is semi-automatically managed: the factors that determine the quality of the output of analytics are being monitored and controlled in order to be able to provide a sufficiently constant and high level of operational performance of the video analytics subsystem(s).' (Den Hollander, 2017)

For example, for face recognition, NIST has initiated an evaluation of face image quality assessment algorithms. This is software that assesses from images quality factors that are relevant for, in that case, face recognition:

> '… focus, illumination, distortion, and noise, and also subject-related properties like head-pose, facial expression, and eyeglasses effects.' (NIST, 2019)

Such software can be integrated into a watchlist surveillance system in order to proactively monitor the quality factors, so that effective system management can be done. Currently, there are no standards for managed analytics, nor are there industry-wide good practices available in other forms, so CI operators and LEAs have to rely on specific suppliers in this regard.

In general, there is ongoing research into cognitive networks that helps improve the performance and helps to relax the operational conditions for analytics.

3.2.8 Alternatives to watchlist surveillance

It is important to acknowledge that there are always alternatives. For the purpose of this report, the reader merely needs a general idea of them, so this section lists just a few examples.

The first option is informed risk acceptance, i.e. understanding what the risk is, and doing nothing to mitigate it. In the context of CI, this becomes risk transfer, i.e. transferring the consequences to others: those depending on the continuity of the CI, individuals and the state that is responsible for generic counterterrorism. If the CI operator and local LEAs assess that the probability of an attack is very low, then this may be a valid option.

A second option is to reduce the risk by traditional means, such as pictures of biometric identifiers (typically faces) of people on the watchlist presented in briefings and displayed in places where security staff can easily look them up (e.g. the reception area, the camera observation room). This method depends on the ability of human professionals to memorise a collection of e.g. faces. For sites with very few faces on the watchlist, this may be a valid approach; and in situations where the capture of biometric identifiers is difficult, this may be the only option for an EWZ. A practical approach is to reduce the watchlist based on the memory-capacity of security staff.

3.3 Operational environments and a fictional use case

With the understanding of what watchlist biometric recognition for surveillance in an EWZ entails, it is now possible to describe operational environments where it may be useful. Second, for one type of environment, it is possible to describe a fictional use case.

3.3.1 Operational environments

The selection of operational environments is done based on the following criteria:

- It must be considered critical infrastructure, although EWZ may also be useful for non-CI situations;
  - This theoretically excludes generic crowds in public places, such as in shopping malls or in entertainment districts, but results may also be applicable there.
- It must be representative for a significant number of real-world places, with a view to maximising the cost-effectiveness of each use case;

- This excludes places with highly specific characteristics.

— It must be conceivable that a high-risk situation can arise from threatening persons in the physical environment.

- This excludes critical infrastructure that e.g. only faces threats in the cyber domain.

Table **3** outlines the main features of each selected operational environment. This selection is not complete and there are probably many other types of operational environments in which EWZs may be useful. This selection was used to help focus the work in this thematic group. In each of these examples, the watchlist itself is typically owned by the local LEA, which is typically not the owner of the biometric sensor. The legal consequences of this situation is the main topic of Chapter 7.

Table 3. Characteristics of selected operational environments for early warning zones

Case id	CI asset	Ring model zone (see section 3.2.1)	Sensor owner
1	High-risk objects in urban environment	Observation zone	Municipality
2	Secured site in urban environment	Secured zone	Site operator
3	Public transport hub in urban environment	Observation zone	Site operator: public transport operator

Source: JRC.

For the purpose of this report, a use case should describe only all relevant factors, without describing unnecessary details. The first operational environment, high-risk objects in an urban environment, is the basis for a fictional use case in the next section. For the other two environments, Annex B contains a more detailed description.

3.3.2 Fictional use case: high-risk object security in urban environment

This fictional use case was prepared by the task leader. It had two specific purposes:

— It integrates several types of technologies (almost all of the abovementioned technological components). This allows the TG to use this fictional use case as a baseline for other tasks, regarding e.g. the definition of additional cognitive technologies, and the discussion concerning privacy.

— It relies on technologies for which, at the start of the TG, there was no consensus regarding their maturity. This stimulated the TG to search for reliable information regarding the state of the art of relevant technologies.

The first generation of real operational EWZ systems should be simpler than this overly ambitious use case. For example, by using only one type of imaging platform.

Many elements of this fictional use case have already been deployed and even found their way into standards. Other, more innovative aspects have not been standardised yet. For example, the automatic monitoring of the operational conditions ('managed analytics') is currently not standardised.

3.3.2.1 Context

The national government has tasked the agency LittleSister (LS) with surveillance tasks as part of the efforts to protect high-risk objects in urban environments on national soil against terrorist threats. The national terrorist threat level is 'elevated' and it is believed

that a successful attack will have a large impact on society. The doctrine of LS is based on:

— Deterrence through covert and open presence, and

— A superior situational awareness through,

  - among others, targeted security questioning, and
  - the use of high-end surveillance systems.

The national government and LS have to adhere to the national implementation of relevant EU directives and to EU regulations, specifically related to the European Convention on Human Rights and privacy and data protection.

3.3.2.2 Environment

The environment is both outdoor and indoor in (semi-)public spaces both high- and low-rise. Objects that are subject to surveillance include public transport hubs, government buildings, educational buildings, hospitals and palaces. An EWZ system is to be deployed in the observation area ([4]) around high-risk objects, extending up to 1 km outward from the object. The objects themselves are protected through access control systems based on conventional security measures, e.g. RFID passes. The local weather is highly diverse (including sunny, foggy, stormy, rainy and snowy) and highly variable (e.g. lighting conditions can change substantially within seconds). These (semi-)public spaces are accessible at all times of the day — including at night, when they are illuminated with artificial lighting. LS does not have ownership of the physical objects in this environment, so the possibilities to install or reuse surveillance systems are limited to 'piggybacking' on existing surveillance cameras. This includes access to their video streams as well as the ability to take temporary control over their viewing angle, focal length, resolution and frame rate. On the other hand, the local infrastructure is of the highest level, including highly reliable power and communication networks.

The public at these locations is there to travel to and from work, for leisure (including tourism) and directly adjacent to the high risk objects there are commercial and residential areas including schools. As a consequence, the public has highly variable behaviour. In some locations it will be possible to attract their attention — and gaze direction, while at many other locations they will be too preoccupied with other factors, such as negotiating traffic. The public is sensitive to privacy invasions, yet there is some support for surveillance systems. The public is accustomed to seeing fixed cameras and body worn cameras, but it should be expected that some subjects may attempt to hinder or frustrate the correct workings of an EWZ — for a variety of reasons, while others will willingly cooperate. The density of persons varies substantially over time and place. For example, during demonstrations (which are a civil right and a common occurrence around governmental buildings) parks and squares can be packed with people.

3.3.2.3 Risk identification and assessment

The specific types of assets to be protected by LS with the use of an EVF system are the functioning and physical integrity of the high-risk objects and the people that work there, and that of the people that live, work, travel and enjoy recreation activities around those objects.

Based on a methodological analysis of available sources, it is believed that there is a credible terrorist threat, with underlying political, religious and/or mental health motives. The threat target can be the building, vehicles or symbolic objects in or around the building, people working there, including VIPs, passers-by, or the personnel of LS or

([4]) The **observation area** is a term from the object security domain, specifically the ring-model (also known as 'security-in-depth'. It is the unprotected area that adversaries have to traverse to reach a protected area. In the context of CIP, the observation area is often not owned by the operator of the CI, but is a public area.

other security services, including people in groups or crowds at these locations, e.g. waiting to enter the building (e.g. people waiting in a queue to enter a museum).

Such a threat can manifest frequently, but not continuously. Attackers can work alone or in small groups (e.g. up to 10 people). Their capabilities range from none to highly trained with small weapons up to moderate explosives. They can move on foot, on bikes, scooters, cars and in public transport. They do not possess the capabilities to simultaneously attack in the cyber domain. However, other (opportunistic) threats will attempt to test the cyber protection of the EWZ system. Besides physically attacking objects or people (including suicide attack, hostage and kidnapping), other modi operandi may include the theft of sensitive information through physical infiltration. A single attack may consist of multiple stages, involving multiple separate targets.

Templates of the faces of potential attackers (i.e. persons of interest) will be known beforehand through various intelligence means, such as facial templates of various quality obtained from the police during earlier apprehensions but also templates made from images made during undercover operations. However, the quality of these images and templates is highly variable. Attackers will count on the fact that it is not possible for LS personnel to memorise, remember and recognise all relevant faces.

3.3.2.4 EWZ system

The LS is looking for an EWZ system for the short-term deployment (not to be confused with deployment on short notice). It is acknowledged that the integrated concept is new and untested, and may require further development, but the technological components should individually have a proven track record in this environment. Deploying and using an EWZ system may require the help of additional smart technologies, as long as that is within the mandate of LS (with regard to a lack of ownership of the existing surveillance infrastructure). The alternative to an EWZ system is an additional security perimeter with additional access control, where every visitor is asked for identification.

3.3.2.5 EWZ objectives

The EWZ must help LS before, during and after a terrorist threat or attack in the observation area around high-risk objects — which is outdoor. It must support both overt and covert ([5]) use. The EWZ will be used as part of intelligence gathering processes, during surveillance tasks and for investigation purposes to detect the presence of known ([6]) high-threat persons and of (known or unknown) persons that frustrate the workings of the EWZ, e.g. by hiding their face. Known high-threat persons must be recognised in 95 % of their visits to an observation area. Given the expected number of visitors to these high-risk objects and the available capacity, a false alert rate of 0.1 % **per visit** is acceptable. Persons that frustrate the workings of the EWZ must be detected (not recognised) in 99.5 % of their visits. For this detection a false detection rate of 10 % **per visit** is acceptable. If the subject is still present when the alert is received by the end-users, then they will be manually checked by local overt LS agents for identification and questioned on their behaviour and purpose of visit.

By using an EWZ in this way, the benefits that LS is hoping to obtain (and on which they will evaluate its performance) are as follows:

— Fewer terror attacks at these high-risk objects because adversaries are deterred by the EWZ;

— Fewer terror attacks because known high-threat persons will be recognised in an early phase of their planning cycle so that LS agents can intervene;

([5]) Overt and covert are terms from the surveillance domain. Covert surveillance means concealed from the subjects under surveillance. Overt is the opposite: in the open/not covert.

([6]) The persons have to be known in the sense that an image is available. A biometric system cannot be used to recognise (high threatening) persons of which no image is available.

— Less damage of terror attacks because multi-stage attacks will be stopped sooner, since the perpetrators can be recognised much faster and with a high level of confidence;

— Shorter investigations after threats because evidence is more conclusive;

— More visitors ([7]) to high-risk objects protected in this way, compared to objects where additional security perimeters (the alternative to EWZ) have been deployed;

— More visitors to high-risk objects compared to similar high-risk objects that have no additional security measures;

— Lower costs of security measures compared to the alternative with additional security perimeters;

— Lower stress-related costs associated with LS agents who feel less vulnerable than when passively guarding high-risk objects ([8]).

3.3.2.6 EWZ constraints

Per visit, it is estimated that persons will appear in the coverage area of at least three cameras (not simultaneously). At those appearances, it is also assumed that at least 10 other people are visible and recognisable in the same image. The EWZ must use analytics to determine the best images to use for recognition, tracking and location of persons, and it must proactively alert end-users (e.g. maintenance personnel) if the quality of sensors (including orientation and lighting conditions) is below acceptable levels. On the other hand, the EWZ must actively improve the quality ([9]) of relevant images which are otherwise unusable.

3.3.2.7 EWZ human-machine interaction

The end-users of EWZ are analysts that work in a back office. They receive the alerts from the EWZ, verify them and inform other services that will act upon the information. In addition, they locate and track the subjects using the EWZ as long as necessary in the observation area, i.e. (pending the security policy):

— until the subject is under control, or

— until the subject has left the area, or

— they are no longer suspected of causing a threat.

They can also assess whether the subject is currently not present in the observation area. In addition, they can create business rules on these alerts. Specifically, for the following cases (parameters to be specified in the business rule):

— If the certainty of an alert is above a certain threshold ([10]);

— If specific combinations of persons visit within a certain timespan;

— If recognised persons visit certain areas (not) in a specific order;

— If specific recognised persons are seen near each other, and later near other persons, etc.

3.3.2.8 EWZ mode of deployment

Where the processing takes place is up to the supplier — within legal constraints. Where available, the EWZ system can use existing secure high-bandwidth wireless networks,

([7]) The objects have a function (e.g. an airport transports people). If people avoid the use of that function because of the EWZ, then the EWZ is — in this regard — worse than the alternative.

([8]) Security staff who feel too vulnerable in their work will look for other work. This is a cost for their employers, because they have to attract and train new staff.

([9]) Improving images **after** they have been recorded can be done using image processing techniques such as super-resolution and image stabilisation.

([10]) Numbers should be specified in a real-world use case.

but the EWZ must also be useful in low-bandwidth settings, and even without any live wireless connectivity. Specifically, the data (watchlist templates and hits) from body-worn cameras must then be synchronised at physical contact points, e.g. at the end of a shift.

The EWZ must use automatic face recognition for the purpose of recognising people. It may additionally use soft biometrics (e.g. clothing, walking pattern, etc.) to locate and track individuals of interest in the observation area after the initial recognition.

It must be vision-based (i.e. using cameras) but without active lighting as that would reveal covert use. It must work with video and image streams from a single viewpoint, i.e. not requiring array technology because that would make the use and maintenance of the EWZ too complex. It must work on two types of sensor platforms. The first is a fixed, yet rotating platform such as pan-tilt-zoom (PTZ) cameras, with a skimming viewing angle from slightly above. The second platform is body-worn cameras carried on the shoulder, oriented in the horizontal plane, looking forward from the carrier's perspective. The distance between the sensor and the subject can vary between 5 and 100 metres for the fixed platform, and between 0.5 and 30 metres for the body-worn camera. LS has approximately 1 000 operational agents. Around an average object, 10 PTZ cameras are in use, and three agents each using a body-worn camera.

3.4 Conclusions from the use cases

Several types of operational environments have been identified where the concept of an early warning zone might be useful. These environments served as backdrop for the functional specification of how an EWZ, specifically based on watchlist biometric surveillance, could contribute to an overall security concept.

It is important to acknowledge that if the presence of biometric sensors is overt, then counter methods of the adversary can be 100 % effective (e.g. running past a camera). This means that for truly high-risk scenarios, the timely detection of persons for which no biometric identifier could be captured is an essential component of watchlist biometric surveillance.

Data describing the operational performance of systems is sparse and it is difficult to make comparisons between different sources of information, as is illustrated with the high-level examination of the NIST and Cardiff studies (see section 3.2.6). For example, the Cardiff study looked at only one vendor.

The NIST study implies that there will be operational difficulties in using the technologies as false alarm rates may be high, even with optimum performance settings. The Cardiff study investigated those operational circumstances and learned that, although technology is certainly not a silver bullet it can be useful with acceptably low hindrance to the compliant audience if used in a supporting role to a human-in-the-loop. However, the definition of what is acceptable hindrance from surveillance systems is very subjective, and is subject to active societal debate.

The combination of requirements of covert sensors, non-cooperating persons, and people in flow requires a very high accuracy of all biometric functional components, a very well-tuned composition of all those components, proactive and adequate maintenance and high-end alarm resolution procedures.

Supporting technologies (such as algorithms that determine relevant image quality metrics) are available (see section 3.2.7). There may be other non-obvious ways to compose EWZ systems based on watchlist surveillance (see section 3.2.3) which may provide better cost-effectiveness, but there are no standards available to help CI operators and their LEAs integrate them in an EWZ system. Therefore, CI operators and their LEAs have to custom-build biometric watchlist surveillance systems, which raises the question of their ability to manage the design process involved in such endeavours, which may lead to unexpected risks.

The ERNCIP TG on EWZ believes that there will be a need to revisit watchlist biometric surveillance in any future work in this area, especially if new developments in relevant technologies or standards are made, or if new trials are conducted and new information sources become available. Vice versa, this report may serve as inspiration for the development of relevant supporting technologies and standards.

4 Biometric recognition

4.1 Introduction

Biometric recognition, also known as biometrics, is defined by the International Organization for Standardization (ISO) ([11]) as 'automated recognition of individuals based on their biological and behavioural characteristics'. Some biometric characteristics (e.g. fingerprint or iris) are predominantly biological, while others (e.g. voice, gait or handwritten signature) are mostly behavioural, requiring a dynamic engagement with the user.

In the context of this report, biometrics is used in computerised applications, where the system incorporating the biometric function is designed to operate with only limited human intervention.

There will be times when the automated system is unable to recognise the individual; for example, an individual may have injured their finger, have the fingerprints abraded through repeated contact with brick dust or be missing a finger. For these cases, there needs to be a fallback process to check whether or not the person is who they claim to be. An assessment should be made early on to determine the number and types of problem cases in the target population of users.

Hence, the biometric component is almost always a part of a larger system designed to deliver specified benefits to the organisation. In some applications, the human aspects of the system are included as an explicit part of the application, for example, in resolving the alerts which are raised when a facial recognition system operates on video footage from a specifically designed video surveillance system.

4.1.1 Biometric applications

Many types of biometric system have been described in research papers, but for today's practical applications by operators of critical infrastructure systems, two aspects are of particular significance.

The first aspect is the type of application; examples of which include:

— Verification of a claimed identity in an access control system to a building, perhaps using a fingerprint biometric system; and

— Identification of an individual seen on a CCTV camera and included in a 'watchlist' of persons of interest (as shown in the previous chapter).

The second aspect relates to biometric modality ([12]), i.e. the specific type of biological or behavioural characteristic employed. Of the many modalities which have been researched, some have been commercialised and widely deployed. More information will be found on section 4.2 and those with potential to be used in EWZ are detailed in section 4.3.

Biometric technologies can be applied in a number of ways, many of which are relevant to the requirements of operators of critical infrastructures who need to maintain the appropriate level of security. Among these applications are:

— Physical access control, to a site or to internal areas within a site (more information below);

— Logical access control, to computers and mobile devices;

— 'On-the-spot' verification of identity, challenging the identity of an individual in a specified zone using mobile biometric devices;

([11]) More specifically, it is the subcommittee of the ISO/IEC International Standardization Group which addresses biometrics and their applications (JTC1 SC37).

([12]) Biometric modalities are different types of biological or behavioural characteristics which can be utilised in automated recognition.

— Verifying the identity of individuals either entering or leaving a country through the use of automatic or semi-automatic means;

— Verification of identity against biometrically secured identity documents at places other than at the national border, e.g. on the first day at a workplace or prior to allowing access to computing facilities;

— Surveillance systems to identify unknown individuals, e.g. individuals repeatedly being seen in the neighbourhood of critical facilities using biometric recognition in combination with video surveillance systems (more information below);

— Vetting of new (or existing) employees and managers as part of a criminal record or counterterrorism check;

— Authorisation and audit of key/critical actions in operation of facilities, to ensure that only authorised personnel are able to initiate specific functions;

— Confirmation of specialised training and qualifications, e.g. in a decentralised organisation with branches in different regions and countries, to allow managers to confirm that certificates of competency have not been tampered with;

— Ensuring integrity of critical components in critical infrastructure networks/facilities, through sign-off of by competent and identifiable individuals (the specific component or tests results can be individually marked with a digitally signed biometric identifier);

— Maintenance of the integrity of documents with a digital signature which includes biometric data of the author.

4.1.2 Biometric components

Biometric components are usually integrated as a part of a larger, overall system that serves an application, with the latter providing one or more benefits to an operator (e.g. offering a more secure way of gaining access to a room or building).

Biometric subsystems may include components such as:

— A tamper-resistant or tamper-evident reader through which the biometric data is collected from the user;

— Computing hardware and a protected interface to deliver the result of biometric processing;

— A data store which holds biometric reference data relating to those people permitted to enter the building;

— Biometric software for isolating the area of interest (e.g. the face area, the fingerprints, the iris, etc.);

— Assessment of whether the quality of the data isolated is sufficient for subsequent recognition — or whether the user should be asked to re-present their (for example) finger to the reader;

— Comparison of the biometric data collected from the user with one or more sets of reference data in the data store;

— Confirming whether the biometric data has indeed come from a living person and is not, for example, a plastic replica of a fingerprint. Another important aspect is confirming that the data is genuine and not elaborated (e.g. made by photo-morphing software);

— Communication to the overall system of the results of biometrics processing.

The organisation wishing to implement the application (e.g. secure physical access control into a room or building) will also need to consider non-functional aspects such as:

— An enrolment process for registering users' biometric references into the system. In a formal enrolment the user's credentials (e.g. a biometric passport) should first be

checked to confirm that they are authorised to be enrolled into the system, thereby precluding unauthorised individuals from being registered. Well-designed and operated processes are needed to ensure that the best possible biometric data is captured. In some cases, there may be a need to repeat the enrolment periodically for those users whose characteristics have changed since the initial enrolment (e.g. due to ageing), and which now cause difficulties in operation.

— A fallback solution for cases when a correctly enrolled person fails to be matched to their reference. Fallback solutions will also be required when individuals cannot be enrolled in the first place, e.g. due to disability — whether temporary or permanent in nature.

— A testing policy for the operation of the overall system to demonstrate that the operational system and/or application delivers the benefits required by the operator.

— A security policy specifying the practices and controls for the secure operation and maintenance of the biometric system.

— A privacy policy (and, perhaps, a privacy impact assessment) to declare how personal data (including the biometric data) will be protected, and — for some systems and in some countries — to demonstrate the legal basis for processing.

It is advisable to consider all of these issues as early as possible in the design process; the later these functions are added, the more expensive and ineffective these will be.

4.1.3 Presentation attack detection

It should be noted that, at present, many commercial biometric systems do not offer resistance to spoofing through measures such as liveness detection. This functionality will vary according to the specific modality and even the way in which the modality is implemented. For example, for iris recognition systems, the response of the iris to changes in illumination or the monitoring of the involuntary movements of the eye may provide evidence of a live iris — and that the presentation to the system is not a photograph or video clip.

System operators should also be aware that someone may intentionally present an artefact such as a glass eye while pretending to be an authorised individual (e.g. by keying in a reference number) with the aim of locking out the legitimate individual.

Adding software to counter such attacks may impact adversely on the performance of systems, and lead to changes in the system error rates such as FAR (false acceptance rate) and FRR (false rejection rate). Users should insist that for systems that are required to have liveness detection, the specification and testing of systems should always relate to operation with the liveness detection functionality switched on. In case there is a need to know the contribution of a liveness detection to overall error rates, a separate testing of the biometric algorithm and the liveness detection algorithm is needed.

4.2 Evaluation of biometric recognition

Applications which use biometric technologies are many and varied. For systems deployed at a large scale, the cost of failure can run to tens or hundreds of millions of euros as well as the associated loss of reputation; and replacement systems may require users to readjust to news ways of working.

Therefore, it is important to make sure that the application performs to the desired specification — and not just that the biometric subsystem functions correctly. However, without a properly functioning biometric subsystem, it is very unlikely that the benefits of the deployed application will be realised.

One of the two fundamental aspects of the operation of a biometric system is the automated comparison of biometric characteristics to obtain a similarity score. If the

similarity score meets (or exceeds) a predefined threshold, the characteristics are deemed to be matched, and the individual is recognised.

The other fundamental aspect acknowledges the limitations of the human–technology interaction which impacts on the representation of individuals' identities by templates in the system; the collection and processing of a biometric characteristic will differ each time the user is involved in the biometric process. For example, a finger may have been pressed unevenly on the sensor's surface, the subject may have been smiling or facing away from the camera (whereas on enrolment they will have been asked to face forward and not smile).

In performance testing of biometric applications, we seek to measure the likely rates of failure:

— Failure to enroll (FTE). For a variety of reasons it may not be possible to capture biometric characteristics from an individual in the first place. This may not be the fault of the individual and they should not be stigmatised or disadvantaged from using the system. But in some cases, the individual could be responsible for this (e.g. user not willing to cooperate for a variety of legitimate or illegimate reasons).

— False non-match (FNMR). This is an incorrect failure to identify an individual, who is not matched by the system against their own enrolled record.

— False match (FMR). This is an incorrect identification of an individual through matching their biometric characteristics to an existing enrolled record of someone else.

— Failure to acquire (FTA). For a variety of reasons it may not be possible to capture biometric characteristics to match to existing enrolled biometric characteristics. This may not be the fault of the individual and if it is not then they should not be stigmatised or disadvantaged from using the system. If this persists, the individual may need to be enrolled again into the application.

The corresponding performance metrics are the rates at which these errors occur in the test population: FTE, false non-match rate (FNMR), false match rate (FMR) and FTA ([13]). Other terms and definitions can be found in the ISO Biometric Vocabulary standard (Annex A).

In addition, there will be metrics specifically associated with tests addressing IT security requirements and assessing the usability of the system by the intended population.

Where the application is intended to identify individuals on a scale of millions, it has to work reliably under the widest range of operational conditions and for a wide diversity of people. That is, the biometric subsystem is required to work at the desired operating point for metrics such as FNMR, FMR and FTE and associated security and usability parameters.

The statistical basis of biometric comparison is affected by a number of factors. These include:

— The underlying population demographics (e.g. age, gender, ethnicity and disability);

— The size of the database; and

— The performance of all elements of the biometric subsystem used to acquire images and compare biometric characteristics.

It is unlikely that an interdependence between these factors and the resulting performance of the system will be simple or even calculable. This means that although test protocols can be guided by previously available test results on similar systems, the performance for a specific application will have to be determined by a bespoke testing

([13]) When 1:1 verification systems are tested, the metrics should be considered on a per transaction basis; several attempts are allowed before a transaction is deemed to be completed. In this case, the error rates are presented as false rejection rate, FRR, and false acceptance rate, FAR, respectively.

approach. Publicly available test results on similar systems also require careful consideration, for a number of reasons, as outlined in the next section.

The reader interested in more background on biometric testing is referred to the *Best Practice Guide* by Mansfield and Wayman (2002) which includes rules of thumb around the optimum sizes needed for test datasets. Further information is provided in relevant ISO standards ([14]).

Publicly available test results are available from the following sources:

— Vendors of biometric equipment;

— Open testing performed by publicly funded bodies, such as the National Physical Laboratory (UK), or the National Institute of Standards and Technology (USA);

— 'Benchmark' testing conducted by organisations procuring biometric systems;

— Academic-led testing for research.

Although they can provide valuable input to any evaluation of biometric technologies, and indeed may have to be used at early stages of any procurement programme for justifying business decisions, they all suffer from a number of limitations and cannot be taken to be definitive for decisions on the procurement of large-scale biometric systems. Where they are used in the initial definition phase, subsequent testing should be used to revisit the initial conclusions, thereby ensuring that these are still valid, as well as confirming the validity of any business decisions based on initial test results.

The principal limitations on the use of such publicly available results include:

— Similarity of application. Seemingly small changes in the system design and context of operation can affect the transferability of the results of tests on one system to the one under consideration by the operator. If there is no cost-effective alternative, a careful analysis of differences in demographics, conditions of collection, etc. between the two systems should at least be undertaken, with tests commissioned to explore the impact of noted differences.

— Progress in biometric technologies. Results obtained in earlier tests will inevitably have used older algorithms, and hence may provide an unduly pessimistic assessment of current performance.

— Availability of test datasets of the required size. Biometric data is rightly regarded as personal data and its use in testing will require significant care to ensure that all of the pre-agreed protocols around access to, and the use and deletion of, such data are followed. These tight access restrictions result in very few large-scale test datasets being available for other groups against which to test new systems.

— Representative test datasets. As discussed in the previous section, experience shows that the performance of biometric systems is dependent on the specific demographic makeup of the population. It is therefore important that all test datasets are representative of the target population. Although synthetically generated test datasets have been investigated, the current advice is not to rely on these until further research demonstrates their robustness.

— Confidentiality of test results. There is a reluctance to disclose details of the test results by operators for fear of inadvertently releasing information which could be of use to those aiming to subvert the biometric subsystem or any applications which make use of it.

— Commercial and competitive pressures. Vendors of biometric technology are in a very competitive marketplace and hence are unwilling to disclose results which could position their products in a bad light.

([14]) ISO/IEC 19795-1:2006 Biometric performance testing and reporting — Part 1: Principles and framework. For operational testing (Type E above), please refer to ISO/IEC 19795-6:2012 Biometric performance testing and reporting — Part 6: Testing methodologies for operational evaluation.

— Costs of testing. The significant costs associated with large-scale testing may mean that large-scale tests may only cover a subset of the available technology and may not include the most appropriate technology for an application.

— Extrapolation techniques. Techniques and methods for extrapolating performance figures for large systems from small-scale tests have been used in the past, but reliance on these extrapolations poses considerable concerns for the test house undertaking the test and the operator relying on the interpretation of results. Clearly, the larger the test, the less the need for such extrapolation with a resulting greater confidence in the prediction of performance on operational systems.

As can be seen, evaluation of biometrics is a complex task to be performed and understood. Further introductory information can be found in Waggett, P. (2015) and details on how to perform it can be found in the ISO/IEC standards previously mentioned.

4.3 Biometric modalities

Biometrics can be applied to a great variety of parts of the body, extracting different features from each of them. Each of these specific implementations of biometric recognition is called a modality. There are several well-known modalities, such as fingerprint, iris, face, voice and handwritten signature, while others are less known, such as vascular or palmprint.

Having such a variety, it is typical to compare all modalities in search for the best one. In order to do so, several parameters can be considered:

— Universality: That indicates the percentage of the population that presents extractable features for that modality. This percentage can depend not only on the physical availability of that part of the body, but also on the adaptation of the population conditions to the acquisition device. For example, the universality of fingerprints depends on the amount of population with one available finger, but also on the percentage of the population that may have eroded fingerprints (e.g. carpenters) that make its capture not possible with certain kind of fingerprint sensors.

— Uniqueness: The probability of two citizens within the population not presenting the same biometric features. This is directly related to the discriminative power of the features extracted in the biometric modality.

— Stability: Whether the extracted features remain stable throughout time, weather conditions, health status, age, etc.

— Acquisition simplicity: If there are acquisition methods that are easily used by an average citizen within the target population. This is directly related to the usability level achieved, and therefore inversely related to the user rejection to use the system. For example, in old or low-end iris recognition products, is the user the one that has to align himself to the camera in order to allow the system to acquire a relevant iris image; this is not an easy task and drives a high level of user rejection. On the other hand, current high-end iris recognition systems, use dynamic location of the user eye, in order to acquire the iris without a significant user interaction.

— There is a parameter directly related to the acquisition simplicity, which is the average time the user needs to get his biometric trait captured, in particular when user has to wait for the trait to be captured (i.e. not when the sample is captured on-the-move).

— Performance: i.e. the error rates achieved by the modality.

— User acceptance: This can be affected by the usability of the system, but also on other conditions, such as cultural behaviour, police implications, etc.

— Resistance to fraudulent use: Whether the modality and its commercial systems can recognise attacks such as spoofing, replay attacks, etc.

— Cost.

— Maturity: If the modality has been deployed already and the success rate of such modality in different scenarios (e.g. overcoming different kind of inconveniences and/or attacks).

— And any other parameter that may impact on the successful deployment of the technology, such as adaptation to the scenario where the system is to be used.

It is important to note from the outset that there is not a single biometric modality which is better than the rest in all cases. With so many parameters, it is impossible that one modality is the best one in each of the different parameters, for all different scenarios. For example, there is the common belief that speaker recognition (i.e. voice) is quite bad because of the lack of stability of the samples and the poor recognition rates achieved. But when considering an application over the phone, such as telephone banking, speaker recognition is the most natural way of identifying the user, as the citizen will talk with normality and the acquisition device is already in the hands of the user (i.e. the phone). This is a simple example where it can be seen that an a priori bad modality can in fact be the best one in certain scenarios. This is the important contribution of this report, as it analyses different biometric modalities for one particular case: early warning zones.

4.3.1 Physiological modalities

4.3.1.1 DNA

DNA is a biometric modality that is frequently used in forensics and healthcare. It is based on capturing a piece of biological tissue or fluid from the user, and extracting from it what are known as short tandem repeat sequences (STRs). Depending on the number of STRs and their contained information, it can be used for identifying individuals or for other tasks such as linking relatives or detecting health issues.

Being considered as 100 % accurate, the possibility of extracting much more information than the simple identity is one of the drawbacks of this modality (this may also happen in other modalities, but in DNA it is particularly important; cf. the discussion on privacy in Chapter 8). Other problems with this modality include the non-friendly acquisition system, the excessive time needed for manipulating the sample and processing the information, and the size and cost of the equipment needed.

Considering the parameters previously mentioned:

— Universality: This is the only modality that can really be considered as 100 % universal, as all human beings have DNA.

— Uniqueness: As mentioned, it is considered as the most accurate means to determine the identity of a person, with an accuracy close to 100 %.

— Stability: DNA is stable along the life of the human being.

— Acquisition simplicity: The acquisition is complex, with the need for excessive user interaction, and invasive (e.g. obtaining a trace of the user's saliva with a cotton swab, or a blood drop after pricking the user's finger). This may mean a huge user rejection of the modality.

— Performance: As mentioned, the current algorithms can achieve a 100 % accuracy.

— User acceptance: Not really tested, but it is expected to be extremely low due to both, the acquisition technique, and the time needed (with Rapid DNA, the whole process can now take about 90 minutes).

— Resistance to fraudulent use: Excellent as it is not only possible to determine if the sample is a living sample, but also no spoofing method is known to date.

— Cost: Currently, the equipment use is both expensive and with little portability.

— Maturity: The modality itself is very mature, as it has been used for decades now. But only in those scenarios where time and cost is not a constraint, such as forensics and healthcare.

4.3.1.2 Fingerprint

Fingerprints are one of the best-known biometric modalities. Having been scientifically studied for more than a century, the modality is based on studying the structure that the skin ridges and valleys of the finger tips. The universality of this modality is well studied and extremely high, considered by police forces as the primary positive identification method since the beginning of the 20th century. From the drawback point of view, this police implication is the reason behind the rejection of this modality by certain population groups. Also, the high performance of this modality may be reduced by using capture devices that are not adapted to the variability of the scenario or the population; typically when using cheap semiconductor sensors.

Fingerprint sensors are to be found in the widest range of biometric physical access control subsystems. Fingerprint sensors may use:

— optical sensors (often these use illuminated glass plates, the plate forming part of a prism and camera arrangement such that frustrated total internal reflection highlights the finger ridges in contact with the plate); or

— solid state sensors, imaging the fingerprint electronically.

For verification systems, such as access control, fingerprint sensors that image a single finger are generally used. For identification in large populations, much larger format 'slap sensors' are also available, capable of simultaneously imaging four fingers from one hand. When necessary, many sensors can be configured to deliver images in conformance to international standards, thereby facilitating cross-checking against law enforcement databases.

It is important to observe the guidance from the supplier of equipment on positioning of the reader. For example, systems can be affected by direct sunlight. There may also be difficulties in obtaining sufficient fingerprint detail in very low or very high humidity environments or in cold weather conditions.

Usability can be affected by the height at which the fingerprint reader is placed, and even the angle at which the sensor is mounted. Ignoring such usability considerations may result in poorer performance of the biometric subsystem. Even if users adjust their behaviour, it may impact on their satisfaction with the operation of the unit.

The US National Institute of Standards and Technology runs tests under the Proprietary Fingerprint Template Test Phase II programme (PFTII) to measure the performance of matching software using the vendor's proprietary fingerprint templates ([15]).

Many systems use variants of the minutiae approach as a starting point for creating templates. In some countries and cultures there may be an association in the minds of the user population between the use of fingerprint biometric systems for automated recognition and fingerprint forensic systems used in police work. The extent of such an association — and the impact this may have on the willingness to use biometric systems — may need to be ascertained through consultation, surveys and focus groups.

Considering the parameters previously mentioned:

— Universality: Although some authors may consider this modality as 100 % universal, this is quite far from being true. Even forgetting those citizens with no arms, some medical treatments have been proved to 'erase' fingerprints from fingertips. In addition, depending on the sensor used, the number of users unable to provide sufficient quality fingerprints could be very high. Manual workers may have their

([15]) http://www.nist.gov/itl/iad/ig/pftii.cfm and results page at http://www.nist.gov/itl/iad/ig/pftii_results.cfm (accessed 17 June 2019).

fingerprints so eroded that some sensors may fail in achieving an acceptable image. Also, some semiconductor sensors may face problems with users when their skin is either too humid or too dry. At the end of the day, the amount of failures to enrol and failures to accept will drive the universality far from the theoretical 100 %.

— Uniqueness: Based on the historical works of Sir Francis Galton, the uniqueness of fingerprint has been considered as excellent. It is estimated that the probability of two fingerprints being identical is lower than 1 in 1 million.

— Stability: The work of Sir Francis Galton has also shown that fingerprints are stable throughout the life of an adult, even after suffering superficial injuries.

— Acquisition simplicity: With most sensors, the acquisition process is simple for most, if not all, human beings. The best proof for this assertion is the huge number of users that are currently using fingerprints to unlock their phones, considering the large variety of sensor technologies, sensor location and detection algorithms.

— Performance: This is one of the few modalities that have gone through many independent evaluations, and in this case, even massive ones with large number of samples and a huge variety of vendors taking part. For example, the evaluations performed by NIST have shown the good performance of this modality from a realistic point of view. For example, in 2015, the FpVTE evaluation showed that there were algorithms able to identify a person within a database of 100 000 people in less than 5 seconds, with a false negative identification error rate of 0.05, forcing the false positive identification error rate to 10^{-3}.

— User acceptance: As mentioned above, the use of fingerprints in smartphones has shown the high acceptance of this modality by all kind of users.

— Resistance to fraudulent use: The bad news on this modality come from the attacks that are continuously published in the use of this technology, in particular with low-cost sensors. Fake fingerprints can be successfully presented, even manufactured, with very low-cost materials and not so much expertise. Some sensors and processing algorithms are adding modules in order to detect several of these attacks before the comparison is made, but there is still a lot of work to be done. But it is important to say that most of these attacks are cooperative (i.e. with the cooperation of the real user) and could be easily detected in a supervised environment.

— Cost: The cost is directly related to the cost of the sensor, and there is a huge difference between live scanners (few thousand euros per unit) to semiconductor sensors (few tens of euros per unit).

— Maturity: This is one of the most mature biometric modalities in the field of both biometric identification and biometric authentication. In several countries it has also been used for border control or for other public services, such as tax payment or healthcare services.

4.3.1.3 Palmprint

Palmprints can be considered as a derivative of fingerprint technology, but instead of using the image of the fingertips, the image of the whole hand palm is acquired. Due to the large image size and its complexity, algorithms are different. Although it has been under research for more than a decade, it has not been deployed. One of the reasons may be due to the sensor size, or the unknown improvement compared to fingerprint.

Considering the parameters previously mentioned:

— Universality: Universality could be considered equal or even better than fingerprint, as it is improbable that the fingerprint erosion also affects the rest of the hand palm.

— Uniqueness: No comprehensive study has been found, but it is expected to be equivalent to fingerprints, as the biological basis for the generation of the palmprint is similar to that for fingerprints.

— Stability: The palmprint is composed of very different kinds of lines, some generated during the user's life and increasing in number with age. Therefore, stability could be questioned and it is initially considered as lower than that of fingerprints.

— Acquisition simplicity: for example, when using multi-finger live scanners, such as the ones used in some airports. There is the need for significant user interaction, being required to stop, place the whole palm in the sensor and wait for the acquisition to be made without moving the hand. But it is not a complex procedure.

— Performance: No independent evaluation has been performed, so there is only the reference of those scientific papers which vary greatly in testing procedure, database size, and results reporting. There are even some authors claiming a 0 % equal error rate and 100 % identification rate.

— User acceptance: As no public deployment has taken place, no conclusion about user acceptance can be found. A minor rejection from some people is expected due to the fact of having to place the whole palm in an 'uncontrolled' surface.

— Resistance to fraudulent use: This has not been tested, but considering the technology involved, being similar to some fingerprint systems, this modality can be subject to the same kind of attacks as those in fingerprint technology. The only benefit of this technology in this respect, is the low probability of being able to obtain a latent image of the whole palmprint, while this is quite easy for fingerprints. This fact indicates the difficulty in executing non-cooperative attacks.

— Cost: In most of the scientific papers, the acquisition device is a flat scanner, which are relatively cheap.

— Maturity: As said, this modality has not entered deployment phase, and therefore cannot be considered mature enough.

4.3.1.4 Hand geometry

Hand geometry is considered to achieve medium security, but with several advantages compared to other techniques:

— Medium cost as it only needs a platform and a low/medium resolution CCD camera;

— It uses low-computational cost algorithms, which leads to fast results;

— Low template size: from 9 to 25 bytes, which reduces the storage needs;

— Very easy and attractive to users: leading to a nearly null user rejection;

— Lack of relation to police, justice, and criminal records.

In the late 1990s, only one system was commercially available, developed by Recognition Systems Inc. It enjoyed a reasonable level of deployment for access control and even a pilot initiative in border control.

The hand geometry identification system takes a photograph of the hand of the user, and after being pre-processed, a set of measurements are extracted, which serve as the features for the biometric comparison.

Unfortunately, the application of this technology is limited by the volume of the capture device, although there are initiatives for using this modality with a non-restricted positioning of the hand, even using smartphones and the hand in the air.

Considering the parameters previously mentioned:

— Universality: As for palmprints.

— Uniqueness: No study has been done in this respect, but it is known that when this modality was used for border control in the early 2000s, uniqueness was lacking with large target populations.

— Stability: The stability is low, as changes in weight and illnesses such as arthrosis can impact the geometry of the hand. But if the system is used on a daily basis, these changes can be detected progressively enabling periodic updates of the user reference.

— Acquisition simplicity: The system is very easy to use, either with pegs or in peg-free mode. It presents the same inconveniences as palmprint.

— Performance: Past deployments show that performance was not good enough with large populations, but acceptable for small groups (e.g. the members of an SME). There have been many scientific papers published in the past decade, but again the testing methodology and database use do not allow the obtaining of reliable conclusions.

— User acceptance: As no negative implication is perceived from this system (e.g. lack of police connection), very little user rejection was found, only some users not willing to place the hand in a non-controlled surface.

— Resistance to fraudulent use: No studies have been found in this respect, but due to the simplicity of the samples used, it is expected that fake samples are easily built with little cost, but needed some cooperation from the real user.

— Cost. The technology needed is not complex, so the cost is not expected to be high.

— Maturity: Even though deployments have been done, this modality cannot be considered mature, or just mature enough for a limited use (e.g. small target population).

4.3.1.5 2D facial recognition

Facial recognition presents characteristics similar to those relating to speaker recognition. It is a modality that has been also studied for decades, but the lack of stability due to age, surgery operations, complements such as glasses or piercings, changes in look especially related to the hair and beard, or different kinds of make-up, leads to present high error rates. Even illumination and facial expression present real challenges to this modality. Current advances in this modality, as well as the use of 3D capture devices (see following subsection), have greatly improved its performance.

The simplicity of an access control system consisting of just a camera and software has intrigued developers of access control systems. Though software for comparison of facial templates remains sensitive to change of pose of the head between enrolment and recognition, to uneven illumination of the face and to variable expressions by the user, the experiences gained by early adopters of the e-passport gates at airports has resulted in operationally robust systems with performance adequate to satisfy the risk appetite of the immigration authorities from a number of countries.

More compact systems have been sold extensively, for example for access control at construction sites, with some suppliers using near infrared illumination to counter the effects of uneven ambient lighting.

This modality has even taken an important share of the smartphone market, as it is included in several mobile models, the most known being the iPhoneX, where face recognition has substituted fingerprint verification.

Considering the parameters previously mentioned:

— Universality: In pure terms of universality, everybody has a face. Even though there are situations that challenge this statement, such as coming out of a head-related surgery or, in some cases, the use of intensive make-up. But most of these cases mean just a temporal denial of service, or the need of a re-enrolment process. In other words, the universality can be considered close to 100 %, much better than other modalities such as fingerprint.

— Uniqueness: Even though there are authors declaring excellent recognition results, it is true that the capability of discriminating among lookalike people, or even twins, is algorithm-dependent, and very few in-depth studies have been done. The traditional claim is that face uniqueness is lower than the one achieved by modalities such as fingerprint and iris.

— Stability: This is by far one of the major challenges of this modality. Stability is weak not only due to natural changes during the life of a human being, but mostly because of cosmetic reasons. Within this kind of impact we can enumerate: plastic surgery, hairdressing, make-up, add-on objects like glasses or piercing, tattoos, etc. Even more, this modality suffers from stability problems during acquisition, including pose, mood, lightning conditions, etc.

— Acquisition simplicity: On the other hand, acquisition is, for the pure technological point of view, extremely easy, as you only need to take a photograph from the subject, preferably when looking in the direction of the camera. It can even be taken at a distance, depending on the zoom and focus capabilities of the camera. But this simplicity has to be achieved once the acquisition conditions are controlled at a certain level, such as lightning conditions, where ambient lightning should not come mainly from the back or one of the sides of the user, but be encouraged to be frontal or ambient-diffused.

— Performance: Before 2010, face recognition was considered as a modality with medium to low performance, in particular in real environments. In the last decade, a huge improvement has been achieved, as can be seen in the latest reports from NIST ([16]). For example, the report from the Face Vendor Recognition Test which started in 2013, showed that for real mugshots, there were algorithms that could identify a person within a database of 160 000 users, in less than half a second, and some of them achieving a false non-identification rate (FNIR) below 2 %.

— User acceptance: This is reasonably high unless the user does not trust who, and for what purpose, their mugshot is taken. Another reason for user rejection is the level of interaction required in several scenarios, where you're forced to look at the camera when this may not be your usual task. With the implementation of face recognition in iPhone X, there have been some users complaining about the system just for the opposite reason: the interaction needed is so low that they are not really aware that they have unlocked the device, or the device gets unlocked even if you only wanted to check the time. But in general terms, users feel comfortable with the modality.

— Resistance to fraudulent use: Within the attacks, the most successful ones are the ones based on obfuscation (i.e. where the user does not want to be identified), but there have been some examples of being able to perform impersonation attacks (i.e. the attacker wants to be identified as another person). Depending on the system, this kind of attack could be as simple as replaying a photo or a video in front of the camera, or needing the manufacturing and make-up of facial masks that could be bought easily on the internet.

— Cost: From the device point of view, the system is costless as a regular camera is just enough. It could be of interest using an infrared camera, in order to detect certain attacks and also compensate lighting conditions. But even in this case the cost is minimal, being only based on the licences to be paid for using the software.

— Maturity: The modality is entering maturity, although there are still many open issues. In particular, it has been implemented in border control, as well as in other access systems.

([16]) National Institute for Standards and Technology, Face Recognition Vendor Test (FRVT) 2013, https://www.nist.gov/itl/iad/image-group/face-recognition-vendor-test-frvt-2013 (accessed 18 June 2019).

4.3.1.6 3D facial recognition

A variation of facial recognition is performing this task but capturing a 3D image of the face of the subject. Several techniques exists to acquire such an image, although there is no compatibility among them. The two mostly known are: (a) the use of multispectral light projection using lines of different colours (and obtaining the 3D information by the deviations of those lines when projected on the face); and (b) the use of several cameras in order to obtain a stereographic effect during acquisition. Then specific algorithms are used (not the same as in 2D Face), and results obtained.

This modality has been under study in several European projects, but there is no major deployment active at this moment. Apple claims that their face recognition is 3D-based, but there is no independent validation of such assessment.

Considering the parameters previously mentioned:

— Universality: The same as in 2D Face

— Uniqueness: Expected to be much better than 2D Face as more data is available.

— Stability: Once again, more or less the same as in 2D Face.

— Acquisition simplicity: The acquisition is a bit more complicated, but depends on how the final system is implemented, as synchronisation on the user interaction with lighting and/or several cameras is requested.

— Performance: There is no independent study. Authors claim that performance rates are much better than for the 2D variant, but there is the need for an independent evaluation to really check this statement and evaluate how much better it is from 2D face recognition.

— User acceptance: A little bit less than for 2D Face as the interaction required by prototypes is a bit larger than the one of commercial 2D Face solutions.

— Resistance to fraudulent use: It is expected to be more robust against attacks as more information is acquired. Some of the 2D Face attacks are not available here (e.g. showing photo or video at the camera), but the use of a mask could make the system fail. If iPhone X really uses 3D face recognition, it is important to note that 1 week after the release, the system has already been successfully attacked ([17]).

— Cost: as it is not yet a product, cost is still high. Anyway, it will always be higher than 2D, as cameras are more complex.

— Maturity: As no major deployments have happened, it is difficult to assess how mature this technology is. But as there are several scientific papers about this modality, we can consider the maturity as medium-low.

4.3.1.7 Iris

Iris pattern is a relatively recent modality, being published by John G. Daugman in 1993. It is based on acquiring an infrared image (i.e. a photograph or a video sequence) of the human eye, and from that, removing all pixels out of the boundary of the iris and the sclera, and inside the boundary of the iris and the pupil. Then that portion of the image is processed using multi-resolution techniques in order to extract features of the texture of the iris (i.e. not about the shape or the colour). Its performance is even higher than the one for fingerprints, presenting some inherent anti-spoofing mechanisms. Unfortunately its cost is too high for most current applications.

This biometric modality makes use of the considerable amount of detail in the coloured part of the visible eye. In the 1990s, Iridian patented the approach and a very powerful comparison and matching algorithm. Since the expiry of the patents, other algorithms have been developed and a number of suppliers offer access control systems.

([17]) Bkav Corporation, How Bkav tricked iPhone X's Face ID with a mask, 2017, https://www.youtube.com/watch?v=i4YQRLQVixM (accessed 18 June 2019).

In normal operation, the eyes are illuminated by near infrared light to ensure that detail from both light and dark coloured irises is captured optimally.

Systems are now available which collect images of either one or both irises at a distance of up to 2 metres. In contrast, the earliest devices required considerable cooperation by the users to position their eyes at exactly the correct distance from the camera.

Considering the parameters previously mentioned:

— Universality: The universality is high, although as in the case of fingerprint, there are some cases where this modality is a challenge. For example, there is a small part of the population with some illnesses of the eye that either impact the iris (e.g. aniridia) or the cornea, not allowing a clear view of the iris from the external part. In those cases where the cameras used do not have dynamic location of face and eyes, then the level of user interaction required may deny the use of the modality to blind people.

— Uniqueness: Even though there is not an in-depth study on the topic, it is sustained that irises present an even higher uniqueness than fingerprints. There have been some tests even including twins, and no two irises were discovered alike. Also, this technology was in place in some Middle East airports for many years, and there has not been any case reported on lack of uniqueness.

— Stability: From the medical point of view, it has been claimed that the iris is a tissue that is fully formed during the first year of life, and remains fully stable during the whole life of the subject, unless a serious injury happens. Even most surgeries related to eyes do not impact iris technology.

— Acquisition simplicity: The acquisition was one of the major drawbacks of this technology. But with current high-end devices, this process has become quite simple, only requiring the user to look to the camera, even while moving. If low-end acquisition systems are used, usability can be compromised for many users.

— Performance: Performance has been reported as one of the best in the world, even under tough conditions. There have been independent open evaluations, such as ICE2005 or ICE2006, both from NIST ([18]), that have shown the modality to achieve over 99 % of identification success rate, when in the database even unfocussed images were used.

— User acceptance: All major deployments have used high-end acquisition devices, and as technology improved the user satisfaction improved. There is a bit a user rejection as some users still think that this technology is using some kind of laser technology, instead of simple infrared photo or video acquisition. Once this is cleared out, it is just a question of how friendly the acquisition system could be for the user. There are even smartphones including this technology for unlocking the phone, which have been accepted by users, although many of them still prefer fingerprint, as requiring a little bit simpler interaction than iris (e.g. not having to look to the phone to unlock it in the case of fingerprint).

— Resistance to fraudulent use: This is one of the major advantages of this technology. Iris acquisition has many features that allow the detection of attacks. The shape of the eye, together with the intrinsic and continuous movement of the pupil, makes it easy to detect if the presented eye is a living object or either a printed image, a synthetic eye or any other kind of spoof. It also can allow the detection of painted contact lenses, and the use of infrared technology also allows the detection of screens presenting a video replay of another iris. In addition, the analysis of the whole context, can detect easily most of the potential attacks. But obviously this is only possible if the system has these mechanisms implemented, and not if the system only use one single photogram to perform the authentication.

([18]) National Institute of Standards and Technology, 'Iris Projects', https://www.nist.gov/programs-projects/iris-projects (accessed 18 June 2019).

— Cost: Unfortunately, the complexity of the acquisition devices makes this modality quite expensive, even though prices have dropped a lot from the early years.

— Maturity: The technology can be considered mature enough, as it has been deployed in some major applications, such as frequent travel border control in some countries (e.g. in the Middle East).

4.3.1.8 Vascular

Vascular biometrics, i.e. acquiring information about the pattern of the veins in a particular part of the body. This is a very recent modality, but its usability, price and performance have made it gain popularity and acceptance. Typically the part of the body used is the hand or a finger, and the image is captured by using infrared photography, which is able to emphasise the image of the superficial veins under human skin. Although further tests should be carried out, the current results obtained by independent tests have shown a performance quite close to fingerprints, with a higher level of universality and usability. Further work should consolidate this modality among the most reliable ones.

Devices have been developed for access control systems using the veins in the hand. In the design patented by Fujitsu, veins beneath the surface of the palm are imaged using infrared illumination. The Hitachi system images the veins of a finger using infrared illumination transmitted through the finger.

Considering the parameters previously mentioned:

— Universality: The universality is considered very high, only being compromised by those people not having the part of the body that it is used for the acquisition (e.g. hand palm or finger). Apart from that, and providing an alternative to these cases, all human beings should be able to use this modality.

— Uniqueness: Without a serious work on this matter, the fact that vein patterns are formed in a random way before birth gives reason for the claim of a uniqueness similar to the one of fingerprint and/or iris.

— Stability: There have not been studies about ageing in this modality, neither about impact of some cardiovascular illnesses in the shape and orientation of the vein patterns. So far there is no proof that will deny a good stability of the biometric trait among humans.

— Acquisition simplicity: The acquisition is somehow simple. It is true that in those cases where no pegs or platforms are used, the user needs a certain period of training to get the optimal position of the hand/finger. But once this is achieved, the acquisition becomes simple and fast enough for most applications.

— Performance: There are very few reports about the performance of this modality. The only independent report was published by the International Biometric Group (2006), which estimated a performance similar to iris recognition although a bit worse.

— User acceptance: The system is perceived by the subjects as simple and with no negative implications. It is even better than hand geometry, as in the case of the palm system by Fujitsu, there is no need to touch a surface with the hand.

— Resistance to fraudulent use: This modality has always been considered as of extreme robustness against spoofing attacks (at least with the commercial systems), as vascular information is internal, and within the acquisition some mechanisms can be applied to detect if the hand is a living sample. But very recently there has been the report of an attack, which has succeeded ([19]), although its viability is highly questioned.

([19]) Cox, J. and Hoppenstedt, M. (2018), 'Hackers Make a Fake Hand to Beat Vein Authentication', *Motherboard*, https://motherboard.vice.com/en_us/article/59v8dk/hackers-fake-hand-vein-authentication-biometrics-chaos-communication-congress (accessed 18 June 2019).

— Cost: The systems are not expensive, being in the same range as medium to low-cost fingerprint systems.

— Maturity: These systems could be considered to be mature, as they have been considered by bank systems in Japan for deployment, and they will be widely used during the forthcoming Olympic Games in Tokyo.

4.3.1.9 ECG

Electrocardiography (ECG) is the process of recording the electrical activity of the heart over a period of time. In order to obtain such activity, a set of electrodes are placed over the skin of the user in specific parts of the body. When considering the use of ECG for biometrics, the number of electrodes is highly reduced, going from the typical 10 or 12 electrodes to just 2 or 3. By changing the number of electrodes, as well as their position, the signal captured changes completely.

The use of ECG as a biometric modality is in a very premature state. Some work has been carried out showing its viability as having, at least, a low-medium performance. But in addition to the capability of recognising a human being, the signal itself provides three interesting benefits. The first is that it provides information from a living subject (whose authenticity can be checked using the discriminative power of the information). The second is that it can provide a means for continuous authentication of the user, checking his own activity and adapting the decision to the current context. Third, as both wrists will be needed, there should be an action by the user, accepting the process.

In addition, some preliminary works have been undertaken to detect heart rate remotely (Amerland et al., 2015; Verkruysse et al., 2008). Further studies should be carried out to enable an analysis of whether these methods could also be used for estimating the ECG and not only the heart rate.

Considering the parameters previously mentioned:

— Universality: Any human being who is alive shall present an ECG, so universality is considered to be 100 %.

— Uniqueness: There is no clear study about the uniqueness of this biometric modality. There are a few comprehensive works that point out that ECG may be considered of medium-high accuracy (Agrafioti, 2012), achieving EERs below 10 %, even with databases of over 100 users (Kim and Park, 2017).

— Stability: Once again there are no comprehensive studies about the stability, and in particular how illnesses such as arrhythmias may impact performance. Also, long-term evolution of ECG is not well known.

— Acquisition simplicity: Acquisition may be done by simple wristbands, requiring the cooperation of the user in order to complete the acquisition (Kim and Lee, 2018). A few seconds (e.g. 5 to 6 seconds) are needed to acquire a signal good enough to perform recognition.

— Performance: Not many studies have shown a comprehensive study of its performance using databases large enough for both inter-class and intra-class. As shown above, performance is considered to be of medium level, reaching EERs below 10 %.

— User acceptance: There have not been any major deployments, except of a bank ([20]), but no report on the user acceptance has been provided. It is expected to be high, as people are now used to wearing smartbands. But it has to be assured that one single smartband provides all the functionalities the user demands.

([20]) Kollewe, J., 'Halifax trials heartbeat ID technology for online banking', *The Guardian*, 13 March 2015, https://www.theguardian.com/technology/2015/mar/13/halifax-trials-heartbeat-id-technology-for-online-banking (accessed 18 June 2019).

— Resistance to fraudulent use: ECG is an internal feature and difficult to acquire without cooperation. Up to now no kind of attack has been known. Futhermore, ECG has been proposed to be used in order to provide a presentation attack detection mechanism to other biometric modalities (Sanchez-Reillo et al., 2018).

— Cost: There is not data at this moment, but it is expected to be low, as bands are not expected to cost much. It can be considered as of the same cost as vascular or medium-low fingerprint.

— Maturity: This modality is still very immature. No major deployments have been done, except for the bank previously mentioned (but no results have been provided).

4.3.1.10 EEG

Electroencephalogram (EEG) is another biological signal of the same nature as ECG, but with less powerful signal levels and requiring a more sophisticated acquisition system. It is based on obtaining signals from the human brain and extracting from them parameters that could serve to discriminate among human beings. It is a modality currently under scientific study (Das et al., 2018), and is considered even more immature than ECG.

Considering the parameters previously mentioned:

— Universality: As in the case of ECG.

— Uniqueness: Is in the same situation as ECG.

— Stability: Also no studies have been done considering the long-term stability of the EEG signal, nor how illnesses impact on EEG signals.

— Acquisition simplicity: Acquisition is quite complex and the person is required to wear a kind of bonnet to get the signals.

— Performance: Not a clear report on performance rates has been found that is based on relatively large databases.

— User acceptance: There is no data in this respect, but with the need of wearing the abovementioned bonnet, might be quite low.

— Resistance to fraudulent use: This is equivalent to ECG.

— Cost: The bonnet might be of a considerable cost, and nowadays those bonnets are mainly prototypes and not for daily use.

— Maturity: The modality is even more immature than ECG.

4.3.2 Behavioural modalities

4.3.2.1 Voice

Speaker recognition is a modality that has been scientifically studied for more than 3 decades now. There are a huge number of methods to extract features and to compare features from samples. Some of these methods depend on the text corresponding to the utterance provided (text-dependent approaches), while some others are considered to be text-independent (i.e. the speaker is allowed to say whatever sentence he/she likes). Speaker recognition systems, in order to avoid replay attacks, even using text-dependent approaches, have a parallel process of recognising the text uttered by the user. This is done to check if the text pronounced is corresponding to a certain text claim requested by the system. Obviously, this claimed text changes every time the system is used to avoid attacks. Unfortunately, parameters such as age, stress, health conditions, surrounding noise, etc. are not yet isolated from the extracted features. This drawback provides one of the most important challenges of this technology, as the stability of the features is quite low.

Considering the parameters previously mentioned:

— Universality: The mixture between physiological and behavioural creates a challenge in considering its universality. If the modality is language-dependent or mother tongue dependent, the universality can be considered as very low. If this is not the case, then universality is high, although there are people with no possibility to speak. Also some illnesses can compromise the temporal use of this modality for some users.

— Uniqueness: There are authors that consider that uniqueness cannot be achieved as voices can be simulated by mimicry. But other authors defend the idea that mimicry does not really get into the same kind of parameters as the genuine voice. Out of this discussion, there are no comprehensive studies about this, and due to lack of further studies and open independent evaluations, no real answer can be provided.

— Stability: This is one of the major drawbacks of this modality, as there are plenty of factors that impact the acquired signal, including: ageing, illnesses, background noise, mood, tiredness, text spoken, etc. All these create serious problems in the stability of the signals for this modality.

— Acquisition simplicity: Acquisition is technically very simple, as a simple microphone can be used for such task. The challenges in acquisition are how to handle the context associated with the acquisition, such as the orientation between the speaker and the microphone, as well as how to deal with the background noise.

— Performance: Although in recent years it has been claimed that performance has been increased, this has not been double-checked by independent studies, except for the one that the International Biometric Group (2006) carried out, which showed reasonable rates, although not outstanding.

— User acceptance: Users tend to accept this modality easily if it is deployed in a scenario where speaking is intrinsic, i.e. within a telephone service. But in any other case (e.g. physical access control systems), users tend to reject the system due to lack of natural interaction.

— Resistance to fraudulent use: There are plenty of attacks available, including the recording of the user voice. Recent works are trying to detect if the sound captured is being uttered from a physical person or from a recording, as to avoid this kind of attacks. In some cases, users are requested to say a certain sentence chosen randomly, checking if the utterance also corresponds to such a sentence, denying the possibility of recordings. In such cases voice synthesisers can be used to attack the system. Very few studies are supporting these claims with comprehensive numbers.

— Cost: The cost is very low or even non-existent, in particular if the modality is going to be used within a context where the recording of the voice is already in place (e.g. a telephone).

— Maturity: The technology is mature, although the lack of performance is reducing the existence of major deployments.

4.3.2.2 Handwritten signature

From the so-called behavioural modalities in biometrics, handwritten signature is gaining much attention recently. One of the reasons for such interest is the deployment of devices that, intrinsically, can capture handwritten data, such as touchscreens. But such proliferation of the technology may not necessarily mean an improvement in the performance, although it is, for sure, a magnificent opportunity to popularise this biometric modality. Laptop computers, tablets and smartphones are currently in the hands of any kind of user. Furthermore, companies have seen in these new technologies the opportunity to avoid paper handling in actions such as credit card payments or parcel delivery, saving huge amount of money in expenses. But some clarity shall be provided as well as focus on further research to be done in order to improve the current state of the art.

The first thing to clarify is that under the term of handwritten signature biometrics, there are two different modalities involved: (a) static signature (also called off-line signature) which is simply based on the graph generated after signing, such as the information obtained when scanning a page with a signature already written; (b) dynamic signature (also called on-line signature) which is based on the set of temporal signals generated while the signature is being written, such as horizontal and vertical movements, pressure, etc. Each of these modalities has its own characteristics and challenges. Static signature is currently the most deployed one (used in card payments and couriers) but not really used as a biometric modality, but only as a means to save on paper handling (i.e. no comparison is made when the signature is performed as the only interest is to store the graph with the acceptance document). Several studies have demonstrated that, when used as a biometric modality, static signature presents low performance and little robustness against fraud, unless taken under the analysis of a human expert. Dynamic signature has shown to be a much better solution for automatic verification, including larger robustness against forgeries when being used by a machine.

Considering the parameters previously mentioned:

— Universality: Depending on the context this modality is applied, the universality can go from high to medium-high. Not everybody knows how to write, and they do not sign in a regular manner (considering regular in a very relaxed way to reach a minimum of one signature every 2 months). If this is not the case, then this modality is not recommended.

— Uniqueness: The lack of uniqueness of handwriting signature has always been claimed, as it is 'simple' to forge a signature. If the data used are the dynamic features this is not the case. But even in that case uniqueness cannot be considered high enough to reach the one achieved by many physiological modalities.

— Stability: Also stability has been considered to be very low, as we can even notice that our own signature differs with time and with condition. But if instead of paying attention to the graph, we consider the dynamics, and relationships among those dynamic features, the stability is much more acceptable. This could be partially proved in a usability and interoperability independent evaluation published in 2013 (Blanco-Gonzalo et al., 2014).

— Acquisition simplicity: Nowadays, acquisition of handwritten signatures is quite simple as the use of touchscreens allows even to capture the data signing with the finger, or using a stylus. The abovementioned publication also showed that in dynamic handwritten signature verification it makes no difference which signature device is used, provided that when signing with the finger the user has briefly trained before to get the new feeling.

— Performance: Also, in recent years some publications have shown that when this modality is used with genuine signatures, EERs below 4 % are reachable (the previous publication also shows this). The case of forgeries is commented on in the resistance to fraudulent use.

— User acceptance: The acceptance of this technology is fully dependent on the application. If the application conceives the need of the user to sign, then this application is fully accepted. If not, due to the time needed to sign and therefore the excess of interaction, this modality is not welcomed.

— Resistance to fraudulent use: One of the major criticisms of this modality is the fact that forgeries are viable and therefore it is expected to be non-resistant to presentation attacks. But a recent work in this area (Sanchez-Reillo et al., 2017) has shown that some forgery detection mechanisms can be added to the algorithm to deny these attacks with a high level of success, leaving the percentage of non-detected forgeries below 3 %, even when attackers have a very high knowledge of the signature to be forged.

— Cost: For desktop applications, a simple sign pad can be used with a cost similar to medium-range fingerprint sensors. For mobile applications, the touchscreen of the smartphone can be used for this task. Therefore the cost can be considered very low.

— Maturity: The modality can be considered in its mature status, as some deployments have already taken place, in particular in health and insurance services, as well as banks and courier services.

4.3.2.3 Gait (Video)

Gait analysis, that is, recognising people by the way they walk, is based on the determination of the gait 'signature' of people using video footage usually in real time. This 'signature' is not unequivocally unique and cannot be used as sole identification source. Thus, the use of gait analysis is always a complement for other biometric identification methods.

Gait analysis can be done in low-quality footage from a distance and can be determined even if there are temporal occlusions (e.g. other people passing by). On the other hand, many factors like the footwear, the terrain, training, possible injuries, fatigue or just the passing of time (people getting older) can modify the signature and hamper the identification. Gait identification is not limited to walking, in general it can refer to any cyclic coordinated movement related with human locomotion. These movements can include walking, jogging, running and even climbing stairs.

Detection can be done in many different ways; subtraction of background, determination of the 'pose' (skeleton and joins determination), extraction of the silhouette, projection of the movement and others. As signature determination methods, there are many used in different approaches, like gait cadence, oscillation of the body or stride length combined with others that are static like people's height, the longitude of body limbs or the distance between body parts.

Considering the parameters previously mentioned:

— Universality: The universality is compromised by those people with motor disabilities, which will not be able to use this system. Also, temporal disabilities can deny the use of this modality (e.g. after getting a leg broken).

— Uniqueness: There are no studies on the level of uniqueness of the way people walk. There are even professionals, such as chiropodist or physiotherapists that consider that the recognition of the people by the way the walk is not possible, as by only changing the kind of shoe being worn the way a person walk changes dramatically. Trying to find a mid-position, let's consider that for particular scenarios and conditions, this modality can be used.

— Stability: This modality suffers as many stability problems as the ones for face: shoes, trousers/dress/skirt, objects worn, illnesses, injuries, tiredness, etc. So stability is not considered to be high enough.

— Acquisition simplicity: From the point of view of the user, it is not too complicated, although in most of the current systems there is the need that the user walks in a certain direction within a determined path. From the systems point of view, the installation is not simple, as the location of the cameras, the orientation, the indication of the path, etc. should be done with care.

— Performance: There is not an independent evaluation using diverse and large databases, so no real claim can be made about the performance of this biometric modality.

— User acceptance: As no major deployment has been started, there is no real information about user acceptance.

— Resistance to fraudulent use: Up to now, there is no information of how to impersonate a person using this biometric modality. But it is expected to be quite

simple to obfuscate your own identity, by changing the way you walk using particular dressing that will impact on your way of walking.

— Cost: Cost depends on the number of cameras to be used, as well as their location and movement. That will also depend on the length of the path to be followed, as well as the environment where the system is installed.

— Maturity: The modality cannot be considered mature enough.

4.3.2.4 Gait (accelerometer-based)

In this case, the gait is collected via the use of accelerometers attached to the body. These accelerometers can be worn in any part of the body with the waist, the hip and the legs being used for different studies.

Key advantages of this method are that it is unobtrusive and can be continuous. For example, an accelerometer can be easily added to mobile devices. As in gait recognition using video, this method cannot be used as the sole determination of identification.

Considering the parameters previously mentioned:

— Universality: Same as Gait (video)

— Uniqueness: Same as Gait (video)

— Stability: Same as Gait (video)

— Acquisition simplicity: It needs the cooperation of the user, as he has to wear a device that is able to acquire the signals. The location and orientation of the device has not been agreed among authors. Depending on this, the acquisition could become more or less simple.

— Performance: Same as Gait (video)

— User acceptance: Same as Gait (video). But somehow we can determine that not much interest has been shown in this modality. This has been included in the Android operating systems for several years now, and almost no user has decided to activate it.

— Resistance to fraudulent use: Same as Gait (video).

— Cost: if the device could be the users' smartphones, then the cost is non-existent. If not, the additional device may be of low cost if only a battery and a gyroscope is needed.

— Maturity: Same as Gait (video).

4.3.2.5 Keystroke dynamics

This biometric modality is based on analysing the cadence of the user when typing in a keyboard. Recently there is also the same kind of study, but instead of using a keyboard, using the virtual keyboard in the touchscreen of a smartphone or tablet.

Considering the parameters previously mentioned:

— Universality: This modality is expected to provide reasonable results only with those users who type frequently. Universality is therefore limited.

— Uniqueness: There are no studies on the uniqueness of this behavioural biometric modality.

— Stability: Also, there is not much information about stability. Open questions are: does the activity being carried out impact on the signal? Tiredness may impact the performance? Are there injuries which can compromise temporally or permanently this modality? etc.

— Acquisition simplicity: If the user types frequently, the acquisition is very simple.

— Performance: No independent evaluations are available about this modality, but the expectation is that the performance to be achieved could be worse than handwritten signature.

— User acceptance: There are also no reports on this, but initially, if the text to be typed is not fixed, this modality could be comfortable for computer users to keep the computer logged in while working.

— Resistance to fraudulent use: There are no studies about this.

— Cost: The system is considered to be costless, as no acquisition device needed is the same gadget owned by the user.

— Maturity: This modality is in a very premature status.

4.3.3 Soft biometrics

Soft biometrics refers to those physical, behavioural or adhered human characteristics that can be used to allow a preliminary classification of human beings, or even tracking a previously detected human being. By their nature, this technology is not expected to provide high performance, or even focus much on the uniqueness of the biometric property, but a piece of information that can be used to discard other users to be confused with the individual that is being targeted for recognition.

There are plenty of features that can be considered within this category of soft biometrics, and can be classified in the following manner:

— Physiological: such as height, weight, skin colour, hair colour, eye colour, presence of beard, presence of moustache, perceived age, perceived gender, face thermal map, body thermal map, etc.

— Behavioural and/or context: movement tracking, smartphone tracking, etc. Some authors consider gait or keystroke dynamics also as soft biometrics.

— Adhered: clothes being worn, tattoos, accessories, etc.

4.3.4 Multimodal approaches

Multimodal is the use of the combination of multiple biometric methods for identifying people. The combination of methods improves the identification compensating the limitations of current technologies.

The limitations of the biometric technologies are:

— Physical limitations of people: some people cannot physically provide one or many biometrical credentials temporally or permanently due to disabilities, accidents or temporal illness. This limitation is related to the universality of the modality.

— Variations from enrolled reference: The data used for authentication (e.g. for face recognition) can be different from the data obtained during enrolment for many possible reasons. This limitation is related to the stability of the modality.

— Noise in data: Voice can be temporal or permanently altered, gait can change due to terrain, etc.; on the other hand, the sensors acquiring the information can be in a poor state. This limitation is related to the ease of acquisition.

— Environment: The environment of capture can modify the result of identification. As a typical example, light conditions or angle change face recognition. Again, this limitation is related to the ease of acquisition.

— Attacks directed to fool the identification: There are many attacks that can alter individual biometrical identification methods. For example, face morphing can be used to fool face recognition. This limitation is related to the robustness against attacks.

The use of one sole biometric method makes these limitations difficult to circumvent. Multimodal approach makes the identification more reliable. Additional benefits of multimodal approach are:

- Improved accuracy;
- Elimination or mitigation of the influence of data noise and variations on data;
- Diminution of limitations due to environmental factors;
- Avoidance of physical limitations;
- Protection against attacks.

4.4 Biometric modalities for EWZ

When trying to apply biometrics into EWZ's, one of the first parameters to consider is the distance at which a person can be identified and, at the same time, the level of interaction required from that person to achieve recognition. In this respect, we can analyse the biometric modalities under the following categories:

- Recognition at long distance;
- Recognition in the vicinity;
- Recognition in proximity;
- Recognition with the user at a specified spot.

The following subsections provide recommendations for each of these categories.

4.4.1 Long-range recognition

If we consider long range as something beyond 50 metres, there are few modalities that could get some valid information. This kind of recognition could be used for either a very-early warning or for tracking an initially recognised person. This kind of recognition can only be achieved by the use of long-distance cameras, or other suitable information.

The recommended modalities are:

- Most of physiological soft biometrics such as height, perceived age, perceived gender, presence of face hair, body shape, etc.;
- Some behavioural soft biometrics such as movement tracking, smartphone tracking;
- Some adhered soft biometrics such as clothing;
- Gait (video);
- 2D Face;
- Voice recognition;
- If we consider a cooperative scenario, where the user is the one demanding to be identified, and providing a real-time network connection between the subject being recognised, and the recognition system:
- Gait (accelerometer);
- ECG.

4.4.2 Medium-range recognition

Considering medium range to be between 5 and 50 metres, the modalities to be used, in addition to those mentioned for long-distance, are those that can be acquired with little, or even no user interaction, but which require more details or a controlled scenario.

The recommended modalities are (in addition to those of long-distance):

— 3D Face;

— Adhere soft biometrics such as tattoos in visible areas.

4.4.3 Short-range recognition

Proximity can be defined as distance shorter than 5 metres, but not requiring excessive interaction from the user (no need to stop to be identified).

The recommended modalities are (in addition to the previous ones):

— Contactless fingerprint on the move;

— Iris on the move;

— Vascular on the move.

4.4.4 Recognition with the user at a specified spot

In this category fall all kind of biometric modalities. This could be considered, for example, as a 2nd line of verification in a CI. In this scenario, the user can be requested to fully interact with all kind of sensors, taking all needed time for performing the recognition. But this scenario is outside the concept of an early warning zone, being closer to scenarios such as automatic border control.

5 The standardisation challenge for EWZ

5.1 Introduction

Continuing improvements in video surveillance, biometric technologies, and increasing use of artificial intelligence (AI) mean that it is now possible to automatically monitor sensitive areas with little human intervention and to automatically trigger alerts when abnormal or suspicious behaviour is detected.

It is widely recognised that standards play a major role in enabling interoperability, uniform quality in provision of services, reduction in costs, future-proofing, and wider still, in enabling the EU security industry to be more competitive globally. However, the development and adoption of standards in the security domain has been poor, and the problem is exacerbated by the large number of current vendors of video surveillance systems (VSS) which are at the heart of most EWZ systems.

The purpose of this chapter is to provide an overview of standards relevant to the procurement, implementation and use of technologies for extended warning zones. This includes standards for video surveillance systems and video analytics software, biometric technologies, both for the identification of 'trusted' subjects (e.g. employees and security personnel with legitimate access to the site) and 'untrusted' subjects who may be either unknown or may be held on a watchlist of people believed to pose a potential threat).

The chapter highlights the need for standards at different levels of interoperability, a universally agreed set of performance evaluation benchmarking metrics for video analytics and video-based biometric systems, and European level certification for surveillance systems and their components.

5.2 Overview

Standards are vital for interoperability of technologies used by law enforcement and other authorities. One of the first standards in this space was the 1986 ANSI NIST ITL standard for the exchange of fingerprint minutiae data, designed to enable local and state fingerprint systems to exchange data with the FBI's Automatic Fingerprint Identification System (AFIS). Support for finger image data was added soon after, quickly becoming the de facto international standard for exchanging police fingerprint records (10 prints and latent images). Subsequent versions of the ANSI NIST ITL standard extended the scope to include other modalities — face, palm prints, voice, DNA and dental records. While it was originally developed to support applications for law enforcement, the standard has been adopted by immigration agencies as well as the military, thereby enabling data exchange between these parties (in some cases internationally).

In 2002, ISO established a biometrics standards subcommittee (SC37). A major driver for this was the introduction of e-Passports that could hold biometric data, such as a facial image, on a chip. The need for international interoperability between chipped identity documents and document readers, and the opportunity to introduce biometric technology both securely on the chipped documents and at the border to automatically verify the identity of the document holder, required new international standards for capturing biometrics and storing data, certifying equipment and assessing the performance of matching algorithms, all of which are essential to assure and maintain confidence in the accuracy and security of automated border controls.

ISO SC37 has now published a large number of standards on all aspects of biometrics, with many more currently in development. At the same time CEN TC224 (Personal identification, electronic signature and cards and their related systems and operations) has also been active in developing European standards for biometrics, in particular the use of biometrics in e-Visas, and ABC gates and mobile devices used by border officials. Those standards that are relevant to EWZ will be considered in more detail later in this document.

In contrast, the security market, and in particularly video surveillance, has had no such common international driver and this has resulted in a plethora of divergent national standards and practices. This was highlighted in an earlier ERNCIP report by the Video Surveillance Thematic Group (Ferryman, 2016). For completeness, parts of that report will be reproduced here, but for a more comprehensive examination of the standards landscape for video surveillance systems the reader is encouraged to download that original report.

Following a number of studies highlighting the need for further standardisation, in 2011 the European Commission issued a mandate (M/487) to obtain a detailed overview of existing international, European and national standards in the security area.

The work was allocated to CEN/TC 391 'Societal and Citizen Security' and a study was undertaken to analyse the current security standardisation landscape and the security end-users requirements of standards. This included border security and ABC gates (and thus biometrics) but did not consider video surveillance or video analytics.

As a result, while low-level general standards (e.g. MPEG) are well established for universal use, agreement on standardisation in video surveillance formats as used by video surveillance systems is lacking. The problem becomes even more severe when considering metadata generated by video analytic methods such as tracking and event/behavioural analysis, the high image quality requirements for the biometric technologies such as face recognition and the need to benchmark the performance of such video surveillance systems.

5.3 Standardisation activities and roadmap

The following sections detail standard development organisations relevant to EWZ, and an overview of their work.

5.3.1 Industry-led interface standards organisations

5.3.1.1 Open Network Video Interface Forum

The Open Network Video Interface Forum (ONVIF) is an established open industry forum and non-profit organisation, founded in 2008 by Axis, Bosch and Sony (currently over 500 member organisations), for the development of a global standard for the interface of IP-based physical security products. The aim of ONVIF is to ensure interoperability between products regardless of manufacturer by creating an open standard for communication between IP-based physical security devices (e.g. surveillance cameras). The ONVIF specification defines a common protocol for the exchange of information between network video devices including automatic device discovery, video streaming and intelligence metadata. The focus of ONVIF is on real-time streaming of data and metadata. As of February 2015, ONVIF has three specialist profiles (Profile S for streaming video; Profile G for recording and storage; Profile C for physical access control) and Release Candidates Profile A, for access control configuration, and Profile Q, for easy installation and advanced security features), but none dedicated to video analytics.

5.3.1.2 Physical Security Interoperability Alliance

The Physical Security Interoperability Alliance (PSIA), founded in February 2008 and incorporated in March 2009, is represented by a global consortium of over 65 physical security manufacturers and integrators including Honeywell, Verint, IBM, Cisco and GE, focused on promoting interoperability of IP-enabled devices. Compared to ONVIF, PSIA have taken a more holistic and systems-based approach to standardisation, with five active working groups (SGs) including one on video analytics, detailed below. In 2010, PSIA released a recording and content management specification describing standards for recording, managing, searching, describing, and streaming multimedia information over IP networks. The specification includes XML Schema definitions and XML examples to aid development of standards-based products.

In September 2010 the PSIA Working Group on Video Analytics released the Video Analytics 1.0 Specification based on ObjectVideo's OV Ready protocol. The main features of the open specification are:

- Enables video analytics to more easily and consistently integrate with video management systems and physical security software platforms through standard interfaces;
- Defines a standard way to share video analytics capabilities supported by an intelligent device and output, receive, store and use various video analytic events;
- Open interface addresses event output including security alerts, counting events and analytics system health messages. The interface also supports the streaming of object metadata output, which includes foundational analytic output regarding all objects tracked by the analytics, including object classification, bounding box data and velocities.

The scope for the initial release of the specification focuses entirely on video analytics capabilities discovery and analytic data output. Video analytic capabilities discovery will include standard configuration data exchange to enable any analytic device to communicate to another device or application its basic analytic capabilities at the device level and the video channel level (for multi-channel devices). This includes information such as the PSIA VAS version number supported, analytic vendor information (name, software version number, etc.), event types and mechanisms supported, and other supported configurations. From an analytic output perspective, the v1.0 Specification includes the definition of multiple types of analytic events, including alerts and counts, as well as video analytics metadata output.

In February 2015, PSIA released an area control specification, which specifies the communication into access control and intrusion products, making them interoperable with the overall security system.

5.3.2 International standards organisations — Technical committees and working groups

5.3.2.1 ISO IEC JTC 1 — Information Technology

JTC 1 is the standards development environment where experts come together to develop worldwide information and communication technology (ICT) standards for business and consumer applications. JTC 1 also provides the standards approval environment for integrating diverse and complex ICT technologies.

JTC 1 consists of a number of sub committees of which the following are particularly relevant to EWZ as their scope includes biometrics and identity-related technologies.

5.3.2.1.1 SC17 — Information Technology: Cards and Security Devices for Personal Identification

The work of SC17 currently consists of:

- Identification and related documents,
- Cards,
- Security devices and tokens,
- Interfaces associated with their use in inter-industry applications and international interchange.

The work of SC17 includes developing standards for e-Passports, visas and ISO compliant driving licences. More recently SC17 has started looking at licences for UAVs and their operators through the development of a new standard, ISO IEC AWI 22460-ISO License and Drone Identity Module for Drone (Ultra Light Vehicle or Unmanned aircraft system).

At the smart card level, SC17 defines security mechanisms to be used within them, such as secure messaging or the way that secret keys have to be handled by the operating system. ISO/IEC 7816-4 and ISO/IEC 7816-8 provide such specifications. In terms of biometrics, SC17 defines the way such data has to be handled and coded in ISO/IEC 7816-11. In addition, on-card biometric comparison is specified in ISO/IEC 24787, and Biometric System-on-Card in ISO/IEC 17839.

5.3.2.1.2 SC27 — Information Technology: Security Techniques

SC27 is concerned with the development of standards for the protection of information and ICT. This includes generic methods, techniques and guidelines to address both security and privacy aspects, such as:

— Security requirements capture methodology;

— Management of information and ICT security; in particular information security management systems, security processes, and security controls and services;

— Cryptographic and other security mechanisms, including but not limited to mechanisms for protecting the accountability, availability, integrity and confidentiality of information;

— Security management support documentation including terminology, guidelines as well as procedures for the registration of security components;

— Security aspects of identity management, biometrics and privacy;

— Conformance assessment, accreditation and auditing requirements in the area of information security management systems;

— Security evaluation criteria and methodology.

Standards published by SC27 include several on digital forensics, including the capture and investigation of digital evidence.

SC27 covers the security and privacy in all information technology fields, but related to biometrics, the major works carried out are:

ISO/IEC 24761 on Access Conditions for Biometrics (ACBio). This International Standard specifies the way that security mechanisms are to be used, and how information is to be coded into the SB.

ISO/IEC 24745 on Biometric Information Protection, which specifies the way biometric information can be used to achieve cancellable biometric references, i.e. what is also known in the industry as 'biometric template protection'.

SC27 engages in active liaison and collaboration with appropriate bodies (including SC17 and SC37) to ensure the proper development and application of SC27 standards and technical reports in relevant areas

5.3.2.1.3 SC37 — Information Technology: Biometrics

ISO SC37 was established in 2002 as a result of rapid expansion in the number of vendors incorporating biometrics into their products and increasing use of the technology by law enforcement and immigration. In particular, the introduction of e-Passports that could hold biometric data such as a facial image on a chip and the need for international interoperability between chipped identity documents and document readers meant that there was an urgent need for international standards in this space.

ISO SC37 has now published a large number of standards on all aspects of biometrics, with many more currently in development.

ISO SC37 consists of six working groups focusing on different aspects of biometrics:

— JTC 1/SC 37/WG 1 Harmonised biometric vocabulary

— JTC 1/SC 37/WG 2 Biometric technical interfaces

— JTC 1/SC 37/WG 3 Biometric data interchange formats

— JTC 1/SC 37/WG 4 Technical implementation of biometric systems

— JTC 1/SC 37/WG 5 Biometric testing and reporting

— JTC 1/SC 37/WG 6 Cross-jurisdictional and societal aspects of biometrics

Details of individual SC37 standards can be found later in this chapter, but projects of direct relevance to EWZ include the following:

5.3.2.1.4 Data formats

The ISO/IEC 19794 series of International Standards provide interoperable ways to code biometric data, depending on the modality. This multipart standard provides a framework to be applied to all parts, some data formats for raw sample data (e.g. sample images), and some others for processed sample data (e.g. fingerprint minutiae). This family of standards has currently two different generations defined, that are both still accepted. The first generation of standards were published in 2005-2007, with second generation standards appearing from 2011 onwards. In both cases, the ISO/IEC 19794 is a multipart standard with the following structure:

— Part 1 provides a general framework to be applied to all the other parts. It defines the general structure for the biometric records and the common elements of such structure. It indicates that each biometric information record (BIR) is to be composed of a general header that introduces the information to be followed, and one or more representations (i.e. biometric samples), which are structured into a representation header and the representation data. Part 1 defines those common elements of each of the headers.

— Parts 2-n provide the information about those extra elements to be added to the different headers, plus the way the representation data are to be coded. This is done for each of the modalities defined (e.g. Part 2: finger minutiae, Part 4: finger image or Part 5: face image)

At time of writing this report, a new generation of data formats (the 39794-x series) is currently being developed by SC37 in response to requests from ICAO. A key difference is that these standards will add the ability to store data in ASN.1 format, in addition to the existing formats supported by the 19794 series.

ISO/IEC JTC1 SC37 has also defined a meta-structure called CBEFF (i.e. ISO/IEC 19785 series of standards), that allows:

— the coding of biometric information from more than a single user;

— the coding of biometric information from more than one modality; and

— protecting biometric data by using security mechanisms that may cipher and authenticate the data included into the record.

A CBEFF record is composed of a:

— header that provides an introduction to the information embedded into the record;

— the biometric data, which can be a BIR as defined in ISO/IEC 19794[11]; and

— an optional security block (SB) that embeds that data needed for protecting the biometric information.

CBEFF also allows the existence of a hierarchical approach that is able to embed multiple simple CBEFF records in what is called a complex CBEFF record.

5.3.2.1.5 Security mechanisms

Under GDPR, biometric data is classed as sensitive personal data, and protection of such data is required. As already mentioned, CBEFF (i.e. ISO/IEC 19785) defines a security block (SB) to hold information for protecting the biometric data (e.g. cryptograms that

will provide integrity and authentication mechanisms). But in order to provide full interoperability the international standards and reports defined within ISO/IEC JTC1/SC27 also have to be considered.

In addition, SC37 has two projects related to security in biometrics. These are ISO/IEC TR 29156 which considers requirements for security and usability in biometrics and ISO/IEC 30107 on presentation attack detection. These projects present an excellent complement to the work being done in SC27.

5.3.2.1.6 Application development

Developing an application involving biometrics usually needs the integration of several modules. In order to ease that integration, the use of standardised application program interfaces (APIs) is recommended. Biometric applications and modules may be developed using BioAPI, which is specified in the multipart standard ISO/IEC 19784. This API is defined in ANSI C, which may not be suitable for the development of some projects. In case an object-oriented approach is needed, SC37 also defined Object Oriented BioAPI in the family of standards ISO/IEC 30106, including an abstract definition in UML, plus implementations in Java, C# and C++.

If the application is expected to be implemented using a service-oriented architecture (SOA), then ISO/IEC 30108 becomes relevant as it defines BIAS (Biometric Identity Assurance Services).

When the application is intended to be developed under low-cost, low-performance devices, such as embedded systems, a simplified version of BioAPI is defined in ISO/IEC 29164 called Embedded BioAPI.

5.3.2.1.7 Application profiles

There are several standards and technical reports published, that should be a reference for a system designer and/or developer, when defining certain applications. This is the case as those standards developed under the umbrella of ISO/IEC JTC1/SC37 WG4 and WG6.

5.3.2.1.8 Technology evaluation

As already mentioned above, the evaluation of biometrics is also standardised. ISO/IEC JTC1/SC37 has a whole WG for developing standards and reports dealing with the evaluation of biometrics (WG5), and among all different projects carried out in such WG, the ISO/IEC 19795 multipart standard, which defines the principles for the evaluation of biometrics, plus some specific application of those principles to certain scenarios, is of major importance.

In order to evaluate the security level achieved with the developed solution, Common Criteria is the major reference. The works in Common Criteria are subsequently standardised under ISO/IEC 15408. Dealing with biometrics, ISO/IEC JTC1/SC27 has developed the ISO/IEC 19792 standard that specifies a methodology for evaluating security in biometric systems.

5.3.2.2 AFNOR Group, ISO TC223 (Societal Security) and ISO TC 292 (Security and Resilience)

AFNOR is an international group composed of an association and subsidiaries and with the general aim to serve the general interest and economic development of organisations. The Security forum of AFNOR (the French branch of ISO TC223 dedicated to public safety) brings together all actors in the field of security including infrastructure and state services.

In November 2008, AFNOR made a proposal to ISO to set up an international working group with the aim of defining minimum conditions for interoperability needed to exploit

videos from different sources as directly as possible. Such a shared understanding of video content would rely on existing efforts/norms, including:

- Video in general moving picture experts group: MPEG4, H264 of ISO IEC JTC 1 SC29;
- Digital TV: Society of Motion Picture and Television Engineers (SMPTE);
- North Atlantic Treaty Organisation (NATO): interoperability mechanisms for animated images STANdardization Agreement (STANAG 4609);
- Format for video content compression with quality required for exploitation in forensic police work, with preferred profiles, based on MPEG4 H264 from ISO CEI JTC SC29;
- Minimum list of data describing the conditions of capture (i.e. metadata) for recording time and date of sequence capture (as well as camera field of view, zoom, GPS coordinates, etc.);
- Synchronisation of various elements captured at the same time (video, audio, metadata, alarms), with a recommended solution of ISO/CEI23000-10;
- Format or transfer protocol enabling person exploiting videos to be aware of what form the content will be sent to them in;
- Integration of constraints relating to security and authentication of content that is evidential in court of law.

The project resulted in the standard ISO 22311 (Video Surveillance, Export Interoperability) being published in October 2013.

Subsequently, ISO/TC 292 Technical Committee on 'Security and Resilience' was established on 1 January and has since taken over responsibility for ISO 22311. It works with standardisation in the field of security to enhance the safety and resilience of society.

ISO/TC 292 is responsible for wide range of standards and other documents including on 'business continuity management', 'emergency management', 'community resilience', 'authenticity, integrity and trust for products and documents', and 'protective security'. The committee is responsible for more than 20 published International Standards. Six working groups have been set up to conduct the work.

5.3.2.3 CEN/TC391 — Societal and Citizen Security

The main objective of European Technical Committee CEN/TC 391 (Societal and Citizen Security) is to elaborate a family of European standards, standard-like documents (e.g. procedures, guidelines, best practices, minimal codes of practice and similar recommendations) in the Societal and Citizen Security sector including aspects of prevention, response, mitigation, continuity and recovery before, during and after a destabilising or disruptive event. In particular, it was planned that a minimum format standard for security events will be developed within the scope of EC mandate M487 of CEN/TC 391.

5.3.2.4 ISO TC 262 — Risk Management

TC 262 is concerned with standardisation in the field of risk management. Risks affecting organisations can have consequences in terms of economic performance and professional reputation, as well as environmental, safety and societal outcomes.

A key standard produced by this committee is ISO 31000 which 57 national standards organisations have to date adopted as their own national standard for the management of risk.

5.3.2.5 ISO TC20, SC16 — Unmanned Aerial Vehicles

ISO TC20, SC16 was established in 2014 to develop standards in the rapidly developing field of unmanned aerial vehicles (UAVs or drones).

SC16 consists of four working groups:

- WG1 General
- WG2 Product manufacturing and maintenance
- WG3 Operations and procedures
- WG4 UAS Traffic management

5.3.2.6 CLC/TC79/Working Group12 — Alarm and Electronic Security Systems

The scope of CLC/TC79 is to prepare international standards for the protection of buildings, persons, areas and properties against fraudulent actions having the purpose to enter in a place or to take or to use something without permission and other threats related to persons. The scope includes (under Working Group 12) video surveillance systems (formally CCTV under Working Group 7, and in addition to access control systems, fire detection and fire alarm systems, etc.) for security applications.

Specifically, IEC 62676 is a multi-part standard addressing the use of video surveillance systems for use in security applications. It includes System and Performance Requirements (Part 1), Application Guidelines (Part 4), image quality specification and testing (Part 5) and testing of video content analysis systems (Part 6).

5.3.2.7 EC TC9 Working Group 46 — Electrical Equipment and Systems for Railways

The scope of EC TC9 is to prepare international standards for the railways, which includes rolling stock, fixed installations, management systems (including communication, signalling and processing systems) for railway operation, their interfaces and their ecological environment.

The relevance to the ERNCIP TG-EWZ is that Working Group 46 addresses 'Onboard multimedia systems for railways' with the scope to define and implement a multimedia framework that includes the standardisation of a number of subsystems within the train that communicate using the subsystem defined by WG43 (Fadin and Umiliacchi, 2011). One of the subsystems considered is 'Video surveillance/CCTV'. Overall, the work contributes to the development of the IEC62580 standards, which includes for video surveillance/CCTV, IEC 62580-2 (Electronic railway equipment — On-board multimedia and telematics subsystems for railway — Part 2: Video Surveillance/CCTV Services) which was published in 2016.

5.3.3 Relevant standards

The following sections outline the main standards which relate to early warning zones and critical infrastructure protection. The main categories of standards considered in this report are:

- Alarm systems
- Multimedia
- Forensics
- Video surveillance
- Risk management
- Biometrics

5.3.3.1 Alarm systems

The European Norm1 50132-1 'Alarm systems — CCTV surveillance systems for use in security applications — Part 1: System requirements' was established with the aim of ensuring a high consistent level of performance of video surveillance systems in Europe.

The latter parts gave recommendations for the selection, planning and installation of CCTV systems comprising camera(s) with monitor(s) and/or video recorder(s), switching, control and ancillary equipment for use in security applications (Part 7) and video transmission (part 5).

Note that EN 50132-1 has now been withdrawn and superseded by EN 62676-1-1 detailed below.

5.3.3.2 Multimedia

ISO/IEC 23000-10 (Information technology — Multimedia application format (MPEG-A) — Part 10: Surveillance application format) is an international ISO standard published in December 2012. ISO/IEC 23000-10:2012 specifies 'a file format designed to store data in and exchange data between surveillance systems. The file format provides an overall structure for media content and associated metadata. Media data coverage includes image, video and audio data. Specific features to support application of the format in surveillance systems include dedicated time information in a separate track as well as segmentation and segment linking provisions for media data.'

5.3.3.3 Forensics

There are a number of relevant forensics standards (ISO 27037; 27041-27043; 27050) whose main purpose is to promote good practice in methods and processes for forensic capture and investigation of digital evidence. Specifically, it includes provision of guidance on digital still and video cameras (CCTV), amongst other devices and formats.

ISO 27037, published in October 2012, is focused on the initial **capture** and storage of the potential image and video evidence and not on the subsequent [automated] analysis of the evidence.

ISO 27041 (2015) provides guidance on general **assurance** aspects of digital forensics. Specifically, that forensic tools and methods are applied properly.

ISO 27042 (2015) covers the analysis and interpretation of digital evidence.

ISO 27050 (2016) addresses **electronic discovery** within the collected forensic data. This includes the actual **processing** (analysis/search) of video data, which would include the application of video analytics.

5.3.3.4 Video surveillance

5.3.3.4.1 ISO 22311:2013

The ISO international standard on 'Societal security — Video-surveillance Format — Export interoperability' provides 'an export interoperability profile which constitutes the exchange format and minimum technical requirements that ensure that the digital video-surveillance contents exported are compatible with the replay systems, establish an appropriate level of quality and contain all the context information (metadata) necessary for their processing.'

The standard is motivated by the needs of law enforcement where 'the authorities [require the capability] to be able to rapidly use the data collected by different CCTV systems from given locations.' The aim was not to invent a new format but to rely heavily on a blend of individual technical standards separately developed, concentrating on the minimum set of profiles required to achieve the objective: for video in general MPEG (MPEG-4 H264 of ISO JTC 1 SC29), for the world of digital television (range of norms Society of Motion Picture and Television Engineers (SMPTE)), the North Atlantic Treaty Organisation (NATO)'s interoperability mechanisms for animated images STANdardization Agreement (STANAG 4609), etc. Furthermore, the goal was that the standard would represent a non-proprietary affordable solution for all future systems.

The standard includes the following video content components:

— Format for video content compression with quality required for exploitation in forensic police work, with preferred profiles, based on MPEG-4 H264 from ISO CEI JTC SC29;

— Minimum list of data describing the conditions of capture (i.e. metadata), the time and date the sequence was recorded, angles of view and the zoom value (for PTZ cameras), GPS coordinates for a camera on a vehicle, etc.; for each of these categories of metadata a specific means of representation (e.g. XML);

— Means to precisely synchronise the various elements captured at the same time, such as video(s), sound, metadata and alarms; the recommended solution is the format MPEG-A (ISO/CEI23000-10);

— Format or transfer protocol enabling a person exploiting the videos to be aware of what form the content will be sent;

— Means to integrate constraints relating to security and authentication of content that is valid as evidence in a court of law.

5.3.3.4.2 NF EN 62676:2014

EN 62676-1-1 (Video surveillance systems for use in security applications, 2013) is a series of standards intended to enable flexibility to overcome problems a system designer may have. It should be noted that the BS EN 62676 series of standards are the first standards for CCTV video surveillance that will be used to any significant extent in Member States and include the use of security grading. The full set of standards is as follows:

— Part 1-1: System Requirements — General) specifies the minimum requirements and gives recommendations for video surveillance systems installed for security applications

— Part 1-2: Video Transmission — General Video Transmission — Requirements

— Part 2-1: Video Transmission Protocols — General Requirements

— Part 2-2: Video Transmission Protocols — IP Interoperability implementation based on HTTP and REST services

— Part 2-3: Video Transmission Protocols — IP interoperability implementation based on Web services) defines procedures for communication between network video clients and video transmitter devices based on Web Services. This new set of specifications makes it possible to build network video systems with devices and receivers from different manufacturers using Web services. This international standard also contains full XML schema and web service description language (WSDL) definitions for the introduced network video services. Furthermore, appropriate protocol extensions have been introduced in order to make it possible for network video manufacturers to offer a fully standardised network video transfer solution to its customers and integrators

— Part 3: Analogue and Digital Video Interfaces

— Part 4: Application Guidelines

— Part 5: Video Content Analytics — Performance testing and reporting (Note — this part is still in development with publication expected in 2020).

5.3.3.5 Risk analysis

ISO 31000:2009 provides a high-level set of principles, framework and processes for managing risk and implementing risk management. This standard can be used by an organisation irrespective of its size, activity or sector.

In terms of critical infrastructure, risks in relation to performance of visual surveillance methods and systems need to be considered as part of the overall risk management profile. In particular, to consider standardisation of methods for visual surveillance as

part of security management system certification it provides a detailed description of a method of risk analysis and assessment responding to the decision-making needs and which allows development of an integrated analysis of the elements an organisation comprises (technological systems, procedures and human factor) through a multi-risk analysis aimed at assessing technological failure, intentional attacks and natural disasters. This enables evaluation, for example, of the effects of the security surveillance systems on safety and vice versa.

Note that ISO 31000 cannot be used for certification purposes, but some bodies do offer professional certification schemes for competence in implementing it.

5.3.3.6 Biometrics

5.3.3.6.1 ISO IEC 30137 — Use of Biometrics in Video Surveillance Systems (VSS)

This multi-part standard provides guidance on how to deploy and operate an automated face recognition system with video cameras.

- Part 1 (System Design and Specification) lists a number of use cases for FR with VSS and provides advice on designing and specifying the system. This includes advice on selecting and positioning video cameras, the size and content of the watchlist, computational considerations and the role of the operator. It also includes annexes looking at the more general use of video analytics and highlighting wider societal issues associated with the use of FR in public spaces. At the time of writing this report, Part 1 of ISO IEC 30137 is with the ISO editors and being prepared for publication.
- Part 2 (Performance Testing and Reporting) defines a methodology for evaluating and reporting the performance of a biometric system working with video data; including both detection and recognition metrics. Note that at the time of writing this report 30137 Part 2 has been cancelled as it was not progressing quickly enough to be published within the ISO timescales. However, it is the intention of SC37 WG5 to restart this work with a view to getting Part 2 published within the next couple of years.
- Part 4 (Ground Truth and Video Annotation Procedure) describes techniques for determining and reporting ground truth of test data.

5.3.3.6.2 ISO IEC 19794 — Biometric Data Exchange Formats

ISO IEC 19795 is a multi-part standard that defines data formats for the storage and exchange of biometric data. Only those parts of the standard considered most relevant to EWZ are listed below.

- ISO IEC 19794-1 (Framework) describes the general aspects and requirements for defining biometric data interchange formats. It is a prerequisite for understanding and implementing other parts of the standard, each of which specifies formats for specific modalities.
- ISO IEC 19794 Part 5 (Face Image Data) defines face image data formats for full size and token, full face and 3D, still facial images. It also includes 'Best Practice' guidance on the capture of compliant images (e.g. plain background, even lighting and a neutral expression). The standard does not support faces in video streams other than as a sequence of still facial images. The standard has been widely adopted internationally for facial images in passports, visas and drivers' licences.
- ISO IEC 19794-6 (Iris image data) defines iris image interchange formats for biometric enrolment, verification and identification.

Note that the ISO IEC 19794 series of standards is currently being revised as 'Extensible' Biometrics Data Interchange Formats (ISO IEC 39794-X) and these are expected to be published from 2019 onwards.

Other currently published parts of the standard are not considered directly applicable to EWZ as they are mostly contact-based biometrics and as thus not listed here. However, there are two new parts of the standard currently under development as part of the revised 39794 series that may be relevant when they are published:

— 39794-16 — Full Body Image Data

— 39794-17 — Gait Sequence Image Data

5.3.3.6.3 ISO IEC 29794 — Biometric Sample Quality

This multi-part standard defines methods and metrics for determining the quality of a biometric sample.

— 29794-1 defines terms and establishes a framework for measuring and reporting sample quality, regardless of modality. These include the purpose and interpretation of biometric quality scores, the encoding of quality data fields in biometric data interchange formats, methods for developing biometric sample datasets for the purpose of quality score normalisation, a format for exchange of quality algorithm results and methods for aggregation of quality scores.

— Subsequent parts of the standard apply to specific modalities, but only Part 5 (Face Sample Quality) and Part 6 (Iris Sample Quality) are considered applicable to EWZ applications. Note that Part 5 has to date only been published as a technical report (TR) and not as a standard.

5.3.3.6.4 ISO IEC 30107 — Presentation Attack Detection

This multi-part standard addresses the issue of liveness and other forms of spoofing detection (more formally known as Presentation Attack Detection) in biometric systems.

— Part 1 of the standard defines terms and establishes a framework through which presentation attack events can be specified and detected so that they can be categorised, detailed and communicated for subsequent decision-making and performance assessment activities.

— Part 2 defines data formats for conveying the mechanism used in the biometric presentation attack detection, and for conveying the results of presentation attack detection methods.

— Part 3 defines principles and methods for performance assessment of presentation attack detection mechanisms, including reporting of testing results from evaluations of presentation attack detection mechanisms and a classification of known attack types (in an informative annex).

5.3.3.6.5 ISO IEC 19795 — Biometric Testing and Reporting

This multi-part standard defines methodologies and metrics for the testing and reporting of the performance of biometric systems in terms of both error rates and throughput rates.

— Part 1 provides the framework for biometric testing and defines terms.

— Part 2 addresses two specific biometric performance-testing methodologies: technology and scenario evaluation. The majority of tests will fall into one of these two generic types.

— Part 3 describes the methodologies relating to modality-dependent variations on the general principles in Part 1. It presents and defines methods for determining, given a specific biometric modality, how to develop a technical performance test.

— Part 4 describes methods for evaluating the interoperability of systems that use biometric data conforming to ISO IEC 19794.

— Part 5 specifies a framework for testing and a grading scheme for reporting the performance of a biometric system suitable for use in access control applications.

— Part 6 provides guidance on the operational testing of biometric systems. It specifies performance metrics for operational systems, details data that may be retained by operational systems to enable performance monitoring and specifies requirements on test methods, recording of data, and reporting of results of operational evaluations.

— Part 7 provides guidance on testing of on-card biometric comparison algorithms, but is not considered applicable to EWZ applications

5.3.3.6.6 ISO IEC 29197 — Evaluation methodology for environmental influence in biometric system performance.

This standard, published in 2015, addresses the requirements for planning and execution of environmental testing evaluations for biometric systems based on scenario and operational evaluations.

5.3.3.6.7 ISO IEC TR 24714-1: Jurisdictional and societal considerations for commercial applications — Part 1: General guidance.

This TR provides guidelines on the legal and societal constraints on the use of biometric data, accessibility for the widest population, and health and safety, addressing the concerns of users regarding direct potential hazards as well as the possibility of the misuse of inferred data from biometric information.

5.3.3.6.8 ISO/IEC TR 29194: Guide on designing accessible and inclusive biometric systems.

This TR provides guidance for biometric system design and procurement to handle the range of accessibility and usability issues. As such it builds upon the generic guidance in ISO/IEC/TR 24714-1

5.3.3.6.9 ISO IEC 2382-37: Vocabulary — Part 37: Biometrics.

This standard establishes a systematic description of the concepts in the field of biometrics pertaining to recognition of human beings and reconciles variant terms in use in pre-existing biometric standards against the preferred terms, thereby clarifying the use of terms in this field.

5.3.3.6.10 Other documents

Other relevant documents currently in development include:

— ISO IEC TR 22604: Use of Biometric-Recognition-in-motion in Access Related Systems

  - This technical report provides guidance for development of biometric solutions for verification and identification processes for secure access without physical contact with any device at any time. Design considerations addressed by the TR include the selection and placement of capture devices (e.g. cameras), management of the flow of individuals requiring access and the proximity of capture devices to the individuals.

— ISO/IEC TR29156:2015 — Guidance for specifying performance requirements to meet security and usability needs in applications using biometrics.

  - This standard provides guidance on specifying performance requirements for authentication using biometric recognition in order to achieve desired levels of security and usability for the authentication mechanism.

5.3.4 Gap analysis

While standards now either exist or are being developed with respect to many aspects of EWZ, there remain some notable exceptions where standards are still lacking.

A particular concern relates to the measurement and reporting of the performance of technologies that may be used in EWZ systems, and especially the lack of any EU-wide certification scheme for surveillance systems. Without this, vendors are able to make claims about the performance of their products which have not been validated and which may bear little resemblance to what is achievable in real world operational use. ISO SC37 has done considerable work on performance measurement and reporting for biometrics applications, but the same is not true when it comes to video surveillance systems. In addition, it must be recognised that an EWZ solution will make use of a range of different technologies and even if performance standards exist for each part individually they may not accurately predict the performance of the wider end-to-end system.

Closely linked to performance is a growing awareness of the potential for individuals to 'spoof' or circumvent biometric and video surveillance systems. ISO SC37 has recently published the ISO IEC 30107 series of standards defining metrics and methodologies for evaluating and reporting how robust a biometric system is to such presentation attacks. However, these are primarily for conventional applications such as fingerprint, face or iris recognition with compliant subjects (e.g. for physical access control) and do not specifically address vulnerabilities with biometric recognition at range, e.g. when used with video-based surveillance systems such as those that may be found in EWZ solutions.

Sample quality has a major impact on the performance of a biometric recognition system. Some years ago NIST published NFIQ, an open source image quality algorithm for fingerprint images, and this has now been widely adopted internationally. However, there is currently no equivalent for facial images. In 2018 NIST announced a new project, the NIST FRVT Image Quality Assessment, with the goal of developing a standardised method for measuring the quality of ICAO compliant (e.g. passport) full-face images intended to be used with face recognition algorithms. Evaluation of currently available face-quality algorithms is expected to commence in May 2019 and could eventually lead to a new open source face image quality standard. While this will be a significant step forward it will not specifically address quality measurement of non-compliant facial images such as those typically captured by video surveillance cameras.

Another more general concern is the ability of standardisation efforts to keep pace with the rapidly changing technology landscape. International standards typically take between 3 to 5 years from commissioning to publication, during which time the technologies they are aimed at may have changed significantly. Whilst this challenge is acknowledged by standards bodies such as ISO it is not clear how it might best be addressed.

6 Suitability of video surveillance solutions for EWZ

6.1 State of the art of academic research

6.1.1 Video analytics

6.1.1.1 Person/vehicle detection and tracking

There has been extensive research by both the industrial and academic communities over the last decades on development of robust pedestrian (including face) and vehicle detection and tracking. A recent review of pedestrian detection may be found in Zhang et al. (2016). Strong performance on pedestrian benchmarks (e.g. PASCAL VOC) has been obtained using deep learning techniques (Tian et al., 2015; Hosang et al., 2015). For face detection (Zafeiriou et al., 2015), CNN-based methods have also shown significant performance gains over previous methods (e.g. Viola-Jones) with (Yang et al., 2015) for example, exploiting boosting and deformable part models on top of CNN features, and combining pedestrian and face detection in a single framework. State-of-the-art vehicle recognition further exploits CNN methods (Sochor et al., 2016). Generalised object detection using a fast (155 frames/second) single neural network architecture has recently been proposed by Redmon et al. (2016). Gidaris and Komodakis (2016) have focused on improving the localisation accuracy. In terms of tracking, recent CNN-based online approaches have shown outstanding performance on existing benchmarks (e.g. VOT) (Nam and Han, 2016). Identity-aware tracking (Yu et al., 2016) where additional contextual information, for example, detected faces, are assigned to recovered trajectories of pedestrians, has also recently been shown to improve the robustness in long-term surveillance scenarios. The main limitations with prior work in both detection and tracking is that they generally do not operate 24/7/52 and do not focus on camera networks with a significant number of cameras, both important requirements for EWZ.

Significant potential exists to develop an identity-aware tracking system exploiting deep learning for CCTV sensor network surveillance of people and vehicles, applied both offline and online (i.e. real-time).

6.1.1.2 Person/vehicle re-identification

The object re-identification problem involves identifying the same object (e.g. person, vehicle) captured in different camera views at different times. This is particularly relevant to EWZ as it helps law enforcement identify persons of interest when they reappear in a surveillance system. Followed by the first attempt in 1996 (Cai and Aggarwal, 1996), dozens of works have been published to solve this problem (Vezzani et al., 2013). It has drawn particular attention of computer vision researchers due to its importance in video surveillance and forensic applications (Vezzani et al., 2013; Gong et al., 2014) as well as EWZ.

The key challenges involved in a re-identification problem are the changes in object poses, viewpoints, and illumination in the scene under consideration, and the background clutter (Vezzani et al., 2013; Zhang et al., 2016; Zhang et al., 2016). In terms of type of camera modality the current approaches widely use standard environmental (i.e. CCTV) cameras, whereas re-identification with body-worn and mobile cameras is a research task where very little prior work exists. Additionally, from an application viewpoint the existing works mostly study the re-identification problem in comparatively smaller-area camera networks, thus considering the reappearance of objects across different camera views within a short time duration. Moreover, another challenge remains to address the problem in 'live' CCTV footage originating from a remote location.

A research challenge is therefore to design robust feature representations that generalise on surveillance scenes with significant variations as recorded from multiple EWZ locations at substantially different time instances (Xiao et al., 2016).

6.1.1.3 Situational awareness, anomaly and threat detection

Situational awareness is the understanding of the EWZ scene, events unfolding in that scene, and the actors and objects involved in these events. This understanding can then be used as a basis for further investigation, decision-making, and implementation of appropriate actions, such as enforcement. Arguably, situational assessment is an essential component of any CIP security-management system.

Threat can be defined as an expression of intention to inflict evil, injury or damage. Hence, the threat concept is inherently hidden (as it is an intention whose outcome is uncertain) and typically cannot be observed directly. There are several ways of defining and classifying threats and for CIP it is appropriate to study methods based on the concept of situation. Three types of threat descriptions can be identified as relevant for CIP: Anomalies, modus operandi pattern, and recall. Anomalies refer to situation change (pattern) that deviates from the typical or normal. Anomaly detection does not identify threats, but does send a signal to study some part of the environment more carefully (possibly with human assistance). What is normal has to be learned or specified. Modus operandi patterns mean that some threats can be (manually) expressed in terms of plans and procedures that can be detected. Recall involves detection of partial situations which have previously occurred in threatening situations.

Currently, there exists a lack of robustness in approaches to automatic situational awareness, anomaly and threat detection in EWZ scenes. This is due in part to the quality and amount of (training) data input to these processes (typically object classifications and trajectories), as well as the overall effectiveness of machine learning approaches to recognition. Further research is needed to fully model EWZ scenes and threats, and development of threat recognition approaches with a level of false alarms acceptable to the operator.

6.1.1.4 Automatic number plate recognition (ANPR)

A number of commercial automatic number plate recognition (ANPR) systems exist today. These include the Talon System from NDI Recognition Systems which is deployed at 30+ UK police forces and 7+ UK international airports as well as at CI worldwide.

6.1.1.5 Crowd image analysis

The analysis of crowded scenes is of high relevance to EWZ. Methods can be categorised as low level: crowd person count and density estimation; mid-level: tracking of an individual or individuals within a crowd; or high level: detection of separate flows and specific crowd events. Depending upon the number of people within the scene, methods are generally either focused on detecting and tracking of individuals, or for particularly dense scenes where tracking individuals as individuals is difficult, holistic approaches treat the crowd as a single entity moving along a given path or direction.

Crowd image analysis remains very much a research domain to perform the above tasks robustly, and in particular in the context of CIs and EWZ. Two recent surveys are detailed in Sami Zitouni et al. (2016) and Li et al. (2015).

6.1.2 Deception detection

In their search for the truth, law enforcement do not only gather as much information as possible, but they also have to determine the reliability of that information. Unreliable information from suspects (or witnesses) in EWZs can steer intelligence/investigation in the wrong direction and cause great disruption. The witness or suspect may deliberately provide false information (i.e. deception) and deception detection is based on the assumption that the act of deceiving affects the deceiver's physiology and behaviour (non-verbal, para-verbal and verbal), and that changes in these behaviours can be identified. To circumvent reliability issues associated with human deception detection (54 %) (Bond and DePaulo, 2006), researchers experimented with automated detection methods based on recordings of truths and lies. Video recordings are of special interest,

because they comprise both physiological and behavioural cues to deceit. A concealed information test (CIT) is constructed of several multiple-choice questions in which crime-related details are presented to a suspect. When the suspect is familiar with a piece of information, they will demonstrate a measurable reflex. When a reflex repeatedly occurs in response to crime-related information that cannot have been accessed in another way (e.g. media coverage or crime scene access), it indicates the suspect holds perpetrator knowledge.

Significant potential exists to develop, deploy and evaluate a multimodal platform to perform deception detection at or away from EWZs (for example, in interview rooms for the latter).

6.1.3 Interrogating large volumes of CCTV

While CI protection may be considered mainly as a proactive surveillance problem, there is a responsibility on government agencies and law worldwide to capture and review significant volumes of CCTV images for intelligence-led operations and in investigations including EWZs. In particular, reconnaissance has previously been used by potential attackers of CI. The advent of large numbers of CCTV cameras of increasing quality in terms of resolution and frame rate, has led to an explosion in the amount of data that is gathered by the intelligence and law enforcement community. The analysis of large volumes of CCTV, however, is a difficult and time-consuming process because of both interoperability problems between the various surveillance systems on the market and the lack of application of video analytics.

Significant scope exists to apply advanced video search and data mining methodology to aid in forensic video archive search.

6.1.4 Cognitive surveillance

The European Commission have identified the objectives of cognitive vision to include the development of robust cognitive vision systems acquiring and using knowledge for decision-making, to focus on adaptive systems for real-time platforms and vision architectures permitting the development of novel computational frameworks, integrating multiple cues for scene modelling, recognising large number of objects and achieving cognition such as temporal learning and incremental learning. Based on this, an increasing amount of research has been undertaken which focuses on the development and integration of cognitive components into surveillance systems. Initiatives include the EUCogIII project (2012 and ongoing) ([21]) a European network for researchers in artificial cognitive systems and related areas who want to connect to other researchers and reflect on the challenges and aims of the discipline.

Future research in cognitive vision includes development of advanced machine learning and reasoning capabilities compliant in a largely unsupervised way to handle variations and novelties in EWZs.

6.1.5 Aerial platforms

Aerial surveillance platforms (specifically drones) bring a number of strengths and weaknesses to standard fixed surveillance infrastructure. The main strengths of UAVs are the possibility of moving the cameras and sensors throughout the EWZ surveillance area, maximising the investment, adaptability to the different EWZ situations encountered, the possibility of responding to alarms from multimodal sensors, and the dissuasive effect of not knowing when a camera may be monitoring an EWZ area. The main weakness is that the autonomy of the UAVs is limited, approximately 30 minutes on average and extending in the most advanced models to 50 to 60 minutes. Alternate technologies, such as fixed-wing systems or hybrid multirotors, can extend endurance to several hours, however with different issues such as greater noise or the impossibility of remaining

([21]) http://www.eucognition.org (accessed 18 June 2019).

static in the air. Furthermore, embedded algorithms may be used in such platforms; however, the greatest computing power is usually on the ground. This means that local and less powerful versions of the algorithms must be used in cases of poor communications coverage or low bandwidth. In addition, operation of drones requires compliance with the legislation of each country.

Significant scope exists to research sensing systems (especially sensor fusion and sensor processing algorithms (for example, CNN-based object classification), and deployment of a single or a coordinated fleet of (autonomous) drones in EWA areas. Such deployment could be used for proactive surveillance or reactive surveillance based, for example, on detections from ground-based sensors.

6.1.6 4D visualisation

4D (3D space + time) reconstruction of an EWZ surveillance scene enables law enforcement to visualise a chain of events. Specifically, to develop efficient and robust video analysis methods for 4D space-time reconstruction of dynamic scenes by integrating data from multiple CCTV cameras and ancillary information when available (see section 3.3.2 above on multisensory networks). A related requirement is development of efficient means to browse the scene at different levels of detail.

Visualisation of a 4D scene with moving pedestrians and vehicles from video requires synchronisation and spatial calibration of the cameras to be able to map images and objects to the 3D model and to estimate their position and motion. Images distorted by non-rigid distortion and rolling shutter can be compensated for (Tian and Narasimahn, 2012; Ringaby and Forssen, (2012)). Cameras can be calibrated in relation to other cameras and to a 3D scene of the model (Mustafa et al., 2016). The calibration requires matching of features or patches between sequences and between the 3D model and the image sequence (Pollefeys, et al., 2004). A set of images can be used to tour a scene but is restricted to the views of the images in the set (Snavely et al., 2006). Visibility in a scene viewed by several or many cameras can be estimated that is relevant both for the visualisation and for analysis of the chain of events (Joo et al., 2014).

Significant potential exists to automatically insert detected persons and vehicles, as well as events and threats, observed in the EWZ scene into a 4D model to enhance visualisation by CI operators.

6.2 Commercial products

A multitude of companies exist that market products providing video analytic solutions for tasks such as object detection and classification, person re-identification, tracking, event detection and alarming, relevant for EWZ application. These companies include Axis Communications, IDIS Europe/DAVANTIS, Avigilon, Hanwha Techwin Europe, intuVision Security, Dahua Technology, Herta, AxxonSoft Ltd, Qognify Ltd, Digifort Pty Ltd, Umbo CV Inc., Brickcom Corporation, Digital Barriers plc, Heras, Huper Laboratories Co. Ltd, Ipsotek Ltd, Alnet Systems Inc., Videmo Intelligente Videoanalyse GmbH und Co. KG, Videmo Intelligente, Aventura Technologies Inc., Samsung SDS Europe Ltd., IPS Intelligent Video Analytics, ACIC S.A, eSurv, iOmniscient Pty Ltd., TechnoAware, Kinesense and SeeQuestor. However, given that there is no EU certification process in existence for video-based security products, it is difficult to assess the performance claims of the respective systems. A significant divide frequently exists between what is claimed by product vendors and authoritative users with respect to performance, especially acceptable false alarm rates.

6.3 EC programmes

There are a number of projects funded internationally, nationally, under FP7 and Horizon 2020, and other initiatives, that relate to EWZ/CI protection and video analytic/surveillance functionality. These include projects ranging from those that address public safety and law enforcement (VALE, VAPS, IARPA DIVA programme) to

specific projects focusing on exploitation of large amounts of (video) data (LASIE, ADVISE, SAVASA), video analytics (P5) to those considering legal, ethical, privacy and societal issues around video analytics (e.g. SOURCE, SURVEILLE, VIDEOSENSE). The following sections detail representative examples of these projects and are not intended to be an exhaustive list.

6.3.1 Critical infrastructure protection

The EC funded two research projects, P5 and ARGOS, under the Framework 7 call topic SEC-2012.2.3-1 — Early warning security systems: physical protection of critical buildings — Capability Project which are of specific interest for critical infrastructure protection.

The goal of the P5 (Privacy Preserving Perimeter Protection Project) project (2013-2016) was to develop an intelligent, proactive perimeter surveillance system for critical infrastructure to give early warning of terrestrial, waterborne or airborne threats. The research focussed on a system that works robustly under a wide range of weather and lighting conditions and that has strong privacy-preserving features.

The goal of the ARGOS (Advanced pRotection of critical buildinGs by Overall anticipating System) project (2014-2016) was to enhance the capacity of infrastructures in order to monitor, deter, and respond to a potential threat using 'early warning technologies'. This included application of video sensors and embedded video analytics for 1st level processing (together with a s2nd level of powerful video analytics placed in the local gateway) such that only metadata is transferred instead of images.

More recently, under H2020, the EU has issued calls under Secure Societies for Critical Infrastructure Protection (e.g. CIP-01-2016-2017). The reasoning behind the call is stated as 'The lines between the physical and the cyber worlds are increasingly blurred. Recent events demonstrate the increased interconnection among the impact of hazards, of the two kinds of attacks and, conversely, the usefulness for operators to combine cyber and physical security solutions to protect installations of the critical infrastructure of Europe: A comprehensive, yet installation-specific approach is needed.' However, none of the funded projects under this call, to the best of the authors' knowledge, focus on video surveillance technologies in urban environments. A call has been issued in 2019 (SU-INFRA02-2019: Security for smart and safe cities, including for public spaces) where it is foreseen that video surveillance solutions are integrated into a holistic approach for protection of public spaces.

6.3.2 Disaster-resilient societies

A number of projects have been funded under digital security (DS) and disaster-resilient societies (DRS) topics which are relevant to EWZ, including:

— DRS-17-2014-1 — Critical Infrastructure protection topic 7: SME instrument topic: 'Protection of Urban soft targets and urban critical infrastructure'.

- Project SURVEIRON (2016-2018): Advanced surveillance system for the protection of urban soft targets and urban critical infrastructure. The aim was to provide those in charge of public and private security with an intelligent surveillance and decision-making service in critical situations.
- Project SafeSky (2015) — Integrated system for critical infrastructure and personal sphere monitoring and protection against aerial threats. The overall aim of this innovation project was to deliver the world's first integrated system dedicated to critical infrastructure and personal sphere monitoring and protection against aerial threats.

6.3.3 Fight against crime and terrorism

A number of projects have been funded under the EC H2020 Fight Against Crime and Terrorism call which are relevant to EWZ, including:

- **SEC-2007-1.2-02 — IMSK (2009-2013):** Developed an integrated mobile surveillance solution which integrates data from sensors in order to enhance knowledge about current situation and ensure higher protection of surveilled area. The main types of sensor used are CBRNE (chemical, biological, radiological, nuclear and explosive), cameras with 3D face recognition support, THz cameras for detection of hidden objects, etc.
- **SEC-12-FCT-2016 CONNEXIONs (2018-2021):** InterCONnected NEXt-Generation Immersive IoT Platform of Crime and Terrorism DetectiON, PredictiON, InvestigatiON, and PreventiON Services: The aim is to develop and demonstrate next-generation detection, prediction, prevention, and investigation services. These services will be based on multidimensional integration and correlation of heterogeneous multimodal data, and delivery of pertinent information to various stakeholders in an interactive manner tailored to their needs, through augmented and virtual reality environments. It addresses the whole lifecycle of law enforcement including proactive crime prevention.
- **SEC-12-FCT-2016 MAGNETO (2018-2021):** Multimedia Analysis and Correlation Engine for Organised Crime Prevention and Investigation: The aim is to prevent and investigate terrorism, as well as crime against persons and property. The focus is on digital forensic investigations involving huge amounts of multimedia and textual data, and includes (1) collection and processing of meaningful information about an event, (2) identification of suspects, (3) understanding and associating the sequence of events and the roles of participants, and (4) providing evidence for charging suspects admissible in a court of law.
- **SEC-07-FCT-2016-2017 LETS-CROWD (2017-2019):** Law Enforcement agencies human factor methods and Toolkit for the Security and protection of CROWDs in mass gatherings. The project aims to overcome challenges preventing the effective implementation of the European Security Model (ESM) with regard to mass gatherings. This will be achieved by providing the following to security policy practitioners and in particular, LEAs: (1) a dynamic risk assessment methodology for the protection of crowds; (2) a policymaking toolkit for the long-term and strategic decision-making of **security policymakers; (3) a set of human-centred tools for law enforcement agencies (LEAs), including real-time crowd behaviour forecasting and novel computer vision techniques.**
- **SEC-12-FCT-2016-2017 ALADDIN (2017-2020): Advanced hoListic Adverse Drone Detection, Identification Neutralization. The project** is studying, designing, developing, and will evaluate, in series of complementary pilots, a counter UAV system as a complete solution to the growing UAV threat problem, building upon a state-of-the-art system and enhancing it by researching on various technologies and functionalities. ALADDIN is following a holistic and heavily user-centred methodology involving a large number of LEAs and critical infrastructure operators.
- **SEC-12-FCT-2016-2017 VICTORIA (2017-2020): Video analysis for Investigation of Criminal and TerrORIst Activities. The aim is to develop** an ethical and legally compliant video analysis platform that will accelerate the video analysis tasks of law enforcement agencies during investigations.
- **COPKIT is considered a sister project to CONNEXIONs. The aim of COPKIT is to create an intelligence and knowledge ecosystem for law enforcement agencies (LEA) in an effort to prevent, investigate and** mitigate the use of new information and communication technologies by organised crime and terrorist groups by developing an early alert/early action system.

6.4 Pre-operative validation and SME instruments

There have also been some projects funded under other instruments which are relevant to EWZs, including:

— **H2020-SMEINST-1-2014** LETS-CROWD (2017-2019): Law Enforcement agencies human factor methods and Toolkit for the Security and protection of CROWDs in mass gatherings: As well as dynamic risk assessment methodology and a policymaking toolkit, the project seeks to develop a set of human-centred tools for LEAs, including real-time crowd behaviour forecasting, innovative communication procedures, semantic intelligence applied to social networks and the internet, and novel computer vision techniques.

— SEC-2013.3.2-1 — Pre-Operational Validation (POV) on land borders EWISA (2014-2019): Early Warning for Increased Situational Awareness — http://www.ewisa-project.eu. The project aims to develop an intelligent video surveillance including capability to detect irregular movements within a monitored area, identify targets and recognise suspicious behaviour.

6.5 Ethics, privacy and societal projects

— SEC-2012.7.4-2 — Networking of researchers for a high-level multi-organisational and cross-border collaboration — Network of Excellence — SOURCE (2014-2019). The aim of SOURCE is to create a robust and sustainable virtual centre of excellence capable of exploring and advancing societal issues in security research and development.

— SEC-2011.6.1-5 — Surveillance and the challenges for the security of the citizen — SURVEILLE. Assessment of benefits and costs of surveillance and legal and ethical issues in the prevention, investigation and prosecution of terrorism and other crime.

— SEC-2010.7.0-1 — Networking of researchers for a high-level multi-organisational and cross-border collaboration: Network of excellence on ethically guided and privacy-preserving video analytics (2011-2015). VideoSENSE (http://www.videosense.eu) (Virtual Centre of Excellence for Ethically-guided and Privacy-respecting Video Analytics in Security) was instigated to foster significant advances in the domain of ethically aware data and video analytics.

— SEC-2010.6.5-2 — Use of smart surveillance systems, data protection, integrity and sharing information within privacy rules — ADDPRIV (2011-2014). The project proposed novel knowledge and developments to limit the storage of unnecessary data in existing camera networks in order to make them better comply with citizen's privacy rights. In addition, development and testing of algorithms for automatic browsing, identification and retrieval of images on the suspicious individuals across the multicamera network.

6.6 Other projects

— SEC-2007-2.3-01 — Detection of unattended goods and of owner — SUBITO. FP7 project (2008-2011) addressed the development of automated real-time (CCTV) detection of abandoned luggage and fast identification and tracking of the owner (pre- and post- event). Typical public space surveillance scenes were considered (e.g. car park, exhibition hall, etc.). Supporting studies examined examine additional sensors. The project developed the metadata language and interoperability required to integrate the surveillance components (detection, tracking, threat detection) and HCI.

— SEC-2007-2.3-03 — Detection of abnormal behaviour — ADABTS. ADABTS aimed to facilitate the protection of EU citizens, property and infrastructure against threats of terrorism, crime, and riots, by the automatic detection of abnormal human behaviour. This included definition of appropriate behaviour descriptors as well as models of

threatening behaviour. Algorithms were developed to detect predefined threat behaviours and deviations from normal behaviour. For accurate and robust detection, data from audio and video sensors was combined with context information.

— SEC-2013.1.6-1 — Framework and tools for (semi-) automated exploitation of massive amounts of digital data for forensic purposes — Integration Project: Open extensible framework for investigation of large amounts of heterogeneous data (e.g. CCTV, internet, social networks, mobiles, ...).

— SEC-2011.5.3-4 — Video archive search — Capability Project: SAVASA (2011-2014). The SAVASA project proposed the creation of a video archive search platform that allows authorised users to perform semantic queries over different, remote and non-interoperable video archives. This project exploited trends in computer vision, video retrieval and semantic video analysis.

— SEC-2012.6.1-2 — Tools and methodologies, definitions and strategies for privacy by design for surveillance technologies, including ICT systems — Capability Project or Coordination and Support Action: PARIS (2013-2016). The aim of PARIS was to define and demonstrate a methodological approach for the development of surveillance infrastructure which enforces the right of citizens for privacy, justice and freedom and takes into account the evolving nature of such rights. Two use cases were demonstrated, one based on video search technology which focuses on the archived data, and one based on biometrics technology.

6.7 International programmes

The following documents international programmes relevant to EWZs, in the area of public safety and law enforcement.

6.7.1 Public safety and law enforcement

— VAPS (US) (2016-): In February 2016, NIST, the OSTP NITRD Video and Image Analytics (VIA) Interagency WG, and the DHS-led Video Quality in Public Safety (VQiPS) WG joined forces to foster the creation of a technically diverse Video Analytics in Public Safety (VAPS) community of interest (CoI) to develop a national R & D strategy in this emerging area and begin critical collaboration, R & D, measurement, and standards activities.

— IARPA DIVA (US) (2016 and ongoing): In July 2016, the U.S. Intelligent Advanced Research Projects Activity (IARPA) instigated the Deep Intermodal Video Analytics (DIVA) programme (https://www.iarpa.gov/index.php/research-programs/diva). The aim of the programme is to 'develop robust automatic activity detection for a multi-camera streaming video environment. Activities will be enriched by person and object detection. DIVA will address activity detection for both forensic applications and for real-time alerting.'

— DARPA: Mind's Eye (US): The Defence Research Projects Agency (DARPA) Mind's Eye was instigated in September 2010 as a video analysis research programme focused on advanced AI. In total 12 international research teams and three commercial integrators were involved in the 5-year programme. A number of collaborative projects were set up under the initiative and methods developed for video event recognition. Specifically, to include recognition of human activities in video and to predict what might happen next. Research also involved developing software to flag unusual events and deduce actions that may be occurring off-camera.

— VALE (UK) (2015 and ongoing): Video Analytics for Law Enforcement is a project run by Home Office CAST on behalf of UK policing to investigate the potential for the use of video analytics in law enforcement scenarios, in particular to determine those scenarios that UK law enforcement feel would benefit from the deployment of effective automated video analytics solutions.

6.8 Privacy considerations

As described in section 6.4.5, there have been several projects funded nationally, under FP7 and Horizon 2020, and other initiatives relating to privacy and ethical aspects of video surveillance in the field of law enforcement activities. From the privacy-by-design point of view, many studies combining law, ethics, sociology and technology have been carried out and which systematically reviewed the impacts of different surveillance systems and assist manufacturers and end-users to better develop and deploy systems, which are of high relevance to EWZs. Important collaborative initiatives, such as the VideoSense (Virtual Centre of Excellence (FP7)) project, have played a significant role by bringing together leading experts and resources to foster significant advances in the domain of ethically aware data and video analytics with a synergic and integrated approach. The SAVASA project (FP7) proposed the creation of a video archive search platform that allows authorised users to perform semantic queries over different, remote and non-interoperable CCTV video archives taking into account the needs of law enforcement agencies (LEAs), judicial authorities, civil protection and other organisational requirements as well as ethicists and legal experts to guide platform development. The ADVISE project (FP7) aimed to ease the work of law enforcement authorities in their fight against crime and terrorism, through negotiation of all relevant legal, ethical and privacy constraints, and through location-based video archive selection and efficient evidence mining of multiple, heterogeneous video archives. The more recent FORENSOR project (H2020) proposed to develop and validate a cover evidence gathering sensor to operate at remote locations, automatically identify pre-defined criminal events, and alert LEAs in real time while providing and storing the relevant video, location and timing evidence. In that project they also aimed to preserve the availability and the integrity of the evidence collected, and comply with all legal and ethical standards, in particular those related to privacy and personal data protection.

6.9 Benchmarks, databases and standards

The following outlines important considerations around benchmarks, databases and standards. For further details the reader is referred to the recent ERNCIP report on *Video surveillance standardisation activities, process and roadmap document* (Ferryman, 2016) and ERNCIP report on *Access to Datasets* (Marcenaro, 2016).

6.9.1 Benchmarks

Performance evaluation, or benchmarking, refers to the process of assessing quantitatively (as well as qualitatively) performance of individual video analysis methods (for example, detection, tracking, recognition) against the ground truth, using a set of appropriately defined metrics. To date, there is no universally agreed set of metrics or overall benchmarking process. Moreover, while initiatives such as the UK's Imagery Library for Intelligent Detection Systems (i-Lids) have also addressed the related area of certification of video analytics systems for specific scenarios, the approach has not been universally adopted for a wider range of video analytic methods and/or scenarios, nor at a European level. More specifically, metrics lack emphasis on a particular application scenario, and furthermore, lack suitable consideration of practical usability, i.e. acquisition and processing time, cost and efficiency, etc.

6.9.2 Databases

The creation of representative data corpora to facilitate common benchmarking and new methodological development of video analysis methods (e.g. identification, tracking, etc.) is essential. Multimodal database collection is a time-consuming process due to the multitude of sensors required to record. Although there are individual databases available (e.g. CCTV, video quality assessment, face, etc.) there are no multimodal databases containing images recorded for investigation of surveillance scenes.

6.9.3 Standards

Relevant standards include those associated with forensics, multimedia, interoperability, video data interchange formats, recognition protocols and procedures, performance assessment. While recent standards address some aspects (see section 3), a lack exists in (1) a universally agreed set of benchmarking metrics for video analytics, (2) video forensic platform interoperability, and (3) a complete set of standards which address the full chain of video analysis application in law enforcement. Furthermore, there is no European certification process for video analysis systems.

6.10 Conclusions

It is widely recognised that automated video (e.g. CCTV) surveillance plays an important role in CI protection. Artificial intelligence (AI) for video surveillance exploits the latest developments in AI methods including advanced video analytics and behavioural understanding. Such developments mean that it is now possible to build large-scale multisensory and multimodal sensor networks that are capable of interpreting, in real time, dynamic scenes and to identify prevailing threats.

Recent years have witnessed significant advancements in AI methods which may support systems developed for CI protection. In particular, methods for automatic machine learning, data analytics and artificial cognition and perception. AI is applicable at all levels. For example, deep learning is a paradigm that has been adopted throughout the full processing chain with significant impact. A wide range of commercial vendors of video surveillance systems also exists, often with claims on system performance which have not been certified.

This document has provided an overview of video surveillance activities and their mapping to use cases identified in section 3 for the protection of early warning zones (EWZs). The main video surveillance functionalities relevant to different EWZ use cases have been identified, as well as their limitations and further research needed to attain a level of maturity required for deployment. Other representative relevant initiatives, including representative EC research projects and international programmes, are also identified and summarised. Finally, privacy aspects are considered as well as relevant benchmarks, databases and standards.

7 EWZ policy options and design requirements

7.1 Introduction

7.1.1 General context and approaches

Today we live in a highly interconnected world. New communication technologies have made it possible for data to travel long distances in the blink of an eye, disseminating massive amounts of information. This opened up a number of possibilities. However, it also introduced challenges related to the correct and secure management of information. For instance, seamless connectivity created a sheer quantity of data that is making managing information harder by the day ([22]).

Personal data does not escape the issues. Information about individuals are constantly shared and moved across the global network. The social media phenomenon, in particular, opened the door to a massification of online interactions. Now, leveraging on the value of personal data (for instance, obtaining 'for-free' services on the internet) is not novel anymore.

If on one side it is possible to say that people grew accustomed to this information-sharing regime, at the same time, a growing number of people are demanding better safeguards for their data. This forced governments and national leaders to take action in the field of data protection and privacy. The European Union pioneered a rapidly expanding set of global initiatives ([23]) with important achievements, which greatly increased the general technological awareness of regulators, courts, and practitioners, meaning that every aspect impacting on privacy will be under heightened and stricter scrutiny.

The current European legal framework provides a number of measures aimed at safeguarding personal data. However, this enhanced protection comes at a cost. Limiting the access to personal data might impair the capacity of police, armed forces, and other security-involved entities to draw clear and precise pictures of what is happening in the operational scenario they operate in, leading to a potential decrease in the effectiveness of public security. In this regard, many are asking whether there should be a more open access to data for combating crime, terrorism and, in general, increasing the overall level of security for European citizens.

Public security is one of the top priorities for policymakers. However, this notion is clashing with the need to ensure adequate protection to personal data, privacy, and freedom of expression. This holds particularly true when looking at new technologies such as biometrics and facial recognition. As they promise to increase the effectiveness of security forces and ensure a more secure environment for the European citizens, they also carry heightened risks related to mass surveillance and privacy violation ([24]).

Critical infrastructures are a category of assets that requires a great deal of security and protection, as they are 'essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people' ([25]). For this reason, it is of the utmost importance that critical infrastructures are protected with the best possible measures. However, adopting new security methods can often result in unforeseen legal consequences, especially when considering privacy and data protection.

([22]) Marr, B., 'How Much Data Do We Create Every Day? The Mind-Blowing Stats Everyone Should Read', *Forbes*, 2018, https://www.forbes.com/sites/bernardmarr/2018/05/21/how-much-data-do-we-create-every-day-the-mind-blowing-stats-everyone-should-read/#720b894a60ba (accessed 18 June 2019).

([23]) For an overview of the most recent achievements of the European Union on data protection see https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en (accessed 18 June 2019).

([24]) European Union Agency for Fundamental Rights, Surveillance by intelligence services: fundamental rights safeguards and remedies in the European Union — Mapping Member States' legal frameworks, November 2015, p. 21.

([25]) Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, Article 2.a.

In this regard, the European Reference Network for Critical Infrastructure Protection (hereinafter, also 'ERNCIP') is looking at the situation, evaluating potential options to move the discussion forward. In particular, ERNCIP aims at investigating the viability of two specific security measures, these being the establishment of early warning zones (hereinafter, also 'EWZ') and the adoption of biometrics-enabled video surveillance means (hereinafter, also 'biometric surveillance'). In order to properly assess this topic ERNCIP involved a number of experts. In this, Working Party 7 (hereinafter, also 'WP7') has been tasked with assessing the aforementioned security measures in the light of the criticalities coming from the data protection regimes, as described above. More specifically, the goal of WP7 is to provide a set of 'points to be considered' with regard to the following aspects:

— The understanding of how the 'need-for-privacy' could be balanced with the 'need-for-public-security';

— The identification of potential approaches that policymakers can adopt to promote the implementation of EWZ and biometric surveillance in the context of critical infrastructure protection, striking a fair balance between security and privacy;

— The identification of the requirements that constitute the legal ground upon which EWZ and biometric surveillance measures for critical infrastructure protection should be assessed.

7.1.2 Legal framework

For the purpose of the present paper, the WP7 looked into two main normative areas within the European framework, these being critical infrastructure protection and data protection regulations.

As for the first area, the main normative document is Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, also known as the critical infrastructure protection directive (CIP directive). The document, which represents the foundation of the current European legal regime in relation to critical infrastructure protection, set the normative framework that European critical infrastructure operators have to observe. The CIP directive is a precious instrument aimed at ensuring an adequate and consistent level of critical infrastructure protection across Europe, and 'it establishes a European Union (EU) process for identifying and designating European critical infrastructure (ECIs), and sets out an approach for improving their protection' ([26]).

A second normative area pertaining to privacy and data protection is very central to this report. It is possible to identify three main groups of data protection norms. The first one pertains to the fundamental rights. In fact, according to Article 8 of the EU Charter of Fundamental Rights of the European Union (hereinafter, the 'Charter'), everyone has the right to the protection of their personal data. What is more, Article 8 of the Charter guarantees the right to respect for private life, mirroring Article 8 of the European Convention on Human Rights (ECHR).

A second normative area includes Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, also known as general data protection regulation (hereinafter, also 'GDPR') and Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, also known as law enforcement directive (hereinafter, also 'law enforcement directive').

([26]) EUR-Lex, Summary of: Directive 2008/114/EC — identification and designation of European critical infrastructures and assessment of the need to improve their protection, 14 November 2016.

The GDPR represents the cornerstone of data protection and privacy laws. Being a regulation, it does not require specific national law to transpose its provisions and is directly applicable to all of the European Union Member States. The law enforcement directive, on the other hand, is narrower both in the scope and in the approach. Designed with a clear and explicit connection to the GDPR, Directive 680 deals with, broadly speaking, the processing and sharing of personal data in the context of policing and execution of criminal penalties.

The law enforcement directive applies whenever three elements are matched together. Firstly, the processing activity shall be performed by 'competent authorities' defined as 'any public authority competent for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security or any other body or entity entrusted by Member State law to exercise public authority and public powers for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security' ([27]). Secondly, the law enforcement directive applies only when competent authorities process personal data for the purpose of 'prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security' ([28]). Lastly, the law enforcement directive applies only on processing activities 'based on Union or Member State law' ([29]). Since it is a directive, it sets out a goal that all EU countries must achieve. However, it is up to each Member State to devise their own laws on how to reach these goals. The third kind of data protection regulations gather norms that are based on principles and follow obligations detailed within the law enforcement directive. An example of these is Directive (EU) 2016/681 (also known as the 'PNR directive'), which 'provides for [...] the processing of the data referred to [the transfer by air carriers of passenger name record (PNR) data of passengers of extra-EU flights], including its collection, use and retention by Member States and its exchange between Member States' ([30]). Lastly, Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, also known as the 'ePrivacy Directive' (as a *lex specialis* with regard to GDPR) deals with the protection of privacy within electronic communication and public communications networks. Even though an updated version is imminent ([31]), it might not be directly relevant to EWZ and biometric surveillance. However, European operators need to be aware of these provisions, and consider their applicability on a case-by-case basis.

7.1.3 Methodological approach

In order to adequately pursue its goals and to extract the relevant requirements and guidelines in the context of critical infrastructure protection, WP7 investigated three different bodies of knowledge, following a step-by-step approach. Firstly, WP7 assessed the most relevant norms currently in force. Section 2.2 presents the main documents that WP7 took into consideration. The analysis of such norms aimed at isolating the crucial points related to the topic at hand. The GDPR and the LED represented the main focus, and were scrutinised in depth. WP7 did not consider national laws and norms. Secondly, WP7 surveyed the relevant case law, collecting the most importance sentences and judgments European courts have delivered throughout the years. The analysis of this relatively 'uncharted territory' of European jurisprudence revealed valuable pieces of information about the interpretation of specific normative aspects. Lastly, WP7 looked for

([27]) Law enforcement directive, Art. 3.1.7.
([28]) Law enforcement directive, Art. 1.
([29]) Law enforcement directive, Art. 8.1.
([30]) Parliament and Council of the European Union, Directive (EU) 2016/681 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, 27 April 2016, Art. 1.
([31]) For an overview of the ongoing review of the ePrivacy Directive see Legislative Train Schedule, JD — Proposal for a Regulation on Privacy and Electronic Communications, last updated 20 March 2019.

additional guidance into the academic and research materials produced by scholars and specialised bodies.

Despite the varied set of sources that has been consulted, it is worth noting that the amount of relevant case law and academic contributions specifically dedicated to critical infrastructure protection and data protection is still very limited. There is certainly a growing trend, though. Therefore, such bodies of knowledge shall continue to be monitored to capture the numerous updates that are likely to be published in the coming years.

All the information gathered was considered not only through the lense of WP7. The working group engaged in a strict cooperation with other WPs in order to more deeply understand the needs related to critical infrastructure protection, and to propose solutions that are respectful of fundamental rights and data protection obligations.

7.2 Striking a fair balance between public security and citizens' privacy

Traditionally, public security and citizens' privacy have been represented as two conflicting principles ([32]). The updated European data protection landscape has given new life to this discourse. On the one hand, 'rapid technological developments and globalisation have brought new challenges for the protection of personal data [while] the scale of the collection and sharing of personal data has increased significantly [and] technology allows both private companies and public authorities to make use of personal data on an unprecedented scale in order to pursue their activities' ([33]). On the other, the recent fatalities from terrorist attacks in the EU increased the friction between security and privacy, and inflated a conflict that is gaining momentum, with citizens vocally demanding a higher level of public security. As a result, policymakers and citizens are engaged in a discussion aimed at understanding whether, and to what extent, it is acceptable and worth losing privacy in favour of security. The outcomes of this discussion are still under debate.

Critical infrastructure operators find themselves in the middle, between the 'pro-privacy' and 'pro-security' camps. The uncertainty that characterises this ideological clash makes it difficult for them to find a balance, and has real consequences for their course of action. Since some measures might be considered 'socially' and 'legally' appropriate in one moment and decidedly unlawful in others, critical infrastructure operators are in a tough spot in deciding what measures and technologies to adopt to protect their infrastructures ([34]).

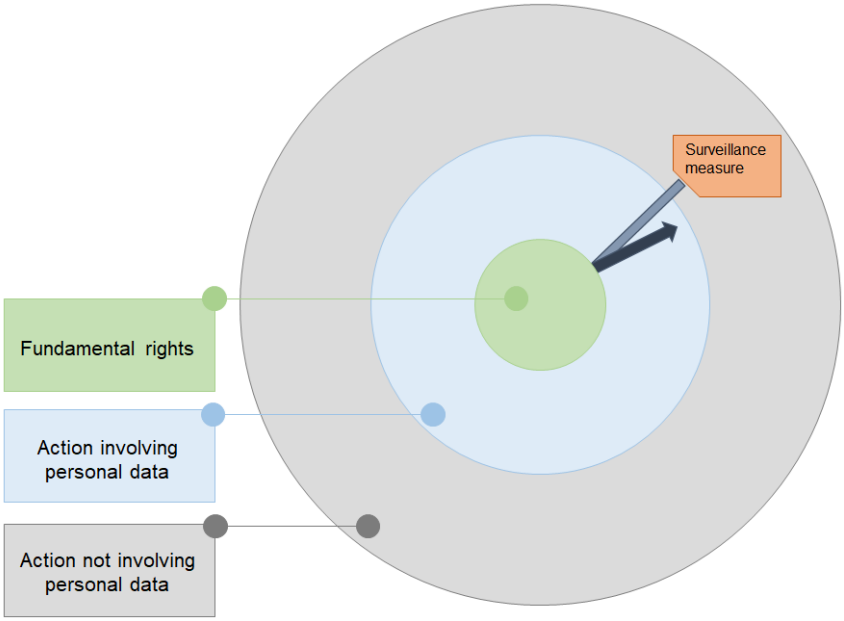
Given the context, understanding how an operator can lawfully implement EWZ and biometric surveillance measures becomes an extremely convoluted legal feat. This is even more complicated since personal data protection falls under the purview of fundamental human rights protection. From a legal standpoint, fundamental rights as enshrined in the Charter of Fundamental Rights of the European Union (hereinafter, also 'the Charter') represent core values for which 'it is necessary to strengthen the protection [...] in the light of changes in society, social progress and scientific and technological developments' ([35]). The Charter, together with the Convention for the Protection of Human Rights and Fundamental Freedoms (hereinafter, also 'the Convention'), represents the pillar of fundamental human rights and freedoms.

According to Article 8 of the Charter, the protection of personal data is a fundamental human right necessary to the preservation and development of the fundamental

([32]) See for instance, Ansley, R., 'Striking a Balance Between Privacy and Security', 28 June 2017, https://www.atlanticcouncil.org/blogs/new-atlanticist/striking-a-balance-between-privacy-and-security (accessed 18 June 2019).
([33]) General data protection regulation, Recital 6.
([34]) The juxtaposition between privacy and security is deeply rooted into the ethical debate as well as the legal one. However, the present analysis does not consider the ethical aspects of the scenario.
([35]) Charter of the Fundamental Rights of the European Union, 2012/C 326/02, Introduction.

freedoms of individuals ([36]). These fundamental rights and freedoms represent the core values of the legal system. Generally, entities acting under regular legal regimes such as the GDPR cannot challenge them, as visualised in Figure 3.

Figure 3. Visualisation of the interaction with fundamental rights



Source: JRC.

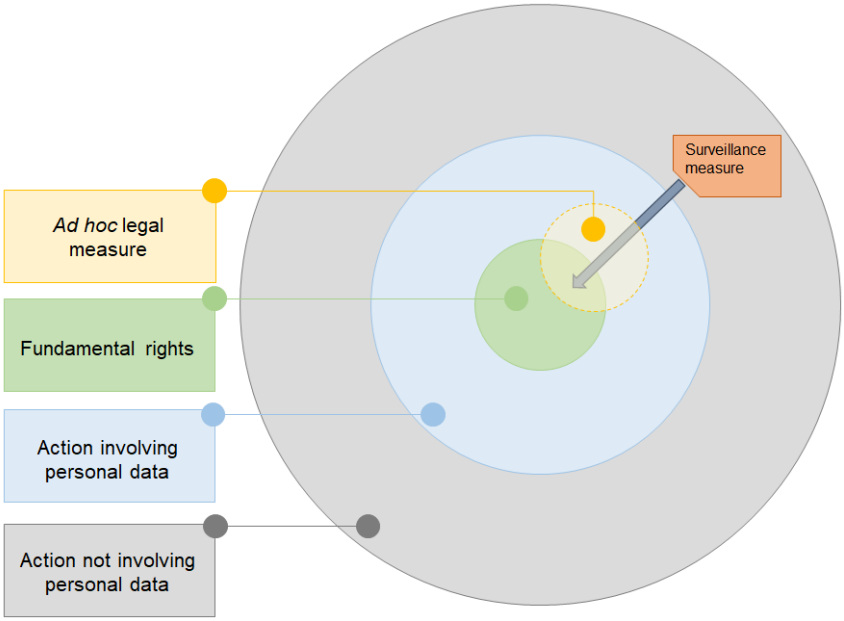
The grey and blue circles represent logical areas in which critical infrastructure operators can design and implement security measures. Some of these measures do not challenge privacy (for instance, an iron gate at the entrance of the premises) and correspond to the grey circle. Others, like the surveillance measures that are part of EWZ, involve the processing of personal data and correspond to the blue circle. According to the circles they interact with, measures are subject to different sets of norms. However, under regular circumstances, they cannot challenge fundamental rights. These are protected by a thicker 'layer' represented by the core regimes enshrined in the Charter and in the Convention.

Even though fundamental rights and freedoms enjoy a special status, regulators made clear that they do not represent absolute rights per se. As stated in Recital 4 of the GDPR, the 'right to the protection of personal data is not an absolute right [and] must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality' ([37]). This notion directly refers to the fact that '[a]ny limitation on the exercise of the rights and freedoms recognised by [the] Charter must be provided for by law and respect the essence of those rights and freedoms' ([38]). The Charter goes on, clarifying that '[s]ubject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others' ([39]). Obviously enough, this does not change the foundational characteristic of the said rights. However, ad hoc legal measures might provide for the appropriate conditions under which certain measures might lawfully

([36]) Charter of the Fundamental Rights of the EU, Art. 8.
([37]) General data protection regulation, Recital 4.
([38]) Charter of the Fundamental Rights of the EU, Art. 52.1.
([39]) Idem.

challenge fundamental rights. This notion is illustrated in Figure 4, which shows the central core of fundamental rights being overridden by an additional layer representing ad hoc norms.

Figure 4. Visualisation of the interaction with fundamental rights and ad hoc legal measures



Source: JRC.

If on one side ad hoc legal measures can open up a completely new lot of opportunities to design and implement security measures, as they grant certain flexibility in challenging fundamental rights, on the other ad hoc legal measures also call for very strict boundaries on how said rights can be challenged.

Even if limitations to the fundamental rights might be admissible when provided for by the law, they have to adhere to the criteria laid down in Article 52 of the Charter. These establish that limitations must respect the essence of the rights, must genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others, and must be necessary and proportionate.

According to this list, the first step is to assess whether 'an accessible and foreseeable law provides for a limitation, and whether the essence of the right is respected, that is, whether the right is in effect emptied of its basic content and the individual cannot exercise the right' ([40]).

Secondly, it should be ensured that the measure meet an objective of general interest. The objective of general interest provides the fundamental ground that has to be analysed in sufficient detail to allow a deep and substantial analysis.

Lastly, the necessity and proportionality of the measures shall be assessed with great care. This means that critical infrastructure operators shall always take these aspects into consideration when designing and implementing security measures.

Assessing necessity and proportionality can be a challenging task, requiring a complex balancing between the purpose of the measures and how the challenges to personal

([40]) European Data Protection Supervisor, Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit, April 2017, p. 4.

rights arising from their employment. The so-called Necessity Toolkit ([41]) and Proportionality Toolkit ([42]) provide useful guidance in this regard. Accordingly, necessity is the criterion against which to assess 'the effectiveness of the measure for the objective pursued and of whether it is less intrusive compared to other options for achieving the same goal' ([43]). In other words, a measure can be considered necessary when it ensures adequate effectiveness in the pursuit of a general interest objective by providing for the least intrusive level possible into the rights of individuals, such as in our case, the right to data protection.

Evaluating the level of intrusiveness is key to understanding necessity. Common interpretation of the legal doctrine by competent authorities such as the EDPS has consistently reiterated that the evaluation shall be performed a priori, before measures are put in place, and should be broad in scope, meaning that a measure can be considered necessary only when all the other possible measures have been exhaustively considered. Intrusiveness has been linked by case law to the possibility to 'allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained, such as everyday habits, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them' ([44]).

It follows that, in the context of EWZ and biometric surveillance, operators 'must always seek the least intrusive means by choosing a non-biometric process, if possible' ([45]). For this reason, critical infrastructure operators requiring biometric surveillance measures shall consider necessity with great care when deciding upon the implementation of said measures.

Proportionality is a general principle that requires measures not to exceed the limitations of a specific right over what is strictly required for them to reach their purpose. It can be said that 'proportionality requires that advantages due to limiting the right are not outweighed by the disadvantages to exercise the right' ([46]). According to recent case law, 'the objective pursued by legislation governing that access must be proportionate to the seriousness of the interference with the fundamental rights in question that that access entails' ([47]). This means that 'serious interference can be justified, in areas of prevention, investigation, detection and prosecution of criminal offences, only by the objective of fighting crime which must also be defined as "serious" ' ([48]). On the other hand, 'when the interference that such access entails is not serious, that access is capable of being justified by the objective of preventing, investigating, detecting and prosecuting criminal offences generally' ([49]).

([41]) European Data Protection Supervisor, Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit, 11 April 2017.
([42]) European Data Protection Supervisor, EDPS Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data, 25 February 2019. Currently, the toolkit is under public consultation.
([43]) European Data Protection Supervisor, Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit, 11 April 2017, p. 5.
([44]) Tele2, §99. This interpretation can be coherently traced data within Ministerio Fiscal, Tele2 and Digital Rights Ireland §27.
([45]) Article 29 Data Protection Working Party, Opinion 3/2012 on developments in biometric technologies, 27 April 2012, p. 11.
([46]) European Data Protection Supervisor, Necessity and Proportionality (https://edps.europa.eu/data-protection/our-work/subjects/necessity-proportionality_en).
([47]) Judgment of the Court (Grand Chamber) of 2 October 2018, REQUEST for a preliminary ruling under Article 267 TFEU from the Audiencia Provincial de Tarragona (Provincial Court, Tarragona, Spain), Case C-207/16 — §55.
([48]) Judgment of the Court (Grand Chamber) of 2 October 2018, REQUEST for a preliminary ruling under Article 267 TFEU from the Audiencia Provincial de Tarragona (Provincial Court, Tarragona, Spain), Case C-207/16 — §56.
([49]) Judgment of the Court (Grand Chamber) of 2 October 2018, REQUEST for a preliminary ruling under Article 267 TFEU from the Audiencia Provincial de Tarragona (Provincial Court, Tarragona, Spain), Case C-207/16 — §57.

The principles of necessity and proportionality are not firmly distinguished, and they often overlap ([50]). This makes it difficult to establish a standardised approach to evaluating them. Moreover, the complexities of the current operational and social environments have a great influence on the outcomes of necessity and proportionality evaluations. These complexities, which are still relatively unexplored, originate from an ever-changing risk scenario that, due to the interconnected nature of the world and the near-instantaneous information sharing speed, can generate devastating ripple effects ([51]).

7.3 Policy options

— In the context of the continuous friction between privacy and security, policymakers and national leaders have the hard role of defining the normative context in which critical infrastructure operators act. This section presents three possible options policymakers and national leaders can consider as potential approaches. Said options range from a very low involvement in how critical infrastructure operators decide to protect their infrastructure, up to a direct intervention by means of law. The options are intended to promote the balancing between privacy and security in relation to the implementation of EWZ and biometric surveillance measures for critical infrastructure protection.

7.3.1 Option 1: Private autonomy

The first policy option (Table 4) establishes that critical infrastructure operators autonomously decide whether to implement EWZ and biometric surveillance measures. This option, which reflects the current situation, provides critical infrastructure operators with a great deal of flexibility, and builds on the premise that most of the critical infrastructures are operated by private entities under free-market conditions ([52]).

Table 4. Private autonomy option

Pros	**Cons**
Maximum degree of flexibility for CI operators	Might not ensure an adequate level of protection for citizens
CI operators can quickly adapt to changes in the operational environment	Does not promote standardisation of approaches
Very low burden on public institutions and regulators	CI operators might sustain extra effort for the management of contractual agreements with other operators

Source: JRC.

According to this policy option, policymakers, governments and regulators do not proactively pursue the adoption of said measures with operators. Therefore, the implementation of EWZ and biometric surveillance measures is only subject to the cost–benefit analyses of the critical infrastructure operators. Obviously, this does not exempt

([50]) See European Data Protection Supervisor, Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit, 11 April 2017, p. 6.

([51]) One of the most prominent cases on the effect of this information sharing speed is what happened in 2013, following a false message shared by a hacked twitter account of the Associated Press. For more information, real-life effects, Greenfield, R., Look What the Hacked AP Tweet About White House Bombs Did to the Market, The Atlantic, 23 April 2013, https://www.theatlantic.com/technology/archive/2013/04/hacked-ap-tweet-white-house-bombs-stock-market/315992 (accessed 18 June 2019).

([52]) Srimoolanathan, B. (2014), 'Adopting a holistic approach to protecting critical infrastructure', *Jane's 360*, https://www.janes.com/article/39495/adopting-a-holistic-approach-to-protecting-critical-infrastructure-es14e3 (accessed 18 June 2019).

them from complying with the relevant legal obligations. They will still need to, whenever required by the law, perform data protection impact assessments (DPIA), undergo prior consultation with data protection authorities, clearly establish roles and responsibilities, etc.

The option presents a number of clear advantages. First, critical infrastructure operators enjoy a tremendous flexibility in their decision-making process. They can evaluate the benefits of implementing EWZ and biometric surveillance without heavy constraints and, therefore, adopt the solution that best suits their needs ([53]). The second advantage strictly relates to the first one. Indeed, when operators can rely on a high degree of flexibility, they will also be able to take and implement decisions in a timely manner. This effectiveness creates benefits both for operators and for citizens, as the former will be able to adapt quickly to the situation at hand, ensuring a better security in the face of a complex and ever-changing threat scenario. Lastly, public institutions gain benefit even from this option, since they have to sustain a low burden.

Policy option one, however, also brings a number of disadvantages. First, since the implementation of EWZ and biometric surveillance measures is subject only to the cost–benefit considerations of the operators, the level of security for the citizens might not be adequately addressed. Moreover, different operators might come up with different cost–benefit considerations, leading to a heterogeneous approach to critical infrastructure protection, which will make standardisation very difficult and might undermine public security as a whole. Lastly, this option might create a complex legal jungle for operators, especially in the context of cross-border federated systems. Each integration with the security measures of other infrastructures will require a formal agreement. The higher the number of the partnerships and federations, the higher the number of the agreements and, therefore, the complexity in managing them. In addition, different operators might be subject to different legal regimes, especially when it comes to aspects such as civil law, fiscal law, labour law, etc. The sheer amount of work and economic resources necessary to manage such a complex network of agreements could result in a severe loss of effectiveness or in discouraging the adoption of federated approaches.

7.3.2 Option 2: Code of conduct

Compared to option number one and number three, the second policy option marks a middle ground, and aims at being the most balanced approach cocerning the level of interference into the activities of critical infrastructure operators. This option consists in the adoption by 'associations and other bodies representing categories [of operator]' ([54]) of a Code of Conduct, as made possible by the GDPR. This approach represents relatively uncharted territory, since no codes of conduct have been adopted yet at the European level ([55]).

The aim of codes of conduct is to 'contribute to the proper application of [the GDPR], taking account of the specific features of the various processing sectors' ([56]). In other words, codes of conduct 'provide detailed guidance which tailors legal requirement to specific sectors and furthers the transparency of processing activities' ([57]), representing 'a practical, potentially cost effective and meaningful method to achieve greater levels of consistency of protection for data protection rights' ([58]).

([53]) Obviously, this flexibility is subject to the minimum level of compliance required by the law. The stricter the requirements, the lower the flexibility for operators.
([54]) General data protection regulation, Art. 40.2.
([55]) To this date, the Register for Codes of Conduct, amendments and extensions of the European Data Protection Board, does not count any entry. See https://edpb.europa.eu/our-work-tools/accountability-tools/register-codes-conduct-amendments-and-extensions-art-4011_en
([56]) General data protection regulation, Art. 40.1.
([57]) European Union Agency for Fundamental Rights, *Handbook on European Data Protection Law*, 2018 Edition, p. 182.
([58]) European Data Protection Board, Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679, 12 February 2019, p. 4.

In the context of this research, the aim of codes of conduct should be to clarify certain aspects of data protection in the context of critical infrastructure protection and EWZ management. This could also promote the adoption of EWZ measures in a coordinated and controlled way. Moreover, codes of conduct focused on critical infrastructure protection could be cross-sector, leveraging on the varied expertise of the different members of different to 'favour finding solutions which are practical and, therefore, likely to be followed' ([59]).

Table 5. Code of conduct option

Pros	**Cons**
High degree of flexibility, but also interoperability	Does not necessarily promote standardisation of approaches due to the voluntary adoption of the Code of Conduct by CI operators
Promote the standardisation of commonly agreed approaches	Might bring additional costs for CI operators
Since they are public, they promote transparency and accountability	

Source: JRC.

Codes of conduct dealing with CIP and EWZ should touch upon certain fundamental aspects. First, they should propose an approach for addressing roles, responsibilities, and data protection obligations related to the different critical infrastructure operators participating into an EWZ. Second, they should detail how to perform DPIA. Third, they should provide guidelines concerning how to engage competent supervisory authorities during the design and implementation processes of the EWZ. This will be helpful for critical infrastructure operators since, due to the particular invasiveness of such measures, it is likely they will have to involve supervisory authorities for prior consultation.

Codes of conduct should also provide for special bodies tasked with monitoring compliance among the adopters. These bodies shall be accredited to the relevant supervisory authority ([60]), shall act independently, shall demonstrate expertise on the matters regulated by the code, and shall have transparent procedures for handling complaints about infringements ([61]). The competent supervisory authority is also responsible for controlling the accredited body, and shall have the power to revoke the accreditation when the necessary criteria is not satisfied any more ([62]).

The second policy option carries many important advantages. First, operators could potentially be able to enjoy a considerable degree of autonomy. Indeed, codes of conduct should not be seen as sets of mandatory requirements. According to different situations, and considering the model adopted for the code (which can make it stricter or softer), there should be enough room for a critical infrastructure operator to define a personalised approach to the implementation of the provision of the code of conduct. Second, the adoption of codes of conduct can promote harmonisation among EWZ implementation approaches, as non-binding codes of conduct might became de facto standards over time. On top of that, the GDPR gives the Commission the power to decide that a specific code has a general validity within the Union ([63]), further reinforcing the

([59]) European Union Agency for Fundamental Rights, *Handbook on European Data Protection Law*, 2018 Edition, pp. 181-182.
([60]) General data protection regulation, Art. 40.4.
([61]) General data protection regulation, Art. 41.2.
([62]) General data protection regulation, Art. 41.5.
([63]) General data protection regulation, Art. 40.9.

harmonising effects of the code of conduct ([64]). Third, codes of conduct may be used as evidence that an operator is fully committed to data protection principles. Given the fact that the adherence to specific code of conducts can, and should, be made public, citizens will be able to check which infrastructure operator decided to adopt EWZ to protect the infrastructure, and how the EWZ has been implemented ([65]).

Obviously, since codes of conduct are voluntary, they do not necessarily ensure the emergence of homogeneity across critical infrastructure operators' approaches. For instance, operators might simply decide not to adopt such codes. Various elements can work to the detriment of their general adoption. First, critical infrastructure operators might not consider them authoritative enough. This risk can be mitigated by involving recognised experts during the drafting process. Second, the costs connected to maintaining compliance might be too high when compared to the potential benefits. This holds particularly true when codes of conduct lack clarity concerning their goals and are not sufficiently detailed.

7.3.3 Option 3: Legal obligation

The third option entails that the implementation of EWZ will be regulated by means of a legal measure. In this scenario, critical infrastructure operators will be required to comply with a set of obligations when implementing an EWZ approach. Some obligations could provide for the situation when the implementation of the EWZ is not up to the discretion of the critical infrastructure operator, but is mandatory. Obviously, this option has the higher level of interference in the activities of critical infrastructure operators.

Table 6. Legal obligation option

Pros	**Cons**
Policymakers and legislators are able to directly address the specific areas they deem to be critical	Might promote among citizens a feeling of being excessively under control
Interaction between CI operators will be facilitated by public institutions	Brings additional costs for the stakeholder
Promotes public–private partnerships	Since processing operations deriving from a legal obligation on EWZ shall be grounded on Dir. 2016/680, a jeopardised implementation among Member States might generate additional costs deriving from legal uncertainty

Source: JRC.

In contrast to the other scenarios, this option envisages a considerable involvement of the regulators ([66]). Given the potential level of interference in the rights and freedoms of individuals as well, regulators shall take great care during the legislative process, in order

([64]) Once a code has been drafted, it must be submitted to the competent supervisory authority before being adopted. In the case of codes applicable to processing activities within several Member States, the Data Protection Authority shall ask for the opinion of the European Data Protection Board before the approval, in compliance with the consistency mechanism. For more information see general data protection regulation, Art. 63 and subsequent.

([65]) WP7 advocates for including, in the code of conduct, the lists of critical infrastructures running EWZ. Publishing such a list is instrumental in building transparency with citizens, and public awareness.

([66]) This policy option reflects the 'ad hoc legal measure' scenario already seen in section 2.

to achieve a fair balance between opposite interests ([67]) and 'do not go beyond what is necessary in a democratic society' ([68]).

European Union case law already provides for some guidance ([69]) upon which the WP29 has been able to identify the so-called 'European Essential Guarantees' ([70]). According to the WP29, duly taking into account all of the four guarantees should help regulators in striking a fair balance between privacy and security when drafting the legislative measure for EWZ implementation. The following boxes describe the main elements for each of the guarantees.

Box 1. Guarantee A — Processing should be based on clear, precise and accessible rules

Every interference on fundamental rights 'needs to be in accordance with the law' ([71]). This means that every processing impacting on said rights must be based on a 'precise, clear and accessible legal basis' ([72]).

Concerning the fundamental right to data protection, jurisprudence identified potential legal bases in 'the nature of the offences which may give rise to an interception or surveillance order, a definition of the categories of people that might be subject to surveillance, a limit on the duration of the measure, the procedure to be followed for examining, using and storing the data obtained, and the precautions to be taken when communicating the data to other parties' ([73]), detailing the procedure for allowing access by competent authorities ([74]).

It is close to a Guarantee. it must be assessed whether 'an accessible and foreseeable law provides for a limitation, and whether the essence of the right is respected, that is, whether the right is in effect emptied of its basic content and the individual cannot exercise the right' ([75]).

Secondly, the measure must meet an objective of general interest. The objective of general interest provides the fundamental ground that has to be analysed in sufficient detail to allow a deep and substantial analysis. With regard to EWZ, it has to be noted that the protection of critical infrastructure relies upon a general interest of 'protection of such infrastructures in order to contribute to the protection of people' ([76]), with a clear reference to the fundamental right to liberty and security ([77]).

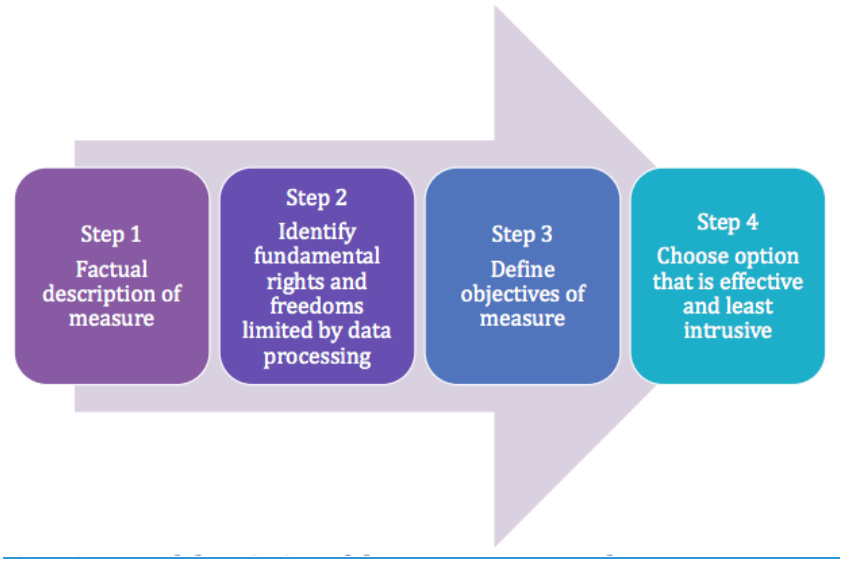
([67]) As described in section 2.
([68]) Article 29 Data Protection Working Party, Working Document 01/2016 on the justification of interferences with the fundamental rights to privacy and data protection through surveillance measures when transferring personal data (European Essential Guarantees), 13 April 2016, p. 7.
([69]) The landmark ruling that gave rise to a growing discussion is *Schrems* v *Data Protection Commissioner of Ireland*, Court of Justice of the European Union, 6 October 2015, Case C-362/14.
([70]) Article 29, Data Protection Working Party, Working Document 01/2016, cit., p. 9. Essential Guarantees are primarily based on the jurisprudence of the CJEU and the ECtHR regarding limits to power of public authorities accessing and retaining personal data and contents of electronic communications. However, the rules outlined here can be generalised in order to propose a correct legislative measure for the implementation of measures such as EWZ.
([71]) Article 29, Data Protection Working Party, Working Document 01/2016, cit., p. 13.
([72]) *Malone* v *United Kingdom*, European Court of Human Rights, 2 August 1984, Application no. 8691/79, §§65, 66, 70; *Zakharov* v *Russia*, European Court of Human Rights, 4 December 2015, Application no. 47143/06, §229.
([73]) Article 29 Data Protection Working Party, Working Document 01/2016, cit., p. 7.
([74]) *Digital Rights Ireland* v *Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, The Commissioner of the Garda Síochána, Ireland and the Attorney General, and Kärntner Landesregierung, Michael Seitlinger, Christof Tschohl and Others*, Court of Justice of the European Union, 8 April 2014, Joined Cases C-293/12 and C-594/12, §61.
([75]) European Data Protection Supervisor, Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit, 11 April 2017, p. 4.
([76]) Critical infrastructure directive, Art. 1.
([77]) Charter of Fundamental Rights of the European Union, Art. 1.

Box 2. Guarantee B — Necessity and proportionality with regard to the legitimate objectives pursued need to be demonstrated

Considering that 'any data processing by government authorities is, by definition, an interference with the right to privacy and data protection' ([78]), a legislative measure can only be justifiable when necessary and proportionate in relation to a legitimate objective. Specific 'differentiation, limitation or exception' and 'objective criterion by which to determine the limits of the access (…) and their subsequent use' ([79]) shall be considered while designing the legal measure. Moreover, the interference 'must be subjected to very close scrutiny both on the domestic level and under the Convention' ([80]).

It is worth noting that guidelines provided by the EDPS on the necessity principle ([81]) have provided further guidance on how to correctly address the necessity principle. Steps are summarised within the process outlined in Figure 5 below.

Figure 5. Guidelines to address the necessity principle



Source: JRC.

Firstly, a detailed description of the envisaged measure is not only a prerequisite to the necessity test, but it also helps in demonstrating compliance with the first condition of Article 52(1) of the Charter and with Guarantee A.

Secondly, an in-depth analysis of the rights and freedoms that are limited by the data processing shall be conducted. Regulators shall consider different levels of invasiveness and the fact that 'distinct processing operations or set of operations (i.e. collection and another operation, such as retention or transfer or access to data) may constitute separate limitations on the right to the protection of personal data and, where applicable, with the right to respect for private life' ([82]).

Thirdly, the measure must genuinely meet:

([78]) Article 29, Data Protection Working Party, Working Document 01/2016 and CJEU, Digital Rights Ireland, §36.
([79]) CJEU, Digital Rights Ireland, §§57 and 60.
([80]) *Szábo and Vissy* v *Hungary*, European Court of Human Rights, 12 January 2016, Application no. 37138/14, §§68-70.
([81]) EDPS necessity toolkit — a dedicated guideline on the proportionality principle is under public consultation at the moment of the release of this document.
([82]) European Data Protection Supervisor, Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit, 11 April 2017, p. 11.

— an objective of general interest recognised by the Union: 'the Union's objectives of general interest include for instance the general objectives mentioned in Articles 3 or 4(2) TEU and other interests protected by specific provisions of the treaties, as well as interpreted in the case law of the Court of Justice' ([83]); or

— the need to protect the rights and freedoms of others: 'the right to the protection of personal data may need to be balanced with other rights, such as the protection of intellectual property rights and the rights to an effective remedy, to freedom of expression and to carry out a business' ([84]).

The problem to be addressed by the proposed norm 'should be concrete and not merely hypothetical' ([85]), with practical evidence as 'facts or statistical data, and should allow scientific verification and convincingly support the existence of the problem' ([86]). For the ECtHR, a limitation will be considered 'necessary in a democratic society' for a legitimate aim 'if it answers a pressing social need' ([87]). In other words, 'the problem to be addressed must not only be real, present or imminent, but critical for the functioning of the society' ([88]).

Lastly, 'the chosen measure should also be effective and less intrusive than other options for achieving the same goal' ([89]). In other words, this means that the measure should be genuinely effective. Not everything that 'might prove to be useful' for a certain purpose is 'desirable or can be considered as a necessary measure in a democratic society' ([90]). In order to correctly enforce this step, each particular aspect of the measure shall be subject to a strict necessity test with a clear explanation of the underlying reasons ([91]).

Within the context of EWZ, it is worth noting that doctrine is consistent in underpinning the high interference of processing activities involving biometric data with the fundamental right to the protection of personal data. Furthermore, legal cases have repeatedly stated that 'serious interference can be justified […] only by the objective of fighting crime which must also be defined as serious' ([92]). More specifically, this principle could be transposed within the EWZ domain, stating that biometric features shall be limited only to serious threat to public security or imminent attacks to a critical infrastructure. What is more, public authorities' access to such data shall be limited only for fighting serious crime as defined by relevant laws and regulations within European or Member States laws.

([83]) European Data Protection Supervisor, Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit, 11 April 2017, p. 14.
([84]) European Data Protection Supervisor, Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit, 11 April 2017, p. 14.
([85]) European Data Protection Supervisor, Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit, 11 April 2017, p. 15.
([86]) European Data Protection Supervisor, Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit, 11 April 2017, p. 15.
([87]) *S. and Marper* v *United Kingdom* — European Court of Human Rights, 4 December 2008 — Applications nos. 30562/04 and 30566/04.
([88]) European Data Protection Supervisor, Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit, 11 April 2017, p. 15.
([89]) European Data Protection Supervisor, Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit, 11 April 2017, p. 17.
([90]) Article 29 Working Party, Opinion 9/2004 on a draft Framework Decision on the storage of data processed and retained for the purpose of providing electronic public communications services, WP 99, 9.11.2004.
([91]) European Data Protection Supervisor, Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit, 11 April 2017, p. 17.
([92]) Ministerio Fiscal, §56.

Box 3. Guarantee C — An independent oversight mechanism should exist

A consolidated position of the ECtHR from the 1970s is that 'any interference with the right to privacy and data protection should be subject to an effective, independent and impartial oversight system that must be provided for either by a judge or by another independent body' ([93]). This has been considered to be 'an essential component of the protection of individuals with regard to the processing of personal data' ([94]). Oversight mechanisms 'can take place at various stages during the lifecycle of a data processing operation' ([95]), before, during or after it.

It is important to consider that 'In a field where abuse is potentially so easy in individual cases and could have such harmful consequences for democratic society as a whole, it is in principle desirable to entrust supervisory control to a judge, judicial control offering the best guarantees of independence, impartiality and a proper procedure' ([96]). It follows that a prior review can be carried out by a court or by an independent administrative body 'whose decision seeks to limit access to the data and their use to what is strictly necessary for the purpose of attaining the objective pursued and which intervenes following a reasoned request of those authorities submitted within the framework of procedures of prevention, detection or criminal prosecutions' ([97]).

The Strasbourg Court has expressed its preference for a judicial oversight for the cases of competent authorities accessing communication data. However, it should not be excluded that another body can be responsible, 'as long as it is sufficiently independent from the executive' ([98]), as much as a Data Protection Authority should be according to the data protection legal framework ([99]).

Box 4. Guarantee D — Effective remedies need to be available to the individual

The data subject 'must have an effective remedy to satisfy his/her rights when (s)he has the idea they are not respected' ([100]). In fact, 'legislation not providing for any possibility for an individual to pursue legal remedies in order to have access to personal data relating to him, or to obtain the rectification or erasure of such data, does not respect the essence of the fundamental right to effective judicial protection, as enshrined in Article 47 of the Charter' ([101]). Even though the Strasbourg Court expects that the body providing the effective remedy is a judicial body ([102]), this does not necessarily need to be a judicial authority ([103]).

In addition to the Essential Guarantees as complemented by the words made by the EDPS, it should be noted that specific legislative measures will not exempt critical infrastructure operators from their main data protection obligations. In particular, due to the nature of EWZ and the intense use of biometric data, it is likely that prior consultation with data protection authorities will be required. Given the mandatory nature that surveillance measures hold in this scenario, data protection authorities will be crucial. Their role in this regard can be seen as twofold. On one side, they will be engaged very often in prior consultations. This will also nudge operators toward a very strict analysis of necessity and proportionality principles as well as on building and demonstrating compliance while assessing specific risks for rights and freedoms for data

([93]) Article 29 Data Protection Working Party, Working Document 01/2016 and *Klass and others* v *Germany*, European Court of Human Rights, 6 September 1978 Application no. 5029/71 §51.
([94]) CJEU, *Commission* v *Germany*, §23.
([95]) ECtHR, *Klass* §§55-56; ECtHR, *Zakharov*, §233.
([96]) ECtHR, *Zakharov*, §233.
([97]) CJEU, *Digital Rights Ireland*, §62.
([98]) ECtHR, *Zakharov*, §258.
([99]) Art. 52, GDPR and Art. 42, LED.
([100]) Article 29 Data Protection Working Party, Working Document 01/2016, p. 11.
([101]) CJEU, *Schrems* §95.
([102]) ECtHR, *Kennedy* §167.
([103]) ECtHR, *Klass* §67.

subject within each specific situation. On the other, given their specific experience and knowledge, they will be in the best position to evaluate the conformity of the legal measure mandating the implementation of the surveillance measure, also becoming contact points for facilitating interaction among CI operators. Lastly, public–private partnership shall be encouraged within this approach in order to reach the intended purpose in a more efficient way.

Obviously enough, resorting to modification of the applicable legal regimes introduces a number of side effects. First, citizens might perceive this as an excessive regulatory interference, and might claim a loss of independence and privacy. Since regulators will define the situations in which EWZ and biometric surveillance measures will have to be implemented, citizens might feel that, when confronted with such situations, they are left without any guarantee of privacy. Government might be seen, is such a scenario, as absolute controllers, fuelling the mistrust of their own citizens. Secondly, the lack of flexibility of this approach might implicate additional costs for all the stakeholders. On one side, critical infrastructure operators will have to implement EWZ and biometric surveillance measures despite any cost–benefit analysis, which for operators might return a result suggesting not to implement the measures. On the other side, regulators and governments will have to keep the legal framework up to date. This might turn out to be a considerably complex and costly feat, given the pace in which the operation scenario changes. Lastly, since this option represents a novel approach, there are no previous cases of application. Therefore, since no prior guidelines are available, adopting an adequate set of norms might end up being a long and costly process.

7.4 Design requirements

Currently, it is not possible to define the most appropriate balance between privacy and security. Different sociopolitical cultures and environments may lead, across Europe and across the globe, to different interpretations on how to best achieve this. However, while the desired outcome is hard to define, it is still possible to bring clarity on the best tools that stakeholders can use while designing a possible EWZ solution.

This section introduces a set of high-level design requirements that could be considered while designing an EWZ, and provides for practical guidance to critical infrastructure operators in relation to the design, configuration, installation and management of the technical solution required within the EWZ.

It is important to notice that the assessment of the design requirements cannot be generalised and shall be performed on a case-by-case basis. In order to do this adequately, critical infrastructure operators shall implement appropriate technical and organisational measures to integrate the data protection safeguards and protect the fundamental rights of the individuals whose data are processed ([104]).

As already said, the Necessity and Proportionality principles represent pivotal elements that critical infrastructure operators need to consider when implementing EWZ approaches and, in particular, when translating the design requirements into specific technical or organisational measures. Effectiveness shall be the 'guiding light' of the process, in order to ensure that fundamental rights are duly respected. In other words, it is not enough for an operator to reach a simple compliance level. The data protection discipline requires them to adopt effective methods to reach the expected outcome of single requirements.

Moreover, 'risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing' ([105]) shall also be taken into consideration, both during the design and the deployment phases ([106]). At this stage, it is worth noting that the

([104]) This approach is coherent with the Data Protection by Design approach defined within Article 25, GDPR and Article 20, LED. For a more detailed analysis on the matter, see European Data Protection Supervisor, Preliminary Opinion on privacy by design, Opinion 5/2018, 31 May 2018.

([105]) Art. 25, GDPR.

([106]) For more information regarding this aspect, see second deliverable.

same requirement might result in a different application and implementation within diverse risks scenarios. Given the complexity of the subject at hand, the following guidelines hopes to bring clarity by providing a high-level general approach to design requirements.

7.4.1 Lawfulness and fairness

Within the data protection legal framework, 'lawfulness' and 'fairness' are very broad principles defining the 'relationship between the controller and the data subject' ([107]). According to these principles, processing operations shall comply with all of the applicable norms. In the context of data protection, processing operations shall comply with one of the lawful grounds set by the GDPR and the law enforcement directive. Article 6 of the GDPR and Article 8 of the law enforcement directive deal with 'regular' data, while Article 9 of the GDPR and Article 10 of the law enforcement directive deal with 'special categories' of data. Moreover, when automated decision-making process is carried out, there are more stringent legal requirements, as defined by Article 22 of the GDPR and Article 11 of the law enforcement directive.

7.4.1.1 Data processing not involving special categories of data

The following boxes provide an overview of the legal grounds set by the GDPR.

Box 5. Legitimate interest

Legitimate interest ([108]) can be found within Article 6.1.d of the GDPR. Accordingly, personal data may be processed lawfully when the processing is necessary to pursue a legitimate interest. The controller, the third parties, or parties to whom the data are disclosed — except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject — are all entitled to pursue a legitimate interest. Moreover, according to Recital 47, the existence of a legitimate interest must be assessed in each specific case.

If the legitimate interests of the controller are identified, than a balancing exercise must be conducted between the interests of the data subject against those of the data controller. In order to reach a balance of interests, the controller shall assess necessity and proportionality with particular care. On the one side, such an assessment helps the controllers to monitor their compliance to the applicable regime. On the other, it can help to demonstrate the existence of a valid legitimate interest in case of objection by a data subject.

It is of utmost importance to consider that whenever personal data is processed under a legitimate interest, the individual has the right to object to the processing ([109]). In that case, the controller must stop the processing, unless he demonstrates compelling legitimate grounds to continue it.

Even if, in the context of critical infrastructure protection, there is a clear legitimate interest related to the protection of critical infrastructure, this does not constitute a waiver for data protection obligations. A deep analysis has to be performed by CI operators in order to understand in a specific situation whether a public and legitimate interest for security should prevail on data subject right. This is strictly related to the specific invasiveness of the adopted technological solution and the risks for the rights and freedoms of data subject that might generate. Interests that can be considered as valuable for a balancing act are linked to liberty, security and freedom of movement.

([107]) European Union Agency for Fundamental Rights, *Handbook on European Data Protection Law*, 2018 Edition, p. 118.

([108]) For a broad overview on the notion of legitimate interest see Article 29 Working Party, Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, WP 217, 9 April 2014.

([109]) As stated in the general data protection regulation, Art. 21.1.

Box 6. Public interest

Article 6.1.e of the GDPR defines the concept of public interest. Accordingly, a data processing can be lawful when it 'is necessary for the performance of a task carried out in the public interest or in the exercise of official authority' ([110]). However, the GDPR also says that '[w]here processing is carried out in accordance with a legal obligation to which the controller is subject or where processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority, the processing should have a basis in Union or Member State law' ([111]).

The idea of finding a legal basis within the Union or a Member State should be understood in a broad sense. Even if specific legal grounds are necessary for a lawful processing operation, it is not required that each single norm has to address a single kind of processing operation. Said law shall outline the mandatory characteristics for different kinds of processing operations and define the activities that data controllers will have to perform in the public interest or in the exercise of official authority.

Within the context of critical infrastructure protection, the CI directive might be seen as a viable ground for processing personal data under the notion of public interest. Indeed, Article 2.1.e of the GDPR defines 'protection' in a broad sense, as 'all activities aimed at ensuring the functionality, continuity and integrity of critical infrastructures in order to deter, mitigate and neutralise a threat, risk or vulnerability' ([112]). This means that the CI directive can be considered as a valuable base for processing operations grounded on public interest.

Box 7. Vital interest

Article 6.1.d of the GDPR defines the concept of vital interest. Accordingly, the processing of personal data is lawful when it 'is necessary in order to protect the vital interests of the data subject or of another person'.

Recital 45 of the GDPR says that vital interest can be invoked as a last resort, only when the processing 'cannot be manifestly based on another legal basis' ([113]). According to WP29, the provision shall be interpreted in a restrictive manner, referring to 'questions of life and death, or at the very least, threats that pose a risk of injury or other damage to the health of the data subject' ([114]).

In the context of critical infrastructure protection, this legal ground could be invoked only when an attack is ongoing or is imminent within the EWZ area.

Box 8. Legal obligation

Article 7.1.c of the GDPR provides a legal ground in the situation where 'processing is necessary for compliance with a legal obligation to which the controller is subject' ([115]).

While this provision might seem to overlap with the concept of public interest, processing operations have to be 'strictly delimited' ([116]) by provisions set out within legal obligation to be applied on CI by operators.

Moreover, the law must fulfil all relevant conditions to make the obligation valid and binding, and must also comply with data protection law, including the requirements of necessity, proportionality and purpose limitation ([117]).

([110]) General data protection regulation, Art. 6.1.e.
([111]) General data protection regulation, Recital 45.
([112]) Critical infrastructure directive, Art. 2.1.e.
([113]) General data protection regulation, Recital 46.
([114]) Article 29 Working Party, Opinion 06/2014, p. 21.
([115]) General data protection regulation, Art. 7.1.c.
([116]) Article 29 Working Party, Opinion 06/2014, p. 20.

While a processing operation under the GDPR can be based on a different set of legal grounds, operations based on the law enforcement directive can only be based on a legal obligation 'based on Union or Member State law' ([118]).

7.4.1.2 Data processing involving special categories of data

Special categories of data are broadly defined as data that, when misused, 'could create significant risks to the fundamental rights and freedoms' ([119]). Biometric data, which are at the core of EWZ, fall into this category. However, not all of the processing operations within EWZ rely on this kind of data. This requires that critical infrastructure operators have to take into account different legal grounds for their processing operations, distinguishing between those relying on special categories and those relying only on standard data. Article 10 of the law enforcement directive provides for a very stringent legal regime related to this kind of data while the GDPR, in principle, prohibits the processing of such data as per Article 9.1. However, Article 9.2 of the GDPR provides for an exhaustive list of exemptions that might provide for legal grounds for processing.

The following boxes provides for feasible legal grounds for personal data processing operations involving special categories of data.

Box 9. Vital interest

All of the elements already described for the vital interest in the context of data processing not involving special categories of data, also apply in this case both in the case of a processing operation grounded on the GDPR and on the law enforcement directive.

Box 10. Legal obligation

All of the elements already described for the legal obligation in the context of data processing not involving special categories of data, also apply in this case both in case of processing operation grounded on the GDPR and on the law enforcement directive.

Box 11. Substantial public interest

According to Article 9.2.g of the GDPR, processing of sensitive data can be lawfully processed when necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

It is important to underline the fact that the legal regime for sensitive data does not have a clear interpretation yet by the academia nor by courts. Within the context of CIP, the notion of public interest can be found within the increased need for protection of citizens as the main goal aimed by the CI directive.

A specific requirement enshrined in Article 10 of the law enforcement directive is of vital importance in order to design lawful processing activities. That is, special categories of data have to be 'strictly necessary' ([120]). According to WP29, this is 'a call to pay particular attention to the necessity principle in the context of processing special categories of data, as well as to foresee precise and particularly solid justifications for the

([117]) Article 29 Working Party, Opinion 06/2014, p. 20.
([118]) Law enforcement directive, Art. 8.1.
([119]) General data protection regulation, Recital 51.
([120]) Law enforcement directive, Art. 10.

processing of such data' ([121]). Moreover, such data have to be 'subject to appropriate safeguards for the rights and freedoms of the data subject' ([122]) in order to avoid discrimination. Recital 37 of the law enforcement directive provides for some examples as 'possibility to collect those data only in connection with other data on the natural person concerned, the possibility to secure the data collected adequately, stricter rules on the access of staff of the competent authority to the data and the prohibition of transmission of those data'.

7.4.1.3 Data processing involving automated individual decision-making and profiling

When so-called 'automated decisions' and 'profiling' are employed, critical infrastructure operators shall take into account a different and more stringent legal regime.

According to Article 22 of the GDPR 'the data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her' ([123]). Article 11 of the law enforcement directive increases the protection for data subjects in such situations. Here, automated decision-making shall be 'authorised by Union or Member State law to which the controller is subject and which provides appropriate safeguards for the rights and freedoms of the data subject, at least the right to obtain human intervention on the part of the controller' ([124]). Since the legal text distinguishes between automated decisions and profiling, it is worth introducing these as distinct concepts.

Under the GDP, profiling is defined as 'any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict personal preferences, interests, reliability, behaviour, location or movements' ([125]). The WP29 further develops on this, stating that '[p]rofiling is a procedure [...] often used to make predictions about people, using data from various sources to infer something about an individual, based on the qualities of others who appear statistically similar' ([126]).

Automated decisions, on the other hand, are decisions 'taken using personal data processed solely by automatic means without any human intervention' ([127]). They have 'a different scope and may partially overlap with or result from profiling' ([128]).

To understand whether EWZ entails such processing operations, the concepts of 'Legal' or 'similarly significant effects' have to be duly understood as core elements. Even though neither the GDPR nor the law enforcement directive define these concepts, the wording makes it clear that only serious impactful effects will be covered by this special legal regime.

According to WP29, a legal effect manifests when the decision following solely automated processing affects someone's legal rights ([129]). The Working Party provides for very clear examples, such as the cancellation of a contract. In the context of EWZ, a legal effect could be the limitation of the freedom of movement of the subject. Moreover, even if a decision-making process does not have an effect on people's legal rights, 'it could still fall within the scope of Article 22 if it produces an effect that is equivalent or similarly

([121]) Article 29 Working Party, Opinion on some key issues of the Law Enforcement Directive (EU 2016/680), WP 258, 29 November 2017.
([122]) Law enforcement directive, Art. 10.
([123]) General data protection regulation, Art. 22.
([124]) Law enforcement directive, Art. 11.1.
([125]) General data protection regulation, Art. 4.4 and law enforcement directive, Art. 3.4.
([126]) Article 29, Working Party, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, WP 251rev.01, adopted on 3 October 2017, as last Revised and Adopted on 6 February 2018, 29 November 2017.
([127]) European Union Agency for Fundamental Rights, *Handbook on European Data Protection Law*, 2018 Edition, p. 223.
([128]) Article 29 Working Party, Guidelines on Automated individual decision-making, cit.
([129]) Article 29 Working Party, Guidelines on Automated individual decision-making, p. 21.

significant in its impact […]; have a prolonged or permanent impact on the data subject; or at its most extreme, lead to the exclusion or discrimination of individuals' ([130]). This represents the essence of the 'similarly significant effects' principle.

In order to lawfully implement automated decision-making processes within an EWZ approach the only feasible ground is a 'Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests' ([131]). This shall also provide for 'at least the right to obtain human intervention on the part of the controller' ([132]). Recital 38 of the law enforcement directive describes human intervention as a means 'to express his or her point of view, to obtain an explanation of the decision reached after such assessment or to challenge the decision' ([133]). Within both the GDPR and the law enforcement directive, the human intervention shall be 'meaningful, rather than just a token gesture [and] it should be carried out by someone who has the authority and competence to change the decision' ([134]).

Even though the CI directive clearly states the protection of critical infrastructure as a purpose for processing personal data by CIP operators, it lacks 'suitable measures to safeguard the data subject's rights and freedoms and legitimate interests'. For this reason, and considering the feasible legal grounds set out by the law, in order for critical infrastructure operators to adopt automated decision-making processes in compliance with the norms, the only lawful and fair approach is to amend the CI directive accordingly. This could also entail a lawful ground for allowing operators to enable an automated decision-making process involving biometric data, that requires 'suitable measures to similarly significant effects safeguard the data subject's rights and freedoms and [that] legitimate interests are in place' ([135]).

7.4.2 Requirement 2: Transparency

The transparency principle represents one of the pillars of the European data protection framework. According to the legal regime, data controllers shall inform data subjects about processing operations involving them. Article 5.1.a of the GDPR and Recital 26 of the law enforcement directive describe such principle. Moreover, specific obligations are described in Articles 12 to 15 of the GDPR and Articles 12 to 18 of the law enforcement directive.

The main purpose behind the transparency principle is to build 'trust in the process which affects the citizen by enabling them to understand, and if necessary, challenge those processes' ([136]). It follows that controllers need to adopt appropriate measures for keeping the data subject duly informed about how their data are being used, making them 'able to determine in advance what the scope and consequences of the processing entails' ([137]).

Transparency requires that data controllers adopt certain precautions in a proactive and efficient manner ([138]). First, the content of the information that the controller shall communicate is defined by Article 13 of the GDPR and by Article 13 of the law enforcement directive. Member State law can impose the data controllers to provide

([130]) Article 29 Working Party, Guidelines on Automated individual decision-making, p. 21.
([131]) General data protection regulation, Art. 22.2.b.
([132]) Law enforcement directive, Art. 11.1.
([133]) Law enforcement directive, Recital 38.
([134]) Article 29 Working Party, Guidelines on Automated individual decision-making, p. 2.
([135]) Law enforcement directive, Art. 11.2.
([136]) Article 29 Working Party, Guidelines on transparency under Regulation 2016/679, 29 November 2017, p. 4.
([137]) Article 29 Working Party, Guidelines on transparency under Regulation 2016/679, 29 November 2017, p. 7.
([138]) This represents a proactive obligation. It does not originate from a request of the data subject, and it applies irrespective whether the data subject wants to receive information about it. Council of Europe, Explanatory Report to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 28 January 1981, §68.

additional information within the context of a processing operation defined by law, expanding provisions of the law enforcement directive ([139]).

Second, information shall be concise, transparent, intelligible and easily accessible, and expressed in a clear and plain language. This is particularly important when providing information to children, as they might perceive messages in different ways, running the risk of not being duly informed. Therefore, data controllers 'should ensure that the vocabulary, tone and style of the language used is appropriate to and resonates with children so that the child addressee of the information recognises that the message/ information is being directed at them' ([140]). Next, the data controller shall ensure communications with the data subjects are carried out efficiently, with the appropriate means, taking into consideration the context (e.g. online versus physical) and with the aim of minimising information fatigue.

The data controller shall also make the information available in 'easily accessible form', meaning that 'the data subjects should not have to seek out the information [and] it should be immediately apparent to them where this information can be accessed' ([141]).

In general, the messages for the data subject shall be 'in writing or by other means, including where appropriate, by electronic means' ([142]). However, in order to make communications to the data subjects effective, other means might be adopted with the aim of enhancing transparency by 'potentially reducing the need for vast amounts of written information to be presented to a data subject' ([143]), such as, for instance, cartoons, infographics ([144]), or audio messages. In addition, data controllers shall provide information in an oral form, whenever data subjects request it ([145]).

Box 12. Example of the application of the Transparency principle

After an evaluation of possible scenarios, a CI operator decides to share information about data processing using a short notice on a clearly visible signpost ([146]) before the entrance to a surveilled area. The signpost is then complemented by additional information on how to reach a complete information notice by means of a QR code.

([139]) Fundamental Right outlines them as the following: the controller's identity and contact details, including the DPO's details, if any; the purpose and legal basis for the processing, i.e. a contract or legal obligation; the data controller's legitimate interest, if this provides the basis for processing; the personal data's eventual recipients or categories of recipients; whether the data will be transferred to a third country or international organisation, and whether this is based on an adequacy decision or relies upon appropriate safeguards; the period for which the personal data will be stored, and if establishing that period is not possible, the criteria used to determine the data storage period; the data subjects' rights regarding processing, such as the rights of access, rectification, erasure, and to restrict or object to processing; whether the provision of personal data is required by law or a contract, whether the data subject is obliged to provide his or her personal data, as well as the consequences in case of failure to provide the personal data; the existence of automated decision-making, including profiling; the right to lodge a complaint with a supervisory authority; the existence of the right to withdraw consent; in cases of automated decision-making, including profiling, meaningful information about the logic involved in profiling, its significance and the envisaged consequences they face from the processing European Union Agency for Fundamental Rights, *Handbook on European Data Protection Law,* 2018 Edition, p. 210. A specific element is then defined by Article 13.2.d, law enforcement directive — where necessary, further information, in particular where the personal data are collected without the knowledge of the data subject.

([140]) Article 29, Working Party, Guidelines on transparency under Regulation 2016/679, 29 November 2017, p. 10.

([141]) Article 29, Working Party, Guidelines on transparency under Regulation 2016/679, 29 November 2017, p. 8.

([142]) General data protection regulation, Art. 12.1, law enforcement directive, Art. 12.1.

([143]) Article 29, Working Party, Guidelines on transparency under Regulation 2016/679, 29 November 2017, p. 23.

([144]) In this regard, Article 12.8 provides for the opportunity to employ standard sets of icons. However, currently there are no such standard icons.

([145]) General data protection regulation, Art. 12.1 and law enforcement directive, Art. 12.1.

([146]) A first example of this application can be found within Garante per la Protezione dei Dati Personali, Provvedimento in materia di videosorveglianza, October 2010.

The signpost within the surveilled perimeter may also provide for a dedicated phone number. This ensures data subjects — with particular regard to visually impaired persons — can listen to the information every time they desire. Data controllers might also consider the opportunity to establish a call centre data subjects can refer to when seeking assistance.

In the context of EWZ, transparency can have profound impacts on data subjects. Since EWZ could involve public or semi-public spaces, data subjects should be made aware of any processing, so that they can freely decide whether to transit into a surveilled zone, or on how to behave in said public spaces. In addition, EWZ may adopt machine learning and automated decision-making techniques. In such cases, the transparency principle increases in relevance and data controllers shall take appropriate steps to ensure compliance, especially when acting in the context of policy option 1 or 2.

First, data controllers shall inform data subjects regarding 'the existence of automated decision-making, including profiling [and provide] meaningful information about the logic involved as well as the significance and the envisaged consequences of such processing for the data subject' ([147]).

Second, data controllers shall adopt all the necessary steps to provide meaningful information about the mechanisms and logic behind the automated processing. Ensuring compliance to this requirement might be challenging due to ever-increasing complexity of the available tools. Moreover, explaining such mechanics with a simple and clear language might be quite a complicated feat.

Third, the data controller should make an effort to understand what might be the consequences of the processing for the data subjects, and explain these in a clear way.

Currently, there is a lively debate about the so-called 'explainability obligation'. Some scholars do not believe the obligation exists, and reject it ([148]), while others support it as a specific right arising from the obligations set by Article 13 and Recital 71 of the GDPR ([149]).

Data controllers should provide information to data subjects not only before the processing has begun, but also during the processing operation itself or as a following step. As already stated, the most common interpretation qualifies the obligation to provide information as a proactive one for data controllers. However, especially in the face of the various stages envisaged (before, during, after), this obligation is complemented by a specific right for the data subjects, this being the right to access. Accordingly, data subjects have the right to request whether their personal data are being processed, which data are subject to such processing, and receive detailed information regarding the processing operation ([150]).

The transparency principle applies to data controllers even when communicating with data subjects in relation to their rights under Articles 15 to 22 and 34 of the GDPR and 14-18 of the law enforcement directive, and facilitates the exercise of data subjects' rights. This last point is strongly emphasised by Recital 59 of the GDPR and Recital 40 of the law enforcement directive, which states 'modalities should be provided for facilitating the exercise of the data subject's rights [and] for requests to be made electronically, especially where personal data are processed by electronic means'.

The transparency principle applies to data controllers both when proactively providing information to data subjects, and when responding to access requests. According to Article 29 of the GDPR, when data controllers are responding to an access request they

([147]) General data protection regulation, Art. 13.2.f. No specific obligation is contained within the law enforcement directive, even if Member State can impose them within specific normative provision.

([148]) Watcher, S., Mittelstadt, B. and Floridi, L. (2017), 'Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation', *International Data Privacy Law*.

([149]) Edwards, L. and Veale, M. (2018), 'Enslaving the Algorithm: From a "Right to an Explanation" to a "Right to Better Decisions"?', *IEEE Security & Privacy*, Issue 16, Number 3, pp. 46-54.

([150]) General data protection regulation, Art. 15.1 and law enforcement directive Art. 14.

shall provide information to data subjects based upon their request, comply with the obligation flowing from the principle of transparency (i.e. relating to the quality of the communications as set out in Article 12.1) when communicating with data subjects in relation to their rights under Articles 15 to 22 and 34, and facilitate the exercise of data subjects' rights ([151]). This last point is strongly emphasised by Recital 59 of the GDPR, which states 'modalities should be provided for facilitating the exercise of the data subject's rights [and] for requests to be made electronically, especially where personal data are processed by electronic means' ([152]).

7.4.3 Requirement 3: Purpose limitation

The principle of purpose limitation is one of the cornerstones of the entire discipline of data protection law in Europe. According to the GDPR, personal data shall be collected for 'specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes' ([153]).

Regarding this specific aspect, the WP29 deeply explored the three main general characteristics related to the principle of purpose limitation. Accordingly, any data processing operations shall have a purpose (or more than one) that is specific, explicit, and legitimate ([154]). The processing of personal data for undefined and or unlimited purposes is unlawful. Likewise, processing of personal data on the mere potential usefulness in the future, without a certain purposes, is unlawful as well. Purpose limitation intends to provide adequate safeguards to 'data subjects by setting limits on how data controllers are able to use their data while also offering some degree of flexibility for data controllers' ([155]). In other words, every time personal data are reused for a different purpose, which is not compatible with the original one, it must have its own particular legal basis and cannot rely on the fact that data were initially acquired or processed for another legitimate purpose ([156]).

As said by the WP29, changing the purpose of a specific data processing operation is not unlawful per se. This requires a case-by-case compatibility assessment on a number of key factors. First, there should be a relationship between the original purpose and the new purpose. Second, it should be proven that data subjects have a reasonable expectation that the processing will continue. Third, the nature of the personal data and the impact of the further processing on the data subjects shall be assessed. Fourth, the controller shall adopt specific countermeasures to ensure fair processing and to prevent any undue impact on the data subjects ([157]).

Clearly assessing, choosing, and disclosing the purpose for the data processing is fundamental to ensure said processing is carried out in a lawful way. In particular, carefully choosing and defining the purpose is crucial as it can drastically change the evaluations on necessity and proportionality. This appears clearly in the context of critical infrastructure protection. Indeed, processing operations with the purpose of 'deterring' will require different assessment than those with the purpose of 'preventing' or 'protecting'.

7.4.4 Requirement 4: Data minimisation

The data minimisation principle consists in the obligation for data controllers to process only the data that are 'adequate, relevant and not excessive in relation to the purpose for

([151]) General data protection regulation, Art. 15-22.
([152]) General data protection regulation, Recital 59.
([153]) General data protection regulation, Art. 5.1.b and law enforcement directive, Art. 4.1.b.
([154]) For a detailed account and analysis of the three characteristics, see Article 29 Data Protection Working Party, Opinion 03/2013 on purpose limitation, WP 203, 2 April 2013.
([155]) Article 29 Data Protection Working Party, Opinion 03/2013 on purpose limitation, WP 203, 2 April 2013, p. 11.
([156]) European Union Agency for Fundamental Rights, *Handbook on European Data Protection Law*, 2018 Edition, p. 123.
([157]) Article 29 Working Party, Guidelines on transparency under Regulation 2016/679, 29 November 2017, p. 4.

which they are collected and/or further processed' ([158]). In other words, controllers shall strictly limit collection of data to such information, as it is directly relevant for the specific purpose pursued by the processing ([159]).

This principle requires that only personal data strictly necessary to reaching the intended purpose can be processed. Therefore, 'personal data which is adequate and relevant but would entail a disproportionate interference in the fundamental right and freedoms at stake should be considered as excessive' ([160]).

Within the EWZ framework, this requirement has to be duly assessed on a case-by-case basis. In fact, different scenarios of public security might require more or different sets of data compared to one another. Therefore, the understanding of how to satisfy the data minimisation principle can only be reached through a case-by-case analysis.

Box 13. Example of the application of the Data Minimisation Principle

After a preliminary analysis, the critical infrastructure operator identifies that certain cameras capture not only pictures of the EWZ, but also images of persons within their houses, as these are adjacent the EWZ. Therefore, he decides to deactivate said cameras, since leaving them active would have resulted in a disproportionate processing operation.

7.4.5 Requirement 5: Accuracy

Pursuant to Article 5.1.d of the GDPR and Article 4.1.d of the law enforcement directive, personal data shall be accurate and kept up to date. In particular, both the GDPR and the law enforcement directive clearly state that 'every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed are erased of rectified without delay' ([161]). This very important data governance and quality principle, which makes it necessary to keep the data up to date, and to check regularly for accuracy, arises from the fact that inaccurate data might produce considerable risks for data subjects ([162]).

In the context of EWZ, this principle carries considerable consequences especially when looking at machine learning applied to EWZ. Critical infrastructure operators must take particular care to use accurate data when 'training the algorithm' in order to prevent unwanted effects like biases or false positives ([163]). Also, as already described in section 4.1, data subjects might request rectification of their data ([164]). Such requests might have the effect of improving the precision of the algorithm as well ([165]). Therefore, it should be fully accessible by the operators.

7.4.6 Requirement 6: Storage limitation

According to Article 5.1.e of the GDPR personal data shall be 'kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for

([158]) General data protection regulation, Art. 5.1.c and law enforcement directive, Art. 4.1.c.
([159]) European Union Agency for Fundamental Rights, *Handbook on European Data Protection Law*, 2018 Edition, p. 125.
([160]) Council of Europe, Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data, 18 May 2018, §52.
([161]) Council of Europe, Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data, 18 May 2018, §52.
([162]) European Union Agency for Fundamental Rights (2018), *Handbook on European Data Protection Law*, 2018 Edition, p. 128.
([163]) For an in-depth analysis see Future of Privacy Forum, The Privacy Expert's Guide To Artificial Intelligence and Machine Learning, October 2018.
([164]) The right to rectification is stated within Article 16 of the GDPR and Article 16 of the LED. For a deep analysis within the context of LED, see Article 29 Working Party, Opinion on some key issues of the law enforcement directive (EU 2016/680), WP 258, 29 November 2017, p. 16.
([165]) Pasquale, F. A., 'Professional Judgment in an Era of Artificial Intelligence and Machine Learning', University of Maryland Legal Studies Research Paper No 2017-33, November 2017.

which the personal data are processed' ([166]). In other words, data controllers shall erase or anonymise personal data when the purposes for their processing are achieved. Following the same principle, the law enforcement directive requires Member States to 'provide for appropriate time limits to be established for the erasure of personal data or for a periodic review of the need for the storage of personal data' ([167]).

It can be said that the data minimisation principle requires that data shall be 'limited to a strict minimum' that has to be proportionate in relation to the purpose of the collection ([168]) and subject to 'a periodic review' ([169]). Indeed, it can certainly be stated that the longer data are retained, the more the processing exposes data subjects to risks to their rights and freedoms. This idea has been reiterated by many important judgments and cases of the CJEU ([170]).

In the context of EWZ, critical infrastructure operators can retain images of people collected within the surveilled areas only for the specific time required to achieve the processing operations purposes.

When considering EWZ involving machine-learning technologies, one has to consider that the algorithm requires a periodical training period. This makes it necessary to retain specific datasets for this purpose. According to preliminary analysis made by the TG, this might result in contradictions with the data retention requirement. In order to overcome such an obstacle, WP7 suggests a solution that consists in defining a specific purpose for the training of the algorithm. On the basis of this purpose, critical infrastructure operators could identify different and specific retention periods for video streams containing personal data. In particular, the exact amount of data needed for the training will be safely stored in a specific area with restricted access, and retained solely until the training has been performed.

Lastly, retention can be considered as a dynamic parameter to be modified according to the threat level. Within a low-threat scenario, only a very limited retention timing may be considered proportionate. Contrarily, when an attack occurred, the processing of personal data can be considered proportionate even if data are retained longer, provided that a due evaluation of risks for rights and freedoms for data subjects of the measure has been performed.

Time limitation for storing personal data only applies to data kept in a form that permits identification. If data controllers can establish a way to separate the data from the identification of individuals (for instance, employing anonymisation techniques), then the storage limitation principle does not apply. Knowing the 'strengths and weaknesses of each technique helps to choose how to design an adequate anonymisation process in a given context' ([171]).

Operators shall pay special attention to the fact that video streams containing personal data cannot be easily anonymised, and that a coherent application of the storage limitation principle shall be defined especially when processing biometric data through CCTV cameras.

7.4.7 Requirement 7: Security

Article 5.1.f of the GDPR and 4.1.f of the law enforcement directive represent the legal basis for the security principle. Accordingly, appropriate technical and organisational measures shall be implemented when processing personal data in order to protect the

([166]) General data protection regulation, Art. 5.1.e.
([167]) Law enforcement directive, Art. 5.
([168]) *S. and Marper* v *United Kingdom*, European Court of Human Rights, 4 December 2008 — Application nos. 30562/04 and 30566/04.
([169]) General data protection regulation, Recital 39.
([170]) See Digital Rights Ireland and CJEU, Tele2 Sverige AB, Joined Cases C-203/15 and C-698/15, 21 December 2016.
([171]) Article 29 Working Party, Opinion 05/2014 on Anonymisation Techniques, WP216, Adopted on 10 April 2014.

data against accidental, unauthorised or unlawful access, use, modification, disclosure, loss destruction or damage ([172]).

Article 32 of the GDPR gives more details about this obligation ([173]). The provision reads that data controller shall take into account 'the state of the art, the costs of implementation and the nature, scope, context and purpose of processing, as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons' ([174]) when implementing such measures ([175]).

Box 14. Appropriateness of security measures

Measures shall be defined by the data controller according to the specific circumstances. Appropriate technical and organisational measures could include, for instance, holding data in a secure physical environment, limiting access control via layered logins and protecting the communication of data with strong cryptography ([176]).

A crucial step regarding security measures consists in defining a process for regularly testing and evaluating the effectiveness of said measures to ensure the processing is secure. This is also related to the Data Protection by Design principle enshrined within Article 25 of the GDPR and 20 of the law enforcement directive. In fact, integrating necessary security measures and safeguards at the very early stage of the development of the EWZ technology will help in increasing effectiveness of security measures. Moreover, coherently with Policy Option 2, adherence to an approved code of conduct or an approved certification mechanism can help to demonstrate compliance with the security of processing requirement ([177]).

EWZ technologies have to deeply consider several factors while assessing and reacting to risks on personal data processing from a security viewpoint. First of all, threats are incumbent due to the likelihood of an attacker that wants to disable the system before attacking the site. Moreover, personal data that are inside the systems might be of very sensitive nature. Biometric data surely generates a critical potential risk, meaning that strong security measures have to be put in force ([178]). Accessibility — usually technologically translated via access control systems — is also a matter of security, especially when accessibility is linked to the possibility to access such data by third parties or law enforcement agencies.

Box 15. Audit log

In order to monitor the accuracy of the instrument employed to process personal data in the EWZ, it is strongly suggested to adopt audit-log technologies and to perform periodical audits. Within the law enforcement directive, this is also an obligation framed in Article 25.

([172]) General data protection regulation, Recital 39.

([173]) Although Article 29 of the law enforcement directive adopts a similar, risk-based approach, the provision is slightly different, as it outlines most important scenarios to consider for correctly assessing appropriateness of security.

([174]) Art. 32, GDPR. For a specific focus on the 'state of the art' aspect, see TeleTrusT in cooperation with ENISA, Guideline 'State of the art' — Technical and organizational measures, 2019.

([175]) The risk-based approach enshrined in this principle has already given voice to a numerous set of stakeholders releasing their guidelines on the topic. See, for instance, ENISA (2018), *Handbook on Security of Personal Data Processing*, 29 January 2018.

([176]) Council of Europe, Directorate-General of Human Rights and the Rule of Law, Consultative Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data — Opinion on the Data protection implications of the processing of Passenger Name Records, Strasbourg, 19 August 2016.

([177]) General data protection regulation, Art. 32.3.

([178]) Security requirement is also strongly linked to obligation related to data breach. In fact, in cases where a personal data breach occurs requires the controller to notify the competent supervisory authority of the breach without undue delay. In case of high risk for rights and freedom of affected data subjects, a similar communication obligation to the data subject exists. Art. 33, GDPR and Art. 30. For a deep analysis on the provision see Article 29 Working Party, Guidelines on Personal data breach notification under Regulation 2016/679, WP250rev.01, Adopted on 3 October 2017, As last Revised and Adopted on 6 February 2018.

7.4.8 Requirement 8: Accountability

As described so far, data controllers have an important role in making data protection work in practice. The accountability principle relates to managing and documenting specific choices made by the organisation itself in applying data protection principles within specific circumstances. The principle, enshrined within Article 5.2 of the GDPR and 4.2 of the law enforcement directive, requires operators to be responsible for and able to demonstrate compliance with the personal data processing principles described so far.

In one of its early opinions, WP29 described the essence of accountability as the controller's obligation to put in place measures that would, under normal circumstances, guarantee data protection rules are adhered to and keep the necessary evidence to demonstrate it to data subjects and to supervisory authorities ([179]).

The Accountability principle extends its area not only to the compliance of processing activities with applicable rules, but also to 'the effectiveness of the measures' ([180]), reinvigorating the importance of a proactive and substantial approach to the entire data protection discipline that operators shall consider. Within the context of EWZ, the principle has to be duly taken into account by operators. In particular, due to the high risks that processing operations might have on rights and freedoms of data subjects, the principle requires the controller to act in a very tailored way in order to find and document best solutions on the areas listed so far.

7.5 Conclusions

As described in the previous pages, implementing an early warning zone requires policymakers and critical infrastructure operators to take into consideration a number of constraints and legal requirements. This is further aggravated by the fact that EWZs can make a substantial use of personal data and, in certain instances, biometric data. Therefore, operators adopting EWZ solutions will be required to carefully balance different interests at stake following requirements mainly set by Article 52 of the European Charter of Human Rights.

From a policymaking perspective, national leaders and policymakers can adopt different approaches to level the playing field. This paper described three of them, these being Private Autonomy, Code of Conduct, and Legal Obligation. The WP7 suggests adopting the second option, as the authors believe that this approach provides for the best balance between standardisation and adaptability. Both these aspects are crucial, but the second one is particularly important given the continuous evolution of the threat scenarios critical infrastructure operators have to look out for in order to manage risks in a legally feasible and technologically mature way.

Despite the approach selected by policymakers, as stated above, critical infrastructure operators will be bound by specific legal constraints. These directly translate in the way EWZs shall be implemented. The last section provides for a list of design requirements that shall be addressed during the implementation and operation phase of an EWZ. That said, requirements shall be duly assessed and defined on a case-by-case basis.

Lastly, WP7 stresses the importance of performing a data protection impact assessment for the processing activities carried out in the context of the EWZ. This should not be seen as a mere legal requirement, but as an important tool that helps operators to maintain the right governance on the data they employ for protecting the infrastructure. The same can be said for another requirement that at least some operators will have to fulfil, that is performing a prior consultation with the relevant data protection authority.

([179]) Article 29 Working Party, Opinion 3/2010 on the principle of accountability, WP 173, Adopted on 13 July 2010.
([180]) General data protection regulation, Recital 74.

8 Data protection impact assessment prototype development

Nowadays, critical infrastructure operators need to respond to a growing number of threats, risks and uncertainties. In addition to this, they are increasingly exposed to regulatory pressure coming from the data protection regimes. This is particularly true for early warning zones, since these measures can easily be designed around technologies, such as video surveillance biometric recognition, that are considered to have high privacy impacts on individuals.

The authors acknowledge this situation, and propose points to be considered for the definition of a new approach to security and privacy risks. This approach is called Security and Privacy Impact Assessment, and builds on the benefits of a dynamic approach to risk analysis, combined with the elements of a Data Protection Impact Assessment.

The approach is still novel and has not been developed fully yet. Therefore, the section provides for some basic elements that the authors hope will pave the way to new research in the field.

8.1 Introduction

8.1.1 General context and approach

The protection of critical infrastructures (CI) is a crucial aspect of European Union security. These assets provide fundamental services, 'essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people' ([181]). In 2008, the Council of the European Union adopted Directive 2008/114/EC (CI directive) with the purpose of ensuring a consistent level of critical infrastructure protection (CIP) across Europe.

The CI directive focuses on energy and transport infrastructures. However, critical infrastructures belong to a considerably wider list of sectors. For instance, financial and water supply infrastructures are usually considered critical ones. The European Commission identified three different types of infrastructure assets. These are '[p]ublic, private and governmental infrastructure assets and interdependent cyber and physical networks[,] [p]rocedures and where relevant individuals that exert control over critical infrastructure functions, [and] [o]bjects having cultural or political significance as well as "soft targets" which include mass events (i.e. sports, leisure and cultural)' ([182]). All of these infrastructure assets may be qualified as 'critical' when they fulfil the requirements set by the CI directive.

Given the relevant societal function critical infrastructures fulfil, it is unsurprising that terrorists consider them to be highly valuable targets. The recent terrorist attacks perpetrated in Europe to essential services and public spaces serve as a proof of the sensitivity of critical infrastructures. This aspect consistently sits at the top of political and security agendas worldwide. In 2017, the United Nations Security Council recognised 'the growing importance of ensuring reliability and resilience of critical infrastructure and its protection from terrorist attacks for national security, public safety and the economy of the concerned States as well as well-being and welfare of their population' ([183]). The European Reference Network for Critical Infrastructure Protection, acknowledging the importance of CIP and the increasing difficulties critical infrastructure operators face to maintain adequate levels of security, started a Thematic Group aimed at investigating the

([181]) Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, Article 2(a).
([182]) Commission of the European Communities, Green Paper on a European Programme for Critical Infrastructure Protection, 17 November 2005, p. 20.
([183]) United Nations Security Council, Resolution 2341 (2017), 13 February 2017.

adoption of so-called early warning zones and biometric video surveillance systems. This paper is part of this research effort.

In the light of the technologies in scope (especially biometric technologies), the research group had to carefully considerate the implications for the privacy and fundamental rights of citizens and users. Indeed, no matter how important a critical infrastructure is, Member States are required to comply with a broader set of norms, some of which may limit the actions critical infrastructure operators can undertake to ensure CIP. The importance of critical infrastructures cannot in itself justify abandoning the obligations set out by other laws and fundamental rights. The issue may arise when public security conflicts with norms aimed at safeguarding other rights and principles such as the right to the protection of personal data and the right to respect for private life as enshrined in the Charter of Fundamental Rights. These are not 'absolute right[s] and there is no doubt they may be limited' ([184]). However, their importance demands any action with potential impacts on them to be approached with caution.

It is not the purpose of this specific paper to analyse all the intricacies of the ethical issues or the nuances of legal safeguards. There is a very lively debate among scholars, and the field is quickly developing ([185]). Here, suffice to say that the law accounts for a balancing of public interest and private rights ([186]). Critical infrastructure operators should aim to strike said balance by adopting a structured, accountable approach and, wherever possible, a standardised one ([187]).

The updated European legal framework on data protection provides for guidelines critical infrastructure operators (in their role of data controllers) can adopt to ensure compliance to the legal regime. The Data Protection Impact Assessment (DPIA) represents one of the most important tools for accountability as it helps data controllers to comply with applicable legal requirements. Working Party 29 described DPIA as 'a process for building and demonstrating compliance' ([188]). However, the authors (Working Party 7, WP7) strongly suggest that qualifying it as a mere compliance tool underestimates the value DPIA can bring to a harmonised approach to data protection and security as well ([189]), especially in the context of critical infrastructure protection.

It holds true that DPIA 'is a tool for managing risks to the rights of the data subjects, and thus takes their perspective, […] whereas risk management […] is focused on the organization' ([190]). At first glance, these two aspects might seem distant ones. However, they share characteristics that might make possible a unified assessment. Given their public function, critical infrastructure operators are well positioned to define a holistic approach that will promote security while accounting for rights and freedoms of data

([184]) Wiewiórowski, W. R. (2017), 'Surveillance for public security purposes. Four pillars of acceptable interference with the fundamental right to privacy', in Vermeulen, G. and Lievens, E. (Eds.), *Data Protection and Privacy under Pressure. Transatlantic tensions, EU surveillance, and big data*, Maklu, Antwerp, Apeldoorn, Portland, p. 173.

([185]) See for instance, Kosta, E. (2017), 'Surveilling masses and unveiling human rights: Uneasy choices for the Strasbourg Court', in: Norris, C., de Hert, P., L'Hoiry, X. and Galetta, A., *The Unaccountable State of Surveillance. Exercising Access Rights in Europe*, Springer.

([186]) A particularly compelling analysis of the so-called 'essential guarantees' can be found in Article 29 Data Protection Working Party, Working Document 01/2016 on the justification of interferences with the fundamental rights to privacy and data protection through surveillance measures when transferring personal data (European Essential Guarantees) 13 April 2016.

([187]) Studies have shown the important of standardisation in this regard. See for instance Wurster, S. (2014), 'Ethics and Privacy Issues of Critical Infrastructure Protection — Risks and Possible Solutions Through Standardization', in *PIK — Praxis der Informationsverarbeitung und Kommunikation*, Volume 37, Issue 3, De Gruyter, pp. 205-210.

([188]) Article 29 Data Protection Working Party, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is 'likely to result in a high risk' for the purposes of Regulation 2016/679, 4 April 2017, p. 13.

([189]) See Gellert, R. (2018), 'Understanding the notion of risk in the General Data Protection Regulation', *Computer Law & Security Review*, vol. 34, issue 2, pp. 279-288

([190]) Article 29 Data Protection Working Party, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is 'likely to result in a high risk' for the purposes of Regulation 2016/679, 4 April 2017, p. 15.

subjects ([191]). This paper aims at investigating and proposing a possible new approach to risk management from the perspective of CIP. By considering some of the measures envisaged for EWZ and biometric video surveillance, WP7 hopes to raise critical points to be considered for future research in the field.

The WP7 acknowledges the fact that in the context of EWZ there is a gap of governance and accountability instruments, with particular regard to the legal feasibility of specific measures. Moreover, the new threat environment is quickly making traditional approaches to risk analysis obsolete. Terrorists and criminal actors are adopting new techniques by the day, increasing their threat level. Critical infrastructure operators need to adapt, leveraging on new technologies to increase their situational awareness, response capabilities, and the effectiveness of their risk analyses. Risk analysis, in particular, is 'the cornerstone of a successful Critical Infrastructure Protection programme [and it is] indispensable in order to identify threats, assess vulnerabilities and evaluate the impact on assets, infrastructures or systems taking into account the probability of the occurrence of these threats' (Giannopoulos et al., 2012).

The need for innovative and more efficient approaches is a clear priority for the international community as a whole. The United Nations Security Council, for instance, 'called upon Member States to consider developing or further improving their strategies for reducing risks to critical infrastructure from terrorist attacks, which should include, inter alia, assessing and raising awareness of the relevant risks, taking preparedness measures, including effective responses to such attacks, as well as promoting better interoperability in security and consequence management, and facilitating effective interaction of all stakeholders involved' ([192]).

It is likely that the surveillance measures within the EWZ will have an impact on data subjects' right to privacy. Therefore, a holistic tool of governance and implementation will be useful to help operators to balance the risk exposure of EWZs and privacy risk of data subject ensuring, at the same time, the proper level of accountability. The proposed new approach should aim at combining risk analysis and DPIA, toward a Security and Privacy Impact Assessment (SPIA) paradigm.

As the approach is currently being investigated, this paper aims at describing the main elements of the suggested approach, rather than providing a detailed account of its specifications. One particular aspect that will be touched upon is the necessity to integrate a dynamic approach to risk analysis that will take into consideration the rapid, sometimes instantaneous, changes in the threat scenarios of critical infrastructure, leveraging on live flows of information from different sources.

This approach carries very important benefits. First, it has the potential to enhance the overall security of critical infrastructures. Second, it promotes a standardisation of information structures, as they will need to be shared among many different actors. Third, it further increases the data protection compliance level of critical operators, as they will be able to modulate their security measure according to a dynamic balancing between security and privacy in any given moment. The model is still at a very early and conceptual stage, and certainly needs further investigation. However, the authors believe that it is particularly suited to make critical infrastructure protection procedures more 'fine grained' and lawful.

8.1.2 Legal framework

WP7 looked into the current legal framework in order to identify the norms and regulations that have impacts on the proposed SPIA model.

([191]) Previous research efforts stressed the importance of adopting a holist approach to critical infrastructure risk management. See for instance Klaver, M. H. A, Luijf, H. A. M., Nieuwenhuijs, A. H., Cavenne, F., Ulisse, A. and Bridegeman, G. (2008), European Risk Assessment Methodology for Critical Infrastructures, First International Conference on Infrastructure Systems and Services: Building Networks for a Brighter Future (INFRA), Rotterdam.

([192]) United Nations Security Council, Resolution 2341 (2017), 13 February 2017.

As for rules pertaining to the protection of critical infrastructures, operators must comply with the requirements set by Directive 2008/114. In particular, Article 5 requires them to adopt an adequate operator security plan (OSP) for the protection of ECI. The OSP must, at minimum, cover three aspects. First, it shall identify all the important assets for the critical infrastructure. Second, it shall provide for risk analysis. Third, it shall identify, select, and prioritise countermeasures, taking into account the distinction between permanent and graduate security measures ([193]).

The WP7 also considered documents produced outside of the European Union, with particular regard to United Nations Security Council resolutions, like UNSC Resolution 2341 (2017). Indeed, such decisions directly affect all of the United States Members and, therefore, are relevant to EU Member States as well.

As for rules pertaining to data protection, the updated legal framework involves two main sets of rules. The first one is Regulation (EU) of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, commonly referred to as the general data protection regulation (GDPR). The second one is Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, commonly referred to as the law enforcement directive.

It is worth noting that, while the GDPR is directly applicable within Member States, the law enforcement directive requires them to adapt their internal legal systems to new principles contained therein. Although it may seem that this approach could jeopardise the effectiveness of the rulings, Member States are given very little room for modification of the norms. Therefore, it is likely that these will be coherently adopted across Europe.

Both Article 35 of the GDPR and Article 27 of the law enforcement directive require critical infrastructure operators ([194]) to perform a DPIA for the adoption of EWZs. This holds especially true when the EWZ employs biometric features. These articles outline responsibilities and minimum requirements and contents to be included within the assessment. The WP29 provided useful additional guidance in understanding the legal obligations related to DPIA that can help operators in better understanding the topic ([195]).

The WP7 acknowledges the importance of other aspects, such as the necessity of prior consultation with data protection authorities by virtue of Article 36 of the GDPR and Article 28 of the law enforcement directive. Although, it does not fully develop on them in order to maintain the focus on the SPIA model itself, these issues certainly represent topics worth of dedicated investigations.

8.2 Security and privacy impact assessment

8.2.1 A new paradigm for risk analysis

In recent years, the overall number of terrorist attacks decreased globally ([196]). Despite this promising data, in certain regions (with western Europe being one of these) the trend is still in the positive, with the number of terrorist attacks increasing on a year-on-

([193]) Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, Annex II.
([194]) See Section 7.
([195]) For more information see Working Party (Article 29 Data Protection), Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is 'likely to result in a high risk' for the purposes of Regulation 2016/679, 4 April 2017.
([196]) Harris, B., Terrorist attacks are in decline for the third year running, World Economic Forum, 5 October 2018, https://www.weforum.org/agenda/2018/10/terror-attacks-have-dropped-2018-us-state-department

year basis ([197]). This, together with the extensive media coverage of recent attacks, created the perception among citizens of a lowering level of public security, providing the higher grounds for terrorist operations. Indeed, as the main goal of terrorism is to spread terror, the current feeling of insecurity that lingers all over Europe can be seen as a victory for terrorist parties.

This situation makes it clear that terrorism represents a concrete threat to the European Union in general. In this regard, critical infrastructures are particularly sensitive targets. A successful attack against one or more of them could not only spread terror among the population, but also generate devastating damages. The potential effects coming from attacks to critical infrastructures makes it evident that the Union needs to address the security for critical infrastructures and public spaces not only with mitigation measures, but also by anticipating the attacks.

Critical infrastructure operators are already under the obligation to protect their infrastructure and to design an appropriate Operator Security Plan ([198]). One of the requirements of OSP is to conduct 'a risk analysis based on major threat scenarios, vulnerability of each asset, and potential impact' ([199]). Traditionally, risk analyses have mostly been characterised by a static approach. Risk managers carry out periodical assessments (often once or twice a year) and they consider the results valid until they perform the next assessment. This 'point-in-time' approach made perfect sense in a mostly analogue world. However, nowadays the scenario is different. Technological advancements enabled new attack vectors and techniques, changing the threat environment and its pace. Every day, terrorists find better and more efficient ways to coordinate and attack their targets.

Ironically enough, what is helping terrorists to increase their success rate might also represent a meaningful response to them. The same technology available to attackers is available to defenders as well, such as law enforcement agencies and critical infrastructure operators. With such powerful technological means, it is possible to overcome the limits of the traditional static risk analysis in favour of a dynamic approach. Technically, a dynamic risk analysis could be capable of providing continuous assessments and real-time updates to risk exposure levels, making it easier for critical infrastructure operators to identify trends and anticipate future scenarios.

In the context of the present study, the video surveillance measures implemented in the EWZ play an important role in lowering the risk exposure. Indeed, especially when paired with other elements such as law enforcement watchlists, they can greatly improve the risk assessment capabilities. However, they also introduce a number of privacy issues that operators need to adequately address.

In this regard, DPIA becomes not only a legal requirement but also a useful governance tool ([200]). WP7 advocates for widening the scope of this tool in order to adapt it to the security needs of critical infrastructure operators since, in their capacity of data controllers, they should have the flexibility to determine 'the precise structure and form of the DPIA in order to allow for this to fit with existing working practices' ([201]).

([197]) For more information, see the data provided by the Global Terrorism Database at https://www.start.umd.edu/gtd

([198]) Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, Article 5(1).

([199]) Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, Annex II.

([200]) For more information, see Wright, D. and de Hert, P. (2012) (eds.), *Privacy Impact Assessment*, Springer, The Netherlands.

([201]) Working Party (Article 29 Data Protection), Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is 'likely to result in a high risk' for the purposes of Regulation 2016/679, 4 April 2017, p. 17.

8.2.2 Orchestrating security risk analysis and privacy impact assessment through SPIA implementation

8.2.2.1 Assessing privacy during the design phase of the SPIA model

As stated above, the objective of the SPIA model is to integrate security and privacy into a unified assessment approach. The main idea is to establish a framework indicating which security measure should be activated in the face of a specific risk level. Since each measure carries different and often considerable privacy impacts on the rights and freedoms of data subjects, it is of the utmost importance to address all the privacy aspects related to the implementation of a SPIA model. In particular, it is crucial to assess what are the privacy impacts connected with the implementation of the SPIA. In order to do so, critical infrastructure operators shall perform a DPIA.

DPIA is not a mandatory requirement for every processing operation. However, the implementation of an EWZ is very likely to require it due to the fact that the EWZ is intended to be applied for 'a systematic monitoring of a publicly accessible area on a large scale' ([202]). Pursuant to Article 35 of the GDPR and Article 27 of the law enforcement directive, critical infrastructure operators shall perform a DPIA prior to the processing. In other words, the data protection implications have to be assessed before deploying an EWZ framework. This approach is also consistent with the Data Protection by Design (DPbD) principle enshrined by Article 25 of the GDPR and Article 20 of the law enforcement directive. According to the DPbD principle, critical infrastructure operators 'shall, both at the time of the determination of the means for processing […], implement appropriate technical and organisational measures […], which are designed to implement data-protection principles' ([203]).

According to the law ([204]), a DPIA shall provide four basic requirements. First, a systematic description of the personal data processing operations and the purposes of the processing including chosen legal grounds. Second, an assessment of the necessity and proportionality of the processing operations in relation to the purposes. Third, an assessment of the risks to the rights and freedoms of data subjects. Last, it shall provide for the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with data protection provisions.

The second requirement, in particular, represents a complex aspect. As investigated in Section 7, Necessity and Proportionality are two fundamental yet difficult-to-understand principles, crucial in performing a Data Protection Impact Assessment. The current European legal framework does not provide for a shared model for understanding Necessity and Proportionality, let alone for a specific approach to DPIA. In this regard, 'it allows for data controllers to introduce a framework which complements their existing working practices provided' ([205]) it takes into account the 'assessment of the necessity and proportionality of the processing operations in relation to the purposes' ([206]).

([202]) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), Article 35.3.c.

([203]) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), Article 25.1.

([204]) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), Article 35.7.

([205]) Article 29 Data Protection Working Party, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is 'likely to result in a high risk' for the purposes of Regulation 2016/679, 4 April 2017, p. 21.

([206]) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), Article 35.7.b.

8.2.2.2 Designing the SPIA framework

EWZs usually employ a very broad set of features, some of which (like biometrics and artificial intelligence) are characterised by a high level of invasiveness on the privacy of citizens. According to the European legal framework and relevant case law ([207]) such a level of invasiveness can be justified only in the presence of serious threats to other values. Therefore, the operator should decide whether to enable one or more of these features according to an analysis of necessity and proportionality from both a security risk standpoint and from a privacy risk standpoint.

A feature 'can be considered necessary when it ensures adequate effectiveness in the pursuit of a general interest objective by providing for the least intrusive level possible' ([208]), while proportionality 'requires measures not to exceed the limitations of a specific right over what is strictly required for them to reach their objectives' ([209]). Therefore, operators need to ensure that the response measures are necessary and proportionate to the expected privacy impacts. Since no standardised assessment approach currently exists, critical infrastructure operators are left with the burden of understanding such aspects, ensuring both effectiveness of the security measures and compliance with data protection requirements.

WP7 suggests approaching such an issue by associating EWZ features, security risk levels, and necessity and proportionality principles. This requires the operator to project what privacy consequences might arise from the activation of each measure and compare them with the risk levels through the lenses of necessity and proportionality taking into account the effect said measures have on the treatment of the identified risk.

Currently, there are a number of different approaches to risk assessment and evaluation critical infrastructure operators can employ. It is important to notice that the model described in the present paper is for illustrative purposes only. The focus of this research is to present an approach to security and privacy risk analysis, not to define a specific methodology of risk management. The SPIA approach is intended to be compatible with risk analysis methodologies and techniques. This means that critical infrastructure operators can employ their methodology of choice among the many already available, or define a customised methodology, and adopt the SPIA approach as a complement to said methodologies.

For the illustrative purpose of the present paper, WP7 assumes a very basic and simple scenario-based approach. The risk level for each threat scenario is expressed as the product of Likelihood (this being the chances that a scenario will manifest and cause damages) and Impact (this being the amount of damages caused by the manifestation of the threat scenario). The values for Likelihood, Impact, and Risk are expressed employing a four-level scale, which ranges from Very Low (1) to Very High (4). The following figure shows the risk matrix ([210]).

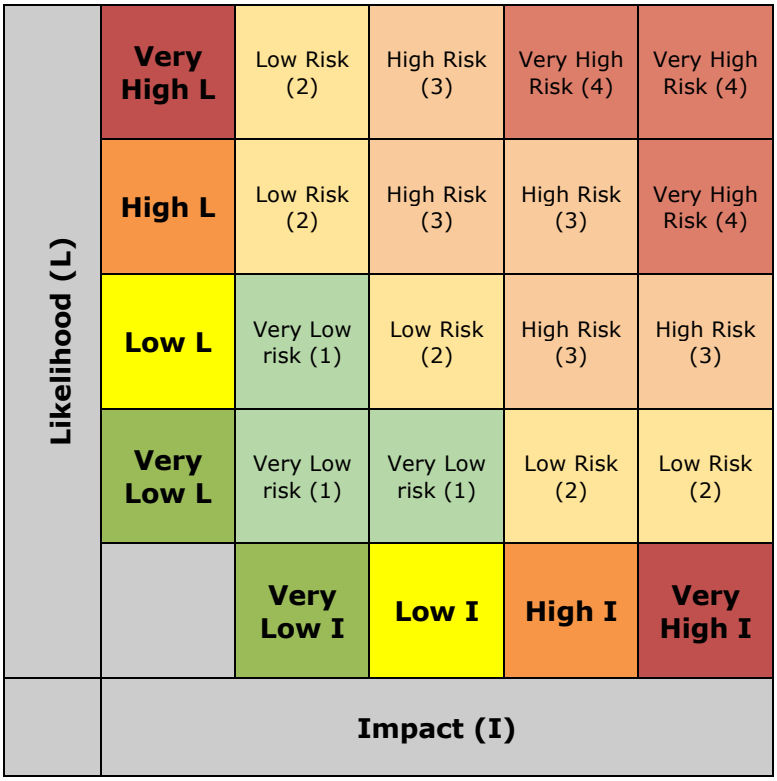
([207]) See, for instance, European Court of Human Rights, Case of *S. and Marper* v the *United Kingdom*, Judgment, 4 December 2008. See also, Court of Justice of the European Union, *Digital Rights Ireland Ltd* v *Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, The Commissioner of the Garda Síochána, Ireland and the Attorney General, and Kärntner Landesregierung, Michael Seitlinger, Christof Tschohl and Others*, Judgment, 8 April 2014. See also Court of Justice of the European Union, *Tele2 Sverige AB* v *Post- och telestyrelsen*, *Secretary of State for the Home Department* v *Tom Watson, Peter Brice, Geoffrey Lewis*, Judgment, 21 December 2016. See also Court of Justice of the European Union, *Ministerio Fiscal*, Judgment, 2 October 2018.

([208]) See Section 7.

([209]) See Section 7.

([210]) For the sake of simplicity, the approach equally weighs the Likelihood and the Impact. Some structured approaches put differential weights on one or the other element. Without prejudice on the validity of such asymmetric approaches, the paper does not consider them, as this would involve additional levels of complexity.

Figure 6. Sample risk distribution map



Source: JRC.

This document employs the map above as a reference for expressing the actual risk (the risk level measured in a given moment) and the residual risk (the risk level expected after the implementation of a given set of measures). Residual risk is then compared with the privacy impact in order to understand whether a certain measure could be implemented. The following table provides for a sample of the approach, applied to the threat scenario 'Armed assault by terrorist group' ([211]).

Table 7 below illustrates an example of template critical infrastructure operators can employ to define, a priori, whether it will be possible to implement each specific measure when a specific risk level changes. For instance, in a given moment, the risk level associated to the threat scenario is Low (2). In such a case, the critical infrastructure operator cannot activate biometric surveillance measures. Suddenly, this risk level changes (through to the dynamic risk analysis approach detailed below) to Very High (4). In this specific moment, the operator knows that he now has the possibility of activating biometric surveillance measures, according to the framework that he previously designed.

The content of the 'SPIA outcome' column is what defines whether the operator can implement a given measure when certain risk levels are measured. Take for instance the measure 'CCTV with biometrics recognition connected with watchlists'. In the example above, the fictional operator who defined the framework decided that this measure could be admissible only when it helps mitigating a Very High (4) risk level. In every other case, the operator established that the privacy impacts of this kind of measure, which amounts to a level Very High (4), could not justify its adoption. Critical infrastructure operators have to decide on these elements according to their own judgement. There is no specific guidance in the norms nor in the literature saying that certain measures introducing a given privacy impact can be admissible only when adopted to mitigate threat of a given risk level. This has to be decided on according to the assessment of

([211]) The values expressed here are not the result of an assessment of the scenario, but are only for illustrative purposes.

necessity and proportionality and the evaluation of the risks to the rights and freedom of data subjects. Necessity and proportionality can be assessed by looking into the design requirements associated to each security measure/feature ([212]). A measure with high impacts on the rights and freedoms of data subject but characterised by a low risk-mitigation (like, for instance, activating biometric video surveillance measures to mitigate the risk of data breach), will be hardly justifiable from a legal standpoint, since it is very unlikely that said measure will withstand the necessity and proportionality test.

Table 7. Sample SPIA framework for the scenario 'Armed assault by terrorist group'

Actual risk	Security measure in the EWZ	Residual risk	Privacy impact	SPIA outcome	Notes
1	Armed security patrols	↔ 1	1	OK - Implement	
1	CCTV w/o biometrics	↔ 1	2	KO - Not implement	Since risk level cannot be lowered below 1, every measure entailing privacy impacts will not be justifiable
1	CCTV with biometrics recognition connected with watchlists	↔ 1	4	KO - Not implement	
2	Armed security patrols	↓ 1	1	OK - Implement	
2	CCTV w/o biometrics	↓ 1	2	KO - Not implement	The privacy impact is not commensurate to the benefit in terms of risk mitigation
2	Biometrics recognition connected with watchlists	↓ 1	4	KO - Not implement	
3	Armed security patrols	↓ 2	1	OK - Implement	
3	CCTV w/o biometrics	↓↓ 1	2	OK - Implement	
3	CCTV with biometrics recognition connected with watchlists	↓↓ 1	4	KO - Not implement	The privacy impact is not commensurate to the benefit in terms of risk mitigation
4	Armed security patrols	↓ 3	1	OK - Implement	
4	CCTV w/o biometrics	↓ 2	2	OK - Implement	
4	CCTV with biometrics recognition connected with watchlists	↓↓↓ 1	4	OK - Implement	

Source: JRC.

Evaluating the risks to the rights and freedoms of data subjects represents another (together with the assessment of necessity and proportionality of each feature) complex aspect. Within the European legal framework, a risk to the rights and freedoms of natural persons 'may result from personal data processing which could lead to physical, material

([212]) For more information on design requirements, see Section 7.

or non-material damage' ([213]). The definition is broad, and encompasses many potential cases, such as the lack of transparency on personal data processing, the lack of participation due to the impossibility to opt out from the processing, the repurposing of images identity captured, discrimination, identity theft or fraud, financial loss, damage to reputation, significant economic or social disadvantages, deprivation of rights and freedoms or prevention from exercising control over personal data, processing involving vulnerable natural persons, processing involving large amounts of personal data, processing affecting a large number of data subjects, etc. Certain technologies can further increase this already vast list. For instance, when artificial intelligence technologies are implemented, there are higher risks coming from potential bias within the algorithm. Many researchers concur that 'Automated systems are not inherently neutral [and] reflect the priorities, preferences, and prejudices […] of those who have the power to mould artificial intelligence' ([214]). This could cause issues like stereotype reinforcement, ethnic or gender bias, constraints of suspicion, increased and/or disproportionate surveillance ([215]).

So far, a number of institutions and entities have published several frameworks, both generalist ([216]) and sector-specific ([217]). Although it is still relatively rare, some of these publications provide examples of specific methodologies ([218]) of DPIA applications ([219]) in the context of public surveillance. In addition, the International Organization for Standardization is currently in the process of drafting a dedicated international standard, with the aim of providing guidelines for carrying out a DPIA ([220]). All of these are potentially useful tools for critical infrastructure operators.

There is a strong momentum for the development of approaches, and the WP7 believes this trend will continue in the next years, further increasing the toolset and knowledge of critical infrastructure operators. However, with regard to EWZ, the process is still lagging behind. In-depth research is necessary to understand the risks for natural persons and data subjects connected with this kind of scenario and, possibly, document them in a shared dictionary, fostering interoperability and comparability.

8.2.2.3 Framework validation

The relationship between security risks, privacy risks, and security measures is the main driver behind the design of an SPIA model. Once this relationship has been established, the operator can proceed to validate the model.

([213]) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), Recital 75.

([214]) Buolamwini, J., 'Algorithmic Bias Persists. Gender Shades project, Massachusetts Institute of Technology Media Lab on Civic Media (https://www.media.mit.edu/projects/gender-shades/overview).

([215]) For more information, see Burt, A., Shirrell, S., Leong, B. and Wang, X., 'Beyond Explainability: A Practical Guide to Managing Risk in Machine Learning Model, Future or Privacy Forum'. See also 'Future of Privacy Forum, Unfairness by Algorithm: Distilling the Harms of Automated Decision-Making', December 2017.

([216]) See for instance The Standard Data Protection Model. A concept for inspection and consultation on the basis of unified protection goals, November 2016. See also Agencia española de protección de datos, Guía Prática para las Evaluaciones de Impacto en la Protección de los Datos Sujetas al RGPD. See also Commission nationale de l'informatique et des libertés, Privacy Impact Assessment, 2015. See also Information Commissioner's Office, Conducting privacy impact assessments code of practice, 2014.

([217]) See for instance Privacy and Data Protection Impact Assessment Framework for RFID Applications, 2011. See also Smart Grid Task Force 2012-14. Expert Group 2: Regulatory Recommendations for Privacy, Data Protection and Cyber-Security in the Smart Grid Environment, Data Protection Impact Assessment Template for Smart Grid and Smart Metering systems, 18 March 2014.

([218]) Wright, D. and Raab, C. D. (2012), 'Constructing a surveillance impact assessment', *Computer Law & Security Review*, Volume 28, Issue 6, December 2012, pp. 613-626.

([219]) United States Department of Homeland Security, Privacy Impact Assessment of the Facial Recognition Pilot, 26 November 2018.

([220]) ISO/IEC 29134 (project), Information technology — Security techniques — Privacy impact assessment — Guidelines, International Organization for Standardization (ISO).

Following the guidance provided by the European legal framework, the validation process might comprise two steps, these being a direct validation with data subjects and a prior consultation in front of the competent data protection authorities ([221]).

In the context of EWZ and biometric video surveillance, the invasiveness of the measures envisaged will be likely to cause very high impacts on the privacy of data subjects, making a validation exercise strongly recommended ([222]).

In particular, pursuant to Article 35 of the GDPR, 'the controller shall seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of processing operations' ([223]). As stated by Working Party 29, GDPR envisages a high degree of freedom on how to perform validations with data subjects. Their 'views could be sought through a variety of means, depending on the context (e.g. an internal or external study related to the purpose and means of the processing operation, a formal question to the staff representatives or trade/labour unions or a survey sent to the data controller's future customers)' ([224]). Publishing the results of the Data Protection Impact Assessment, despite not being a legal requirement in itself, might also help critical infrastructure operators 'to foster trust in the controller's processing operations, and demonstrate accountability and transparency [and is a] particularly good practice to publish a DPIA where members of the public are affected by the processing operation' ([225]).

Critical infrastructure operators intending to validate the model with data subjects, especially by publishing the DPIA, should carefully manage the process so that the public interest and effectiveness of the security measures will not be jeopardised. In particular, they should bear in mind that '[t]he published DPIA does not need to contain the whole assessment, especially when the DPIA could present specific information concerning security risks for the data controller' ([226]).

8.2.2.4 Framework update and maintenance

As already stated, nowadays threats and risk levels changes constantly due to several intrinsic or extrinsic factors. Therefore, it is of outmost importance that 'the controller shall carry out a review to assess if processing is performed in accordance with the data protection impact assessment at least when there is a change of the risk represented by processing operations' ([227]).

Given the context, the framework should be kept up to date. The update process should be designed to be a sustainable one, in order to ensure its effectiveness. This can be achieved by clearly defining the conditions under which the framework needs to be updated. For instance, the association between a risk level and a specific surveillance measure might be relevant and appropriate at a specific moment, while being not valuable at other times. Critical infrastructure operators should assess the validity of

([221]) As for prior check with data protection authorities, this document does not delve into the nuances of this process. For useful guidance on the topic, see Article 29 Data Protection Working Party, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is 'likely to result in a high risk' for the purposes of Regulation 2016/679, 4 April 2017, p. 18.

([222]) See section 7.

([223]) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), Article 35(9).

([224]) Article 29 Data Protection Working Party, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is 'likely to result in a high risk' for the purposes of Regulation 2016/679, 4 April 2017, p. 13.

([225]) Article 29 Data Protection Working Party, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is 'likely to result in a high risk' for the purposes of Regulation 2016/679, 4 April 2017, p. 17.

([226]) Article 29 Data Protection Working Party, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is 'likely to result in a high risk' for the purposes of Regulation 2016/679, 4 April 2017, p. 17.

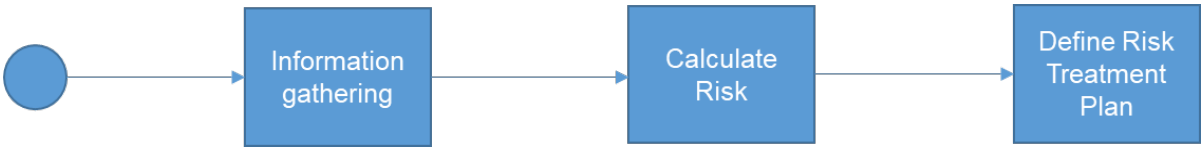
([227]) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), Article 35.11.

their frameworks with specific reviews aimed at understanding these aspects. The said reviews should be performed periodically at planned intervals and ad hoc, when significant changes occur. This could happen, for instance, when new surveillance or security technologies emerge, when there is a change in the perimeter of the EWZ, or when regulators publish new data protection norms.

8.2.2.5 SPIA implementation and run

Once the SPIA has been modelled, validated, and updated processes have been established, it is then ready to be implemented in the broader risk management process of the critical infrastructure operator. In its most essential form, any risk management process looks like the one in Figure 7 below.

Figure 7. High-level view of risk analysis and management



Source: JRC.

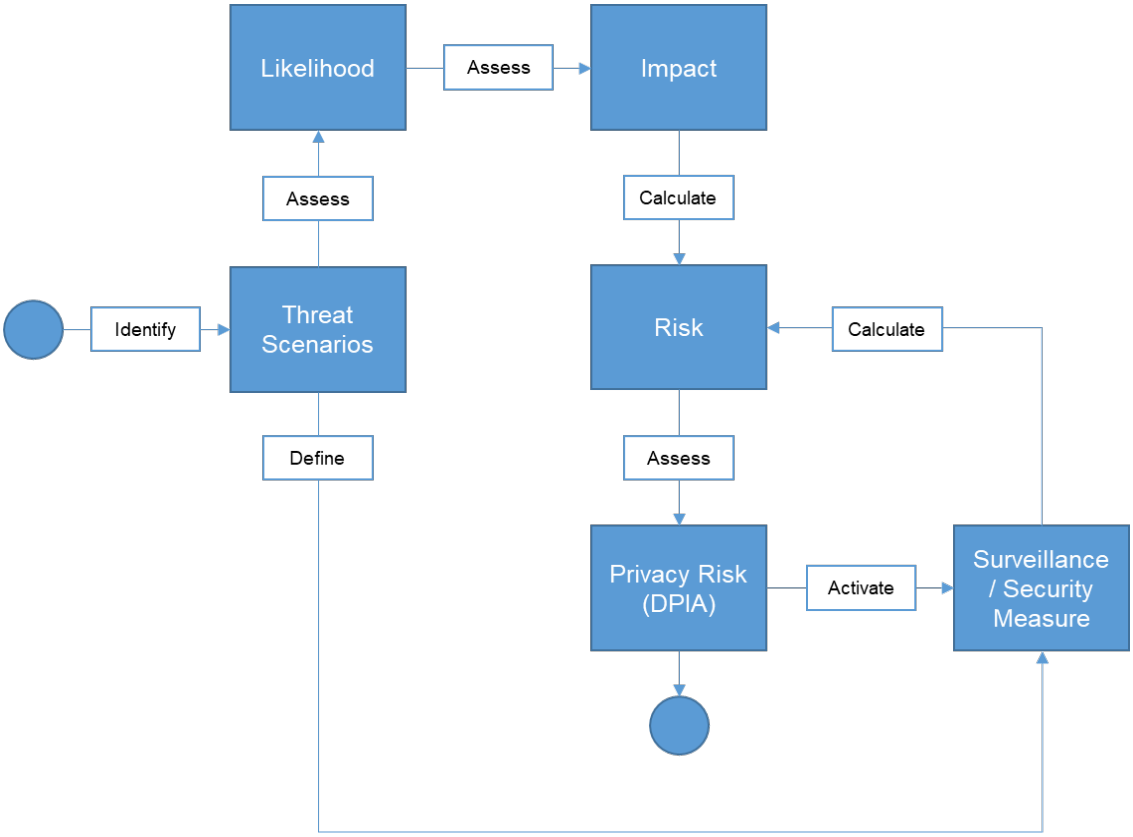
The high-level representation shows the logical approach behind the process. Critical infrastructure operators can pick from a number of different methodologies to operationalise it, each one with its own peculiarities. This means that, across the network of critical infrastructures, a very heterogeneous situation can be found. The dynamic approach to risk analysis is not intended to substitute these other methodologies. It is not meant to influence the structural element of risk analysis, like the algorithms, weights, taxonomies, etc. Since it represents an approach rather than a structured methodology, dynamic risk analysis can be adapted to risk management activities that are already in place.

The 'Information gathering' and 'Calculate Risk' boxes in Figure 7 represent the core elements of the risk analysis process. Figure 8 shows the standard approach to this process. First, the critical infrastructure operator should identify all the relevant Threat Scenarios that need to be monitored and assessed. The list should consider different kinds of threat scenarios to account for all of the potential risks the infrastructure is exposed to (scenarios leading to physical risks, scenarios leading to cyber risk, scenarios leading to country/political risks, etc.).

Secondly, he should define the catalogue of Surveillance and Security Measures that are most relevant to the identified Threat Scenarios. Critical infrastructure operators can freely choose the taxonomies and granularity that satisfy their security needs. Obviously, such decision should take into consideration the sustainability of the model (for instance, an endless list of very granular measures will be very hard to manage and update). This step is extremely important. Indeed, these measures represent the bedrock against which the operator has to assess the Necessity and Proportionality principles.

Subsequently, the operator assesses the expected Likelihood (this being the chances that a scenario will manifest and cause damages) and Impact (this being the amount of damage caused by the manifestation of the threat scenario) for each of the Threat Scenario and uses the results to calculate the Risk level. How these elements are assessed, correlated, and measured is, again, a decision for the critical infrastructure operator. They can adopt complex statistical models, or simpler qualitative approaches. Regardless of the methodology of choice, unless the operator already has considerable experience in risk analysis, the WP7 suggests adopting a scalable approach, beginning with a simple implementation and increasing its efficiency over time.

Figure 8. Generic risk analysis process



Source: JRC.

Assessing the Impact of a Threat Scenario represents a major challenge for operators. Critical infrastructures, and certainly ECI, are characterised by a high degree of interconnectivity among them. Energy, telecommunication, finance, transportation, etc. All of these sectors require their infrastructures to connect seamlessly across Europe and, often, worldwide. This aspect strictly relates to the necessity to understand the level of criticality of an infrastructure asset, as described above in this study. For this reason, the WP7 reiterates the importance of a shared approach to criticality assessment.

The next step is to evaluate whether the measures activated to counter the threat and mitigate the risk stands the test of Necessity and Proportionality. Figure 9 calls this step 'Privacy risk' in order to stress that it represents a check between security requirements and privacy requirements. At this stage, the critical infrastructure operators will have a fully developed framework as a reference tool (see Table 1 for an example). If the operator correctly designed and constantly updates the framework, there should not be differences between what is written in the framework and what is observed in the field. However, before activating any measure, it is advisable to perform such a direct verification, without relying only on the predetermined framework. This is why there is a dedicated activity box in the logical flow illustrated above.

The outcomes of the previous steps indicate the operator whether he should activate further measures, or accept the risk as all Necessary and Proportionate measures have already been exhaustively assessed and activated.

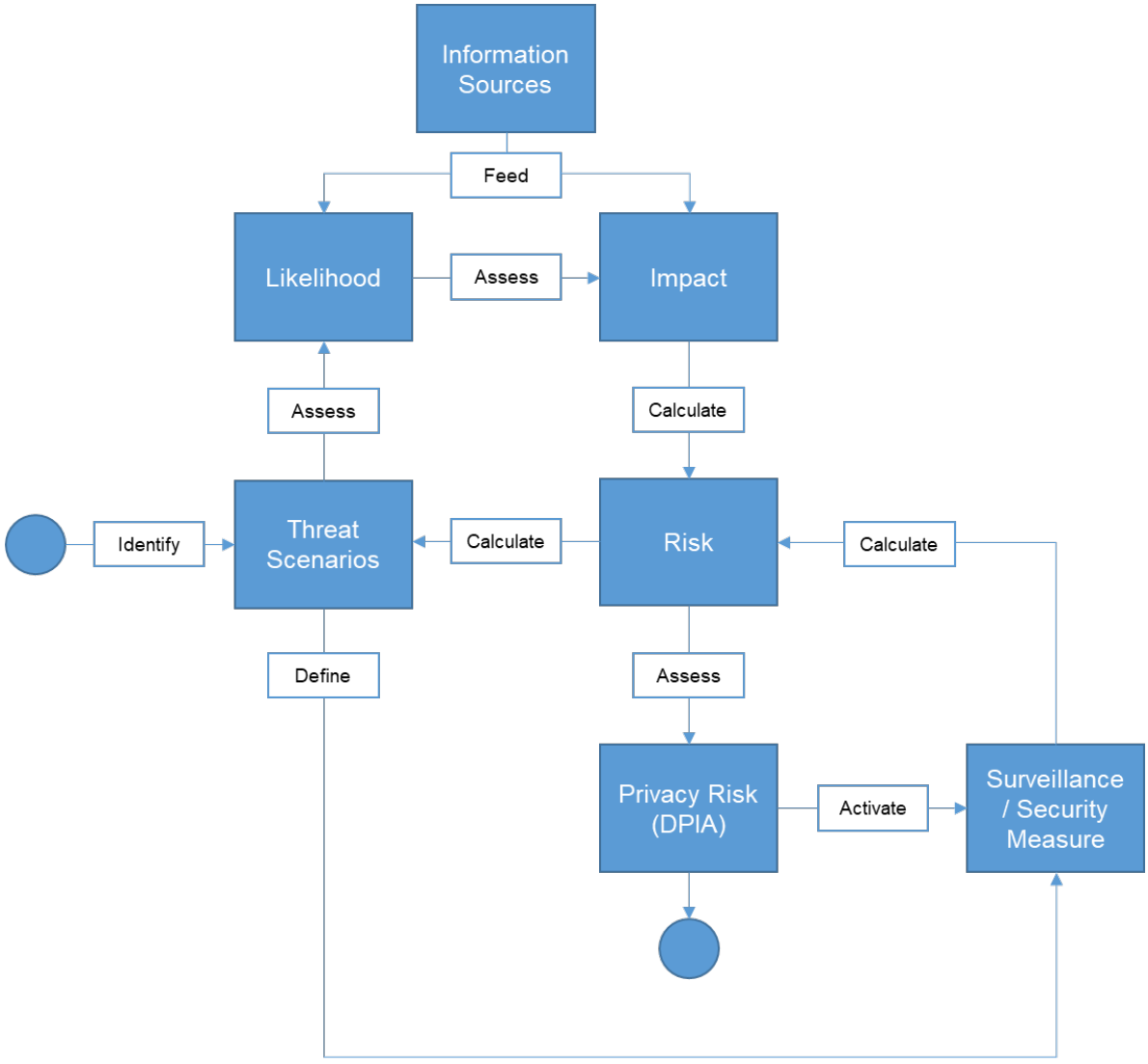
It is clear from the description above that the framework described in this study could be, in theory, applied to a traditional static risk analysis. In such a case, the operator performs a risk assessment at a certain time, employing the information available at that moment. The analysis might still drive the activation of certain security measures or features, requiring therefore an analysis of privacy risks as well. However, given the static nature of such an approach, the evaluation whether to keep or deactivate these

features will be postponed until a new risk assessment is performed. This is anachronistic. Binding the activation of certain features to the measured risk level necessarily requires a continuous assessment of said risk in the face of effectiveness and compliance of the related measures.

Think about a situation in which an operator decides to activate real-time facial recognition due to heightened levels of risk. For instance, law enforcement authorities might alert the operator that certain individuals are planning an attack to the infrastructure, which may fall in the threat scenario employed above as example (armed assault by terrorist group). Until police or other law enforcement bodies seize said individuals, the risk will remain high. This could take a long or a short time. Therefore, the critical infrastructure operator needs to monitor the situation closely in order to know when the individuals are apprehended or stopped. As soon as this happens, he should assess the new level of risk and evaluate whether or not the activation of facial recognition can still be justified.

The constant information flow is core for the dynamic model. In particular, correct and up-to-date information is necessary to monitor the Likelihood and Impact of the scenarios.

Figure 9. Dynamic risk analysis process



Source: JRC.

In the process above, 'Information Sources' is what makes the model dynamic. By ensuring the continuous assessment of Likelihood (for instance, by identifying a spike in usage of certain techniques among certain malicious actors) and Impact (for instance, by factoring the higher sanctions arising from brand new regulations, or the change in the value of certain assets), it is possible to ensure that risk is constantly updated.

There are no limits to the amount and quality of the information feeding the risk assessment. Threat intelligence, security monitoring ([228]), information sharing ([229]), security report, and bulletins are all examples of feeds. These can be more general, like political risk analyses helping critical infrastructure operators in understanding the broader picture of their operational scenario ([230]), or more specific, like the list of most-wanted issued by law enforcement agencies ([231]). The more an information source can be automated, the more the risk assessment can be made dynamic. In theory, this could provide for real-time analyses. The technology is still developing, and areas such as big data and artificial intelligence look promising for these kinds of application.

8.3 Conclusions

The goal of this paper was to investigate the main issues critical infrastructure operators face with regard to maintaining compliance with data protection norms while ensuring adequate levels of security for the infrastructure they are called upon to protect. The authors approached the topic by providing for a conceptual model to risk management that critical infrastructure operators can implement to manage security risks and privacy risks at the same time. However, such a model is still to be fully developed, and the WP7 is committed to further defining the topic through future analyses.

Among the main points that emerged during the analysis, WP7 recognises the necessity to address more effectively the threat of terrorism in the European Union's territory. Given the 'fluid' nature of this ever-changing threat, critical infrastructure operators need to consider approaches to CIP that are equally flexible.

Dynamic risk analysis is one of the said approaches and responds to the necessity of continually updating the situational awareness of critical infrastructure operators. Today the technology is mature enough to leverage fully on such an approach, and the future promises to make it even more effective through technologies such as big data mining and analysis, and artificial intelligence.

This approach to risk can also respond to the legal requirements arising from the data protection legal regimes. Since a dynamic approach to risk analysis provides the tool for a continual modulation of the security measures implemented, this means that critical infrastructure operators will be able to manage more effectively the adoption of certain security measures in response to specific security issues, taking into account the criteria for complying with the law. These criteria are primarily the principles of necessity and proportionality; which thanks to the dynamic approach, can be addressed nearly real-time.

The relation between security and privacy holds the key to ensure that public security is maintained at adequate level without forfeiting the values of a democratic society. Therefore, WP7 strongly believes that this aspect should be one of the main research point for academia and professionals in the coming years.

([228]) See for instance, Global Incident Map. A Global Display of Terrorism and Other Suspicious Event (http://www.globalincidentmap.com).

([229]) The Critical Infrastructure Warning Information Network (CIWIN) is an example of an information sharing programme undertaken by the European Union that could be further developed to meet the need of a dynamic risk analysis approach for CIP. For more information, see https://ec.europa.eu/home-affairs/what-we-do/networks/critical_infrastructure_warning_information_network_en

([230]) Currently there are a number of commercial services offering political risk reporting, like Riskline.

([231]) See for instance Europe's Most Wanted Fugitives (https://eumostwanted.eu), and FBI Most Wanted (https://www.fbi.gov/wanted).

9 Guide for implementing an EWZ system

This guide provides recommendations and guidance for the implementation of an early warning zone (EWZ) system using recognition technologies. In particular it covers:

— Planning for the implementation of an EWZ;

— Acceptance testing an EWZ; and

— Operating an EWZ.

This document focuses on the specific aspects related to the inclusion of a biometric system at the core of a recognition system (where the recognition of people is an important requirement of an application). It should be noted that biometrics is only one element of the EWZ.

This document has applicability across a wide range of applications that incorporate a biometric system. The recommendations and guidance are intended to support the needs of users in small to medium-size organisations without biometric expertise but in charge of requirements capture, planning, procuring and accepting the biometric system whose development is outsourced to a system developer. A checklist to record the evidence of completing the assessment steps necessary is included as Annex A.

9.1 Planning for the implementation of an EWZ

9.1.1 General

An application using an EWZ responds to a need outlined in the ConOps. For example, the requirement may be for improved security through recognising customers and/or employees more securely.

In order that the implementation of the application addresses these requirements and to facilitate decision-making about the various factors listed in this clause, the organisation should carefully consider the requirement and the environment in which the EWZ will be deployed, before making any decision about a particular installation which they have seen or heard about.

A systematic approach could consist of the following steps:

— Documentation of an overall description of the problem;

— A description of the role that recognition plays in the solution to the problem;

— An analysis of the risks of incorrect recognition, both falsely accepting imposters and failing to recognise legitimate subjects, ranked with the likelihood and impact of incorrectly recognising individuals, taking account of other management and security measures forming part of the solution;

— A list of any constraints to the implementation and operation of the solution including at least costs, timescale, and environment;

— A list of statutory requirements that might apply;

— Assessment of the suitability of different EWZ systems to the application.

This approach will support the selection of the most appropriate solution consistent with the documented risks and constraints.

Planning for the implementation of an EWZ system shares many of the considerations associated with planning for the implementation of any recognition system. Some of the key factors to be considered include:

— Consultation with interested parties;

— Selection of biometric modality;

— Determination of performance parameters;

— Security;
— Usability;
— Accessibility;
— Data capture;
— Exception handling;
— Privacy and data protection;
— User acceptance;
— Convenience;
— Stakeholder management;
— Vulnerability to spoofing; and
— Universal applicability (i.e. failure to enrol rate).

These factors are included because they are either specific to an EWZ system or important in addressing the ethical concerns raised when introducing such a system. Note that some factors, such as cost and project risk, are not discussed in detail in this section as they are general considerations that could equally apply to the implementation of any technology.

Whilst these factors are listed separately for convenience, they are interdependent and, as such, cannot be considered in isolation. Therefore, planning for the implementation of an EWZ system is a process of selection and trade-off, with trade-off decisions being made on the basis of finding the right balance between all these factors through an iterative process.

In addition, proper consideration of all these factors, without prior engagement with stakeholders could result in the selection of an EWZ system that fails to deliver the results for which it is intended. Therefore, stakeholder engagement is highlighted here as an important factor to be considered at an early stage in planning for implementation. Stakeholders, including potential data subjects, should be engaged at an early stage when preparing for the use of an EWZ system in order to communicate the reasons for its use and to identify and address any concerns, particularly in relation to privacy and data protection.

The success of a EWZ system is critically dependent upon the extent to which users want it to succeed, and in this regard it is probably more vulnerable to adverse perceptions than most types of technology. 'Users' in this context include not only the subjects whose characteristics will be used, but also attendants, administrators, supervisors and those who have to maintain the EWZ system.

A shared understanding of the business problem and the anticipated benefits is clearly a significant element in this engagement, as is a shared appreciation of the risks, both real and imagined. Individual judgements on acceptability are also influenced by their views on the value these benefits can give them as individuals.

9.1.2 Biometric modality

There are a number of biometric modalities that could be considered for EWZ as outlined in the previous sections. For example, for long-range recognition, these could include:

— Most of the physiological soft biometrics such as height, perceived age, perceived gender, presence of face hair, body shape, etc.;
— Some behavioural soft biometrics such as movement tracking, smartphone tracking;
— Some adhered soft biometrics such as clothing;
— Gait (video);

— 2D Face;

— Voice recognition.

All of these modalities are available commercially and have been deployed as part of a variety of access or workflow applications.

All biometric modalities have particular considerations that could have a bearing upon selection and choosing the right biometric modality for the ConOps which requires optimising trade-offs between numerous conflicting factors such as convenience to users, security requirements, acceptance by users and costs.

One consideration, for example, is whether the preference is for a biometric modality that requires contact or non-contact technology.

Another consideration might be whether the preference is for a biometric modality that requires behavioural characteristics or biological characteristics. Dynamic signature and voice recognition modalities are considered as behavioural characteristics, whereas fingerprint, facial image, iris image, hand geometry, finger vein and palm vein modalities are considered as biological characteristics.

An assessment of the range of biometric modalities available should be conducted in order to determine which modality to use for the intended application. The assessment should identify:

— Suitability to the target subject population (e.g. whether there are any constraints);

— The level of subject interaction with the biometric system (e.g. whether contact with the data capture device is required);

— The suitability of the environment in which data capture device will be located;

— Required performance parameters;

— The implementation risks (e.g. project and technical risks);

— The costs, both initial and ongoing (e.g. maintenance and upgrade costs).

9.1.3 Performance parameters

The performance of a biometric system and its application is generally described in terms of error rates, throughput volumes and rates, and exception handling volumes.

Other performance parameters for the application, such as availability and repair times, will also need to be established but such parameters are considered general to all IT system requirements and so are outside the scope of this code of practice.

The most commonly quoted error rates are the biometric system false acceptance rate (FAR) and false rejection rate (FRR), which are interdependent. A biometric system usually allows a threshold to be adjusted to provide a trade-off between the acceptance and rejection of a match. The most appropriate trade-off for a specific application will depend on the relative importance of security, convenience and cost for the application.

When a biometric system is used in an early warning system, it is generally considered that the FAR relates to security and that the FRR relates to convenience. In practice, the situation is more complicated in that too many false rejections can result in false rejection fatigue and a lowering of defences against rejection of actual impostors. The FRR is probably more important than the FAR in most applications and more likely to give rise to operational problems and user rejection.

Typically, error rates are quoted for a biometric system and are then difficult to verify when this forms part of an application. Therefore, there is no easy answer to determining the required error rates for a biometric system. The performance parameters that are most important are those that relate to the application, in particular throughput volume and rate, and exception handling volume. Specifying the requirement for these two

application performance parameters is fundamental in ensuring the biometric system provides the right solution to the business problem.

From throughput volumes and exception handling volumes, the target application throughput rate and application false rejection rate (App-FRR) can be established.

There is a direct correlation between App-FRR and the biometric system FRR but they will not be the same because the final App-FRR will be influenced by other factors, including the management system and processes in place.

Evaluation of the security risk of incorrect recognition (and thus allowing impostor access) will enable the target application false acceptance rate (App-FAR) to be established. Again, there will be a direct correlation between App-FAR and the biometric system FAR but they will not be the same because the final App-FAR will be influenced by other factors including the management system and processes in place.

Note that App-FAR and App-FRR are not widely used terms and therefore discussion with the biometric system supplier is essential to establish a mutual understanding, particularly when agreeing acceptance criteria.

Another significant error rate of a biometric system is the failure to enrol (FTE). FTE is affected by many factors including the subject population, the operational environment and usability. A high FTE is likely to lead to increased exception handling volumes that will have to be accommodated. There is also an impact on the FAR and FRR if the enrolment process controls the quality level of biometric references accepted by the biometric system.

Buyers of a biometric system would naturally wish for ideal performance in all aspects of the system, such as accuracy, usability, accessibility, throughput and security. However, applications using biometric systems are no different from applications using other technologies in that it becomes necessary to make trade-offs between the various competing factors that constitute desirable performance.

Establishment of the required level of performance for an application will provide information that will allow buyers to eliminate biometric systems that will not meet the required level when integrated into the application.

Having identified biometric systems that meet the required level of performance, there will be a need to consider all the remaining performance trade-offs and decide on an optimum balance for the application. Depending on the relative importance of the different factors involved (such as accuracy, usability, accessibility, throughput and security), different choices might be indicated. This judgement is application dependent and it is of paramount importance that those responsible for establishing the required level of performance have a thorough understanding of the application in order to make correct decisions about these trade-offs.

The level of performance required of a biometric system and its associated application should be identified and described in terms of performance parameters, including:

— Error rates, for example:

— False acceptance rate (FAR);

— False reject rate (FRR);

— Failure to enrol (FTE);

— Application FAR (App-FAR);

— Application FRR (App-FRR);

— Throughput volumes and rates; and

— Exception handling volumes.

The level of performance required should be documented alongside a justification for the level chosen.

Where any performance parameters used to describe the performance of a biometric system under consideration are unclear, an explanation of the parameter should be sought from the supplier.

9.1.4 Security

Security goes beyond the successful recognition of individuals. It is multidimensional and depends upon the nature of the threats as well as the overall system design. Security is affected by:

- fundamental discrimination limits of the technology;
- policies and procedures, which if misstated or misapplied, can completely negate the security; and need to include other interfacing systems including the risks to those systems;
- technical vulnerabilities, errors and oversights by users, and the sophistication of the attack; and
- physical vulnerabilities and the low resistance of physical components to attack.

The detailed evaluation of risk, the design of secure systems and the writing of security policies is not covered in this code of practice. Instead, further guidance on this and, more generally, information security management systems can be found in ISO/IEC 27001 and ISO/IEC 27002.

However, it is worth explaining that the level of security offered by a security mechanism is typically expressed in terms of its resistance to attack, using internationally recognised attack potential levels of basic, moderate and high.

Resistance to an attack potential level of basic is normally considered adequate for access control in a wide range of commercial applications such as those that use four-digit PINs for access control.

Where the application risk assessment has indicated that resistance to a higher attack potential level (i.e. moderate or high) is needed, specialist security expertise can be sought to advise on suitable solutions for particular requirements.

Annex A provides guidance on specifying values of FAR for biometric systems capable of resisting attack potentials levels of basic, moderate and high. For example, a biometric verification system with a FAR of 1 % or lower is deemed to offer adequate resistance to an attack potential level of basic. As most commercially available biometric verification systems can achieve this figure, for many commercial applications the choice of biometric modality and technology can often be made from other considerations such as FRR, convenience, usability, accessibility and cost.

Specifying a FAR requirement that is more demanding (i.e. lower) than actually needed for the application can be counterproductive because, in seeking to meet an over-specified FAR requirement, the usability and other desirable properties of the system can suffer and the implementation and operating costs are likely to increase.

In some smaller applications, the ability for a biometric system to connect to, or interoperate with, another system will not be a necessary requirement. From the point of view of security and privacy, it might be more acceptable to operate a stand-alone biometric system without the capability of sharing data with other systems. However, often the biometric system will form part of an organisation’s wider network and processes. For example, it might be integrated with building access control, time and attendance systems, and logical access to a computer network. In such instances, care needs to be taken to ensure integration does not introduce network security weaknesses.

The security risks associated with the use of a biometric system for a specific application should be assessed and documented. This should include an assessment of:

— the risks likely to result from the incorrect recognition of a subject;

— the risk of integrating the biometric system into other systems;

— data protection risks; and

— risk of system failure due to power outage or other operating problem.

The security requirements for the biometric system should be documented as part of an organisation-wide security policy and information security management system. Annex A outlines some of the security risks and countermeasures associated with a biometric system.

9.1.5 Privacy and data protection

Data protection is an important consideration in planning for the implementation of a EWZ system and its associated application.

The use of biometric data, as personal data, may be regulated in national or international laws. Privacy and data protection compliance is better designed into systems holding personal data right from the start, rather than being added on afterwards. Sometimes it is not even possible to add privacy protection afterwards without completely re-implementing the system.

A core set of identity data often centres on personal data such as name, birth date, and address. The introduction of a biometric system might reduce the amount of additional personal data that has to be collected and stored purely for identification purposes. However, many people still have concerns about the privacy of their biometric and associated data, specifically that the data might be used for purposes other than those that have been declared or that the data might be shared with organisations other than those that have been declared. This could be perceived as a heightened risk as the biometric data could provide a means of linking data about an individual across different systems. Therefore, privacy safeguards can be a critical acceptance factor for individuals who are to use biometric systems.

Experience shows that privacy concerns can be minimised by transparency, particularly in the publication of advance information about the justification for the biometric system and the ways in which the biometric data will be used, shared and processed. The provision of a privacy notice can provide confidence to subjects about the use of their data.

A policy relating to the protection of personal data should be documented and include:

— A requirement that biometric data are considered as personal data and that mechanisms to secure that data are provided;

— How any biometric data are to be secured;

— Details of who is responsible for the security of retained personal data;

— How long any biometric data are to be held;

— How any biometric data which are no longer required are to be deleted;

— Which authorities can be provided with biometric and/or associated data;

— The conditions and limitations under which any biometric and/or associated data can be disclosed;

— What authorisations are required to be in place to provide biometric and/or associated data to other authorities;

— Who should have specified access rights to personal data (including rights to modify and delete), under what circumstances and under what supervision;

— What personal data can be accessed, modified and deleted;

— What notification will be given to the data subject;

— The process for investigating and redressing any complaint of retention contrary to the policy;

— The process for persons to have errors in stored biometric and associated data corrected.

The following aspects should also be addressed:

— The personal data to be collected by a biometric system should be identified and its collection justified;

— A privacy notice should be made available to enrolees to inform them, as a minimum, about which organisation is collecting the data, what data the organisation will be collecting and what the organisation intends to do with the data (including any organisations the data will be shared with);

— Assurances about the measures in place to protect stored biometric and other personal data from loss or unauthorised disclosure should be available to subjects;

— A method for verifying the accuracy of the collected personal data and providing support for the correction of any identified errors should be in place;

— All access and modifications to personal data should be documented;

— A senior person who is accountable for the purpose and manner in which personal data are collected, processed, stored and disposed of should be appointed;

— All staff who act as handlers of personal data should be informed and trained in their responsibilities in the management of personal data.

ISO/IEC TR 24714 1 gives the following privacy recommendations:

— Transparency. There should be a general policy of openness about the use of biometric data, which should include the purposes for which the data is to be used and the point of contact responsible for its use. Any subsequent changes should be made known to data subjects;

— Consent. Biometric data should be collected, used, disclosed and retained with the knowledge and consent of data subject, except where local laws have exemptions to this principle;

— Preference for opt-in. Where feasible and practical, opt-out or opt-in procedures should be made available to the subject. In general, opt-in is the preferred option;

— Limitation of purpose. The purpose(s) of the biometric applications should be specified before implementing the biometric system and documented and made available to affected individuals. The biometric data processing should be limited to the stated purpose;

— Limitation of collection. The collection of biometric data should be limited to the minimum required to achieve the stated purpose(s);

— Limitation of period of retention. The biometric data should be kept only for the period of time necessary for the specified purposes. Procedures should be specified for secure removal of data that is beyond its retention period;

— Adherence to performance criteria. The system operator should ensure the correct function and stability of the system according to its specification and that system malfunction does not cause unnecessary invasion of the subject’s privacy;

— Access rights of the data subject. The data subject should be given reasonable access to verify the correctness of the biometric data and to have incorrect data amended;

— Protection of the data. Biometric data should be protected against unauthorised use or unlawful processing. Opportunities for such misuse should be minimised at the design and development stage of a system. Back-up and archival data should have the same level of protection as active data;

— Secure audit. The EWZ system should be designed to permit a secure audit of the use of biometric data including its deletion or removal from the biometric system. See ISO/IEC 27002:2005;

— Data transfer between jurisdictions. As a best practice, and unless the law of the receiving jurisdiction already provides adequate protection of transfers of biometric data between jurisdictions, the system operator should take reasonable steps to ensure that the data transferred continues to be adequately protected, such as by following model contracts for the transfer of personal data such as those offered by the Article 26(4) of directive 95/46/EC Data Protection Working Party of the European Commission, even though this may not be a legal requirement in the jurisdictions in which the organisation operates;

— Significant automated decisions. Where EWZ systems are used to make significant and fully automated decisions about individuals, a mechanism to request the intervention of a person should be provided. Individuals should be notified of such automated decisions;

— Accountability. A person within the system operator's organisation should be accountable for compliance with these principles;

— Accuracy of biometric data. Biometric information should be as accurate, complete, and up to date as is necessary for the purposes for which it is to be used;

— Anonymisation of data. Release of biometric data for academic, statistical or testing purposes should be considered and controlled carefully. Links to other personal information should be removed where they could lead to identification of an individual.

9.1.6 Usability

The usability of a biometric system is crucial for optimal performance and it is important that detailed attention is given to this aspect.

Specific usability issues for EWZ biometric systems are addressed in ISO/IEC TR 24714 1. The impact of these issues will vary considerably according to the specific biometric system being used and the application in which it will be deployed.

An EWZ biometric system should be assessed to determine its usability. The assessment should include a determination of whether the EWZ biometric system is:

— intuitive, logical and easy to understand;

— simple to use with a low physical and cognitive effort;

— efficient in respect of time taken to accept or reject subjects; and

— tolerant of error by the subject.

If the subject has to perform a number of actions (e.g. enter an account number, present a card and use a biometric system), the sequence of actions should be logically ordered to help the subject.

Prompts and instructions should be provided by the biometric system:

— to indicate the location of any user interface;

— to provide feedback on the success or failure of an action performed on the biometric system by the subject; and

— where there is a need for an action to be repeated.

Further recommendations and guidance can be found in ISO/IEC TR 24714 1.

9.1.7 Accessibility

All recognition systems, whether through smart card, PIN or password, need to cater for impaired populations to some extent. Biometric systems are no exception. ISO/IEC TR 24714 1 discusses in detail issues of accessibility in biometric systems and should be referred to for full details. It is important that all reasonable efforts are made to ensure a biometric system is able to be used by as large a proportion of the intended subject population as possible.

No current biometric system can be designed to recognise all individuals. The degree to which a biometric system is accessible will depend on a number of factors, including the nature of the subject population, the usability of the system and the physical environment in which it operates.

Some people might have cultural objections to a specific biometric modality. Most cultures accept photographic evidence of identity and therefore might accept a biometric system that incorporates face recognition, but this might not be the case if the culture encourages the wearing of veils or headscarves for certain groups. Individuals in other cultures might have strong objections to touching shared surfaces like fingerprint sensors or hand geometry units, especially if these are not fully visible to the subject. Some biometric systems might perform more poorly when encountering cultural or socially related body ornamentation, such as make-up, tattoos, jewellery, clothing or facial hair, and therefore might not be practical or acceptable.

Some people have registered disabilities that might make biometric recognition difficult. A relatively larger number of people have some other form of impairment that might prevent them using a biometric system as effectively as a subject without such impairment. Some people have a combination of impairments, the cumulative effect of which will amplify the impact of individual impairments. For example, there will be subjects who cannot be enrolled on the system because they lack the required biometric characteristic or the characteristic is so poorly defined or is so unstable as to be unsuitable for use.

Difficulties with accessibility can be long term or temporary and can occur without warning, for example, following the sudden onset of illness such as laryngitis or a sore throat, dental or eye surgery or other physical injury.

In some cases, the problems of accessibility can be mitigated by changes in the design of the environment, for example, by providing height-adjustable data capture devices or optimised lighting conditions. For other degrees of impairment, radical changes in design might be needed.

Whatever strategy is employed in addressing accessibility issues, a biometric system designed with accessibility in mind at an early stage will reduce the risk of challenge under discrimination legislation.

Attention is drawn to the requirements of international equality standards and conventions. These generally require equal treatment in access to employment as well as private and public services, regardless of the protected characteristics of:

— age;

— disability;

— gender reassignment;

— marriage and civil partnership;

— pregnancy and maternity;

— race;

— religion or belief;

— sex; and

— sexual orientation.

A biometric system should be assessed to determine its accessibility. ISO/IEC TR 24714 1 discusses in detail issues of accessibility in biometric solutions and should be referred to for full details. The assessment of accessibility should include a determination of whether the implementation of the biometric system and the application would discriminate against any particular ethnic or social group.

There should be a documented assessment of how a biometric system enables an organisation to meet its obligations under any equality laws in the particular jurisdiction, or any international standards or conventions which provide for equality for several protected characteristics, including disability. This assessment should be reviewed whenever there is a change to such legislation, standards, or conventions.

There should be provision for subjects who cannot use the biometric system or would find it difficult to use, for example:

— Extra assistance;

— Facilities for carers or accompanying guardians;

— Physical privacy; and/or

— An alternative recognition system.

Prompts should be provided in a combination of audio, visual and tactile forms.

When an EWZ biometric system is intended for use by a multicultural subject population, the style of language, metaphors and imagery that are included in any information and training material to be provided in relation to the use of a biometric system should be appropriate for all the respective cultural groups.

Instructions and prompts should be provided in the languages that the subject population would understand.

The location of the data capture station should be clearly indicated to meet the needs of blind or partially sighted people.

9.1.8 User acceptance

ISO/IEC TR 24714 1 describes user acceptance as a crucial factor for system performance. A non-cooperative user will decrease the performance of the system, in a mandatory environment as well as in a voluntary environment. Concerns that influence user acceptance can either be logically founded and on a technical level or they can be subjective and less tangible.

ISO/IEC TR 24714 1 describes factors, such as reliability and performance, privacy, convenience or ease of use, that influence user acceptance. It also recommends actions for accessibility testing.

However, even if all technical and non-technical factors are dealt with, especially when a new system is installed, the user needs an additional benefit of using this system rather than a traditional means of identification. This additional benefit might again be objective (e.g. less time spent at border control) or subjective (e.g. being the first to use a contactless fingerprint system).

9.1.9 Data capture

9.1.9.1 Enrolment

Enrolment is generally defined as the process of collecting one or more biometric samples from an individual, and the subsequent creation of a biometric reference against which future comparisons will be made to recognise the known individual. The authentication of

the individual as part of the enrolment process is critically important. The performance and usability of a biometric system is critically dependent on the quality of the biometric enrolment data. Poor quality enrolments might require comparison thresholds to be set in ways that weaken the security of the application to mitigate the poor usability of the biometric system by the subject. See also ISO/IEC TR 29196.

There are a number of factors that affect the quality of the biometric sample captured during enrolment, these include:

— Enrolment procedures;

— Training of biometric attendants;

— Design of the data capture station;

— Environmental factors at the data capture station.

Well-trained biometric attendants can often provide valuable assistance to enrolees who are experiencing difficulties, although this can be subject to limitations where, for example, the operational policy prohibits biometric attendants from physically touching enrolees to help position them correctly. The biometric attendants' experience can reduce the variability of quality of the biometric reference introduced by unhelpful aspects of human behaviour including the wrong pose, an unwanted facial expression, dry skin or a medical condition.

The use of biometric attendants might also be an effective safeguard against malevolent enrolees who might seek to subvert the enrolment process, e.g. through the attempted use of an artefact.

The presence of well-trained biometric attendants at enrolments has been shown to significantly improve the quality of biometric references. The quality of biometric references in turn has a significant effect on the biometric system FAR and FRR.

A subject's entitlement to be enrolled in a biometric system can be established as part of the enrolment process. For example, their identity might be confirmed through the registration of non-biometric personal data (e.g. using ID cards or passports) whose authenticity and integrity can be checked by trusted biometric attendants ('identity proofing').

The enrolment process is likely to be the first time that the subject comes in contact with the biometric system equipment. The enrolment procedure needs to inform and relax the subject and is likely to include:

— Direct face-to-face support;

— Written material (provided in an inclusive and comprehensible manner) in the form of posters and information leaflets;

— Multimedia demonstrations.

As with the introduction of any new technology, subject familiarity and past experiences of biometric systems will have a considerable effect upon acceptance and subsequent successful use. So, it is important to train the subject in the use of the system early on and to ensure the training is a positive experience. Also, providing an opportunity to practice using the system will help habituation, which can improve both the quality of biometric samples taken and the throughput of the system.

Even simple issues can cause additional problems, which could be avoided by planning ahead and training. For example, if a subject and biometric attendant sit facing each other, they need to establish a mutually agreed view of 'left' and 'right' if this is significant in the enrolment process.

In some cases the subject could be unaware of the fact that a biometric enrolment is taking place, for example, when submitting a photograph for an application where the photograph is used to enrol the subject in the system. In such circumstances, it is

important that a subject is aware of what data are being recorded and how the data are going to be used. Some legislations require the explicit agreement or at least the information of the person to be enrolled and/or that certain data is used in a biometric system.

One systematic source of variability of biometric performance is the changes that occur over time in a subject's biometric characteristics caused by biological ageing or behavioural changes. This can give rise to an increase of false rejections. A subject's capability to use a biometric system can also degrade with illness or injury. Therefore, it might be necessary for re-enrolment to be carried out at a fixed interval of time or in response to reductions in matching performance recorded by the system over time.

An enrolment process should be in place and documented, including details of:

— What credentials to check to establish eligibility to enrol;

— Who is allowed to conduct enrolments in terms of authorisation and training;

— Any quality thresholds that have to be met for an enrolment to be deemed successful;

— How to decide that an eligible subject is unsuitable for enrolment and therefore should use an exception handling process;

— Whether informed consent is required and how to obtain it;

— Training for subjects in using the biometric system;

— When re-enrolment takes place and when a subject's enrolled details expire.

An assessment should be made as to whether biometric attendants are to be present at enrolment. If biometric attendants are present, they should be specifically trained in the process and the data capture station should provide feedback to them as to the success or failure of enrolments.

Subjects should be informed, as a minimum and as part of the enrolment process, about the reasons for the use of a biometric system, about how accessibility has been built into the system (including reference to exception handling) and of the privacy notice (see 7.5.2).

Subjects should be trained in the use of the biometric system during enrolment and given the opportunity to practice using the system in order to increase familiarity.

9.1.9.2 Data capture station

The ergonomic design of a data capture station has a very strong correlation with the quality of captured biometric characteristic (for both enrolment and recognition) and for the satisfaction felt by the subject.

The design of a data capture station needs to take account of the target subject population, in particular whether there will be a need to accommodate subjects who might have difficulties with enrolment or recognition because of disability or other physical or cognitive problems. Examples include wheelchair users, arthritis sufferers, those with auditory or visual impairments and those with medical conditions that render them unable to control their limbs, head or eyes.

Designing data capture stations to deal with these conditions can be extremely challenging. Conditions will militate against the choice of a specific biometric modality. Flexibility in adjustment in height and angle of data capture devices or a choice of alternative data capture devices can help to improve accessibility for a wider range of enrolees with disabilities and other medical conditions. Therefore, the position and orientation of a data capture device is also an important consideration.

Feedback to assist subjects in presenting their biometric characteristics correctly to the data capture device is helpful, for example, feedback on where to place a finger on a

fingerprint reader or where to stand and look for a facial recognition or iris systems. This feedback could be provided either automatically by the equipment or manually by a biometric attendant (if present) and is best given at the point of use.

Appropriate designs of a data capture station for enrolment or recognition can take the form of, for example, a desktop workstation, an 'across the counter' setup, a 'pod' configuration, a kiosk or a mobile kit. Selection of the configuration will depend on a number of factors, including environmental, space and cost considerations.

Protective clothing can present problems for data capture devices depending on the biometric modality used. For example, if protective gloves have to be worn, fingerprint recognition would be unlikely to be suitable. Other examples of possible problem clothing types are hard hats, protective glasses, goggles and welders' masks, face masks that cover the mouth and nose, and heavy boots or knee protectors that could modify a subject's posture.

A data capture station should be designed to be usable and accessible for both subjects and biometric attendants.

The configuration of a data capture device should be determined through an assessment of:

— how the subject will interact with the device and any biometric attendants in terms of both physical and psychological comfort; and

— how easy it is to collect a biometric characteristic with the best achievable quality.

The design of a data capture station should take account of whether the station is attended or unattended.

A data capture station should be designed and located to prevent individuals not involved in data capture from interfering with the process of data capture.

An assessment of whether biometric attendants and personal assistants are allowed to assist subjects during data capture should be conducted and, if so, the design of any designated data capture station should be such that it accommodates this assistance.

A data capture station should be designed to accommodate variations in the height and reach of the subject population.

Feedback should be given to the subject to assist with the correct presentation of their biometric characteristic.

If a subject is required to wear personal protective equipment (PPE) when using a biometric system, the system should be one that allows the subject to present a biometric characteristic without having to remove the PPE. The data capture should not require the subject to change his or her usual behaviour. For example, a person wearing glasses should not have to remove them but the system developer should note that ISO/IEC 19794-5 makes recommendations that should be considered.

9.1.9.3 Environment

All biometric systems are subject to variability in performance due to a range of environmental factors, including those associated with the built environment, such as lighting, temperature, audible noise and electrical noise. ISO/IEC 29197 is being developed (currently in draft form) and should be consulted on environmental issues.

It is particularly important to ensure good environmental conditions for enrolment because poor conditions will usually result in the creation of low quality biometric references, which will lead to poor performance through increased biometric recognition error rates. The failure to enrol (FTE) rate and application false rejection rate (App-FRR) are likely to be substantially higher than those that can be achieved under good environmental conditions.

Problems can be created by extremes of temperature and humidity, contamination from dust or chemicals, the need for protective clothing and protection against vandalism, levels of artificial or natural illumination, the position and orientation of the biometric device and the presence of other fixtures and fittings in the vicinity. The extent to which these have an impact on the biometric system performance varies according to the biometric modality.

Climatic extremes, in particular extremes of temperature or humidity, can present problems to sensitive data capture devices and hinder the capture of good quality biometric data. For example, extremely dry environments might not allow optimal capture for fingerprints and in outdoor locations exposure to fog, rain or snow and ice or condensation on a sensor such as a camera lens can affect data capture.

Subjects can also be affected by climatic conditions in a way that impacts upon biometric system performance. They might have to remove gloves, hats, scarves or sunglasses. Extremes of temperature can cause fingerprints to be more dry or moist depending on the environment. High temperatures could cause the subject to sweat excessively impeding the capture of the biometric data.

The ambient environment can also have an adverse effect. High levels of ambient noise from people, machinery, public address systems or traffic might prevent biometric data from being collected or recognised where the biometric modality is sensitive to noise levels (e.g. when voice recognition is the biometric modality). Such noise interference can also prevent users and subjects from hearing spoken instructions, which can be especially problematic for blind or partially sighted subjects who rely on these instructions.

Contamination from dust or chemicals is another environmental factor to consider (e.g. in engineering or industrial locations or in locations where food is prepared and there are high levels of oil particles from frying food). Under such conditions, it can require unusually high maintenance to keep a data capture device clean and to prevent corrosion, so it is a good idea to keep devices in an enclosure that is protected from the working environment.

A data capture device in an external location or internal public space can be subject to additional challenges, such as vandalism including attack with a heavy or sharp object or by spray-painting. The use of CCTV or the presence of biometric attendants could act as a deterrent to such activities.

In many public areas it could also be useful to provide booths or kiosks where the environment can be controlled to enable the performance requirements of a data capture device to be achieved.

Further information on the environmental sensitivities of biometric modalities can be found in ISO/IEC TR 24714 1.

A data capture device should be maintained in the environmental conditions specified by the manufacturer of the device as optimum for the performance of the biometric system otherwise performance could be compromised.

An assessment should be conducted to identify whether there is a need to house the data capture device in an enclosure (such as in a separate room, in an enclosed booth or with a simple guard covering the device) to ensure the optimum performance of the device is maintained.

Where a data capture device is monitored in direct line of sight or using CCTV to enable assistance to be given or to spot and record malevolent behaviour, the device should be located in such a way that there is an unobstructed view of the interaction between the subject and the device.

Lighting in the vicinity of a data capture device should be assessed to determine if it maintains the level of security required for the vicinity whilst minimising possible interference to the device by excessive or uneven illumination.

Ambient noise in the vicinity of a data capture station should be assessed to determine whether the noise could interfere with audible instructions given to subjects or could interfere with the acquisition of a biometric sample, e.g. for voice recognition.

9.1.9.4 Exception handling

It is important to recognise that an exception handling process is a potential security vulnerability because many exception handing processes can offer less security than the biometric system.

An assessment of the likely exception handling volume, perhaps by reference to other similar biometric systems that have already been deployed, is an essential part of planning for the implementation of a biometric system. The exception handling volume can even amount up to 5 % to 10 % of the expected total number of subjects using a biometric system.

The exception handling process can consist of:

— another instance of the same biometric modality (e.g. a different finger on a fingerprint system);

— an alternative modality (e.g. iris image modality instead of a fingerprint modality);

— some other form of machine-readable identification (e.g. smart card and PIN); and/or

— another individual, normally a member of staff, identifying the individual using comparison of his/her appearance or signature to the corresponding image on an identity document.

For example, in the case of physical access control where biometric recognition might generally be controlling a turnstile or door, the exception handling process could be an attended entry facility for wheelchair access.

It is important that any exception handling process is designed to accommodate the number of exceptions that an application is expected to encounter. The exception handling volume can be estimated by assessing the expected application false rejection rate (App-FRR) against the expected throughput volume.

Exception handling processes will need to be designed and implemented with attention to security requirements. If the exception handling system security is weaker than the primary recognition system, forcing an exception could be used to exploit this security weakness.

An exception handling process should be in place to provide an alternative means of recognition to accommodate:

— occurrences of false rejection; and

— a subject who is unable to use the biometric system as a result of a particular disability or impairment.

The exception handling process should be capable of handling the volume and nature of exceptions likely to be encountered among the population of subjects.

The exception handling process should be reviewed after a specified period of time and in the light of operational experience with the aim of improving the process to address issues where they are identified.

9.1.10 User acceptance testing

The extent of acceptance of a biometric system is often evaluated by means of focus groups or running surveys, usually managed at an early stage of consideration of the introduction of a biometric system. Questions can also be asked of participants in scenario tests directly after they have taken part in a trial.

Focus group studies offer the opportunity to explore issues with specific candidate devices, follow up on concerns raised in the discussion and explore the receptiveness to proposed interventions.

Surveys allow a wider sample of the target group to be questioned, although it can be difficult to get a representative population to respond. It may be that those with most concerns or most interested in the technology will reply, skewing the response. Also, many of the participants in the survey may never have had contact with the technology and may base their replies to questions on idealisations popularised by films and TV series. Furthermore, answers will depend on the context in which the question is put and the trust that the respondents place in the integrity of the survey organisers. As a consequence, a reply that a specific biometric technology is more or less acceptable to a population needs to be examined critically. There should always be supporting evidence of a validated survey methodology in the context of the specific type of application under consideration. As a minimum, a study using surveys should offer the following in order to interpret its results:

— A sample questionnaire and the associated telephone scripts, especially if the questions relating to biometrics form part of a more general survey; (scripts may describe certain features of the technology, while remaining silent about crucial aspects of their operation);

— The dates of start and completion of the survey, as media comment during the survey period may affect the results;

— The method of selection of participants, the numbers successfully contacted, together with an indication of reasons for non-response and any weighting factors applied to the results; and

— Any incentives which were offered.

Ideally, best results would come from combined scenario trials and facilitated focus groups using individuals from the target population, along with supporting questionnaire surveys.

Focus groups can be used at first to elicit the major concerns. This qualitative research can then inform the design of questionnaires which could track changes in acceptance as individuals experience the application in both limited proof of concept trials as well as preliminary rollouts. Results from the surveys can then influence decisions on the design of systems, the information which is provided to new entrants to the scheme, telephone helplines, etc. Tracking the levels of acceptance as a deployment proceeds allows the organisation to assess the impact of habituation to the system, highlighting those areas which are proving particularly difficult to gain acceptance for.

Whichever approach is taken, test organisations should use experts in their respective fields, whether it is for facilitating the focus group or to design questionnaires to survey perceptions.

9.1.11 Usability and accessibility testing

Throughput volumes, exception handling volumes and App-FRR testing are all interdependent. The App-FRR will be the main driver in the generation of exceptions. Increased volumes of exception handling will reduce the throughput of the application. However, altering the biometric system threshold settings to reduce the number of false rejections might not be the solution to an unacceptable App-FRR as this might not meet the security requirements for the application. The most likely reasons for a higher than anticipated App-FRR will be:

— subject unfamiliarity with the biometric system;

— poor biometric reference resulting from poor enrolment;

— inadequate training of biometric attendants; and

— poor design of the data capture station, in particular instructions and prompts (including signage).

Impostor testing can also form part of the usability and accessibility testing. This will not directly represent the FAR of the biometric system or the App-FAR. However, by attempting impostor testing, an assessment can be made of the application security with all of the security procedures in place. In particular, the exception handling process and fallback arrangements can be exercised to assess if unacceptable security weaknesses have been introduced into the application.

Usability and accessibility have to be tested to quantify the subjective nature of subject perceptions. Surveys of these perceptions can be compiled to elicit issues and provide quantifiable measures. Such surveys can be anonymous. Note, however, that personal data might need to be collected to enable the assessment of trends or groupings within the results. Such data might include:

— Age;

— Gender;

— Ethnicity;

— Left or right handedness;

— Known impairments; and

— Height.

Quantification of subject perceptions can be arranged in steps from 'strongly agree' to 'strongly disagree'. It is preferable to ensure the number of steps force a decision rather than allowing an easy default to 'neither agree nor disagree'.

Subject surveys can also be supplemented by in-depth subject interviews and behavioural observations conducted by trained independent observers.

Usability and accessibility results can be used for acceptance testing as well as for corrective action or improvement planning.

Some usability and accessibility testing can require an extended period of time for completion, so system acceptance might not be signed off until well after operational use has commenced. For example, biometric system performance is likely to improve as subject familiarity increases. Similarly, as familiarity increases, the volume of exception handling might decrease. This can provide the opportunity to review the biometric system threshold settings as part of change management procedures, noting that biometric system performance would need to be retested if thresholds are changed.

Further information on biometric performance testing and reporting can be found in the ISO/IEC 19795 series of standards, in particular, parts 1, 2 and 6 which address Principles and Framework, Technology and Scenario Evaluations and Operational Evaluations, respectively.

Acceptance of the biometric system should be based on tests that demonstrate conformance to the performance requirements specified during procurement, including:

— Throughput volumes and rates;

— Exception handling volumes;

— Application FRR (App-FRR) and application FAR (App-FAR);

— Usability in terms of the efficiency of the system, its effectiveness and the satisfaction of users (such as subjects, biometric attendants and supervisors); and

— Accessibility.

The number of subjects selected to test the performance parameters should be representative of the expected type and volume of subjects and biometric attendants.

All biometric system settings including threshold settings that are set during acceptance testing should be documented and subsequently controlled during operation

If the biometric system threshold settings are altered at any stage during or after usability and accessibility testing, any usability and accessibility testing related to the changed settings should be repeated.

All results generated from usability and accessibility testing should be documented.

9.2 Operating an EWZ system

9.2.1 General

An organisation operating an EWZ system is advised to make necessary efforts to identify legislation that applies to their particular use of a system. Particular attention should be given to legislation concerning equality and data protection. Where legislation is not in place an organisation may review the applicability of international standards or conventions.

Legislation applicable to the use of a biometric system should be identified and a review should be conducted to determine how the legislation applies to the operational processes associated with a biometric system.

The operational processes associated with the biometric system should be reviewed whenever there is a change to applicable legislation to determine whether any changes to operational process are required.

9.2.1.1 Maintenance

The maintenance of an EWZ system once it is in operation needs to be considered prior to its initial deployment and, just as for any other IT system, a maintenance plan should be part of the procurement of the system and should be negotiated with the system supplier. The IEC 60300 family of standards give much useful advice on dependability management of such systems and how to include this in system procurements. There are, however, some specific issues for biometric systems which need to be considered and these are discussed below.

Some data capture devices, particularly those that come in contact with people during use, will need regular maintenance. Manufacturers generally specify details of their equipment's maintenance requirements, including which types of cleaning products to use. It is important that maintenance and cleaning personnel be instructed in these requirements.

A biometric system should provide alerts in the event of malfunctions or degradation in performance so that maintenance procedures can be performed.

A biometric system that has undergone maintenance should be tested to determine that it is still operating as expected. A description of the type of testing to conduct after each maintenance task should be documented.

A data capture device should be cleaned in accordance with the manufacturer's instructions to avoid contaminants such as moisture, dust or debris from affecting the performance of a biometric system.

9.2.1.2 Change management

EWZ biometric system thresholds that have an impact on FAR and FRR are set at the time of installation and are only changed following a documented procedure. Where thresholds are relaxed in an attempt to lower the number of false rejections of legitimately enrolled subjects, without the support of a structured risk assessment and testing, security breaches can occur that have not been anticipated. Therefore, it is essential that a thorough risk assessment is first completed before making any changes

in the biometric system threshold to minimise the risk that the security of the system is compromised if the FAR is allowed to increase.

It is useful to consider developing a policy for equipment replacement as part of the change management process. This might involve a change of supplier, equipment or software rather than just a like-for-like swap. The use of equipment that conforms to international standards, such as those produced by the International Organization for Standardization (ISO), could simplify the replacement process and ensure long-term viability of the biometric system.

Changes to the settings of a biometric system should be made in accordance with a documented procedure, which should include a risk assessment and an auditable approval of the new settings.

Following any changes to the settings of the biometric system, testing should be conducted to verify that the performance conforms to specified criteria. Such tests can be a repeat of those performed during acceptance testing.

9.2.1.3 Management information system data

Management information system data could include data capture times, data quality and system match/non-match decisions. Trend analysis of such statistics could help in making decisions on, for example, equipment replacement or alterations in maintenance schedules.

A biometric system should make provision for the collection of management information system data, to allow the monitoring and analysis of trends in performance.

9.2.1.4 Fallback arrangements

- Fallback arrangements are specific to the biometric system and would form part of an organisation's overall business continuity plan. Further guidance on for information and communication technology readiness for business continuity is given in ISO/IEC 27031.
- Fallback arrangements should be in place in order that an application can continue in the event of a biometric system failure or while elements of a biometric system are under repair or adjustment.
- Fallback arrangements should conform to previously defined security requirements to ensure that system security is not compromised during fallback operation.
- Fallback arrangements should be tested to validate their effectiveness.

10 Conclusions

Organisations throughout Europe are looking to deploy early warning zones (EWZs). Some early practical tests of the concepts behind EWZs have shown at least anecdotal benefits that can accrue from such systems. There is, however, very little information that has been made available in the open press to enable a detailed scientific analysis of the expected performances of such systems.

Recent years have witnessed significant advancements in AI methods which may support systems developed for EWZs. In particular, methods for machine learning, data analytics and artificial cognition and perception. It is widely recognised that automated video (e.g. CCTV) surveillance plays an important role in EWZs and CI protection. AI for video surveillance exploits the latest developments in AI methods including advanced video analytics and behavioural understanding. Such developments mean that it is now possible to construct sensor networks that are capable of interpreting proactively in real time, or post event, dynamic EWZ scenes and to identify persons and vehicles of interest, events and threats. However, significant gaps in capability exist. Future research for protection of critical infrastructure should address methodologies and systems which exploit the latest advances in machine learning (e.g. deep learning), which are robust in their deployment and analytic performance across a wide range of EWZ environments, operate both on fixed as well as mobile platforms over an extended period of time, and exploit the latest research in user interfaces, to increase the likelihood of acceptance by operators.

This report captures the work performed by the team as it has looked at a range of issues that would need to be quantified to enable organisations to fully plan and quantify the benefits from such systems.

The team would welcome the opportunity to extend this work into new areas and look to enhance the integration of the work using the outline tools it has presented including the use cases, data protection impact prototype and the implementation checklists.

References

Agrafioti, F. (2012), 'ECG in Biometric Recognition: Time Dependency and Application Challenges', University of Toronto, Toronto, http://hdl.handle.net/1807/31673 (accessed 19 June 2019).

Amerland, R., Scharfenberger, C., Kazemzadeh, F., Pfisterer, K. J., Lin, B. S., Clausi, D. A. and Wong, A. (2015), 'Feasibility of long-distance heart rate monitoring using transmittance photoplethysmographic imaging (PPGI)', *Scientific Reports*, Vol. 5, doi: 10.1038/srep14637.

Blanco-Gonzalo, R., Sanchez-Reillo, R., Miguel-Hurtado, O. and Liu-Jimenez, J. (2014), 'Performance evaluation of handwritten signature recognition in mobile environments', *IET Biometrics*, Vol. 3, No 3, pp. 139-146.

Bond, C. F. and DePaulo, B. M. (2006), 'Accuracy of deception judgements', *Personality and Social Psychology Review*, Vol. 10, No 3, pp. 214-234.

Burt, A., Shirrell, S., Leong, B. and Wang, X. (2018), 'Beyond Explainability: A Practical Guide to Managing Risk in Machine Learning Model', Future or Privacy Forum, Washington, DC, https://fpf.org/wp-content/uploads/2018/06/Beyond-Explainability.pdf (accessed 19 June 2019).

Cai, Q. and Aggarwal, J. K. (1996), 'Tracking human motion using multiple cameras', Proceedings of 13th International Conference on Pattern Recognition, Vienna, Austria, Vol. 3, doi: 10.1109/ICPR.1996.546796.

Clarke, R. (2004), 'A History of Privacy Impact Assessments', 6 February 2004, http://www.rogerclarke.com/DV/PIAHist.html (accessed 19 June 2019).

Common Criteria (2009), 'Common Methodology for Information Technology Security Evaluation Version 3.1', https://www.commoncriteriaportal.org/files/ccfiles/CEMV3.1R3.pdf (accessed 19 June 2019).

Common Criteria (2017), 'Common Criteria for Information Technology Security Evaluation — Part 1: Introduction and general model Version 3.1', https://www.commoncriteriaportal.org/files/ccfiles/CCPART1V3.1R5.pdf (accessed 19 June 2019).

Das, R., Maiorana, E. and Campisi, P. (2018), 'Motor Imagery for Eeg Biometrics Using Convolutional Neural Network', 2018 IEEE International Conference on Acoustics, Speech and Signal Processing, Calgary, Alberta, Canada, doi: 10.1109/ICASSP.2018.846190.

Davies, B., Innes, M. and Dawson, A. (2018), 'An evaluation of South Wales Police's use of Automated Facial Recognition', Cardiff University, Cardiff, UK.

Den Hollander, R. J., Bouma, H., van Rest, J. H., ten Hove, J. M., ter Haar, F. B. and Burghouts, G. J., 'Automatically assessing properties of dynamic cameras for camera selection and rapid deployment of video content analysis tasks in large-scale ad-hoc networks', *Counterterrorism, Crime Fighting, Forensics, and Surveillance Technologies,* Vol. 10441, doi: 10.1117/12.2268797.

Edwards, L. and Veale, M. (2018), 'Enslaving the Algorithm: From a "Right to an Explanation" to a "Right to Better Decisions?" ', *IEEE Security & Privacy*, Vol. 16, No 3, pp. 46-54.

European Union Agency for Network and Information Security (ENISA) (2017), *Handbook on Security of Personal Data Processing*, ENISA, Heraklion, Greece.

Ferryman, J. (2016), *Video surveillance standardisation activities, process and roadmap*, Publications Office of the European Union, Luxembourg.

Future of Privacy Forum (2018), 'The Privacy Expert's Guide To Artificial Intelligence and Machine Learning', Future of Privacy Forum, Washington, DC, https://fpf.org/wp-content/uploads/2018/10/FPF_Artificial-Intelligence_Digital.pdf (accessed 19 June 2019).

Giannopoulos, G., Filippini, R. and Schimmer, M. (2012), *Risk assessment methodologies for Critical Infrastructure Protection. Part I: A state of the art*, Publications Office of the European Union, Luxembourg.

Gidaris, S. and Komodakis, N. (2016), 'LocNet: Improving Localization Accuracy for Object Detection', 2016 IEEE Conference on Computer Vision and Pattern Recognition (CVPR), Las Vegas, NV, USA, doi: 10.1109/CVPR.2016.92.

Gong, S., Cristani, M., Yan, S. and Loy, C. C. (eds.) (2014), *Person Re-Identification*, Springer, Berlin.

Grother, P. J., Quinn, G. and Ngan, M. (2017), 'Face In Video Evaluation (FIVE) Face Recognition of Non-Cooperative Subjects', National Institute of Standards and Technology, Gaithersburg, MD, https://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8173.pdf (accessed 17 June 2019).

Grother, P. J., Ngan, M. L. and Hanaoka, K. K. (2018), 'Ongoing Face Recognition Vendor Test (FRVT) Part 2: Identification', National Institute of Standards and Technology, Gaithersburg, MD, https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8238.pdf (accessed 17 June 2019).

Harris, B. (2018), 'Terrorist attacks are in decline for the third year running', World Economic Forum, https://www.weforum.org/agenda/2018/10/terror-attacks-have-dropped-2018-us-state-department (accessed 19 June 2019).

Hosang, J., Omran, M., Benenson, R. and Schiele, B. (2015), 'Taking a deeper look at pedestrians', 2015 IEEE Conference on Computer Vision and Pattern Recognition (CVPR), Boston, MA, USA, doi: 10.1109/CVPR.2015.7299034.

International Biometric Group (2006), *Comparative Biometric Testing Round 6 Public Report*, International Biometric Group, New York.

International Organization for Standardization (ISO) (2018), ISO/IEC 19794 Information technology — Biometric data interchange formats (series), ISO, Geneva, Switzerland.

International Organization for Standardization (ISO) (2018), ISO/IEC TR 24741:2018 Information technology — Biometrics — Overview and application, ISO, Geneva, Switzerland.

International Organization for Standardization (ISO) (2015), ISO/IEC TR 29156:2015 Guidance for specifying performance requirements to meet security and usability needs in applications using biometrics, ISO, Geneva, Switzerland.

International Organization for Standardization (ISO) (2013), ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements, ISO, Geneva, Switzerland.

International Organization for Standardization (ISO) (2013), ISO/IEC 27002:2013 Information technology — Security techniques — Code of practice for information security controls, ISO, Geneva, Switzerland.

International Organization for Standardization (ISO) (2011), ISO/IEC 27031:2011 Information technology — Security techniques — Guidelines for information and communication technology readiness for business continuity, ISO, Geneva, Switzerland.

International Organization for Standardization (ISO) (2008), ISO/IEC 15408 Information technology — Security techniques — Evaluation criteria for IT security (series), ISO, Geneva, Switzerland.

International Organization for Standardization (ISO) (2008), ISO/IEC 18045:2008 Information technology — Security techniques — Methodology for IT security evaluation, ISO, Geneva, Switzerland.

International Organization for Standardization (ISO) (2008), ISO/IEC 19795 Information technology — Biometric performance testing and reporting (series), ISO, Geneva, Switzerland.

International Organization for Standardization (ISO) (2008), ISO/IEC TR 24714-1:2008 Information technology — Biometrics — Jurisdictional and societal considerations for commercial applications — Part 1: General applications, ISO, Geneva, Switzerland.

IT Security Association Germany (TeleTrusT) and European Union Agency for Network and Information Security (ENISA) (2019), IT Security Act (Germany) and EU General Data Protection Regulation: 'State of the art' — Technical and organizational measures, https://www.teletrust.de/fileadmin/docs/fachgruppen/2019-05_TeleTrusT_Guideline_State_of_the_art_in_IT_security_ENG.pdf (accessed 19 June 2019).

Johnson, D., Zagorecki, A., Gelman, J. M. and Comfort, L. K. (2011), 'Improved Situational Awareness in Emergency Management through Automated Data Analysis and Modeling', *Journal of Homeland Security and Emergency Management*, Vol. 8, No 1, doi: 10.2202/1547-7355.1873.

Joo, H., Park H. S. and Sheikh, Y. (2014), 'MAP Visibility Estimation for Large-Scale Dynamic 3D Reconstruction', 2014 IEEE Conference on Computer Vision and Pattern Recognition, Columbus, Ohio, USA, doi: 10.1109/CVPR.2014.147.

Karagiannis, G. M. and Synolakis, C. E. (2017), 'Twenty challenges in incident planning', *Journal of Homeland Security and Emergency Management*, Vol. 14, No 2, doi: 10.1515/jhsem-2016-0061.

Kim, J. and Park, K. S. (2017), 'Human Identification Using Non-Invasive Biological Signals', 39th Annual International Conference of the IEEE Engineering in Medicine and Biology Society, 11-15 July, Jeju Island, Korea.

Kim, J. and Lee, S. (2018), 'Telebiometric Personal Authentication Technologies using Bio-Signals', 40th Annual International Conference of the IEEE Engineering in Medicine and Biology Society, 17-21 July, Honolulu, HI, USA.

Klaver, M. H. A., Luijif, H. A. M., Nieuwenhuijs, A. H., Cavenne, F., Ulisse, A. and Bridegeman, G. (2008), 2008 First International Conference on Infrastructure Systems and Services: Building Networks for a Brighter Future (INFRA), Rotterdam, Netherlands, doi: 10.1109/INFRA.2008.5439614.

Li, T., Chang, H., Wang, M., Ni, B., Hong R. and Yan, S. (2015), 'Crowded Scene Analysis: A Survey', *IEEE Transactions on Circuits and Systems for Video Technology*, Vol. 25, No 3, pp. 367-386.

Mansfield, A. J. and Wayman J. L. (2002), 'Best Practice Guide for Biometric Testing', National Physical Laboratory/Centre for Mathematics and Scientific Computing, Middlesex, UK, http://eprintspublications.npl.co.uk/2460/1/CMSC14.pdf (accessed 17 June 2019).

Marcenaro, L. (2016), *Access to Datasets*, Publications Office of the European Union, Luxembourg.

Mustafa, A., Kim, H., Guillemaut, J.-Y. and Hilton, A. (2016), 'Temporally coherent 4D reconstruction of complex dynamic scenes', 2016 IEEE Conference on Computer Vision and Pattern Recognition (CVPR), Las Vegas, NV, USA, doi: 10.1109/CVPR.2016.504.

Nam, H. and Han, B. (2016), 'Learning Multi-Domain Convolutional Neural Networks for Visual Tracking', 2016 IEEE Conference on Computer Vision and Pattern Recognition (CVPR), Las Vegas, NV, USA, doi: 10.1109/CVPR.2016.465.

National Institute of Standards and Technology (2019), 'FRVT Quality Assessment', https://www.nist.gov/programs-projects/frvt-quality-assessment (accessed 17 June 2019).

Pollefeys, M., Van Gool, L., Vergauwen, M., Verbiest, F., Cornelis, K., Tops, J. and Koch, R. (2004), 'Visual Modeling with a Hand-Held Camera', *International Journal of Computer Vision*, Vol. 59, No 3, pp. 207-232.

Redmon, J., Divvala, S., Girshick, R. and Farhadi, A. (2016), 'You Only Look Once: Real-Time Object Detection', 2016 IEEE Conference on Computer Vision and Pattern Recognition (CVPR), Las Vegas, NV, USA, doi: 10.1109/CVPR.2016.91.

Ringaby, E. and Forssen, P. E. (2012), 'Efficient Video Rectification and Stabilisation for Cell-Phones', *International Journal of Computer Vision*, Vol. 96, No 3, pp. 335-352.

Sami Zitouni, M., Bhaskar, H., Dias, J. and Al-Mualla, M. E. (2016), 'Advances and Trends in Visual Crowd Analysis: A Systematic Survey and Evaluation of Crowd Modelling Techniques', *Neurocomputing*, Vol. 186, pp. 139-159.

Sanchez-Reillo, R., Quiros-Sandoval, H. C., Goicoechea-Telleria, I., and Ponce-Hernandez, W. (2017), 'Improving Presentation Attack Detection in Dynamic Handwritten Signature Biometrics', *IEEE Access*, Vol. 5, pp. 20463-20469.

Sanchez-Reillo, R., Tirado-Martin, P., Miranda-Escalada, A. and Bartolome-Molina, P. (2018), 'Fusing ECG and Fingerprints to Improve Recognition Performance and Robustness', 40th Annual International Conference of the IEEE Engineering in Medicine and Biology Society, 17-21 July, Honolulu, HI, USA.

Smith, L. (2017), 'Unfairness by Algorithm: Distilling the Harms of Automated Decision-Making', Future of Privacy Forum, Washington, DC, http://fpf.org/wp-content/uploads/2017/12/FPF-Automated-Decision-Making-Harms-and-Mitigation-Charts.pdf (accessed 19 June 2019).

Snavely, N., Seitz, S. M. and Szeliski, R. (2006), 'Photo tourism: exploring photo collections in 3D', *ACM Transactions on Graphics*, Vol. 25, No 3, pp. 835-846.

Sochor, J., Herout, A. and Havel, J. (2016), 'BoxCars: 3D Boxes as CNN Input for Improved Fine-Grained Vehicle Recognition', 2016 IEEE Conference on Computer Vision and Pattern Recognition (CVPR), Las Vegas, NV, USA, doi: 10.1109/CVPR.2016.328.

Tian, Y., Luo, P., Wang, X. and Tang, X. (2015), 'Pedestrian detection aided by deep learning semantic tasks', 2015 IEEE Conference on Computer Vision and Pattern Recognition (CVPR), Boston, MA, USA, doi: 10.1109/CVPR.2015.7299143.

Tian, Y. and Narasimhan, S. G. (2012), 'Globally Optimal Estimation of Nonrigid Image Distortion', *International Journal of Computer Vision*, Vol. 98, No 3, pp. 279-302.

van Rest, J. H. C. (2015), *Surveillance and video analytics: factors influencing the performance*, Publications Office of the European Union, Luxembourg.

van Rest, J. H. C., Grootjen, F. A., Grootjen, M., Wijn, R., Aarts, O., Roelofs, M. L., Burghouts, G. J., Bouma, H., Alic, L. and Kraaij, W. (2014), 'Requirements for multimedia metadata schemes in surveillance applications for security', *Multimedia tools and applications*, Vol. 70, No 1, pp. 573-598.

Verkruysse, W., Svaasand, L. O. and Nelson, J. S. (2008), 'Remote plethysmographic imaging using ambient light', *Optics Express*, Vol. 16, No 26, pp. 21434-21445.

Vezzani, R., Baltieri, D., and Cucchiara, R. (2013), 'People reidentification in surveillance and forensics: A survey', *ACM Computing Surveys*, Vol. 46, No 2, doi: 10.1145/2543581.2543596.

Watcher, S., Mittelstadt, B. and Floridi, L. (2017), 'Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation', *International Data Privacy Law*, Vol. 7, No 2, pp. 76–99.

Waggett, P. (2015), *Experiences from Large Scale Testing of Systems using Biometric Technologies*, Publications Office of the European Union, Luxembourg.

Wiewiórowski, W. R. (2017), 'Surveillance for public security purposes. Four pillars of acceptable interference with the fundamental right to privacy', in: Vermeulen, G. and Lievens, E. (eds.), *Data Protection and Privacy under Pressure. Transatlantic tensions, EU surveillance, and big data*, Maklu, Antwerp.

Wright, D. and de Hert, P. (eds.) (2012), *Privacy Impact Assessment*, Springer, Heidelberg.

Wurster, S. (2014), 'Ethics and Privacy Issues of Critical Infrastructure Protection — Risks and Possible Solutions Through Standardization', *Praxis der Informationsverarbeitung und Kommunikation*, Vol. 37, No 3, pp. 205-210.

Xiao, T., Li, H., Ouyang, W. and Wang, X. (2016), 'Learning Deep Feature Representations with Domain Guided Dropout for Person Re-identification', 2016 IEEE Conference on Computer Vision and Pattern Recognition (CVPR), Las Vegas, NV, USA, doi: 10.1109/CVPR.2016.140.

Yang, B., Yan, J., Lei, Z., and Li, S. Z. (2015), 'Convolutional channel features for pedestrian, face and edge detection', 2015 IEEE International Conference on Computer Vision (ICCV), Santiago, Chile, doi: 10.1109/ICCV.2015.18.

Yu, S-I., Meng, D., Zho, W. and Hauptmann, A. (2016), 'The Solution Path Algorithm for Identity-Aware Multi-Object Tracking', 2016 IEEE Conference on Computer Vision and Pattern Recognition (CVPR), Las Vegas, NV, USA, doi: 10.1109/CVPR.2016.420.

Zafeiriou, S., Zhang, C. and Zhang, Z. (2015), 'A survey on face detection in the wild: past, present and future', *Computer Vision and Image Understanding*, Vol. 138, pp. 1-24.

Zhang, S., Benenson, R., Omran, M., Hosang, J. and Schiele, B. (2016), 'How far are we from solving pedestrian detection', 2016 IEEE Conference on Computer Vision and Pattern Recognition (CVPR), Las Vegas, NV, USA, doi: 10.1109/CVPR.2016.141.

Zhang, Y., Li, B., Lu, H., Irie, A. and Ruan, X. (2016), 'Sample-Specific SVM Learning for Person Re-identification', 2016 IEEE Conference on Computer Vision and Pattern Recognition (CVPR), Las Vegas, NV, USA, doi: 10.1109/CVPR.2016.143.

List of abbreviations and definitions

Abbreviations

AFIS	Automatic Fingerprint Identification System
App-FAR	application false acceptance rate
App-FRR	application false rejection rate
BRKTP	biometric recognition of known threatening persons
CEN	Comité Européen de Normalisation
CIP	critical infrastructure protection
CNN	Convolutional Neural Network
ECI	European critical infrastructure
ECG	electrocardiography
EEG	electroencephalography
EU	European Union
FAR	false acceptance rate
FRR	false reject rate
FTE	failure to enrol
GDPR	general data protection regulation
JHA	Justice and Home Affairs
JRC	Joint Research Centre
EWZ	early warning zone
IBG	International Biometric Group
ONVIF	Open Network Video Interface Forum
PSIA	Physical Security Interoperability Alliance
PPE	personal protective equipment
SPIA	security and privacy impact assessment
VSS	video surveillance system

Definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 2382-37:2012, Information technology — Vocabulary — Part 37: Biometrics, and the following apply ([232]):

access control	function to determine whether to grant an individual access to systems, resources, facilities, services or information based on pre-established rules and specific rights or authority associated with the requesting party
accessibility	possibility for everyone, regardless of physical capability or technological readiness, to access resources and use technologies and services

([232]) For a freely available copy of ISO/IEC 2382-37:2012 (E) Information technology — Vocabulary — Part 37: Biometrics, see: http://standards.iso.org/ittf/PubliclyAvailableStandards/index.html (accessed 17 June 2019).

application	set of interrelated software components, policies, business processes and information designed to fulfil a particular purpose
attack potential	measure of the effort to be expended in attacking an IT system, expressed in terms of an attacker's expertise, resources and motivation ([233])
biometric modality	type of biometric characteristic utilised by a biometric system and the mode with which the biometric characteristic is compared against a biometric reference ([234])
data controller	person who either alone or jointly or in common with other persons determines the purposes for which and the manner in which any personal data are, or are to be, processed ([235])
data subject	individual who is the subject of personal data
false acceptance	acceptance of a biometric claim that ought to have been rejected
false acceptance rate	number of false acceptances as a proportion of the total number of biometric claims that ought to have been rejected
false rejection	rejection of a biometric claim that ought to have been accepted
false rejection rate	number of false rejections as a proportion of the total number of biometric claims that ought to have been accepted
identification	act of attributing a known identity to an individual
impostor	subversive biometric capture subject who attempts to be matched to someone else's biometric reference ([236])
performance parameter	quality metric which characterises a particular aspect, capability or attribute of a system ([237])
personal data	data which relate to a living individual who can be identified from those data, or from those data and other information, which is in the possession of or is likely to come into the possession of the data controller
recognition system	system for the recognition of an individual using distinguishing data provided by the individual
replay attack	attempt by a person to appear to be a legitimate user of a system by submitting data acquired during a previously legitimate transaction by someone else
spoofing attack	attack on a biometric system by an unauthorised person that uses artefacts to allow the perpetrator to masquerade as a specific authorised individual ([238])

([233]) A physical attack on system components can be as or more effective than cyber-attacks on the system.
([234]) For example, facial image recognition and fingerprint recognition.
([235]) NOTE 1: A data controller can be an individual, an organisation, or other corporate and unincorporated body of people. NOTE 2: A data controller will usually be an organisation but can be an individual, for example, a self-employed consultant. Even if an individual is given responsibility for data protection in an organisation, they will be acting on behalf of the organisation, which will be the data controller.
([236]) *Concise Oxford English Dictionary* defines impostor as: person who assumes a false identity in order to deceive or defraud.
([237]) The quality is usually quantified by a numerical value.
([238]) NOTE 1: Examples of artefacts include false fingers, photographs and voice recordings. NOTE 2: Use of an artefact to avoid being recognised as someone already enrolled in the database would not generally be termed spoofing but disguise.

subject	individual who provides biometric data or biographical data for storage, processing or comparison, or about whom such data is collected by others
transaction	discrete event between an entity and service provider that supports a business or programmatic purpose
usability	extent to which a product can be used by specified individuals to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use

List of boxes

List of figures

List of tables

Annexes

Annex A Checklist of activities for implementers of EWZ biometric systems (informative)

The checklist given in this annex is one mechanism for documenting that the processes documented in this report have been considered and actions have been taken where appropriate. Evidence supporting the actions in this checklist should be documented and available for inspection by auditors.

NOTE Where documentation is specified, items from more than one of the listed activities can be aggregated to create fewer documents.

Options for the completion of Column 5 could be:

— NOT UNDERTAKEN — with a reason or explanation for why this activity was not undertaken, together with a date and name of person making the decision.

— COMPLETED — with date and name of person confirming the completion of the activity.

— COMPLETED WITH EVIDENCE — with data and name of person confirming the completion of the activity, alongside a pointer to source of the evidence. In one instance this evidence may be a paragraph in a design document for the system.

Table 8. Checklist of activities for implementers of EWZ biometric systems

	Clause	Activity	Typical output	Decision, with/ without evidence
Preliminary considerations				
		Assessment completed including:	Document that contains:	
1		(a) a definition of the business problem;	(a) an overall description of the business problem;	
2		(b) a description of the role that recognition plays in the solution to the business problem;	(b) a description of the role that recognition plays in the solution to the business problem;	
3		(c) list of business risks together with an assessment of the likelihood and impact analysis;	(c) an analysis of the business risks of incorrect recognition, both falsely accepting imposters and failing to recognise legitimate subjects, with the likelihood and impact of incorrectly recognising individuals, taking account of other management and security measures forming part of the solution;	
4		(d) list of constraint factors;	(d) a list of any constraints to the implementation and operation of the solution including at least costs, timescale, and environment; and	
5		(e) list of relevant obligations and recommendations under statutory requirements.	(e) a list of statutory requirements that might apply.	
Assessment of the acceptance of a biometric solution				
6	7.8 7.11	(a) Survey or focus group of potential subjects, operators, and other stakeholders completed;	A documented assessment from a survey or focus group involving the potential subjects, operators, and other stakeholders (e.g. parents or guardians), which documents their attitudes, concerns,	

		and	and suggestions about the introduction of a recognition system.	
7	7.8	(b) Assessment of stakeholder attitudes, concerns and suggestions completed.		
8	7.8	Completed review of assessment of the views of stakeholders, including further dialogue as to the biometric modality chosen, and any concerns raised regarding the implementation.	A review of the original assessment of the views of stakeholders (see 3.2), together with a document produced for the stakeholders outlining why the type of recognition system was selected [including the selection of biometric modality (see 5.2), and how any stakeholder suggestions and concerns will be addressed during the planning and implementation stages of the system.	
Considerations in the selection of a particular biometric modality				
9	7.2 7.7 7.9.3 7.3	Assessment of biometric modality completed, identifying: (a) suitability to the target subject population; (b) the level of subject interaction with the biometric system; (c) the suitability of the environment in which data capture device will be located; (d) required performance parameters; (e) the implementation risks; and (f) the costs, both initial and ongoing.	Document that lists all the biometric modality solutions being considered, shortlisted on the basis of evaluation of: (a) the suitability of the biometric modality for the application (e.g. in respect of accessibility for the people being recognised); (b) how well the required interaction of the subjects with the biometric capture devices meets system and subject expectations and constraints; (c) the suitability of the biometric modality and implementation to meet system environmental conditions, particularly in cases of challenging environments such as external locations or extreme temperature, humidity, dirt, lighting or noise. Note that providing a specially suitable environment will likely add to the cost of implementation and possibly operation; (d) the ability to achieve the required performance parameters of throughput, error rates and exception handling volume; (e) the risks to timely project delivery within budgeted cost resulting from the choice of modality. This assessment can be based on a study of existing similar systems using the modality in the context of the specific application; and	

			(f) costs of implementation and future ongoing costs, including training, operating, maintenance and upgrade costs.	
Planning for the implementation of a biometric system				
10	7.3	Performance parameters determined, including: (a) error rates: i. false acceptance rate (FAR); ii. false reject rate (FRR); iii. failure to enrol (FTE); iv. application FAR (App-FAR); v. application FRR (App-FRR); (b) throughput volumes and rates; and (c) exception handling volumes.	Documentation of the performance parameter requirements, based upon the evaluation of the requirements for the application. NOTE The application error rates; throughput volumes and rates; and exception handling volumes are the key system performance parameters that are determined by the system requirement. Suppliers of shortlisted systems may offer reference installations that have data as to volumes of exceptions and appropriate procedures. (a) The biometric system error rates will influence the application performance but will not be the only determining factors; (b) Throughput rates should be sized to take account of peak loadings in order to ensure that queuing and overall time to execute the transaction remain within acceptable limits; and (c) When determining exception handling volumes, due account should be taken of the number of subjects who cannot be biometrically enrolled (i.e. given by the FTE rate) as these subjects will always be referred to exception handling.	
11	7.3 Annex B	Justification for performance requirement is documented.	Documented justification of the performance level chosen. NOTE If security considerations indicate a FAR rate that is not met by a basic level FAR requirement (see Annex B), the manager is recommended to seek expert advice on overall system security.	
12	7.3 8	Performance parameters agreed with supplier(s).	Recorded dialogue with supplier(s) of supplier-quoted performance parameters and how these align to application performance requirements. Given the need to understand the likely performance based upon a 'live system' as opposed to laboratory testing, it is important that a full understanding of supplier-quoted performance parameters is	

			obtained.	
13	7.1	Risk management plan completed.	Document detailing the risk assessment of the selected biometric system. This will pick up on the original evaluation of the risks, but include a risk assessment of the biometric system integrated into the application, including data protection of personal data. Further information on risk management can be found in ISO/IEC 27005 for more detailed information and guidance on Information Security Risk Management.	
14	7.4	Organisation's security policy updated.	Updated organisation security policy and information security management system after the introduction of a new type of IT system.	
15	7.6 8	Usability proposals evaluated against requirements. Usability testing agreed with selected supplier(s).	Evaluation of the usability aspects of the proposed application using the biometric system. As part of acceptance testing such assessment will be through observation, trial, and possible subject survey of a representative selection of subjects.	
16	7.11	Subject interaction evaluated against requirements. Subject interaction acceptance tests agreed with selected supplier(s).	Documentation detailing the test protocols.	
17	7.9.1 7.9.2	Proposals for prompts and instruction to the user of the biometric system evaluated against requirements. Prompts and instruction acceptance tests agreed with	Documentation detailing the interface to the user and test protocols.	

		selected supplier(s).		
18	7.7 8	Accessibility proposals evaluated against requirements. Accessibility testing agreed with selected supplier(s).	Evaluation of the accessibility of the proposed biometric system while selecting the biometric system, as determined from suppliers' proposal documentation and any demonstrations. As part of acceptance testing, such assessment will be through observation, trial, and possible subject survey of a representative selection of subjects.	
19	7.10 7.7	Exception handling system designed and documented.	Document describing the exception handling system and what circumstances the exception handling system is designed to deal with. Explanation of how the planned exception handling procedures will operate in a non-discriminatory way in compliance with relevant equality legislation and disability laws.	
20	7.9.1	Enrolment process designed and documented, including: (a) what credentials to check to establish eligibility to enrol; (b) who is allowed to conduct enrolments in terms of authorisation and training; (c) any quality thresholds that have to be met for an enrolment to be deemed successful; (d) how to decide that an eligible subject is unsuitable for enrolment and therefore should use an exception handling process; (e) whether informed consent is required and how to obtain it; (f) training for subjects in using	Document describing the enrolment process including details of: (a) what credentials to check to establish eligibility to enrol; (b) who is allowed to conduct enrolments in terms of authorisation and training; (c) any quality thresholds that have to be met for an enrolment to be deemed successful; (d) how to decide that an eligible subject is unsuitable for enrolment and therefore should use an exception handling process; EXAMPLE Description of pre-enrolment assessment of lack of suitability of subject for enrolment; number of failed enrolment attempts before FTE is declared; absence of subject consent; or other criteria specified by the system enrolment policy. (e) whether informed consent is required and how to obtain it; NOTE Informed consent will usually be necessary. Only under special circumstances would enrolment without subject/guardian consent be allowed. (f) training for subjects in using the biometric system; and	

		the biometric system; and (g) when re-enrolment takes place and when a subject's enrolled details expire.	(g) when re-enrolment takes place and when a subject's enrolled details expire. EXAMPLE Change in subjects' biometric characteristics (as a result of e.g. normal ageing, illness or injury); observed falling off of recognition performance; change of subjects status or biographical data such as name or gender; or other factors specified by the system enrolment policy.	
21	7.9.1 8	Decision on use of biometric attendants made. Training designed for biometric attendants. Data capture feedback proposals evaluated against requirements. Data capture feedback acceptance tests agreed with selected supplier(s).	Decision of whether biometric attendants are to be present at enrolment. NOTE Systems are likely to employ attended enrolment to ensure optimum recognition performance and, where system enrolment security is relevant, to meet the requirements of the system security policy. Training documentation if using biometric attendants. Any periodic checks on the effectiveness of the training should be documented, together with a programme of refresher training. Evaluation of the data capture feedback of the proposed biometric system while selecting the biometric system, as determined from suppliers' proposal documentation. Description of the testing of data capture feedback as part of acceptance testing.	
22	7.9.1 7.5	Documentation for users prepared, including: (a) reasons why a biometric system is being used; (b) details of the enrolment process; (c) details of the exception handling system and when used; and	Document for users covering: (a) reasons why a biometric system is being used; (b) details of the enrolment process; (c) details of the exception handling system and when used; and (d) the privacy notice.	

		(d) the privacy notice.		
23	7.9.1	Enrolment training designed for biometric attendants and data subjects.	Document detailing subject training procedure and how enrolment will be monitored to detect problems that can be resolved through improved training. Document for each enrolee to confirm: (a) acceptance of the enrolment process and privacy notice; (b) receipt of enrolee documentation; (c) receipt of guidance in using the biometric system; and (d) receipt of practice in using the biometric system.	
24	7.9.2	Positioning of data capture stations agreed with suppliers(s), together with assessment of performance with use of Personal protection Equipment (PPE).	Document describing the environment(s) in which the data capture station(s) will be sited, and also if PPE will be required to be worn by subjects.	
25	9	Updates to organisation's maintenance procedures.	Updates to the organisation's equipment maintenance documentation to include: (a) the data capture device manufacturer's procedures (including maintenance periods); (b) the procedures for maintenance following system alerts; (c) the training required to be given to equipment maintenance personnel; and (d) periodic monitoring of the environment to ensure compliance with the specified environmental conditions.	
26	7.9.3	Operational environment of the data capture stations.	An assessment report of the operational environment(s) in which the data capture station(s) will be sited, together with factors affecting the performance of the specific modality being utilised.	
27	7.10	Determination of the exception	Document describing the exceptions that the exception handling	

		handling requirements.	process is designed to deal with and how these will satisfy the business requirements for the system and its target population in a comprehensive and non-discriminatory way.	
28	7.5	Conformance with laws on privacy and personal data protection.	Document explaining how the organisation's obligations under the privacy and personal data protection legislation are met following the introduction of the biometric system.	
29	7.5	Documentation of policy on privacy and personal data protection.	Document describing how the protection of personal data is met, (including the recommendations of ISO/IEC TR 24714-1).	
Testing and reporting on the results of tests				
30	8 7.3	Reporting the statistics of performance in tests.	Review report detailing statistics of: (a) error rates achieved; (b) throughput; and (c) exception handing.	
31	8	Usability and accessibility report.	Document describing each test, the expected result and actual result, including details of: (a) number and description of data subject representation; (b) biometric system settings, including threshold settings; and (c) audit trail of when tests performed, by whom, and overall sign off of audit results.	
32	8	Specific recommendations on reporting the details of the usability and accessibility tests.	Details of any test requiring data subjects should include the number and description of representatives required for the test (e.g. x number left handed, x number taller than 1.8m) and details of the actual representation at the test. Any untoward circumstances, and actions which were not included in the calculations leading to the declaration of performance measures; the environmental conditions; dates and other relevant	

			context for the tests should be documented. See ISO/IEC 19795-6 when published for further details (and 19795-2:2006 in the interim).	
33	9.1 8	System alert function tests.	Evaluation report of the biometric system alerts provided by the supplier. As part of acceptance testing, tests to exercise the alerts.	
Operational measures				
34	9.1	Maintenance procedures.	Description of test procedures to be conducted after maintenance keyed to specific maintenance functions. NOTE Tests may be based upon some of the acceptance tests listed in section 8.	
35	9.1	Cleaning checks.	Description of cleaning schedule and procedures provided.	
36	9.2	Procedures for change management.	Document describing change management procedures for the biometric system, or modification to equipment change management procedures.	
37	9.3	Management information system data.	Document detailing statistics to be recorded (automatically or manually). Document detailing periodic review processes.	
38	7.10, 9.4	Documentation for exception handling/fallback measures.	Reviewed and validated document detailing fallback arrangements and when such arrangements are to be invoked. NOTE Where fallback arrangements are to be provided by existing exception handling procedures, these must be sized to cope with the full system loading.	

Annex B Request for information

Background

The EWZ4CIP Thematic Group is investigating the state of the art of surveillance and observation systems in early warning zones. The Group defines an early warning zone (EWZ) as a designated physical observation area surrounding a protected area:

— wherein people can move freely,

— where early signs of threats may manifest,

— where an observation capability is realised that could generate early warnings of those threats.

A specific technology capability that may support an EWZ is the biometric recognition of known threatening persons (BRKTP). The purpose of BRKTP could be to detect early phases in the modus operandi of terrorists, such as hostile reconnaissance of a potential target. This typically happens well before the actual attack. Detecting this behaviour could give security organisations (law enforcement agencies and security departments of critical infrastructures) more time to deploy countermeasures.

Assessing the state of the art of BRKTP in the EU requires input from security organisations and policymakers in Member States. With this information, the EWZ4CIP Thematic Group will be able to give more useful advice to critical infrastructure owners, law enforcement agencies and relevant policymakers.

REQUEST FOR INFORMATION — Biometric recognition of known threatening persons (BRKTP):

1. Details of responder:

— Member State:

— Organisation:

— Name and function of person responding:

— Contact details, telephone, email and address:

2. What is the role of your organisation with regard to BRKTP (e.g. policymaker, critical infrastructure operator, law enforcement agency, etc.)?

3. Are you aware of any operational early warning zones using BRKTP in your country?

YES/NO

— If 'YES', please provide further information for each solution, i.e.:

  - What are the main technology components?
  - What is the primary purpose of the BRKTP?
  - What is the legal base?
  - Is it considered effective in practice?
  - If not considered fully effective, what are the issues? How could it be improved?
  - Are you able to provide specific information for further contact by the ERNCIP Thematic Group?

— If 'NO':

  - Do you think BRKTP would be desirable in certain circumstances?
  - Do you think BRKTP would currently be feasible in your country (technically, operationally, ethically, socially and politically)?
  - What do you consider to be the main inhibitors?

4. Are you aware of any initiatives or plans to further investigate the possibilities of introducing BRKTP in your country? And if so:

— What types of organisation are involved in these initiatives, and in which roles?

— Would you/they be interested in the outcome of this thematic group on EWZ due in 2019?

5. Any further comments you wish to make?

Annex C Additional operational environments

Operational environment 2: secured site in remote environment

Context

The site concerned is located in the countryside where it is served by limited public transport means (i.e. limited number of local buses, no passenger trains) most people arriving in the area by car.

There are several public roads leading to the site and almost all of them are locally equipped with video surveillance cameras, supported by a licence plate recognition system, managed by the local police of individual communes/municipalities in support of law enforcement.

The site has an extensive campus area of about 160 ha with a 6 km perimeter fence. There are several entrances to the site for staff but only one can be used by visitors and another for goods delivery.

The site has more or less 100 buildings with a dispersed population even if there is an ongoing strategy to concentrate staff in what has been called a 'high density zone'. It has vast green forest areas, some of them being rather dense, and some even untouched, i.e. left to nature.

Weather is usually slow changing but variable alternating periods of heavy rainfall with rather strong thunderstorms to clear blue skies. Foggy days are rather limited but more frequent than snowfalls that occur usually two or three times a year.

Security awareness on site is medium to high due to nature of the site and the presence of armed guards as well as a well-instated access control. Privacy awareness on the other hand has increased over time and can be considered as medium.

Intent around the site is usually homogeneous with differences between each type of entrance (staff, visitors, goods delivery, etc.) almost never reaching high intensity unless there are programmed events, e.g. Open Day where we have had a peak of 10 000 visitors or in the future when a new on-premises Conference Centre will be fully used.

Within our perimeter and the surrounding territory under our jurisdiction, the relation between the managers of the video surveillance system and the data subjects involved can be considered as having a high level of trust within an easy-to-change environment. This clearly differs if the need to extend the perimeter towards the outside and beyond the current territorial boundaries so as to be able to have more time for a reaction to a potential threat.

Environment

The site has a rural surrounding with a significant amount of vegetation and dense forest area. The only noteworthy natural hazards are the possibility of flooding due to heavy rain with a significant difference in altitude from the higher side to the opposite lower one of the site.

It is in fact a rather big campus similar to that of a small village which is not densely populated. It has tens of km of internal roads and series of underground technical galleries in support of the various utilities.

There is a high level of infrastructure including a well-developed technical network and virtual server infrastructure in support of all physical protection systems, along with specialised personnel.

Within the site a 'Defence in Depth' system is applied with an outer and various inner perimeters in protection of the more vital areas. In this sense the presence of several closed compartments following the logic of vital area, secured area and observation (outer not closed) area may be considered in place.

People density is medium/low with a main population of several thousand people with slight tendency to increase. The same can be said for visitors with a current average of several hundreds per working day.

Risk Cause

The assets to protect are manifold: dangerous scientific equipment, security accredited areas, laboratories, etc. Clearly we also want to preserve the life and well-being of anyone on site, i.e. staff as well as visitors, that could include VIPs. Business continuity is important and we have a 24/7/365 armed guard service.

All targets are to be considered: VIPs, individuals, crowds, buildings, small objects, ICT infrastructure, industrial infrastructure, vehicles, overall security system and associated data.

The site is potentially prone to the most varied threats like activism, extremism, crime, espionage as well as terrorism. The motivation behind an eventual threat may be of political, religious, economic and personal nature thus eventually being perpetrated by an individual or group. All threats mentioned above leading to security incidents can be considered as being of a persistent nature with a different level of sophistication, i.e. financial, skill, etc. capability.

Threats to be mainly considered are those via the ground and air, in respect of the physical domain, but the cyber world should not be neglected. Plausible modus operandi should include burglary/theft, vandalism, bombing, suicide attack, kidnapping and hostage taking, espionage, infiltration and hacking.

An appropriate incident life-cycle management with collection of durable evidence for further analysis is considered key. Preventive measures should be seen as the most effective but a quick and efficient response is also key.

Possible issues linked to vulnerability are the established routine, false alarms, eventual lack of information or intelligence. Focus on human nature or error is key in also taking advantage of supporting technology. It is fundamental that technology is well understood, i.e. training and awareness, even of limitations, is crucial. Good working order (i.e. both preventive and corrective maintenance) and effectiveness of technological support, rendering trustworthy and reliable, is of extreme importance.

Risks should be minimised (i.e. probability as well as impact) in a systematic way and should be considered throughout all levels of responsibility: from individual to supranational.

Extended warning zone systems

Sensor

No specific modality or sensor type should be excluded but most importantly these should be implementable (in an effective and cheap way …) in the most varied conditions, e.g. day and night, cold and hot temperatures, etc. Possibly passive and the least invasive, i.e. embedded or mimicked with the surroundings.

The number of sensors can vary as long as cost-effectiveness remains a priority and the greater the distance the better with the idea to gain time for a better more accurate analysis and to enact in an eventual response.

Situational awareness

Focus on people and individuals but not only … individuals usually use or drive a means of transport, carry something with them or remote control some kind of equipment, e.g. UAVs. Possibly detecting what they carry would be of interest but identifying behavioural patterns linked to loitering, tailgating, trespassing and pickpocketing is certainly vital.

The number of subjects or objects to be observed in any given scene would be limited and in the order of 10s.

Optimising the initial detection to then classify and analyse would certainly improve the identification of a specific problem needing attention or that of the concerned individual seen as a threat. Accuracy of situational assessment should be configurable and kept rather low even if prioritised, i.e. with many situations the more significant one should be analysed first by operators.

Threat assessment

A threat assessment is regularly carried out and updated, thus being realistic and reliable. It includes possible scenarios where elements like threat direction, threat motivation, frequency, number of attackers, capabilities, threatening objects or persons, modus operandi, equipment, target, physical angle of attack and incident phase, etc. are all considered.

System

Focus on a usable complementary system that may be easily installed with possibilities of being eventually integrated and supported by what already is installed within the existing Control Room is deemed crucial: that is to say an extensive reuse of existing system's subcomponents (including sensors, storage, network, processing units, viewing station, mobile interface, command and control units).

Such a system should also be easily installed, configured as well as maintained.

Due to this complementarity the complexity can thus not be so high.

Specific scenarios for the application of EWZ

Monitoring potential attacks from above

Monitoring of 'no fly zone' and associated air space, i.e. any airborne vehicle coming close or violating the established perimeter should be identified.

Focus initially should be on detection. The ability to distinguish between various type of flying objects from small drones to larger UAVs to fully-fledged air vehicles, i.e. from helicopters, to small and larger airplanes is essential. Note that occasionally such an air space, that has a defined limited altitude of 2 000 ft, is most probably violated and tools, in possession of generic commercially available information are used for monitoring this.

Early warning zones and checkpoints of internal areas

In a large site campus like the one in this use case, where visitors, staff, etc. enter the site through a limited number of entrances it could prove extremely interesting to associate anyone entering the site with the area they are most probably heading to.

Visitors for instance have to pre-register and their host and meeting on-site location is known beforehand. Visitors also receive clear instructions to take the most direct route to their meeting location with their host. With special focus on large events or the more sensitive areas it could prove extremely interesting to detect and identify situations when someone is far from the expected location for a further verification, e.g. why is someone nearby a sensitive area when he should be attending a conference at one of our major meeting rooms?

This would certainly need the clear identification of the various types and sensitivity level of macro areas, e.g. semi-public, access controlled, sensitive, vital, etc.

Another area of interest, not so 'internal' but under our jurisdiction, as to where to create an early warning zone with its own characteristics would be our social facility and lodgings area.

Extended outer virtual perimeters

As mentioned the site currently has an extensive outer perimeter fence. One of the issues with this is that even if it is alarmed and dog handling units are used for tracking eventual intruders it could prove interesting to understand if a particular threat, e.g. unusual traffic related to many trucks or buses full of people, is about to hit the site over the ground or by road. We also have the whole area regarding our social facilities as well as lodgings that is not comprised within such a fenced area. This would mean extending the existing perimeter border towards the surrounding territory.

Note that the actual virtual extended perimeters could be of a bigger dimension and virtually placed at a greater distance so as to give additional time for analysis as well as the eventual preparation of a reaction or response. Clearly the implementation of such a scenario would need the buy-in of all local authorities, etc. and could prove difficult to implement.

Operational environment 3: public transport hub in urban environment

Case A

Rationale

The checklist was compiled identifying both the AS-IS and some characteristics of the site identified in a manner that makes it possible to analyse and develop security solutions precisely.

General description of the context

The place under consideration is a central square of an average-sized city, inside which there is an important interchange of multimodal transport. Almost all types of transport that operate in the city are present, and there is a high level of crowd that makes it particularly interesting for defining/experimenting new and innovative protection and monitoring measures.

Transport assets and systems

— Railway terminus station

— Underground node for multiple metro lines

— An overland tram line

— Multiple bus lines

Description of the premises:

— Square:

  - Size: approx. 20 000 m^2
  - Six access routes to the square
  - Small green area with grass and trees
  - Small fountain and monument in the centre of the square

— Railway station:

  - The station is placed at street level, both the pre-gate area and the train access platforms. It can be accessed by two stairways; a main one in the square and a secondary one in the side street.
  - The mezzanine can be accessed from the square and the side street.

- The platforms for train access are parallel and alongside each other, and they can only be accessed through gates.

— Metro:

- Characteristics: Mezzanines alongside each other and connected by two parallel corridors (two pre-gate and one post-gate) that allow interchange between the two lines; two separate platforms which are alongside each other and connected by two corridors. In some cases the interchange can be made through the corridors positioned at platform level.
- Access to the station: seven stairways, two escalators and one lift.
- The following areas are inside the station: nine business activities; 26 offices (technical support and maintenance).
- Surfaces: Mezzanine approx. 4 000 m^2; Platforms approx. 2 000 m^2.

Context

— Weather: rain, clear, snow, fog and cloud;

— Weather dynamics: stable, very slow change;

— Roofing: underground (metro station), open-air (square), partially covered (metro access stairway on the railway side), roof (railway station);

— Privacy awareness: low (client and business staff), medium (security staff);

— Security awareness: low (client, business staff), medium (security staff);

— Intention (risk vectors, causes): heterogeneous and medium-high intensity;

— Relationship (among the causes): the same and separate;

Environment:

— Type of environment: tall buildings (in the square) underground (metro station), road, inside closed (railway station main building);

— Type of object: multimodal point for public transport (railway, metro, bus and tram), road and vehicle;

— Existing infrastructure (presence): highly developed;

— Compartments present: railway station, square, metro station (area before and after the gate);

— Closed compartments

- Metro:
- Between the square and the metro station entrance including the pre-gate businesses: stairs (always) and gates (night);
- Between the metro station and the platforms for the metro trains: gates closed at night;
- Between the gate and the technical areas of the metro: doors closed but not always with alarm.
- Railway station:
- Between the square and the train platforms: gates.

— Person density:

— The average data per hour identified by the gates (in/out accesses):

- Low (on average 1 000 access every hour) from 10 p.m. to 2 a.m. on working days and from 9 p.m. to 8 a.m. during holidays;

- Very high (above 10 000 access every day) from 7-10 a.m. and from 5-7 p.m. on working days;
- High (above 3 000 access every day) during all the other hours.

Risk

Risk cause

— Asset to be protected: public order, the wellbeing of a crowd, the life and wellbeing of a person, transport service continuity and integrity of the assets needed to perform it;

— Threat:

- Target: individual, building, business activity, crowd, small object (e.g. wallets as a result of pickpocketing), vehicles (metro or railway trains);
- Threat vector: accident, illness, activist, criminal, extremist, terrorist;
- Motivation: politics, religion, economy and personal;
- Frequency: single (for serious episodes), multiple (for theft or harassment);
- Number of attackers: individual, group;
- Offender capacity: none (for theft, harassment), medium low with proper or improvised weapons (in the other cases);
- Physical angle of attack: above the ground, underground and cyber;
- Modus operandi: AS-IS human error (low risk), theft/pickpocketing (high risk), break in (medium risk), political demonstration (medium risk), harassment (medium risk), vandalism (medium risk); POTENTIAL suicide attack (medium risk), explosive attack (medium risk), sniper in the square (low risk).
- Equipment: AS-IS: personal and improvised weapons; POTENTIAL explosive, poison, banner, camouflage, electronic device, vehicle, firearms, dirty bomb, chemical weapon.
- Incident phase: Before: risk analysis; During: incident response with qualified staff; After: service recovery with qualified staff.

Vulnerability

False alarms, lack of precise access checks, security-level awareness, sensor coverage (CCTV only in some passage points, no coverage of critical areas by the intrusion systems, etc.), staff sensitivity, risk assessment process quality.

Resulting risk

— Possibility: medium;

— Impact: medium and high;

— Responsibility: service manager for the metro area and railway area and police.

Extended warning zone systems

Sensor

— Mode: visible light (camera);

— Sensor type: camera, IR or human;

— Active: staff, sound diffusion (actuator);

— Invasion level: not significant, light;

— Array form: single (camera);

— Platform: fixed (no horizontally rotating cameras);

— Number of sensors: 84 CCTV cameras and 12 intrusion sensors;

— Sensor-object distance: camera up to 70 m, intrusion sensors up to 10 m;

— Direction: from up to down;

— Image improvement: absent.

Situation awareness

— Type of object: individual, group, bicycle, motorbike, car, van, bus, lorry, train, tram, tanker, public transport vehicle;

— Type of material to be observed: with the instruments that are currently available, only objects and containers that are visible to the naked eye and of various materials (metal, plastic, pottery, wood, fabric) can be identified;

— Behaviour: soliciting, harassment, pickpocketing and abusive access;

— Number of objects to observe: more than 100 on average during the day;

— Function: observation, face recognition and identification if the person is known;

— Surveillance model: camera-view of the different access levels (square, entry stairway, gate level, and platform level);

— Aspect: presence, position in the context (square, metro or railway station), behaviour, communication, luggage and objects, weapons, electronic devices;

— Situation evaluation precision: protection tied only to the camera view by a specialist operator in the absence of other automatic instruments.

Threat assessment

— Security process: active risk assessment process, unit for crisis management and business recovery, territorial protection through platoons composed of internal and external armed personnel.

Case B

General description

The square has approx. 5 000m^2 with seven access routes, and it faces a river. Almost all types of transport in the city are present here.

On one side we have a train station connecting the city to a neighbouring city along the river (30 km) with the metro station on underground. Between the train station and the river we have a ferryboat terminal.

On the other sides off the square we have two high-risk objects, and a symbolic statue. Nearby is one of the main city night amusement places.

Railway station

Placed at street level. Accessed from the street by three entries (one comes from the ferry terminal). Platform accessed through gates in the main mezzanine and in an intermediate mezzanine connected directly to the metro station.

It has a commercial area in non-paid area.

Metro station

The metro station is the end of a line. It is near the river. It is below the train station and near the ferry boat terminal.

We have two connections to the train station (one for the non-paid area — two escalators and two stairways — and the other through a medium level mezzanine to the train platforms — one large stairway).

The metro station also has an entry directly from the square — two escalators and two stairways.

Three to four commercial places.

Each station is built in three/four levels:

— First level is the track with a space under the platforms for cables, ventilating installation and sewage pumps.

— Second level is platform level with closed technical areas (examples: sometimes electric substation, electric power transform area, emergency batteries, main low voltage frame with circuit breakers, sometimes signalling room, …).

— Third level is the mezzanine with the personnel installations, public installations and other technical area. We have the gate line. Sometimes we have a fourth level in deep stations and in the train stations we have small mezzanines with the train gates and direct access to train platforms.

In old times we built stations with opposite mezzanines. Nowadays we build stations with one central mezzanine.

Nearby these metro and train stations we have two tram lines, 17 bus lines and taxis.

Ferry terminal

Placed at street level. Connections to several nearby municipalities. It has four docking stations. One is for people and cars. No stairs. Each docking station has a different boarding lounge on land.

Security risks that we consider:

— Attacks, terrorism

— Active shooter

— Internal threat

— Improvised explosive device (several types)

— Abandoned object or equipment

— Sabotage

— Cyberthreat

— Drone threat

— Provoked fires,

— Theft, robbery, assault

— Burglary, vandalism, graffiti

The national threat level continues to be low.

In our OCC we have one police agent of the Public transport police department that works closely with us.

We host the police in a central station for a police squad.

We developed a training programme for our personnel (internal and external) with the collaboration of the police and national intelligence service.

We make a risk assessment concerning the transport network and every main event.

CCTV

In all stations. The metro station (and terminal line) has multiple cameras. The cameras in technical areas are always in movement detection.

All the cameras without night vision capability are in movement detection during off time.

Internal security personnel

In this country private security staff are not allowed to use any type of weapon or similar.

During the night we have security patrols inside the network (protecting trains and main points) and four patrols outside with car and dogs to control ventilating shafts, emergency doors or technical doors).

Europe Direct is a service to help you find answers to your questions about the European Union.

Freephone number (*)**:**

00 800 6 7 8 9 10 11

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

More information on the European Union is available on the internet (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).

KJ-NA-29814-EN-N

JRC Mission

As the science and knowledge service of the European Commission, the Joint Research Centre's mission is to support EU policies with independent evidence throughout the whole policy cycle.

EU Science Hub
ec.europa.eu/jrc

@EU_ScienceHub

EU Science Hub - Joint Research Centre

Joint Research Centre

EU Science Hub

Publications Office

doi:10.2760/806546

ISBN 978-92-76-08963-6