PrivAcy pReserving Infrastructure for Surveillance

Deliverable D5.4
Video Surveillance Lifecycle Management Use Case Evaluation

Project:	PARIS
Project Number:	SEC-312504
Deliverable:	D5.4
Title:	Video Surveillance Lifecycle Management Use Case Evaluation
Version:	v1.1
Date:	23/06/2016
Confidentiality:	Public
Contributors:	Z. Ma, S. Veigl, D. Hovie (AIT) M. Bossuet (THALES), F. Jaime (UMA) F. Coudert (KUL), R. Alonso (VT)

Funded by the European Union's Seventh Framework Programme

Table of Contents

DOCUMENT HISTORY **3**

LIST OF FIGURES **3**

ABBREVIATIONS AND DEFINITIONS **4**

EXECUTIVE SUMMARY **4**

1. INTRODUCTION **5**

2. DESCRIPTION OF VIDEO SURVEILLANCE MANAGEMENT USE CASE AND SALT FRAMEWORK **7**

2.1 USE CASE DESCRIPTION **7**

2.1.1 Technical requirement influenced by SALT framework 9

2.1.2 Use case scenario 10

2.2 SALT FRAMEWORK AND SALT GLOBAL PROCESS **14**

2.2.1 SALT framework 14

2.2.2 SALT compliant process 15

3. EVALUATION OF VIDEO SURVEILLANCE LIFECYCLE MANAGEMENT USE CASE 17

3.1 EVALUATION APPROACH AND METHOD **17**

3.2 EVALUATION AT THE SALT FRAMEWORK LEVEL **17**

3.2.1 SALT taxonomy aspect 20

3.2.2 SALT questionnaire aspect 21

3.2.3 SALT references aspect 24

3.2.4 SALT validation tool aspect 27

3.2.5 Functional aspect 30

3.2.6 Usability aspect 32

3.3 EVALUATION AT SYSTEM LEVEL **37**

3.3.1 Lessons learned regarding legal, Social-ethical, privacy & accountability aspect 37

3.3.2 Technical aspect 39

3.3.3 Evaluation of design process 45

3.4 SALT FRAMEWORK ADDED VALUE **46**

4. RECOMMENDATIONS FOR EXTENSION **48**

5 CONCLUSION **50**

REFERENCES **51**

APPENDIX COMPARISON OF FUNCTIONALITIES AND KPIS OF EXISTING SYSTEMS WITH PARIS' SYSTEM **52**

Document History

Version	Status	Date
v0.1	First draft of ToC	08/10/2015
v0.2	Improvement of ToC and evaluation methodology	20/10/2015
v0.3	Integrate contribution from UMA	13/11/2015
v0.4	Integrated contribution from THALES, KUL	09/12/2015
v0.5	Integrate rest contributions, edition and read for review	14/12/2015
V1.0	Integrate reviews, finalisation	21/12/2015
V1.1	Add appendix for comparing the functionalities and KPIs of existing commercial systems and PARIS's system	21/06/2016

Approval		
	Name	**Date**
Prepared	Z. Ma (editor)	21/06/2016
Reviewed	C. Jouvray, M. Bossuet, R. Alonso	22/06/2016
Authorised	Z. Ma	22/06/2016

Circulation	
Recipient	**Date of submission**
Project partners	21/06/2016
European Commission	24/06/2016

List of Figures

Figure 1: WP5 use case architecture 8
Figure 2: WP5 use case component overview 10
Figure 3: Creating a new investigation 11
Figure 4: Editing permissions 11
Figure 5: Timeline of motion in surveillance video (marked blocks indicate the timeslots where motion was detected) 12
Figure 6: approving the investigation 12
Figure 7: Overview of the permissions of the new investigation 13
Figure 8: snapshots of detected motion in videos (sample images are taken from iLIDS video footage) 13
Figure 9: Signed video export feature of the NVR 14
Figure 10: Stages of the SALT compliant process 15
Figure 11: SALT compliant process and user types 16
Figure 12: Process refinement for WP5 use case 19
Figure 13: Example taxonomy presentation within SALT tools 20
Figure 14: example edition screen dedicated to taxonomies 21
Figure 15: example screen dedicated to questionnaire edition 23
Figure 16: example edition screen dedicated to questionnaire edition 23
Figure 17: Example SALT reference contents 26
Figure 18: Example SALT reference edition 26

Figure 19: System architecture before taking into account PARIS video surveillance model 28
Figure 20: PASIR WP5 video surveillance use case system model 28
Figure 21: WP5 system model taking into account PARIS video surveillance model artefacts 29
Figure 22: overview of SALT tools within their ecosystem 30
Figure 23: SALT knowledge input by expert 35
Figure 24: Web form for SALT reference in online SALT repository 35
Figure 25: Basic search in SALT repository 36
Figure 26: Advanced search in SALT repository 36

Abbreviations and Definitions

Abbreviation	Definition
BoK	Body of Knowledge
ICT	Information and Communication Technologies
IVT	Integration, Validation and Tests
OCL	Object Constraint Language
PARIS	PrivAcy pReserving Infrastructure for Surveillance
PbD	Privacy by Design
PIA	Privacy Impact Assessment
PAERIS	PrivAcy-by-design EngineeRIng aSsistant
PEAC	Privacy preserving Access Control
SFMT	SALT Framework Management Tools
ToE	Target of Evaluation
UML	Unified Modelling Language
VAS	Video Archive Search
WP	Work package

Executive Summary

The main goal of the PARIS project is the definition and demonstration of a methodological approach for the design of surveillance systems optimizing the surveillance capabilities together with privacy protection and integration of the concept of accountability. For this reason, we define a framework called SALT (Social, ethicAl, Legal and Technical), and two use cases for its demonstration.

The main objective of Work Package (WP) 5 is to apply the SALT methodology and the design processes for video surveillance data lifecycle management. Within this WP, a privacy control layer is defined on top of the video archive search layer and integrated into existing technology stack. The privacy control applies the SALT framework and demonstrates the feasibility and value of the framework and the associated process.

This deliverable is the last one in this WP with the objectives to evaluate the 1) added value and relevance of the conceptual SALT framework as well as 2) the associated SALT compliant process and 3) management tools, all in the context of the surveillance video data management use case. It also provides recommendations for the extension of the management tools the conceptual work in general.

Note that the latest version also integrates EC reviewers' comments from the final review in the Appendix.

1. Introduction

This deliverable is the last one in WP5 “Using SALT for video surveillance data lifecycle management”. The purpose of the deliverable is to evaluate the added value and relevance of the SALT conceptual framework in the use case, provide recommendations for extensions of the SALT framework management tools, and evaluate the added value and relevance of the SALT compliant process.

The SALT framework[1], in a nutshell, is a knowledge-based approach for collecting, analysing, and representing privacy concerns related to surveillance infrastructure. The knowledge is represented in digital forms in a repository that contains all relevant information which can evolve over time with the help of management tools for the digitalised knowledge. The knowledge can be searched, updated, and applied to specific surveillance systems by system engineers or designers. Information related to SALT framework is described in D2.1 to D2.4. The SALT framework covers relevant knowledge in four dimensions, i.e. social, ethical, legal, and technical. The framework is a joint work of a multi-disciplinary project team. A user of the SALT framework is assumed to have a domain-specific approach, depending upon the user’s domain and level of expertise. Knowledge outside the domain can be inquired from the framework. The value of the framework is to provide step-by-step assistance and decision support through the design phase, in which privacy and accountability is incorporated “by design” in this phase.

The SALT management tools are a set of technical means to regulate and interact with the digitalised knowledge in the SALT framework. Therefore, the tools are an integral part of the SALT framework. There are four tools developed in the PARIS project for various purposes. The questionnaire tool is an interactive Web-based questionnaire to collect accurate and detailed information of a planned surveillance system for privacy impact assessment (PIA). Afterwards, privacy experts can use the information from the online questionnaire tool to conduct PIA, which as a sub-tool, integrated in the questionnaire tool. The taxonomy tool is a complementary tool for the questionnaire to resolve the issues of differences in terminologies existing in different domains along the social, ethical, legal, and technical dimension. The taxonomy tool allows a user to create and update items in the taxonomy. The SALT repository is an online tool to store, update and exchange structured information as a way to digitally represent knowledge related to the SALT framework. The SALT repository use references, i.e. structured forms, to capture and store concerns related to social, ethical, legal, and technical aspects of surveillance systems design. The repository allows for cooperative work among SALT experts. The UML (Unified Modelling Language) profile and PrivAcy-by-design EngineeRIng aSsistant (PAERIS) validation tool is a technical solution to validate whether a system design fulfils the defined privacy and accountability requirements. A surveillance system is modelled in

[1] Note that SALT framework is an overarching concept to describe the PARIS approach to integrate privacy and accountability concerns in the design and development of surveillance infrastructure. However, depending on the context, SALT framework can either refer to the methodology of the multi-disciplinary approach and the associated tools and processes, or refer to the body of knowledge related to the topic.

UML diagrams using optional predefined UML profiles. The validation is conducted by validating whether the models are conformed with the OCL rules (retrieved from the SALT repository) attached to the UML models. D3.1 to D3.4 describe the design and development of these tools.

The SALT compliant process is a part of the methodological approach to surveillance system design while taking into account privacy and accountability. The SALT process defines the action/work flow followed from the initial phase of a surveillance system until deployment and operation as well as system disposal. The main focus of the SALT process, however, is on the design phase. The SALT compliant process has undergone several revisions during the project, taking into consideration feedbacks from multi-disciplinary expertise. D4.1 to D4.4 describes the SALT compliant process.

The main work of this deliverable is based on Task 5.*6 Evaluation of framework and framework management tool* and Task 5.7 *Evaluation of design process in the context of the video surveillance lifecycle management use case*. The use case was initially specified in D5.1, describing technology and concerns of video surveillance system and video archive search from a technical and functional perspective. More detailed specifications of the use case are given in D5.2, which covers application scenario to demonstrate SALT values for privacy by design and accountability by design. D5.3 went into more details of the implementation of the use case as demonstrators to show the technical feasibility. Parallel to the development of the video surveillance data management use case, various concerns are generated during the process based on specific and detailed use case scenario, which are provided to SALT framework, SALT management tools, and SALT compliant process as an input to revise end extend the conceptual work in an interactive way. In the same time, feedbacks from other work packages are taken into account to improve and fine-tune the use case developed in WP5.

One important aspect of the video surveillance data lifecycle management use case is that it is NOT a use case to mimic the design and development of a video surveillance system from *ground-up*. The focus of the use case is rather on the data management of video surveillance data in existing surveillance infrastructure. In other words, the focus of the use case is on the extended usage of the data, not the infrastructure itself. Note that the work is synchronised with the use case in WP6 of using SALT for surveillance using biometric. Therefore, while the evaluation of the use case in WP5 demonstrates the added value of the SALT approach in the design and operation, the evaluation of the use case in WP6 focuses on the added value of the SALT approach in the initialization and design phase.

In the following, Section 2 summarises WP5 use case and the existing implementation of the demonstration, as well as a brief introduction of the SALT framework and the SALT process. Section 3 evaluates SALT framework and process in the context of the video surveillance lifecycle management use case from various aspects. Section 4 provides recommendations for SALT tools and process, and the visions for next steps. Section 5 concludes the document.

Note that the latest version (v1.1) also integrates EC reviewers' comments from the final review in the Appendix.

2. Description of video surveillance management use case and SALT framework

2.1 Use case description

This section gives a general description of the WP5 use case and the actual implementation. It provides the context of video surveillance data management, upon which the SALT framework, the SALT compliant process and the SALT management tools are evaluated. Note that minor updates have been made to the WP5 demonstration since the last deliverable D5.3 Video Surveillance lifecycle management use case, which is described below.

The WP5 use case is dedicated to a video surveillance security system, and more especially to two features considered in the scope of the PARIS project: the management of the lifecycle of the video surveillance footages, and the Video Archive Search (VAS).

The demonstration mock-up has been built by Thales and AIT by interfacing and modifying within the frame of the PARIS project with their background products, which are:

- A Network Video Recorder (NVR, from Thales)
- A Video Archive Search module (VAS, from AIT).

These products have been interfaced to build a mock-up representative in its functionalities of a real-life surveillance system. Moreover, some privacy–preserving features have been developed in each of the modules to illustrate results of the application of the SALT approach (process and tools) to this operational case. The architecture of the use case is depicted in Figure 1. This type of video surveillance system is very commonly used for the surveillance and protection of humans and assets. The “intelligent video” technologies such as VAS are more and more requested by the customers to cope with systems featuring themselves more and more cameras; it is a very representative example of a security system where privacy and accountability issues are at stake together with surveillance and security objectives. Also the legal, socio-ethical points of view widely vary over the world for this type of systems; the technologies available are themselves very versatile.

The goal of the use case is to illustrate the application of the SALT tools and processes defined and developed within the PARIS project, and especially how their use in the scope of this use case enables to perform the optimisation of the privacy, accountability and security capabilities provided by the system.

The use case scenario is the surveillance of a public space using video-surveillance systems. This public place is located in France. At the beginning of the story, the video surveillance system is not equipped with advanced technologies such as Video Archive Search, and might not manage properly the lifecycle of the recorded video footages.

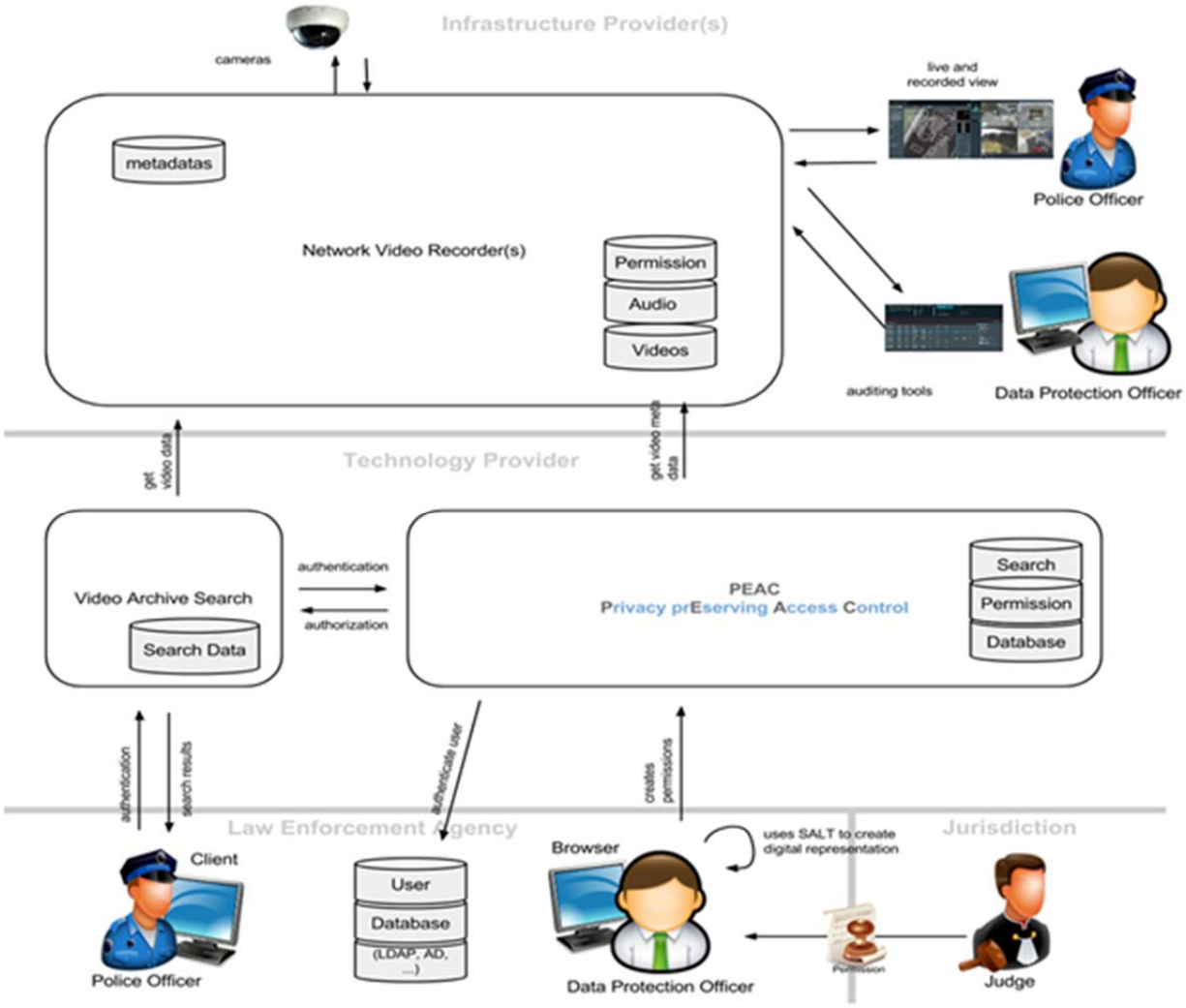


Figure 1: WP5 use case architecture

In the story adopted within the use case, we assume that due to the installation of security system, numerous requests for investigations are made to the system operator. Due to the quantity of video surveillance footages, the owner of the system together with its operators (Police officers) decide to add some more features to the system, especially intelligent video management.

To perform the system modifications, the SALT approach is adopted, in order to select the best technologies while performing an in-depth analysis of the privacy and accountability concerns about both, the existing system and the capabilities to be added.

The SALT process is applied by a multi-disciplinary team and results in some recommendations and requirements (and also in a system model). These requirements are fulfilled by the system developers, who modify the system in the frame of the PARIS project:

- By adding a video-lifecycle management tool within the NVR,
- By providing log and audit tools about the operator actions,
- By hardening the authentication of the operators and the network-level security features,
- By tuning the VAS capabilities,

- By developing a new PEAC (Privacy Enhanced Access Control) building block on top of the system.

2.1.1 Technical requirement influenced by SALT framework

According to the SALT framework, different SALT references and concerns can influence design decisions and introduce new requirements and therefore components of the system design. The following list gives an overview of three (non-technical) requirements of the proof-of-concept system and gives a short summary on how they were influenced by SALT references. The effects of these requirements and the introduced design decisions, for the users of the system, will be demonstrated in the next section with our use case scenario.

1. **User authentication / user management**: This requirement is introduced by a couple of references (e.g. CNIL security guide → Security: authorization management, Architecture design: access control for video archive search, Information Commissioner's CCTV Code of Practice → Access to images, etc.)
2. **Access management:** A dedicated component is introduced to manage the access to specific videos and/or algorithms. This component is influenced by several references (Access to images by law enforcement agencies, Architecture pattern: access control for video archive search, EU Data Protection Regulation Proposal, etc.)
3. **Logging:** This feature is required due to the following references: CNIL security guide → Security: keeping records and documentation of data processing operations, log and audit tools for operator actions for enhanced accountability.
4. **Privacy enhancement**. These are the requirements on general consideration in the design phase, to have technical measures that realize privacy-by-default.
5. **Privacy policy**. Privacy policy might be high level guidance and code of practice on how the system and its user handle surveillance data. It might also be translated into access control policies as who is allowed to access what under which circumstances.
6. **Legal compliance**. The designer must take legal requirements into consideration. This means to obtain the knowledge and opinion of domain experts in the legal domain.

The impact of the design decisions described above is illustrated in the system overview diagram (Figure 2). The **user authentication** introduces a user database and management component (1). To have fine grained control over the rights of different users and to enforce access and privacy policies as requested by the **access management** requirement, a dedicated privacy preserving access control component (PEAC) is added to the system (2). The network video recorder (NVR) is required to implement a **logging** feature, to protocol access to data and operations (3). The **privacy enhancement** feature is implemented by adding a video analytics service to the system, effectively minimizing the amount of privacy invading data being exposed (4). The NVR has the ability to export signed video snippets in order to gain **legal compliance** for possible evidence (5).

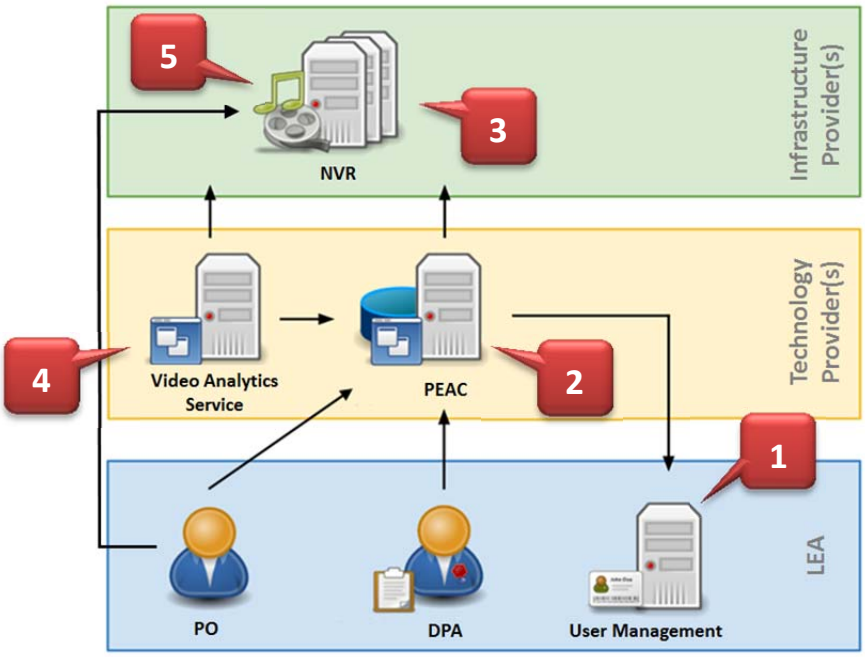


Figure 2: WP5 use case component overview

2.1.2 Use case scenario

Below we present a refined and more "common sense" use case scenario, based on previous work in the previous deliverables.

A ticket machine at a railway station has been broken into twice during the last week. As the method was the same, it is presumed that it was the same person in both cases, so both investigations are merged into one. Unfortunately there is no video camera surveying the ticket machine, but there is video surveillance at the elevator which is on the way to the ticket machine. For both cases there is a possible time window of about one hour during which the crime has been committed. The objective of the investigation is to find persons that used the elevator on both days during the according time windows.

The workflow of the SALT compliant proof-of-concept system would be the following:

1. The Police Officer (PO) logs into PEAC to get access to the system. **(user authentication)**
2. Within PEAC, the PO opens a new investigation, provides requested information and selects the desired surveillance video time frames and analytic algorithms as well as possible conditions to self-restrict privacy related data. **(access management)**
3. Then the PO must wait for the approval of the Data Protection Officer (DPO). He must also log into PEAC and can then decide to approve the requested permissions and or change the request so that it complies with current data protection policies. **(user authentication , access management , privacy policy)**
4. After that, the PO can start the Video Analytics Service (VAS) to perform the actual search. **(privacy enhancement)**
5. The VAS requests the videos from the Network Video Recorder (NVR) and renders the results. PEAC provides the VAS with the authentication information in order to access the NVR. **(access management)**
6. Every access is logged by the NVR. It logs every video data and management access on behalf of the Law Enforcement Agency and the PO in charge for this investigation. (**logging)**
7. After the VAS finishes the analysis, the PO can view the results provided as part of PEAC's user interface. **(privacy enhancement)**
8. If the PO finds evidence, he can export a signed copy of the corresponding video timeframe from the NVR. **(legal compliance)**

The following fictional use case shall show how the proof-of-concept system can enhance privacy as well as support investigations:

After the PO logs into PEAC, he creates a new investigation in the PEAC user interface (see Figure 3). He then continues to add permissions for the according cameras and time frames of the investigation and selects the motion detection algorithm (see Figure 4). The motion detection algorithm is used to compress the video to the meaningful snippets to speed up the search time by magnitudes (see Figure 5).

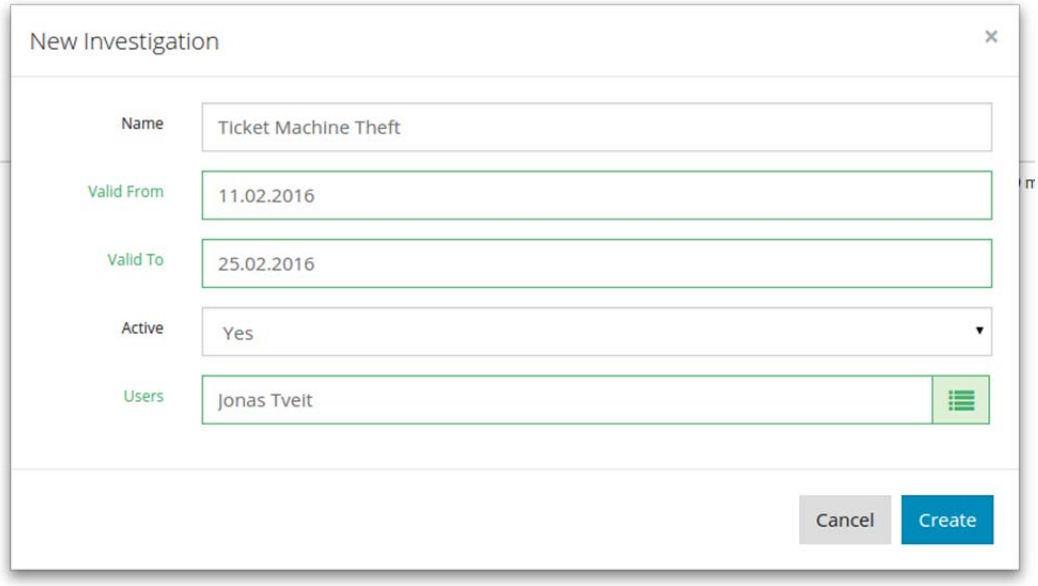


Figure 3: Creating a new investigation

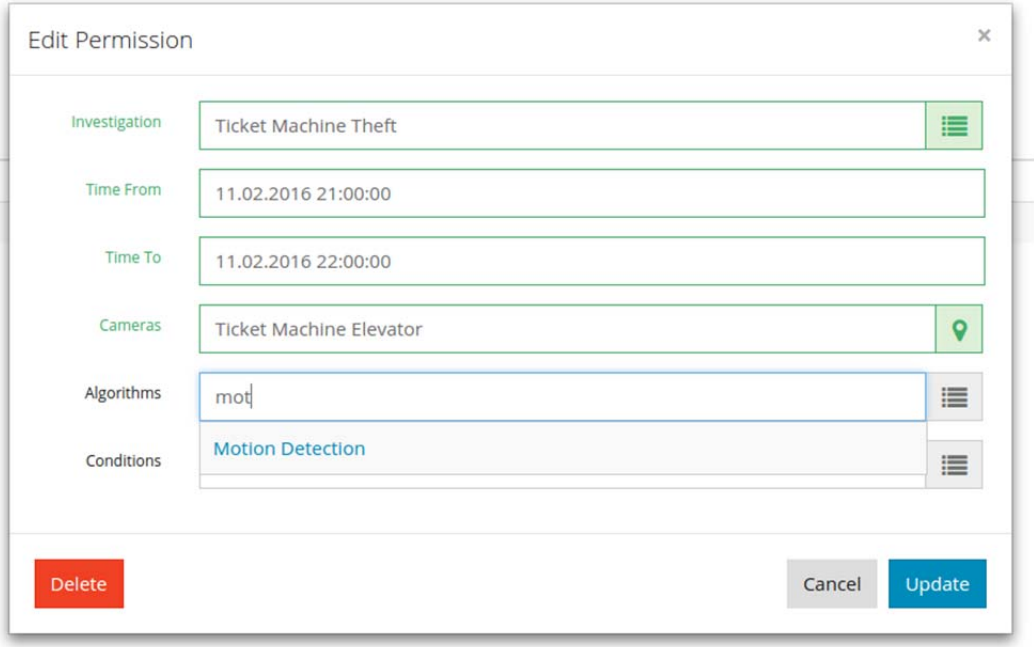


Figure 4: Editing permissions

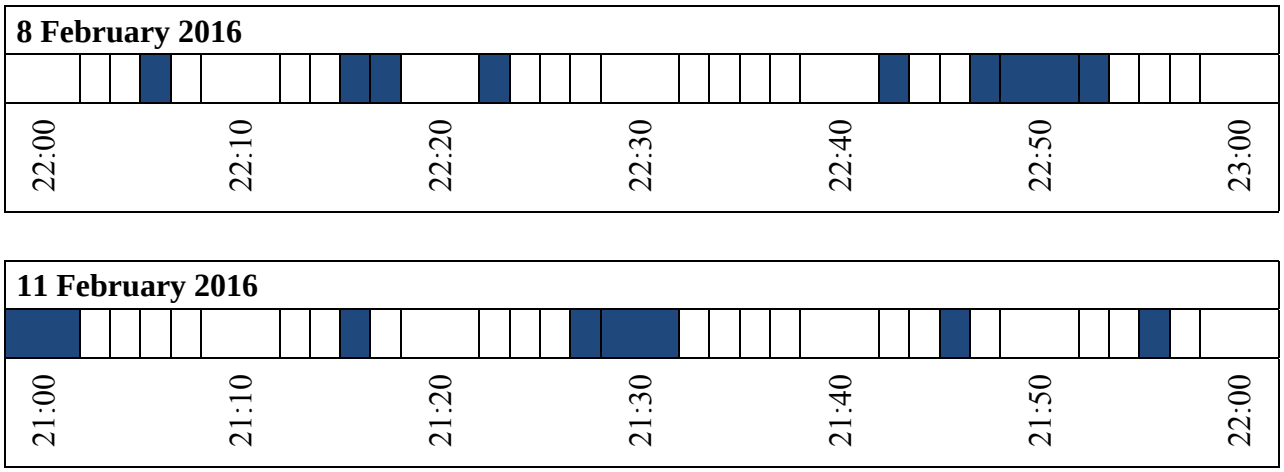


Figure 5: Timeline of motion in surveillance video (marked blocks indicate the timeslots where motion was detected)

The DPO then logs into PEAC and reviews the new investigation. As the requested permissions comply with the privacy policy, she approves the new investigation (see Figure 6). The VAS immediately starts to analyse the data with the permitted algorithms. Figure 7 shows the fully configured investigation.

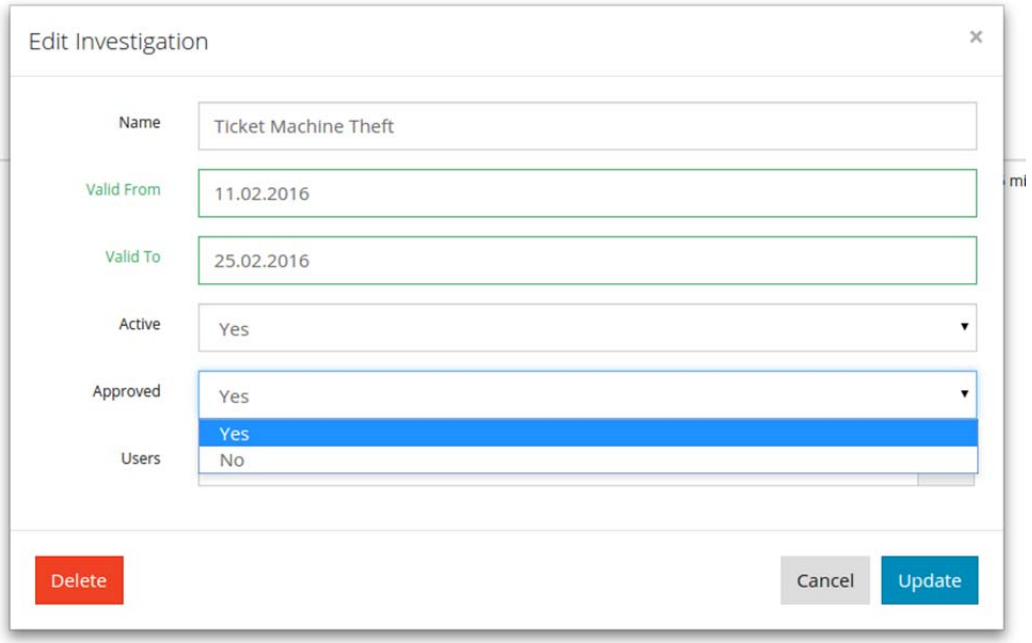


Figure 6: approving the investigation

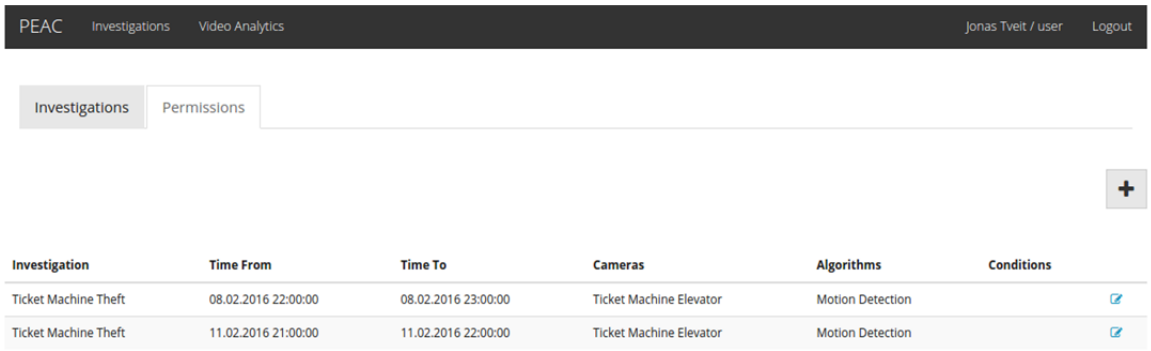


Figure 7: Overview of the permissions of the new investigation

After the analysis is finished, the PO can view the results. To provide the PO with a better overview of the situation, a meaningful snapshot of each motion snippet is made and presented in a thumbnail overview. This makes it possible to show the detected persons of both days side-by-side (see Figure 8) and simplifies the search and comparison of the persons.

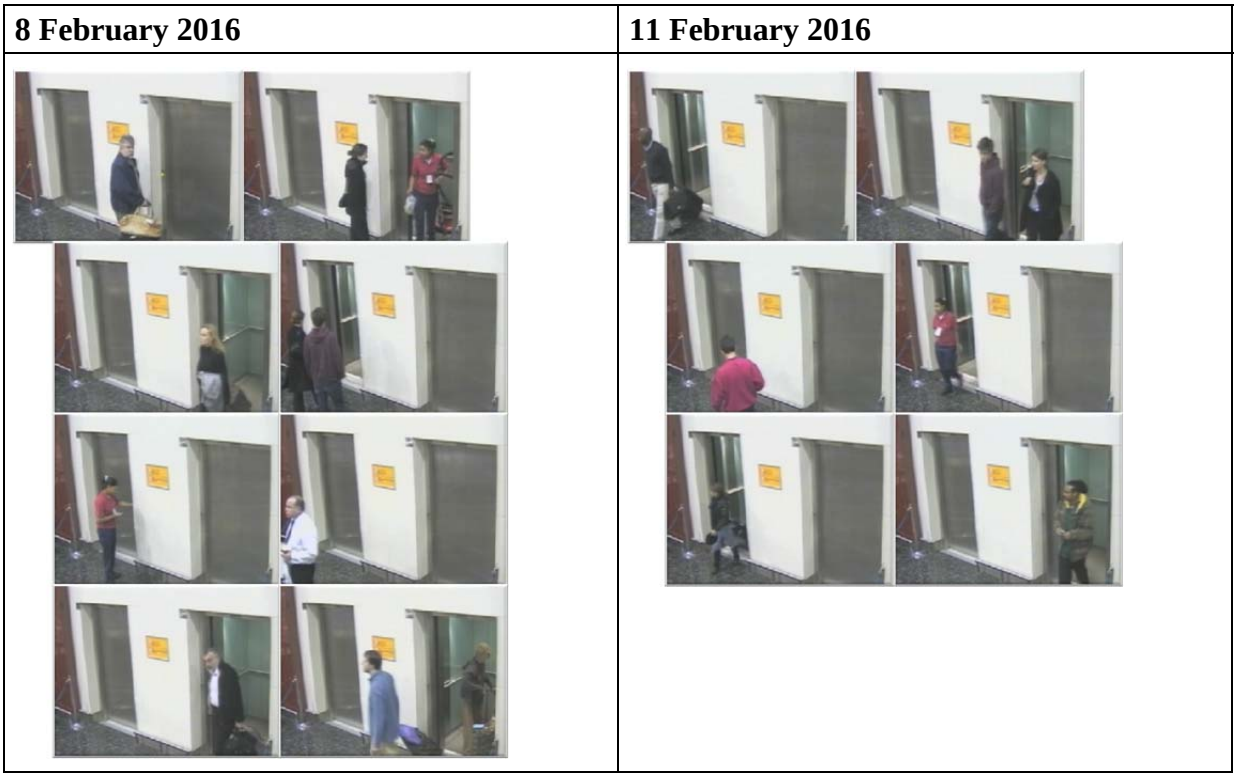


Figure 8: snapshots of detected motion in videos (sample images are taken from iLIDS video footage)

Once one or more suspects are identified, the needed snippets can be exported from the NVR as evidence (see Figure 9) and further investigations can be started. This could involve another video search or other analysis. However these further activities are out of scope of the demonstration use case of the PARIS project.

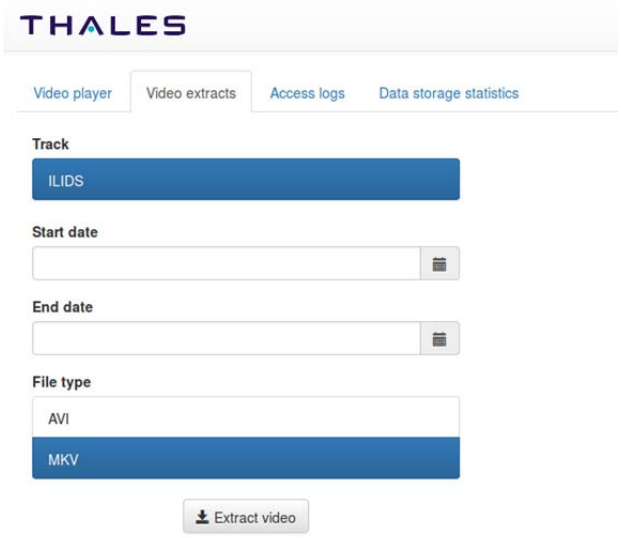


Figure 9: Signed video export feature of the NVR

Automatic face detection and evaluation has been left out consciously for two reasons. Up to this point, no personal data has been extracted or computed from the video. Automatic face evaluation is a very strong algorithm in regards to possible privacy impacts. The fact that such an algorithm would extract personal data of many innocent people in the video makes its use questionable for this investigation, concerning the principle of least privacy intrusion. The second – technical – reason is that not all faces of the persons in the video are visible in a way that they can properly be detected by automatic face detection and evaluation algorithms. The likelihood of false alarms and missed detections is quite high and makes this type of analysing not very useful for the given scene.

Concerning the WP5 video surveillance use case the description of the investigation will stop at this point and the next section will continue with the description of the implementation of a privacy-preserving system according to the SALT processes.

2.2 SALT framework and SALT global process

In order to make this document self-contained, this section provides an overall description of the SALT framework and the SALT compliant process (see deliverable D4.4 “SALT Compliant Processes General Guidelines” for an in depth description).

2.2.1 SALT framework

The SALT framework refers to the whole set of information regarding privacy and accountability concerns for video surveillance and biometric systems that is used by the SALT methodology. This is a key component in the SALT methodology, since as much the developed tools as the SALT compliant process, are highly dependent of this information.

In practice, the SALT framework is stored into the SALT repository, a kind of database where all the information is structured following a template called SALT reference. Each reference contains relevant privacy/accountability information divided into several (the minimum is just one) concerns. But not only that, a whole set of information regarding the source, area, and context of the information is also provided, ant together with that, a series of OCL rules (some concerns may not have them) that will be used by the automatic validator during the design phase of the process.

The size and the quality of the SALT framework lies in the SALT experts, users with a relevant knowledge in privacy and/or accountability in one or several of the following areas: socio-contextual, ethical, legal, technological. These experts are the ones who will create the SALT references and populate the SALT repository, that is, they will contribute to the creation of the SALT framework.

2.2.2 SALT compliant process

The SALT compliant process bounds to the lifecycle of a surveillance system. It describes the whole system work flow through all the stages, from the concept phase to the final system retirement, indicating what type of actors and their roles is involved at each stage. Besides, the particularities of this process ensures the creation and usage (if followed) of a SALT compliant system, that is, a surveillance system where privacy and accountability concerns have also been taken into account, together with the rest of functional requirements.

Even though the application of the SALT compliant process guarantees a SALT compliant system, it is important to nuance this statement. Since the content of the SALT framework depends on the input given by experts (see Section 2.2.1), it is clear that the information stored into the SALT repository will evolve as the time goes by with addition of new concerns, possible extensions, modifications to some others, etc. This means that a particular surveillance system developed following the SALT compliant process may differ on its final design/implementation according to the time when it was created, that is, depending on the maturity of the SALT framework. However, in every case we say we obtain a SALT compliant system because the privacy/accountability concerns that were available at that moment were taken into consideration.

Having clarified the nature and reason to be of the SALT compliant process, Figure 10 depicts the lifecycle of the process as it goes through the different stages. Starting from the concept phase, where the system stakeholders have the intention to create (and the initial requirements) a given surveillance system, and ending with the retirement of such system after its whole operational period.

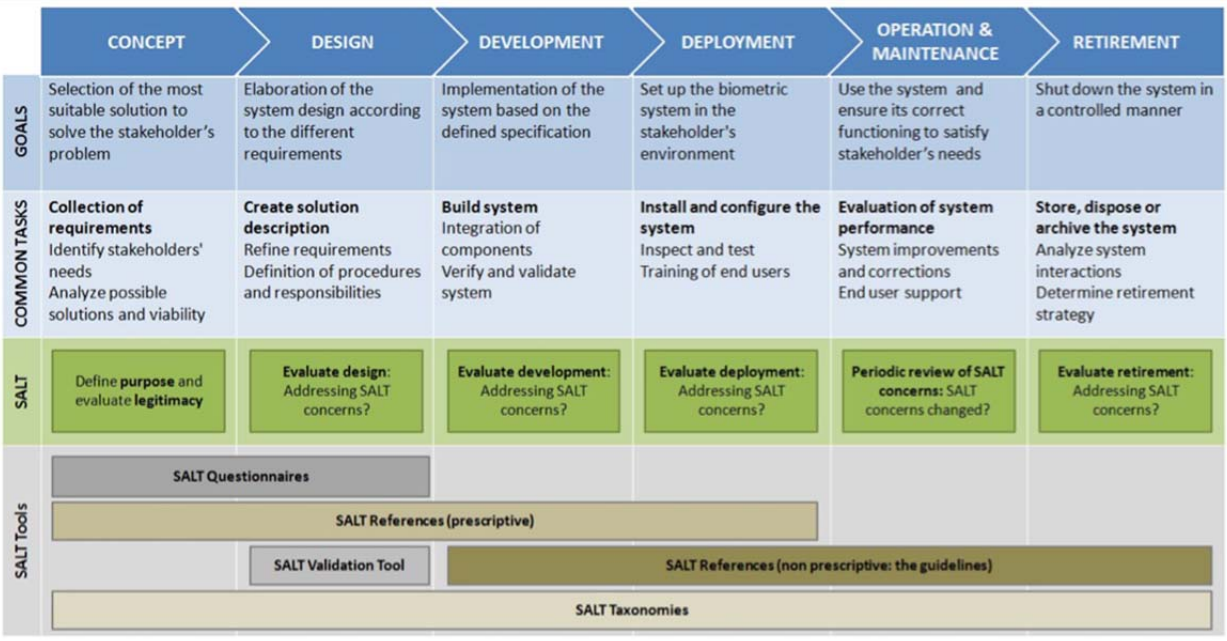


Figure 10: Stages of the SALT compliant process

Figure 11 shows a different perspective of the SALT compliant process, where different user types (or roles) for each stage of the process can be seen. Nevertheless, it is important to understand that a user can assume different roles in the process. He or she is not forced to interact with just one stage of the process, as it may seem from Figure 11, but it can take part in any other stage if necessary (or not). For example, a system designer could participate in the design phase and also in the development phase, just to mention one possibility.

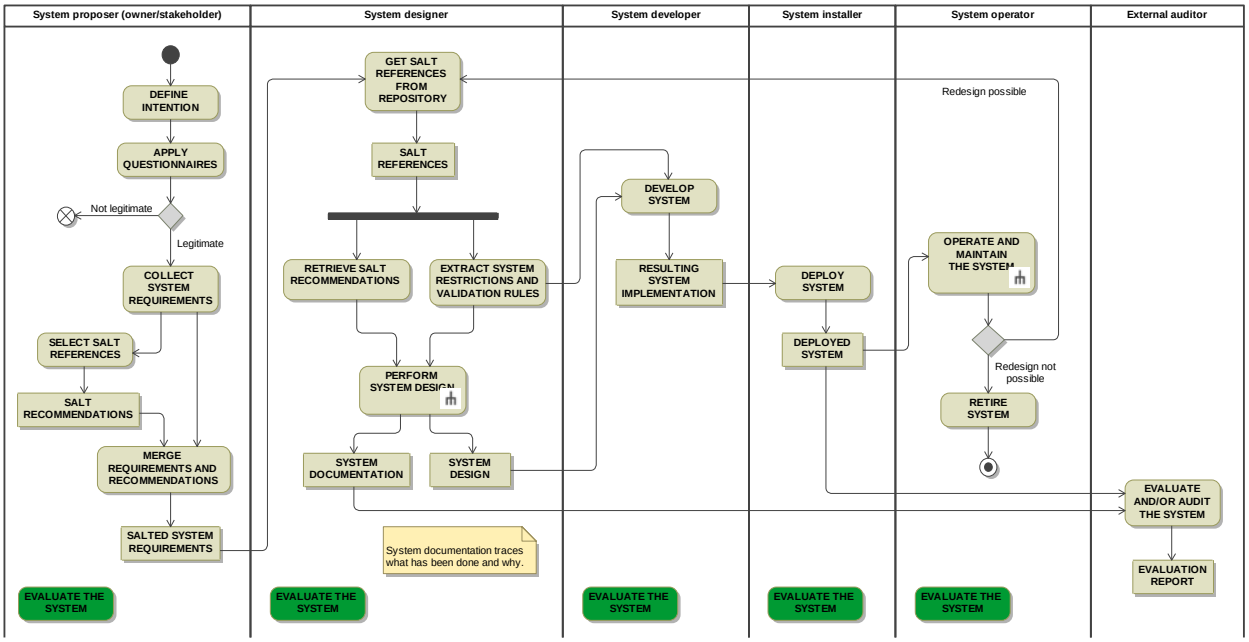


Figure 11: SALT compliant process and user types

3. Evaluation of video surveillance lifecycle management use case

3.1 Evaluation approach and method

The SALT framework is, by definition, a conceptual framework which integrates multi-party concerns in the design and development of surveillance systems. The digitalised representation of privacy and accountability relevant knowledge in the SALT repository and the associated management tools are computerised ways to interact with such knowledge. The SALT framework is associated with SALT design processes, designed by the PARIS consortium to streamline privacy-by-design process for surveillance systems.

“Evaluation” by definition, is a systematic determination of a subject's merit, worth and significance, using criteria governed by a set of standards [1]. However, in this case, it is obvious that the target of evaluation (ToE), i.e., the SALT framework, is neither a pure software system nor a pure concept. While the technical partners and the legal and social partners are familiar with evaluations in their respective domains, the consortium found it a challenging task to evaluate such a mixed framework. After multiple discussions, the PARIS consortium decided to tackle the evaluation in a pragmatic way. The goal isis to evaluate the added value of SALT conceptual framework, management tools, and the SALT compliant process in the context of the video surveillance system use case.

The evaluation in D5.4 is thus divided into two parts:

1. An evaluation of the practical use case based on requirements specified in D5.1. The evaluation is led by the two main use case partner (THALES and AIT).
2. An evaluation of the added value by subjective opinions on the ToE in form of “lessons learned” from all partners (UMA, KUL, THALES, and AIT).

3.2 Evaluation at the SALT Framework level

This section is dedicated to the evaluation of the SALT framework and tools from the perspective of the WP5 use case which is related to a “video surveillance archive search” security system, supposed to be located in France.

The operational use case considered in the WP5 is based on a video surveillance system which is installed in premises open to the public (such as a metro or public transportation station), and that it is forecasted to use a video archive search technology in addition to the existing system in order to cope with new threats (including robbery at an automatic distributor).

In this use case, the system is modified using the SALT process and tools to optimize the security and the privacy of the final system. This results in 2 types of actions on the existing video surveillance system:

- The modification of the already existing component, which is the Network Video Recorder. These modifications are performed in order to interface it to the new Video Archive Search module and also to refine the privacy protection level it provides,
- The addition of a Video Archive Search component, which provides the new security measures that are foreseen.

There is an interesting difference to note with the WP6 related use case (which takes as the example biometrics-based security system): within the WP6 the system is designed from scratch using the SALT tools and processes, whereas in the WP5 the existing system is modified using the SALT tools and processes. This gives a second point of view about the SALT tools and processes. It has to be emphasized that this second point of view is closely related to realistic and representative security projects that are deployed over the world, for several reasons:

- The Video Contents Analytics (VCA) technology and the Video Archive Search (VAS) technology are more and more mature and requested by end customers,
- Many customers have in the same time already invested in video surveillance systems and do not wish to replace them all because of the adoption of the new VCA and VAS technologies.

This allows us to assess the use of the SALT framework and tools in the context of a system upgrade/extension. In this type of approach; this difference also results in the fact that the first phase of the SALT process (concept phase, cf. Figure 10) is lightly applied, the type of system which is under consideration being already defined. This is also the reason for providing in this case a questionnaire which is mainly a PIA (Privacy Impact Assessment) nicely reused from the EU FP7 ADVISE project[2].

The adapted process for this use case where the system already exists and the technology to deploy is already defined is described in Figure 11. The process for the WP5 use case is mainly based on the generic process (illustrated in Figure 10); however it is adapted to correspond to the WP5 specificities: the upgrade of an existing system with a new security technology, and also a focus on the design/develop part rather than on the purely operational part (system deployment and maintenance, including configuration and retirement).

It also explains where each of the SALT tools is used within the whole process; SALT taxonomies are not here cited as they are potentially used in any of the stages, in relation with any of the other tools provided by the SALT methodology.

[2] FP7 project ADVISE (Advanced Video Surveillance archives search Engine for security applications), http://www.advise-project.eu/

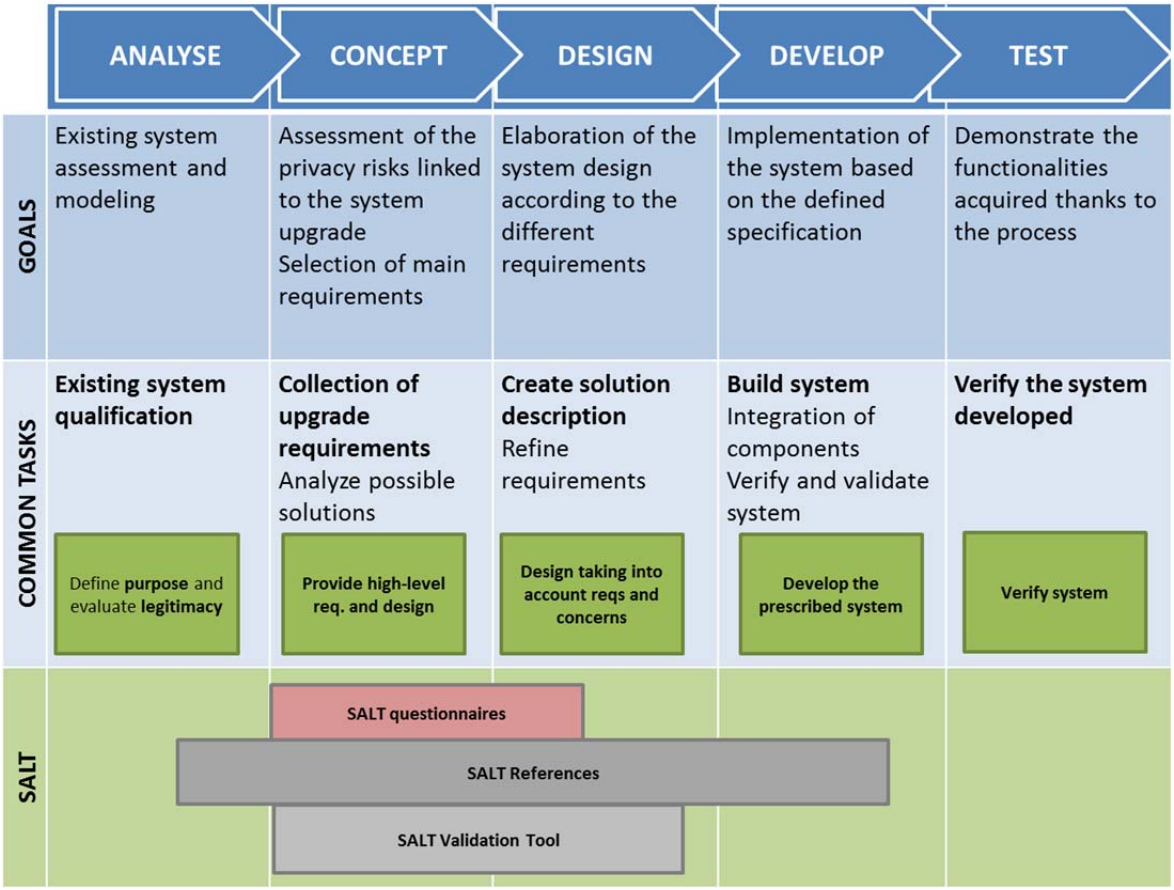


Figure 12: Process refinement for WP5 use case

Also of interest as a preliminary part to this evaluation at the SALT level is to identify the users who would be likely to be implied within each of the steps:

- The “ANALYSE” phase would mainly be performed by system experts and system designers, in relation with operational system specialists (system operators),
- The “CONCEPT” phase would be performed together by privacy experts and system designers,
- The “DESIGN” phase would be performed by system designers,
- The “DEVELOPP” phase would be performed by system developers,
- The “TEST” Phase would be performed by IVQ experts (Integration, Validation and Tests).

This process as presented above can however be considered as a simplified one (compared to actual design processes) for 2 main reasons:

- The actual process followed is very often made of the aforementioned steps; nevertheless, iterative loops “naturally” happen between the steps: the process is not followed in a purely linear way,
- This presentation of the process simplifies the fact that in many cases it is shared between a “client” and a “provider”, with a tendering process in between; the boundaries between these 2 process parts are variable: the “customer” sometimes is likely to perform the process up to the design stage (in this case the customer is said “mature” or “educated”); sometimes most of the definition and development tasks are requested to be performed by the provider.

This process is nevertheless representative of real-life processes as the main steps followed remain present in the internal process followed by the security industry.

Within the next sections, the way each of the SALT tools is used within the WP5 use case is described together with an evaluation of these tools:

- The SALT questionnaire tool,
- The SALT taxonomies tool,
- The SALT references tool,
- The SALT modelling capabilities.

The evaluation of the global interrelation between different types of tools is performed with a section dedicated to the functional aspect. The ergonomics related considerations are enclosed in a section dedicated to usability aspects.

3.2.1 SALT taxonomy aspect

In the course of the WP5 Use Case, the taxonomy tools provided by the SALT methodology have been used to provide general awareness about the domain of application (video surveillance).

The creation of concepts has been performed to provide an example of taxonomy for the domain. Figure 13 below shows the presentation of the concepts provided by the tools:

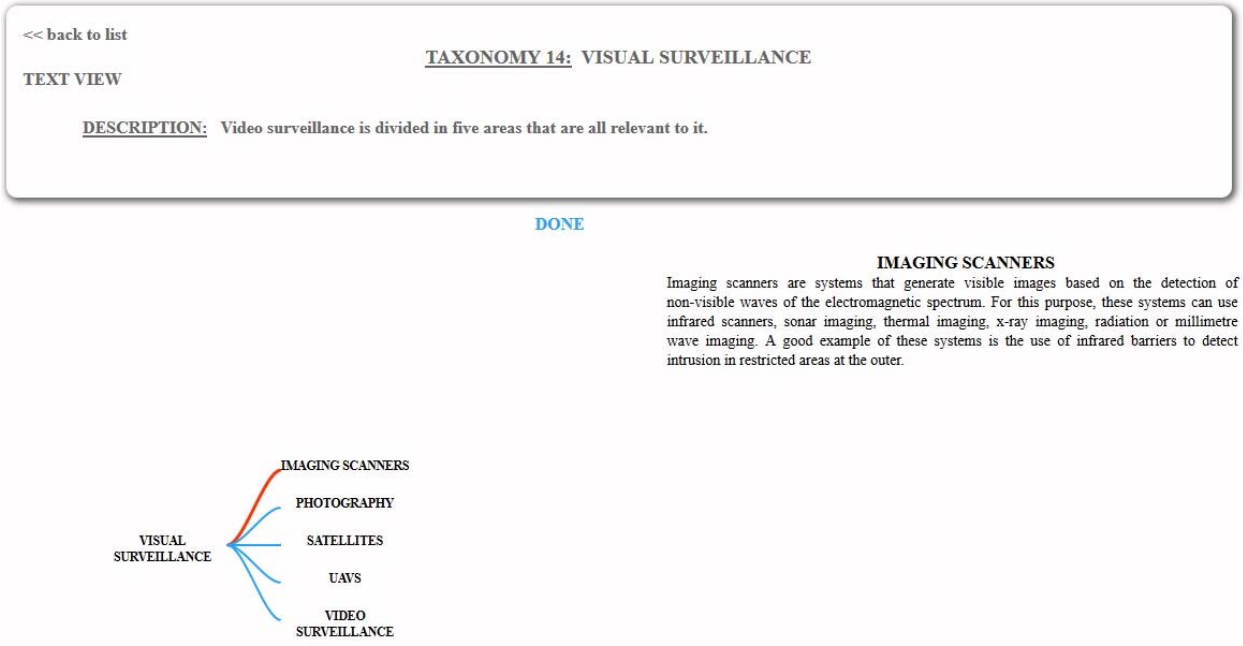


Figure 13: Example taxonomy presentation within SALT tools

The tools for the edition of the concepts have been used without important difficulty. A screen capture of these tools is provided below in Figure 14

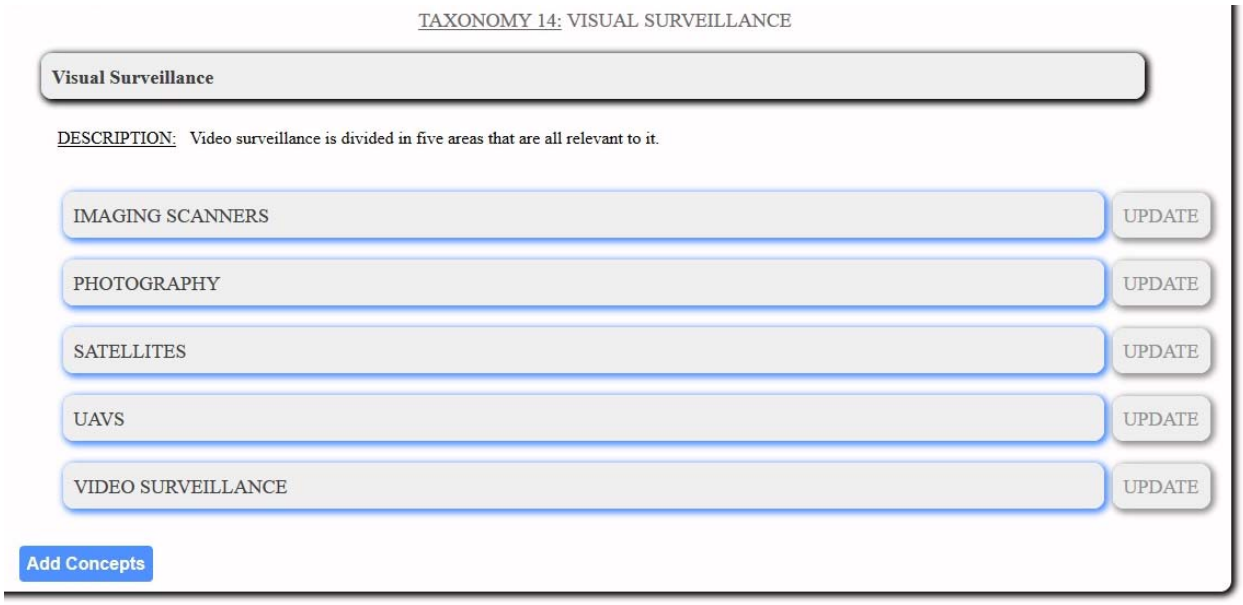


Figure 14: example edition screen dedicated to taxonomies

As an evaluation in the frame of the WP5 "Video surveillance data lifecycle management" encompassing a Video Archive Search dedicated topic, it seems that this tool is suitable and adapted to the needs:

- It provides multidisciplinary and open contents to raise sufficient awareness within the community of the users of the SALT tools,
- It is easy to browse and the graphical presentation of the concepts makes it easily understandable,
- It is really useful in the context of a system design and development: the different actors and stakeholders implied within the process have very different backgrounds, knowledge and goals,
- It relies on authentication mechanisms for the edition of the concepts which enables to clearly differentiate the users by their authorizations (to consult and to edit),
- The edition itself is easily performed,
- Moreover, a help page easily accessible is available.

The only feature that might be of help in addition would be the capability to link taxonomies to other SALT tools and contents (within questionnaires, references and even within the modelling and validation tool); this could be done by hyperlinks insertion.

From a pure use case, and more generically video surveillance perspective, it could also be enriched with many other concepts of interest in the Socio-Ethical, Legal and Technical fields; most of the items would be of interest for other types of security systems (this is expected to happen in the future when the tool is used by the community).

3.2.2 SALT questionnaire aspect

As explained above, in the scope of the WP5 use case, dedicated to video surveillance data lifecycle management and to Video Archive Search (VAS), the system of interest is not build from zero, but it corresponds to the upgrade of an existing video surveillance system, with lower capabilities.

The role of the questionnaire (and its expected outcomes) is a bit different in this case from the role it has when a new system is being built (this relates to the differences between the Figure 10 which presents the most generic process and the Figure 12 which adapts to the use case).

In the generic case, the role of the questionnaire is to assess and specify the salient requirements regarding a security system taking into account its expected mission, its environment; this is done taking into account the four SALT pillars (Social, Ethical, Legal and Technical), even if at the intention stage there is more weight on the first three pillars: Social, Ethical and Legal. This gives the best opportunity to tune both the privacy and security capabilities and performances provided by the system. In some cases this happens concurrently (co-optimization of security and privacy/accountability); in other cases choices and trade-offs have to be made (balance between privacy and accountability).

Within the WP5 use case, the questionnaire is expected to provide some feedbacks and analysis about the system already in use (video surveillance management and recording system) and to help specifying some new features (video archive search). The Privacy Impact assessment (PIA) questionnaire from the ADVISE FP7 project is adapted to this needs and fully reused using the SALT management tools.

The ADVISE PIA was produced within the deliverable D2.3 of the ADVISE project (Identification of practices and procedures of compliance for the use of video surveillance archives) [2]; this deliverable was produced under the supervision of J. Peter Burgess and Dariusz Kloza from VUB (Vrije Universiteit Brussel). This questionnaire is re-used in the PARIS project, under their written authorization.

Within the scope of the ADVISE project, the PIA produced is paper-written; the SFMT (SALT Framework Management Tools) enable to computerize the contents, and also the answers. This is an important gain provided by the SALT tools. The figures (Figure 15 and Figure 16) below give examples of SALT tools screenshots dedicated to the edition of the SALT questionnaires (including their creation, update), and example of screens that are experienced when filling the questionnaires.

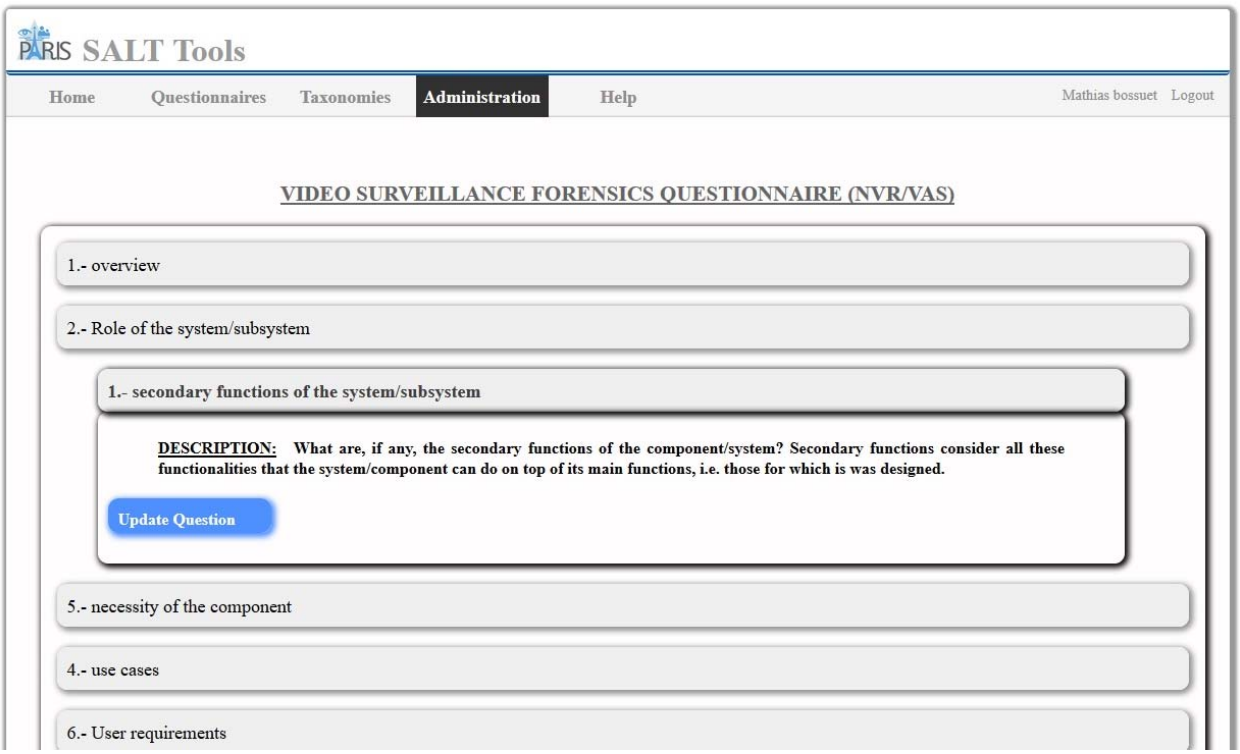


Figure 15: example screen dedicated to questionnaire edition

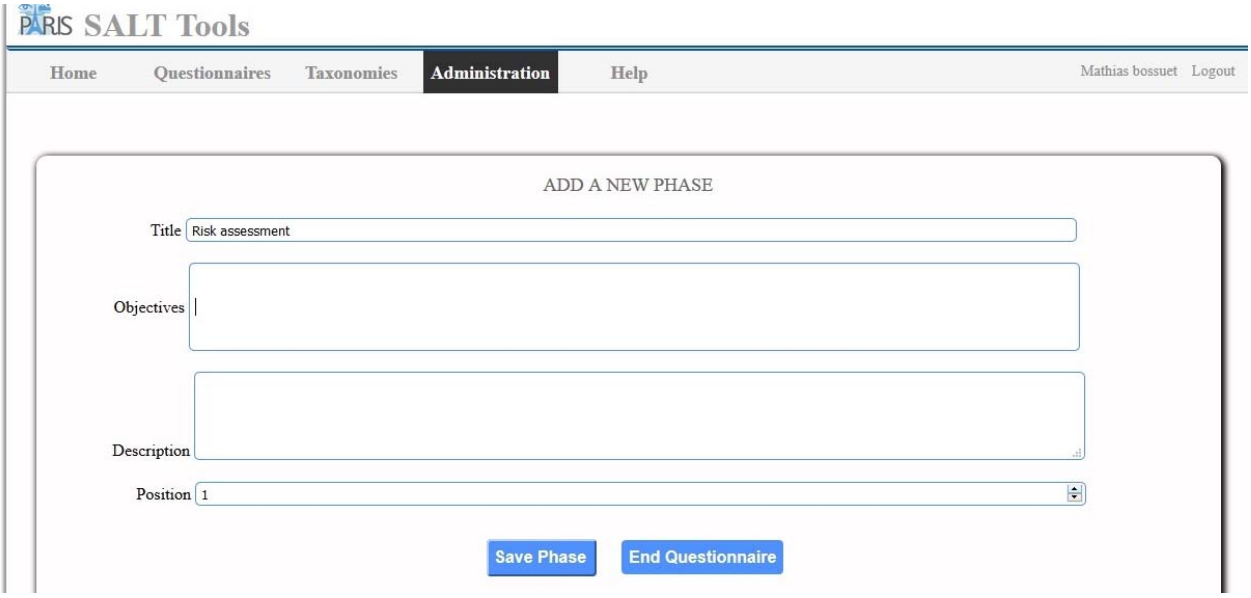


Figure 16: example edition screen dedicated to questionnaire edition

In the scope of the PARIS WP5, the questionnaire based on the ADVISE PIA allows to raise awareness about the constraints to take into account at design phase and about the risks that might weight on the system from privacy/accountability point of view, but also from the security point of view.

The SALT tools dedicated to the management of the questionnaires enable to fully integrate the PIA questionnaire without any modification.

The sections of strong interest within the questionnaire given the exact topics addressed in the WP5 Use case (assessing an existing video surveillance system and assessing some new functionalities about VAS) are:

- The section dedicated to the risks identification (Ethical risks, Privacy risks, personal data related risks),
- The section dedicated to the risk assessment,
- The section dedicated to the recommendations for the design and development for the system.

It is very interesting that the ADVISE partners had anticipated a link between their PIA and the design and development of the system; the PARIS tools enable to go further as it encompasses capability to address also the design and development phases of the security systems.

This also underlines that there are some important links (from the semantic, logic and process points of view) between the different stages and tools provided within the PARIS project: the questionnaire naturally raises design constraints, requirements, guidelines that are to be linked to those embedded within SALT references.

An evaluation of the SALT questionnaires from the WP5 points of view underlines the following salient points:

- The SALT questionnaire tools are fully adapted to the needs raised in the scope of the work-package, as they allow, without any modification, to integrate contents from one other project; the contents from this other project (the ADVISE PIA questionnaire) have not taken into account any of the constraints of the PARIS project and of its tools; conversely, the PARIS project tools have not taken into account the ADVISE PIA in its structure. This is a sign that the questionnaire tool is versatile enough to cope with several viewpoints or approaches,
- This versatility and flexibility is a key requirement to underline within this type of tool, as it is likely to be used by people with very different backgrounds and cultures. The questionnaire, by its nature, is a very open tool for gathering wide-range inputs; also time has been spent to define functionalities that are of real interest such as questionnaire phases (can be seen as sub-questionnaires within the questionnaire), sub-questions, multiple choices answers as well as free text answers. This really enhances and optimizes the features of the questionnaire tool,
- The shape this tool takes (questions), given its mission and its position within the design process (first phases, where most of the multi-disciplinary interactions happen) seems perfectly suited,
- From the experience of the WP5 work-package, it appears that a questionnaire might not be fully filled for a given application; as an example in the use case considered, as the system already exists, some choices have been already made: first parts of the questionnaire might not be of interest in this type of system. It would be interesting as an enhancement of the tool to have the capability to discard some steps,
- Also, the capability to comment the actions performed (computerized stickers) would be of interest to add some information in a more informative way about the options, understandings retained during the questionnaire answering process.

3.2.3 SALT references aspect

The SALT references are at the heart of the SALT framework regarding the WP5 use case, as they provide recommendations and guidelines for solving the issues and concerns at stake especially at design phase (cf. Figure 12).

The exhaustive list (and contents) of references that have been provided for the PARIS project for the WP5 is given in D5.3 Video Surveillance Lifecycle Management Use Case [3]. It has been

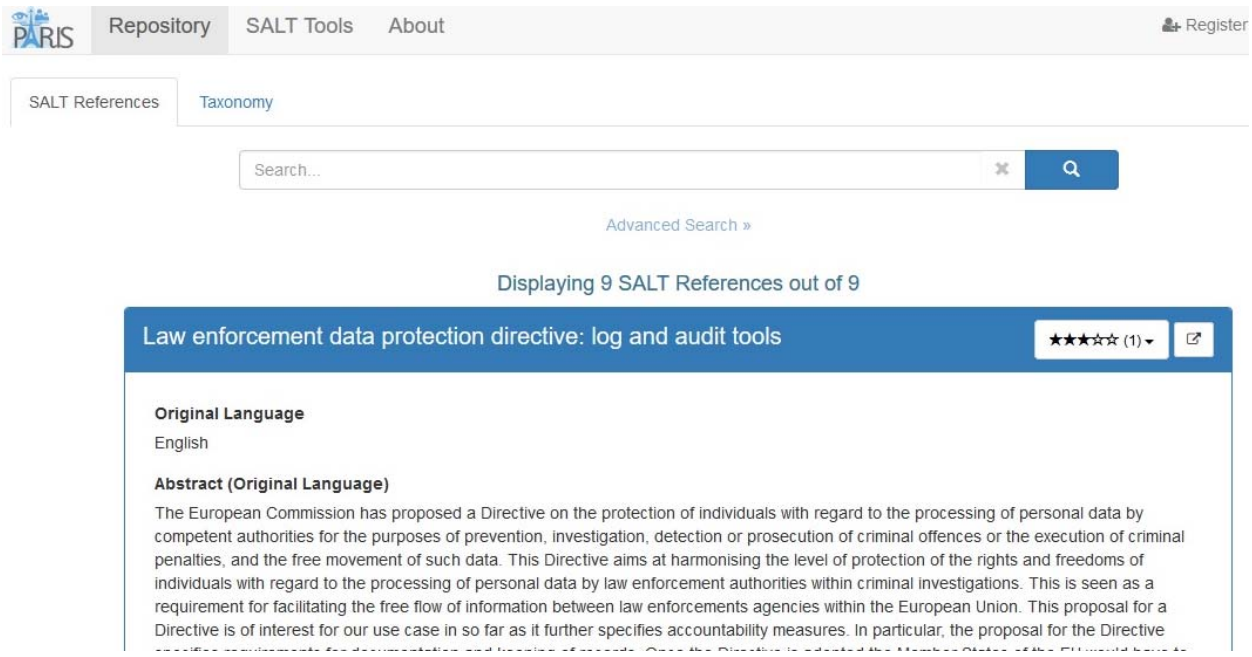
provided a wide variety of references, within the four domains of interest of the SALT (the SALT "pillars"), which are the Socio-Contextual, Ethical, Legal and Technical domain.

Part of the internal structure of a SALT reference is depicted in Figure 17. It is basically made of a header that provides descriptive contents and several concerns (free number of concerns) that each contains an atomic part of knowledge. Also, a concern can be prescriptive (in the sense that it proposes some measures to adopt to reach a given objective); in this case, the prescription is provided within a human-language form, but it can also contain a system-model objective and non-ambiguous rule (using the Object Constraint Language, OCL). This opens to the use of many tools ranging from system design to system development and validation.

There can be a very huge number of SALT references within the SALT framework; fortunately, they are tagged using a multiple dimension approach, combining:

- The type of contents of the references,
- The type of system addressed,
- The phase(s) of the process addressed by the references,
- The type of concerns enclosed in the sense of the privacy principles (in the sense of the 95/46/EC Directive),
- Free comments.

Moreover, the language used for the reference contents is specified. These features enable to efficiently sort and browse the SALT contents even if very large. This enables at the end to select the references of interest for a given context based on the exact needs and options taken by the stakeholders responsible for the choices made around the system. This selection provides explicit or implicit requirements that are used within the system design and development. A compelling approach with restrictive requirements formulation and verification based on system modelling (optional step) is proposed in the next document section, dedicated to SALT validation tools. An example reference contents is provided in Figure 17. An example reference edition is provided in Figure 18.



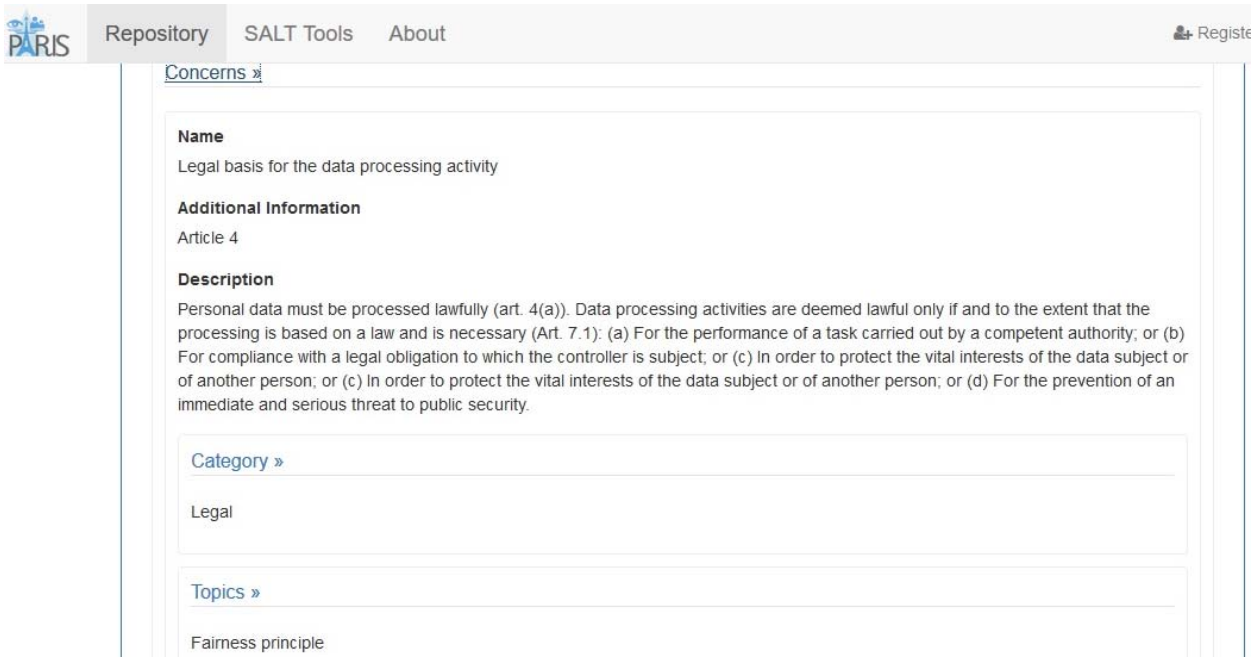


Figure 17: Example SALT reference contents

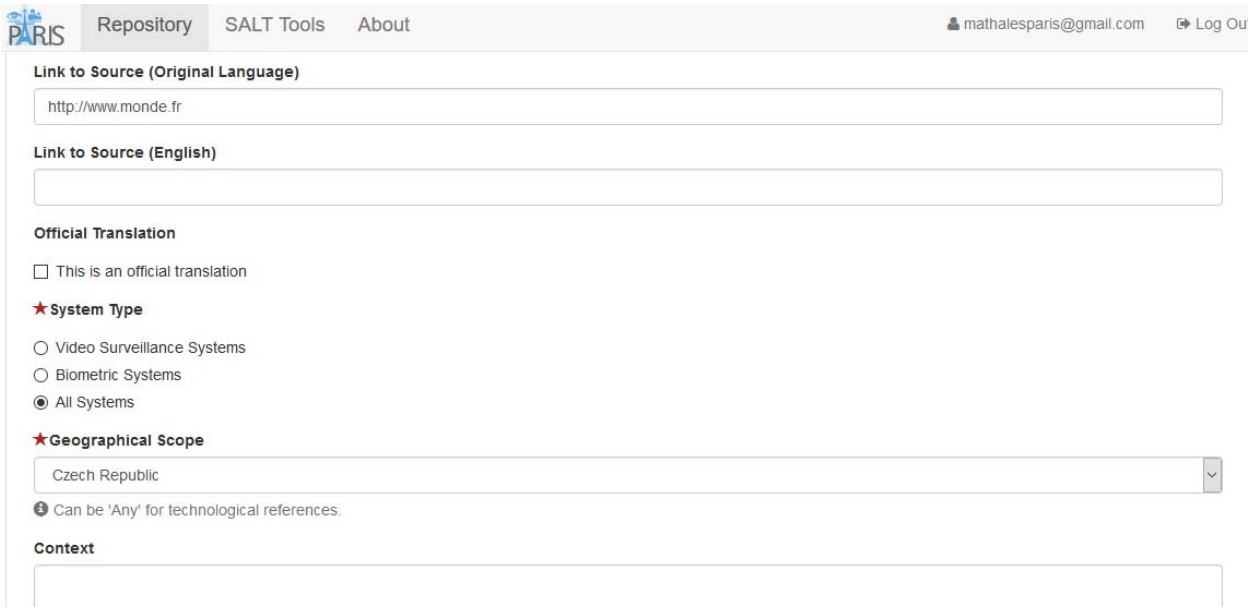


Figure 18: Example SALT reference edition

Within the context of WP5 use case, the references (and concepts) that would be selected from a demonstration point of view are the references that point the enhancements that have been realized by THALES on its Network Video Recorder (NVR) product, and by AIT on its VAS (Video Archive Search) and PEAC (Privacy-preServing Access Control) research prototype. The contents of interest mainly fall in the legal and technical domains. Assuming that the use case is located in France for exemplification, the references of specific interest for the WP5 would especially be (cf. D5.3 [3] for extensive contents):

- Reference: French Homeland security code (Legal reference)
- Reference: French ministerial decree of 3 August 2007 (Legal reference)

- Reference: French code of criminal procedure (Legal reference)
- Reference: Law enforcement data protection directive (Legal reference)
- Reference: Encryption and signature of the video data (technical reference)
- Reference: Operators actions logging (technical reference)

Some of the concerns of interest within these references embed guidelines; some of these guidelines are also formally expressed using OCL rules (cf. the next document section dedicated to the SALT validation tool).

For the evaluation of the references and of the SALT related tools, the WP5 use case provides the following feedbacks:

- The reference tool combines the flexibility of free text (the description of the concerns) and the structuration thanks to multi-axis description and tagging of the references. These tags include crucial information such as the geographical zone of application, and the process phase(s) where the reference application makes sense.
- The reference tool provides a versatile and flexible platform that enables the interrelating of contents from domains and stakeholders as different as social, legal, ethical and technical domains and mind-set; moreover, it combines references which are purely informative (not prescriptive) and references which embed formal statements and requirements.
- The reference tool also provides browsing and selection capability that are needed to build a set of references (or even a set of concerns, which are the atomic parts of the references) applicable to a given context. Once more, flexibility is a keyword: the selection performed is not unique for a given context, it will depend on who performs the selection. The SALT tools dedicated to references allow this flexibility,
- To even enhance the usability and relevance of the reference tools, it would be interesting to provide means to add some informative comments related to any project using the tools (especially to explain how and why the selection of applicable references is realized, the reason of the choices made). Ideally, this would happen in a workspace dedicated to each project and the actions performed and comments would be identified with the identity of their authors.

3.2.4 SALT validation tool aspect

The SALT process adapted to the WP5 use case model (Video surveillance lifecycle management and Video Archive Search) has been depicted in Figure 12. The questionnaire is used to assess the existing video surveillance system and the new envisaged technology (from the privacy/accountability and security points of view); then applicable SALT references are selected to address the stakeholders needs (mainly system proposers and system designers at this stage) and to match the outcomes of the previous analysis (the one based on the questionnaire).

The chosen SALT references provide (at least for some of them) some prescriptive guidelines on the system: constraints about the type of system, its functionalities (e.g. presence or absence of a functionality), and even quantitative functionalities.

The guidelines are generally expressed in natural language; for this reason, their application on the system design is to be performed by system designers using adapted tools. A typical (first level) system architecture for the WP5 is proposed below, illustrated in Figure 19.

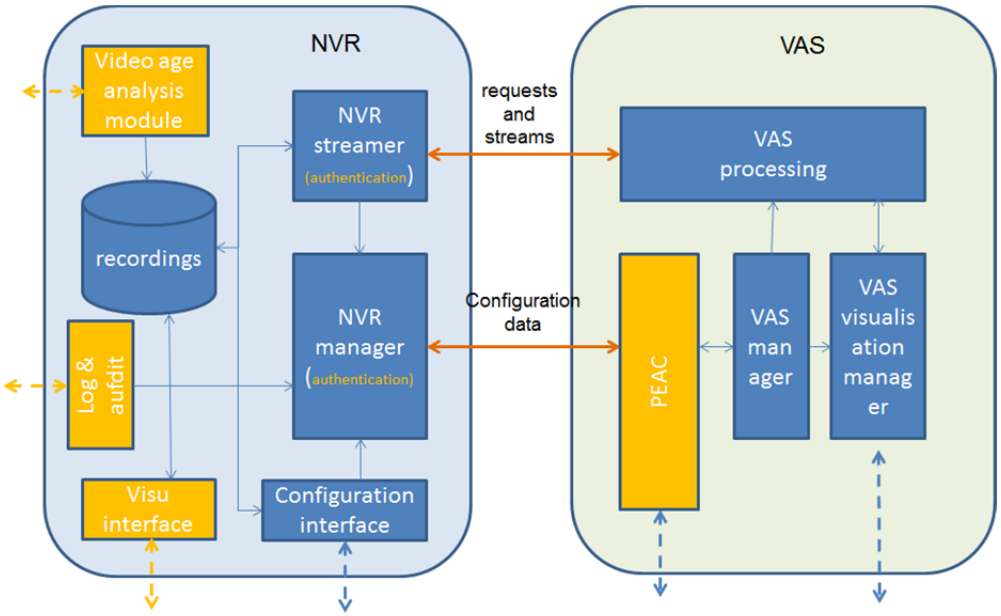


Figure 19: System architecture before taking into account PARIS video surveillance model

On the architectural view, the blue boxes are system elements which exist previously to the use case analysis (reason for the existence of the first step “analyse” in Figure 12); the yellow boxes (and texts) are added to the system after the PARIS project analysis; in a way, the outcomes of this analysis and the guidelines of the selected references are hosted within these system elements. In this case, the approach in designing the system and in taking into account references guidelines is not systematic and relies on the stakeholders responsible for managing system developments.

The PARIS project proposes, thanks to its WP4 “SALT compliant processes”, a more systematic approach, however optional. This approach is based on the automatic verification of guidelines and adopted constraints on the system thanks to dedicated tools.

This automatic validation requires that the system designed is expressed using blocks from a standard dedicated model expressed in the widespread modelling language UML. The standard model elaborated in the frame of the PARIS project is shown below on Figure 20.

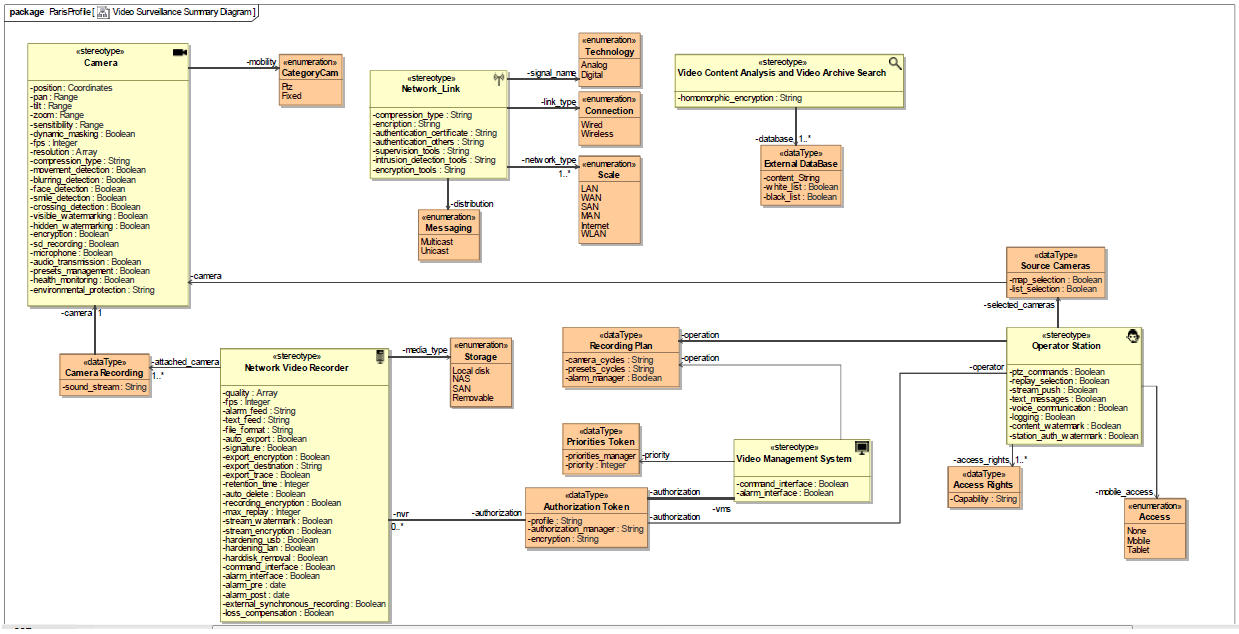


Figure 20: PASIR WP5 video surveillance use case system model

This model is based on « artefacts » that have « properties »; the very important point is that the guidelines expressed in the concerns of the SALT references can most of the time be expressed as unequivocal constraints on the artefacts and their properties. These constraints are expressed in a standard form using Objet Constraint Language (OCL) rules.

This opens the door to the formal validation of all or parts of the system model; moreover, as very often the development chain used in the firms is equipped with tools that trace during the whole development process the consistency of the developed system with its model, this formal validation can be expected to produce at the end a system which is coherent with the expressed guideline from the start of the designing process.

The condition for this validation to be possible is that the Use Case system model is bridged with the PARIS dedicated model. This is performed very simply on the Figure 21 below thanks to a merge between a very first WP5 use case architecture (architecture from Figure 19, enriched using the artefacts from Figure 20).

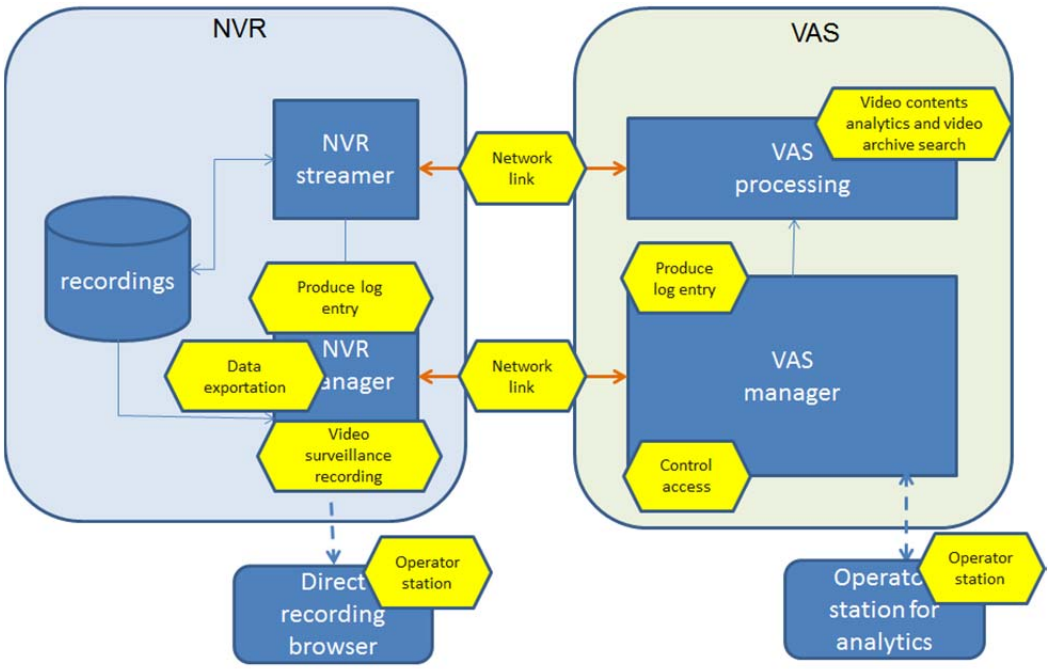


Figure 21: WP5 system model taking into account PARIS video surveillance model artefacts

The artefacts from the model are attributed to the system elements from the system architecture. This mapping allows performing a validation of the system design as soon as the attributes of the artefacts are filled.

The final validation step itself has not been performed within PARIS WP5; however the use case illustrates clearly the validation process. The evaluation points proposed from the WP5 for the SALT validation tools are:

- The formal validation by itself of the design guidelines and constraints is something really interesting; the raw objective of the PARIS project being to produce a SALT compliant process, this enables to go a bit further to at least partially prove the compliance of the system itself,
- As it relies on the widespread UML language, it is easily understood and used by the main stakeholders implied at this stage: the system designers and the system developers. Also as this modelling language is at the core of many tools they use for system design and development, it immediately benefits from numerous tools which are available to support systems design; this

products embraces many features all along the development chain, such as requirements management, code skeleton automatic generation, reports automatic generation,

- The validation tool is flexible in the sense that it allows that the system is partially validated: only part of the system elements would be subject to the OCL rules coming from the SALT process; there is thanks to this flexibility no need to define rules and constraints for all of the elements,
- However, the modelling tasks related to this system validation, even using widespread languages, are to be performed by specialists (system and software designers); this wouldn't probably make possible to train other disciplines specialists to the use of these tools. This means that specialists are needed for all the maintenance and update the validation tools: this typically consists of model and rules maintenance and evolution when new guidelines are set or existing guidelines are modified, Note that only the experts who add new content to the SALT repository need to know about OCL rules. Designers don't need to know about them. They use the rules for validating their systems designs, but this task is transparent for them, since it is carried out in the background by the automatic validator.
- There would be an advantage of providing a capitalization around a given project of the SALT modelling and validation tasks and steps performed; this would allow the multiple stakeholders implied to share and keep track of the validation steps; also a capability to comment freely the operations and choices performed (computerized tag with author identity management) would complement this project-related capitalization space.

3.2.5 Functional aspect

This section is dedicated to the evaluation of the whole SALT process and tools with regards to the WP5 use case; especially about the global approach it provides and about the interrelation between the tools.

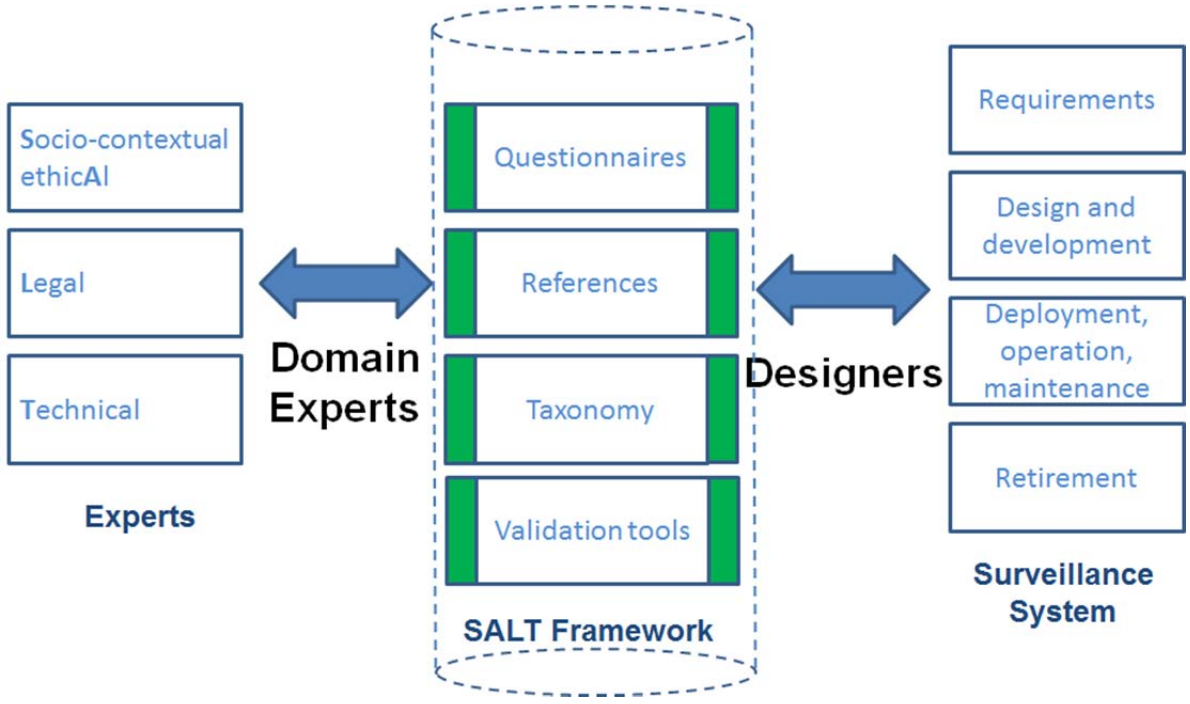


Figure 22: Overview of SALT framework within the ecosystem

According to Figure 22, the SALT tools are used by two types of users:

- Those who create the SALT raw contents (questionnaires, references, taxonomies, models); they are mainly experts of a domain addressed by the SALT framework,
- Those who use the SALT contents to optimize a surveillance system belonging to the same domain.

The barrier between these two populations of users is nevertheless permeable because an interdisciplinary communication is desirable during the lifecycle of the SALT framework contents: experts might be required to help designers on some precise points; on the other hand, designers might trig some specific issues that would inspire experts in the creation of new SALT contents. Some users may belong to both categories; this is especially possible regarding the technical contents of the SALT framework (likely to be found within any of the SALT tools); this is less likely to happen about legal and socio-contextual issues as the designer population is generally not skilled in these domains.

The set of tools available in the SALT methodology (the taxonomies, the questionnaire, the references, and the validation tools) appears loosely coupled. The taxonomy tool clearly lies independently from the other tools; the interdependencies that exist between the other tools are mainly:

- The questionnaire tool which is very likely, when filled, to cause the selection of one or several guidelines to meet the upstream expectations, needs, constraints that appear. It is important to note that this correspondence in the contents of the 2 tools is mainly manual (in the sense that it does not happen automatically thanks to the tools while using them)
- The SALT repository is also automatically linked to the modelling and validation tool as soon as there is a selection of a reference featuring OCL rules for the application of the guidelines to the domain-model.

Also it should be emphasized that the reference tool offers very wide flexibility in its use, and that 2 references can be very independent one from the other; it is even possible to imagine that on a given subject addressed (concretely we can think about providing solution to a privacy issue) concurrent references addressing very similar subjects are found. The end consistency resides in the choice performed by the stakeholder team dedicated to the use of the SALT tools on a concrete project.

From this global functional perspective, and from the experience gained within the WP5 of the PARIS project, the following evaluation statements are synthetized:

- The fact that the SALT tools are flexible and adaptable is a very important gain in their use; these tools are likely to be applied by stakeholders of very different mind-sets, culture and goals; they also provide knowledge in various forms that the SALT tools will help integrating easily. This flexibility enhances interdisciplinary interactions. A possible enhancement about the tools, that would even higher their interdisciplinary properties would be to add a FAQ (Frequently Asked Questions) enabling the “designers” population to request advice, help from the “experts” population.
- The SALT browsing capabilities are of key interest, as the volume of the SALT information is virtually unlimited. The fact that there is both free texts search (comparable to an internet search engine), and structured searches based on choices performed when knowledge is entered (geographical axis, privacy principles category, phase in the process), is very adaptable

and very powerful. It might be possible in addition to add something like expert system and/or natural-language search based search engines to even enhance these capabilities,

- The OCL rules that are (optionally) applied to a system design allow to validate aspects of the design choices performed; it could be of interest to provide a capability to add manually some more rules in order to reuse the SALT tooling process to integrate design constraints arising from other sources (although this would require the assistance of experts in both fileds, OCL rules and the new sources of information),
- There would at the end be a huge benefit in adding a project-space management capability, enabling to record and recover among a community of selected and authorized users the contents related to a given security project; a capability to comment the choices and operations performed would fit perfectly in such an environment.

3.2.6 Usability aspect

According to the general SALT compliant process description, the main **users** of the SALT framework include two groups:

- SALT experts, which include social, ethical, legal, and technical experts in the area of privacy, accountability, and surveillance system, who helps to continuously contribute multi-party concerns to the SALT repository in terms of SALT references, i.e., a structured and searchable representation of various concerns and corresponding solutions or answers. An integral part of the SALT repository is the questionnaire-based approach to cover the ethical dimensions. The questionnaires intends to foster stakeholders' thinking and decision. The content of the checklist and ethical questionnaires are initiated by SALT experts to generate self-questioning and eventually debate among stakeholders (cf. D2.3 Guidelines for use cases for SALT framework).
- Stakeholders, which include system owner, system operator, system user, system maintenance personnel, system designer, and system contractor, as well as public, individuals, data protection authority, representatives from civil society, and enforcement authorities (cf. D2.2 Structure and dynamics of SALT framework). If we align the stakeholders along a surveillance system lifecycle, they will include system proposer, system designer, system developer, system installer, system operator, and potential external auditor (cf. D4.2 SALT compliant processes definition).

Thus the usability aspect focuses on how an aforementioned user utilizes and interacts with the SALT framework. In software design and application development, user journey is one of the approaches to collectively describe a user's experience with a system. A thorough evaluation of the SALT framework would require the involvement of users and stakeholders at all level with different roles in a very large scale. This is however beyond the capacity of the consortium. Thus we use the perspectives of a technical expert and a system designer/developer to determine the added value of the SALT framework.

A major task of a technical expert is for the knowledge management of the SALT framework, which include providing initial knowledge input to the SALT repository according to the "template" specified by the consortium, and accessing and extending the knowledge in the repository to account for the evolving nature of privacy concerns. The former requires an expert to conduct a survey of the existing body of knowledge (BoK) on privacy and surveillance technology, under the guidance of the SALT template. The latter requires an expert to interact with the SALT repository using SALT management tools.

During the PARIS project, the SALT template has gone through several rounds of modification and refinement. The template elicits information from the experts and save it in the form of "SALT references". Therefore, the activities in the first stage of a technical expert is to collect, summarize, and represent the knowledge in a structured way, i.e., to fill the forms of the SALT references.

A SALT reference has the following fields (cf. D5.3 [3]):

Field	Type	Description
Reference name	Mandatory	Name that serves to identify the reference that should be as descriptive as possible. In case the references correspond to a law, an article, a report or any other official document, the name should be the title of that document. In case the original language of the reference is not English, the name should be indicated in two languages: English and the original language, both included in this field, and separated for example by an hyphen. Example: *Organic Law 15/1999 on the Protection of Personal Data - Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal*
Original language	Mandatory	Original language of the reference (this is intended to support another language apart from English, thus users may be aware of potential translation inaccuracies).
Abstract	Optional	Brief summary of the contents of the reference *(~ 100 words maximum)* In case the original language of the reference is not English, the «Abstract» must be in two languages: English and its original language. They will appear in two separate text boxes (they can be different fields).
Link to source	Optional	Link to the source of information in the original language
Link to translation	Optional	Link to the source of information translated to English
Official translation	Optional	[Yes, No] This field indicates whether the translation provided is official or not (thus users may be aware of potential translation inaccuracies).
System type	Mandatory	The system type to which the reference applies. *Possible values: Video surveillance systems / Biometric systems / All systems*
Geographical Scope	Mandatory	A first layer of context information, which will define the territorial scope of application. The SALT Framework Tool for the creation of references will provide a drop down list containing a set of predefined countries (by now, all the European countries and also the option "European Union" to cover all them). There is also the option "Any" for the cases where this information is not relevant for the reference (e.g. technical information).
Context	Optional	Additional layers of information based on the criteria used to define the material scope of application of the reference (*e.g. specific cases/conditions where the reference is applicable).*
Version	Mandatory	Version of the reference in the format vA.B. By default this field has the value: v0.1
Keywords	Optional	List of words or terms, separated by commas, that serve to highlight the most relevant aspects of the reference
Creator	Automatic	Person responsible for the creation of the reference in the SALT Repository *(automatically filled by the SF Tool)*

Last update	Automatic	Date and time of the last reference update *(automatically filled by the SF Tool)*
***List of concerns** (privacy and accountability related concerns for surveillance systems)*		
Concern ID	Automatic	Unique Identifier for the concern (generated automatically by the SF Tool)
Name	Mandatory	Title for the concern, which should give a brief idea of the contents or aspects covered by the concern. The concern should be some concrete information or aspect in the source text that is related to privacy/accountability and that can be relevant for surveillance systems. A text would probably include more than one concern. In case the original language of the reference is not English, the name of the concern should also be indicated in two languages: English and the original language, both included in this field, and separated for example by an hyphen. Example: Duty to inform - Deber de informar
Additional information	Optional	Extra information that helps readers find the concern in the source text.
Description	Mandatory	A textual description of each concern, thus anyone accessing the SALT reference can understand what the concern is about. It can contain a reference to a source with more detailed information regarding the concern: an internet URL (Uniform Resource Locator), a journal, a book chapter, etc.
Category	Mandatory	Category of the concern, that can be one or several among this options: *Legal, Socio-Ethical, Technical.*
SALT Topics	Mandatory	SALT legal topics addressed by the concern, that are based on the 95/46/EC Directive and that are intended to ease legal analysis and legal compliance checks.
Stage	Optional	Stage or stages of the SALT Process in which this concern applies. These are the stages defined and their goals: • **concept** (intention): selection of the most suitable solution to solve the stakeholder's problem; • **design**: elaboration of the system design according to the different requirements; • **development**: implementation of the system based on the defined specification; • **deployment**: set up the system in the stakeholder's environment; • **operation & maintenance**: use the system and ensure its correct functioning to satisfy stakeholder's needs; • **retirement**: shut down the system in a controlled manner.
Keywords	Optional	List of words or terms, separated by commas, that serve to highlight the most relevant aspects of the concern.
Guidelines	Optional	Any guidance on how to include the concern in the development of the system. This could be a concrete artefact or solution, a strategy or procedure, or just any tip about how to take this concern into consideration.
OCL Rules	Optional	One or several OCL rules that allow to verify that the system addresses the concern. The OCL expert needs to fully understand the meaning of the privacy/accountability concern for which the OCL rules are created. These rules will be used for the automated (or human assisted) validation of the concern it relates to, once its corresponding solution provided by the SALT reference has been implemented in the system design.

The template comes with instructions on what to consider during the filling out stage, such as the consideration of the coherent and reusability of all SALT references in the SALT repository. The expert also needs to consider different stages of a system development lifecycle, and

indicate them in the reference. Although a quality assurance is not explicitly defined in the project, the filled references are subject to internal reviews and improvements among the partners. Figure 23 illustrates this process.

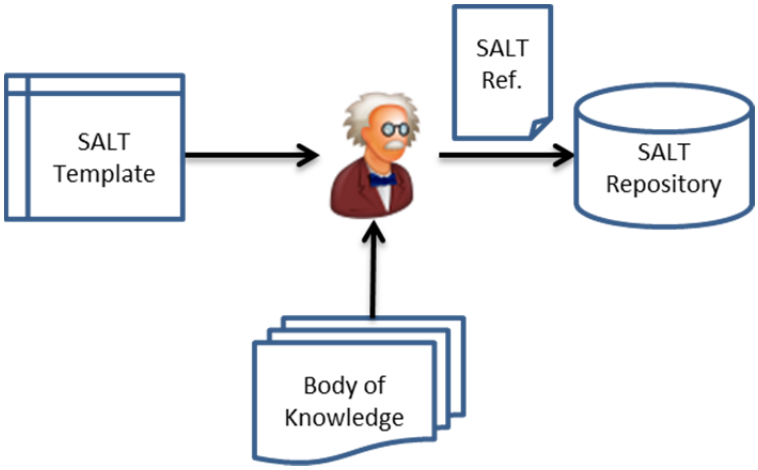


Figure 23: SALT knowledge input by expert

In actual implementation, the SALT template for content can be either a paper document or a web form, which is exemplified by the screenshot in Figure 24. A user must register and login into the SALT repository in order to fill out the references. The user experience is comparable to the interaction with an online portal, which is straightforward and common to most people. To an experienced Internet user, the SALT repository do not offer more advanced features such as auto suggestion, posting, discussion forum, conflict resolution etc. However, the basic function fulfils an expert's need to create and "publish" his/her concerns. In the same way, an expert can review and modify the content of a reference in the SALT repository.

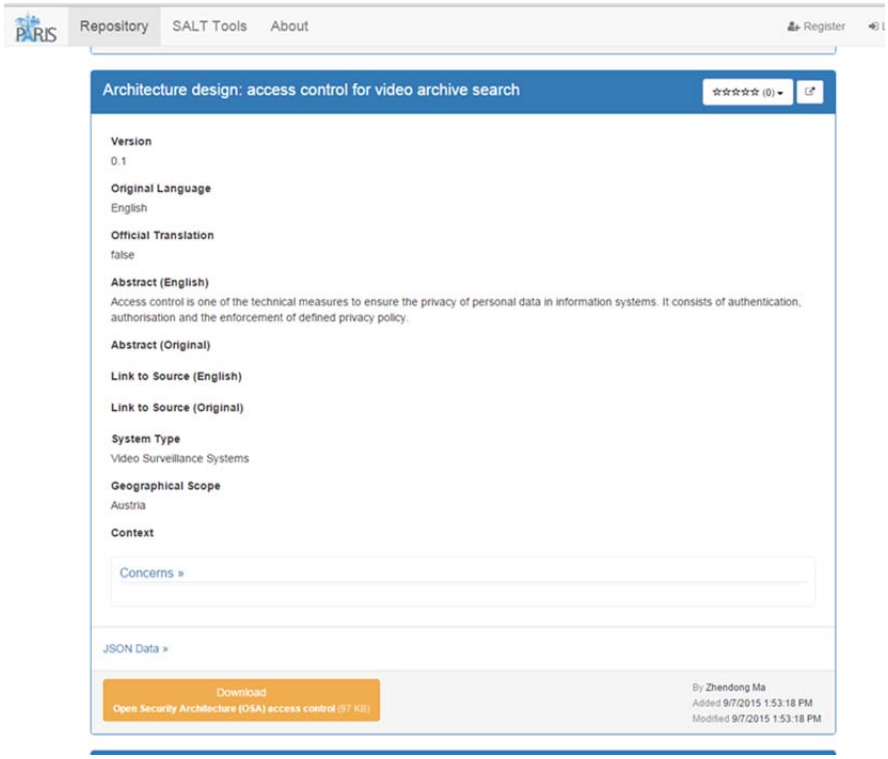


Figure 24: Web form for SALT reference in online SALT repository

The main interaction of a system designer (or developer) is to use the knowledge stored in the SALT references during the system design and development phase to ensure all privacy concerns are duly considered and addressed. To perform a system design, the designer searches and retrieves relevant SALT references from the SALT repository. The SALT repository provides the browsing and search function. A user of the SALT repository can conduct basic searches for certain key words contained in the references (see Figure 25).

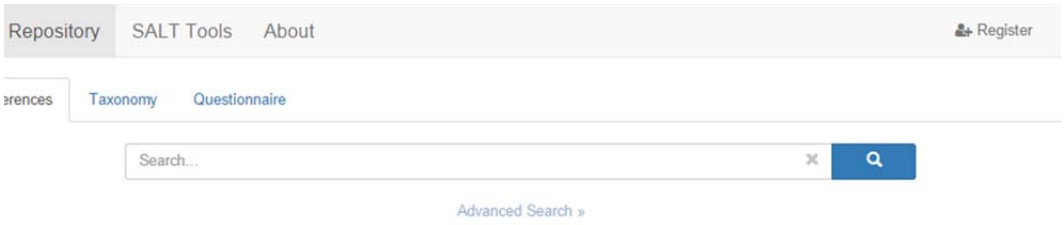


Figure 25: Basic search in SALT repository

An advanced search function provides more flexibility and accuracy in the search of related SALT references. As shown in Figure 26, a more granular search is based on certain fields. The designer can quickly find related concerns captured and represented in SALT references. Although as a proof-of-concept, the SALT repository does not contain many references. However, it is obvious that the search function can be very useful when the repository grows to a large scale.

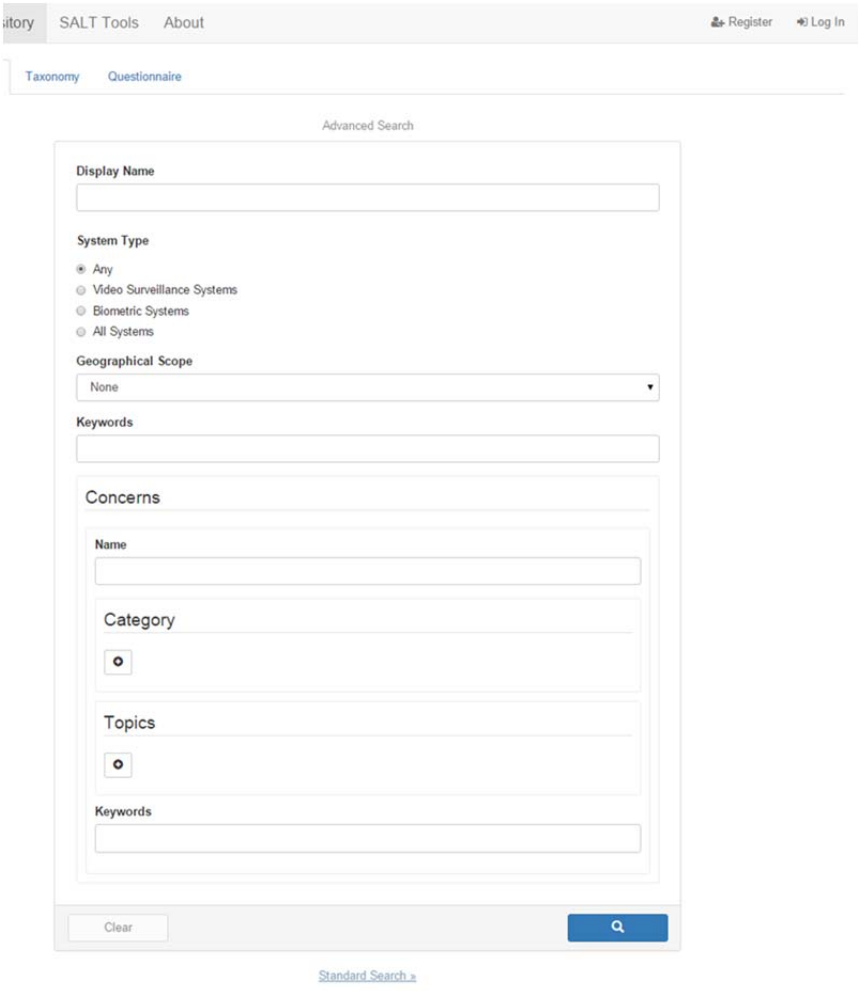


Figure 26: Advanced search in SALT repository

A designer needs to consider many issues at the same time, e.g., at system level, specific component level, software development level etc. The SALT references in the SALT repository provide guidance as well as concrete examples as how privacy can be preserved, from which a designer can carry out a new design accordingly. System design according to best practice is a common practice in software system engineering. For example, Microsoft creates and maintains a collection of software patterns and best practices for “predictable results”. Early research exploited the possibility of using security patterns for system security engineering. Website such as Stackoverlow.com allows question & answer based knowledge sharing among software developers. From a usability perspective, the SALT repository in this way is similar to these approaches to facilitate the reuse of existing body of knowledge and community-based knowledge sharing for privacy, which is familiar to most software system designers.

3.3 Evaluation at system level

This section evaluates the added value of the SALT framework and SALT compliant process, as well as the related SALT management tools against the video surveillance data management lifecycle use case developed in WP5. As mentioned in Section 3.1, the evaluation is a collection of subjective opinions gathered from experts from social, legal, and technical domain. For the evaluation of the conceptual framework, we focus on the lessons learned from multi-disciplinary work. For the evaluation of technical artefacts, we focus on how the technical requirements are fulfilled in the implementation.

3.3.1 Lessons learned regarding legal, Social-ethical, privacy & accountability aspect

From a legal perspective, while a large number of references were provided to cover the use case in WP5, the fact that the use case was limited to the design phase of the system restricted the application of the socio-ethical and legal concerns. To take the example of accountability measures that, as explained in D.2.4 [4], take different shapes depending of the domain approach and that will intervene at different moments of the process, only the technical domain seemed to provide relevant input for the design phase. The measures implemented were thus exclusively related to ensure the traceability and verifiability of the actions performed over the data (audit mechanisms). This resulted for example in the implementation of an access control policy or logging mechanisms.

This use case led us to clarify the role of the different domain approaches at different stages of the process. While the initial concept of the SALT framework relied on the idea that each domain should contribute to each phase of the process, it appeared clearly in the context of WP5 that this is not always the case for several reasons:

- Inputs from the ethical domain are often less relevant at this stage of the design process in this specific context. For example, in this particular case, the data controller responds to a legal obligation, leaving little possibilities to engage into a dialogue with relevant stakeholders other than on devising the best ways to comply with the legal framework.
- Inputs from the legal domain are only relevant as to clarify the extent of the legal obligation to which data controllers are subject to. Access to video surveillance system by law enforcement authorities is strictly regulated, thus leaving little margin of manoeuvre as of design choices. The reflexive process developed through WP6 questionnaire is for instance not possible in that context.

- Inputs from the technical domain had a clear and predominant role in providing the system designers with relevant artefacts to ensure the traceability and verifiability of the actions performed over the data.

Taking a global perspective to the SALT framework, the socio-contextual and socio-contextual and privacy/accountability contents appeared as the most complex to apprehend and to communicate and share within the whole stakeholder community. One reason is that it is less unequivocal than pure technical contents, and that it requires expert knowledge which is a bit less common compared to the technical one. Also the technical experts are often more numerous than the ones specialized in social sciences.

A strong multi-disciplinary interaction has arisen within the scope of the project, both when dealing with the transversal WPs (WP2 dedicated to the concepts of SALT frameworks, the WP3 dedicated to the SALT tools, and the WP4 dedicated to the SALT process) and within the application oriented WPs (WP5 and WP6), especially about Legal and Socio-Contextual aspects.

This interaction has led to several important results:

- a paper (to be published at this date) on specific multi-disciplinary interaction linked to the different field of knowledge implied within the design of a security-system,
- the inclusion of multi-disciplinary related features and tools within the SALT framework; these features and tools are the taxonomy tool, which is especially suited for a domain of knowledge to expose its raw principles and concepts; also the multi-dimensional categorization provided within the SALT references: any concept exposed within a reference has to be identified, referring to one or several key privacy principle and to a geographical area of interest (social sciences reference) and to a phase within the system development process, ranging from concept to retirement through deployment and maintenance (which is much more related to a technical point of view on the system).

Moreover, it appears that the versatility and flexibility provided by the SALT tools is especially suited (as explained within 3.2 Evaluation at the SALT Framework level) to the handling of several viewpoint, especially those rising from social sciences. The availability of tools with very different shapes (the questionnaire and the references) with numerous options enables to foster very different viewpoints: those related to the different fields of knowledge entering the playground, but also the different personal preferences within each field.

On the technical level, we notice that many solutions for privacy and accountability are closely related to information security. The lessons for us as technical system engineers are that information security controls such as encryption and access control consist of a big part of the privacy protection arsenal. These security controls implement privacy and accountability in surveillance systems and beyond. Therefore, security controls should be treated as a part of the technical building blocks in the design phase.

Furthermore, as shown in the CNIL privacy assessment methodology [5], privacy can often be approached using existing concepts and techniques from the field of information security. Although security and privacy are in many places different in their focus, priority, and mind-set, many privacy concerns and the consequent solutions are very similar to information security. For example, ensuring confidentiality is the basis for privacy. Keeping personal data confidential is both privacy and security problem. When data must be shared with third party, access controls can enforce privacy policies defined by the user or oversight bodies. To this date, there is no standard on comprehensive privacy controls at the technical level. Thus many existing security standards and best practices such as ISO 27000 series [6] or NIST 800-53 [7] are very

useful and necessary to systematically address the privacy issues at the system level. In our opinion, without considering information security, it is difficult to establish privacy at the technical level. Useful information security that is applicable to privacy and accountability in video surveillance systems include:

- Access control policies and procedures,
- Account/user management,
- Separation of duties,
- Identity management and authentication.

3.3.2 Technical aspect

This section is dedicated to the evaluation of a system from the technical perspective of the SALT tools, whereas a global feedback about the tools is given in Section 3.2 Evaluation at the SALT Framework level.

The evaluation is performed for each SALT tool:

- The taxonomies enable to provide knowledge to end users about important concepts at stake within the development process of security systems. From a technical perspective, this is of interest to raise awareness about very precise technical facts, performances; also this is used by the stakeholders community to share information (technical information with non-technicians, non-technical information with technicians),
- The references, which provide a structured way to virtually input any knowledge from any field; elements of knowledge are stored as concerns (atomic part of references) and these contents are tagged with multi-dimensional criteria (and free text and keywords); these criteria are mainly the geographical area of application, the privacy principle(s) at stake (if any), the stage within the design process. Also a reference can host some prescriptive statements about the systems (some requirements), that can be expressed in natural language, or in formal statements weighting on system model (OCL rules). From a technical point of view there is in this tool an important flexibility either to propose knowledge or design choices in an open way, or to express technical solutions. Providing the possibility to express guidelines within UML is clearly at the core of the technical usage of the SALT tools,
- The questionnaires, which provide open and flexible way to interrogate and raise awareness about issues regarding the system; being clearly multi-disciplinary and applied most of the time upstream in the design process of the security system, it provides outcomes that have impact on technical choices, but which are not in their final shape (the use of references in conjunction or as a consequence of the use of the questionnaire allows this refinement). Nevertheless, the questionnaire tool might also be used to provide RIA (Risk Impact Assessments, which can take an important technical dimension),
- The validation tool, which usage is optional within the SALT process; this tool is clearly addressed to technical stakeholders and especially useful when defining and developing the system. It is based on the most open and most worldwide used modelling approach (Unified Modelling Language), together with OCL rules.

The WP5 has been the occasion to use these tools in the context of the design of a video surveillance system, and more precisely about the upgrade of a (supposed) already existing video surveillance system.

WP5 use case is more related to the refurbishing, the refactoring of a surveillance system rather than the definition and development from scratch of a new system given an operational context and a mission (the WP6 addresses more precisely the design from the very beginning of a biometrics system). This specificity is of key interest from a representativeness point of view, as it is more than common that a video surveillance system is upgraded rather than deployed in a place where no previous system was already installed. In this case, as explained above, all the SALT tools are likely to be used, but with a prominent role given to the reference tool and to the validation tool: the questionnaire tool remains used for assessment of very precise points, but the full analysis regarding the choice of the type of the system is not performed in this case.

The global feedbacks that can be triggered from this exercise about technical features, functionalities and capabilities provided by the SALT tools are described below. They merely rely on what has been exposed above in this document (cf. Section **Error! Reference source not found.**3.2 Evaluation at the SALT Framework level).

- The tools provided within the SALT methodology can be seen as a complete portfolio enabling to address points of view of very different stakeholders; also these tools enable to manage different ways of inputting and representing knowledge. This appears key for the usage that is forecasted: to embrace the full deployment cycle of a surveillance system wherever in the world using any type of currently available or future technology,
- The SALT tools foster interdisciplinarity, which is a key strength especially when optimizing together of privacy/accountability and security properties. From a purely technical perspective, what is important in such a context is to be capable to perform informed choices and to make decisions about the system, while keeping track of these decisions,
- The SALT tools (available on the web), are easily accessible and globally user-friendly and easy to use. The search capabilities that are included (free text search, search based on attributes such as geographical zones and phase) are very well suited,
- From the point of view of the management of the technical requirements, the SALT portfolio provides very interesting and adapted capabilities which range from management of high-level or fuzzy requirements (outputs of SALT questionnaires, which are guidelines or preferences in natural language and SALT references guidelines more precise but which remain expressed in natural language) to directive and non-ambiguous rules applicable on the system model in UML. A value-added option would be the capability to add free guidelines (prescriptive or not) in order that other topics of interest within the design (other than pure privacy and security considerations) can be added,
- The use and the link with a model expressed in UML is a very interesting feature as this language and model bias is widely adopted; moreover, many other tools come with the UML models all along the design and development chain, such as code skeleton automatic generation, end-to-end traceability of requirements, automatic reports generation,
- A capability to build a project space that would be dedicated solely to a project of interest, featuring authorization capabilities, selection capabilities would be of great interest. A useful related feature would be the possibility to put computerized stickers within the space to inform about the choices made. The project space would facilitate report generation about the choices performed about the design of a security system using the SALT tools.

Envisioned to be a multi-disciplinary approach, a very important part of the SALT framework is to take into account privacy and accountability concerns manifested in the principle and policy level and translate them into actionable technical means.

On the technical level, the design of privacy-preserving surveillance data management lifecycle follows engineering process, including requirement, design to implementation and deployment. Therefore, for the evaluation of the technical aspects, we focus on how the technical requirements on privacy and accountability are addressed by the implementation of the use case.

An early version of the technical requirements is given in D5.1 Video Surveillance Lifecycle Management Use Case Description. The related technical requirements are given again below.

The following requirements are formulated based on the use case system architecture, which contains the backend Network Video Recorder (NVR) and the Video Archive Search (VAS) and the Privacy Preserving Access Control (PEAC) at the front-end. Note that the requirements in D5.1 are grouped into those for NVR, VAS, and the privacy control at both NVR and VAS.

Technical requirements on NVR	
Requirement ID	Description
RG_1.1	The NVR shall be capable to host I-LIDS video footages (full library) as H264 video streams
RG_1.2	The NVR shall be compatible with common off the shelves hardware and Operating system components
RG_1.3	The NVR shall be capable of responding to RTSP requests for video streaming
RG_1.4	The NVR shall be capable of streaming videos on an IP network as H264 over RTP
RG_1.5	The NVR shall provide an administrator interface enabling to monitor its operation
RG_1.6	The NVR shall provide a capability for an operator to visually inspect the videos that are recorded
RG_1.7	The NVR shall be capable of auditing the data that are recorded inside to check that the maximum storage time allowed for video is met
RG_1.8	The NVR shall be capable of replaying data faster than real time (e.g. As Fast as possible)
RG_1.9	The NVR shall be capable of handling operator login/password embedded within an RTSP request for authentication
RG_1.10	The NVR shall be capable of exporting video data within a standard video file format for external replay

Technical requirements on VAS

Requirement ID	Description
RG_2.1	The VAS shall be capable of treating common format videos
RG_2.2	The VAS shall be capable of applying several types of Video Content Analysis (VCA) algorithms, upon operator choice
RG_2.3	The VAS shall be capable of proposing to the operator an interface enabling to parameterize the VCA algorithms
RG_2.4	The VAS shall be capable of proposing to the operator an interface enabling to choose the video footages that are to be analysed
RG_2.5	The VAS shall be capable of displaying the results of the processing performed
RG_2.6	The VAS shall be capable of providing the capability to the operator to replay a video stream from one event detected by the processing
RG_2.7	The VAS shall be capable to be installed on a standard hardware and Operating System.
RG_2.8	The VAS shall be capable of handling operator login/password entered at login
RG_3.1	The VAS shall be capable to be authenticated as a valid system by the NVR
RG_3.2	The VAS and the NVR shall be interfaced using existing video data transmission protocols RTP, Payload H.264
RG_3.3	The VAS and the NVR shall be capable to negotiate speed control of the video streaming
RG_3.4	The VAS shall be capable to send to the NVR login information from the VAS operator

Technical requirements on the privacy control at VAS and NVR	
Requirement ID	Description
RUC1_1	There shall be a mean VAS side to authenticate the persons involved in the search
RUC1_2	There shall be a way on the NVR side to restrict access in terms of data origin, timespan and video content
RUC1_3	There shall be a way on the NVR side to log all actions of the user
RUC1_4	There shall be a way on the VAS side to log all actions of the user

RUC1_5	There should be no way to manipulate the loggings VAS side
RUC1_6	There should be no way to manipulate the loggings NVR side
RUC1_7	The VAS user shall be notified what access rights he has at the moment and notify the administrator if he tries to extend these rights.
RUC1_8	There shall be a way (essentially from NVR) to check the integrity of video recordings
RUC1_9	There should be a list of all technical interfaces of the software where data access can be performed
RUC1_10	There should be a list of all entry/exit points for data of the complete system

It should be noted that these requirements were specified in the early stage of the use case development. During the development of the use case, slight changes have been made as a result of interactions with other work packages, especially WP2, WP3, and WP4. The purpose is focused on the added valued of SALT framework, instead of developing another technical platform for video surveillance data management. In the following, we evaluate the use case and demonstration implemented in WP5 against the requirements, and specifications.

The following tables summarise the fulfilment of the requirements.

Requirement ID	Description of fulfilment
RG_1.1	The NVR is capable of importing and storing i-LIDS video footages in H.264 format.
RG_1.2	The NVR runs on Linux, which is compatible with common off the shelf hardware and OS. It is also successfully installed on the AIT server farms for development and testing.
RG_1.3	The NVR is capable of responding to RTSP requests for video streaming. RTSP port can be used stand-alone or as RTSP over HTTP for video streaming.
RG_1.4	The NVR is capable of streaming videos on an IP network as H.264 over RTP.
RG_1.5	The NVR has an administrator interface for accessing logging information.
RG_1.6	The NVR has GUI to browse and inspect all stored video clips.
RG_1.7	The NVR is capable of auditing the data that are recorded inside to check that the maximum storage time allowed for video is met. The GUI includes information of the storage time of each of the video footages.
RG_1.8	The NVR is capable to replay video in fast forward mode in a software video player.

RG_1.9	The NVR is capable of handling operator login/password embedded within an RTSP request for authentication. The request from VAS to NVR will establish a secure communication channel SSL and then the login/password is sent in an RTSP request. Only the request matching login/password will be granted certain operation at NVR.
RG_1.10	The NVR is capable of exporting video data within a standard video file format for external replay, which is compatible with French legal requirements for using video data as evidence.

The functional requirements on NVR, although not directly related to SALT evaluation, are the technical capabilities to underline a video surveillance data management. Fulfilment of the requirements is a prerequisite for a realistic demonstrator.

The next table summarises the fulfilment of the requirements on VAS.

Requirement ID	Description of fulfilment
RG_2.1	The VAS is capable of treating common format videos such as H.264, AVI, MPEG.
RG_2.2	The VAS is capable of organising a chain of connected vision modules. A module can be a Video Content Analysis (VCA) algorithm.
RG_2.3	The algorithms can be configured by an operator. The current configuration is done by editing a configuration file.
RG_2.4	The VAS is capable of listing available video footages using the PEAC GUI.
RG_2.5	The VAS is capable of displaying the results after performing the configured VCA algorithms.
RG_2.6	The VAS is capable of providing the video footages related to the detected event.
RG_2.7	The VAS is capable to be installed on a standard hardware and Operating System. It is installed on the AIT server farm for development and testing.
RG_2.8	The VAS uses PEAC for access control and system log in.
RG_3.1	The VAS is capable to be authenticated to NVR by predefined login/password pair.
RG_3.2	The VAS and the NVR are interfaced using existing video data transmission protocols RTP, and H.264
RG_3.3	The VAS and the NVR use pre-negotiated speed control of the video streaming. In the demonstration environment, they are installed on virtualized environment on the same physical platform.

RG_3.4	The VAS sends login/password to NVR. The local access control is managed by PEAC. In other words, the access control to NVR is delegated at VAS side.

Similar to the requirements to NVR, the functional requirements to VAS provide a technical basis for the functioning of a remote video archive search demonstration system.

Requirement ID	Description of fulfilment
RUC1_1	User authentication is enforced when log into VAS for performing search.
RUC1_2	The NVR can be configured, based on the username to restrict the access to certain video content.
RUC1_3	NVR can log all user actions. An administrator access is needed to access such information.
RUC1_4	The PEAC can be used to log user logins. We decide that it makes more sense to only log at the NVR side, as it is the source of the surveillance data access.
RUC1_5	As the logging function has moved to the NVR side, this requirement becomes obsolete.
RUC1_6	Only the user with administrator right is able to access the log data and make changes.
RUC1_7	The VAS use PEAC for privacy-preserving access control. The access control policy can be flexibly configured.
RUC1_8	The NVR has integrity check for direct video export for legal evidence.
RUC1_9	APIs are documented during the demonstrator development.
RUC1_10	The system is documented during the demonstrator development.

These requirements are directly related to technical measures to enforce privacy and accountability, which implement the high level policies and guidelines in SALT framework into software code. Fulfilling these requirements are the technical answers to the SALT framework. At the same time, during the specification and implementation of the requirements, the output is used as input to formulate SALT references and provide feedbacks for the work in SALT framework.

Most of the technical details are given in D5.3 “Video surveillance lifecycle management use case” that describes various technical aspects of the use case implementation.

3.3.3 Evaluation of design process

The standard design process proposed within the frame of the PARIS project is merely described in the Figure 10 and in the Figure 11 above in this document; the main steps at stake during all the phases of the lifecycle of a security system are identified in these generic processes.

In most of the cases, the process that will be followed will result from an adaptation of the SALT standard process, for many reasons, including:

- The existence within organizations of processes that pre-exist (large organizations like Thales decide and implement their own processes based on best of the breed practices and tools and also to the exact nature of systems that make their core activity),
- The fact that in many cases the development process is based on modern engineering and coding techniques which can be much less sequential compared to a simple “V-Cycle” standard linear process : extreme programming, agile processes are examples of processes more and more spread within the industry (for their increased productivity and adaptability) which are based on iterations of the whole conception, development and test cycle,
- In most of the cases, the responsibilities and stages described in the SALT process are shared between several organizations, which can be very different in their size or location. Standard sharing of the tasks on a big size surveillance project may at least imply:

    - The organization that will run the system
    - The organization that will act as prescriber of the system
    - A consulting company who will partially issue the specifications
    - A company that develops and installs the system
    - A company that maintains the system.

A simple illustration of the adaptability of the actual processes is given within this deliverable where a slight adaptation of the generic process is proposed (cf. Figure 12).

The SALT tools demonstrate a very important flexibility in their use and deployment. This is a key feature to allow coping with this versatility of the organizations and of their practices.

3.4 SALT framework added value

From a legal perspective, the main added value of the SALT framework was to provide the system designer with a clear overview of the different pieces of legislation applicable to the technology to be designed. This however requires the SALT expert to make comprehensive research and select the relevant provision applicable to the case. It allowed the system designer to select the most relevant artefacts to give effect to these provisions, specifically in terms of traceability and verifiability of the actions performed over the data.

From a system engineering point of view, thanks to the SALT framework, together with the whole SALT methodology, companies and institutions with existing production processes regarding to surveillance systems have the opportunity to increase their efficiency (and even their productivity) in relation to the privacy and accountability issues inherent to this type of systems.

Those companies willing to adapt their existing processes by the adoption of the SALT methodology (or even introducing the SALT compliant process from scratch, See D4.4. "SALT Compliant Processes General Guidelines"), will benefit from a series of added values, which are the main objectives of the entire PARIS project.

In first place, the SALT compliant process provides a structured work flow that enables the monitoring of a given surveillance system from the very beginning of its lifecycle (starting at the concept stage) until its end with the system dismantling and retrieval. And not only that, the adoption of the SALT compliant process ensures the user will know what to do, when to do it, and what tools to have at hand in order to provide a privacy-aware and accountability-aware

surveillance system. The final output will be what we called a SALT compliant system (see D4.4 "SALT Compliant Processes General Guidelines" for more details).

The SALT framework is the body of knowledge gathering all the privacy and accountability information for surveillance systems. It is physically materialized in the form of a digital data base called the SALT repository, becoming one of the most important (if not the most) tools of the SALT methodology. Here we can find all data relevant to surveillance systems that will be accessed during the different stages of the SALT compliant process. The use of this data, together with the appropriate tools ensures the achievement of privacy and accountability requirements that are not usually addressed in the design, implementation, deployment and operation of current surveillance systems.

The SALT framework tools and processes provide a large range of capabilities to address the design of a system taking into account very wide constraints and fostering the interaction of numerous stakeholders implied in the conception and design of the system.

The tools provide the possibility to address low-structured to high structured contents, with affirmative statements but also by raising questions to the stakeholders implied within the development of the system. It provides efficient means to take decisions about systems design and development within fuzzy environment and conditions. This is made possible also to interdisciplinary teams where interaction is especially needed to produce outcomes by balancing and arbitrating possible solutions. Privacy and accountability properties of a technical system together with the security level it provides are typically heterogeneous and interdisciplinary topics that the SALT tools and processes enable to address.

It could be added that the SALT tools and processes proposed are very generic and that they are not really tightly coupled to the privacy/accountability/security triad; they could be used in any domain where the development of a system is at stake with several viewpoints to integrate and balance.

From a technical perspective, the SALT framework raises a very interesting question: Is it possible to use computation power to assist human being to design privacy-preserving ICT systems in a more efficient and correct way? As a starting point, the SALT framework investigates the possibility to digitalize documents and provide them to system designers and engineers, such that the technical experts can quickly locate related information and re-use existing approaches for privacy purpose. Although the retrieved information is still subject to understanding and interpretation, the SALT framework and the SALT management tools simplify this process. The SALT framework provides a repository which can be used for eliciting, collecting, and storing knowledge from a broader range of experts. Although at this stage, the SALT repository is basically a document system that stores structured information; the references can provide basic information to system designers and engineers the way Wikipedia, stackoverflow.com [8], or other knowledge portal providing valuable information for privacy-by-design and accountability-by-design concerns. This is very useful for engineers, who are mostly not domain experts in legal and social issues, who get used to take functional and non-functional requirements and implement them into system designs and hardware and software.

As we stated in [9], privacy is multifaceted, subjective, and evolving. The definition and perception of public and private spaces are constantly shaped under social, political, legal, and cultural influences. The SALT framework can be a first step to build a knowledgebase for decision support to assist the understanding of common concerns in complex and evolving environments and to facilitate the decision-making process. The SALT compliant processes are associated with the SALT framework, which specify how to use the knowledge to support the design of video surveillance systems that integrate privacy and accountability from the start.

4. Recommendations for extension

From a legal perspective, the tools developed put great emphasis on the accountability mechanisms, thus on the traceability and verifiability of the actions performed over the data. Further work could focus on two additional aspects:

- The tagging of the data shared in order to ensure the traceability of the data when they enter the system of the third party. This would allow data subjects or supervisory authorities to verify whether the information is being used only for the purposes that motivated the sharing in the first place.
- Tools to facilitate the exercise of the right to access by data subjects. It has been shown that it is often difficult for data controllers to ensure access to the footage because of the amount of data that should be searched or the need to blur the persons that appear on the footage.

From a system engineering perspective, possible extensions to the PARIS project that could be taken into account for future works:

- The creation of a "project space" in the SALT repository. This would be intended to store al the references, questionnaires and artefacts related to a single surveillance project. In this way, only accredited personnel for the given system would have access to this project space (authors of the system model, users of a given company, etc.).
- Establishment of a third party authority in charge of the validation of the contents to be added to the SALT repository: SALT references, questionnaires, taxonomies. This entity would ensure the quality and accuracy of each data gathered within the repository.
- Establishment of links with public authorities in order to ensure the correctness and regular update of all mandatory restrictions regarding surveillance systems and privacy, at least from the legal perspective. This would ensure that every SALT compliant system is also fully compliant with the local laws.

During the development of the SALT framework, we investigate the possibility to apply knowledge engineering approach to collect, transform, and represent privacy-related information to knowledge. On an abstract level, the input of knowledge engineering is often textual documents such as legal, social studies and guidelines. The output from knowledge engineering is actionable knowledge for system design such as system requirements, policies, or other design artefacts. The current way of populate SALT framework is mainly done manually by domain experts. From a technical perspective, this approach can be extended to use computer and smart processing algorithms and methods for scalability. In our recent attempt [10], we investigate the possibility to apply content analysis to guideline documents on implementing privacy-preserving video surveillance systems to semi-automatically extract and formalize technical privacy policies. We test knowledge engineering method based on the example of content analysis for the extraction of privacy requirements from text or unstructured data such as regulatory documents or laws. The results derive business process models reflecting privacy requirements from text such as regulatory documents. Other knowledge engineering approaches such as text mining or natural language processing can also be used to automate the process of collecting knowledge into the SALT framework. A vast amount of information and literature related to privacy exists today. Computer-based approach to knowledge elicitation can assist human experts for scalability and efficiency to build up the SALT repository.

The SALT compliant process can also benefit from following the principle of secure development lifecycle (SDL). SDL focuses on integrating security considerations into existing software development lifecycle. The concept of SDL is that by considering security in design and implementation of software systems, one can develop secure and dependable systems that have minimal security vulnerabilities and flaws, and are more resilient against security attacks.

Most proposed SDLs are not intended to replace existing development lifecycle models. Instead, SDLs often define security activities that can be added to common development methodologies in a flexible way. The underlying lifecycle models in most SDLs can be traced back to the waterfall model and its variants, including the V-model, rapid application development, and prototyping.

Take NIST 800-64 [11] for example. The secure development lifecycle is defined by the National Institute of Standard and Technology; it is based on the waterfall model, including initiation, development and acquisition, implementation and assessment, operations and maintenance, and disposal phase. Each phase is associated with security activities and control gates. The control gates are used to verify that security considerations are adequately addressed. Activities and components addressing specific security risks are included as an integral part. The security components include milestones, deliverables, control gates, and interdependencies. Comparing and aligning the SALT process with the NIST SDL can be an interesting extension, since the NIST SDL is well-known for developing secure systems. Mapping activities defined in the SALT compliant process to NIST SDL can increase the applicability of PARIS results and the acceptance in the industry involved in systems development.

5 Conclusion

This is the last deliverable in WP5, Using SALT for video Surveillance data lifecycle management to evaluate the added value and relevance of the conceptual SALT framework and SALT compliant process, as well as to make recommendations for extensions of the framework management tool in the context of the use case.

Basically, in this document, we perform the evaluation with two focuses: an evaluation of the functions of the use case based on requirements specified in D5.1; and an evaluation of the added value by subjective opinions on the SALT framework, SALT management tools, and SASLT compliant process in the form of “lessons learned”.

Based on the personal experiences gained from developing the use case for video surveillance data management, we state our opinions regarding the SALT methodology and its components, including SALT taxonomy, SALT questionnaire, SALT repository, SALT reference, SALT validation tool, SALT management tool, and SALT compliant process. Besides, the functionality of the use case implementation is evaluated in relation to all aspects of the SALT framework.

The use case is about the access and use of video surveillance data from existing video surveillance infrastructure, which demonstrated how privacy and accountability can be integrated into security systems on the further usage of existing data.

We state our opinions on the SALT framework in different parts corresponding to different aspects of the framework, the management tools, and the compliant process.

We conclude that the SALT framework does integrate knowledge from different domains regarding privacy and accountability. The management tools provide the possibility to interact with the digitalised knowledge representation. Following the SALT compliant process, multi-disciplinary concerns can be integrated into the system design phase.

In addition to the evaluations, several directions for the extension of the SALT framework and the SALT management tool are proposed.

References

[1] Wikipedia: Evaluation, https://en.wikipedia.org/wiki/Evaluation

[2] ADVISE project, “D2.3 Identification of practices and procedures of compliance for the use of video surveillance archives”, 2012, available at: http://www.advise-project.eu/sites/default/files/content/ADVISE_D2.3_v3.4_newQ_no_diagram_final.pdf

[3] PARIS project, “D5.3 Video Surveillance Lifecycle Management Use Case”

[4] PARIS project, “D2.4 Guidelines for SALT Conceptual Frameworks v2”

[5] Commission Nationale de l’Informatique et des Libertés (CNIL), “Methodology for Privacy Risk Management,” 2012

[6] ISO/IEC 27000 series “Information technology — Security techniques — Information security management systems”

[7] NIST, “SP 800-53 Security and Privacy Controls for Federal Information Systems and Organizations,” 2013

[8] Stackoverflow.com, http://stackoverflow.com/

[9] Ma, Zhendong, Denis Butin, Francisco Jaime, Fanny Coudert, Antonio Kung, Claire Gayrel, Antonio Maña et al. "Towards a Multidisciplinary Framework to Include Privacy in the Design of Video Surveillance Systems," Annual Privacy Forum 2014.

[10] S. Rinderle-Ma, Z. Ma, and B. Madlmayr, “Using Content Analysis for Privacy Requirement Extraction and Policy Formalization,” 6th International Workshop on Enterprise Modelling and Information Systems Architectures, 2015

[11] NIST, “SP 800-64 rev.2 Security considerations in the system development life cycle,” 2008.

Appendix Comparison of Functionalities and KPIs of Existing Systems with PARIS' system

Introduction

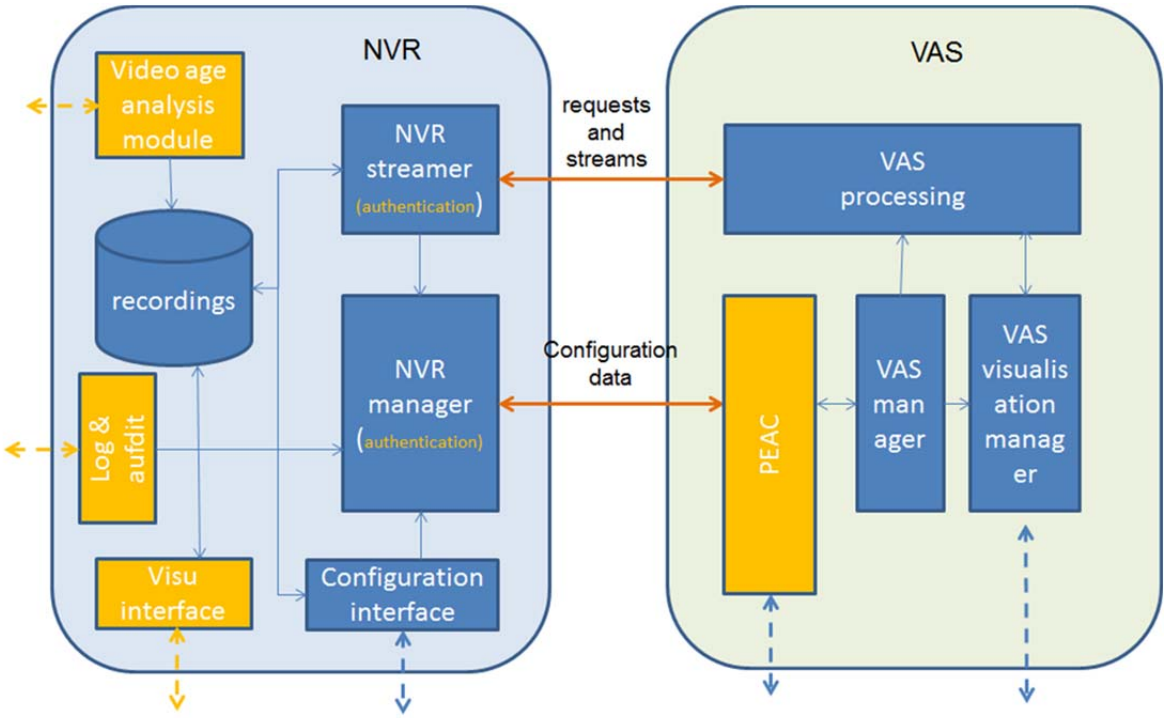
One of the recommendations from the interim review was that "the consortium should define unambiguous measures of success for the project against which assesses its progress". The changes to this deliverable have been discussed in the final review meeting, which include a table comparing the functionalities of existing commercial systems and PARIS' system; exploitation: transfer the content of a webpage by Trilog in the deliverable; stating explicitly the potential impact in standardisation (as discussed in the review meeting); quantify the expected exploitation of the project results; state how the framework has influenced (if it did) processes at Thales (internal) and Morpho (external).

This appendix addressed the first recommended change for comparing PARIS systems with existing commercial systems in order to access the progress of the project. The comparison is conducted to assess the progress of the PARIS project as a part of the consortium's effort for unambiguous measures of success of the project. The comparison is divided into two parts: the comparison of video surveillance systems and the comparison of biometric systems.

Video surveillance systems

The following figure shows graphically the differences of the PARIS system before and after the project. The system consists of two sub-systems. The sub-system at the left side is the Network Video Recorder (NVR) system developed by Thales. The sub-system at the right side is the video archive search (VAS) system developed by AIT as a research prototype. The system is developed as the application of the PARIS SALT framework. The main part of this deliverable gives the details of the design, development, and evaluation of the system.

As shown in the figure, the **blue** boxes are system components existed before the PARIS project, while the **yellow** boxes are system components added to the system during the PARIS project. These new components are intended for enhancing privacy to the existing system.



In addition, the following table shows the comparison of the PARIS improvements to existing commercial video surveillance systems.

Topic	State-of-the-art (SoA) commercial systems before the PARIS project	Improvements proposed within the PARIS project
Taking into account the privacy needs according to a given context	Not really possible within the commercial systems: they propose a set of operational and technical features that are of interest, but that are not at all flexible and adaptable to contexts (country of usage, public or private space)	Clear process to gather the needs for privacy/security related to video-surveillance systems within a given context; tools for proposing solutions to meet these needs within the whole design cycle.
Taking into account non-technical /non-functional properties of systems	Very few capabilities to address non-functional topics, such as organizational topics, awareness of stakeholders..	The video-surveillance system is considered globally encompassing all its dimensions
Taking into account much wider panel of stakeholders	Usually, the only difference taken into account within commercial systems is between operators and administrators	The process proposed within the PARIS project includes much wider stakeholders: the users, the authorities, the public, the designer.

Note: the SoA considered here for commercial systems is related to the most commonly distributed video-surveillance systems, typically represented by the following suppliers and products:

- MILESTONE systems, distributing the Xprotect product,
- GENETEC distributing the Omnicast product,
- VERINT distributing the EVMS product.

Biometrics KPIs: False Accept Rate (FAR) and False Reject Rate (FRR) of the biometric system

1.1 Introduction

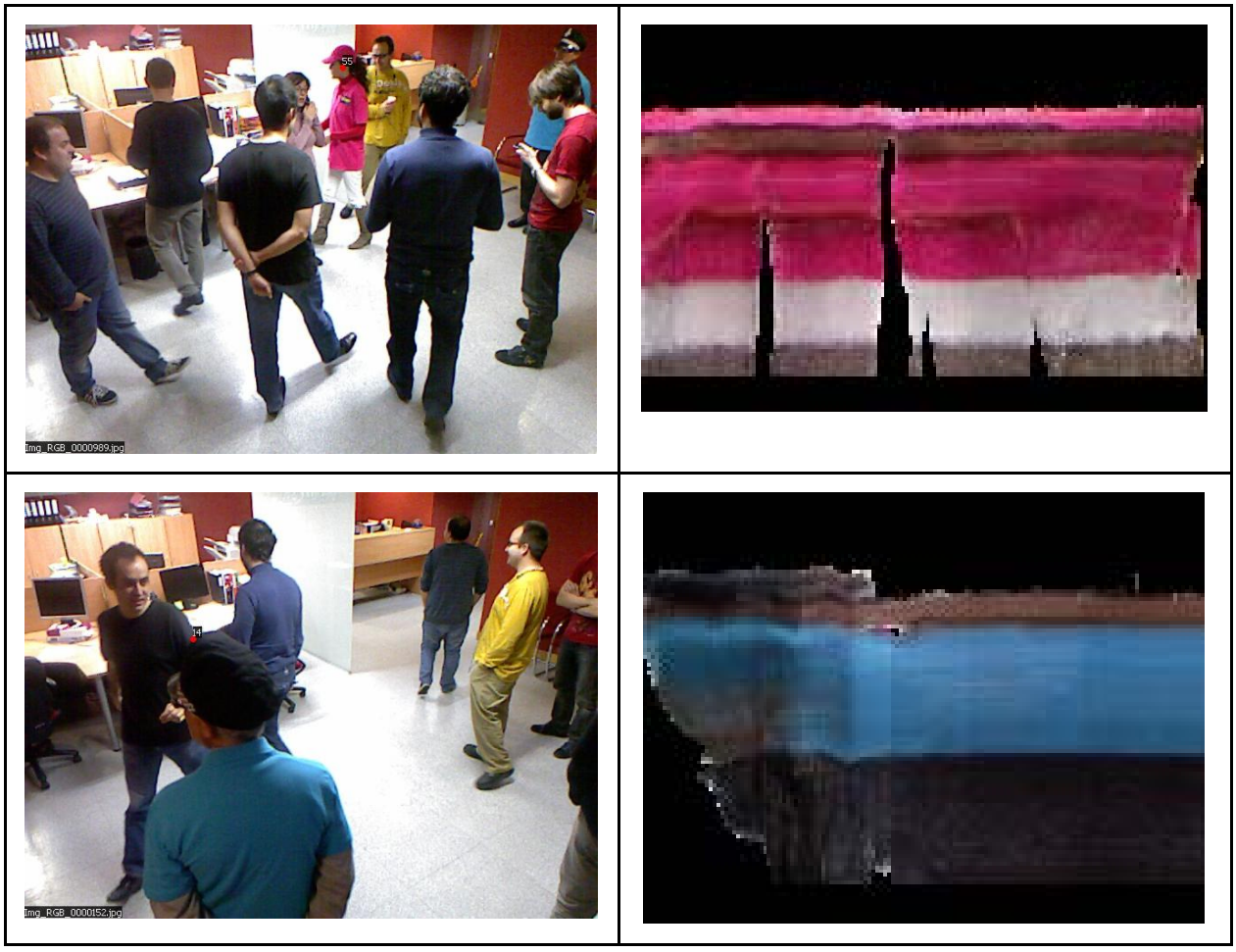
During Paris Project we worked in the specialization of the SALT framework for biometric systems. This specialization involved among other things (control layers, support profiles, socio-political, anthropological and legal artifacts …) the usage of some technology building blocks with a focus on biometrics. One the them was a re-identification algorithm used for extracting the bodyprints.

As is is mentioned in the rest of the deliverables related to the demonstration, the idea behind the biometrics use case was to apply all the SALT recommendations and the SALT process to a prototype for the detection of unauthorized people in a private office with access restrictions located in Spain.

The idea behind the re-identification algorithm comes from the availability of the information provided by the Microsoft Kinect sensor, where each pixel has an associated RGB and depth information.

With this information combined we can create a kind of people descriptor based on the color appearance at different heights, this allow us to discriminate between people wearing similar clothes as long as their height is different.

Below, some images captured from Kinect sensor and its signature used to obtain the bodyprints.



In order to take into account a recommendation from reviewers, related to the performance and the false alarms of the algorithm, we have made this annex **detailing some tests, together with the results and our conclusion**.

1.2 FAR and FRR

The False Accept Rate (FAR): It is the probability that a biometric system will incorrectly identify an individual or will fail to reject an impostor. It measures the percentage of invalid inputs which are incorrectly accepted. It is also known as the false positive rate.

The False Reject Rate (FRR): It is the probability that the system produces a false reject. A false reject occurs when an individual is not matched to his/her own existing biometric template. It is also known as the false negative rate.

1.3 Description of the experiment

We made some tests with the version of the algorithm we used for the final demo.

1.4 Bodyprint Objects

For the tests we used two videos recorded with Microsoft Kinect in the Madrid office of Visual Tools:

- Hall_entrada (Entrance Hall)
- Hall_interior (Interior Hall)

With each video we created a separate object for the analysis by bodyprints:

- BP1 → hall_entrada (Entrance Hall)
- BP2 → hall_interior (Interior Hall)

File structure of each "bodyprint object":

- **bpX**:
  - **analyzer/**
    - **groundCal/**: Camera calibration files
    - **tracks/**: bodyprints of detected persons
    - <other configuration archives>
  - **images/**: folder with the images and depth information
  - **bp_analyzer**: scripts for launching the analyser
  - **bp_status**: flag for managing the analysis

For each object we created a script that allows to easily manage the analysis:

```
#!/bin/bash
# $1: command "start" or "stop"
# kheight -q: no mostrar display
if [[ $1 = "start" ]]; then
     echo "2001" > ~/c1
```

```
        echo "ANALYSING"> bp_status
        value=$(<bp_status)
        cd analyzer
        rm -rf tracks/*
        while [[ "$value" == "ANALYSING" ]]; do
              cd ../analyzer
              kheight -t ~/c1 1> /dev/null &
              cd ../images
              filevideoserver   -t   ~/c1   -D   listadepths
        listaimgs 1> /dev/null
              value=$(<../bp_status)
        done
  elif [[ $1 = "stop" ]]; then
        echo "STOP"> bp_status
        killall -9 kheight
        killall -9 filevideoserver
  else
        echo
        echo "Wrong option, allowed commands: start, stop"
        echo "Syntax: ./bp_analyzer <command>"
        echo

  fi
```

1.5 Authorized Personnel Database

Among all the people who appear in the images we have selected the following persons in order to add them to the authorized database:

1. **Person 1: db_0013**

2. Person 2: db_0014

3. **Person 3: db_0036**

1.6 Comparison

We used the shell script *compareFeatures* (kinect/mains/) in order to compare the features of the different bodyprints.

Usage:

```
$ compareFeatures <track> *
   ➢ <track>: Candidate bodyprint
   ➢ *: Bodyprint with which you want to compare the <track> or "*"
     if you want to compare it with all the tracks of the current
     folder
```

This program returns a list correlations between the candidate and the samples available in the database, and selects the most similar one. Example result of *compareFeatures*:

```
0001 <---> 0019 ::::: 0.3626 ::::: dy= 2.55 dist= 3.01 duration= 404
Height = 160
0001 <---> 0041 ::::: 0.4002 ::::: dy= 2.2 dist= 2.2 duration= 124
Height = 156
```

```
0001 <---> 0039 ::::: 0.5036 ::::: dy= -1.2 dist= 1.21 duration= 30
Height = 150
[...]
Query : 0001 dy= -1.54 dist= 1.55 duration= 20 Height = 136
Winner: 0039 dy= -1.2 dist= 1.21 duration= 30 ::::: Corr= 0.503629
```

In order to simplify the comparison with the results of the different objects and in order to parse the results, we have created a small piece of software in python. The script is the responsible of running *compareFeatures* for comparing one by one all the tracks generated during the analysis with the ones in the authorized personnel database.

This python program parses the results and prints on the screen only the most suitable candidate along with its correlation and confidence. We also added a threshold value in order to consider whether the comparison is good enough based on the correlation value (DB_TH).

With all this information a "matcher" object is created for comparison, with the following structure:

- **Matcher:**
  - **auth_db/**: folder with bodyprints of the authorised personnel
    - 0013/: bodyprint of the fellow 0013
    - 0014/: bodyprint of the fellow 0014
    - 0036/: bodyprint of the fellow 0036
    - [...]
    - nnnn/: bodyprint of the fellow nnnn
  - **tracks/**: folder for the comparisons
  - **compare.py**: Python program for the comparison management

1.7 Steps of the experiment

1. The analysis for different objects is executed in order to generate all bodyprints (tracks) of people detected in the images (*./bp_analyzer start*)
2. Fellows who are part of the database of authorized staff are selected (*auth_db*).
3. The comparison script is launched (*python compare.py*)

2 Results

Based on previous experiences a value of 0.7 is selected for the decision threshold (DB_TH).

2.1 Entrance Hall

Video	hall_entrada
DB_TH	0.7
Comparisons	90*
Fails	1

*: Comparisons with samples taken for the database of authorized personnel have been removed

2.1.2 Successes

- Comparing track: 0074
- Match found: db_0013 Correlation: **0.716186** Confidence: None

- Comparing track: 0049

- Match found: db_0013 Correlation: **0.746116** Confidence: 6.06

- Comparing track: 0100
- Match found: db_0036 Correlation: **0.96777** Confidence: None
- Comparing track: 0055
- Match found: db_0013 Correlation: **0.881677** Confidence: 3.43
- Comparing track: 0086
- Match found: db_0013 Correlation: **0.860446** Confidence: 6.75
- Comparing track: 0071

- Match found: db_0013 Correlation: 0.780637 Confidence: 5.42

- Comparing track: 0014
- Match found: db_0036 Correlation: **0.976078** Confidence: None
- Comparing track: 0077
- Match found: db_0013 Correlation: **0.862459** Confidence: 4.88
- Comparing track: 0107
- Match found: db_0036 Correlation: **0.976667** Confidence: None
- Comparing track: 0110

- Match found: db_0036 Correlation: **0.859415** Confidence: None

  - This case is worth to be noted because the individual shown in the image db_0036 is hatless, and still is credited with a quite high correlation value

- Comparing track: 0096
- Match found: db_0036 Correlation: **0.919296** Confidence: None
- Comparing track: 0006
- Match found: db_0036 Correlation: **0.869115** Confidence: None
- Comparing track: 0063
- Match found: db_0036 Correlation: **0.965469** Confidence: None
- Comparing track: 0028
- Match found: db_0013 Correlation: **0.903537** Confidence: 3.65
- Comparing track: 0039
- Match found: db_0013 Correlation: **0.806456** Confidence: 5.42
- Comparing track: 0076

➢ Match found: db_0013 Correlation: 0.794132 Confidence: 4.32

➢ Comparing track: 0085

➢ Match found: db_0013 Correlation: **0.880864** Confidence: 6.11

2.1.3 Failures

➢ Comparing track: 0072

➢ **No match. Result most approximated: db_0013 Correlation: 0.600885 Confidence: None**

- In this case the algorithm hits with the most approximate result but the correlation is below the threshold.

2.2 Interior Hall

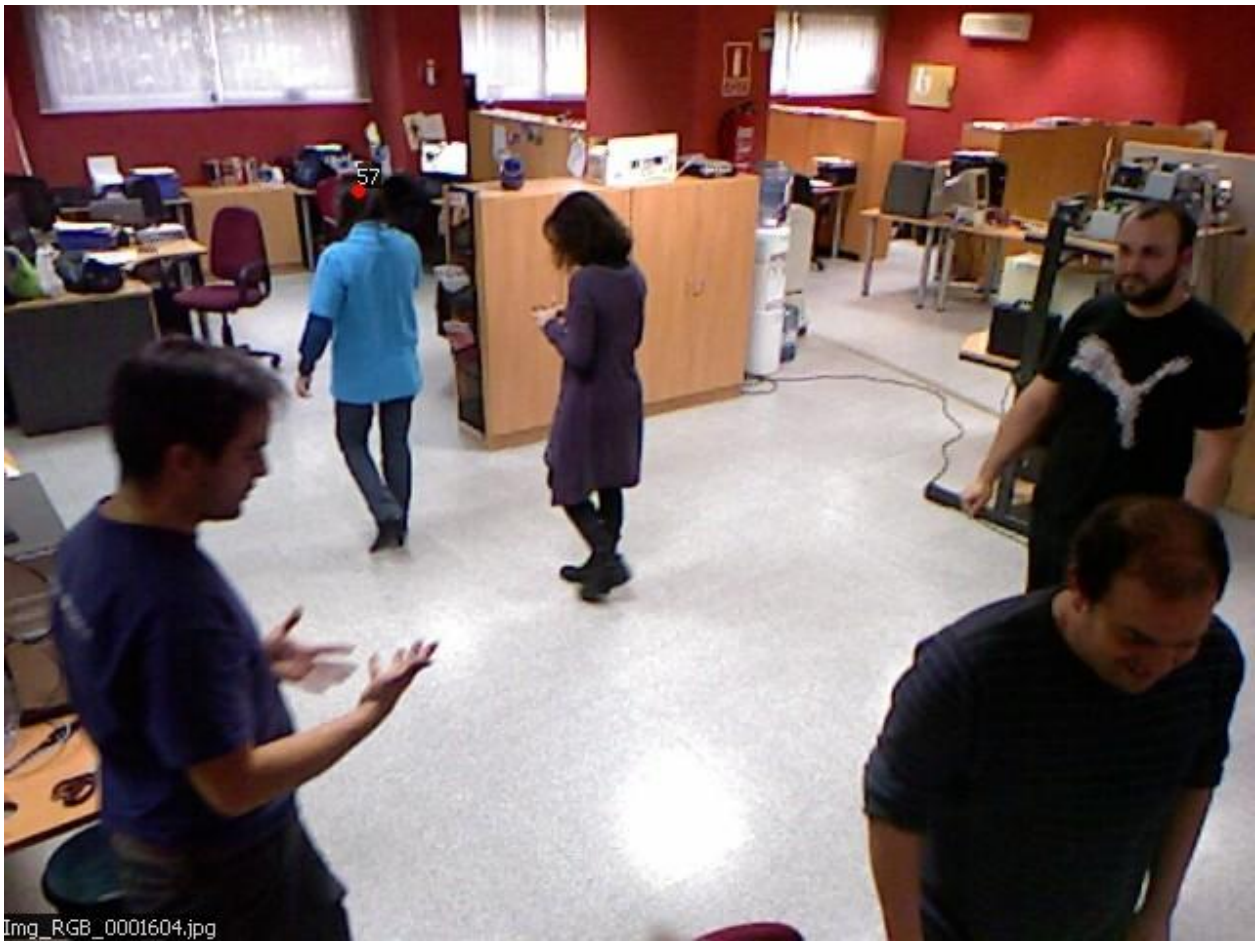
Video	hall_interior
DB_TH	0.7
Comparisons	50*
Fails	0

*: Comparisons with samples taken for the database of authorized personnel have been removed

2.2.2 Successes

- `Comparing track: 0049`
- `Match found: db_0013 Correlation: **0.967188** Confidence: 3.7`
- `Comparing track: 0024`
- `Match found: db_0014 Correlation: **0.72002** Confidence: None`
  - Interesting case because the person is not facing the camera

- Comparing track: 0054
- Match found: db_0014 Correlation: **0.82142** Confidence: None
- Comparing track: 0033
- Match found: db_0014 Correlation: **0.881508** Confidence: None
- Comparing track: 0057
- Match found: db_0014 Correlation: **0.836673** Confidence: None
    - Also an interesting case because the person is far from the camera and is not facing it



- Comparing track: 0027
- Match found: db_0013 Correlation: **0.990691** Confidence: 4.05
- Comparing track: 0025
- Match found: db_0013 Correlation: **0.934105** Confidence: 4.7

3 Conclusion

The value 0.7 selected for the threshold seems the most suitable one.

The results seems quite good. For example, It is interesting that the algorithm never confuses the individual db_0014 with db_0036 although dressed similarly.

As a summary, we are going to answer two questions which were also answered in the deliverable D6.2 and which summarised the result of the evaluation and also our point of view.

3.1 What is the False Accept rate and False Reject Rate of the biometric system?

In order to answer this question we have performed different tests to determine if the approach based on bodyprints is effective enough for the goal pursued:

3.1.2 Technology testing in a laboratory environment

This test served to evaluate the bodyprints algorithm for re-identification, with these results:

- The **average correct re-identification performance obtained was 93% (IR)** with bodyprints obtained always from the same view (frontal or rear).
- The **average correct re-identification performance obtained was 55% (IR)** with bodyprints obtained from any view (frontal or rear). The main problem here was the existence of logos in the clothes that appear in one view but not in others, which increased the number of false negatives.

3.1.3 Scenario testing

We have carried out several tests in a controlled scenario with conditions that are similar to the environment where the system was be installed, in which the test system tries to recognize people wearing uniforms:

- The **average correct re-identification performance obtained was 98.5%,** with bodyprints from different views. We could also observe that the system distinguished perfectly different people wearing the same uniform.

3.2 Is this FAR and FRR acceptable? Why?

The evaluations showed a good performance of the bodyprints algorithm for the recognition of people wearing uniforms under conditions similar to the scenario where the system was deployed.

Besides, the biometric system is aimed to be an aid in the surveillance tasks of security guards, which means that whatever the results of the recognition process, **there will be a human verifying the alarms, so the impact of a failure in the matching process can be reduced or mitigated**.

In the different tests carried out, most of the errors during the matching were false negatives, that means that the system didn't recognize a person whose bodyprint was stored in the

template database. This type of errors will make the defined biometric system to generate an incorrect alarm, that will be discarded by the system operator in charge of monitoring the office, so this type of errors are acceptable.

In the proposed scenario, the main risk in the recognition process is obtaining a false positive, meaning that an unauthorized person has been classified by the system as authorized. In light of the results of the tests performed, this type of errors are least likely to occur. Moreover, the matching is performed several times for each person appearing in the scene, increasing the probabilities of detecting correctly an unauthorized person.

Finally, in order to detect inaccurate bodyprints stored in the template database (APDB), the number of false negatives for each bodyprint stored in the APDB are monitored.