PrivAcy pReserving Infrastructure for Surveillance

Deliverable D4.1
Generic process for surveillance

Project: PARIS
Project Number: SEC-312504
Deliverable: D4.1
Title: Generic process for surveillance
Version: v1.2.
Date: 15/10/2014
Confidentiality: restricted to PARIS consortium

Authors: Mathias BOSSUET (Thales)
Víctor Manuel Hidalgo (Visual Tools)
Francisco Jaime (UMA)

Funded by the European Union's Seventh Framework Programme

Table of Contents

Document History

Version	Status	Date
V1	First version, submitted 06/2013 to the commission	28/06/2013
V1.1	Amended version accordingly to the EC reviewer's comments and submitted to the consortium	08/10/2014
V1.2	Final amended version accordingly to the EC's reviewer comments [major changes are listed in the executive summary]	15/10/2014

Approval		
	Name	**Date**
Prepared	Mathias BOSSUET	30/06/2013
Prepared	Victor Manuel HIDALGO	30/06/2013
Prepared	Francisco JAIME	30/06/2013
Authorised		
Circulation		
Recipient	**Date of submission**	
Project partners	day/month/year	
European Commission	day/month/year	

Executive Summary

This document provides:

• A description of the salient features of surveillance systems from the privacy perspective

• A specification of a generic process involving all the phases (procurement, development, operation)

• A tentative meta-model of design processes.

The surveillance systems that are considered in this document are video-surveillance systems and biometrics systems. The main features of these types of surveillance systems are described, including their technical and operational features and the potential privacy harms they may generate.

The key stakeholders associated with these systems, the specification and purchasing typical processes associated are depicted.

From this information, a generalization about the structure, properties and functionality of the surveillance systems considered is proposed through a meta-model. This meta-model could bring value to the engineering process of a surveillance system and would be used within the scope of the SALT framework.

Note that this deliverable is confidential. It will not be uploaded in the project website. The information contained therein will not be disseminated in whatever other form.

EC Reviewer's Comment:

This deliverable has been reworked to meet the expectations expressed in the Consolidated Review Report issued by the Commission following the mid-term review of the project held in July 2014. The following expectations from the consolidated review report have been taken into account while processing these modifications:

- "clearly build on in the project and refer in the deliverables to all relevant European principles (e.g. data minimization and proportionality) and ISO documents (e.g. ISO/IEC IS 29100:2011 and ISO/IEC 24760-1:2011" [from Overall Assessment of Consolidated Review Report],
- "In the revised deliverable, please elaborate on the relationship between PARIS (and the SALT framework) and recent frameworks such as that on data minimization. It would be interesting to state how these recent frameworks can and will influence SALT. [from the Annex 2 of the Consolidated Review Report].

This document completed version refers the 2 ISO standards aforementioned. These standards have been carefully reviewed. Their contents, and the relations with the PARIS and SALT approach are briefly investigated in the introduction of this document. Then, the document subpart 2.2.7 entitled" Main privacy issues linked to video-surveillance systems and possible design mitigations" has been completely reviewed to reflect the privacy principles issued from ISO/IEC IS 29100:2011, rather than those from OECD guidelines that were considered in the previous version of the deliverable.

List of Figures

Abbreviations and Definitions

Abbreviation	Definition
CAGR	Constant Annual Growth Rate
CCTV	Closed Circuit TeleVision
CONOPS	CONcept of OPerationS
FPS	Frames Per Second
HTTP	HyperText Transfer Protocol
ICT	Information and Communication Technologies
IP	Internet Protocol
LAN	Local Area Network
NAF	NATO Architecture Framework
NVR	Network Video Recorder
OS	Operating System
OSI	Open Systems Interconnexion
PARIS	PrivAcy pReserving Infrastructure for Surveillance
PET	Privacy Enhancement Technology
PbD	Privacy by Design
PIA	Privacy Impact Assessment
PII	Privacy Identifiable Information
PPOF	Privacy Point Of Failure
PTZ	Pan Tilt Zoom
SALT	Social, Anthropological, Legal, Technical
SGDSN	Secretariat General de la Défense et Sécurité Nationale
SPOF	Single Point Of Failure
VCA	Video Content Analysis
VLAN	Virtual LAN
VMS	Video-Management System
WAN	Wide Area Network
WP29	Article 29 data Protection Working Party

1 Introduction

1.1 Deliverable Objectives and Scope

The goal of the PARIS 4th WorkPackage "SALT compliant process" is to define and describe how a "by-design" process will enable to ensure as far as possible that a surveillance system complies with principles derived from a balance between surveillance and privacy protection. The balance principles are themselves hosted and expressed within a SALT framework instance, embedding technical, Legal and Anthropological considerations as the SALT acronym implies (Socio-Anthropological Legal and Technical).

The goal of this document (D4.1, entitled "generic process for surveillance") is to describe the "salient features" and processes typical to the design and operation of surveillance systems. This could be seen as a "state of the art" process description preliminary to the application of an explicit privacy/surveillance balance capability, expressed within a SALT framework, and applied during the design phase of the surveillance systems ("by design" approach).

This document also embeds first considerations about privacy harms of biometrics and video-surveillance systems, and possible mitigations that could be taken into account within the "by design" process resulting from the PARIS project. The mitigations based on technological means and answers fall in the scope of PETs, the Privacy Enhancing Technologies.

The approach in this document is bottom-up, based on an abstraction method. The typical process for video-surveillance systems on the one side, and for biometrics systems on the other side is described. Then, a common, generalized and abstracted "meta-models" for a global process for the design of a surveillance system (of any kind) is proposed.

The description of the design and operation processes for video-surveillance systems and biometrics systems, seen as typical surveillance systems in the PARIS project, include their scope of application, their main features/specifications and the involved stakeholders.

Regarding biometric systems, due to the special nature of the biometric data that can be considered in most cases personally identifiable information, standards on Identity Management can be applied. As a recommendation from the EC, the standard ISO/IEC 24760, providing guidance on Identity Management Systems, has been reviewed.

The standard ISO/IEC 24760 [H] is aimed at creating a framework for the secure management of identities in ICT systems. The first part of this standard (ISO/IEC 24760-1:2011) provides an in-depth study of the different concepts of identity and identity management, including a precise terminology and the identification of the main privacy concerns. There are other two parts under development, which will focus on a reference architecture, requirements and best practices.

In this document, the main concepts pointed by ISO/IEC 24760-1:2011 are reflected in section *3 Generic process for biometrics systems* although the terminology is slightly different. This section is focused on the elaboration of a high-level description of the process required for the design of biometric systems, covering the complete development life cycle and identifying the

main users interacting with the system at the different phases. Further details about the different processes and operations in biometric systems will be provided in the deliverables of WP6.

The standard ISO/IEC IS 29100:2011 “Information technology, Security Techniques, Privacy framework”, has been extensively reviewed and considered. This standard “provides a high-level framework for the protection of Personally Identifiable Information within informational and communication technology systems”.

This framework embeds a wide and generic set of terms, concepts and recommendations for privacy protection. This framework is especially applicable to ICT systems, category in which most of the surveillance systems fall, including video-surveillance systems and biometrics systems.

The key point for the PARIS project from ISO/IEC IS 29100:2011 resides in its fifth section “The privacy principles of ISO/IEC 29100”. The 11 privacy principles that are listed here embed and complete the OECD guidelines that were considered in the present document previous version (version prior to the amendment realized on the 11 of July 2013 on the OECD guidelines). ISO/IEC 29100 especially introduces as a guideline the data minimization principle, that was not explicitly brought to attention in the considered OECD guidelines.

By contrast, the SALT framework is a collection of concepts and overarching principles concerning privacy including social-contextual, ethical, legal, and technical viewpoints. It is envisioned to be a reference for decision support during the design of video surveillance systems. The SALT framework is enhanced by a set of tools for accessing to the information and for helping designers throughout the surveillance system process.

The ISO/IEC 29100 guidelines (data minimization included) are to be used within the SALT framework as key classifying categories for the atomic contents of the SALT framework referred to as “SALT concerns”. The possibility to tag each SALT concern with one of the 11 categories of ISO/IEC 29100:2011 will be considered in the precise definition of SALT framework tools. In addition, these categories could be used as a first level check list of privacy-related elements to consider when assessing completeness of a SALT reference.

This deliverable update applies (in the §2.2.7) the 11 privacy guidelines embedded within the ISO/IEC IS 29100 standard, whereas the previous version was using former OECD guidelines.

2 Generic process for video-Surveillance

*[The content is indicative and subject to change through the writing process of this deliverable.]

Figure 1: Video-surveillance big topic

2.1 Introduction to generic process for video-surveillance

The objectives of the present section of the report are to describe what a video-surveillance system is, which kind of missions is typically allocated to this type of surveillance system, and the main stakeholders involved.

An overview of the size, the segmentation, the geographical repartition and the growth of the video-surveillance market enables to underline key missions and trends of video-surveillance systems.

The Urban Security use-case, which seems of typical interest for the PARIS project (the infrastructure here protected being clearly the most generic public space possible), is highlighted and described.

This section also proposes an analysis of the privacy interests at stake in a videosurveillance system and the typical possible mitigations.

In addition, the Annex 1 provides a taxonomy applied to video-surveillance systems.

2.2 Key features about video-surveillance systems

2.2.1 Introduction to video-surveillance systems

From a privacy point of view, Video-surveillance systems can be characterized at 2 main levels:

- At the sensor level, meaning by the camera (CCTV) features (position, image quality..),
- At the exploitation system level. This system implements capabilities that enable to real-time or offline watch, process, tag. The video-streams produced by the sensors.

The first point (CCTV features) enables to characterize the information that is captured by the device, and that is subject by its use to cause privacy harms. The second point (exploitation system) embeds all of the tools and capabilities made available to use the pieces of information produced by the sensor.

2.2.1.1 A quick introduction to CCTV sensors and their characteristics

The CCTV sensors, usually referred to as “cameras” are built of:

- An optical lens that enables to focus the light on a physical sensor, with eventual zooming capabilities,
- A sensor that periodically (e.g. 25 times a second) acquires the information provided by the light. The digitization can be 3-channel (color camera) or mono-channel (monochrome camera),
- An electronic circuit that encodes the information to make it available to external consumers as an expected format.

Most of the cameras are sensible within the visible portion of the electromagnetic spectra (comparable to human eye spectral capabilities). Nevertheless, some cameras are sensible in the Infrared portion of the spectra, making them capable to image thermal information, they are called “thermic cameras” and will operate as well under night and day conditions. Some cameras are built with illuminators that operate in their sensible portion of the spectrum.

Some of the cameras (the oldest ones) are analog, meaning that the signal they use to encode the video signal is an analogical one, while some cameras are digital, meaning the information they transmit is hosted within an analogical signal. The more recent cameras provide digitized information suitable to be dispatched on standard networks such as LANs and WANs (“IP cameras”)..

A very important difference to be noted is the capability for the camera to rotate and/or zoom. A camera can be capable to zoom (enlarge or shrink the image) with very important zooming ratios.

We propose in this document to consider mainly the case of PTZ IP cameras, which are the most standard ones for the use in typical systems used in open public spaces, typically for urban-security applications.

The figure below represents a fixed camera and a PTZ one.

Figure 2: Example fixed and PTZ cameras

For a given zoom level, remain the important factor that influence the quality of the video-stream that is made available by the camera, which are:

- The stream resolution (number of pixels produced in height and width, e.g. HD 720p)
- The number of images produced per second (e.g. 25 images per second),
- The type of compression for the video stream (e.g. MPEG4).

(the compression is a computational way to dramatically decrease the volume of data produced per second by the camera, it has also an effect on the image quality). The pictures below illustrate the difference, for the same camera placed at the same place, between 2 streams qualities. One should notice from a privacy point of view that the left quality make the identification of the person impossible whereas it is certainly possible to guess something about the right one.

Figure 3:illustration of image quality impact on a visual perception of a scene

Finally, compared to the human eye, we could retain the following differences for a video-surveillance classical IP camera:

- Capability to enlarge objects with a magnitude far more important than human eye,

- Capability for some of them to image thermal radiations (thermic or infrared cameras),

At the end, some cameras may also host embedded processing capabilities that will enable to produce additional information (motion detection, intrusion detection).

2.2.1.2 A quick introduction to video exploitation systems, the example of TVS, Thales Video Solution

A video exploitation system is connected to the same network as the cameras it uses, and allows to perform (mainly by human operators, but also sometimes automatically) real-time operations (on the video stream that is being produced now), and operations on recorded video streams.

A video exploitation system is mainly a software enabling to manage and operate video-surveillance systems.

The raw capabilities expected for this type of system are:

- The capability to select a camera, display its video stream, and perform orientation and zoom commands,
- The capability to record the video streams, and to replay them.

A standard video-solution also features many other functions that come in addition to ease the operation of the system, such as: displaying cameras on a map, automating video-surveillance tasks, managing priorities between operators, monitoring the health of the equipments…

The following figure depicts the 3 main modules that make the example video exploitation system, namely the TVS product.

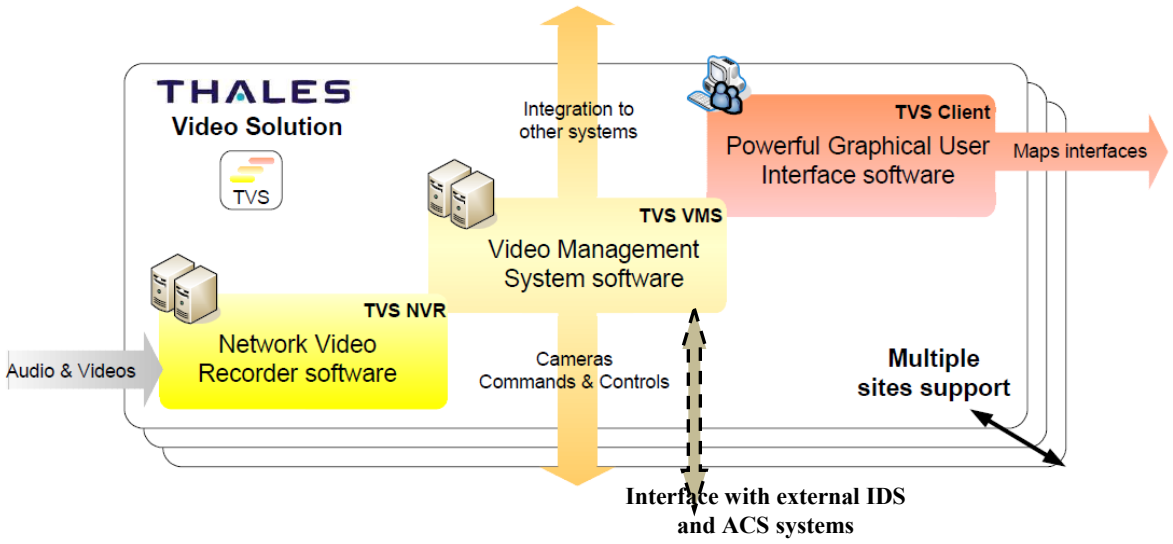

Figure 4: TVS product first level presentation

The 3 main modules building TVS are:

- the TVS NVR (Network Video Recorder), which performs the recording of the video streams outputted by the cameras, the streaming of the recording streams enabling their display and the indexation of the recorded streams sequences,
- The TVS VMS (Video Management System), at the heart of the system, implements the user and camera management functions,
- The TVS Client is the module used by each operator using the product to visualize live and recorded streams, and to configure specific functions.

A typical screen display for a video exploitation system is being reproduced below:

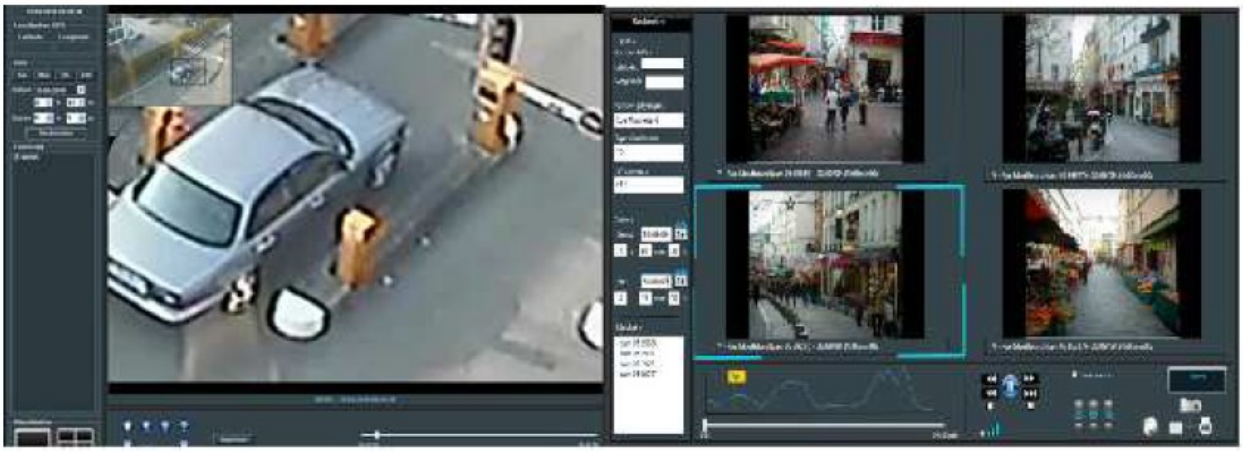

Figure 5: Example operator position for a VMS system

Typically, a realistic video-surveillance system is being operated by 3 to 300 operator positions (with respect to the complexity of the system and to the number of cameras), in Control Centers (C2) equipped also with very big screens called “video-walls”. A photography of a C2 is reproduced below.

Figure 6: Photography of a video-surveillance control center

2.2.1.3 Typical architecture of a video-surveillance system

The typical functional architecture for a video-surveillance system is reproduced below. The sensor part of the system is highlighted in green. The server part of the system is highlighted in yellow. Note that a more detailed architecture and definitions for a video-System can be found in the Annex 1 of this document ("video Surveillance Taxonomy").

The sensor part of the system is made of:

- The camera itself,
- On board processing capabilities (optional, can be within the camera, or near the camera).

The server part of the system is made of:

- The video-management server that typically hosts the management of access rights and priorities among operators using the system,
- The Network Video Recorder that manages the recording of video-streams,
- The Geographical information Server (optional) that will enrich the operator HMI with contextual information (e.g. name of streets, inter-visibility between points..)

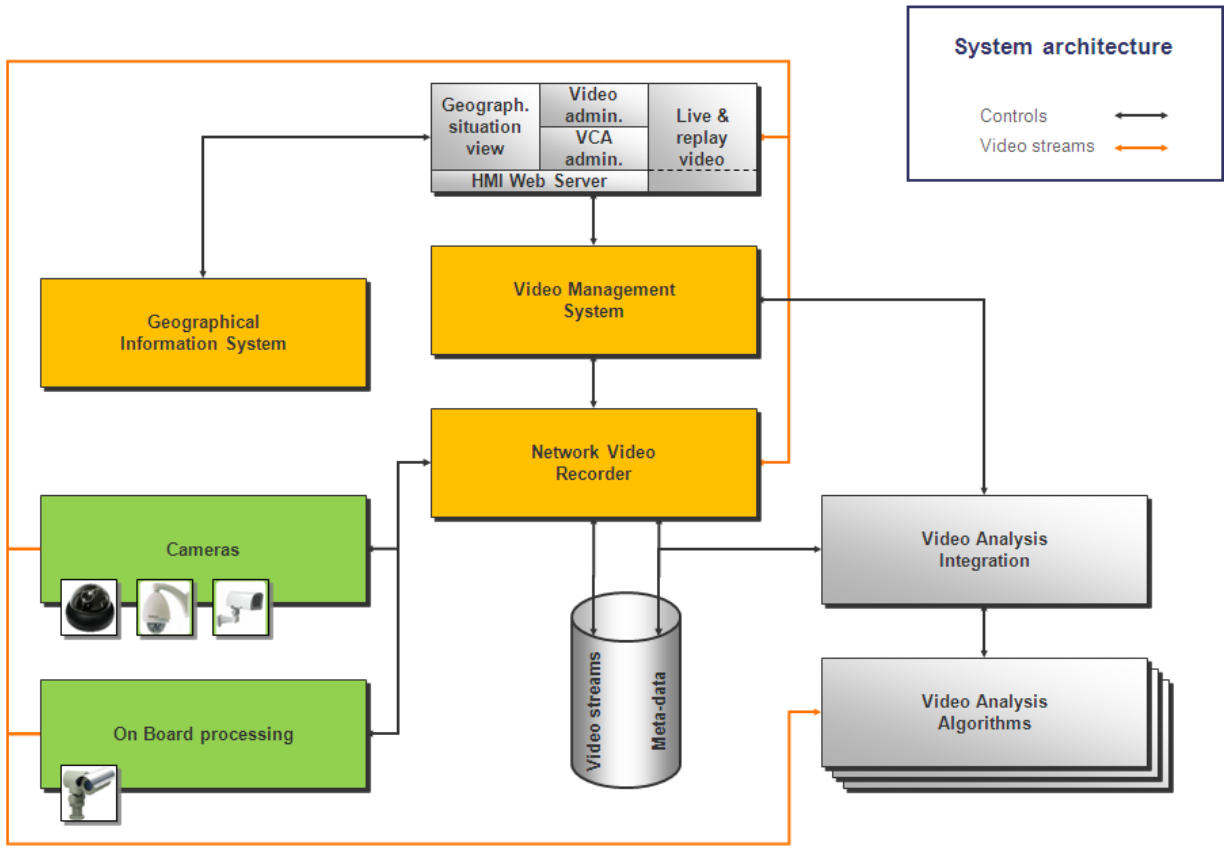

Figure 7: Typical functional architecture of a video-management system

The operator HMI (top of the schematic, in grey) contains:

- Control/command capabilities: selection of a camera, recording of a camera, command (PTZ) of a camera…,
- Visualization capability for live and recorded streams,
- Administration functions (e.g. parametrization of the system) available only to some users with dedicated privileges).

The video analysis algorithms, enabling to extract real-time features within the video streams, are hosted and interfaced in this schematic through a video Analysis integration capability.

In addition to this functional architecture, the figure below depicts a physical deployment for a simple video-surveillance system (this is a mixed analogical/IP architecture).

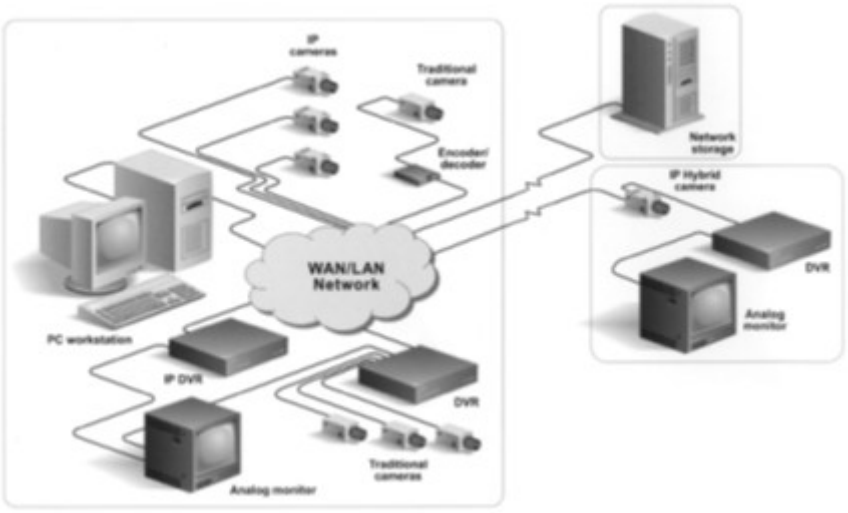

Figure 8: Example for a physical architecture of a video-surveillance system

This physical architecture makes also more straightforward the presence of the IP network (LAN and WAN here presented in a cloud). From a privacy point of view, this element has to be taken into account as it is itself subject to specific privacy harms.

2.2.2 A few words about the video-surveillance market

It is of interest to pay attention to the raw figures regarding the video-surveillance market, for its size, its geographical repartition, and its growth rate. The figure below depicts the global video-surveillance market and its geographical repartition between 3 zones:

- EMEA (Europe, Middle-East and Africa),
- Asia,
- Americas.

Note that this is the typical first level decomposition of the world in market zones used for marketing purposes. This is because these 3 zones are considered to represent the most homogeneous dividing from a distribution point of view.

Moreover, this figure is extracted from the IMS research 2010 (one of the most internationally known marketing and consulting firm) study. Its conclusions can be confirmed by the more recent versions of the study, which state the same orders of magnitude for the markets sizes and growths. IMS research gives 2 types of figures in this study:

- 2009 figures, which are real market sizes,
- 2014 estimated figures, which are projected figures.

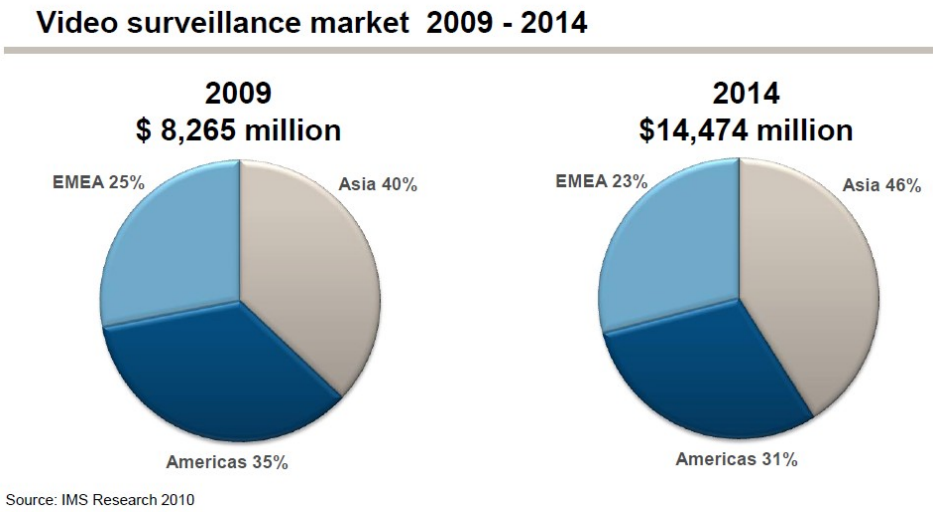

Figure 9: Video-surveillance worldwide market, according to IMS Research [B]

These figures include the purchasing of the hardware (cameras, servers) and the purchasing of the Video management Systems. From the evolution of these figures between 2009 and 2014, a clear and important rise of the market is expected, **which means that the video-surveillance is developing.** The CAGR (Constant Annual Growth Rate) of the global market is evaluated to 12%. The figures presented above also show that the growth **rate is even more important in Asia, where many important video-surveillance projects are being launched**.

An interesting characterization of the market is also given by the segmentation of the suppliers of the video-surveillance market, as this enables to draft the typical procurement chain for a video-surveillance system. The figure below proposes a segmentation of some of the most important actors of the video-surveillance domain (may be a little bit biased by a Thales/European point of view for the list of suppliers, the segmentation categories are general).

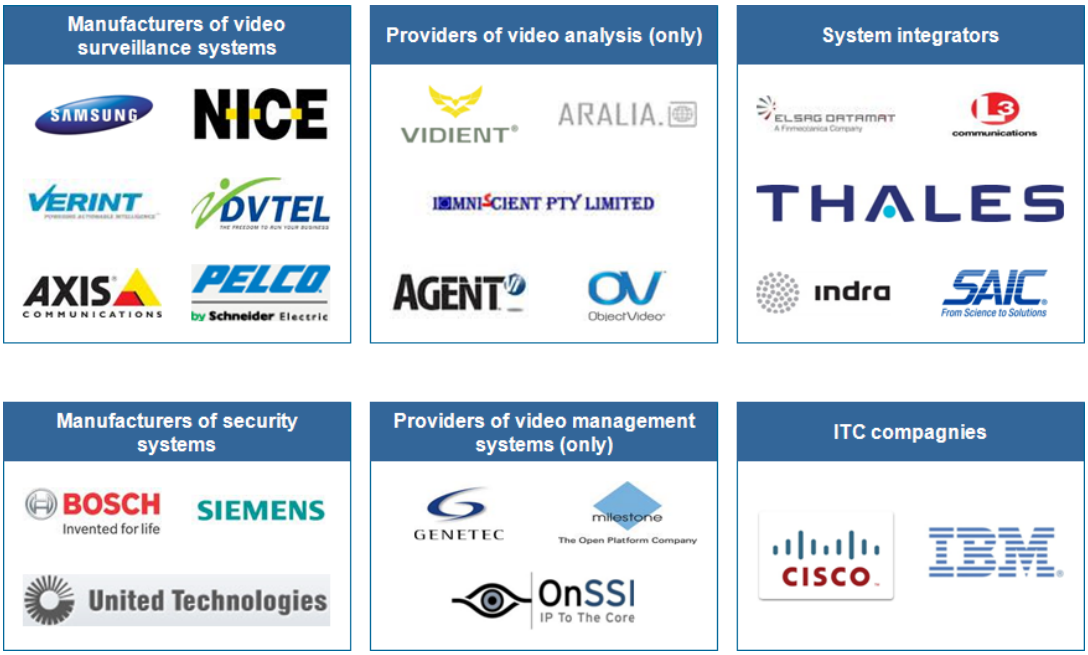

Figure 10: Segmentation of video-surveillance market players

This segmentation gives a very interesting and representative view of the panorama of the video-surveillance market players. The list below provides some more explanations about these suppliers categories and some **first statements about the impact of the features of their products towards privacy**.

- At the lower end of the value chain are found manufacturers of video-surveillance equipments (cameras, servers for recording of streams), such as PELCO, AXIS.. These providers never act as installators or operators of a video-surveillance system. They try to differentiate from others by including in their product features that are requested by the market, such as (about privacy):
  - dynamic masking within the camera of privacy zones (typically dwelling places, private firms),
  - watermarking (technical feature enabling to provide robust integrity/non repudiation proofs regarding the video streams),
  - network based security mechanism to avoid violation of data (encryption..).

- A comparable position is the one of “security systems providers”, who delivers hardware and pieces of software for deploying a whole security system. This means that they will deliver intrusion detection devices, (physical) access control devices as well as cameras. These suppliers rarely (except sometimes SIEMENS) act as installators of security systems. Their economic model is based on the reselling of hardware and software to installators and integrators, their added value is the “ready to deploy” capability of their security systems. They most often incorporate simple capabilities within their video-surveillance systems (few advanced ones such as video analytics) and simple means for operators rights management.

- The suppliers of video-management systems offer software-only video-management suites (no hardware parts such as servers or cameras are part of their offer). They are compatible with most of the hardware on the market, and will differentiate by advanced capabilities that will be deployed by installators / integrators using their products. The capabilities that may impact privacy may e.g. be (from [E]):

    - Advanced management of recorded data and archiving,
    - Operators role management,
    - Privacy zones masking,
    - Operation from mobile devices,
    - HTTPS camera connectivity,
    - Built-in VMD (Video Motion Detection).

- The suppliers of video-analysis systems are very often specialized SMEs. They propose most of the time software dedicated to a specific application domain VCA (Video Content Analysis) use cases (e.g. intrusion detection, abandoned luggage detection..). They do not themselves install the cameras and the software, neither decide to apply such or such VCA capability in a given context. The system design and installation is most of the time carried out by installators and integrators. A chapter is dedicated below to an introduction to VCA systems. From a privacy point of view, it is interesting to note that most of the time, these algorithms are not dedicated to the identification of persons that are filmed, but rather to the identification of specific events or situations (this does not nevertheless mean that their use do not raise privacy issues).

- Most of the time, the actor of the video-surveillance market who is directly in contact with the end-customer is a system integrator (or installators for smaller systems), who will perform at least the purchasing of the video-surveillance system parts (hardware and software), their integration, and the installation within the client infrastructure. This integrator may also install the IP network used by the system. The installator most of the time purely complies (including privacy issues) with the requirements of the end-customer, and/or with approved standards. The requirements may nevertheless let some degree of freedom to the integrator about items that may impact the video-surveillance system, such as:

    - Position of the cameras,
    - Performance of the cameras,
    - Hardening measures enabling to protect the system against internal or external attacks.

    In some cases, the integrator also acts as consultant towards the end-customer. This kind of situation may offer wider degree of freedom for the integrator to influence privacy requirements.

2.2.3 Generic video-surveillance missions and relations to technical parameters

The following extract of document [C] (SIEMENS products datasheet)provides, from the privacy protection point of view, an interesting list of missions that can be expected from the exploitation of video-surveillance system, and the relation between these missions and technical specifications of the system.

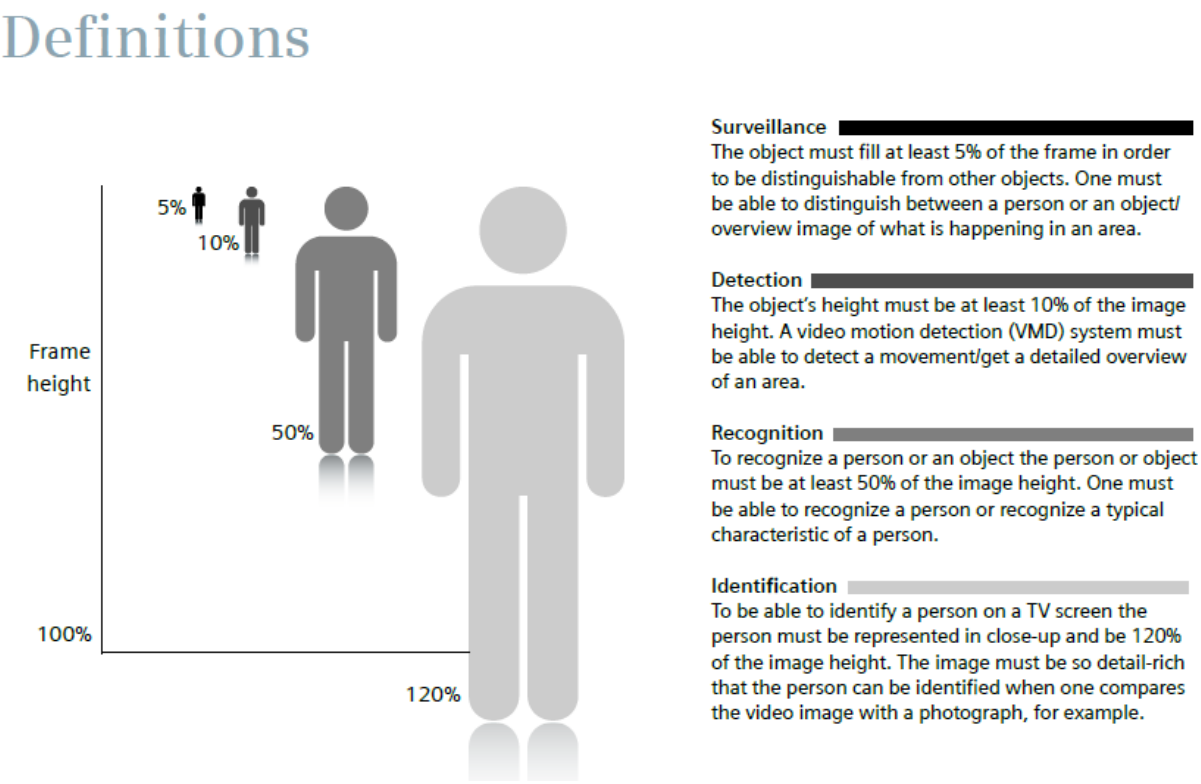

Figure 11: Video-surveillance systems generic missions (extract from [C])

This classification is very useful to differentiate the missions that are handled by a video-surveillance system, especially towards persons that are in the field of surveillance cameras. From surveillance to identification, the goals of the system are very different, and so are the potential privacy harms linked to the normal or abnormal use of the system. Another way to see it is that the position and zooming performances of the sensors (plus their image quality) do impact privacy.

This relation between system missions and quality/features of the video sensor sometimes appear in law, as illustrated by the table below, which reproduces partially French regulation "arrêté du 3 août 2007" related to video-surveillance systems quality expectation in relation with their missions.

Situation	Résolution	Nombre d'images	Plan
Caméra de surveillance de la voie publique en agglomération aux abords d'un site sensible ou d'un monument	CIF	6	Large
Caméra de surveillance en entrée ou sortie d'un commerce, d'un musée, d'une agence bancaire, d'un lieu ouvert au public	4 CIF	12 ou 6	Etroit
Caméra de surveillance d'un automate (DAB...) ou d'un lieu de distribution de fonds transportés	4 CIF	12 ou 6	Etroit
Caméra de surveillance d'un comptoir, d'un guichet, d'une caisse ou d'un terminal de paiement	4 CIF	6	Large
Caméra de surveillance de rayons d'un magasin ou de lutte contre la démarque inconnue	CIF	6	Large
Caméra de surveillance d'une pompe de carburant ou sur une issue de secours	4 CIF	6	Etroit
Caméra de surveillance à l'intérieur d'un véhicule de transport public	4 CIF	6	Etroit
Caméra de surveillance sur un quai de gare	CIF	6	Large
Caméra de surveillance de voie sur route ou autoroute, ou de régulation du trafic routier	CIF	6	Large
Caméra de surveillance aux abords d'un péage routier	4 CIF	6	Etroit
Caméra de vérification et de contrôle d'accès (filmant dans la zone ouverte au public)	4 CIF	6	Etroit

Figure 12 French Arrêté du 3 août 2007: quality specification of the video stream with respect to system missions

2.2.4 Segmentation of video-surveillance systems types

Video-surveillance systems can be used in different types of locations to fulfill different goals. An interesting segmentation of the system types is provided by the segmentation of the video-surveillance market within industry segments (see figure below). This figure is extracted from IMS Research 2010 study on video-surveillance. Figures for 2009 are real figures, figures for 2014 are estimations.

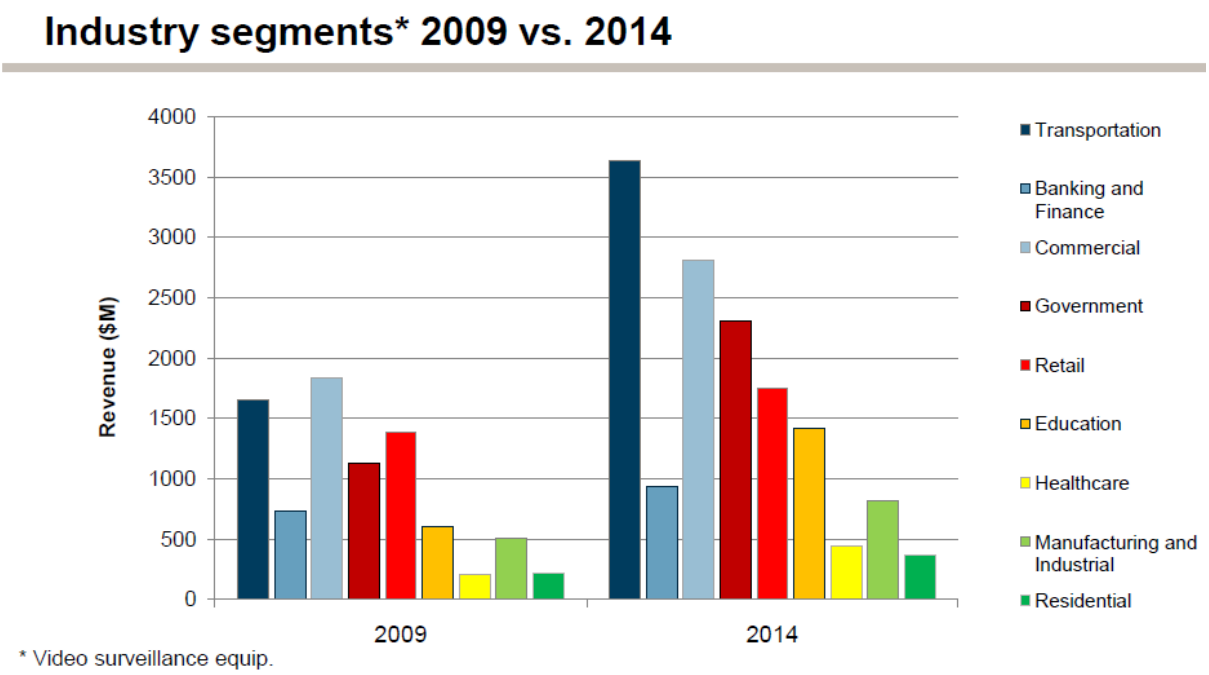

Figure 13: Video-surveillance by industry segments (according to IMS Research)

This figure lets appear a very important development of the market (i.e. of the video-surveillance systems over the world) between 2009 and 2014, especially in transportation systems.

What is of special interest here is that IMS splits video-surveillance systems in categories that enable to differentiate these systems. The most important classification axis may be for these systems:

- Is the infrastructure equipped with a video-surveillance system a public or a private infrastructure?
- Who operates the video-surveillance system? (private, public entities),
- What is the goal of the surveillance system (safety of people, surveillance of a system/a process, safety of goods).

From these points of view, the video-surveillance systems in the IMS-identified industry segments appear to be very different:

- Commercial, Retail, Banking and Finance video-surveillance systems are most of the time privately owned and privately operated. Their goals are to protect goods rather than persons. The data produced by these systems may be used to prosecute persons (customers, employees..),

- Government systems are mostly dedicated to the surveillance and protection of goods and persons within critical infrastructures (ministry premises, nuclear facilities..). They are operated most of the time by public authorities, in deep relation with (physical) access control and intrusion detection systems. This segment also embeds urban-security systems dedicated to the surveillance of public spaces in order to ensure

citizens' and public goods' protection (against volunteer actions, natural disasters, accidents..),

- Transportation systems, which do represent an important part of the video-surveillance market, are often dual-use systems. The typical infrastructures supervised are metro, main lines (stations and on-board) and airports. On the one hand, the video-surveillance system is used in conjunction with the operation of the system or the infrastructure (surveillance of a train position in a station, of the state of electromechanical devices, of queue length in airports). The operation is in this case performed by private operators belonging to the organization responsible for the operation of the infrastructure. On the other hand, a police use of the video-surveillance system is often performed for protection of goods and persons. Typically, the Paris metro network is equipped with thousands of video-cameras, used both by RATP operators (RATP is the operator of the Paris metro), and French Police, but in 2 separated supervision rooms.

One of the trend of the market regarding police missions (protection of citizens) is the integration into a single network of heterogeneous video-surveillance systems. This typically takes the shape of integration of cameras in streets with cameras in metro stations. It seems that some end-users do also consider the possibility to integrate to police video-surveillance systems "semi-private" camera networks such as those installed in shopping malls for example.

2.2.5 Introduction to video analytics and forensics analysis

Video-analytics and forensics analysis both deal with capabilities to automatically process video-streams to extract features of interest for a given application. The goal is more or less to provide assistance to human operators within a huge quantity of data. The difference between analytics and forensics is that analytics is performed real time and forensics is performed on recorded streams. Analytics may help operators by focusing their attention on some devices during real-time operation. Forensics may help investigators identifying video sequences of interest within huge volume of data.

Analytics and forensics rely on high-performance analysis algorithms, most of them falling in the following categories:

- Intrusion and movement detection. This is specially used within zones where nobody should be,
- People tracking. The goal here is to track somebody with one or several cameras, but without identification of the person,
- Stationarity detection. The goal there is to identify dangerous events (abandoned luggage, stopped vehicle);
- Behavior analysis. The Goal is to identify abnormal behavior of people,
- Automatic Number Plate Recognition. The goal is to read cars plates and often to match them with black lists,
- Abnormal direction detection. This is specially applicable to cars, but sometimes also to pedestrian,
- Excessive speed detection;
- Objects classification;
- Facial recognition, which overlaps with biometrics systems.

The most classical and mature algorithms are Plate recognition and Intrusion/movement detection. Processing of sound is also often used jointly with video-processing to enhance results. For most of the algorithms, few normalization exists about results productions and performance measurement. Video-analytics remains an active field of research.

The performance for these algorithms depends on cameras quality, position and orientation. The privacy potential harm linked to analytics may reside in the data that are produced by analytics, but also by the raw video that are most of the time recorded.

The figure below presents the global video-analytics process.

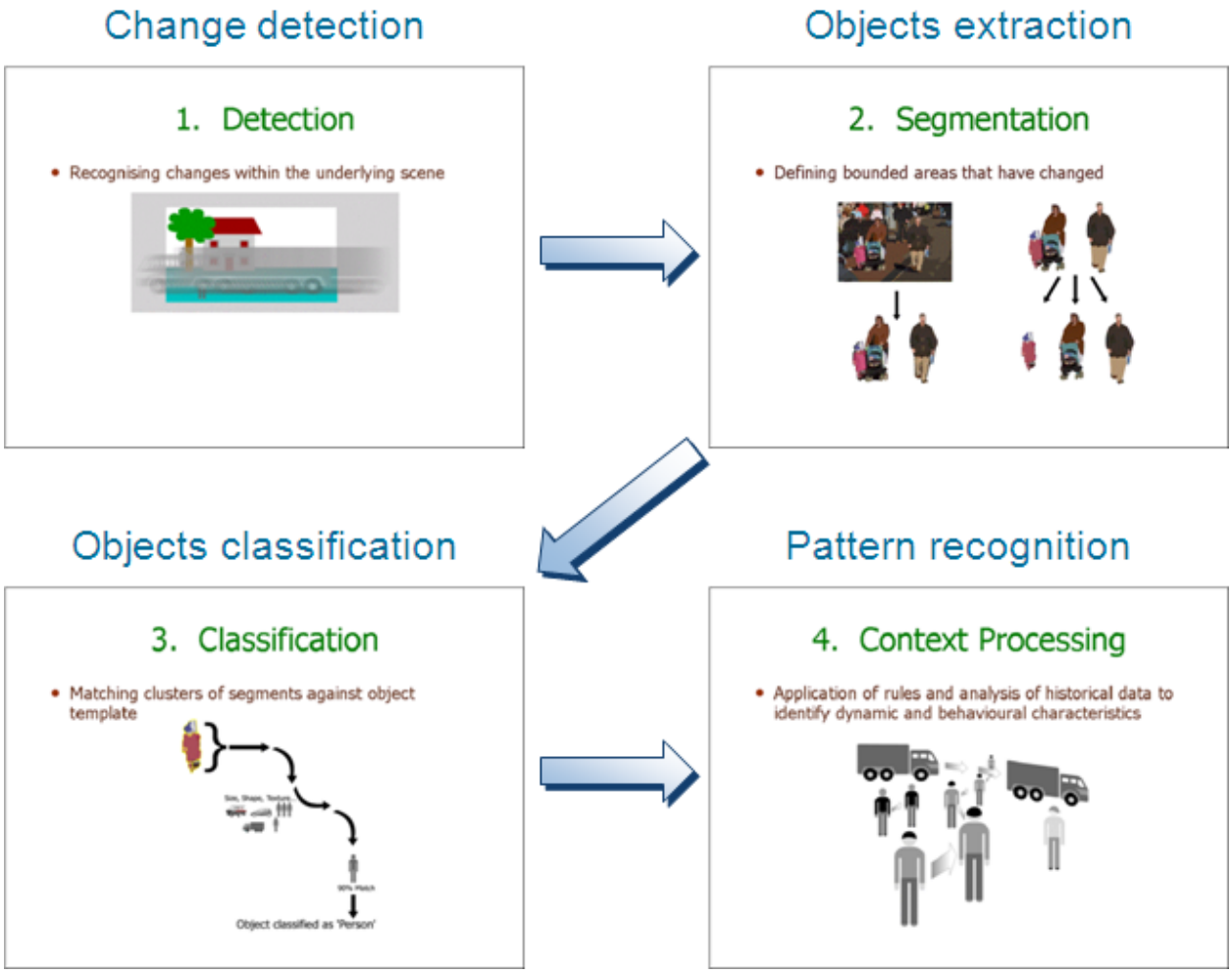

Figure 14: Generic analytics process

Note that the advanced generic steps (classification and recognition) may not be useful for simpler algorithms.

The figure below represents, for concrete illustration goal, the use of video-analytics to prevent tourists to climb the “piazza della Signora” statue, system installed by Thales in Firenze.

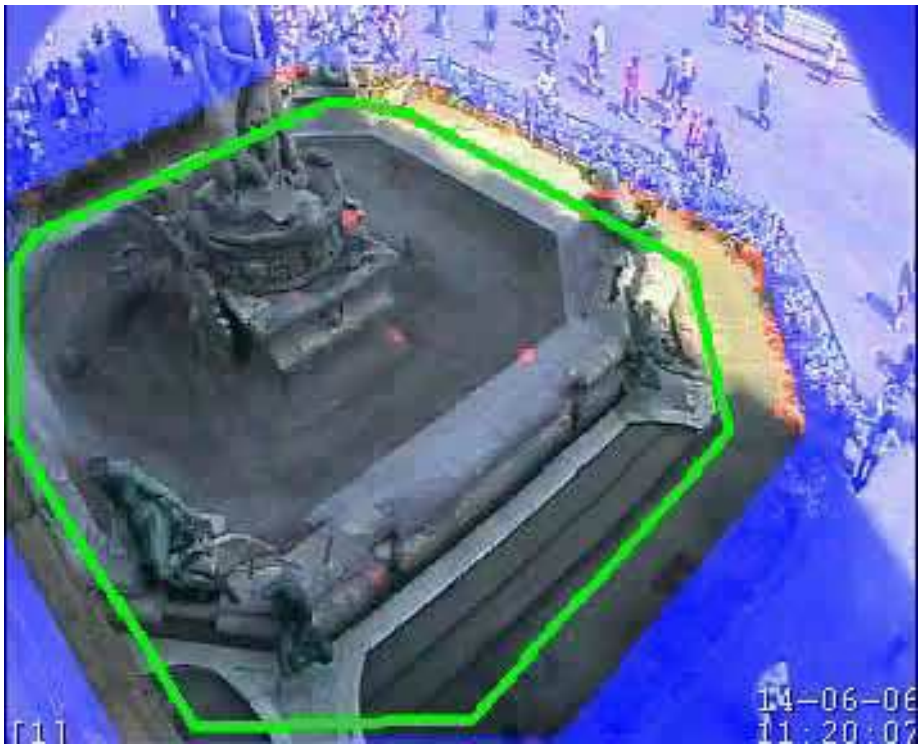

Figure 15: Intrusion detection on Piazza Della Signora statue using video-analytics

2.2.6 Focus on urban-security systems missions and stakeholders

Video-surveillance for big systems rarely comes as an isolated capability. The video-surveillance system is one of the systems used to achieve a complete mission, which can e.g. be the protection of a site. This part focuses on urban-security systems, which are systems using cameras as surveillance sensors mainly dispatched in open public areas, jointly with other systems (typically communication systems and Resources Management Systems).

2.2.6.1 Main goals for a urban security system deployment

FROST & SULLIVAN 'safe city report' focuses in its introduction on the definition of what is, globally speaking, a 'safe city' providing answers about the main goals of the deployment of urban security systems.

Figure 16: How to define a safe city? From Frost & Sullivan 2011, safe city report part 1.

These definitions, very general, insist on the global answer to security and safety within the city. Video-surveillance is one of the components of the security system. Some cities may also wish to extend their supervision system to the management of crisis such as natural and industrial hazards.

2.2.6.2 Stakeholders of a urban security system

The figure below depicts a typical urban security system (adapted to a city size ranging from middle to big), showing the organization of the system, some of its stakeholders, and 3 scenarios for its use:

- Management of a crowd e.g. near an exhibition,
- Management of the attack of a bank,
- Management of a fire.

Figure 17:Big picture of a urban security system

A wide range of persons can be considered as stakeholders within these systems. A few details about these persons and organizations are described below.

2.2.6.2.1 Decision making about a urban security system

In general, the decision makers for Urban Security projects are not the end users, who are the operators in the control centers and the resources deployed on the field (policemen for instance). The decision makers are:

- Either the City Authorities: their objectives are in this case to provide a more secure city to their citizens to make the city more attractive from an economic point of view, and to ease the re-elections at the end of their mandate;
- Either a City Department in delegation of the City Authorities. If this Department is in charge of the management of a domain of the city (for instance, the security), they behave the same way as the City Authorities: they look for a system that will provide a better efficiency to their operators, at a good price. Their main competence may have an impact on the development of the surveillance system. For instance, if the Department which has the delegation of the City Authorities is the IT Department, they will pay less attention to the end-users and they will look more at the technology.

In both cases, besides the usual political leverages which are very important for a project in a city, the key influencers are the end-users, who are typically the police forces.

2.2.6.2.2 Operation: users of the system

The users of the system are mainly members of public forces, and can be described using the typical army commandment chain paradigm between:

- Those who are near the event (tactical level): policemen, firefighters. They may use a remote terminal from the central system enabling them e.g. to view videos pushed by the central,
- Those who are organizing the global response to a given event (operational level): they are operators who use typically video-surveillance as a detection and confirmation mean, mobilize the tactical level, and document the events,
- Those who are taking care about the global health of the ecosystem supervised and of the global policy to apply (strategical level). They are typically political authorities, or belong to the high level management within responders organizations.

2.2.6.2.3 Supply and maintenance of the system

The other stakeholders of the system are its suppliers. Generally speaking, concerning a urban security system, a unique supplier is responsible for the whole system delivery and maintenance. This supplier will subcontract parts of the system to other companies. The main lots are generally:

- provision (or adaptation) of the IP network for information transmission (video streams mainly),
- provision of the video-surveillance system,
- provision of the mission-management system (often called the CAD, for Computed aided Dispatch),
- provision of the communication system (e.g. radio system).

Most of the time, the suppliers have to comply with a contract (Statement Of Work), which generally embeds most of the constraints linked to the functionalities and performances attached to the system. This document may also reference national or international norms and standards to comply with. At the end, the commitment of the supplier(s) is “only” to fulfill the requirements expressed by the customer.

In some cases, the customer expresses more fuzzy requirements about its security system, and expects the provider to act as a consultant, especially for the definition of operational procedures to follow.

At the end of the delivery phase (sometimes called the “build”), the suppliers’ employees do have a very good understanding of the system, but normally do not gain any more access to the system.

Nevertheless, it is very common that the contract includes a maintenance phase, which is performed by suppliers’ employees that may by force need access to any part of the system.

2.2.6.2.4 Other stakehorlders

The other stakeholders of a urban security system are those who are filmed by the system (citizens, tourists, workers), and those who may use some of its productions (courts, judges).

2.2.6.3 Main processes for the use of a urban security system

The main use cases and high-level processes for the use of a urban-security system are depicted in the table below.

Type	Business process type	Case
Operations use cases	Surveillance management	Observe Scene
		Assess alarms
		Manage citizen calls
	Missions management	Create incident
		Dispatch incident
		Update incident
		Close incident
		Plan mission

Type	Business process type	Case
		Supervise call taking
		Supervise dispatching
		Manage shift
	Citizen services	Inform Public and collect Public opinion and complaint on Web Portal
	Operational Support	Generate statistics
		Manage case folder
Support use cases	Training and simulation	Manage training and simulation
	Administration and supervision	Administrate system

Figure 18: Main processes for the operation of a urban surveillance system

The video-surveillance part of the system is mainly used within the "surveillance management" process.

2.2.7 Main privacy issues linked to video-surveillance systems, and possible design mitigations

The analysis performed here is based on the privacy principles of ISO/IEC 29100 [G] Information technology, Security techniques, Privacy framework. These principles are of great interest, not only because they build upon the principles contained in the OECD Guidelines and the European data protection framework, but also because they specify these principles for the design of ICT systems. Quoting the aforementioned [G] standard itself: "This framework focuses on the implementation of the privacy principles in ICT systems and the development of privacy management systems to be implemented within the organisations using these systems. These privacy principles should be used to guide the design, development, and implementation of privacy policies and privacy controls." These principles are for these reasons an appropriate analysis grid towards privacy issues at stake with video-surveillance systems.

There are 11 privacy principles in ISO/IEC 29100:

1. Consent and choice
2. Purpose legitimacy and specification
3. Collection limitation
4. Data minimization
5. Use, retention and disclosure limitation
6. Accuracy and quality
7. Openness, transparency and notice
8. Individual participation and access
9. Accountability
10. Information Security
11. Privacy compliance

For each of these 11 principles, an identification of the privacy harms / solutions related to the use of video-surveillance systems is proposed below.

ISO/IEC 29100:2011E privacy principle	related privacy harm on VS system	possible mitigations on VS system
1- consent and choice	The principle of consent and choice is, in general, irrelevant for videosurveillance system. However, specific concerns relating to the possibility for the PII principal to gain information about the system and to raise feedback can positively contribute to involve PII principals and mitigate the absence of consent.	
	Impossibility for the PII principal to gain information about the implememtation of the system	To give to the public an access to the description (camera positions, field of views), to the features and to the performances (example images) of the system in an understandable and easily reachable way.
	Impossibility for the PII principal to raise feedback about the system	To give a mean to the citizen to raise comments about the system (free notes on a web site e.g.)
	No impact of PII principals feedbacks on the sytem features and system's organisation processes	To organize periodic reviews of the public feedbacks and requests and to hold a decision process to modify the system or its usage processes
2- purpose legitimacy and specification		
	PII principals not aware of the installation and use of the video-surveillance system	To inform the public of the existence and golas of the system before it is being used
	No clear identification of operational needs during conception leading to poorly balanced system	To put in place a clear process for operationnal needs qualifiation
3- collection limitation		
	Too much sampling of space compared with the system missions (e.g. possible identification of persons where not needed)	To adapt the number of cameras to the needs To adapt the positions of the cameras to the needs To adapt zooming capabilities of the cameras to the needs To adapt the image quality (resolution, FPS, compression) to the needs
	Private data may be captured by the system without need (faces, private housing..)	To provide dynamic masking of fixed privacy zones (may be reversible to certain operators) To provide dynamic obfuscation of moving privacy zones (may be reversible to certain operators)
	More accurate than needed content analysis	To limit the type, pertformances and field of application of VCA algorithms.
4- data minimization		
	Wider than needed authorisations to operators	To define clearly the roles of the operators and to limit strictly their rights within the system to their roles
	Punctual need-to-now results in permanent authorization	To set by-default rules and access rights that minimize the access to the information. Punctual need to access video data to be requested and justfied by the operators.
	Too much metadata information attached to the video	To limit metadata streams computations and recordings, especially when highering the privacy harms linked to the video data (behavior analysis, free coments from operators, oher systems informations such as access control systems)
5- use, retention and disclosure limitation		
	No deletion of recordings that should be deleted	To provide automatic capabilities for recrding lifecycle control To perform audits on the data present in the system
	Recorded data available to non authorized operators	To put in place a clear role definition and administration policy To control Physical access to the operator stations
	Live data available to non authorized operators	To put in place a clear role definition and administration policy To limit the right to acess to recordings with respect to the mission of the system To control Physical access to the operator stations
	Metadatas enable too fine search within videos	To put in place within metadata tools limitations in capabilities based on operators roles
6- accuracy and quality		
	The system performance might not allow sufficient performance to achieve its purpose (recognition of PII principal, identification of PII principal)	To assess that the caemra positions, fields of view, resolutions, frames per second allow sufficient performance to meet the needs of the system
	Possible alteration of streams	information security analysis and penetration test of the system
	Need for proving the integrity of streams	To use network-level capabilities (HTTPS, 802.1X) To watermark the streams
	Need for proving the integrrity of recordings	To encrypt the recordings To hash-sign the recordings
7- openess, transparency and notice		
	PII principals do not gain access or sufficient awareness of the video system use	To provide to PII principal clear and understandable notice about the use of the video surveillance system, its goals and the processes that apply to its usage
8- individual participation and access		
	No sufficient information for the PII principals about the video-surveillance system	To inform about the position of each camera To inform about the features of each camera To inform about the purpose of the system To propose demonstrations of real operation of the system To allow (internet) access to (downgraded) video-streams
	No sufficient information for the PII principals about the privacy identifiable information used in the system (car plates, face bases)	To make available the Privacy Identifiable Information to PII principals
	No participations of the citizens to the design of the system	To allow participation of citizens to the design of the system
	No capability for the PII principals to officialy react about the system	To put in place a possibility to record and track citizens questions and complaints

Figure 19: Video surveillance privacy harms and possible mitigations

ISO/IEC 29100:2011E privacy principle	related privacy harm on VS system	possible mitigations on VS system
9- accountability		
	No track of operators actions	To timestamp and to record all actions of operators. To film the operators. To record the operator screens. To Limit the possible operator actions: hardware hardening, OS hardening
	No understanding of the operator of privacy	To establish a privacy awareness program to train the operators
10-information security		
	Possible IT attack from insiders	To harden the operators positions (hardware and OS) To harden logical access (to the network) from operator positions To authenticate at network level any device connected (e.g. 802.1X)
	Repudiation of actions by insiders	To put in place an efficient password management tool/policy To harden the authentication (biometrics, smart card..) To control and record physical accesses to physical control room
	Possible IT attack from outsiders	To provide adapted security at the network level To avoid any wireless data exchange To physically segregate video-networks To logically (VLAN) segregate video-networks To use armoured wires for network
	Possible security failures in the system	Information security analysis and penetration test of the system
11- privacy compliance		
	Privacy protection defined measures and processes not fully implemented or followed	To conduct periodically audits on the videosurveuillance system to check that the whole privacy related measures and processes are held
	Evolving or incoming privacy risks not managed	To conduct regular privacy risks assessments on the videosurveillance system, especially taking into accout new privacy risks (new harming technologies, privacy encountered problems on video systems)

It is noticeable that the privacy harms related to the misuse or hack of the video-surveillance system are related to the whole components of the system, including the hardware and Operating Systems of the servers hosting the VMS software, and to the network (LAN and/or WAN) underlying.

We could introduce the notion of Privacy Point Of Failure (PPOF) by analogy with the Single Point Of Failure (SPOF) concept used within highly-available systems designs. Possible PPOF, as shown within the figure below (left schematic, operators excluded), can arise from one of the 3 main components of the whole system: Network, Operating System and Application. A more precise decomposition of a system for PPOF identification may be derived from the OSI model (right schematic on the figure below).

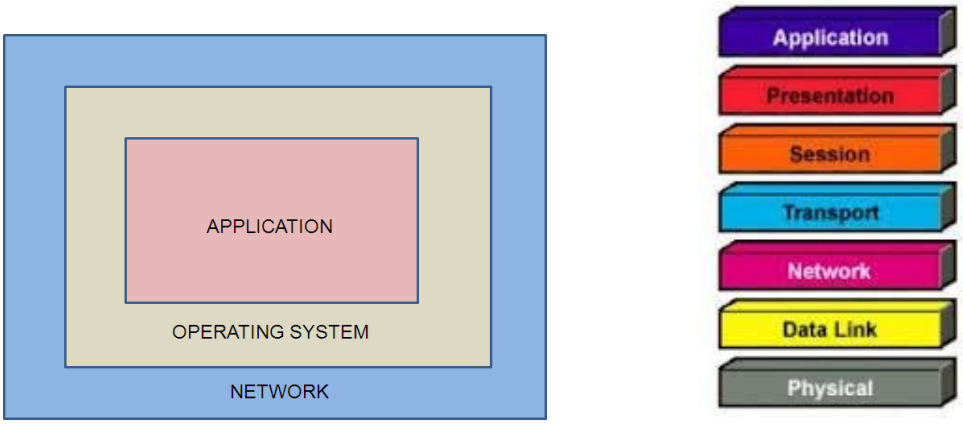

Figure 20: Possible Privacy Point Of Failure (PPOF) in a global Video-Surveillance System (operators excluded)

This is illustrated by a recent recommendation (see [F]) issued by the French Prime Minister office about video-surveillance security systems deployed for public security-related missions, and falling under the scope of systems of "videoprotection" (see D.2.1 the legal requirements applied to "videoprotection" in France). The primary objective of this recommendation is mainly to provide data security recommendations in order to ensure the confidentiality of the video-system data. Most of the recommendations enclosed within this paper are about the network and not about the video-surveillance system itself. Examples of recommendations are:

- To logically or physically isolate video-network from other-purposes networks,
- To use network encryption mechanisms,
- To use network device authentication mechanisms (802.1X).

2.2.8 A methodology for Operational needs (CONOPS) capture

This part describes the fundamentals of the Thales Internal methodology that is used to describe with a customer his needs e.g. during consultancy actions about video-surveillance systems.

The methodology is inspired from the NAF methodology (NATO Architecture Framework). The main questions the methodology ambitions to answer are depicted on the schematic below.

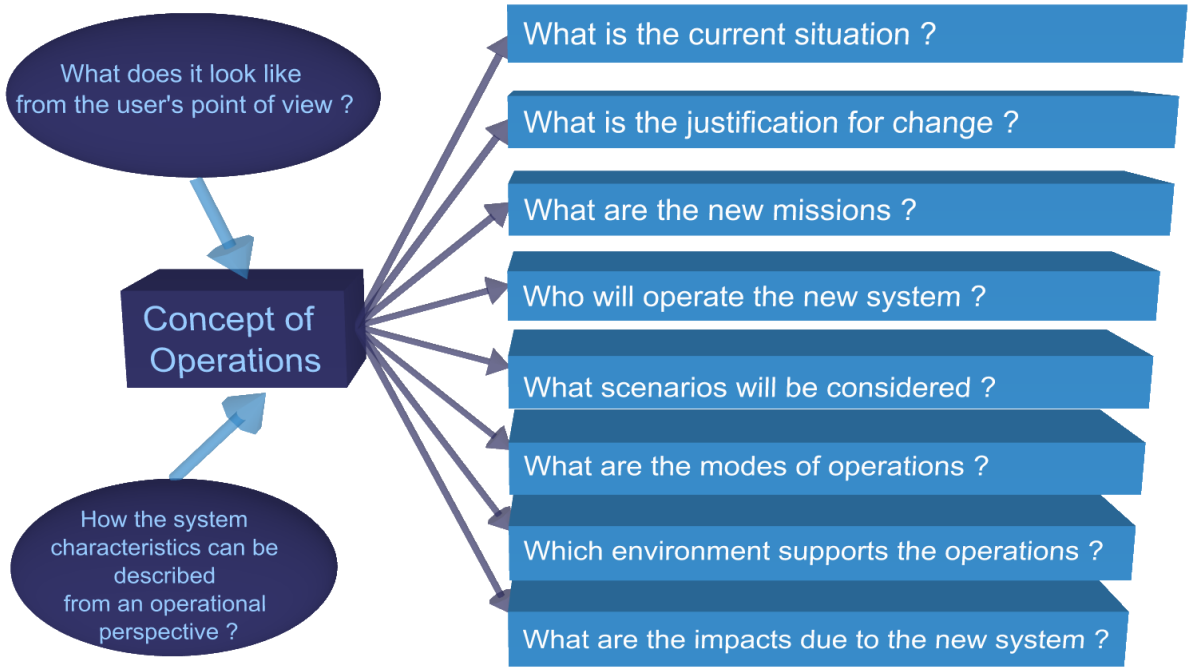

Figure 21: Operational concepts questions within Thales internal CONOPS methodology

2.3 Conclusion: Typical end-to-end design process for a video-surveillance system

This document underlines two important distinctive features for video-surveillance systems missions: the first feature is that video-surveillance systems can be deployed in very different contexts: from the protection of an highly-restricted place (e.g. military base, ministry..), the surveillance with the simplest system possible of a shop, to large scale systems that can reach the size of a city. The second feature is that, very often (except for the simplest applications), the surveillance system deployed is not solely based on video. It embeds e.g. access control, communications, resources (first responders) mission management capabilities.

The case of the urban security systems seems to be very relevant for the PARIS project for several reasons. The first reason is that it applies within a generic public space (streets, parks..), which makes particularly concrete the privacy protection issues. The second reason is that urban security systems are predicted to grow quickly all over the world (and especially in Asia). Moreover, an identified trend is that these systems may interface video-surveillance systems from semi-private spaces (railway stations, shopping malls..). Another reason is the number of stakeholders entering the loop, especially during the operation of the system.

The analysis, coming from real-life (Thales) implementations and commercial approaches, shows that the key decision makers for the decision to purchase a video-surveillance system are at politic level.

When the purchase decision is taken, the key stakeholder involved within the system design is a consultancy agency that will define the most important topics for the system, which are its operational missions and generic specifications. This consulting agency can be either an external private society, a state agency, or even the chosen provider for the system.

One should note that an important point for the balance between surveillance and privacy is the operational concept and missions attributed to the system.

The technical specifications are normally derived from the concept of operations. The derivation is either performed by the consultancy firm, or by the installator/integrator of the system. For sure, this point of the design process is critical from a privacy point of view, in the sense that for many reasons the technical specifications might exceed the minimum dictated by the operational needs.

The installator / integrator, responsible for the system deployment has to fulfill the technical and operational specifications. These specifications are most of the time understood (and tested) as “minimum required”, meaning that a far more performant than needed system would be accepted. This can be of importance for privacy versus surveillance balance control.

The installator /integrator remains most of the time in the loop, even when the system has been delivered through maintenance actions. Some maintenance experts may access most of the part of the system to be capable to guarantee quick and efficient repair in the case of any failure within the system.

After the delivery has been performed, the users of the system become the main stakeholders, i.e. its operators, administrators, who can own specific roles and responsibilities, such as police

ones. The system shall most of the time enforce limitation of access to data to each of these stakeholders, according to their roles and access rights. One shall notice that the adequate definition of each of the roles, and adequate control of the enforcement of this policy have a strong impact on the global privacy protection of any person whose image is captured by the system. This is one of the chore issue related to the “accountability” of the surveillance system (See D.2.1).

3 Generic process for biometrics systems

In this section, we are going to describe the generic process used to design the different biometrics systems. First, we start seeing a brief introduction about the generic process. Then, we will see other important points about biometrics systems such as the different phases, modules and the different modes of operation involved in a biometrics system, some privacy issues, or how the privacy issues can affect the design process. Finally, we will comment the final conclusions.

3.1 Introduction to generic process for biometrics

The main idea of this section is to understand all the processes and operations that are common, as a general rule, to biometric systems.

Nowadays, biometric systems are growing considerably as they are being used for security issues in different contexts. Some examples of the use of these systems are: border control and immigration programs, security in airports, access control in banks, casinos, private organizations and so on. All of these systems follow a common process that we are going to describe next.

Generally, almost all biometric systems have two main phases. These phases are the enrollment and matching.

The target of the enrollment phase is to link the data processed by the system to a person, and subsequently store it. A good example is an access control which uses a fingerprint recognition system in order to allow people to enter in a specific room. Everybody which is going to have the enough permissions to enter the room must provide the appropriate data to the system in the enrollment process.

The aim of the matching phase is to compare the previously stored data (enrollment phase) with the data the user is currently exposing to the biometric system.

Once defined the different phases, we are in position to understand the generic process of the biometric systems. On this generic process we can differentiate various phases in the lifecycle of a biometric system. These phases are: requirements, design & development, testing and maintenance.

Before starting with the description of the different phases, it is important to mention that we will make a special emphasis on the requirement phase, since the other phases are based on the requirements. Finally, we will see a graphical representation where we can observe the different iterations between the system, citizens and organizations.

The first step before capturing the requirements is to have a clear idea about the perspective of the system. For this reason, we need a description from the organization point of view. In addition, it is very important to understand the criticality of the system in order to have an intuitive knowledge of the security problems.

3.1.1 Requirements

Now that we have a clear description of the system, we are positioned to capture the different requirements of the system. Before starting with the description of the requirements, it is very important to highlight that this document only provides a summary of the most important requirements, and that the list of requirements could therefore be longer.

We can divide the requirements in two main groups: Functional and Non Functional requirements. In turn, we can split the Non Functional requirements in four groups: Operational, Environment, Technical and Privacy requirements.

3.1.1.1 Functional Requirements.

First of all, we will concentrate on the functional requirements, which detail the **specific functions to be accomplished by the system**. We can consider four main different functions:

- Enrolment functions

As we will see later, the enrollment phase is the prior stage that everyone using the system must pass. Hence at this point, we must decide whether the system is going to need such phase. It is common that biometric systems need an enrollment stage.

In that case, it is necessary to understand if, apart from the biometric data (described in section 3.2), we need some extra information from the user, such as a PIN or password. Besides, it is relevant to establish whether the user's presence will be needed (On-line Live Enrollment) or not (Off-Line Enrollment). For example, we can use a photo for an off-line enrollment.

- Response of the system (positive or negative)

After completing the enrollment phase, the system could identify or verify the user. However, depending on the system, the action taken in response to a negative or positive identification may be different.

For example, imagine we have to pass an access control to enter in the offices of the company where we work. In this case, when the system recognizes us it opens the doors. However, if the system fails, the user cannot enter his/her offices. So, it is likely that we need an operator to verify the identity of the person and open the door.

Another example could be a system to detect possible suspects. In this case, when a suspect is detected, it is needed to have an operator to avoid false alarms. Therefore, it is crucial to know the system response to a negative or positive identification/verification.

- Data Management

Another important point is the data management. Here, we have to detail the data which the system is going to store, how the system is going to use the data and how and under which circumstances the system will delete the data of the user. For example in an access control when a person leaves the company, the personal data must be deleted.

- Special Functions

The functions specific to the system must be clearly detailed.

3.1.1.2 Operational Requirements.

The Operational Requirements of the system detail the concepts for how the system is used, the classes and privilages of the users, and the availability required of the system to support all aspects of the organizations.

First of all, it is necessary to describe the different procedures, within the organization and/or between different organizations, if there are several organizations involved.

The goal is to understand the objective of each set of operational procedures. For example, we have to explain the procedure of an operator responding to a specific operation (i.e alarm). On the contrary, we also have to define the procedure for unattended operations.

After understanding the different procedures, it is important to detail the information flow. Hence, among other things, we have to identify the data source, where the data is processed/analysed, where the data is stored and in some cases what kind of data is transferred between different organizations.

The operational requirements must also address user-specific functions and processes , not only defining the processes that can be performed by each class of users, but also defining information and control requirements as access privilege.

Moreover, the interaction between the user and the system must be described: for example, if the system requires from the users to perform some specific action (i.e put his/her finger over a reader), or if the user needs external help.

Finally, the operational requirements must also reflect the availability of the system, that is to say the amount of time a system is operational. The system could be working during the whole day or only when the user presses a specific button.

3.1.1.3 Technical Requirements.

The technical requirements detail the specific capacity, performance and the different technical requirements associated to each operational procedures and system functions.

First of all, we have to describe if the system processes the data in a central system or if the process is made in a distributed system. In the same way, we have to define if the system stores the data in one or several databases.

Secondly, we have to take into account the communication requirements. We must specify the connectivity of the systems (i.e WAN, LAN) and the security mechanisms (i.e firewalls etc...).

Thirdly, we should have a clear idea of the number of users who undergo the system in order to establish if the system will be a small, medium or large scale. Furthermore, we need to describe if the system is likely to grow much. In that case, we will have to design the system to bescalable.

In terms of performance, we have to take into account the accuracy, frame rate and time of response. The accuracy and frame rate are closely related to the criticality of the system. For instance, if the system must be highly secure, we will need a very accurate system with a very low error rate. It may be considered to include more than one biometric system in order to make the system safer. Concerning the time of response, we need to assess whether we need an immediate response of the system or not.

Finally, the technical requirements must also reflect the integration issues. The integration issues are an assessment of how to accomplish the development and integration of custom capabilities and to integrate the application with the existing systems infrastructure.

3.1.1.4 Environment Requirements.

These requirements describe the physical and environmental conditions and constraints associated. Environmental conditions are very important to select a specific biometric system.

Therefore, we have to detail if the system will operate indoors or outdoors. Another important point is the light, humidity, noise and temperature conditions of the place where we will install the system. For example, depending on the light conditions we may rule out a camera as a sensor.

Finally, we have to detail the different places we have to cover: for instance, If we have to cover one room or several.

3.1.1.5 Privacy Requirements.

As the biometric system can have a big impact on people, it is very important to describe the privacy requirements of the system. We must emphasize that we only give some general requirements regarding privacy at this stage, since the integration of privacy requirements is

one of the main goal of this project and therefore is something that will be tackled in more detail throughout the project duration.

First of all, it is important to consider some issues related to the interaction between the system and the user in terms of privacy. The user must be informed that his/her own personal data are processed, as well as the purpose for which the system processes and stores his/her data. Moreover, the users may have the right to access, modify and delete their personal information, according to the circumstances.

Secondly, as these kinds of system can be used to detect some possible suspected criminals, we have to describe the consequences of a system failure. Furthermore, we need to describe the potentially impact of the misuse of the processed and stored data, since a system failure or data misuse can damage a person's identity. For these reasons, these factors are extremely important to select a system with a very low error rate.

Thirdly, in order to prevent damage to the person's identity, we must specify mechanisms for data protection and the misuse of the data.

Finally, the last important point related to privacy is the accountability. We have to describe the different operations of people (i.e operator) who can manipulate the data that will be recorded, based on limited access rights and authorizations to handle the data. For example, it will be revealed more or less information about users, depending on the kind of operator who is trying to access the information.

After describing the most important requirement for a biometric system, we are in a position to present the other phases of biometric systems: design & development, testing and maintenance. As we previously stated, we will not enter in much detail in these phases since the vast majority of the decisions in these phases are based on the requirements shortly presented above and which are the object of WP2 of the project.

3.1.2 Design & Development

Once the different requirements have been presented, we are going to present some details about the design and development phase.

One of the first thing that we have to decide at this point is whether we are going to deploy a single biometric system or several (multimodal system). We will make this decision based mainly on some requirements captured, such as the place that we have to cover, the accuracy level or maximum error rate.

After that, we have to decide the specific biometric systems that we are going to deploy (i.e face recognition, vein recognition or fingerprint recognition) based mainly on the criticality of the system, privacy issues, the different environment conditions, the number of users who undergo the system and so on.

Once we have selected the number and kind of biometric systems, we can focus on more detail in the architecture of the system. Here, we are going to establish the connection between the different modules of the system, the place or places where we are going to store and process the data, the communications including security measures (i.e firewalls), and some integration issues with other systems.

Finally, we try to minimize the impact of the privacy issues on the person's identity. For example, we can decide to encrypt the personal data, use a policy of access to the data, record all the actions that the operators will carry out over the personal data and so on.

3.1.3 Testing

During and after the development process, we should do different tests in order to check all the functionalities and procedures of the system. We can split the testing in three groups: Technological, Scenario testing and Operational testing,

- Technological testing: Such tests are done in a laboratory environment. The goal of this type is to test the acquisition, processing, storage and comparison of data as well as the system decisions and the different procedures of the system.
- Scenario Testing: Such tests are carried out with the particular conditions of the environment where the system will be subsequently installed. Another important point, it is that the population is controlled.
- Operational testing: Such tests are performed in a real environment and the population is not controlled.

3.1.4 Maintenance

The last part of the process is to maintain the system. The system maintenance includes the biometric devices, the system, the environment conditions (i.e maintain a right level of light) and so on. We can classify the maintenance of the system in two groups: Preventive and Corrective maintenance.

Preventive maintenance: the idea is to keep the environment under appropriate conditions. For example, regarding a finger recognition system, we must keep clean the surface where users put their fingers in order to avoid low quality samples.

Corrective maintenance: the idea is to identify the source of an equipment or software malfunction and either repairing or replacing the malfunctioned component or subsystem.

After presenting the different phases of a biometric system, we will tackle the different interactions between the user, system, organizations and authorities. For a better understanding of this process we will focus on the figure below.

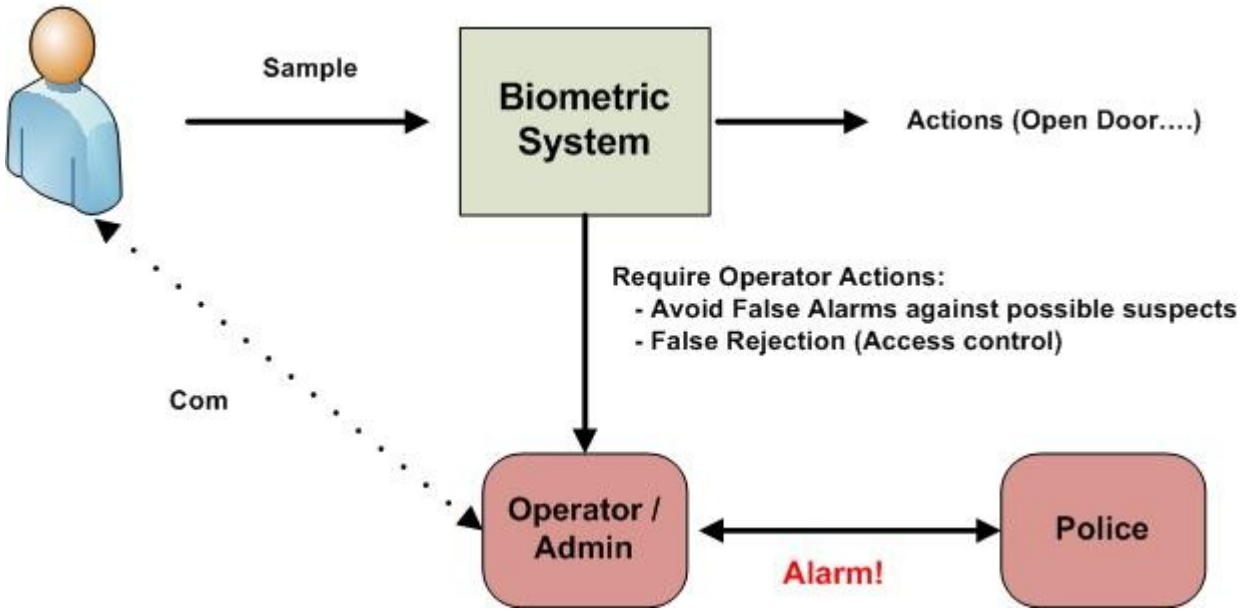

Figure 22: Generic process for biometrics

:

The biometric systems are higly dependat on the application. For this reason we have tried to make as simpler as possible. First of all the biometric characteristics of the user are captured and processed by the biometric system. As a consequence, the system can do some specific actions as opening the door in an access control, or can require some operator actions. For example if the system is in charge of detecting possible suspects. When the system detects a suspect in order to avoid a big number of false alarms, an specific operator should check the coincidence of the persons with the possible suspect.

Another example where the operator's intervention is required is when a false rejection happens in an access control. Imagine you have to pass an access control to enter to your job position and the system fails. In that case, you will probably need a direct communication with the operator to verify your identity and open you the door. Finally, the operator can do different actions such as opening the door in an access control or calling the police if the operator sees that there is a big risk.

3.2 Key features about biometric systems

Following the presentation of the general process for biometrics, we are going to present some key features about biometric systems. First of all, we are going to see the different modules involved in a typical biometric system. Then, we will classify biometrics according to their operation mode. Thirdly, the main privacy issues in biometric system will be presented. Later on, we will see how this privacy issues impact on the system design. Finally, we will present a typical end-to-end design process for a biometric system.

Now, we are going to observe the different modules involved in the generic process for a biometric system. In the following figure, we can see a graphical representation of the different modules. These modules are:

- Acquisition. The first module is the acquisition of the biometric sample which contains people's information (i.e fingerprint, images). At this stage, some specific sensor, as a camera or a fingerprint reader is responsible for collecting data. Some, but not all, biometric systems collect data at one location but store and/or process it at another. In that case, data must be transmitted through some medium such as network or video cable.
- Pre-processing. In some cases, the data collected needs to pass a pre-processing stage in order to make possible the processing of data by the main algorithm. For example, the systems which capture images as biometric sample need to make a series of operations on the image such as decompress the image in a raw format (RGB or YUV) or resize the original image.
- Feature extraction. In this module, the acquired or pre-processed biometric sample is processed to extract a set of salient or discriminatory features. For example, in the face recognition system the features extracted are related to the location and shape of the facial attributes such as the eyes, eyebrows, nose, lips and chin, and their spatial relationships.
- Template generator. The features extracted in the previous module are the inputs of the template generator. These features are used to generate the template. After that, the template created is sent to the storage or matching module depending on which phase, enrollment or matching we are.
- Storage: This module is in charge of linking, when necessary, the template with something that identifies the person and storing it in database for later comparison.
- Matching: Once the template has been generated, and as long as we are not in the enrollment phase generated, the template is compared against the stored templates to generate matching scores. Depending how the system is classified according to its mode of operation, which will be described in the following section, this module compares the current template obtained with N templates or a single template stored in the database. The result of the comparison between two templates is usually a statistic result whose value tells us the probability that both examples are equal.
- System Decision: This module receives as input the result of the matching module. According to this result, the system can, for example, allow or deny access to a restricted area, identify a suspect or generate an alarm to detect any anomalous behavior.

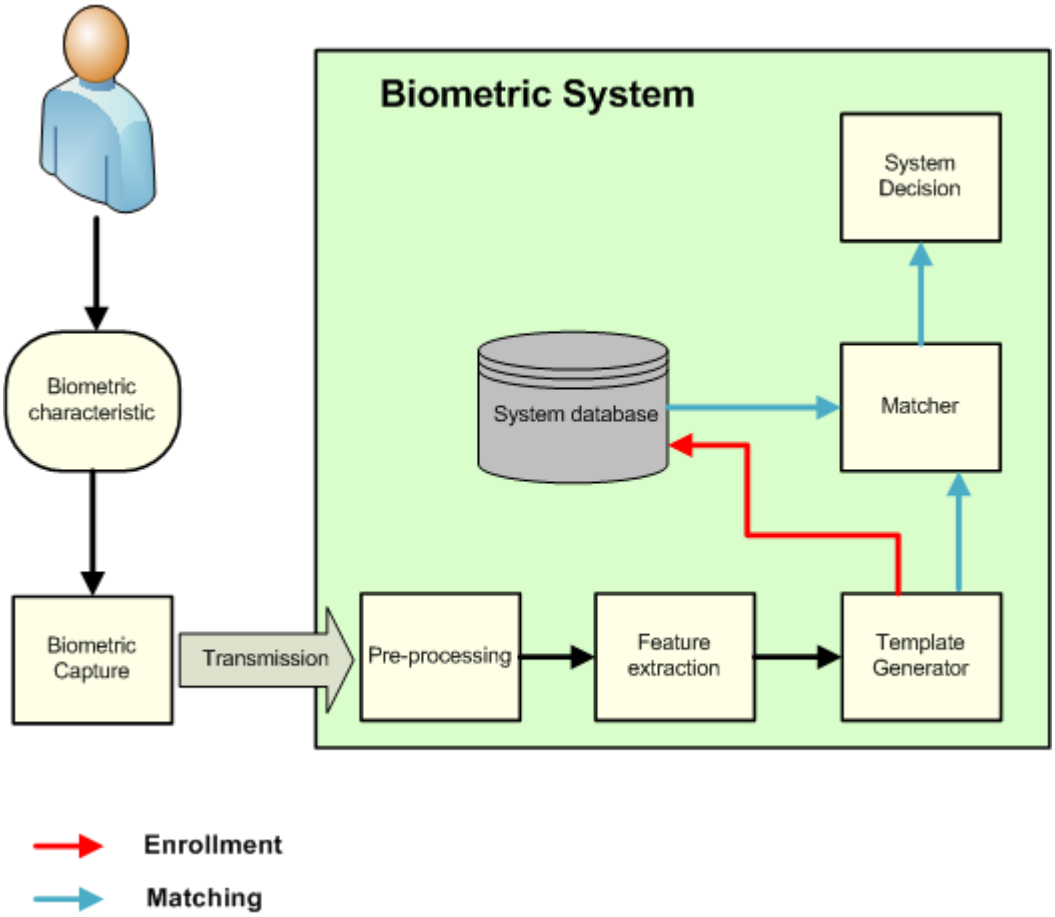

Figure 23: Architecture of a biometric system

3.2.1 Segmentation of biometric systems types

As has previously been mentioned, we are going to classify the biometric systems depending on their mode of operation. The goal of biometrics is to know whether the individual is going to be accepted or not. For that, the system has two traditional basic operations: identification and verification/authentication. In addition, due to last technological development is also possible another operation mode: categorization/segregation.

- Identification: the system attempted to detect the identity of the individual without that individual claiming a particular identity. In this case the template generated by the biometric system is compared with a portion or all the templates previously stored. This is known as a "one-to-many" comparison. The result of the matching can be the best matching score or a set of best matches. Finally, the system decision module is responsible for deciding whether the person has been identified, based on the result from the matcher result and a pre-established threshold. The decision module can also perform other actions such as generating an alarm where the person is identified as a possible suspect. In the figure 24, you can observe a graphical representation about this operation mode.
- Verification/authentication: is where the biometric system authenticates an individual's claimed identity. In this aim, the template generated by the biometric system is only compared with the corresponding enrolled template of the person. To choose the

appropriate enrolled template of the person, the system needs a credential that identifies the individual, such as a pin or password. Finally, the system decision module is responsible for deciding whether a person is who he/she claims to be, based on the result from the matcher result and a pre-established threshold. In the same way as in the identification mode, the decision module can also perform other actions such as opening the door in an access control. Figure 25 illustrates the verification mode.

- Categorization: In this operation mode, it is not important to identify or verify the identity of the person. The purpose of this mode is to know whether the biometric data belongs to a specific group or not. For example, according to whether the user is a woman or a man, the system may behave in a different way.

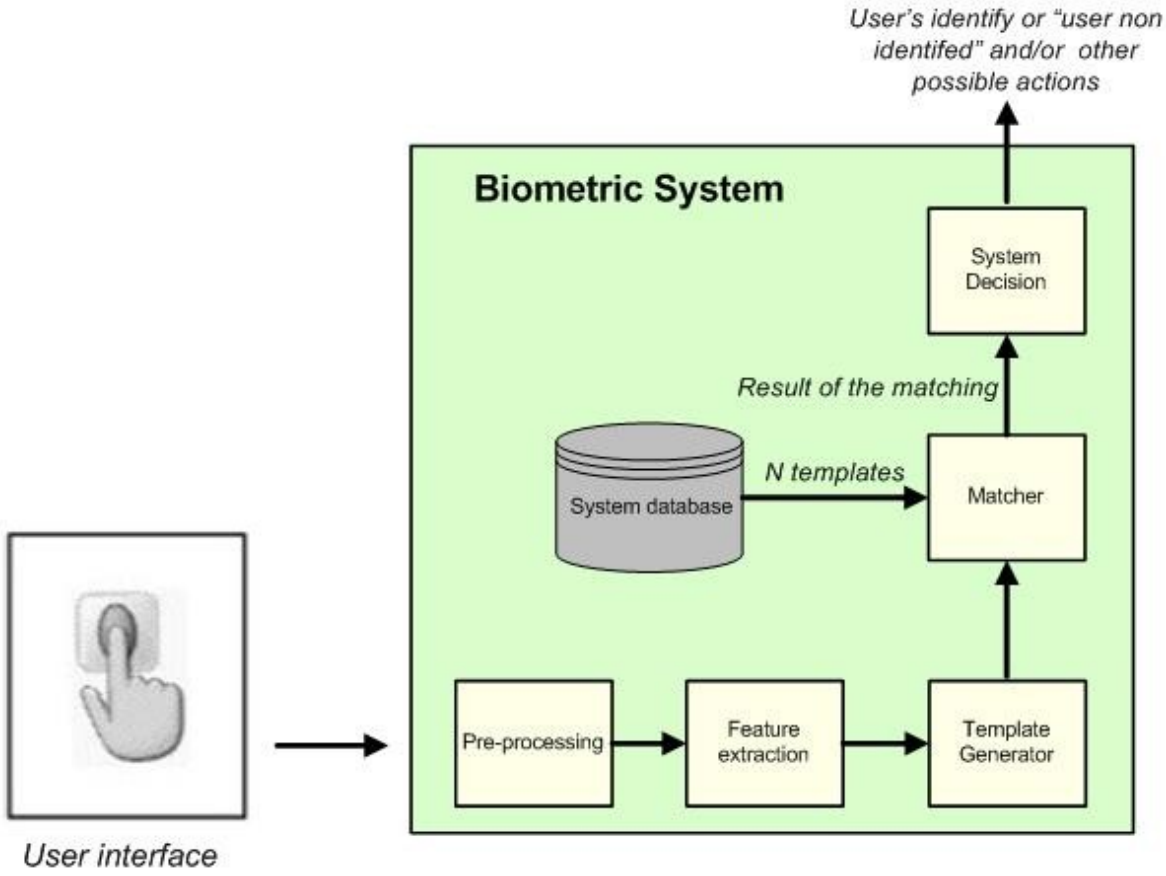

Figure 24: Identification process

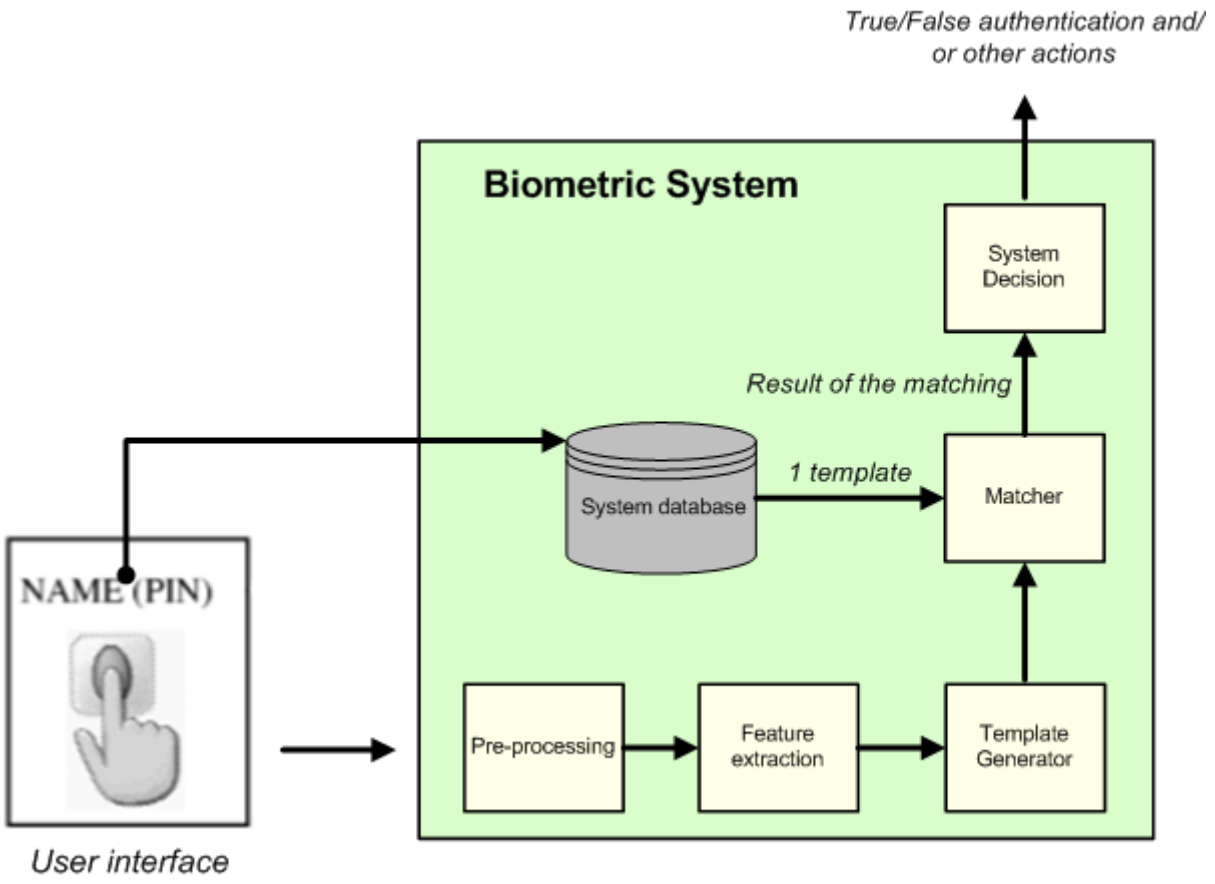

Figure 25: Verification/Authentication process

3.2.2 Main privacy issues related to biometric systems

Following the presentation of the generic process and some of the main features of biometrics, we will present in this section the main aspects of biometrics that affect or could affect individuals' privacy.

Any technology based on biometrics is traditionally seen as a threat to privacy rights of the individual. We could even say that the privacy issues are the main barrier for wider acceptance of these systems. Many people have a sense of privacy, understanding that some aspects of their lives are not a business. From a privacy point of view, biometric systems can have a **positive or negative impact on a person**.

From a **positive** point of view, biometric can be seen as privacy enhancing since they provide an accurate and rapid method of identification, verification or categorization. The traditional authentication or identification system introduces for their purpose two important factors, "something you know" and "something you have" (i.e a number pin). On the other hand, Biometric systems do not only have these characteristics, but they can also offer a more important factor "something you are". As a consequence, biometric system are more reliable, since biometric data cannot be lost, forgotten or guessed, and more user friendly since the user does not have to carry or remember something. In addition, Biometrics can provide more secure access to personal data than traditional means like PINs and passwords. Also, to ensure that personal data can be linked exclusively to the right person and therefore can only be used in the name of the right person.

From a **negative** point of view, biometrics can present a potential threat to privacy, since the personal information about a specific individual could be available to others. Here, we can

classify the privacy concerns related to biometrics in two different groups: *personal privacy and informational privacy*.

- Personal privacy has to do with fears about the erosion of personal identity and body integrity. The biometrical information tends to be unique and is very difficult to duplicate it. For that reason, biometric data could be considered as the optimum form of identification. Therefore, we can say that the body become the password. However, the information of the body could be used for the categorization of a person as legal or illegal, low or high security risks. This could damage the identity of a person. Another important point is that biometric systems are not perfect. A good example that represents this type of error is the case of Brandon Mayfield. He was arrested over two weeks in 2004 in connection with attack on some trains in Madrid. The fact that led to his arrest was that the fingerprint found, by the Spanish police and analysed by the FBI (US Federal Bureau of Investigation), in the attacks coincided with his ones. After that, Spanish authorities found out that the fingerprints actually belonged to someone else.
- Informational privacy has to do with the misuse of private data. This group is focused on the potential impact of the collection, use, retention, and disclosure of biometric data. Some of the concerns related to informational privacy are:
    - Privacy and Right to Anonymity. Many people prefer to keep their biometric data private and to only make them available according to their own terms. If the biometric data is not kept private, the different organizations could extract more information related to religious beliefs, political opinions and so on.
    - Collection of the appropriate information. The information collected should be used only for a specific purpose. For example, vein and retinal scanning can reveal medical information as hypertensions. All the information which is not needed for identification/verification purposes should be deleted from the system.
    - Rights of transparency and access. Everybody should know what, where and why the data is stored and who accesses to it. However, depending on the scenario this information could be restricted, (i.e the use of a fingerprint in a criminal investigation).
    - Function creep and interoperability. The interoperability between different organizations generates higher data exchanges, as a result the likelihood to use the biometric data for other purposes is greater. However, we must also say that the correct use of information between different systems can improve the functionality of a specific system. In addition, the different operators could do a bad use of the data that they can access. For this reason, operator must only access the information that they required to do their job.
    - Gathering information and profiling. Collecting information from different sources make possible that the person can be tracked and a profile about the persons can be created according to his/her behaviour or activities. As a consequence, the profile associated to the person could be used to categorize the person and to predict and individual's behaviour or activity.

3.2.3 Main degree of freedom within the design of a biometric system

Designing for privacy: there is a challenge for engineers who design biometric systems in order to protect the user's privacy. As previously mentioned in section 3.2.1, a biometric system can impact in a negative way user's identity.

In order to protect this personal information, we have to incorporate security features into the design of biometric systems which are based on the handling of personal information. However, this security measures can have a big impact on the design of the system.

In the following figure we can see the impact that some security measures can cause in the design of biometric systems. First of all, we are going to focus on those measures which least impact on the system design. These measures are typical and have to do with the protection of personal data. For example we can encrypt the data that the biometric system is going to store or we can establish some specific policy of access based on the different roles of people or organizations that access to the data. These measures have a low impact on the design because the data is processed in the same way and the system stores the same data.

The second group of measure has to do with the data separation. The data separation consists of separating the identity of a person from his/her biometric data by a pseudo-identity. In this way when someone without the necessary permission (i.e operator) will access the biometric data, he/she will not know the person to whom this biometric data belongs. For that purpose we need a trusted third party. A trusted third party is an independent party who is trusted by both the user and service provider. This party can be entrusted with keeping such things as the master key linking digital pseudonyms with the true identities of their users. The trusted party knows that the relationship between a user's true identity and his/her pseudo-identity must be kept completely secret. However, under some circumstances, the trusted party will be permitted to reveal the user's identity (i.e police order).

The third group is the privacy management system. These systems protect the data from an unauthorized access. The system must be able to distinguish what information should be exchanged in what circumstances to which party based on the different permission of the operators. An example of this kind of system is the Privacy incorporated Software Agent (PISA) project.

Finally, the ideal situation for all the biometric systems is not recording personal information or deleting any personal information after the process. Based on this ideal situation, every time the system captures the user data the system could not compare against other data since has not stored anything. To enable the system verify the identity of the person, the user will provide his/her enrolment data stored on a card or something similar.

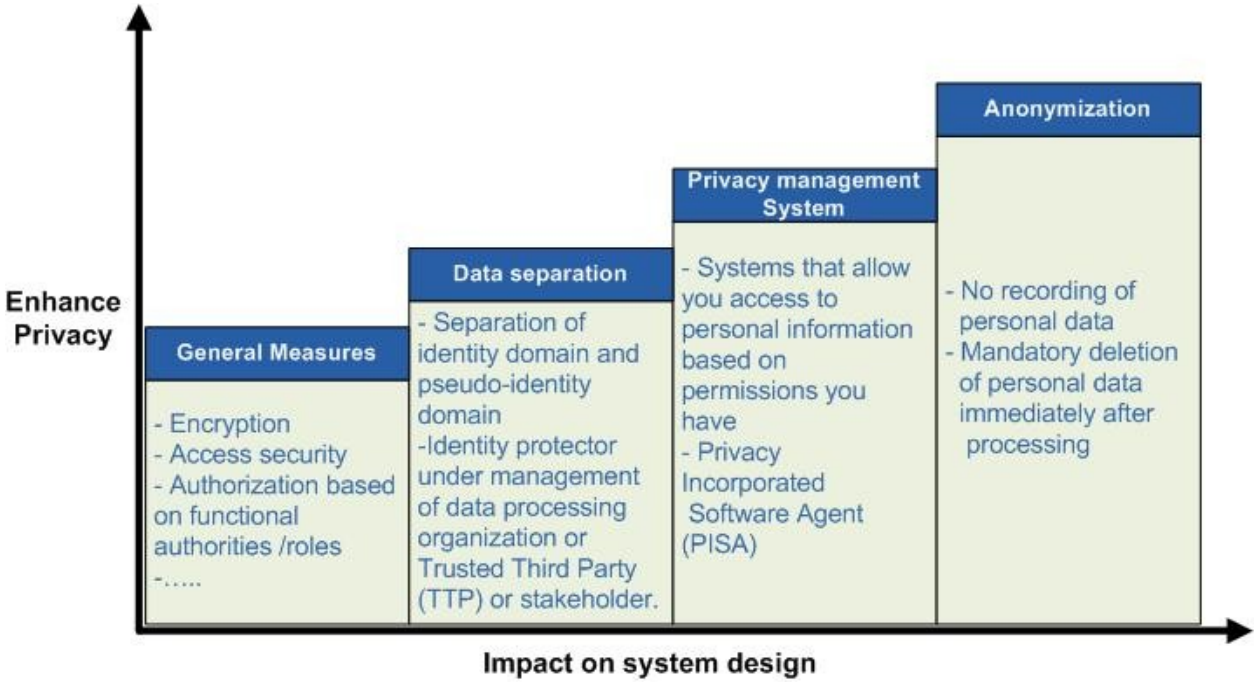

Figure 26: Privacy enhancing technology and their impacts on system design

3.2.4 Typical end-to-end design process for a biometric system

In this section, we are going to describe how the different actors of the system interact with the biometric system. Based on the information presented in section 3.1 *"Generic process for biometrics",* we can distinguish different actors: **users or citizens, operators, authorities, software designer and the system owner of the system.**

We will start with the **owner** of the system. Although the owner of the system will not have a direct interaction with the system, he/she is a critical piece because he is responsible for describing the system to the system designer. Some of the critical parts that the owner is going to define are: the purpose of the system, the space where the system will be deployed (i.e school, bank, private office, border control and so on), the level of criticality of the system (i.e low, medium, high and critical), the space that the system must covert (i.e one or several rooms etc...), the different operational procedures, if we have users with different permissions, the number of users who undergo the system (i.e Small, Medium, or Large Scale), if the system is intrusive or not, how the system reacts to a positive or negative response, if we are going to integrate the systems with others and the data which can be transferred.

Secondly, we will see how the **designer** interacts with the system. The designer has a great interaction with the systems since, he/she has to cope with a design/deployment process based on the description done by the owner. In addition, the designer can have serious difficulties regarding privacy issues, because he/she may not have the appropriate knowledge of laws, social and anthropological issues. Based on these points, the system will take a series of decisions as:

- If the system will be composed of a single or multimodal biometric.
- The kind of sensors and systems (i.e camera and face recognition).
- The mode of operation of the system (i.e identification, verification or categorization). In case that the designer would choose the verification mode, the designer specifies the extra information that the user must enter.

- The inputs and data to be stored (output). For example the input could be a video stream and the output could be a raw image or a mathematical representation.
- If there are integrations with other system, the data which is exchanged.
- The possible actions that the system could perform (i.e open a door, launch an alarm).
- Measures to protect the personal data.
- Measures to avoid the misuse of the personal data.
- Measures to guarantee the transparency.
- Other measures to ensure compliance with legal, social and anthropological aspects.

Thirdly, we are going to see how the **operators** interact with the system. The different interactions are explained below:

- The system can launch certain events to the operator. As a result the operator acts in a specific manner.
- The operator could have to interact with the user. For instance, if the user requires help to interact with the system in any of its phases: enrollment and matching.
- Depending on the permissions of the operator, he/she can access certain information. For example, if the system stores images of the user's faces when the operator tries to access some images, he/she will be able to see the faces of the user if he/she has the appropriate permissions.
- The operator is responsible for the use of personal data, because he/she could make improper use of such information. For that reason, the system may record the different actions that the operators carry out.
- An operator (i.e. administrator) can configure some specific parts of the system, as the operator permission.

Then, we are going to see how **users or citizens** interact with the system. In many cases, depending on the type of system, the user may not have knowledge that there is a system collecting their biometric data, for example a camera which uses face recognition in order to detect possible suspects. In cases where citizens have knowledge about the system, the possible interactions are:

- Citizens can be informed of the data that are being collected.
- Despite being informed, users might not have clear or sufficient knowledge of the purpose or purposes of collection of their biometric data.
- As we previously mentioned on the operator interactions the user could interact with the operators.
- Users may contact the organization to exercise their right of access, modification and deletion of the personal data relating to them.
- In many cases, the user or citizen does not know how the system or organization use his/her personal data and how they are protected.

Finally, we are going to see how **authorities** interact with the system. The interactions are:

- The operators can contact public authorities if the organization requires the authorities' presence to prevent a possible security risk.
- The authorities (i.e police) could ask the organization for some possible data in order to investigate a specific fact.

- The authorities can also ask the organization for the logs in order to know what have been the different operations performed over the personal data.

3.3 Conclusion about generic process for biometrics

Finally, we will discuss the findings for the generic process for biometric.

First of all, it is important to notice the two different phases of these systems and the different modes of operation. These phases are enrollment and matching. In the enrollment phase, the biometric data of the user is going to be stored and linked to something that identifies the person. In the matching phase, when the user is exposing to the system, his/her biometric data is compared with the previously stored data (enrollment phase). Depending on the comparison, there are three different modes of operation, Identification (1 to N comparison), Verification (1 to 1 comparison) and categorization (to know whether the user belongs to a specific group or not, we could say that it is a mix between identification and verification)

After seeing the different phases and modes of operations, we are going to focus on the deployment of the system. First of all the organization desiring to implement the system carries out a description of the system. With this description the organization in charge of the deployment must understand the level of criticality and capture the requirements of the system. These requirements must give a special attention to the functions to be accomplished by the system, system procedures as well as the flow of information, the number of users who are going to undergo the system in order to establish the system size (Small, Medium and Large Scale system), environmental conditions where the system will be deployed and how the system can impact on the privacy of the users, since we are dealing with personal information this is a very important point. After capturing the requirement, we are in a position to carry out the other phases. These phases are based on the requirements. In the design phase we will select the type of devices, create the architecture of the system and try to minimize the impact of the system on user's privacy among other things. Then, we will test the system and will make its maintenance.

From the privacy point of view, we have seen that these systems can produce positive or negative effects to the users. Positively, on account of the fact that people can feel safer. And negatively since these system can damage the identity of the users due to errors by the biometric system or misuse of data. These facts which can impact on users' privacy must be taken into account in the design phase. In this phase, we should try to protect the user's privacy as much as possible. We have seen how this kind of decision can impact on the system design. For example, if we can avoid storing whatever kind of personal data which can have a negative impact on people, the data which will be compared with the extracted biometric data in the matching phase could be provided by the own user (e.g using a card that stores his/her biometric data).

Finally, although these systems are very application dependent, we have tried to show the interaction between the system, users and organizations at general level. We have seen how the system interacts with the user and depending on the case with operators. Also, we have found that it is possible for the operator to interact with the user and the specific authorities.

4 TENTATIVE META-MODEL FOR GENERIC SURVEIL-LANCE PROCESSES

This section proposes a first version of an abstract meta-model for a generic surveillance process. This meta-model is a tool designed to help us capture the structure, properties and functionality of a surveillance system. It is neither intended to capture the knowledge of a SALT framework[1] nor to manage it. In this case, the meta-model is a high level abstraction, consisting of a set of elements and relationships, of a generic surveillance system. As we instantiate these elements, we get better approximations of the particular surveillance system we are dealing with. In this way, this meta-model becomes a great tool for the engineering process of the surveillance system, although it could also be used by the SALT framework, but that is not its main application.

This meta-model is suitable for any kind of surveillance system, but next it is refined considering video-surveillance and biometrics systems, which are the type of systems considered by the PARIS project.

4.1 Global approach for a meta-model dedicated to surveil-lance processes

Figure 27 shows the proposed meta-model for a generic surveillance system. It has been divided into four different sub-models, each one printed with a different colour for the sake of clarity. These are the considered sub-models:

- PM: Properties (sub)Model (printed in yellow).
- RM: Requirements (sub)Model (printed in pink).
- DM: Domains (sub)Model (printed in orange).
- TM: Threats (sub)Model (printed in green).

This approach will help to further modify, extend and improve the original meta-model. PARIS members with a deep knowledge of any sub-model area will be able to easily focus in the corresponding sub-model for a better improvement of the whole meta-model.

We also are going to distinguish between CPM (Core Privacy Meta-model) and DPM (Domain Privacy Meta-model). The first one is the meta-model located at the highest level of abstraction, which corresponds to the Meta-model from Figure 27. The second one refers to a first instance of the CPM, where the system domain is already known. The CPM is a language that will be used to describe the knowledge of a certain domain. The actual representation of this knowledge is the DPM. This said, let's explain the elements shown in the meta-model of Figure 27.

[1] Let us remember the definition of a SALT framework: a set of knowledges from social, anthropological, legal and technological fields, which (within the PARIS project) will help us to design, operate and use surveillance systems.

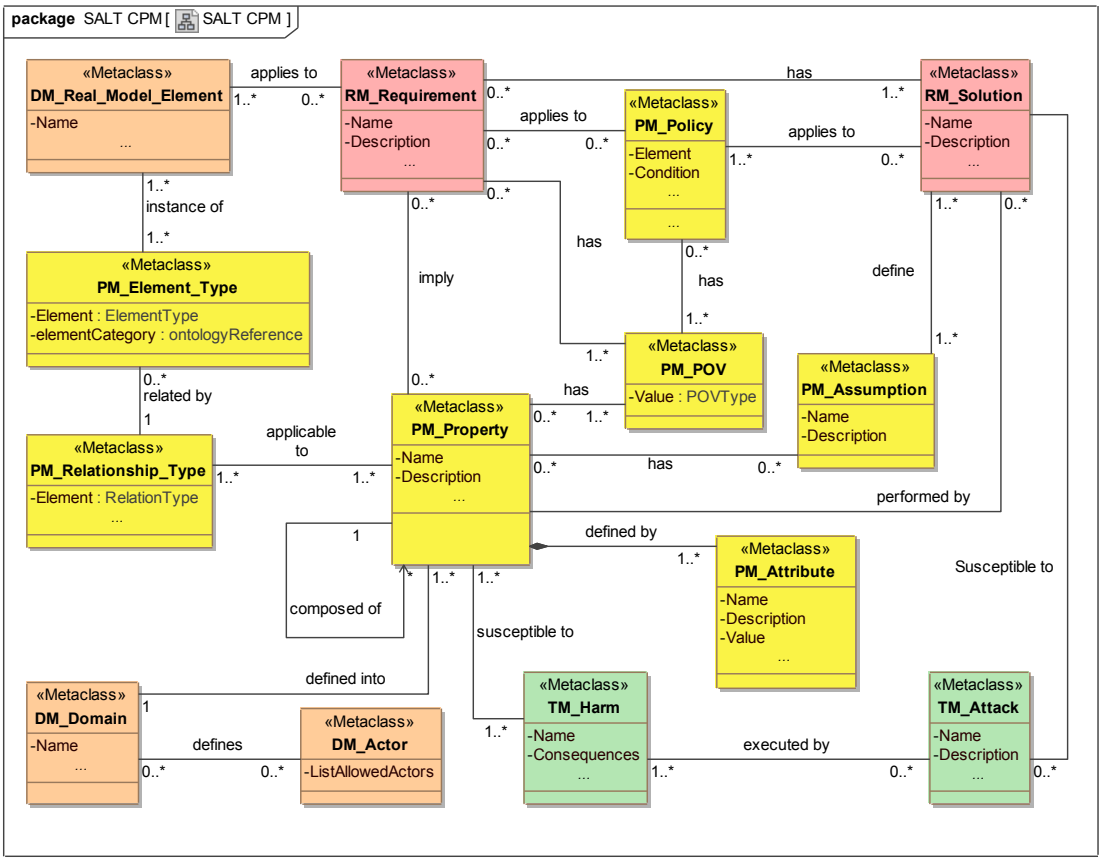

Figure 27 Generic surveillance system meta-model

Property: it defines the properties that system elements must fulfil, such as privacy or accountability. A given property can be composed of several properties. Furthermore, there can also be several sub-properties, such as anonymity, persistence (guarantee data keeping/deletion), subject recognition, etc. Each property has the following attributes:

- Name: the name of the property.
- Description: a text describing the property.

Attribute: it modifies, somehow, a given property. For example, for the privacy property the system could need: accuracy, safety, limited data collection, etc. Besides, each attribute may have different values. For example, some values for *accuracy* could be *subject tracing* or *subject identification*. Each attribute has the following attributes:

- Name: the name of the attribute.
- Description: a text describing the attribute.
- Value: the corresponding value for a given attribute.

Assumption: it defines the necessary assumptions required by a given property. For example: a user cannot come in twice unless he has exited before; concerning to privacy, we assume that cryptography is secure; if a video-camera is connected to a computer via SSL protocol, we assume data transport is secure; we assume nobody accesses the database directly, but through a control access; physical security (nobody is going to physically steal an HDD, for example); etc. An assumption has the following attributes:

- Name: the name of the assumption.
- Description: a text describing the assumption.

Element type: it refers to the type of element that a real model element can be. It has the following attributes:

- Element: it denotes the element type, which can be a class (a physical element, user data, a recorded video, etc.), operation, parameter, message, attribute, etc. As we can see, it refers to UML elements.
- Element category: it is used to specify the category of the element in real world terms. Example values of this attribute could be: *camera* (this category would include thermic cameras, IP cameras, analogical cameras, etc.), *finger-print reader*, etc. This attribute makes possible the comparison between different models.

Policy: a policy is given by a set of concerns. Concerns express a series of limitations for requirements and solutions. It has the following attributes:

- Element: it defines the type of policy, which can be *mandatory*, *desirable* or *conditional*.
- Condition: it defines under what conditions requirements and solutions can be applied to the system. This attribute is meaningful when the policy is *conditional*. It can be a set of numbers defining a range of age, a circumstance that may occur, etc.

POV: this is the point of view than can influence a property, a policy or a requirement. It has one attribute:

- Value: it defines what point of view is considered according to the PARIS project definitions. It can be *anthropological*, *social*, *legal* or *technological*.

Relationship type: it defines the relation between a property and an element type. It has one attribute:

- Element: it defines the type of relationship, which can be association, aggregation, use, etc.

Requirement: a requirement is a property applied to a particular element. A policy can affect a requirement, making it mandatory or even not appropriate for the system. Each requirement has the following attributes:

- Name: the name/identifier of the requirement.
- Description: a text describing the requirement.

Solution: it specifies a solution for a given requirement, for example: *data ciphering*, *face blurring*, etc. Due to its relation with policy, a solution can (or cannot) be adequate for a determined requirement. A solution has the following attributes:

- Name: the name of the solution.
- Description: a text describing the solution.

Domain: it describes the system domain, that is, the system type. The DPM should be known when designing the system (the designer should know the system domain). A single system can

import (use) more than one DPM. The domain expresses the knowledge that refers to the system under development. It has one only attribute:

- Name: the name of the domain: video-surveillance, access control, biometrics, etc. Several domains can also be mixed.

Actor: this artefact defines the list of users/roles who can interact with the system according to its domain. It has one attribute:

- List of allowed actors: these are the actors for the system domain defined by the DPM, for example: a cashier, a security guard, a monitor operator, etc. They can have a correspondence with PARIS defined actors: *SALT expert*, *owner*, *designer*, *operator*, *citizen* and *public authority*.

Real model element: it refers to a real element from the final architecture (system) that will be deployed in a given scenario. Physical elements are included here, such as *database system*, but operations can also be considered as real elements, such as *write data into storage system*, for example. It has one attribute:

- Name: the name of the element.

Harm: it specifies a system's harm. It has the following attributes:

- Name: the name of the harm: *disclosure*, *exposure*, *confidentiality breach*, etc.
- Consequences: a text describing the consequences of the harm: it may affect a single individual or to a bigger group of people, for example.

Attack: it defines the attack that leads to a system's harm. Each attack has the following attributes:

- Name: the name of the attack, such as *database hack*, *equipment malfunction*, *information publication*, etc.
- Description: a text describing the attack.

Now that we know the meaning of each artefact within the proposed general meta-model, let's see how they are related. The main part of the meta-model is the *property*, which refers to the properties applicable to the elements of the system. It is worth to notice that a property can be composed of several properties. Besides, each property may be somehow modified by one or more attributes.

The *element-type* artefact refers to UML element types. Therefore, when a property applies to an element type, it does it through a relationship type that also takes into account all possible UML relationships. Furthermore, each real model element can be categorized within the different element types.

The meta-model includes an artefact for requirements, which are properties applied to a real model element. The way a requirement affects a real element is given by a policy. The policy will determine whether a requirement is mandatory, desirable or if it has to be applied under some conditions. We also should notice that following the PARIS project' definitions, policies,

properties and requirements can be seen from different points of views (POVs): social, anthropological, legal and technological.

A system' requirement can be satisfied by one or more solutions, but solutions are affected by policies in the same way as requirements are. Therefore, we could have the case of having a solution for a particular requirement that cannot be used because of a policy prohibition. This circumstance would force us to search for another different solution. The set of solutions implemented by the system will provide the required properties.

The proposed meta-model also considers that each property may (or may not) require some assumptions in order to exist. These assumptions will define the solutions adopted by the system. In summary, a solution will satisfy a requirement according to a policy and following a set of assumptions.

Each property belongs to a domain (each domain may have several properties). The type of surveillance system we want to design and deploy will determine the system domain. Depending on the domain we are working with, the system will be used by a set of actors or another. These actors may have a correspondence with those described by the PARIS consortium: *SALT expert*, *owner*, *designer*, *operator*, *citizen* and *public authority*.

Finally, a property may be susceptible to different harms. These harms are the consequence of attacks derived from the solutions adopted by the system.

4.2 Application to PARIS project case-studies

The next subsections propose a DPM (Domain Privacy Model) for each of the case-studies considered within the PARIS project.

4.2.1 Example DPM for video-surveillance systems

According to the video-surveillance process description from Section 2 and following the CPM depicted in Figure 27, a tentative DPM for video-surveillance systems is proposed. Due to the length of a single diagram, this DPM has been divided into two diagrams, looking for a better clarity of the concepts displayed in it. Figure 28 and Figure 29 show the obtained result.

The DPM describes a generic video-surveillance process, independently of the final system deployed. However, if we also know the system related specifications, such as *real elements* and *system requirements*, we can provide a richer diagram that also instantiates these elements from the CPM. It is important to notice that such diagrams are system-dependent, hence they stay at a lower abstraction level in relation to the DPM.

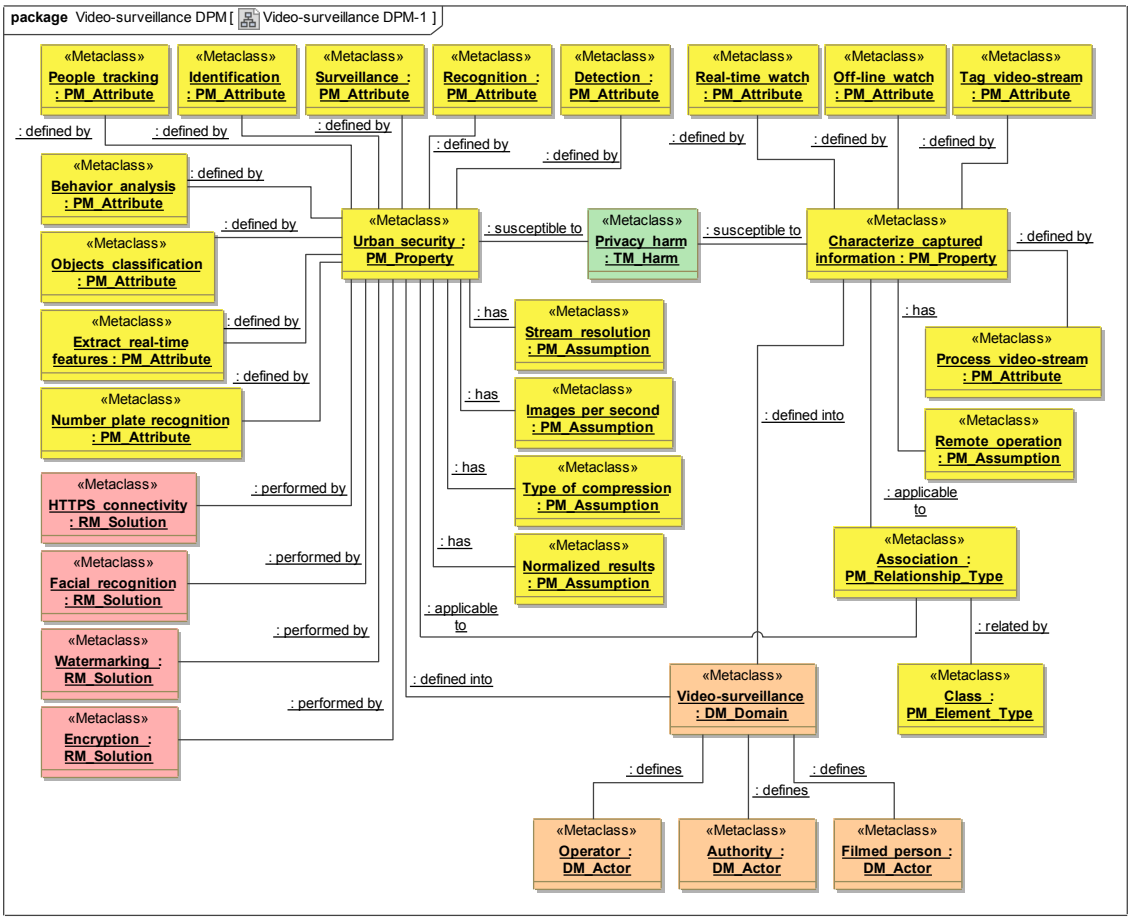

Figure 28. Video-surveillance DPM (part 1)

Taking into account the information from Section 2, we can instantiate some *real model elements* of a video-surveillance system, and hence we are also able to provide a system definition following the CPM from Figure 27. Once again, for the sake of clarity, the system has been described using four diagrams instead of just one. They are shown in Figure 30, Figure 31, Figure 32, and Figure 33.

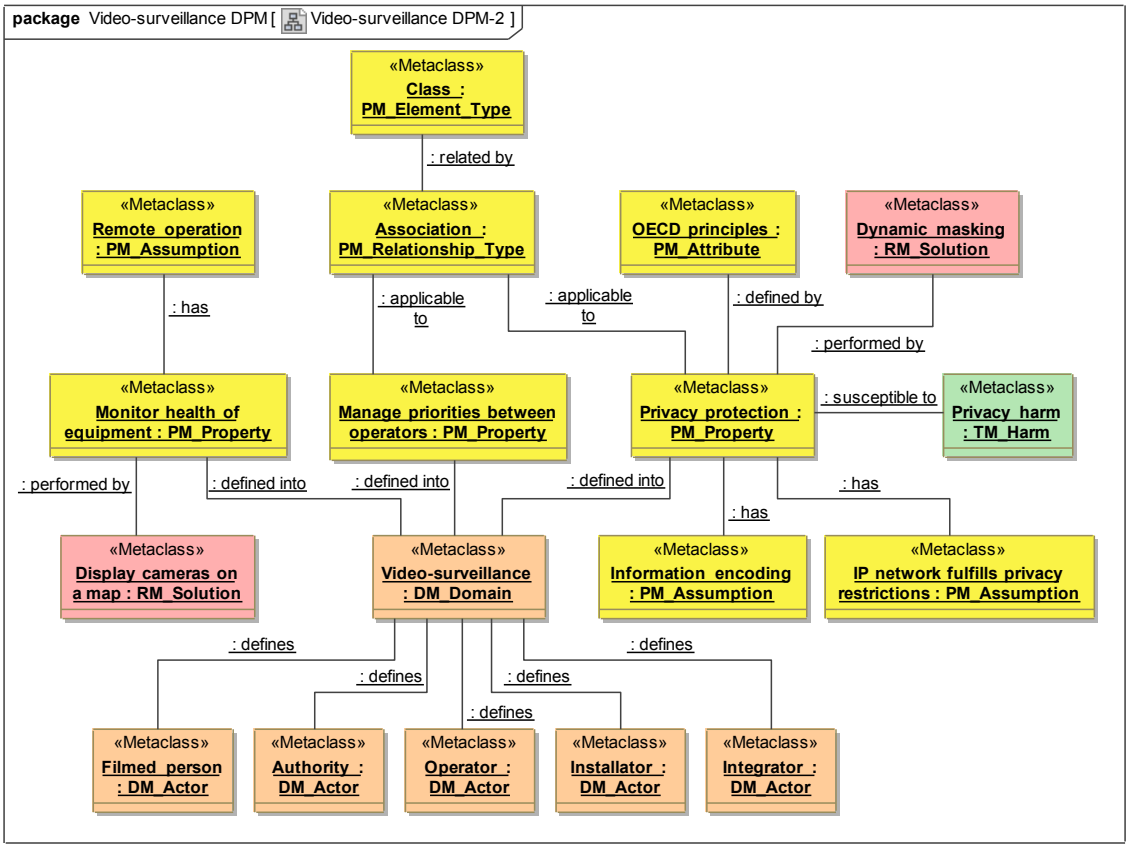

Figure 29. Video-surveillance DPM (part 2)

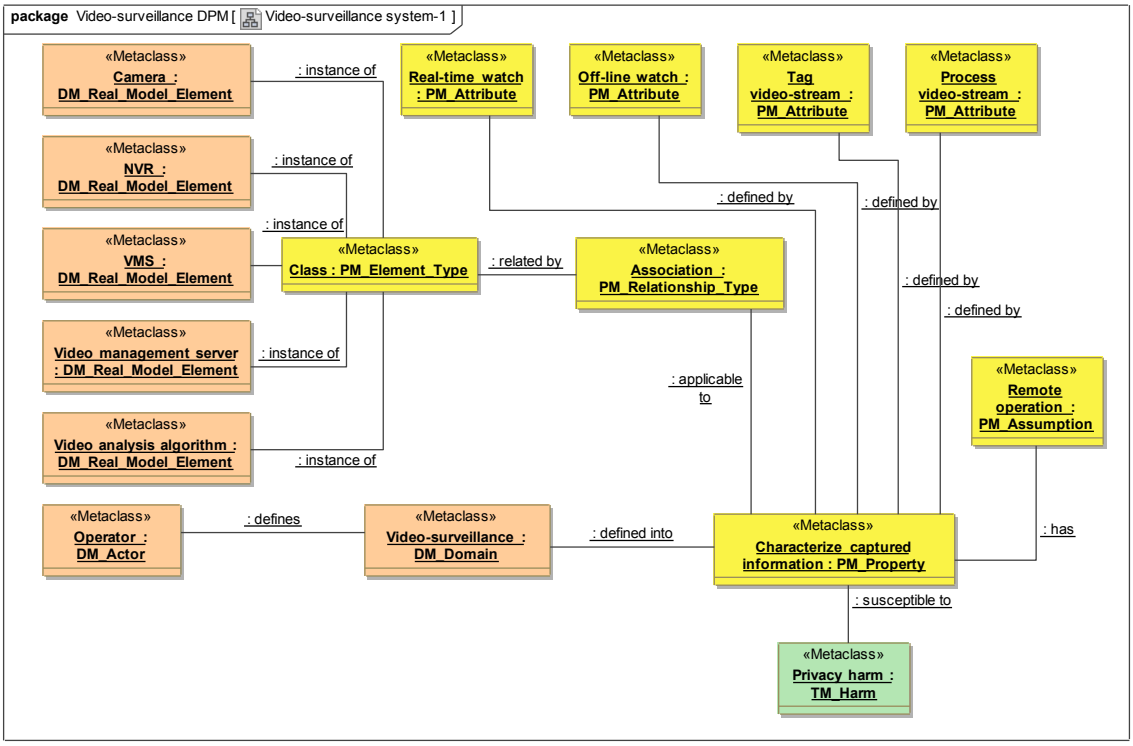

Figure 30. Video-surveillance system (part 1)

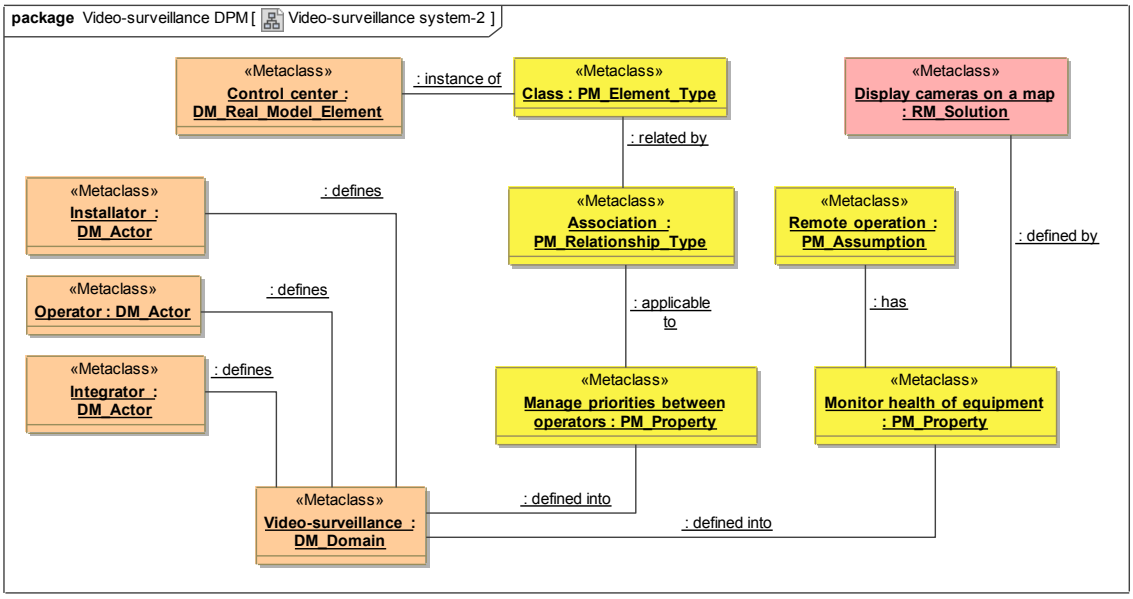

Figure 31. Video-surveillance system (part 2)

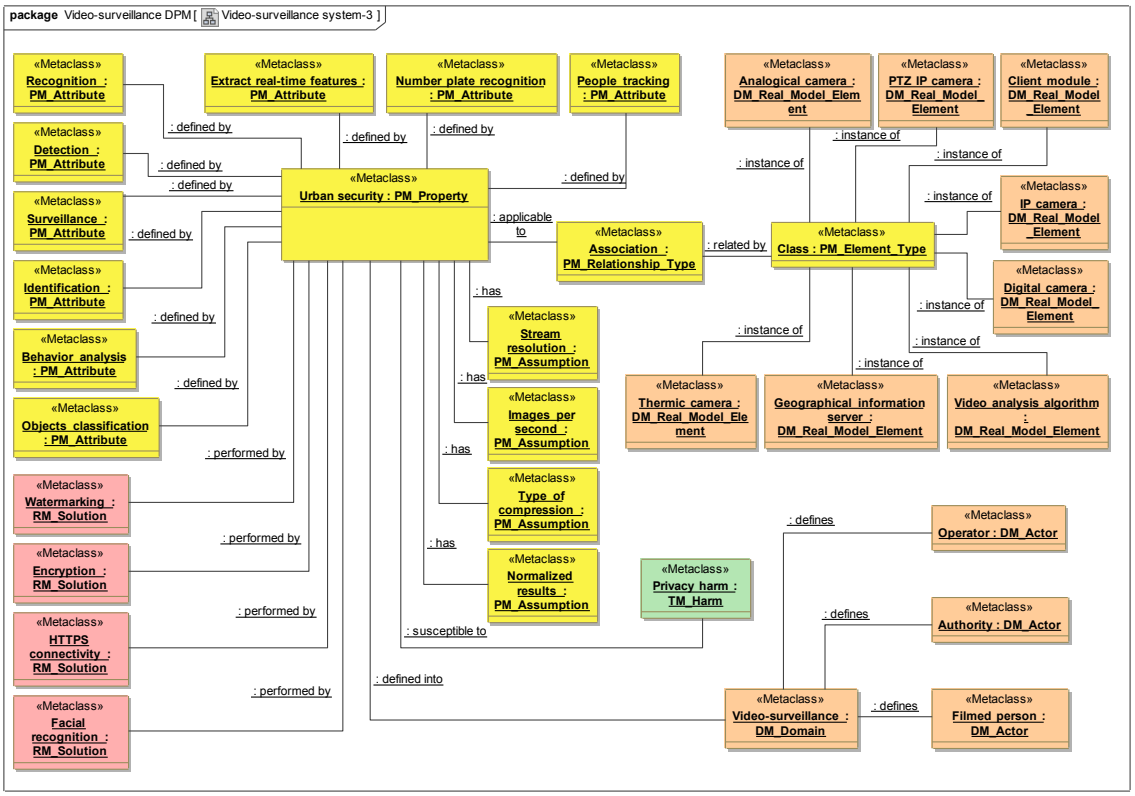

Figure 32. Video-surveillance system (part 3)

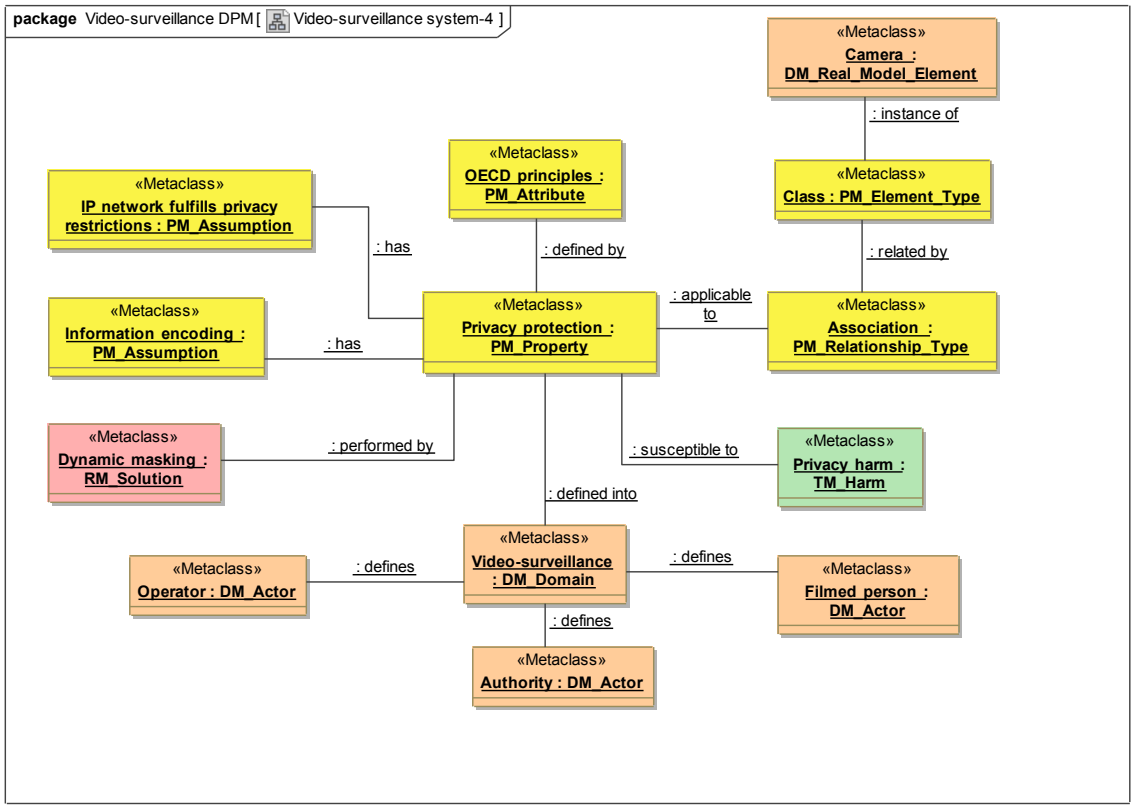

Figure 33. Video-surveillance system (part 4)

4.2.2 Example DPM for biometrics systems

Analogously to the methodology followed in Section 4.2.1, here we create another DPM, but in this case focused to biometrics systems. According to the description of a generic process for biometrics systems from Section 3 and the CPM from Figure 27, we derive the DPM depicted in Figure 34 and Figure 35 (two diagrams again for the sake of clarity).

Taking into account the information specific to biometrics systems from Section 3, we instantiate some *real model elements* from the CPM, obtaining in this way a couple of diagrams that describe a biometrics system (not the process itself, that is the DPM mission). We can observe the result in Figure 36 and Figure 37.

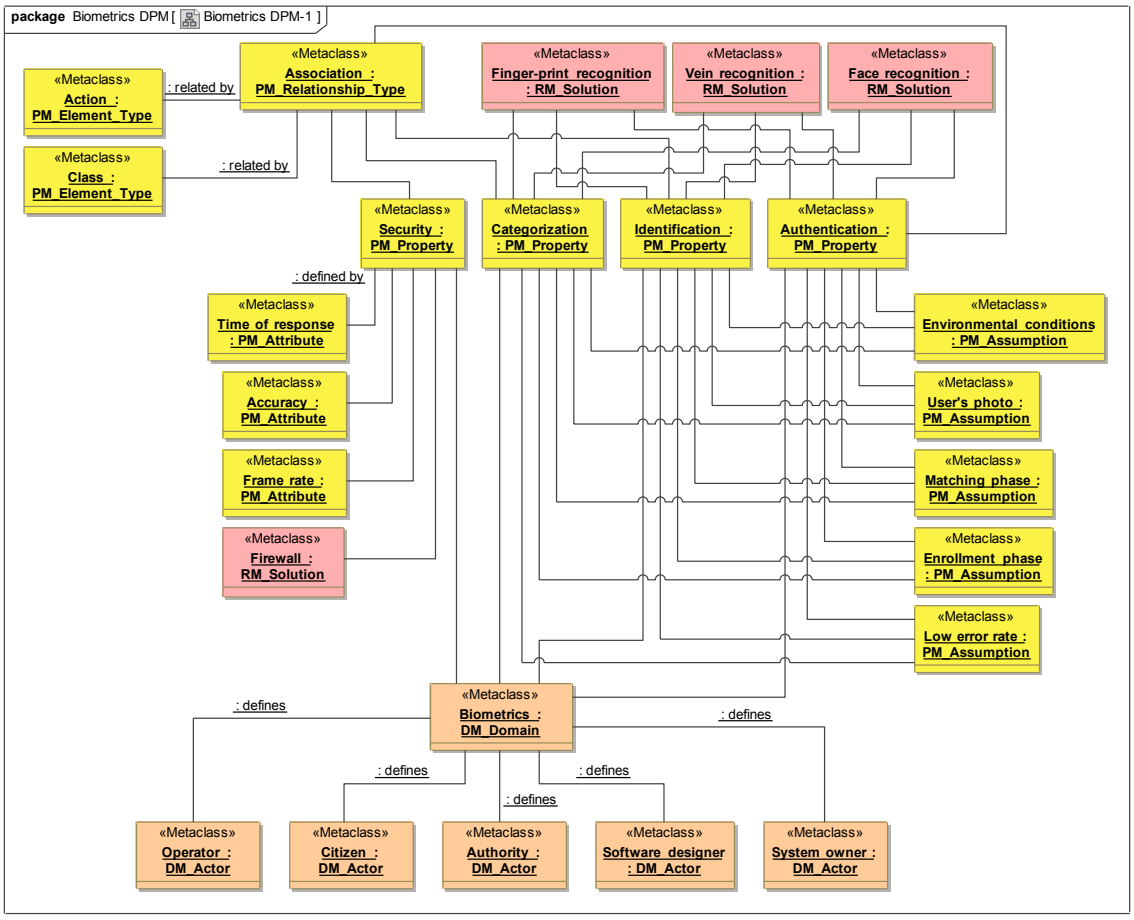

Figure 34. Biometrics DPM (part 1)

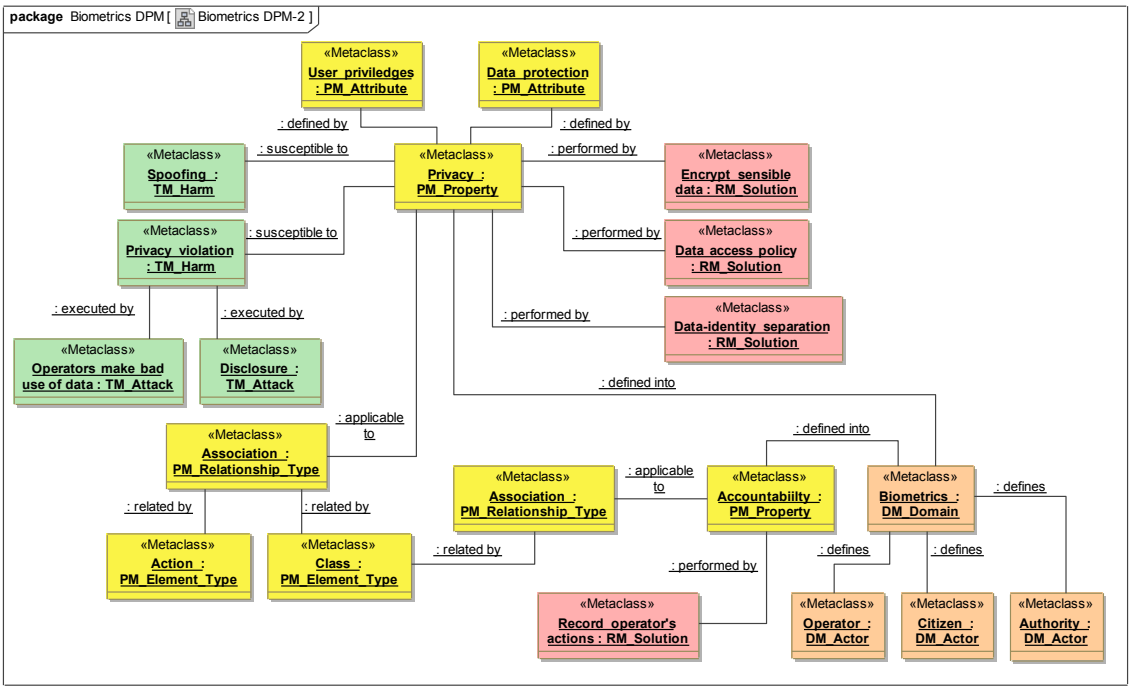

Figure 35. Biometrics DPM (part 2)

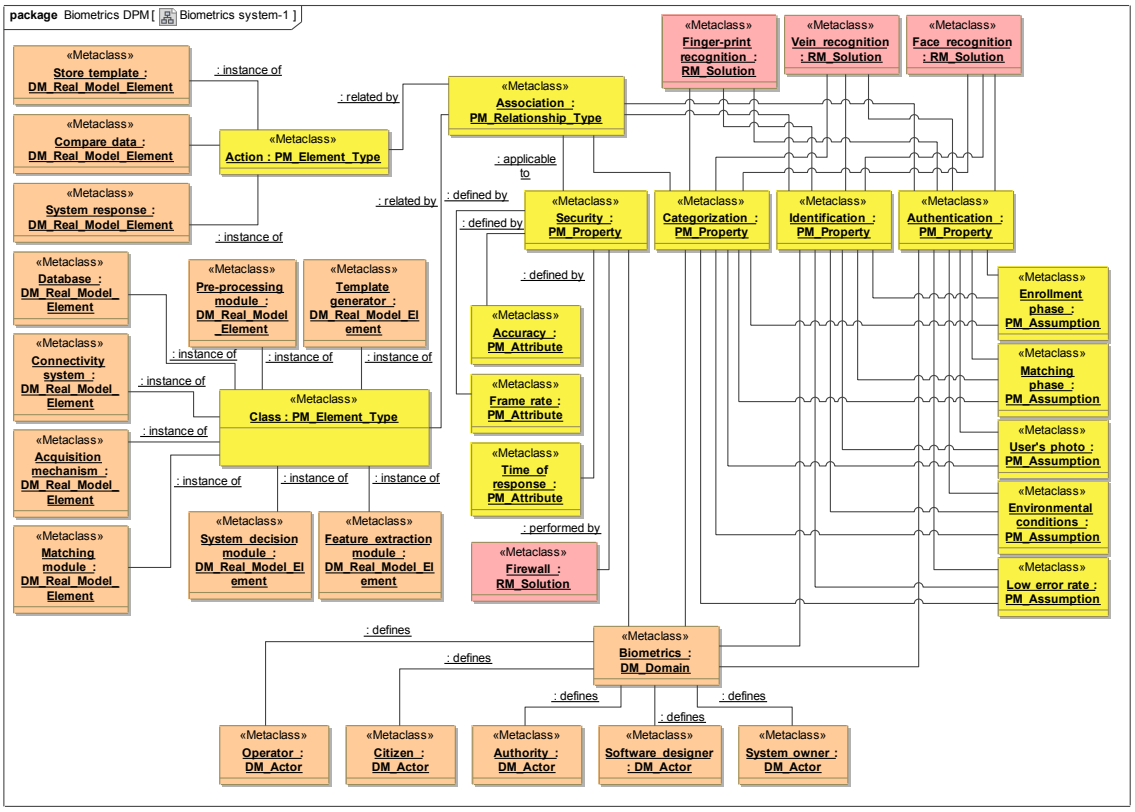

Figure 36. Biometrics system (part 1)

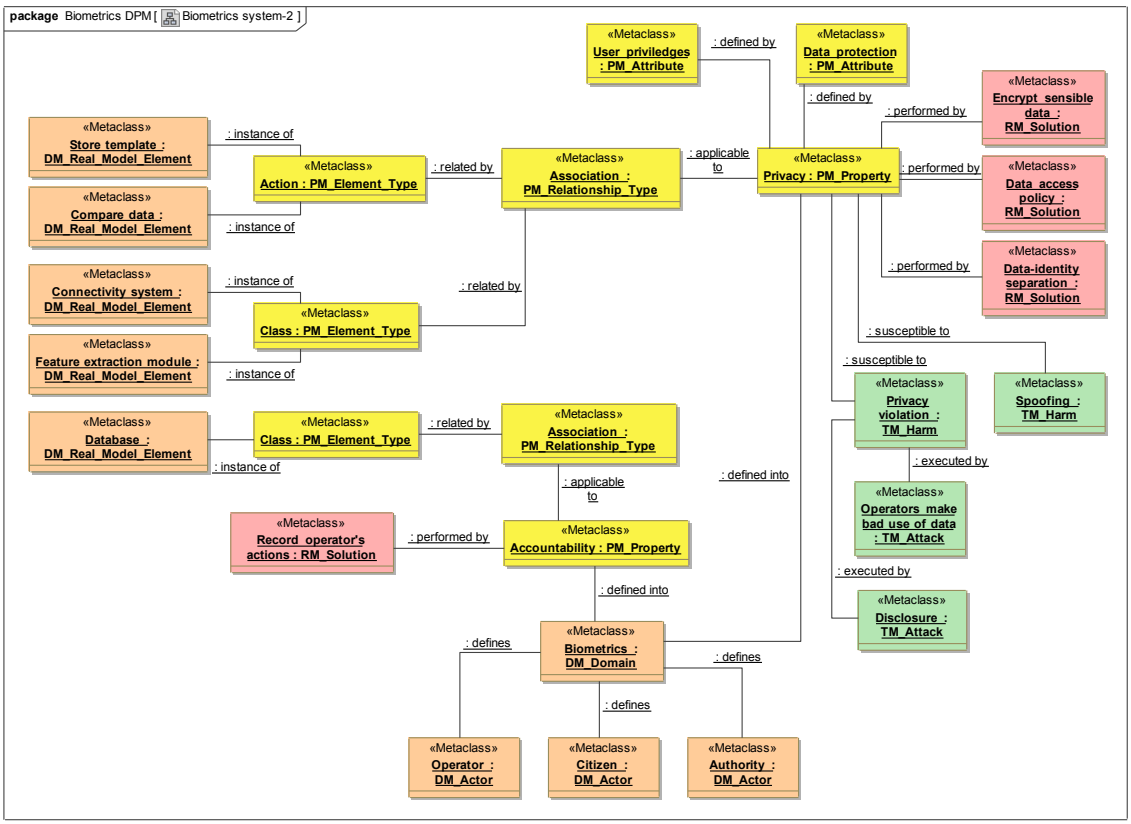

Figure 37. Biometrics system (part 2)

5 References

*[The content is indicative and subject to change through the writing process of this deliverable.]

[A] EDPS Video-Surveillance Guidelines, 2010
http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Guidelines/10-03-17_Video-surveillance_Guidelines_EN.pdf

[B] IMS research study on video-Surveillance, 2010

[C] Video Surveillance Portfolio overview, SIEMENS 2010

[D] PARIS FP7 Project Deliverable D2.1 "SALT Framework guidelines"

[E] Milestone Systems XProtect Video Management Software (VMS)
Product Comparison Chart March 30, 2012

[F] Security Recommendations for video-surveillance systems. SGDSN (National Security and Defense General Directorate), French Prime Minister Office, n°524/ANSSI/SDE, 14th of February 2013.

[G] ISO/IEC 29100:2011(E) standard: Information technology, security techniques, privacy framework

[H] ISO/IEC 24760-1:2011(E) standard: Information technology, security techniques, a framework for identity management

[I] OECD Guidelines governing the protection of privacy and tranborder flows of personal data, chapter 1, Recommandations of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data [C(80)58/FINAL, asmaended on 11 July 2013 by C(2013)79]

6 Annex 1: Video surveillance taxonomy

This section describes video surveillance taxonomy based on its functional blocks that is relevant to the PARIS project. The main difference with the taxonomy presented in [D] (PARIS project D2.1 deliverable "SALT Framework Guidelines") is that this is focused on the functional blocks from a viewpoint of architecture and the taxonomy presented in [D] is a higher-level taxonomy where we can see the access rights to information, who can access to such information and the relationships between the organization that deploys the system, users and authorities The purpose of the taxonomy is to give an overview of the concepts, definitions, and terminologies related to video surveillance, as well as the classification and relations among them. Note that the taxonomy will be continuously updated to reflect the progress of work in the PARIS project.

6.1 Taxonomy related to video surveillance system

To illustrate how different modules and components are working together that forms a video surveillance system, we define a reference video surveillance system architecture shown in . The architecture and its functional blocks in the figure are intended to give a generalized view of state-of-the-art video surveillance production systems. Systems in actual deployment might implement some or all of the functions in different ways, depending on actual requirements and budget.

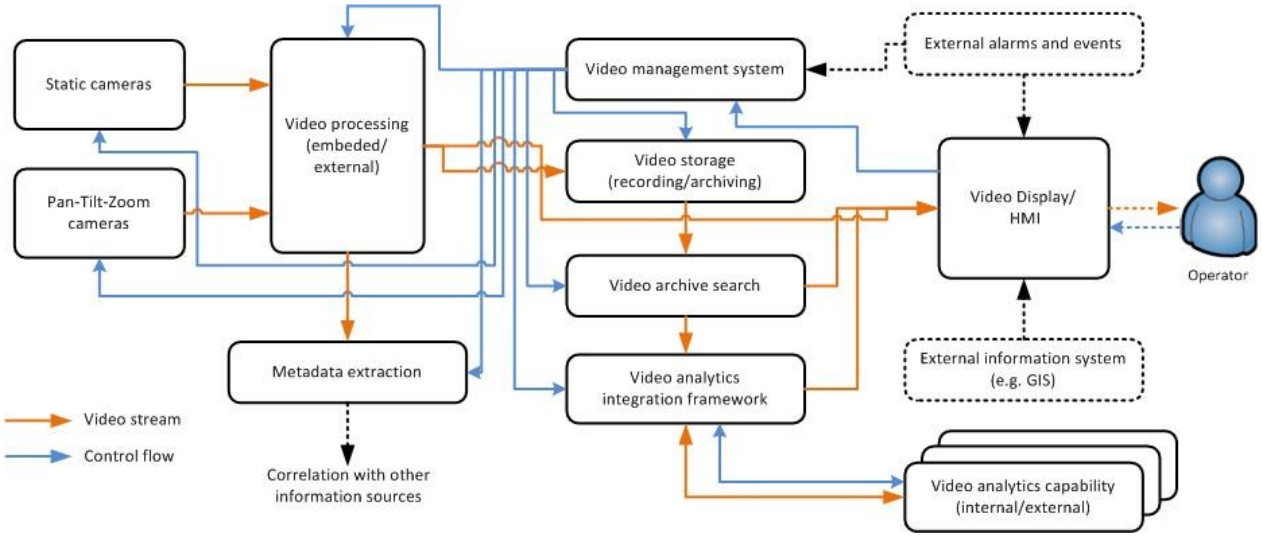

Figure 38 A reference architecture of video surveillance system

Our reference architecture shows three important privacy-related aspects of a video surveillance system:

- the functional blocks related to video capturing, processing, and storing;
- the video flows among the functional blocks;
- the command & control flows in the system.

The following is a short description of the entities in the reference architecture.

Static and Pan-Tilt-Zoom (PTZ) cameras. Cameras are devices that translate light into video streams and transmit those images to a monitor for viewing. It contains the image sensor and other electronic circuitry to create a video signal[2]. The difference between a static and a PTZ

[2] Video Surveillance CCTV Glossary Terms http://www.usscctv.com/surveillanceandsecurityglossary.aspx

camera is that a PTZ camera can be remotely controlled to provide both vertical and horizontal movement with zoom[3], while a static camera does not have movable mechanical base.

Video processing. Video processing technologies are widely used in smart video surveillance systems for processing or analysis of video data, for example, for moving object detection, region localization, object classification, object identification, tracking, human motion analysis, and activity understanding[4]. The video processing capabilities can be either embedded into cameras (smart cameras) or located within dedicated servers outside the cameras to reduce camera costs and increase video processing power.

Metadata extraction. Non-video data can be extracted or derived from video streams, which can be used to correlate with other data sources. The extracted data are no more video data. Instead, they are metadata that describe or characterize the video data. For example, a customer's biometrics can be extracted from video images taken from the camera at an ATM and used to correlate with his or her transaction on the ATM. The video metadatas can also be fed from external sources (PTZ absolute position, camera position..)

Video management system. Video management system (VMS) usually refers to control software used to manage various components of video system. Although management functions can be implemented in different places in the system, we use a central functional block to represent the controlling of the system.

Video storage. Video storage is the software, hardware, and digital media to record and store video data. We distinguish between short term storage by "recording" and long term storage by "archiving". Video storage can range from large scale data centers and servers to tapes or DVDs.

Video archive search. Video archive search allows a user to search across the entire video library (or archive) for useful video information of a specific event. In the search, different search criteria can be defined using description languages, avatar or example images. These descriptions are translated to a mathematical representation of the investigated events (e.g., models, histograms etc.). The representations are afterwards compared with the video images from the archive. This results in a value, which gives a measure for the probability of the similarity between the described event and the image data in the video archive. In an interactive process tailoring the search space, the operator can quickly restrict and focus the search with respect to the search period and camera location. The results can be presented using a ranked image list of candidate matches.

Video analytics integration framework/Video analytics capability. Video analytics refer to software based video tools used to make determinations based on the changing video content of a camera, e.g., car tacking, motion exception, missing/found object, people count etc.[5]. Indeed, this definition is very similar to video processing defined before. However, in our reference architecture, we distinguish these two functions. We use video analytics to refer to video processing on stored video data at the backend system. The video analytics integration framework provides an interface for running internal or external third-party video processing software and services on video data captured in the system. As a upcoming trend to video analytics as a service, third party service providers may in the future provide video processing

[3] Glossary of CCTV Terms – An Infinova White Paper

[4] Sedky, M.H.; Moniri, M.; Chibelushi, C.C., "Classification of smart video surveillance systems for commercial applications," Advanced Video and Signal Based Surveillance, 2005. AVSS 2005. IEEE Conference on , vol., no., pp.638,643, 15-16 Sept. 2005

[5] Above **Erreur ! Signet non défini.**

capability by leveraging on Cloud computing infrastructures for elastic, on-demand, and pay-per-use video analytics needs.

Video display/HMI. The video display shows unprocessed or processed video streams on monitors in front of the operators. The video display might also integrate additional data source such as the **External alarms and events** signals and other data from **External information source** such as map data to increase the operators' situation awareness and help them focus on relevant events on the screens. The HMI part is the interface for an operator to monitor and control the video surveillance system.

The directed **orange lines** indicate the video data flow and the **blue lines** indicate the control flow from the operator. In the reference architecture, the data flow shows how the video is transmitted, processed, and viewed in the system. The control flow shows how the functional blocks in the system are controlled by the video management system and the operator. The information provides insights on how and where privacy can be achieved at the system level.

7 Annex 2: Model-driven engineering

Model Driven Engineering (MDE) focuses on the creation of different models (usually depicted in the form of diagrams) related to a determined field of engineering. Its main objective is to achieve a high level of abstraction of a given system: a software program, an industrial factory, an electronic platform, etc. Regarding to PARIS project, MDE is particularly applied to surveillance systems: video-surveillance and biometrics systems. Another important MDE objective is to increase automation in systems development.

The underlying functionality of MDE lies in the use of models at different levels of abstraction for developing systems. An increased automation of the system development is reached by means of also automating the models transformations. In this way, higher-level models are transformed into lower level models, until we get a particular transformation that accurately resembles the desired system. Usually, model transformation takes one or more source models as input and produces one or more target models as output, following a set of transformation rules. Therefore, in MDE, models are used not just as simple diagrams, but as a mechanism to provide systems implementations through the application of transformations.

According to the OMG (Object Management Group), there are four different levels of abstraction:

1. The M3-level or meta-meta-model: it formalizes the notion of concepts and defines a language for specifying meta-models. Examples of this level are MOF (Meta-Object Facility) and EMOF (Eclipse Meta-Object Facility). To avoid a succession of layers, this level is sufficient to define itself.
2. The M2-level or meta-model: it is an instance of the previous M3-level. It formalizes paradigm concepts and defines a language for specifying models. A meta-model is a formal specification of an abstraction, usually consensual and normative. The meta-model provides the concepts and relations that will be used to filter the relevant entities of a given system in order to extract the model.
3. The M1-level or model: it is an instance of the M2-level and defines a language to describe an information domain.
4. The M0-level or user model: it is an instance of the previous level representing the real system.

According to this definition, the diagrams depicted in Section4ave the following correspondence:

- M2-level:Figure 27.
- M1-level: Figure 28, Figure 29, Figure 34 and Figure 35.
- M0-level: Figure 30, Figure 31, Figure 32, Figure 33, Figure 36 and Figure 37.