PrivAcy pReserving Infrastructure for Surveillance

Deliverable D5.1
Video Surveillance Lifecycle Management Use Case Description

Project:	PARIS
Project Number:	SEC-312504
Deliverable:	D5.1
Title:	Video Surveillance Lifecycle Management Use Case Description
Version:	V1.0
Data	13/06/2014
Confidentiality:	Public
Editors:	Zhendong MA (AIT)
Contributors:	Zhendong MA, Bernhard STROBL, Christian WAGNER, Stephen VEIGL (AIT) Mathias BOSSUET (THALES) Francisco JAIME (UMA)

Part of the Seventh Framework Programme
Funded by the EC - DG INFSO

Table of Contents

List of Figures

List of Tables

Document History

Version	Status	Date
V0.1	Initial	15/02/2014
V0.3	Intermediate	02/06/2014
V0.9	Ready for review	11/06/2014
V1.0	Final	13/06/2014

Approval		
	Name	**Date**
Prepared	Zhendong MA, Bernhard STROBL, Christian WAGNER, Stephen VEIGL (AIT) Mathias BOSSUET (THALES) Francisco JAIME (UMA)	11/06/2014
Reviewed	Marioli Montegegro Molina (UMA) María Cinta Saornil Gómez (VT)	12/06/2014
Authorised	Zhendong Ma	13/06/2014

Circulation	
Recipient	**Date of submission**
Project partners	11/06/2014
European Commission	13/06/2014

Executive Summary

D5.1 “Video Surveillance Lifecycle Management Use Case Description” aims to integrate video archive and search technology in the SALT conceptual frameworks and to specify the use cases for video surveillance lifecycle management. In this deliverable, we describe technology and concerns of video surveillance system and archive search from a technical and functional point of view. Under this context, we further include measures for privacy-enhancement and the selection of specific knowledge to be chosen from the SALT framework.

The rest of the deliverable specifies the use case scenarios and a system platform, which will be further developed and implemented for demonstrating SALT capabilities and evaluating the feasibility of the SALT framework and other conceptual work developed in WP2-4.

Abbreviations and Definitions

Abbreviation	Definition
CCTV	Closed Circuit TeleVision
CIA	Confidentiality, Integrity, and Availability
DPA	Data Protection Authority
DPO	Data Protection Officer
EU	European Union
GUI	Graphic User Interface
ICT	Information and Communication Technologies
IdP	Identity Provider
IETF	Internet Engineering Task Force
I-LIDS	Imaging Library for Intelligent Detection Systems
IP	Infrastructure Provider
IPSec	Internet Protocol Security
LDAP	Lightweight Directory Access Protocol
LEA	Law Enforcement Agency
NVR	Netowrk Video Recorder
OSI	Open Systems Interconnection
PARIS	PrivAcy pReserving Infrastructure for Surveillance
PbD	Privacy by Design
PC	Personal Computer
PDP	Policy Decision Point
PEP	Policy Enforcement Point
PIA	Privacy Impact Assessment
PO	Police Officer
RTP	Real-time Transport Protocol
RTSP	Real-Time Streaming Protocol
SALT	Social-contetual, ethicAl, Legal, Technical
SAML	Security Assertion Markup Language
SO	System Operator
SOA	Service Oriented Architecture
SSL	Secure Sockets Layer
SSO	Single Sign-On
TLS	Transport Layer Security
UI	User Interface
UK	United Kingdom
VAS	Video Archive Search
VMS	Video Management System
WPF	Windows Presentation Foundation
XACML	eXtensible Access Control Markup Language

1. Introduction (AIT)

1.1 Objectives and Scope

The objective of Work Package 5 "Using SALT for video surveillance data lifecycle management" is to apply the SALT framework and the design process for video surveillance data lifecycle management. This will serve to

- **demonstrate** the application of the SALT framework and guidelines (WP2), SALT management tools (WP3), and SALT processes (WP4), to address privacy and accountability capabilities in video surveillance data lifecycle management,
- and **evaluate** the SALT Framework to provide feedback to help the fine-tuning of the framework development in WP2-4.

The objective of this deliverable, D5.1 "Video Surveillance Lifecycle Management Use Case Description", is to integrate video archive and search technology in conceptual frameworks (Task 5.1), and to specify video surveillance lifecycle management use case (Task 5.2).

The objective of Task 5.1 is to enrich the SALT conceptual framework with specific description of technology artefacts related to video data life cycle management in surveillance systems. The conceptual framework must integrate the functional viewpoints (i.e. which surveillance capability), the technology viewpoint (i.e. search and processing features), and the constraints for private/public balance (i.e. constraints during the video data life cycle). The following activities will be performed in this task:

- Collecting today's technology on video data life cycle
- Characterisation of the technologies

The objective of Task 5.2 is to define the video access use case to be demonstrated. The following activities will be performed:

- Selecting the data from SALT framework to be used
- Specification of the surveillance capabilities
- Specification of the platform to be used
- Procurement of the various elements needed for the use case
- Specification of the criteria for evaluation, at the SALT framework level and at the design process level.

In summary, the main tasks in this deliverable include the collection of technology foundations related to video surveillance system and video archive search, selection of related SALT framework artefacts, specification of the use cases for the demonstration activities and the definition of the system architecture and requirements, as well as the specification of evaluation criteria for the use cases and for SALT framework.

1.2 Overview of D5.1

D5.1 reports the research work that fulfils the objectives defined in Section 1.1.

In Section 2, we first provide a technical and functional view on the technology related to video data life cycle. Specifically, we focus ourselves on common considerations for video surveillance system design and video archive search. We list various technical possibilities and issues related to video surveillance, including the characterisation of video surveillance technologies and surveillance capabilities. Section 2 is envisioned to be the domain-specific knowledge, which can be captured and stored in the technical dimension of the SALT framework. It also provides detailed options during design time, which can be used for capturing design process for video surveillance.

Section 3 extends the surveillance technical and functional view from Section 2 to include privacy and accountability aspects. This section elaborates the concerns and technologies on privacy in surveillance and video archive search technology, which links the “pure” video surveillance system to the integration and optimisation of privacy and surveillance capabilities into the SALT framework. It includes how privacy and security issues are meant and addressed in video surveillance and information systems, from a technical point of view. The last subsection discusses how these technical considerations can be coupled with the SALT framework.

Section 4 proposes two scenarios for the demonstration of SALT framework. The scenarios may give rise to a set of use cases. At this stage, we only define one use case for each scenario. The scenarios and use cases reflect the “realistic” demands from the market and the stakeholders of video surveillance systems. The use cases are chosen because we regard them as very representative for demonstrating the conceptual work of the SALT framework to address realistic problems.

Section 5 specifies the demonstration platform which will be used to implement the use cases. The platform combines the system components and capabilities from both AIT and THALES. We anticipate that the use cases will be developed in an iterative and dynamic way, i.e. the use cases will provide technical input to SALT conceptual work on how surveillance system and archive search technology work, the SALT conceptual work will influence how we integrate the framework in the use cases. Therefore, in D5.1, we define the system platform without all extensive technical details. More details will be defined in the next deliverable (D5.2) in an iterative process.

Section 6 and Section 7 specify the high level requirements of the demonstration platform, as well as the requirements and criteria for evaluating the SALT framework with the use cases. The requirements and criteria in these two sections provide a baseline for the work in future steps.

Section 8 summarizes D5.1.

2. Technical and Functional Viewpoint

This section provides a technical description of video surveillance system and video archive search. It also concludes design choices typically involved in the technical design and development phase.

2.1 Video Surveillance System

From a functional viewpoint, the main components of a video surveillance system are:

1. The camera, which produces one or several video-stream(s), and possibly some additional information (health, alarms). The camera is here supposed to be connected via IP technology.
2. The network link between the camera and the rest of the system.
3. The Network Video Recorder that records the streams.
4. The Video-Management System, that realizes central operations such as authentication, priority management, and authorization.
5. The Video Content Analysis and Archive search servers.
6. The operator stations, that provides access to the streams to the operators.
7. The network link between the system and the operator stations.

The typical design of a video surveillance system can be provided by a MILESTONE system architecture as shown below.

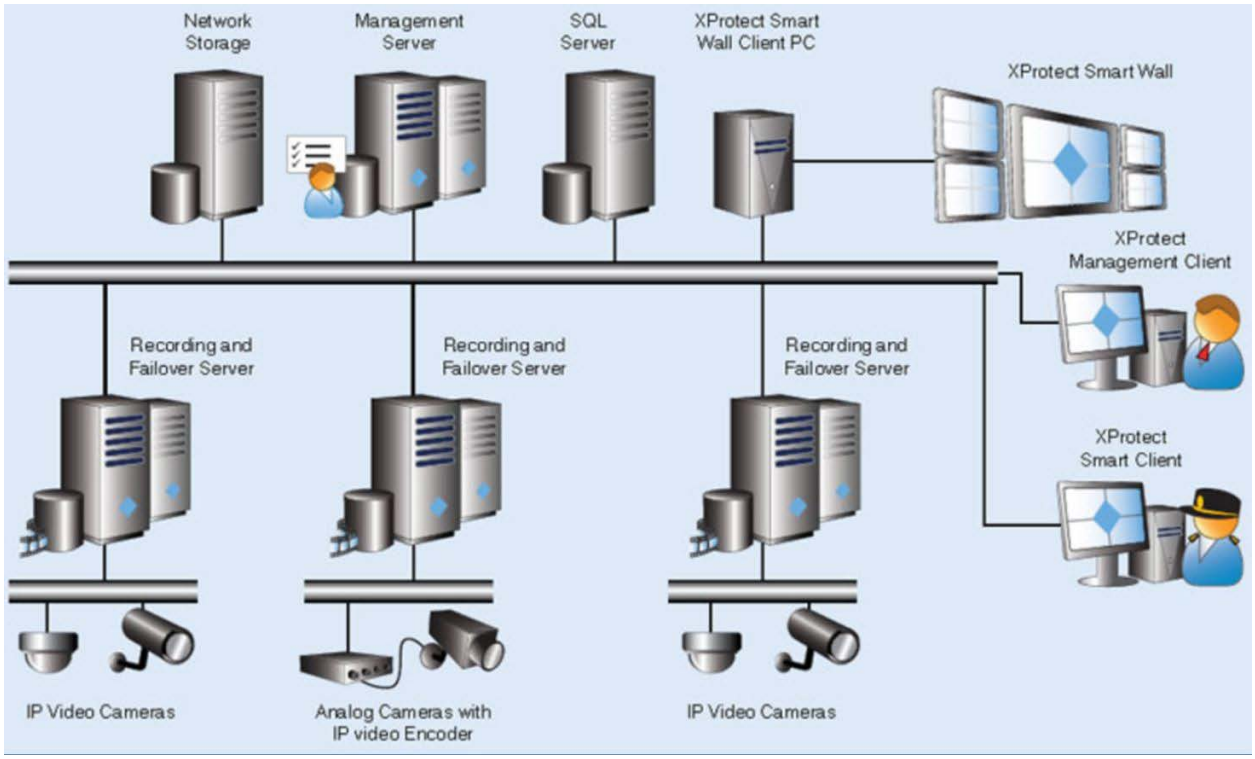

Figure 1: Typical video surveillance system architecture, from MILESTONE systems

The databases/systems that store information such as the rights granted to each operator and the actions of the operators on the system are included within the Video Management System.

Note that some of these sub-parts may be merged for some systems, or not be used for some other ones. Simplest video-systems may be reduced to the camera, the operator station and the network between these two components.

Two types of choices will strongly impact the privacy and accountability of the whole surveillance system:

- Initial design choices that are not intended (or cannot) to be modified during the lifecycle of the system: typically network protections, models, performance and position of the cameras.
- Modifiable design choices that can easily be modified during the lifecycle of the system. This concerns typically the configuration of the system and the authorization of actors.

Next section will list the main design choices of both types on the seven identified typical components of a video surveillance system.

2.2 Initial Design Choices of the Video Surveillance System

One important fact is that in this global study, it is assumed that the video surveillance system works (and potentially causes harms to privacy) mainly alone. It means that special use cases where an additional capability is used jointly with the video surveillance system are not considered as the (potentially huge) privacy harms are most often caused by the additional system rather than the video surveillance system. This is typically the case when a database that contains identification features of individuals is used; a repository containing car owners from car plate numbers typically falls in this category.

2.2.1 Initial Design Choices about Cameras

The main design choices are:

- Those which impact the global viewing capability of the camera:
  - Position,
  - Mobile (PTZ) or fixed,
  - Pan range,
  - Tilt range,
  - Zooming range,
  - Dynamic masking features,
  - Sensibility spectrum.

- Those which will impact the image quality
  - Frame per second,
  - Resolution of the image,
  - Compression type.

- The on-board alarming capabilities of the camera:
  - Movement detection,
  - Blurring detection,
  - Face detection,
  - Smile detection,
  - Virtual line crossing detection.

- The on-board security capabilities of the camera:
  - Visible watermarking of the stream,
  - Hidden watermarking of the stream,
  - Encryption of the stream.

- The on-board recording capabilities of the camera:
  - Recording on SD card capability.

- Others
  - Capability to sense and stream sound (embedded microphone),
  - Presets management,
  - Health monitoring,
  - Environmental protection features.

The most impacting design decisions about privacy and accountability are: the global viewing capabilities of the cameras and the image quality. The global viewing capabilities remain nevertheless much more important than image quality in the global performance of the system. The watermarking capability is also of interest, but rather in a pure positive way as it allows bringing to the users some privacy protecting features such as a very high level of confidence towards the recorded videos (non-repudiation) that also enables potential safe use of recordings during crimes prosecution.

The “global viewing capability” provided by a network of cameras remains a global complex feature that is not easy to specify, to analyse, and to test. A simpler and more operational approach to the privacy of video surveillance systems would be to use the zones of the infrastructure where the system possibly allows performing a certain type of potential privacy harming operation (such as the recognition of a person). The given zone is the geometrical area within the infrastructure where it is possible, using one of the cameras of the system, to perform the privacy harming operation (e.g. the zone where somebody can be recognized using his face view through a camera stream).

This type of zone can be sketched using the camera parameters (focal, positions) in simple environments, and calculated by simulation in more complex cases, taking into account the simple image ratio versus mission proposed. This approach has the great benefit that it can also be easily tested. The other great benefit is that this would not be harmed or misled by evolution of technology (use of un-precedent zooming capability, usage of cameras capable to move on drones etc.).

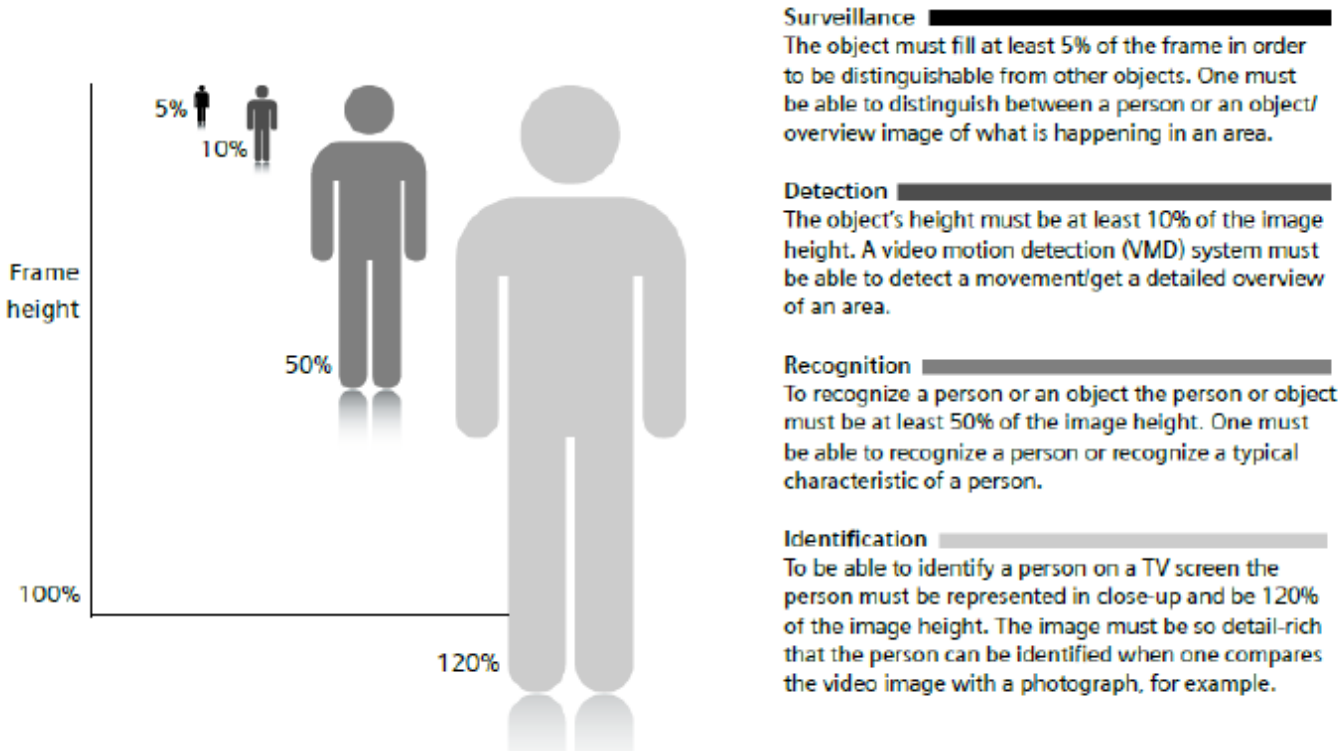

Figure 2: Image ratio versus video surveillance system capabilities

Several types of zones within an infrastructure may be considered, of example

- the zone where the network may give the possibility to perform a detection (of a person),
- the zone where the network may give the possibility to perform the recognition of a person,
- and the zone where the network may give the possibility to perform the identification of the person.

This type of zone definition and/or testing has the great advantage that it deals with operational features that can be directly linked with privacy. Moreover, it is applicable and makes sense both for human usage of the system or for the use of automatic recognition algorithms (the information quantity available and used being basically the same).

A scaling factor may be used in addition to take into account fine grain performances capabilities.

This approach might lead to representation within 2D or 3D mappings as shown below.

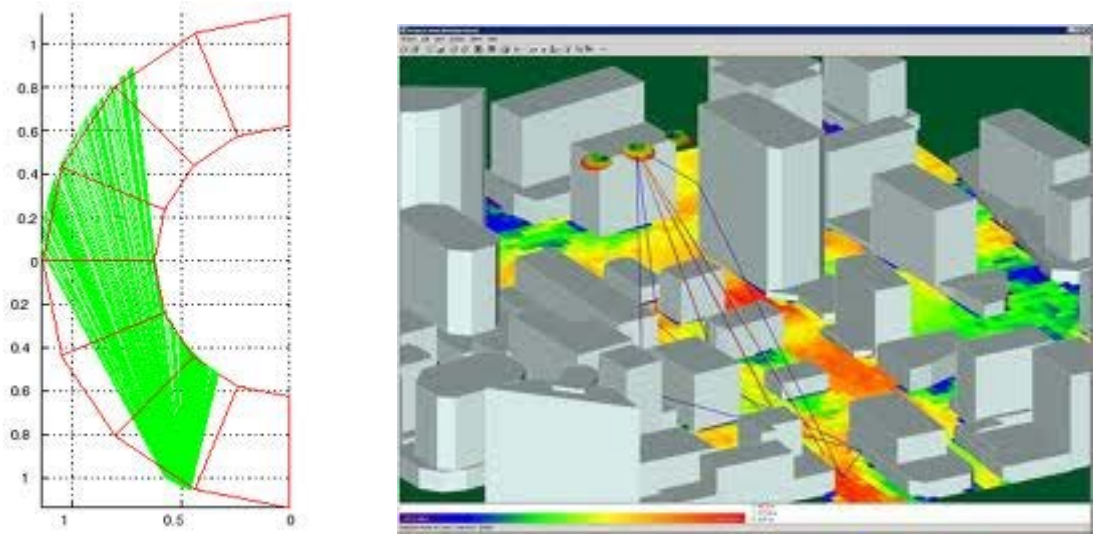

Figure 3: Example of privacy 2D and 3D heat maps related to a video surveillance system

2.2.2 Initial Design Choices about the Camera Network Link

The main design choices about the portion of the network used to link the camera to the rest of the system are:

- The type of network used for the connection:
  - Analogical or numerical,
  - Wired or Wireless,
  - Proprietary Local Area Network (LAN),
  - Proprietary Wide Area Network (WAN),
  - Internet (World Wide Web) Network,
  - Multicast or unicast connection.

Within very complex systems, several types of networks can coexist. A diagram example of hybrid network is given in the illustration below.

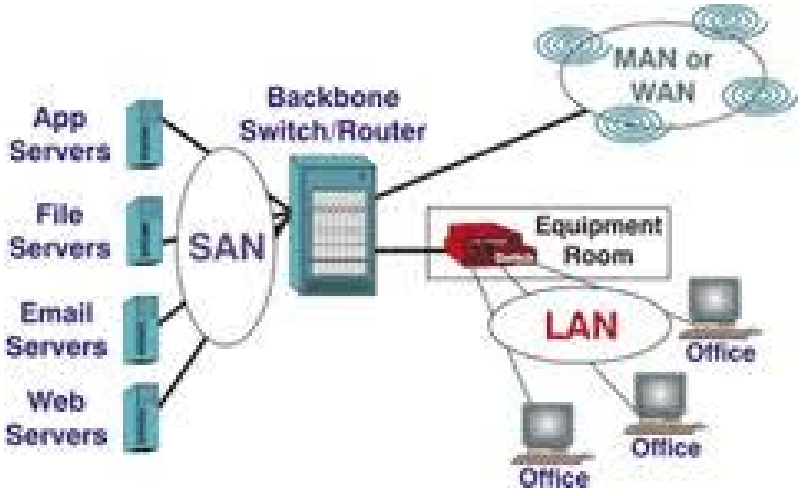

Figure 4: Example system architecture using hybrid network types

The main design choices about the portion of the network used to link the camera to the rest of the system are (continued):

- The data format used for the transmission:
  - Compression type,
  - Encryption type (if any).

- The specific features that can be deployed at the network level:
  - Authentication certificates (e.g. based on 802.1X standard) that will enable to prove that the network device connected is the one expected (ensuring non-repudiation and intrusion detection),
  - Authentication by other means such as MAB (Mac Address Binding), also enabling
  - Network supervision tools (mainly at routers level), that will enable to monitor in real time (and from logging tools),
  - Network intrusion detection tools,
  - Network encryption tools (e.g. VLANs).

From the privacy point of view, the network features are mainly a potential point of failure upon hostile behaviour targeting the stealing of video data. The more protected the data transfer is, the safer the system is against unauthorized attempts to access data.

2.2.3 Initial Design Choices about the Network Video Recorder

The main design choices about the Network Video Recorder (NVR, limited here as the server part of the global capabilities of the system regarding video recordings) are listed below. It is here considered that the main operations performed by the NVR are the continuous recording of streams, the export of video files upon need of portions of streams, and the streaming of the recorded streams to the operator stations.

The main design choices about the NVR are:

- The quality of video recorded:
  - with the same image resolution as the one from the camera, or lower,
  - with the same frame rate as the one from the camera or lower.

- Recording media:
  - Local disks, NAS, SAN,
  - Removable disks.

- The types of metadata that are associated which can be:
  - Sound stream (typically from camera microphone),
  - Orientation of cameras (Pan and/or Tilt),
  - Alarms feeds,
  - Text feeds.

- Export capabilities:

  - Type of file for the export: AVI,..
  - Automatic exportation capabilities,
  - Signed or not (integrity proof),
  - Encrypted or not,
  - Possible destinations for files, e.g. USB stick, DVD-ROM, hard disk drive (HDD) etc.

- Recorded data lifecycle management capabilities:
  - capability to automatically erase (safe deletion) data when the maximum retention delay is attained,
  - capability to encrypt the recordings,
  - capability to trace all the exports realized.

- NVR Streaming capabilities:
  - Number of concurrent replays that can be performed,
  - Watermarking of the streams,
  - Encryption of the streams.

- Authorization management regarding the streaming requests (can be shared with the Operator Station and the video-management system):
  - Management of profiles (e.g. operator, administrator, super-administrator),
  - Use of a central authentication capability (e.g. LDAP).

- The exposition of interfaces to external systems:
  - Interfaces to send external commands (video streaming)
  - Interfaces to get information from (alarms).

- NVR server Hardening:
  - Possibility to access the file system from USB,
  - Possibility to access the file system from LAN interface,
  - Possibility to extract the hard disks.

- Other generic features of the NVR:
  - Pre and post alarm record,
  - External synchronous streams recording,
  - External commands from interfaces,
  - Network loss compensation using camera edge storage,
  - And many more.

From the privacy point of view, the most important features are:

- The recorded data lifecycle management (ability to limit the data retention time),
- The export capabilities (video files that are potentially extracted from the system), their possible signature, their possible encryption.
- The hardening of the server as barrier against unauthorized exports of data or usage of unauthorized media.

2.2.4 Initial Design Choices about the Video Management System

The main design choices about the Video Management System (limited here as the server-side features) are:

- The priorities management:
  - Among operators,
  - Among system operations and operators.

- Central features (typically common to several operator stations):
  - Cameras cycles,
  - Alarm management features.

- Authorization management (can be shared with the Operator Station):
  - Management of profiles (e.g. operator, administrator, super-administrator),
  - Use of a central authentication capability (e.g. LDAP),
  - Protections of the authentication capabilities (encryption).

- The exposition of interfaces to external systems:
  - Interfaces to send external commands (video streaming, camera commutation..)
  - Interfaces to push information within the system (alarms).

Here clearly the possible weak point regarding privacy lies within the authorization management features. If they are not sufficient, or if they can be attacked, possible access of non-authorized people or systems to video data is possible.

2.2.5 Initial Design Choices about the Video Content Analysis and Video Archive Search

Video Contents Analysis (VCA) and Video Archive Search (VAS) provide the capability to apply automatic processing to video streams. This is a live (real-time) feature with VCA, and a post-processing capability with VAS. Typically the VCA is used as an aid capability to the operator watching videos, and the VAS to perform investigations.

The main design choices about video-contents analysis and Archive search are:

- The type of treatment performed, with following examples:
  - Motion detection,
  - Intrusion detection,
  - Virtual line crossing detection,
  - Abandoned luggage detection,
  - Person counting,
  - Licence plate recognition,
  - Face recognition.

- Possible advanced privacy-preserving features:
  - Homomorphic encryption

- Use of external data bases (e.g.: photos, white and black lists):
    - Name of drivers from licence plates,
    - White database of faces,
    - Black database of faces,
    - White database of licence plates,
    - Black database of licence plates.

One important point is that most of the time, the algorithm capability is much less efficient than an operator eye (from a recognition performance point of view). Nevertheless, it may be capable to replace a huge number of operators. The conclusion of this is that the main privacy harm generated by this type of approach (VCA and/or video archive search) are:

- The access to very important volumes of data (or number of cameras) that is often possible from this type of system. The access right management (which is very often realized specifically within the system rather than directly inherited from VMS or NVR rights) is of prime importance,
- The access to external databases, which are the root to possible capabilities to identify people or assets: a VCA or archive search cannot by itself generate an important privacy harm, but when used with a database, then it may be different.

2.2.6 Initial Design Choices about the Operator Stations

The main design choices about the Operator Stations (limited here as the server part of the global capabilities of the system regarding video recordings) are:

- Access rights and authentication
    - Segregation by geographical zone,
    - Capability to access to live videos,
    - Capability to access to recorded videos,
    - Capability to export videos,
    - Capability to view alarms,
    - Capability to view meta-data,
    - And many more.

- Real-time and replay
    - Selection of cameras from map,
    - Selection of cameras from list,
    - Selection of date/time of replay,
    - PTZ commands,
    - Definition of presets cycles,
    - Definition of cameras cycles,
    - And many more.

- Inter-operator station features
    - Push video stream form one station to another,
    - Send text messages from one station to another,

    - Vocal communication between operators.

- Operator actions logging
    - Logging of commands to the system.

- Advanced privacy-related capabilities
    - Hidden watermarking for integrity/non-repudiation proof,
    - Hidden watermarking for video operator station identification (DRM like).

- Mobile and remote accesses to streams
    - From smartphone,
    - From tablet.

The main privacy-related features about the operator station are clearly about the operators rights management. Nevertheless, the remote viewing capabilities (smartphone, tablet) may also be seen as potential weaknesses.

2.2.7 Modifiable Design Choices of the Video Surveillance System

The way the video surveillance system is used, and the way this usage is audited are very important for privacy/accountability performance. The two crucial points are the management of the users of the system rights, and the management of the data lifecycle, especially the one of video export files.

Most of these choices depend on the system operator's requirements.

2.3 Video Archive Search

2.3.1 Overview

Video surveillance is the technological approach to improve safety and public security on a "continuously monitoring" basis. However, an increase in data does not necessarily lead to an increase in understandable information. The widespread use of cameras for surveillance (e.g. there are 1800 cameras in Vienna International Airport, 3700 cameras for the Austrian Railroad ÖBB including 700 cameras for the newly-built central station) shows that it is increasingly difficult for targeted search and monitoring of individuals or situations. Increasing the number of cameras and the amount of video footages do not necessarily makes it easier for human operators for better situation comprehension. Consequently, it remains to the end users to work its way through the flood of recorded data to find the relevant sequence.

2.3.2 Video Archive Search

Search and evaluation algorithms for video data can be improved through the interactive use of the cognitive abilities of the system. Automatic detection of critical sequences is more suitable as a vision and strategic roadmap but unrealistic as a target for significant improvements in the field of monitoring tools for field operations. The concept of interactivity for the important use case "forensic examination of video material" when viewed retrospectively (event related) can interactively incorporate the user's knowledge. At the moment a preventive parameterization for online detection purposes is currently not seen.

Here is where the Video Archive Search (VAS) starts. The objective is to use current algorithms and research trends in image processing already existing, integrate them into a framework for video archive search and extend it with the concept of intelligent, semi-automated user interaction methods. Interactivity can only be validated in real live scenarios with demonstrators in the application domain of the end users. The latest research trends in person and object detection, the integration in an interactive framework and the validation together with the operators of the video archives and forces is necessary to get away from the pure collection countless video material with time-consuming manual analysis towards an intelligent and user-interacting video search tooling for surveillance purposes.

The field of Image processing algorithms is huge. There are many different solutions for various problems available, each solution comes with its own user interface. There are many Software Development Kits (SDKs) available, different libraries on different platforms with different performances, implemented with various techniques (CUDA, OpenMP, OpenCL). In addition we have a lot of specialized approaches such as Face Detection and License Plate Recognition. Both examples are supported by SDKs from different vendors. Other image processing algorithms are not so populated, such as solutions for detecting fire in a stadium, or recognition of an

emergency car. The following table gives an overview of interesting algorithms with their input and output parameters.

Name of Algorithm	Parameter	Input	Output
Face finder	Expected Min, Max Face size, possibly distortion	Region of Interest (ROI)	ROI, Confidence, Face Template
Face matching		2x Face Template	Confidence
License plate finder	Expected Min, Max LP Size, possibly distortion	ROI	ROI, Confidence,
Text region detection	Expected Min, Max Text size, possibly distortion	ROI	ROI
Optical character recognition	Expected Min,/Max Size; Constraints (e.g.: 1. Character is a letter, minimum 8 chars)	ROI	String, Confidence
Logo detection (symbols)	Template	ROI	ROI, Confidence
Detection of Moving Objects (1 camera)	Accuracy	ROI	ROI
Tracking of moving objects (1 camera)	Inertness of the tracker, recapture window if target lost	ROI Sequence	Trajectory, ROI´s
Event trigger through trajectory analysis	Tripwires, complex Regions, Rules	Trajectory	Timestamp
Trajectory analysis	Pixel size/Real size relation, Relation pixel movement to real speed	Trajectory	Speed
Object classification (on Blobs, 2D)	Min/Max X, Y, Proportion, Speed	Trajectory	Class, Confidence
Main color of object		Trajectory	
Similarity in color	Color histogram Values thresholds	Color histogram Values	Confidence
Structure of object		Trajectory	
Similarity in structure			Confidence
Person counting (normal surveillance camera view)	pose of Person	ROI	Number, Confidence, Direction of movement
Person flow (optical flow)		ROI Sequence	

Throwing of things == (possibly special case of tracking of moving objects)	Expected Size	ROI Sequence	Timestamp
Note: ROI - Region of Interest Confidence - Detection quality measured by the system			

Table 1 Overview of video processing algorithms

It can be seen that algorithms have a very special parameterization. However, the input and output concentrate on a few data types. Input data are often the same: images, streams of images, parts of images. For an evaluation of movement structures we need trajectories, some algorithms produce special templates (face signature template) but also confidence values which can be displayed easily.

If we target scalability, security and interoperability we have to think about the "outer world" of an algorithm. Figure 5 shows that an algorithm, packed into an application, needs to implement many additional components such as data interfaces and result interfaces. In addition we see that some parts (video data access, results views, video decoding, frame scaling, etc.) are similar to other solutions (in fact they are 99% the same).

The calculation part or "algorithmic core" defines the platform and the resources used. How the algorithm is used should remain the task of the "user" which is depending on the complete context of the solution.

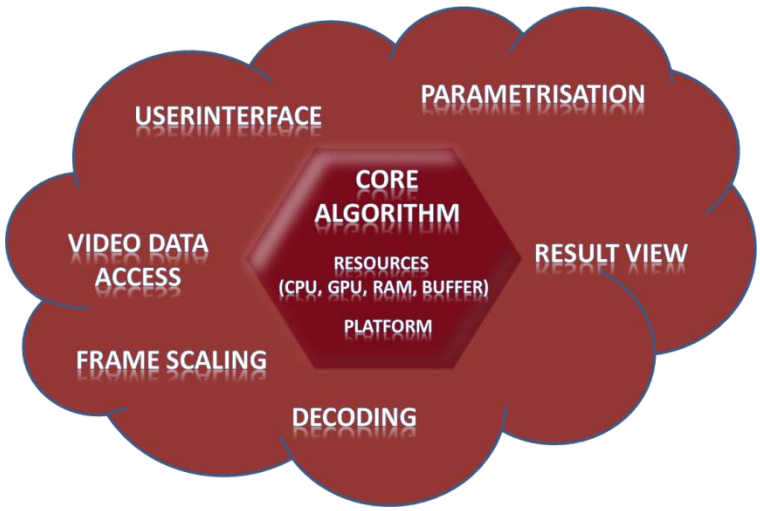

Figure 5: If an algorithm is mixed with application parts and interfacing functions, scaling, replacement or adding security mechanisms get complicated

2.3.3 An ideal Atomic Processing Module

If we try to connect modules to set up a complete processing chain it would be useful to embed the algorithmic core into a service layer. If this is done on a network interface basis this would result into scalable basis architecture. The service layer would be the same for different

algorithms, control structures and functions would have the same interface (start, stop, process, status, progress, etc.).

Input, output and parameterization would be derived from the properties of the algorithm, but only with a limited number of data types.

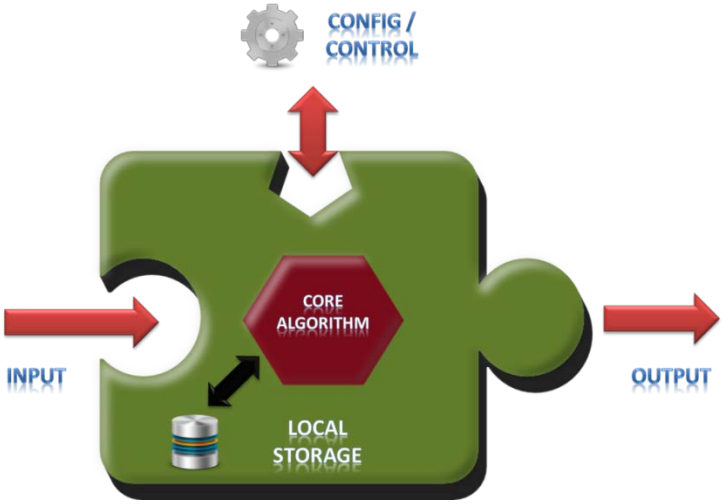

Figure 6: Interfaces of a module are: Input, output and parameterization

2.3.4 Client-Server Architecture

The client of an archive search system is a graphic-based frontend layer between the end user and the server which contains various video analytic algorithms. The client is responsible for all the user interactive activities, such as drawing a process chain which is sent to backend and visualizing the results such as generated detection thumbnails and video sections of a processed chain provided by the backend.

The client is a web application which could be based on Microsoft .NET framework, which is able to run on distributed PCs having access to network shared with servers (see Figure 7). Servers publish their service to the network, and client applications consume these services by sending web request and getting response.

Such client-server model has the following characteristics:

1. Clients are physically independent from servers. Client and server can be run on a same PC as well as run separately in distribute PCs and communicate remotely.
2. Clients are able to consume services provided from more than one server. Therefore the whole processing performance is optimized as tasks are distributed among multiple servers.

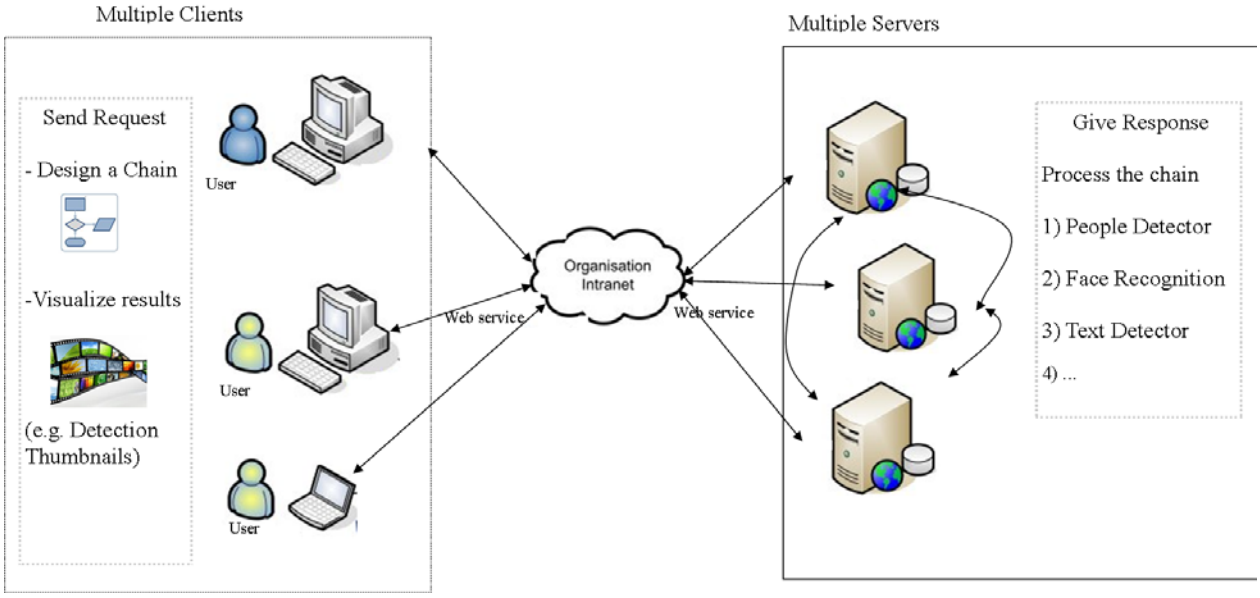

Figure 7: User interface of video archive search with interactive client

2.3.5 Rich Client User Interface

In our current implementation, we use WPF (Windows Presentation Foundation) Technology to implement our GUI (Graphical User Interface). WPF is a graphical tool for designing rich graphic elements, such as graphs, charts, 2D/3D effects, frames and more. WPF is provided as component of Microsoft .NET framework.

By implementing a rich user interface, the client is not only “appealing”, but also facilitates the use of various higher features for end users. Users are able to visualize the output in a customized manner, or browse and order the results by specific criteria. Rich client application provides clear visibility of different options, thereby enriching the end- user experience.

Designing a chain and visualizing the thumbnails results are the two main functions of the client system. As shown in Figure 8, the user interface consists of three panels. The Module pool lists all the available video analytical algorithms detected from the backend. Each module in the pool is corresponding to a web service published by the server side. Using drag and drop mouse operation, user is able to select a collection of modules from the pool and draw connection in between to form a process chain. Results display panel lists all the detections of a processed video, for instance, all the detected vehicles in the given video, with providing sorting options.

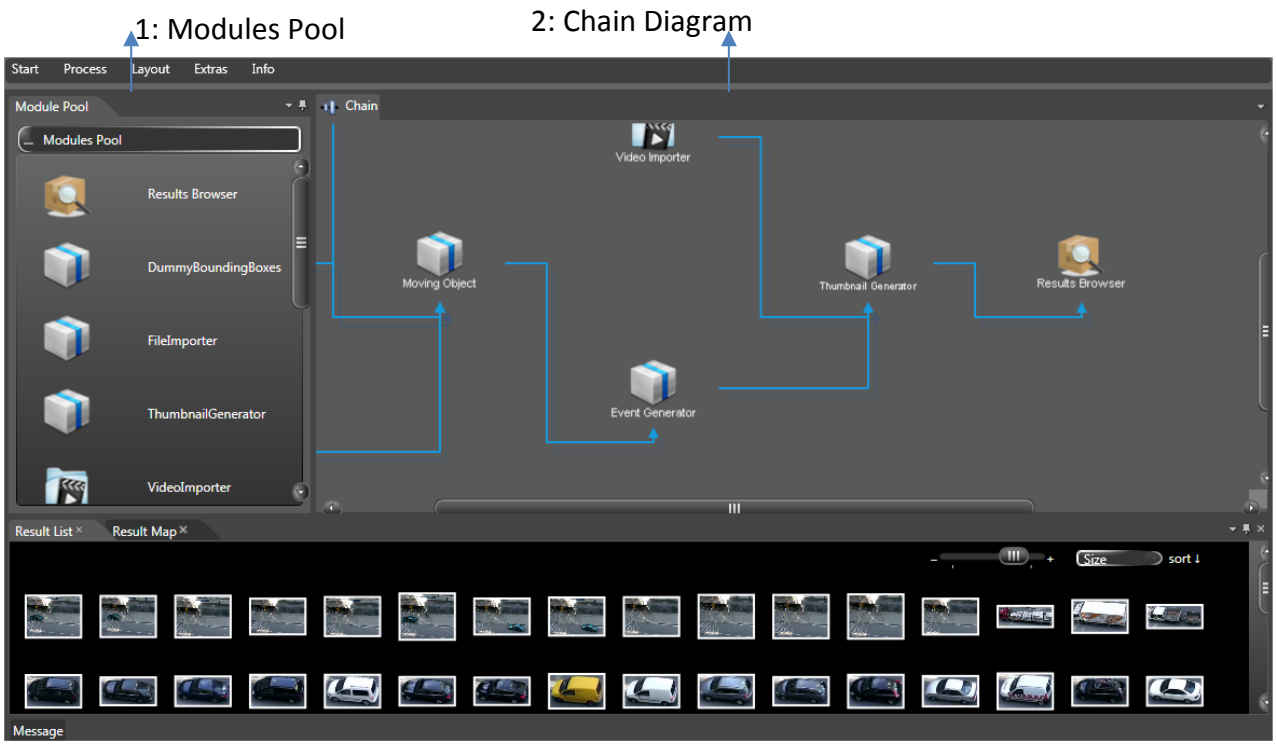

Figure 8: Processing chain and results

2.3.6 Design a Chain

Web based client-server architecture allows various module services to be exposed over the web. This gives client applications the freedom to choose the services that they would like to load. When the client starts, a modules pool will be loaded, appearing as a list on the left side of the user interface. This module pool can be pre-configured via text editing. Otherwise, a default configuration is available.

Figure 9 shows the procedure of loading the module pool. The configuration of module pool is indeed a text file consisting of a list of http addresses. When the client starts, it sends all the requests (the http addresses) to the web. If the client gets response of a service, this service will appear in the module pool as an available video-analytical-algorithm module.

Selecting the modules from the modules pool is done by drag and drop feature. The user selects a certain module by clicking and dragging it to the drawing panel.

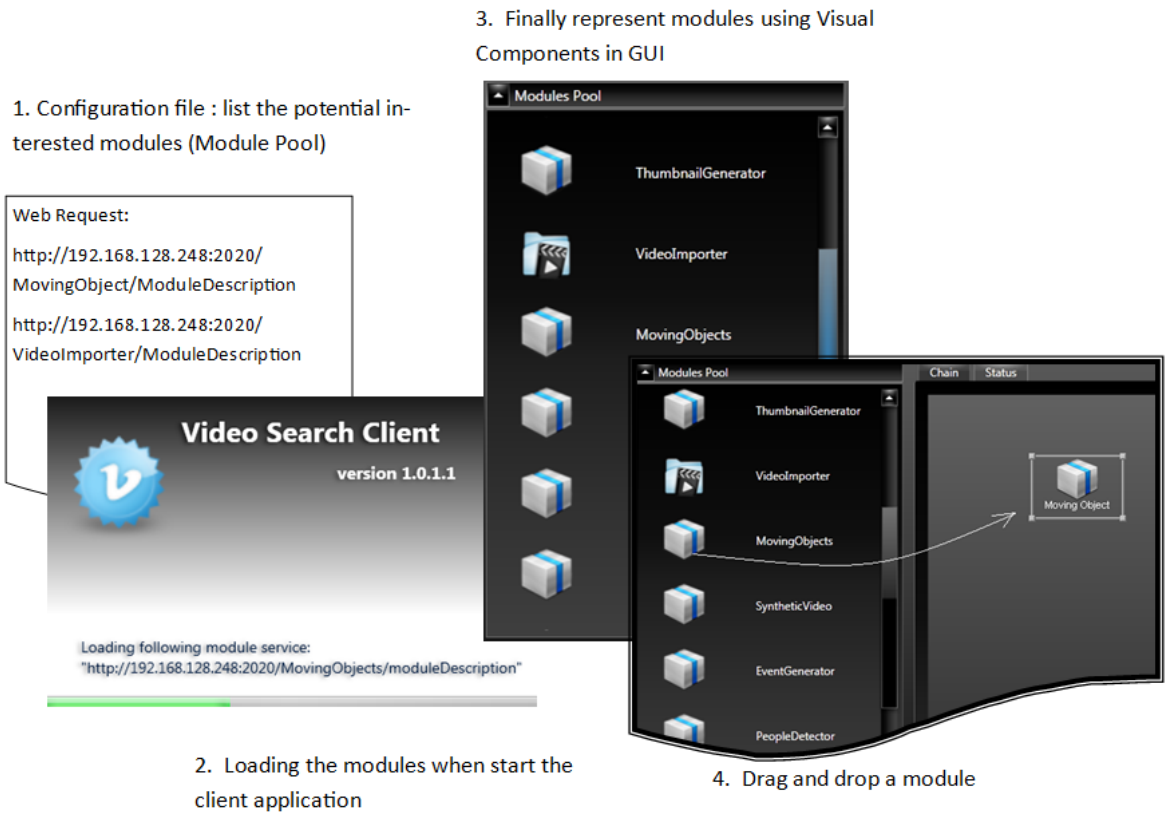

Figure 9: Load and select a module

To create a chain, users connect the selected modules by drawing directional edges (See Figure 10, the blue lines with arrows represent the data flow direction).

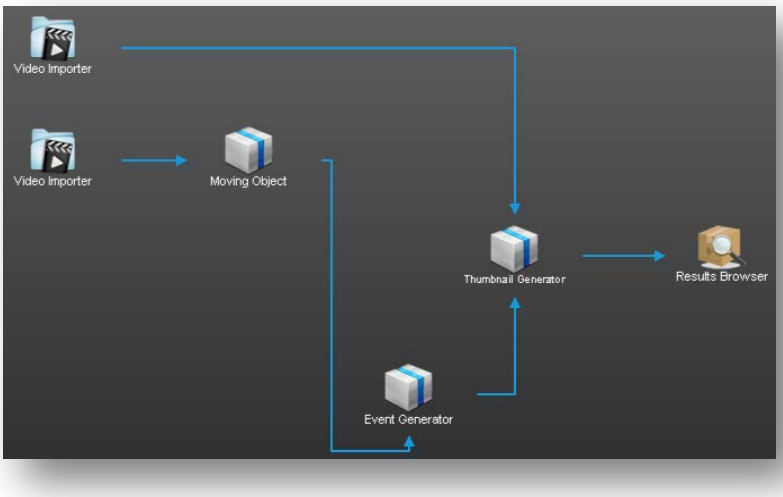

Figure 10: A complete chain

Each module has to set parameters. For instance, sensitivity value needs to be set for moving object detection algorithm. Adjusting parameters can help to achieve better detection results.

The user runs the chain by simply pressing a “run” button, and the chain configuration will be post to the backend server via web service. The status will be sent back to the client side, so that the user is able to monitor the progress (see Figure 11)

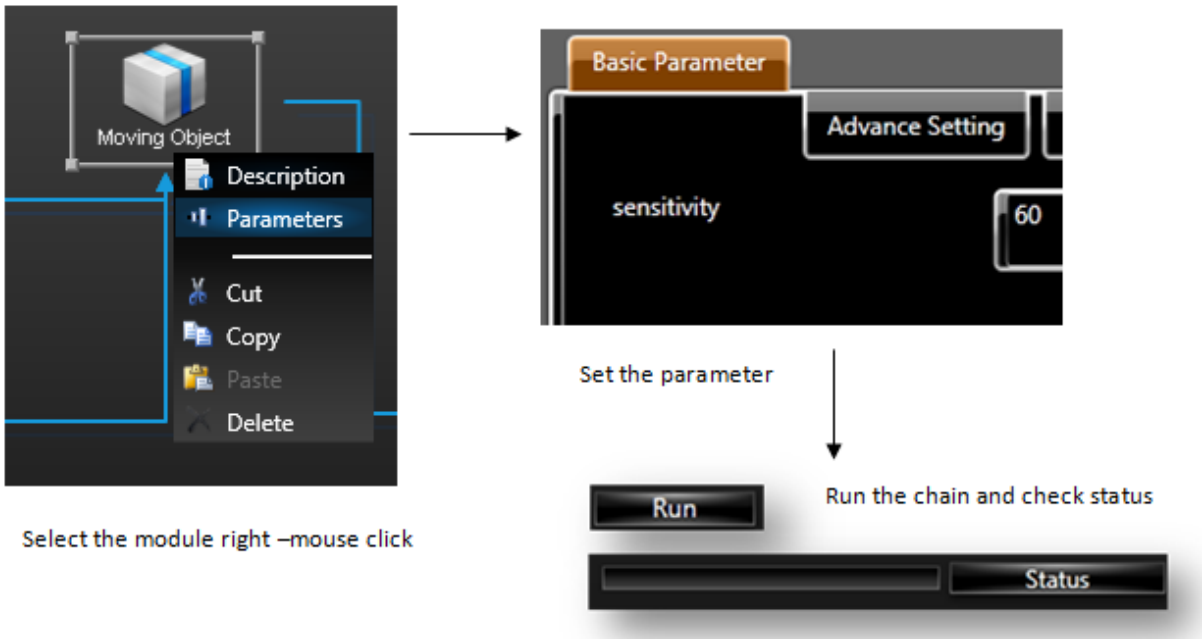

Figure 11: Run the chain

2.3.7 Summary

In this subsection, we have described basic video archive search technologies and design concerns. As a topic of its own, video archive search is under actively research aiming for scalability, efficient and precise detection for public security surveillance, and interoperability with other video surveillance systems or other information systems. Moreover, we have shown a research prototype developed at AIT for a “configurable” video archive search to flexibly and efficiently specify and construct video archive search algorithms and video processing capabilities.

It should be noticed that our current research prototype does not include any components for privacy and accountability. Privacy and accountability will be addressed during the development and specification of the use cases for SALT framework, which will be an iterative process to integrate privacy and accountability into the software stacks that realize video archive search functions in video surveillance systems.

3. Integration of Video Archive and Search Technology in Conceptual Framework

3.1 Optimization of Privacy and Surveillance Capabilities

The "Guidelines for public video surveillance"[1] from the US non-profit organization "The constitution project" clearly adopts this co-optimization approach of both privacy and security perspectives. Its introduction states:

"It is understandable that American cities and their law enforcement officers place great emphasis on developing new tools to confront the increased threat of terrorism faced by Americans in the twenty-first century—and the apparent value of surveillance footage in the investigation into the July 2005 bombings in London only strengthens the appeal of this particular tool. Likewise, it is understandable that authorities would want to use any available means to prevent or deter other serious threats to public safety. But the value of modern video surveillance must be balanced with the need to protect our core constitutional rights and values, including privacy and anonymity, free speech and association, government accountability, and equal protection. The new technologies may help protect the public, but they also enable authorities to more deeply intrude upon these rights. Lawmakers can no longer rely on constitutional law and technological limits—they need to proactively seek ways to harmonize constitutional rights and values with the new surveillance capabilities. We believe that constitutional rights and values can be reconciled with law enforcement and antiterrorism goals, but officials often lack the resources to properly gauge how to achieve such reconciliation."

This is also the point of view of Ann Cavoukian, Information and privacy commissioner for the Canadian Ontario State, who has pushed the privacy-by-design concept in its early stages (the 4th principle promulgated by A. Cavoukian is "full functionality, positive sum, not zero sum", which, as described on the website[2], "avoids the presence of false dichotomies, such as privacy vs. security, demonstrating that it is possible to have both").

The surveillance and privacy optimisation problem may be addressed in several ways. The most efficient one, which is the one proposed in the PARIS project, is first to determine the exact need for surveillance in the context of use and according to the goals assigned to the surveillance system (cf. the description within the D2.2 deliverable "structure and dynamics of SALT frameworks" of the "SALT intention stage"). From this analysis the precise needs and goals are assigned to the security system. These needs actually may widely differ from one context to one other (high dependency on the type of infrastructure, on the level of risk faced of feared). An example simple correspondence between the mission of a video surveillance system and the surveillance context is proposed below (the precise content of this table could be challenged, what is of interest here is the high dependency of actual surveillance needs versus the context of use).

[1] The constitution project, "Guidelines for public video surveillance," http://www.constitutionproject.org/wp-content/uploads/2012/09/54.pdf, 2012

[2] Privacy-by-design, http://www.privacybydesign.ca/

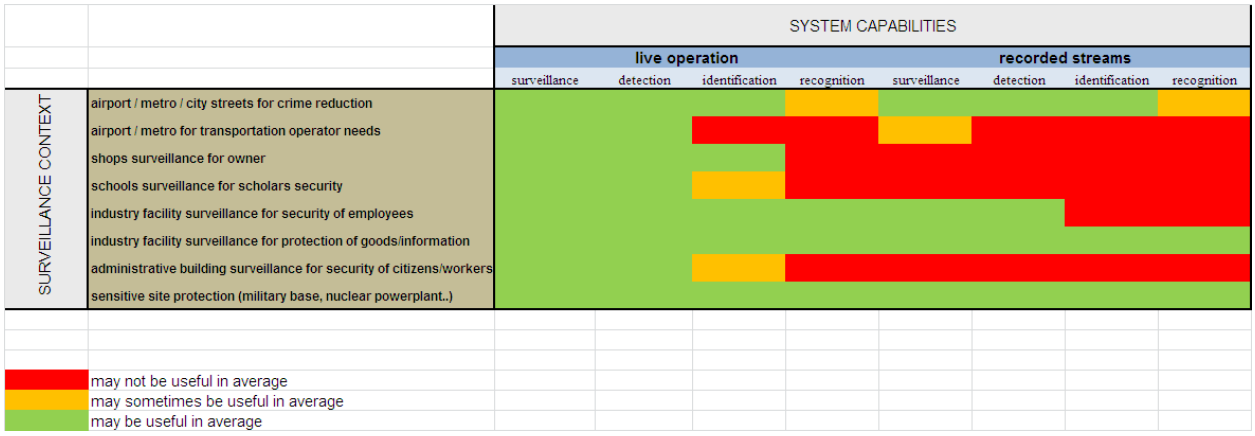

Figure 12: Correspondence between video surveillance system example mission and its expected average capabilities

What is at stake here is the tuning of an abstract quantity that can be called “performance of the surveillance system on the security axis”. A simplified presentation (but of didactic interest) of the first optimization step is presented below within an hypothetic 2-dimensional diagram encompassing on its second dimension the privacy performance of the system.

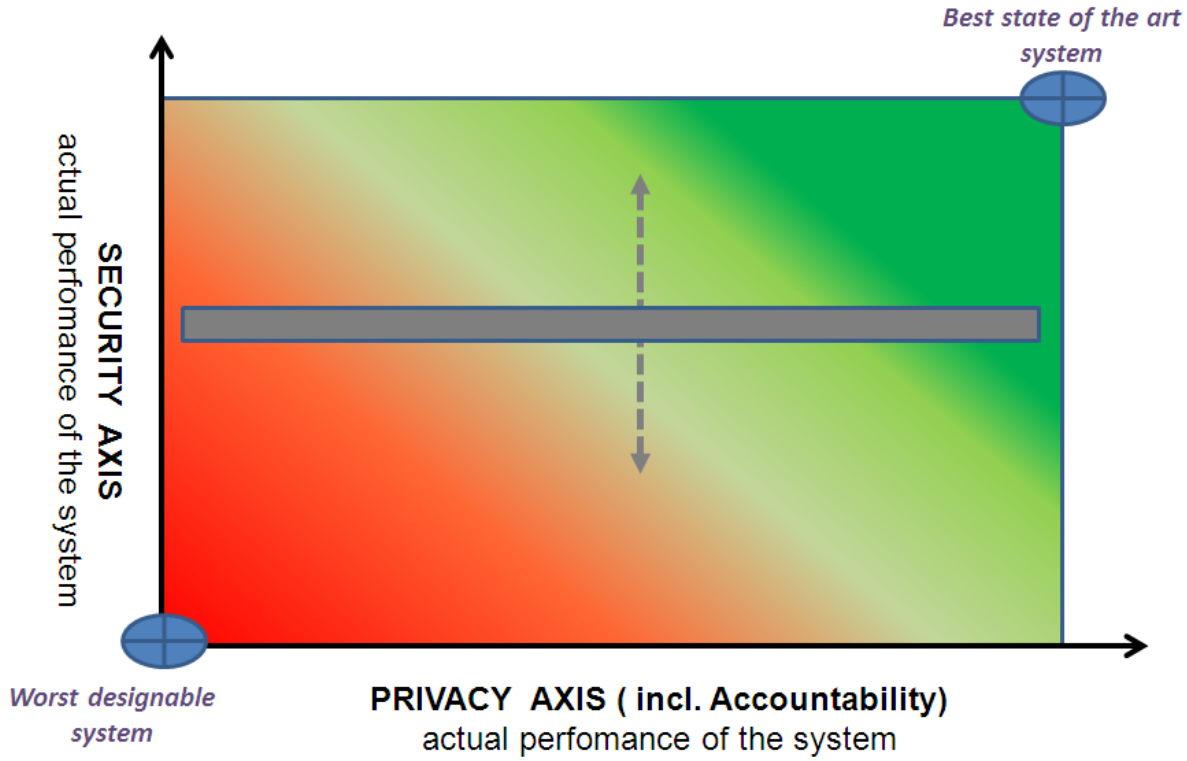

Figure 13: The first optimization step for privacy vs. security

We shall note at this stage that there is here a supposition made that it is possible to design a security system compatible will the whole applicable framework of laws (including those about privacy and accountability), i.e. that the initial problem has a solution.

The second step then covers the design of the system with an additional objective, which consist of a target privacy and accountability set of requirements. Remaining in our bi-dimensional diagram security performance / privacy performance, this may be idealized the following way:

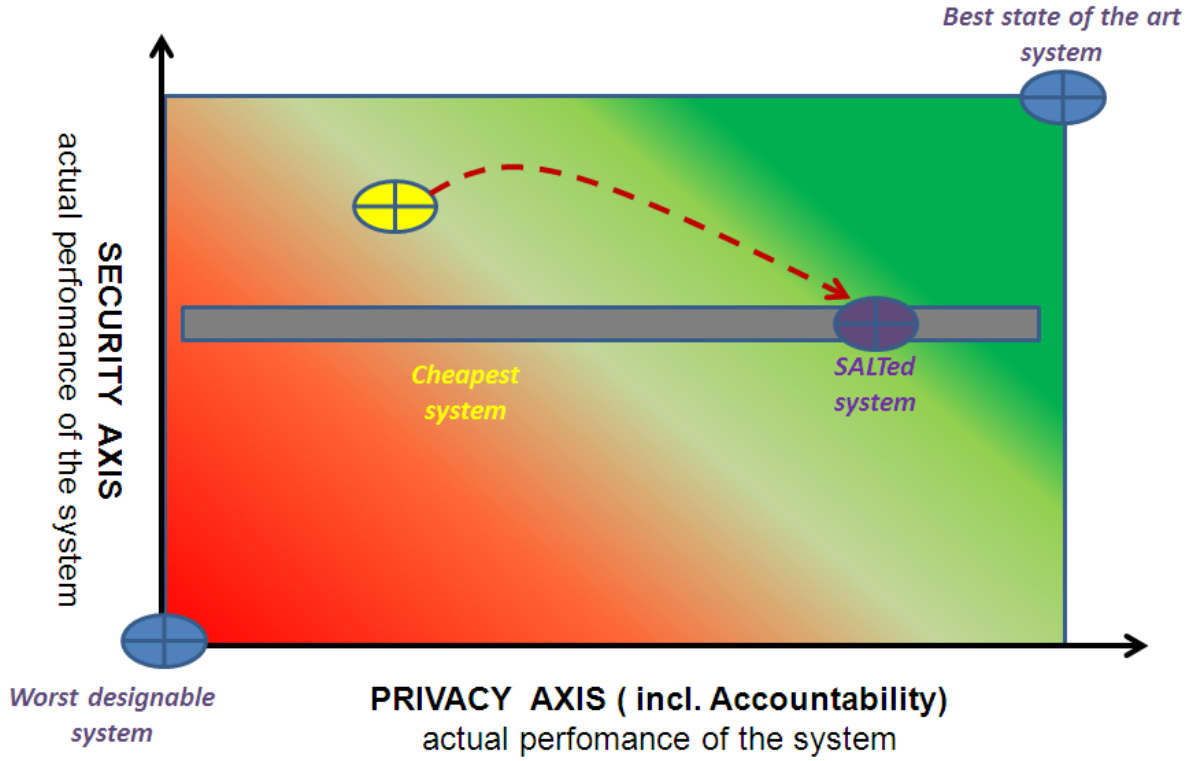

Figure 14 The second optimization step for privacy vs. security

The SALT design process helps to reach the requested level of security and the requested level of privacy / accountability. It is important to note that the privacy performance and the security performance of the easiest system to deploy (the cheapest one that meets at least the security level requirements) are unpredictable for several reasons:

- Most often the suppliers of systems deploy standardized products, meaning the same system for a wide range of needs. The system will often allow more than needed (a simple example is the zooming performance of a camera: it may be much less easy to find a 2X camera zoom than a 10X),
- Most of the requirements arising from customer about performance consists of lower limits ("the system shall at least.."),
- Some privacy and accountability enabling modules (encryption, rights management, logging..) are additional modules featuring themselves their own cost.

At the end, it is also important to note that a high performance system from the security point of view offers more possibilities to the security operators, meaning for them an augmented cognitive load. This may lead at the end to a lower performance of the couple (system, operator) even from a security point of view. In other words a system designed to meet exactly the needed security performance level may be most efficient because focusing "by design" the operators on their expected tasks.

3.2 Information Security for Privacy in Video Surveillance

The relation of information security and privacy is commonly recognized as: *you can have information security without privacy, but you cannot have privacy without information security.*

Many technical building blocks for security are also the building blocks for privacy. In the context of video surveillance, especially video data lifecycle management, the following security controls are indispensable:

Authentication. Authentication is the process that is necessary to identify and verify an entity. An entity can for example be a human user or a service. The entity claiming a specific identity has to provide one or more credentials to back up its claim. The credentials can fall in one of the following categories:

- Something you know. This can be a username/password combination or a personal identification number.
- Something you are. This can be any unique characteristic of a human being that can be used to identify a person (biometrics), for example a finger print or a retina scan.
- Something you have. For example, this can be a one time pad, a smartcard or a hardware security token.

An important aspect of authentication is identity management. In many traditional applications, each application has its own management functionality. In networking environments this is not feasibly due to the increasing administration overhead. A central identity management service, for example, a directory service based on Lightweight Directory Access Protocol (LDAP), is the next step to limit the administration overhead. But for SOA environment that spreads over multiple domain boundaries, a central service still might not be the optimal solution. Hence, the use of a federated identity management system is the most feasible solution. A federated management system provides authentication across multiple systems and organizations, enables single sign-on (SSO) and user attribute exchange cross multiple domains. An important concept of federated identities is the mutual trust relationship between the participating parties.

Authorization. The process of authorization is to determine if an entity is allowed to access a resource or perform an action. The outcome of an authorization decision is influenced by different factors, e.g., which identity requesting to access the resource and which resource is being accessed.

Figure 15 shows a general model for authentication and authorization in SOA, implemented according to the XACML reference model and the SAML standard. A Policy Enforcement Point (PEP) ensures that only authorized users can access a service. If only authenticated users shall have access to a service, the authentication of an user must take place before the authorization process. Before participating and accessing a service in SOA, a user must first register at an identity provider (IdP). The client service of a registered user then can present a proof of identity (for example a SAML ticket) in the service request. Access control is enforced at the Policy Enforcement Point (PEP) at the authorization service. In any case, the services are not directly accessible by the user client; all user communication is intercepted by the PEP. Upon

receiving a service request, the PEP performs an authorization decision request on the Policy Decision Point (PDP). This request can contain user attributes provided by the IdP and other necessary context information, for example, the service request or the request target. The PDP then makes authorization decisions based on a set of stored policies. In case of a positive authorization decision, the PEP relays the original service request to the protected service. The service response is also send back to the client.

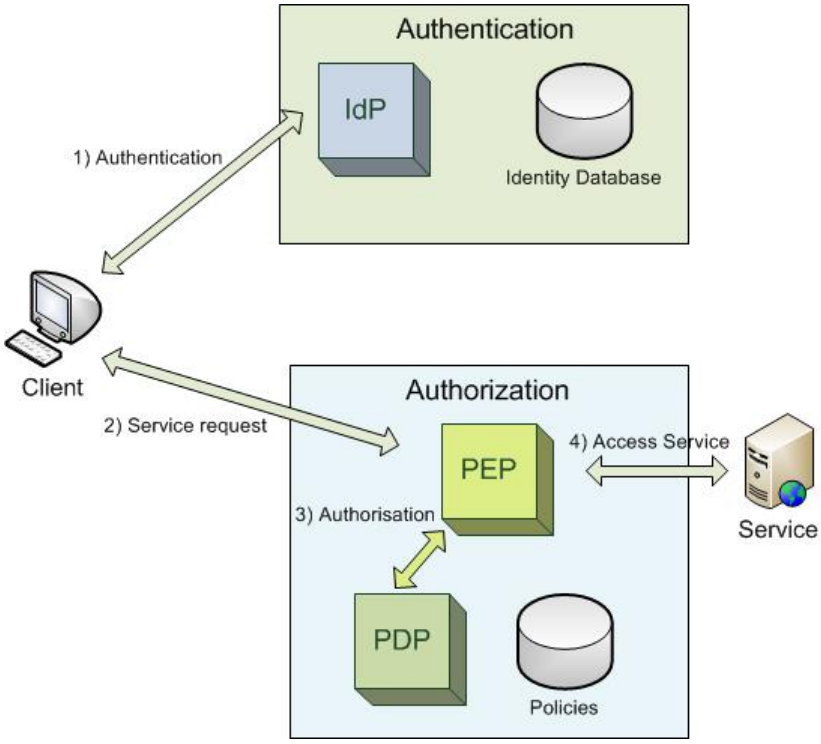

Figure 15: Reference access control architecture in Service oriented architecture (SOA)

Access control. Access control aims at allow only authorized party to have access to resources and the right to perform operations. Following a SOA paradigm, the access control components for authentication and authorization can be implemented as special services, that is, ``security as a service''.

A normal access control process consists of identification, authentication, and authorization in a sequence. The purpose of identification is to identify the entity requesting a service. The identity contained in the service request needs to be authenticated to be valid. Authorization decisions are then made based on the request and the access rules.

Encryption. Encryption is the process of encoding information such that only authorized party can read the information. Encryption enables and enforces access controls. Encryption addresses confidentiality in the Confidentiality, Integrity, Availability (CIA) information security triangle. When information (e.g. login credentials, or video stream) needs to be transported over distributed networks which are usually assumed to be non-trustworthy because of eavesdropping, confidentiality is accomplished by setting up a secure channel for information exchange between communication partners. The IPSec protocol suite, developed by the Internet Engineering Task Force (IETF), operates on the network layer. It consists of protocols for encrypting and authenticating IP packets. Secure Sockets Layer (SSL)/Transport Layer

Security (TLS) is used to encrypt data exchange and operates on the transport layer of the OSI model.

3.3 Selection of SALT Framework

Even though the SALT framework is envisaged to collect information regarding privacy and accountability concerns for surveillance systems in general (video surveillance systems and biometric systems are covered by the PARIS project), it is possible to observe certain characteristics that are more focused to video-archive systems, and hence we can enclose those features that are more likely to affect the selection of SALT References corresponding to video archive systems.

When dealing with video surveillance systems together with the SALT framework, the main fact to take into account is the violation of the privacy of the subject under surveillance (typically a person, but it could also be a car, a building, etc.). It is important to consider what actions are recorded, in what context or location, and the safety of this sensitive material. Therefore, the search criteria for video archive related SALT reference is typically ruled by the following parameters:

- Localization: it determines where the video-recording takes place. This parameter is tightly linked to the privacy of individuals, since depending on the type of localization the SALT repository will provide different sets of SALT references. The types of localization are commonly classified into public, semi-public and private. But this classification by itself is not always decisive to delimit the selection of SALT references, it is needed more information regarding the localization for each of the three previous categories. E.g., different public places may result in different SALT references. We could take an airport and a public park as an example. They both are public places, but they have very different surveillance systems (this is related to the purpose of the system, which we cover next). Besides, even within the limits of a same localization the SALT repository may provide different SALT references, e. g., continuing with the airport example, we should get different SALT references (different privacy concerns) regarding the lobby, the toilets or the departure gates.

- Purpose: the purpose of a surveillance system clearly determines what set of privacy concerns, and hence what set of SALT References, are going to be selected for particular surveillance systems. Besides, the purposes associated to video-archive systems are commonly different from those associated to biometrics systems (crowd counting, search a particular subject within a video stream, etc.). The purpose of a system directly influences the technology used, not only for the recording, but also for the storage of the recorded footage.

- The subject under surveillance: the subject under surveillance is another parameter that clearly discriminates the selection of SALT references, particularly between those related to video-archive systems and the ones related to biometrics systems. Subjects for biometrics systems are always persons (they need quantifiable data related to human characteristics and traits), whereas video-archive can be applied to any kind of object, not only persons, typically cars and license plates. Therefore, search criteria related to non-human subjects will result in a set of SALT references for video-archive

systems. Apart from this, even considering just human subjects, we can get different sets of SALT references for different classifications of subjects: ethnic group, nationality, age, etc. However, this may also apply to biometrics systems.

- Type of processing: the image quality is a very influential factor for the privacy of the subjects under surveillance, since a good quality image may allow for not only the detection of the subject, but also for the identification. Additionally, the processing performed to the data is also important, such as techniques to limit the identification of subjects (e. g. blurring). Since video-archive is associated to video data, the type of processing associated to it is usually different to the processing applied to biometric data. Also regarding the processing, we may also take into account the methods used to determine who has the rights to access what videos and under what conditions, i.e. access control to stored data. Video archive systems usually require a safe processing to ensure the proper access to sensitive data, thus allowing for disclosure prevention. It is also remarkable that data from video archive systems are commonly accessed when some determined event has happened. Consequently, different search criteria regarding different processing methods may result in different SALT references from the SALT framework.

These parameters are all interrelated, meaning that searching by one of them can limit the range of the remaining.

4. Surveillance Use Case and Scenario

4.1 Use Case I: Secure Law Enforcement Access to Video Archive Search

Short Description:

Law enforcement agencies search video surveillance archives of infrastructure provider in forensic investigation

Actors:

- Law Enforcement Agency (LEA)
- Police Officer (PO) of the LEA investigating the crime
- System Operator (SO) which operates the video surveillance recording system:
- Data Protection Officer (DPO) of the Infrastructure Provider (IP)
- Data Protection Authority (DPA)

Aims:

Establish trusted relationship between PO and IP over network. Authorize PO by DPO for a specific crime case. Permit secure access to video data stored in the infrastructure video archive to the PO searching for evidence in the video footage for a specific crime. Log all query and data transmission actions on both sides.

Preconditions:

- Legal recording permission for IP
- Accepted viewpoint for involved cameras by DPA
- A crime has been committed (in German “Anzeige gegen Unbekannt”)

Scenario description:

A crime is committed in the premises of an IP (e.g. railway operator). The crime does not interfere with the security rules of the IP (not significant for safe operation of their systems) because it is not the responsibility of the IP. For this use-case it is sufficient to assume that it is a typical crime (theft or assault) and it is within the responsibility of the law enforcement agencies.

The victim reports the crime to the police. At this moment personal data is involved in the use-case. Information on time, place, actors and description is assembled into a “case”. The “case” is entered by the PO in paper or electronic form according to some predefined workflow of the LEA. Depending on the law enforcement agencies’ resources or the urgency of the crime, it sooner or later enters the stage of “collecting evidence”. Implicit knowledge reveals that the crime might have been recorded by the video surveillance system operated by the IP.

For simplicity it is assumed that the PO in charge of the case crime is the same person investigating the video data.

The PO asks the IP for the video footage to look for proof that something had happened and to secure the evidence. Therefore the PO has to be recognized as a legally authorized person to access and view the video data. This authorization should be formally proved and recorded. If

this has happened, the IP, represented by the DPO for this specific case is allowed to hand over video data. The amount of data is restricted to the necessary data for this case. Permission for the PO should be restricted to the amount of cameras involved, to the time of the crime.

This permission should be logged and instantiated by a “token”. This token is built by the DPO at the IP and given in a secure way to the PO. With this permission a connection between a video search system (at the premises of the LEA with the PO working in it) and the archive of the video surveillance system of the IP can be established.

Data can be retrieved by the PO. Activities related to retrieval are logged. At this point the real police forensic work starts. The PO investigates the scenes and tries to gather evidence. Any data access more than permitted is blocked. Typically it needs time to find the relevant scenes in the video footage and typically more data to be investigated is retrieved (e.g. to find accomplices or hints for a better pursuit of the offenders or to retrieve a better frontal face snapshot during entry to the train station). This work is entitled “video forensic search”.

As mentioned it could be possible that during this forensic search an extended permission is needed to access more data if PO sees enough evidence. This process should be formally proved and logged as well.

If evidence is gathered, relevant video footage should be secured and provided in a form that it can be transferred and presented at the court. If not, retrieved data has to be deleted according to the specification of the data life cycle management.

A proof of integrity, i.e., the data has not been manipulated from the beginning to the end, is required.

The dynamic view of the use case is shown below.

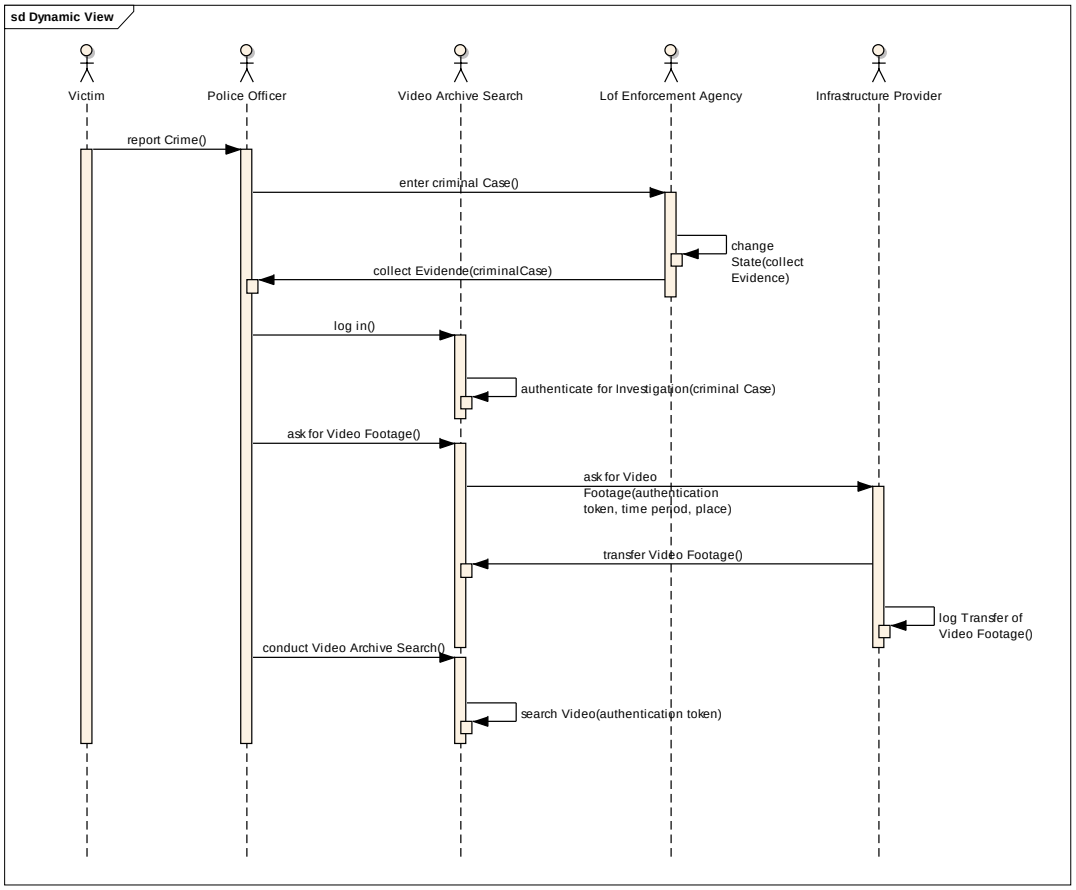

Figure 16: Dynamic view of secure law enforcement access to video archive search

4.2 Use case II: Use of secured logs for operator actions auditing

Short Description:

This use case aims at demonstrating how an accountability request performed by a court about surveillance operator actions can be handled within a privacy- and accountability by design system.

Actors:

- Victim of a car hijacking (citizen)
- Judge from court
- Law Enforcement Agency (LEA)
- System Operator (SO) which operates the video surveillance system
- Data Protection Authority (DPA)

Aims:

To provide and demonstrate an access control system to video management system, featuring authentication capabilities and authorization capabilities (applicable both to live view of videos and to their replay). Based on this access control module, to provide a logging and auditing tool of operator actions, and to demonstrate the use and interest of this auditing tool to process accountability-related requests about the operators' actions.

Note that the scenario that is proposed below (based on a criminal case) is intended to image the real-size, real-life interest of this scenario. In the demonstration, as recorded video footages will be used, the demonstration will be based upon a different case (depending on the content of the available video footages). The aim of the scenario will remain to demonstrate the power of auditing and logging tools (based on access controls to the recordings) to prove that a video sequence has been or not displayed on an operator workstation or video-wall, which is a very strong accountability statement.

Preconditions:

- Legal recording permission for IP
- Accepted viewpoint for involved cameras by DPA
- Accepted operators actions auditing strategy by DPA
- A crime is committed and a subpoena exists.

Scenario description:

The goal of this use case is to illustrate the interest of logging the operator actions.

Tabasco-City is equipped with a wide video surveillance system, featuring a very large number of cameras (10000). The surveillance of the city is performed by hundreds of operators using this system in conjunction with communication means (citizens, responders). The organization of the supervision is very complex as:

- Some operators perform the supervision from local police district buildings,

- Some operators perform the supervision from city-wide police headquarters,
- Some operators belong to the fire fighters organization,
- Some operators use sometimes the systems mainly for road traffic supervision.

Moreover, Tabasco-City is very well illuminated enabling a permanent supervision (day and night). A single operator position is used by several persons rotating.

The Tabasco city has nevertheless purchased a privacy and accountability –by design proven system, featuring advanced operators management policy. Moreover, a strict enforcement of the maximum retention period for video recordings is performed by the system (7 days retention period for some cameras, no recording at all for some others).

A woman was injured last week in a car hijacking in one street downtown. The judge required an extract of available video-footages from the place where the crime occurred (use case I). From this footage it appeared that images of the crime from a distant large angle camera were available (no sufficient details to identify the thief), but that nobody had neither noticed the problem live and given the alert, nor tried to focus the other cameras available within the zone to collect precious evidence information about the ongoing crime. This appears surprising, to the judge, but also to the population.

The judge decides to request the DPA administrator to perform an extract of the log bases of the system to understand:

- If someone (and who) was viewing the camera with clear crime images,
- What the operators in charge of the zone were watching at this precise moment.

It finally appears that the operators were all watching other cameras at this time. The video footages have shown that many other incidents that happened in the same time focused unfortunately their attention.

The dynamic view of this use case is shown in Figure 17.

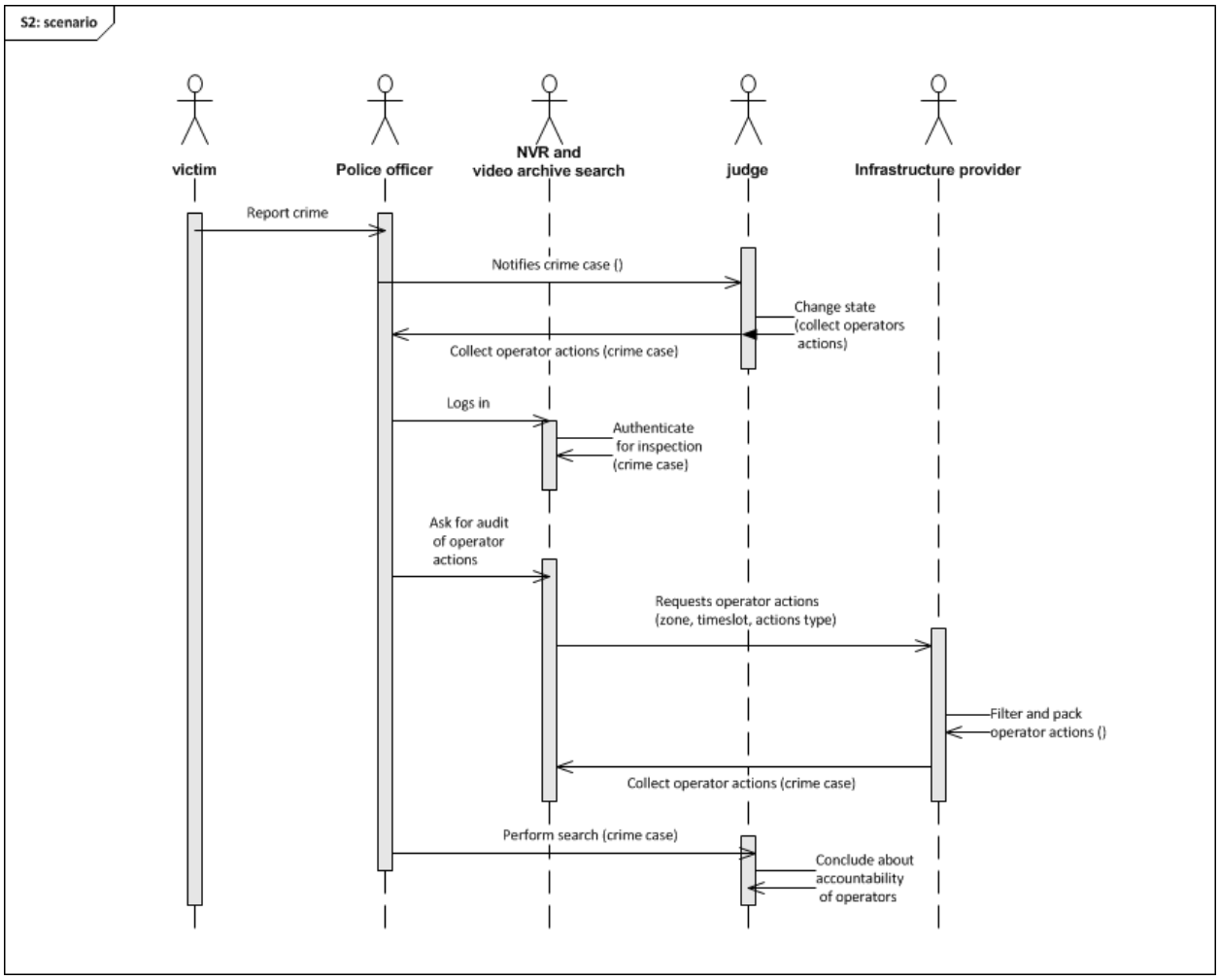

Figure 17: Dynamic view of Use of secured logs for operators actions reviewing and auditing

5. Demonstration Platform Specification

This section specifies the system architecture of the demonstration platform. In general, the demonstration platform combines the video surveillance and archive search components and capabilities from the two technological partners, AIT and THALES.

5.1 Architecture Diagram

The architecture consists two parts: a Network Video Recorder (NVR) from THALES, and a Video Archive Search (VAS) from AIT. The VAS connects to NVR for obtain stored video data for performing video archive search. The NVR and VAS can be regarded as foreground of the two technological partners. They are purely developed for video surveillance purpose, without privacy and accountability.

These components will be added to the architecture. The design of these components will follow the guidance of the SALT framework. See Section 5.2 for detailed component description, and Section 5.3 for interface description.

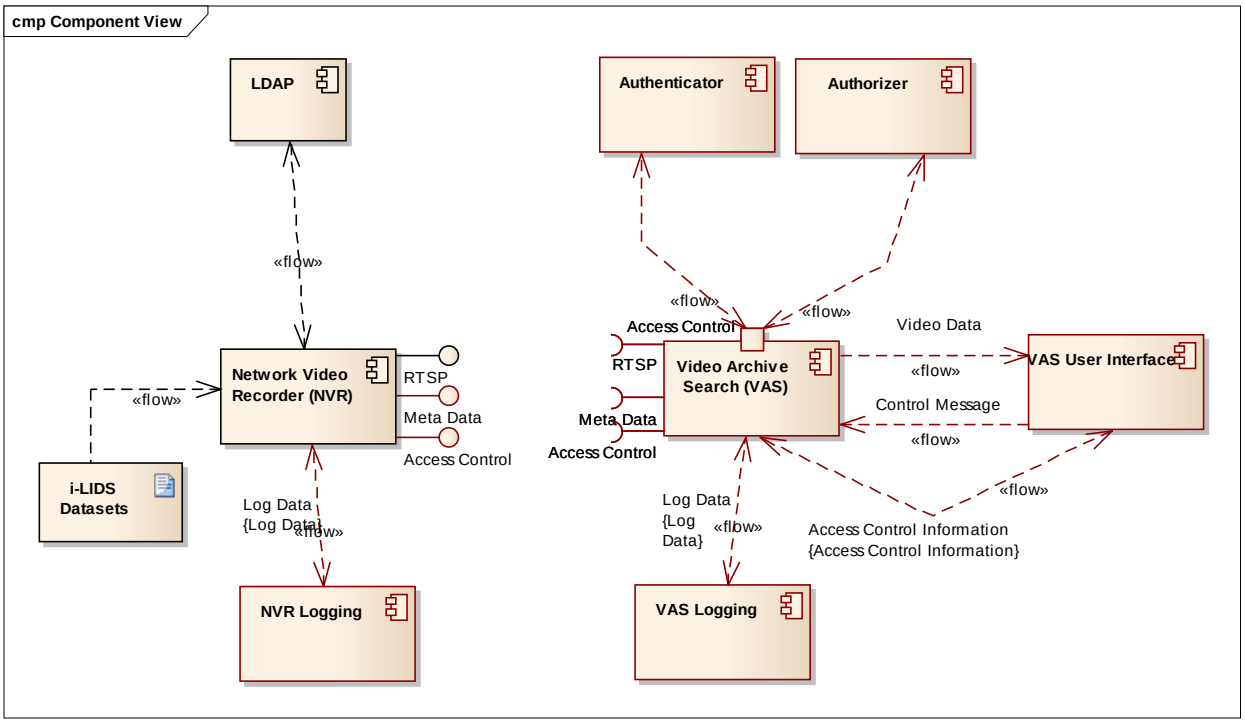

Figure 18: Video surveillance lifecycle management architecture

5.2 Description of System Components

- *i-LIDS Datasets:*
  - Dataset will be used for the simulation of camera recordings (https://www.gov.uk/imagery-library-for-intelligent-detection-systems). The material is provided by a UK governmental organization and contains material of public available scenes.
- *LDAP:*
  - LDAP (Lightweight Directory Access Protocol) represents a user directory server which stores the video surveillance lifecycle management system's users.

- *NVR Logging:*
  - This component will log all relevant activities carried out by the network video recorder.
- *Network Video Recorder (NVR)*:
  - The NVR stores the video data collected from multiple surveillance cameras. After receiving requests from the VAS the NVR responds with the requested video data.
- *Video Archive Search (VAS)*:
  - The VAS processes user input from the UI frontend. Search algorithms are applied on video data requested from the NVR.
- *VAS User Interface*:
  - This component represents the graphical user interface (GUI) for the VAS. It receives input such as search parameters, login etc. from the user and provides the resulting video as output.
- *Authenticator:*
  - The Authenticator is responsible for verifying the identity of a user that is logging in to the system.
- *Authorizer:*
  - The Authorizer component takes care of the access rights of users within the system.
- *VAS Logging:*
  - This component will log all relevant activities carried out by the video archive search.

5.3 Description of Interfaces

The main interface locates between NRV and VAS, assumed to be over a wide area network.

- *RTSP (Real-Time Streaming Interface) Interface:*
  - Format (typical format, the definitive form will have to be confirmed):

    RTSP://1.2.3.4/ Name_of_Camera/Delta_T/Duration/speed/login/password
  - *Name_of_Camera* is (somehow) the video source denominator
  - *Delta_T* is the video starting timestamp
  - *Duration* is the video end timestamp
  - *Speed* is the transmitted speed of data
  - *login* is the account login of the person (or system) requesting the streaming
  - *password* is the password login of the person (or system) requesting the streaming.
  - H.264 via RTP/RTSP with High profile

This RTSP request is an example of what could be achieved. The exact information and the attributes will be confirmed later in the project. We will also investigate the possibility to encrypt the video stream and the possibility to encrypt/hash the exported records (used as evidence by Police/court).

Besides, two optional additional interfaces are envisaged. However, the actual implementation of the two interfaces is subject to more detailed technical discussion, which will be finalised in D5.2.

- *Meta Data:* This interface is used to exchange video metadata.

- *Access Control:* This is a logic interface envisioned to allow the VAS for obtaining directory information at the server side (NVR).

5.4 Surveillance Capabilities

The surveillance capabilities will be simulated in the demonstration system. Note that no actual surveillance activities will be carried out. The video-footages that are used (streamed from the NVR) and analysed by the Video Archive Search, are the ones from the UK-government I-LIDS (Imaging Library for Intelligent Detection Systems).

The primary purpose of the I-LIDS database is to provide a reference dataset to compare Intelligent Video Systems from the detection performance point of view. This is of great importance with this industrial and research field mainly for the following reasons:

- Aggressive marketing by some suppliers of this category of systems that lead to performance statements that have to be checked,
- The market for Intelligent Video Surveillance is very fragmented, meaning that many suppliers and many solutions are available and remain to be assessed and compared.

The I-LIDS database provides datasets enabling performance evaluation for the following use-cases (six scenarios which are crucial to government requirements):

- Abandoned baggage: detection with alarm events consisting of unattended bags on the platform of an underground station
- Parked vehicle detection: with alarm events consisting of suspiciously parked vehicles in an urban setting
- Doorway surveillance: with alarm events consisting of people entering and exiting monitored doorways
- Sterile zone monitoring: with alarm events consisting of the presence of people in a sterile zone between two security fences
- Multiple-camera tracking: with Target events consisting of people (“targets”) travelling through a network of CCTV cameras
- New Technologies footage is made up of cooled and un-cooled thermal imaging and infrared illumination with alarm events consisting of pedestrian attacks over a large area and along a jetty and water based attacks.

This means that we emulate with the proposed demonstration system a wide range of use cases, especially within the video-analytics field and the forensics field.

Most of the components of a real-size real-life surveillance system do take part in the demonstration. Moreover, the use of these datasets limits the specific privacy mitigations that might have to be found about the demonstration system itself. These privacy issues would typically link to the privacy rights of the people that may be monitored. These privacy issues would moreover not be representative from the PARIS project point of view because the type of infrastructure we forecast to address is a public space rather than restricted working places.

The limits to the representativeness of the system (compared to a full size video surveillance system) are mainly linked to:

- The absence of real-time cameras within the system, which limit the possibility to harm privacy by e.g. reaching viewing problematic angles and zones by camera movements and zooming,
- The absence of interfaces with other surveillance systems (typically access control systems) that may cause wider harms to citizen privacy.

Globally speaking, most of the typical privacy harms (and therefore their related mitigations) and accountability enforcement that can arise on a full-size video system can be modelled, including e.g. the access rights of the operators to the data (raw video, results of processing), the audit of the operator actions, the protection of data transmission.

5.5 Description of Functional Components

A functional decomposition of the demonstrator adapted to architecture description and to the identification of requirements and tests is proposed below, by the identification of the following functional demonstrator components:

- *The Network Video Recorder*. It has the following main capabilities:
    - To connect to CCTV cameras, unicast or multicast,
    - To receive external alarms,
    - To record streams continuously or upon alarm,
    - To stream upon request records using RTP/H264,
    - To create video files from part of the recordings
    - To hash the video files and match candidate files with original file using hash.
- *The Network Video Recorder raw operating station*. It has the following main capabilities:
    - To display from 1 to 4 video streams (among the streams that were recorded by the NVR) simultaneously,
    - To provide simple controls enabling to select the cameras to be displayed,
    - To provide simple controls enabling to select the replay parameters.
- *The NVR authentication and authorization component*. It has the following main capabilities:
    - To implement the NVR operators access rights and segregation policies,
    - To provide and interface to an administrator to modify the NVR users privileges and accounts settings.
- *The NVR auditing and logging tool*. It has the following main capabilities:
    - To record the actions performed by the NVR upon external demand, along with the time and date and with the requestor name,
    - To provide an administrator interface enabling to perform enquiries.

- *The auditing tool dedicated to video recordings*. It has the following main capabilities:
    - To provide an analysis of the video files hosted within an NVR repository and to find the oldest video-data within the system
- *The Video Archive Search component*. It has the following main capabilities:
    - To apply to video footages selected video contents analysis algorithms
    - To apply to video content analysis result pre-defined correlation rules to extract meta-events
- *The Archive Search user interface component*. It has the following main capabilities:
    - To provide a capability to the operator to select the video footages to be analysed,
    - To provide a capability to the operator to parameter the video algorithms and fusion rules implemented by the archive search,
    - To provide a capability to the operator to display the results of processing and fusion performed by the Archive Search.
- *The Archive search authorization and authentication component*. It has the following main capabilities:
    - To implement the Archive Search operators access rights and segregation policies,
    - To provide an interface to an administrator to modify the Archive Search users privileges and accounts settings.
- *The communication component (IP network)*. It has the following main capabilities:
    - To enable transmission of data between other components
    - To secure these data transmissions
- VAS authentication and authorization component. It has the following main capabilities:
    - Authentication of a user by its predefined login credentials
    - Authorizatioin of a user's search operations based on predefined access rules and the user's access right.
- VAS logging component. It has the following main capabilities:
    - Log the user's search requests.

5.6 Consideration for Security and Privacy Components

It should be noted that we distinguish two sets of security and privacy components at both the VAS (client) side and the NVR (server) side. The rationale is as follows:

We anticipate that the access control requirements and corresponding information as basis for access control will be different at the client and server side. At the server side, access control focuses on who has the access to what stored video surveillance data; while at the client side, access control focuses on who has the right to perform what kind of search operation on the fetched video data. For example, a user might be granted access to 10 hours of video footage captured by Camera n at the NVR, but the user might not be allowed to search the 10 hours footage for a specific object. This is analogous to the recent EU privacy ruling that requires search engine Google to remove certain links from its search results, instead of asking the content provider to remove the original content from the Internet.

Although in commercial systems, these functions are often integrated into one Video Management System (VMS), for our demonstration, we take a modular approach, such that we can have a clear definition of functionalities in the demo system and to have the access to code based for development.

6. Requirements specification

This part is dedicated to the first level requirement specification, describing the most relevant requirements both from functional and technical viewpoints), at both the surveillance system level and the SALT framework level.

6.1 Functional and technical requirements about the surveillance system

The surveillance system architecture which is targeted to achieve as a demonstration is described in the Section 5 of this document. It is mainly based on the interfacing of one component provided by THALES (a Network Video Recorder, NVR) and of one component provided by AIT (the Video Archive Search, VAS), both working seamlessly to provide a coherent demonstration. This part of the document is dedicated to the requirements, from functional and technical points of view that are to be taken into account by this demonstrator.

These requirements are organized in 3 sections below:

- The first section is dedicated to generic requirements, that are of generic usage and which can be of interest for the 2 use cases,
- The second section is dedicated to requirements that are (at least within the field of the PARIS project WP5 demonstration) more specific and at stake for the correct running of the proposed first use case,
- The third section is dedicated to the requirements, which are specific to the second use-case.

The requirements are tagged with a category qualifying the type of requirement (functional, or technical). All of these requirements remain to be confirmed within the enhanced analysis to be produced in the D5.2 deliverable.

6.1.1 Generic functional and technical requirements

Requirement ID	Description	Category
RG_1	Provide a network video recorder (NVR) with base capabilities for video streaming and replay	Functional
RG_1.1	The NVR shall be capable to host I-LIDS video footages (full library) as H264 video streams	Technical
RG_1.2	The NVR shall be compatible with common off the shelves hardware and Operating system components	Technical
RG_1.3	The NVR shall be capable of responding to RTSP requests for video streaming	Technical
RG_1.4	The NVR shall be capable of streaming videos on an IP network as H264 over RTP	Technical

RG_1.5	The NVR shall provide an administrator interface enabling to monitor its operation	Technical
RG_1.6	The NVR shall provide a capability for an operator to visually inspect the videos that are recorded	Technical
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	Technical
RG_1.8	The NVR shall be capable of replaying data faster than real time (e.g. As Fast as possible)	Technical
RG_1.9	The NVR shall be capable of handling operator login/password embedded within an RTSP request for authentication	Technical
RG_1.10	The NVR shall be capable of exporting video data within a standard video file format for external replay	Technical
RG_2	Provide a Video Archive Search module with base capabilities for video analytics parameterization, application, and results display	Functional
RG_2.1	The VAS shall be capable of treating common format videos	Technical
RG_2.2	The VAS shall be capable of applying several types of Video Content Analysis (VCA) algorithms, upon operator choice	Technical
RG_2.3	The VAS shall be capable of proposing to the operator an interface enabling to parameterize the VCA algorithms	Technical
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 analyzed	Technical
RG_2.5	The VAS shall be capable of displaying the results of the processing performed	Technical
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	Technical
RG_2.7	The VAS shall be capable to be installed on a standard hardware and Operating System.	Technical
RG_2.8	The VAS shall be capable of handling operator login/password entered at login	Technical
RG_3	Establish a connection from an archive search system to a video recording device with different control	Functional
RG_3.1	The VAS shall be capable to be authenticated as a valid system by the NVR	Technical

RG_3.2	The VAS and the NVR shall be interfaced using existing video data transmission protocols RTP, Payload H.264	Technical
RG_3.3	The VAS and the NVR shall be capable to negotiate speed control of the video streaming	Technical
RG_3.4	The VAS shall be capable to send to the NVR login information from the VAS operator	Technical

Table 2: Generic functional and technical requirements

6.1.2 Specific functional and technical requirements for Use Case 1

The first use case deals with “Secure Law Enforcement Access to Video Archive Search”.

Requirement ID	Description	Category
RUC1_1	There shall be a mean VAS side to authenticate the persons involved in the search	Technical
RUC1_2	There shall be a way on the NVR side to restrict access in terms of data origin, timespan and video content	Technical
RUC1_3	There shall be a way on the NVR side to log all actions of the user	Technical
RUC1_4	There shall be a way on the VAS side to log all actions of the user	Technical
RUC1_5	There should be no way to manipulate the loggings VAS side	Technical
RUC1_6	There should be no way to manipulate the loggings NVR side	Technical
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.	Technical
RUC1_8	There shall be a way (essentially from NVR) to check the integrity of video recordings	Technical
RUC1_9	There should be a list of all technical interfaces of the software where data access can be performed	Technical
RUC1_10	There should be a list all entry/exit points for data of the complete system	Technical

Table 3: Functional and technical requirements for Use Case 1

6.1.3 Specific functional and technical requirements for Use Case 2

The second use case deals with “secured logs for operators’ actions auditing”.

Requirement ID	Description	Category
RUC2_1	The NVR shall audit all operator actions	Technical
RUC2_2	The NVR shall propose a mean to request and search operators actions	Technical
RUC2_3	The operators login information shall be transmitted from VAS to the NVR	Technical
RUC2_4	There shall be a mean to prove the integrity of the operators log and audit file	Technical

Table 4: Functional and technical requirements for Use Case 2

6.2 SALT framework requirements

This section describes the requirements of different users of SALT framework. Note that with respect to SALT framework, the general requirements are valid for both video surveillance systems and biometric system (cf. D6.1 “Biometrics Use Case Description”).

We identify four types of users to interact with the SALT Framework in video surveillance systems:

- The *System Designer*, who uses the framework to get recommendations concerning privacy and accountability for the design of the video-surveillance system, and who also use the framework to validate the design as SALT compliant.
- The *Law Enforcement*, e.g. police, who check the SALT framework to ensure that any investigation or request of video footage complies with existing data protection legal framework.
- The *Operator,* who uses the SALT framework for ensure day-to-day operations are privacy-preserving, or consults the SALT framework for instructions upon receiving requests for video data.
- The *Data Protection Authority*, who may require access to the recommendations that have been provided for the design of the system being audited.

The following describes the interactions of these users with the SALT framework. The users should first know which tools are provided by the SALT Framework, and which information can be extracted with them and how, so the framework shall be adequately documented. It is desirable that the information shared with the SALT framework is adequately protected and not shared to third parties, unless it is required for auditing purposes. In the same way, the accesses by the different users to the SALT Framework for the extraction of recommendations or for validation could be recorded.

6.2.1 Obtaining information from the SALT Framework

During design phase, the *System Designer* should be able to obtain guidelines from the SALT framework that facilitate the design of the surveillance system taking into account the privacy and accountability aspects from the start. These guidelines are provided in the form of concerns and recommendations of mechanisms that can be implemented to apply those

concerns. Besides, in some cases, the recommendations will be given with a set of OCL rules that can be used for the validation of the system.

As the guidelines depend on the specific context and features of the system, the *System Designer* shall be able to provide the characteristics of the system based on the requirements collected to the SALT Framework. This action requires the use of an interface that allows the *System Designer* to introduce information of the different type of requirements (operational, technical, business constraints, etc.), features and procedures that are relevant for the selection of policies and recommendations concerning privacy and accountability.

The SALT Framework will analyse these specifications and will search in the knowledge repository the instances that are most adequate for that particular system. These instances shall be provided to the *System Designer* in a user-friendly way, taking into account that the *System Designer* does not necessarily have background on ethics or laws, so it would be useful to provide also complementary information on how to apply the different recommendations.

The interface used for this process should be suitable at least for a user with the profile or skills of a *System Designer*, who has certain technical knowledge, and should provide feedback and visual hints to facilitate the process of extraction of knowledge from the framework.

Besides, requirements from the *Law Enforcemen*t and the *Operator* on the SALT framework might be regarded as a subset of the requirements as for the *System Designer*. Since System Designer needs to consider ALL technical and operational possibilities in order to facilitate the requirements from the *Law Enforcement* and the *Operator*, we can use the requirements from the *System Designer* as a basis, and elaborate whether we will need further requirements to represent *Law Enforcement* and *Operator*.

6.2.2Validating the system design

The *System Designer* elaborates a design of the video surveillance system based on the surveillance requirements as well as the guidelines obtained from the SALT Framework. Before the implementation and deployment of the system, the *System Designer* should verify that the design complies with the recommendations on privacy and accountability provided by the SALT framework. If the recommendations obtained in the previous phase include OCL rules, this verification can be automatically performed using the SALT Framework. In that case, an interface is required to introduce the design created and display the results of the validation process. This interface should be adapted for a user with a technical profile that may not have knowledge on system modelling, so the design shall be introduced in a format easily understandable by the *System Designer*. Besides, this interface should provide feedback and visual hints to facilitate the process of validation, including clear warnings to point to the concerns not fulfilled.

After being implemented, the system should also be validated anytime it is modified to check that the resulting system also addresses the SALT concerns.

6.2.3 Auditing the system

During the audit of the system, the *Data Protection Authority* may require access to the SALT Framework in order to review the technical privacy policies, logs and compliance rules in the SALT knowledge repository that have been used to elaborate the recommendations for the system being audited. The user of the SALT Framework in this case has background in laws and current regulations, but does not have to have any technical expertise, so appropriated documentation about how to use the framework is required.

6.2.4 List of requirements for the SALT Framework

Note that the same list of requirements also appears in D6.1 for biometric system. This list provides a generic SALT framework requirements.

Id	SALT Framework requirement
REQ_FU_0.1	Users should be adequately informed about the different tools provided by the SF, for which purpose and how to use them
REQ_FU_0.2	The information shared with the SF shall be adequately protected and not shared with third parties except for auditing purposes
REQ_FU_0.3	The accesses by the different users to the SF can be recorded
REQ_FU_2	The SALT management tool should provide an interface to system designer for describing context information of design requirements
REQ_FU_2.1	The interface for the extraction of recommendations shall be adequate for a user with technical profile
REQ_FU_2.2	The interface for the extraction of recommendations shall provide feedback and visual hints to facilitate its use
REQ_FU_2.3	The interface for the extraction of recommendations shall be adequately documented
REQ_FU_5	The Surveillance system designer introduces in the SALT management tool the specification of the Surveillance system
REQ_FU_5.1	The designer shall be able to introduce different type of requirements and features for the system
REQ_FU_6	The SALT management tool has to select a proper instance or instances based on the specification done by the system designer
REQ_FU_7	The SALT management tool shows in a proper way the recommendation to the new system based on the instances
REQ_FU_7.1	The information shall be provided in a user-friendly way, taking into account that the System Designer does not necessarily have background on ethics or laws
REQ_FU_7.2	The framework should optionally provide information on how to apply the different recommendations
REQ_FU_3	The SALT management tool might document the purposes and reasons for all decisions made in the design process
REQ_FU_9	The SALT management tool should provide pointers to existing compliance checking mechanisms to users of the framework, depending on the privacy

	policy language used, if any exist.
REQ_FU_10	The SALT management tool should provide pointers to relevant information, such as official specifications, in case the privacy policy language is a commonly used one
REQ_FU_4	The SALT management tool might be able to verify a system design is SALT-compliant or prompt warnings if the technical decisions harm privacy
REQ_FU_4.1	The interface for the validation of the system shall be adequate for a user with technical profile and without knowledge of system modelling
REQ_FU_4.2	The interface for the validation of the system shall provide feedback and visual hints to facilitate its use, especially when the system is not valid
REQ_FU_4.3	The interface for the validation of the system shall be adequately documented
REQ_FU_11	The SALT management tool might be able to issue a certificate guarantying the design process has been SALTed
REQ_FU_12	The SALT management tool might be able to propose a check list that enables to check periodically that the system privacy level has not been modified
REQ_FU_13	The SALT management tool may be able to propose light guidelines enabling fast SALT compliance checking when slight modifications are realized
REQ_FU_8	Auditors should have access to technical privacy policies, logs and compliance rules in the SALT knowledge repository through the SALT management tool

Table 5 List of SALT Framework requirements

7. Specification of evaluation criteria

This section outlines the criteria for evaluating the use case at SALT framework level and at design process level. These criteria cover different aspects during the video surveillance system Lifecycle. Note that similar criteria are also used for evaluating the biometric system described in D6.1 “Biometrics Use Case Description”.

7.1 Evaluation at the SALT framework level

The objective is to evaluate if the SALT framework provides the results expected at the different stages of the lifecycle of the system proposed. For this, it is first necessary to define the **goals** or aspects of the framework that have to be evaluated (SFG_X).

- *SFG_1: Functional aspects of the SALT Framework*

  The SALT Framework shall provide all the capabilities required by the different users during the video surveillance system lifecycle, thus the first goal consists of evaluating if the SALT Framework includes all the functionalities needed, which are:
  - Provide a tool to introduce the specification of a system.
  - Provide a list of references about accountability and privacy for a particular system.
  - Provide a tool to introduce in the SF the profile of a video surveillance system.
  - Provide a tool for the validation of the system (OCL rules).

- *SFG_2: Data requirements for the SALT references*

  The SALT references shall provide useful information for the design, development and deployment of SALT compliant systems. Thus the second goal is to verify that the references provide the necessary concerns and recommendations about privacy and accountability, and that they are adequate to the system specified. For the evaluation of each reference, these are the aspects that will be considered:
  - If they are able to provide useful information to help make design decisions
  - If they are reliable and cover the most important concerns
  - If they do not provide unrelated information or the amount of unrelated information is acceptable

  A set of test use cases can be used for the evaluation of this criterion, to evaluate if the SALT Framework provides the references expected for existing and known SALT compliant systems.

- *SFG_3: Usability of the SALT Framework*

  The SALT Framework shall be adequate to its users, so this goal will be focused on evaluating usability of the framework. In particular, the requirements of Section 6.2.4 will be checked. This evaluation can be performed through surveys and questionnaires that collect the feedback of a group of test users.

The following table summarizes the aspects that should be evaluated for each of the goals defined:

Goal	Evaluation criteria	Aspect to evaluate	Type of evaluation	Instrument
SFG_1	The SALT Framework includes all the capabilities required during the design process	Usefulness/ Functionality	qualitative	Human inspection: verification that all the tasks listed under SFG_1 can be performed with the SALT Framework.
SFG_2	Appropriateness of the references to the system specified	Efficiency	qualitative	Human inspection: check if the recommendations are really applicable to the system specified. Use of test cases.
SFG_2	Provision of concerns about accountability	Efficiency	qualitative	Human inspection: check if the references cover the main accountability concerns for the system specified. Use of test cases.
SFG_2	Provision of concerns about privacy	Efficiency	qualitative	Human inspection: check if the references cover the main privacy concerns for the system specified. Use of test cases.
SFG_2	Accuracy of the references	Reliability	qualitative	Software or human inspection (experts) of the information sources: check if the references are valid and updated. Use of test cases. ** UMA is studying to apply reputation software based on user and expert opinion.*
SFG_3	Easy to learn	Usability	quantitative	Time required to perform several predefined tasks
SFG_3	Easy to use	Usability	qualitative	Survey to extract the opinion of different users

Table 6: Evaluation criteria at SALT Framework level

7.2 Evaluation at the system level

In this case, the criteria are focused on evaluating if the design process defined leads to the creation of a SALT compliant system. For this evaluation, these are the goals defined (*DPG_X*):

- *DPG_1: Functional aspects of video surveillance system*

  A SALT compliant video surveillance system shall provide a certain surveillance service, so the first goal of the evaluation at this level is the verification that the system does what it is supposed to do. The functional requirements are specified in Section 6.1.
- *DPG_2: Legal requirements*

A SALTed system shall comply with the current regulations on privacy and data protection in the context for which it was built, so the compliance of the legal requirements shall also be evaluated. This task should be performed by legal experts.

- *DPG_3: Socio-ethical requirements*

  A SALTed system shall also take into consideration the socio-ethical issues, thus the awareness of the system about the socio-ethical concerns shall also be evaluated by experts on this field.

- *DPG_4: Privacy and accountability requirements*

  Finally, the measures implemented for privacy and accountability will be evaluated. It is important to verify if the mechanisms for data and privacy protection, and the different policies and procedures defined are sufficient to cover the main privacy and accountability requirements. This evaluation can be performed by inspection, and also through a set of test cases covering the negative scenarios where the threats to privacy appear.

This table enumerates the main evaluation criteria to consider at design process level:

Goal	Evaluation criteria	Aspect to evaluate	Type of evaluation	Instrument
DPG_1	The system provides the surveillance service for which it was built	Usefulness/ Functionality	qualitative	Human inspection: check if the system performs the specified functions. Use of acceptance test cases.
DPG_2	The system complies with the laws in the context for which it was built	Legality	qualitative	Human inspection: check if the system complies with the current legislation.
DPG_3	The system shall take into consideration the main socio-ethical concerns	Socio-ethical awareness	qualitative	Human inspection: check if the system addresses the main socio-ethical concerns.
DPG_4	The system shall take into consideration the main accountability concerns	Accountability	qualitative	Human inspection: check if the system addresses the main accountability concerns.
DPG_4	The system shall cover the main privacy requirements	Privacy	qualitative	Human inspection: check if the system addresses the main privacy concerns.

Table 7 Evaluation criteria at design process level

8. Summary

This deliverable integrates video archive and search technology in the SALT conceptual frameworks, and specifies video surveillance lifecycle management use cases.

We present details on video surveillance system and video archive search from a technical and functional point of view. We also describe the privacy aspects of the technology and ways to integrate the technical dimension into the SALT framework.

Most importantly, we specify a high level view of use case scenarios and the demonstration system platform architecture. Moreover, we specify requirements and evaluation criteria of the use case and platform. The use case will be further developed in the upcoming tasks of WP5 (e.g. T5.3) to demonstrate and evaluate the SALT framework.