FRONT PAGE

PUBLISHABLE SUMMARY

Grant Agreement number: 312784

Project acronym: P5

Project title: Privacy Preserving Perimeter Protection Project

Funding Scheme: Collaborative

Period covered: from August 1st, 2013 to October 31st, 2016

Name of the scientific representative of the project's co-ordinator, Title and Organisation:

Dr. David Lindgren, The Swedish Defence Research Agency, FOI

FOI Document Designation: FOI-2012-1668

Tel: +46 (0) 8 555 030 00

Date: December 3, 2016

E-mail: david.lindgren@foi.se

www.p5-fp7.eu

Content

Executive Summary

A central project objective is to describe an efficient and proactive perimeter protection system for critical buildings. The envisioned system is by design privacy preserving, which means that there are built-in functions to protect and restrict the visibility of private data, for instance from high resolution cameras.

The typical system end user is a security operator with a mission to control the area around a protected facility or building, and call in guards or the police if a security threat is observed. In this respect, the P5 system is developed as an efficient tool for the operator with sensor support for an early warning of imminent security breaches. The user requirements on the sensor system have consequently been established by interviews of security staff at power plants in Sweden, UK and Spain. Statements from the staff have been compiled to system capabilities that have formed the scenarios worked with and directed the P5 research efforts. The details of the resulting requirements are classified information, but in essence they confirm the anticipated need for an around the clock early warning support that is robust against weather and climate variations.

From an architectural viewpoint, technical support for early warning around the clock implies large area multi-modal sensor coverage, which in turn typically requires a large number of sensors, and also sensors of complementary types. A conclusion is that an advanced surveillance system architecture needs to support an infrastructure of geographically distributed sensors with automatic detection, tracking and classification of objects that enter the control area.

The envisioned system, with a high level of autonomy regarding detection and tracking of humans, raises both legal and ethical concerns. A special case study has been conducted regarding which implications a virtual fence would have if it would be used at a public prison in Belgium. Furthermore, the P5 system is designed with privacy preserving functions from the start that control the access of private data, for instance images. These privacy functions are based on the European legal framework. P5 has an advisory board with ethical and legal experts as a support in privacy matters. The advisory board also reports to the European Commission.

P5 sensor nodes have autonomous capability for target detection. An advanced robust motion segmentation technique for visual cameras, combined with a local tracker based on stochastic diffusion search provides real-time visual detection performance in the P5 system. A new tracking algorithm has been developed especially for thermal imagery and clearly outperforms previously published methods. Two methods have been invented for reducing background contamination the effects of thermal detection noise that are called *background-weighted distribution field tracking* and *adaptive object region distribution field tracking*, which are independent of each other and can this easily be combined. Algorithms for ground object detection and tracking with both thermal and visual images have been embedded on an AXIS camera that supports the execution third party applications. UAV detection has successfully been approached with background subtraction combined with track-before-detect algorithms. Privacy filtering techniques have been developed that distort the visual appearance of humans beyond recognition, although they preserve the usefulness for the operator.

Both the software and hardware performance of a 24 GHz radar unit has been advanced in P5, and elevated the radar unit as a complementary surveillance system capability. A radar network controller features the interconnection of up to 4 radar modules with a CAN-bus interface to the P5 sensor network. Connecting multiple radars this way extends the area coverage, which increases the usefulness of the radar in many surveillance contexts. The radar features target classification based on micro Doppler patterns that stem from the characteristic movements of, for instance, arms and legs of animals or humans or the revolving blades of a helicopter. By using a support vector machine together with a set of signal features, we have demonstrated classification between human and animal with encouraging results.

Sensor fusion algorithms combine the input from multiple sensors into a compact and informative data for the user, for instance in terms of object tracks and alarms. An important research challenge is that of associating multiple objects in the data from multiple sensors, which is a difficult but necessary step into forming a common state estimate. For this purpose we use an advanced multi-hypothesis target tracking algorithm,

which, although very computer intensive, gives real-time performance in the P5 scenarios. The target tracker requires that sensors are geo-calibrated in a global coordinate system, which has been achieved with excellent precision by the manual use of land survey techniques combined with well-known calibration procedures. However, promising experiments have also been done to automatically identify geometrical correspondences between sensors, for instance between a camera and a radar sensor. Classifying objects as either a vehicle, an animal, a human or other is done by image-based multi-class boosting techniques at the sensor level, and classifier fusion at the system level. An indicative behaviour is a behavioural pattern that a priori is known to be associated or correlated with situations that escalate to violence or crime, and that motivate an alert to the operator. An early warning module automatically detects such behaviours by analysing object tracks. The module is capable of detecting behaviours such as speed change, direction change, meeting, split/Leave, detach, catch up, and reconnaissance. The output of both the target tracker and the early warning module are presented to the user via specially developed human machine interfaces that both alert the operator in real-time and allow the forensic inspection of past event.

A selection of components ranging from detection to the early warning module are integrated into the real-time P5 demonstrator. The integration is partially based on open software libraries for network communication like ZeroMQ and ProtoBuf, and can manage live data streams as well as pre-recorded sensor data. The integrated system, along with standalone modules, have been demonstrated in front of an invited audience first in the UK, March 20, 2016, and finally in Sweden, October 5, 2016. Results have also been disseminated by scientific publications and active participation at both technical and privacy related workshops, conferences and exhibitions.

Context and Objectives

The vision of the Privacy Preserving Perimeter Protection Project, P5, is an intelligent perimeter proactive surveillance system that works robustly under a wide range of weather and lighting conditions. The system will monitor the region outside the security area of critical buildings and infrastructures, and give an early warning if terrestrial or airborne threats are approaching. The envisioned system will support, rather than replace, a human operator. A low false alarm rate from animals or other innocuous events, combined with high threat detection sensitivity and privacy standards, are central ambitions of the project.

By design, the envisioned systems will handle current as well as expected future requirements on privacy preservation and surveillance system legislation. The aim is to describe a sensor system that for different protection contexts can be tuned to balance between potent but potentially invasive surveillance techniques, and the personal integrity of the citizens. The sensor system should adhere to a publicly accepted principle of proportionality. To monitor the privacy aspects, P5 has a group of independent advisors with expertise in ethics and law.

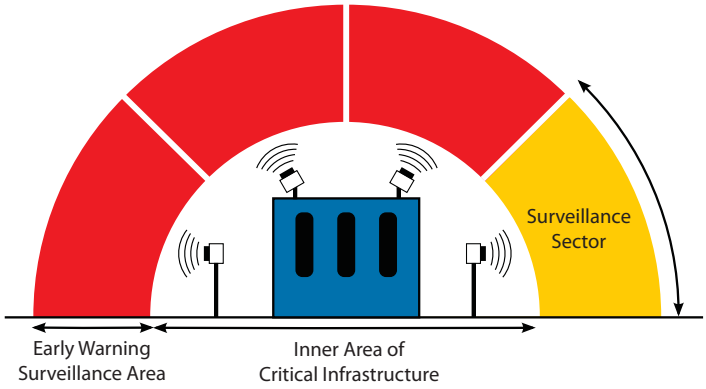
The P5 project is strongly user driven and the goal of P5 is to demonstrate beyond state-of-the-art surveillance abilities at the OKG nuclear plant outside Oskarshamn, Sweden, and at CAST outside London, UK. Both demonstrations will display new functions that are aimed at enabling a more cost effective perimeter protection of critical infrastructure in relevant scenarios, and that are privacy preserving, practically useful, and commercially successful. P5 goals also include contributions to the technological and scientific community in the form of articles, workshops and conference presentations, and contributions to the ethical and legal community in the form of reports and workshops. To make sure that the technical achievements are in line with end user needs, P5 has an advisory stake holder group with international representation from both critical infrastructure protection and surveillance providers.

Threats of particular interest are terrorists, saboteurs and thieves approaching from land (walking or in vehicles), water (boats), or air (mainly small aircraft, UAVs). The envisioned system will give automatic and reliable alarms to an operator that make the final threat assessment. The alarms are based on radar, thermal and visual cameras collaborating in a network where sensor fusion and anomaly detection support efficient and robust surveillance of large areas with limited sightlines. The work within P5 has a focus on large area surveillance outside the physical perimeter (fence) of critical buildings. The objective is to give an *early warning*,

that is, the operator should be given the opportunity to react on the threat well before it reaches the perimeter of the inner area of the critical infrastructure. Therefore P5 has the focus on the early warning surveillance area, see figure below. If, despite all measures taken, the perpetrator manages to reach the fence undetected, there may be little time left to prevent unauthorized ingress and a security breach of magnitude may then follow in the worst case.

Scenarios

The P5 scenarios are based on the needs of the users and they have a focus on critical infrastructure intrusion attempts. An important effort in P5 is indeed paid to identify the user needs. The scenarios are developed to give a common and tangible context for both the technical development and for the final demonstrations. For instance, in one of the scenarios, we aim to detect suspicious movements by potential intruders in an area with otherwise innocent people or authorized personnel.



The scenario set also includes transportation of goods (weaponry) with an aerial drone, as well as movements of cars and animals. The scenarios was staged for data acquisition at both the OKG nuclear plant outside Oskarshamn, Sweden, and at the CAST test and training facility outside Horsham, UK. At OKG we staged a major part of an intrusion scenario as well as different bits of scenarios to get much variation needed for development and evaluation of algorithms, see the photographs below (from left to right): one of four elevated sensor platforms built for the scenario, an example of sensor kit with thermal and visual cameras, the 24 GHz radar module developed in P5.



Expected impact of P5

It is anticipated that P5 will contribute to the understanding of how critical infrastructures can be protected in a both cost effective and privacy preserving manner. A number of enabling techniques for this protection will be developed and integrated into a system architecture where the privacy preservation is an integral part of the fundamental design. A narrow selection of these beyond state-of-the-art techniques are

- Image based detection, classification, and tracking techniques for visual and thermal sensors.
- A sensor system concept where new surveillance abilities are enabled by fusion and algorithms for automatic threat detection together with efficient human-machine interaction.
- Built in privacy modules and filters.
- Small radar sensors with new network techniques and classification abilities.

New knowledge produced in P5 has been published and these publications are expected to have impact through the scientific community. The new techniques will both enhance the critical infrastructure protection to benefit the security and well-being of the citizens, as well as give European enterprises better chance to take marked shares in the expanding security sector. Two technique demonstrations, the first in the UK, the final in Sweden, are aimed at encouraging the privacy discussions and inspiring users and authorities to consider new opportunities with both state-of-the art and future surveillance techniques.

Main S&T results/foregrounds

Outline

This summary starts with the P5 scope of privacy and activities and results related to the ethical and legal research are presented. The ethical and legal advisory board is also introduced. Then follow the User Requirements section, where we discuss how the user needs have been accounted for, how relevant security scenarios have been developed, and research sensor data been acquired. The System Architecture section addresses how the user and privacy requirements form the design of an effective sensor system. The architecture is an important result and also the fundament for the P5 demonstrator. The Thermal and Visual Solutions section presents new detection techniques for thermal and visual cameras. The Radar Solutions section introduces new concepts for radar based surveillance capabilities – detection, tracking and classifications using efficient 24 GHz radar modules as a complement to visual and thermal cameras. The Early Warning Solutions section presents fusion algorithms that refine the input from multiple sensors to an efficient and effective decision support for the user. Integration and Validation presents the efforts and results regarding the integration of the P5 demonstrator and how project results have been validated. Finally the Dissemination and Exploitation section summarises the efforts made to publish results, participating in workshops, and otherwise spreading the new knowledge developed in P5.

In each technology related section we reflect our view of how the proposed techniques could and should relate to the P5 core principle of “privacy-by-design”.

Scope of privacy

An important objective in P5 has been to explore the scope of the major privacy issues raised by the technologies at stake into the project and by the system to be configured. In the P5 Deliverable 2.1 Social Acceptability Studies, we have proposed an ethical and sociological analysis of the issues related to privacy raised by the “virtual fences” developed in the P5 project.

First, we acknowledged that virtual fences are still at a very early stage of development, hence being still prospective in scope and tentative in their outreach. Because they are still prospective in scope and tentative in their developments, virtual fences don’t have yet a public, which could be addressed *per se*. There are not visible in the public area, they do not raise controversies, there are no local settings where there are to be found as such. The solution methodologically to solve this issue was to adopt a “speculative” approach. In an experimental manner we tried to figure which kind of issues virtual fences could give rise to, in which kind of

social settings they might get inserted and, lastly, we tried to anticipate / speculate on their potential effects and consequences. Using qualitative and quantitative methods, we organized what we called "deliberative arena" where we have debated these effects:

- The first “arena” is called “internal” in the sense that it encompassed P5 partners themselves and explored the question of how they frame “normality” as in “detecting abnormal behaviour”.
- The second arena is the public of prisons. We elaborated on prisons as a case study and try to unfold a variety of prospects regarding the way Belgian prisons work, with in mind the question of “what would happen if a virtual fence device was ready to implement in Belgian prisons”? In this case study we questioned the potential effectiveness of such a technology in a social context such as this one, and try to highlight many practical challenges in situation.
- The third deliberative arena deals with the “public opinion” at large, trying to suggest what virtual fences could do or not do in a variety of settings. To do that, we set up an online survey that gathered 288 complete answers but which has met some limitations, which we make explicit.

The results of P5 privacy research have been presented on several occasions:

- During the first meeting with the P5 Ethical and legal advisory group (ELAG) (10 march 2015)
- On the International Conference on Computers, Privacy and Data Protection, CPDP, January 2015, Brussels. P5 was part in the panel “Ethics of the security researcher”.
- CPDP, January 2016, Brussels. P5 was part of the panel “Ethical and political dimensions of virtual fences”.
- We presented the results of P5 deliverable 2.1 Social Acceptability Studies at a workshop organized on the virtualisation of surveillance with Olivier Razac 13 May 2016, in Namur, Brussels.

Privacy and ethical requirements

An objective of the P5 privacy efforts is to integrate the privacy dimension (based on legal and social issues) as design criteria for the P5 technology. An important objective has been to define the ethics and the privacy’s requirements of the system based on P5 results. Different privacy constraints have been identified. More specifically, the rights to privacy and data protection have been considered as relevant to the issue of virtual fences for the security of critical infrastructure. The P5 deliverable 2.2 Privacy and Ethics Implementation discussed the legal impacts of virtual fences from this human rights perspective, including both the right to private life and the right to data protection. In particular, the analysis of the relevant ECHR case law allowed us to identify the human rights requirements applicable to the installation of virtual fences in a specific context. Besides, a presentation of the legal framework of data protection applied to the context of video surveillance in EU legislation and some national legislations contributed to illustrate the complexity of the legal framework to be taken into account prior to the deployment of such technology in a specific given context. We presented the results of this research on different occasion:

- During the second meeting of the P5 ELAG group, at the University of Namur, 2 December 2015.
- During the P5 Stakeholder meeting at University of Reading, 20 January 2016.
- During the 1st Demo at CAST in Horsham, 20 April 2016.

Privacy Protection Implementation (Privacy-by-design)

The first period of the project focused on the design of the P5 system where the privacy aspects were taken into account for every task of the project. These include the P5 user requirements analysis, the design of the P5 system architecture, the design of privacy enhancing technology in visual and thermal cameras and the integration of the privacy protection modules in the P5 demonstrator.

Privacy and legal aspects have influenced the P5 system requirements from the start. We used the EU directive 95/46/EC for analysing the legal requirements for personal data usage and processing. The ethical studies were also conducted in order to have the view from people who may be affected by the system when it is deployed. Based on the P5 user requirement definitions, we translated those requirements into functional system requirements (required system capabilities) and then proposed a complete P5 system architecture. We adopted the privacy-by-design approach for P5 system where the privacy protection issues are taken into account for every step of data processing and the privacy protection modules were introduced in the system architecture level. To ensure a proper privacy protection in the P5 architecture, we introduced three modules: a Privacy-filter, a Privacy-aware access control module (PACM) and a Trusted Third Party (TTP). The privacy filter is responsible for filtering the privacy-related information, for instance, if an object is a physical person, it hides the face of that person. The PACM is responsible for controlling the access to raw data generated from sensor. It decides who is allowed to access raw data based on the access control policies defined by TTP administrator. TTP is responsible for controlling the processing of personal information in P5. These include, defining access control policies, defining user account and tracking user activities in the system.

After the initial definition phases of P5, the main focus of the privacy work shifted towards the implementation of the privacy protection modules and integration of such modules into the P5 demonstrator. Particularly the following three important modules, which are responsible for controlling the usage of personal data of individual who may be affected by the surveillance and ensuring the accountability of personal data usage, and which all have been demonstrated at the P5 final demo at CAST in Horsham, 2016:

1. Authentication and authorisation module: this module is responsible for controlling who can use the P5 application through which user can access data generated from sensors installed in the protected facility. User is authenticated with an account representing by his username and password. The authentication server is developed as Java package connecting to P5 player, which is used to view data from visual or thermal camera. The secure username and password storage and processing is also developed and integrated into the authentication server. Hashing function (MD5) is used to transform the plaintext password into human unreadable text before storing it into a *MySQL* database. We also integrated authentication and authorisation server with P5 player module

2. Privacy-aware access control module: once user is authenticated, he can access data from different sensors installed in the facility when needed, by default he can access only filtered data. Access to raw data from visual or thermal sensors are subjected to another level of control by a module called “privacy-aware access control module”. This module controls access to such data, like who can access under which conditions, based on the predefined access control policy, which is generally defined by authorised trusted third party (TTP administrator). Since raw data from visual or thermal sensor bears privacy-related information, it is necessary to control who have accessed to such data in which circumstances. This kind of control allows us to limit unnecessary access to raw data. Other role of privacy-aware access control module is to record all the access activities of users in the system for auditing purpose. Authorised trusted third party performs the auditing of users’ past activities. We implement privacy-aware access control module in the high-level computer programming language Java with the support of standard software libraries for working with data on the XACML format (eXtensible Access Control Markup Language). We also successfully integrated the privacy-aware access control module with P5 Player module developed in the computer programming language Python with the help of a software library for computer communication called *ZeroMQ*.

3. Trusted Third Party: to ensure the accountability of personal data usage in P5, we propose to use an entity called “Trusted Third Party”. This entity can be inside or outside protected facility. We developed a system called “trusted third party” system, which is responsible for creating users, defining the access control policy for every user in the system and auditing users’ activities. Trusted Third Party is developed in Java where we use *MySQL* database for storing users’ activities. This module has been tested and validated.

For privacy protection and access control issues in P5, before the actual implementation in P5 system, we have conducted a thorough research on privacy-by-design system architecture for P5 as well as privacy-aware access control. Consequently, we have published two scientific papers. One paper published in 29th Annual IFIP WG 11.3 Working Conference, DBSec 2015, Fairfax, VA, USA, July 13-15, 2015 with the title "Protecting Personal Data: Access Control for Privacy Preserving Perimeter Protection System", see [1]. The first publication dedicates to the P5 privacy-by-design system architecture, the privacy-aware access control model and system and the implementation of such system.

The second paper was published in the form of poster in the Second Industrial Surveillance day, 12th IEEE International Conference on Advanced Video-and Signal-based Surveillance, August 25-28, 2015, Karlsruhe Institute of Technology Fraunhofer IOSB, Karlsruhe, Germany with the title "Protecting Personal Data in Privacy Preserving Perimeter Protection System: From Legal to Technical Requirements and Implementation", [2]. The second publication focuses mostly on the legal and ethical studies, the user requirements and how we translate the legal and ethical requirements to technical requirements for P5 system design and implementation.

The P5 Ethical and legal advisory group (ELAG)

The ELAG consist of three experts on legal and research ethical aspects that are specially engaged in issues with modern surveillance technology and personal data usage. The role of ELAG is to support P5 in issues regarding laws and ethics, and also to finally summarise their view of the P5 project to the European Commission. Two meetings with the ELAG group have been organized in Namur. In the first meeting in March 2015 the discussion was focused on the P5 work with user Requirements and Privacy

- Discussion based on the user requirements: Presentation of user requirements and scenarios discussion.
- Discussion based on privacy: Presentation of the P5 deliverable 2.1 Social Acceptability Studies; findings and Presentation of the prison use case.

In the second meeting in December 2015, the discussion was based on

- P5 deliverable 2.2 Privacy and Ethics Implementation.
- Early warning module.
- Trusted Third Party and Access Control Module.

Privacy FAQ and roadmap

A task in P5 has been to collect and answer Frequently-Asked-Questions (FAQ) about ethics and technology assessment. An objective has also been to elaborate an ethical roadmap and to collect methods and best practices to help other projects to manage the balance between security and privacy. In that aim, a list of core legal questions that should addressed in the course of a surveillance project and Frequently-Asked-Questions about ethics and Technology Assessment has been provided. The results of this task have been integrated in the P5 deliverable 2.2. Privacy and Ethics Implementation:

- In a first step, we identified questions to be addressed in the course of the development of a surveillance project concerning the security of a Critical Infrastructure.
- Then we answered Frequently-Asked-Questions about ethics and technology assessment.
- Thirdly, we provided a list of references relating to assessment tools.
- Participatory methods.
- And privacy by design.

User Requirements

The purpose of the P5 user requirements is to guide the technology development towards relevance for the users, where a user could be a security operator or an organisational unit responsible for the protection of a critical building, etcetera. The task to determine and formulate the user requirements has been carried out in two steps. First we assess the user needs through extensive interviews, and secondly these needs, or rather the statements of the interviewees, are analysed and reformulated in terms of surveillance system capabilities. The details of this methodology are published in [3, 4]. Through the interviews, problematic situations could be identified, and also useful technical solutions suggested. The P5 user requirements in its whole will not be made publicly available since it may potentially inspire criminal minds or terrorists to exploit weaknesses in the protection of our critical buildings. However, some general conclusions are given below.

Users of surveillance systems guarding critical infrastructures require early warning of threats to their facility in order to alert security personnel and secure the operations in case of an imminent threat. The security personnel needs to keep track of persons and vehicles moving in the vicinity of the perimeter of the restricted area to be able to determine if any one may pose a threat. The staff needs to detect forbidden and suspicious behaviour in order to determine if there could be hostile intents behind. Some behaviours are described by the staff but they also need to detect unusual behaviour and determine if the persons behind could pose a threat to the facility. Behaviours include relations between persons and vehicles and to some extent objects, small flying aircrafts and boats.

A person leaving or joining a group of people may be suspect in some circumstances or a person diverting from a pathway into the woods. Around many critical infrastructures it is necessary to keep a high consistent security around the clock and around the year. The surveillance must be operational continuously and with the same level of security. If one subsystem cannot cover every situation, other systems will have to cover. It is necessary to view outside the perimeter to get early warning implying that in many cases the area under surveillance is public. The user's stress that they follow the current regulation on where and how to conduct surveillance. The values at risk differ to a wide extent and thus what measures are justified. The values range from public health, delivery of services critical to society to business values. The users stress both requirement to respect privacy and to keep a sufficient level of security to keep the risk of damage sufficiently low.

It is not uncommon that wild animals move around close to the perimeter. A specific requirement is that the number of false alarms due to animals and other events not threatening the facility must be kept low to ensure the usefulness of the surveillance system. A late alarm or a failed alarm in the event of an attack on a critical infrastructure may have severe and even catastrophic consequences on society. But also false alarms bring about costs and may have consequences on society in case unnecessary action are taken to secure the facility.

Scenario definitions

The P5 scenarios are developed to encompass interesting chain of security related events that are relevant to the P5 users. The purpose of the scenarios is to focus the research efforts towards common goals and towards a common result demonstrator. The chain of events are divided into scenes to be staged at the data collection campaigns. The scenes are designed to be relevant for wide set of situations including threats and normal events outside the perimeter of a critical infrastructure. The scenes include persons, vehicles and animals moving in the vicinity of the perimeter. Their behaviour include both actions considered normal and actions that could be motivated by intentions to harm the facility and thus should be considered a potential threat and be ground to alert the security staff.

The scenario includes a sketch of an imaginary plan of an intrusion into a critical infrastructure. The infrastructure is situated on a peninsula in a rural area. The perimeter of the facility has a fence and tight security. The facility welcomes interested persons to visit the facility in guided groups. There is a security check at the entrance so it is not possible to bring any unauthorised equipment into the facility. The plan of the intruders is that one person follows a guided group into the facility, diverts from the group trying not to be noticed. Moves on the ground in the facility without being noticed to a place to where the equipment has been air-

lifted in with a small radio controlled helicopter. The person transporting the equipment arrives by boat outside to the perimeter to launch and fly the helicopter.

The normal activity in the vicinity of the critical infrastructure includes persons moving, could be both on streets and pathways and in the woods. Staff and security guards pass from time to time and there are some traffic with vehicles. There could also be wild animals.

The scenarios include persons moving outside the perimeter of a critical infrastructure, vehicles, both aerial and land based and objects. The scenario includes relations between persons, e. g. belonging to a group, meeting, forming a group, moving together, and leaving a group. Animals are also indirectly part of the scenario because in many places there is a problem that animals are mistaken for persons. Our scenarios reflect areas outside the protected area which in many cases mean public areas and possibly restrictions on surveillance due to respect for privacy. We decided to consider public areas with persons moving around. It could be a public pathway where some peoples pass. We decided not to consider crowded areas. The activities of the perpetrators range from reconnaissance to early stages of an attack.

The figure below illustrates one of the staged scenarios including an intruder. There is a restricted area behind a perimeter with fence and surveillance systems. It is public area outside the perimeter meaning that the public is allowed to move and dwell as long as they do not have any intentions to harm the facility. A damage to the facility means loss of serious values which could include health, life and environment. The security staff need to discriminate between staff, public and perpetrators before an attack on the fence or perimeter while respecting privacy of the public.

End user engagement

End users have had an important influence on P5. First a number of end users are involved into the process of determining the user requirements as explained above. These end users come from Sweden, UK and Spain and represent different types of critical infrastructures: nuclear power plants, solar power plants, ports, air traffic control centres. P5 also has input from other actors representing wider interests in the security business. Second, we have appointed a group of three stakeholders, with which a non-disclosure agreement are signed that allows us to share otherwise restricted project content. The group has representatives from Sweden, UK and Spain and also represent organisations operating critical infrastructure as well as organisations delivering security and security services to critical infrastructure. We arranged a meeting with the stakeholder group at UoR in January 2016. The stakeholder group was invited to the demonstration at CAST in the UK April 20th of 2016 and are also invited to the demonstration at FOI, Sweden October 5th of 2016.

Database

Recorded sensor data is needed for research, development and evaluation of algorithms. It is used to demonstrate the capabilities of the developed surveillance system. Two major data collections campaigns were planned and performed. Sensor were mounted as in a surveillance system and scenes from the scenarios were staged. Sensors were calibrated and synchronised to be able to relate the findings in the sensor data with a common real world coordinate system. Calibrated and synchronised sensors is a fundamental condition for fusion of sensor data and improves the possibility to interpret observations from sensor data in terms of persons, objects and their activities. Some minor data collections were performed by partners to get data for specific tasks och from specific sensors. The full database is available for the partners. A subset of the data was selected and published as part of the IEEE Advanced Video and Signal-based Surveillance (AVSS) 2015 in Karlsruhe, Germany. The published data set can be downloaded by researchers for scientific purposes.

User requirements and the principle of privacy-by-design

The end users stress that it is necessary to respect law and regulations regarding privacy. In this context it is foremost the video cameras that intrude on privacy when they are used so that individuals may be recognised or identified. The work in this project have advanced the possibilities to protect the privacy. The trade-off between intrusion into the privacy of persons and the interest and obligation of the operators to protect their critical infrastructures has been improved. There is a fundamental problem in that while it is not necessary or even interesting to identify innocent public when there is not a threat it is vital to be able to identify perpetrators and witnesses in case of a suspected crime. It may be necessary to see faces to determine if there is a threat or not when there is an alert. With a permit it is legal to record video and retain it for a limited time. A filter determining who can take part of the data in which it is possible to recognise persons may be a tool that can improve protection of privacy.

User requirements included questions about the need for privacy and the need for information from the sensor system to be able to determine an acceptable trade-off between the right to privacy and the justifiable interest of the operators of critical infra structure to detect threats to the facilities. The work with privacy design was continued in the work package devoted to privacy. Questions about privacy was also raised during other meetings with stake holders.

System Architecture

A global, step by step, methodology was proposed to derive a system architecture that is compliant with the user requirements and to define the architecture of the P5 demonstrator. The related works are described in the P5 deliverable 4.1 Final P5 System Architecture Report. The analysis is conducted in two steps. First we design of a future privacy preserving perimeter protection concept of system with the following main characteristics:

- Consisting of a modular, scalable set of networked sensors that provides a multispectral observation capacity: The main sensors are visual and infrared cameras and radars able to detect and track pedestrians and vehicles. Acoustic sensors are considered for the omnidirectional detection of air targets such as drones.
- Including advanced algorithms (main focus of P5 project): for object detection, classification and tracking, fusion of information, high level modelling of intent and behaviour analysis allowing early warning, protection of personal data.
- Including a set of services supporting the implementation: integrating privacy preserving services, network management, data management and man machine interaction that could be used as a complement to existing perimeter systems: to monitor an area beyond the barrier in order to detect threat early as they are approaching or preparing their attack.

Secondly, the design of the demonstrator of the P5 Project is provided, focusing on the implementation of the new modules developed in the P5 project and to assess their contribution to the design of the future pro-

ject. The design methodology adopted is inspired by the standardised value management and functional analysis methods:

- The studied system is replaced in its use environment in order to identify the required operational functions and the constraints.
- Then a rigorous method for understanding complex systems by converting the operational activities performed in then system to the technical functions performed by the system for the users.

The analysis provides the technical specification including hypotheses on the interaction between system and operator. The architecture of the future system is then refined.

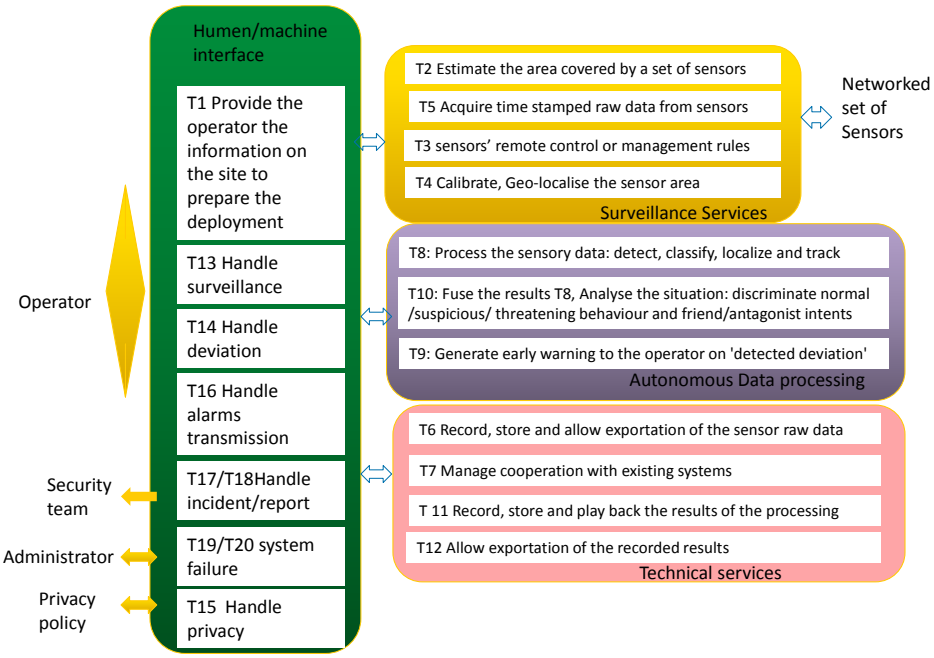
Specification: Operational and technical requirements and constraints

Operational functions were outlined and then a set of technical functions required to fulfil them were identified. Those are presented in the figure below, considering the system interaction with the involved human operators. A set of requirements and constraints were then provided at the operational level and then refined at the technical level. Among these, were identified those taken into account in the P5 demonstrator.

Architecture of a future system

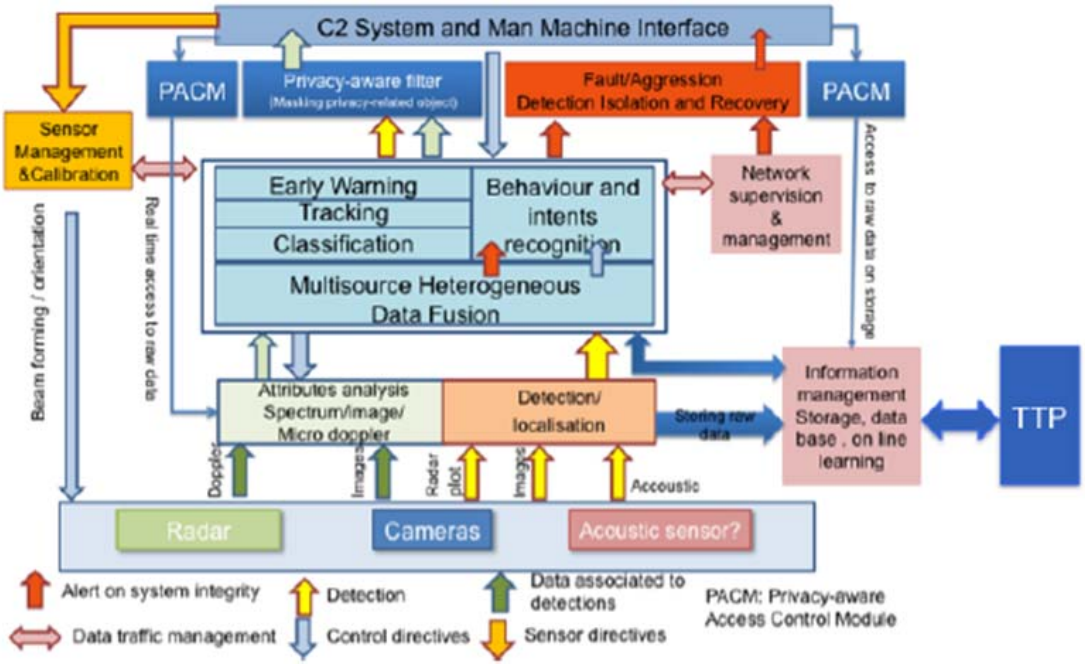
The architecture of the future system is described in three complementary views:

- The technical view characterises the physical components: sensors, computer, networking components, storage units and command and control stations.



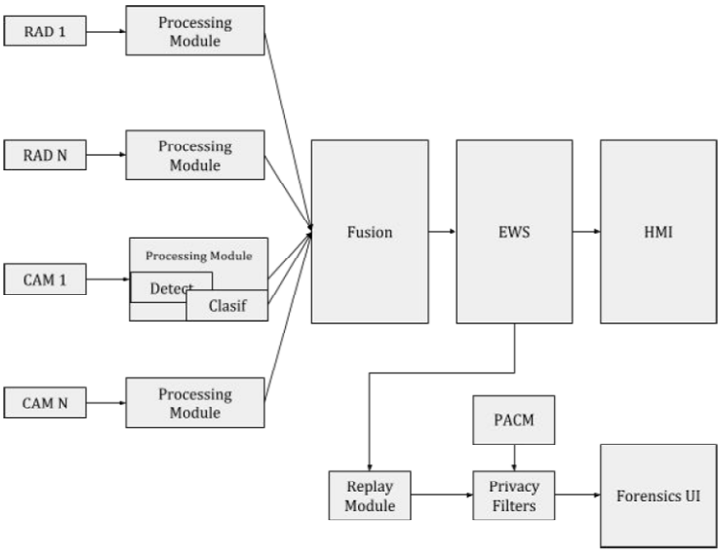
- The system view focuses on the networking of the system: the distribution of the processing modules over the network nodes and computers. To ensure scalability, a hierarchical organisation was proposed that is able to manage several data fusion nodes, each one handling a set of sensors.
- The functional view presents the steps of the processing chain in a layered structure and identifies the data exchanged between levels: from the lowest sensors layer to the upper man machine interface layer; through the detection, classification, tracking and fusion, behaviour analysis and early warning modules; under control of privacy preserving modules.

The architecture is depicted in the figure below.



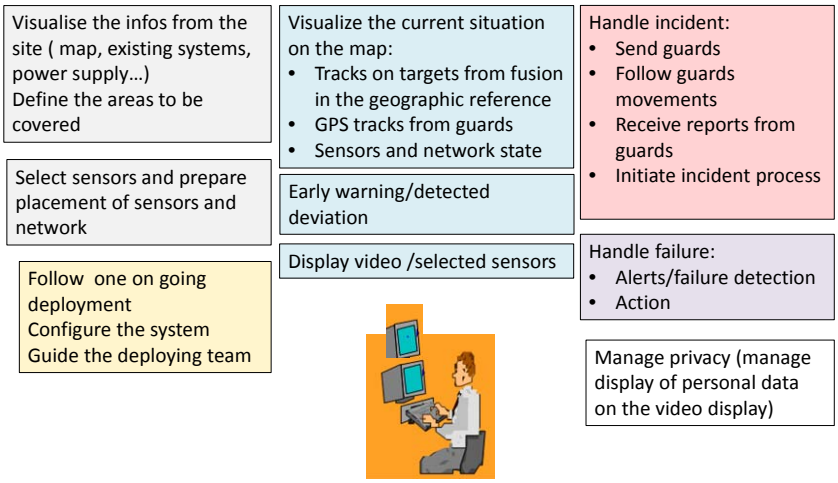
Architecture of the P5 project demonstrator

The P5 demonstrator is a prototype of a data fusion node, implementing the innovative principles developed in the P5 project: sensors, autonomous processing, and privacy preserving functionalities, see figure below.



Human Machine Interface

The expected functionalities of the human machine interface (HMI) were identified in the functional analysis and are summarised in the figure below. The system should provide services to support the deployment of the system. The system should provide the operators early warnings and all information to understand the situation and control the proper operation of the system. The responsibility for the final decision on threat analysis and the final alert belongs to the operator. Two prototypes were specified and developed: one dedicated to the interface with the fusion processing, the other demonstrating the privacy preserving functionalities.



P5 architecture and the principle of privacy-by-design

The privacy by design concept was a guiding principle in the design of architecture; in the definition of deployment recommendations, preserving private places, and for identifying the necessary measures to ensure protection of personal data, when acquired and the best way to implement them in the architecture. Privacy concern happens when the operator wants to view the raw data/unmasked data directly from sensors in real time or accesses the past raw data from storage for a particular reason. The data, we refer in this context, are mostly related to data generated by thermal or visual cameras/sensors while data from radar are considered as non-privacy-related data. Thus, any access to raw data needs a special treatment to ensure that data are not used excessively. With this reason we propose to insert in the architecture, three modules: Privacy-filter, Privacy-aware access control module (PACM) and Trusted Third Party (TTP). Privacy filter is responsible for filtering the privacy-related information (e.g. if an object is a physical person, it hides the face of that person). PACM is responsible for controlling the access to raw data generated from sensor. It decides who can or cannot access raw data based on the access control policies defined by TTP administrator. TTP is responsible for controlling the processing of personal information in P5. These include, defining access control policies, defining user account and tracking user activities in the system.

Thermal and Visual Solutions

In P5 a significant amount of research and development has been conducted into real time analysis of video data from both visual and thermal sensors. The work has been focussed on detection and tracking of targets from air, sea, and land environments, ranging from single sensors for single target detection to multi-target tracking using multiple sensors. The key contributions and innovations for the work done under 'Object detection and background estimation' and 'Object Tracking' are briefly described below.

- As a part of the overall P5 system, the detection module [6] has been implemented to provide single-camera detections from multiple visual cameras to feed the fusion module (see the Section on Early Warning Solutions) at later stage. The detections are passed into a custom single-camera tracker [8] based on Stochastic Diffusion Search (SDS) and other techniques, which effectively removes a lot of the problematic detections by combining detectors, and using higher reasoning from other predictive measures. Moreover, a framework for the performance evaluation and testing robustness of tracking algorithms [8, 9] has also been developed. Furthermore, in preparation for the demonstrations at one of the Home Office's CAST sites, the detection module (including multiple detectors and a single-camera tracker) have been adapted to also run live from IP cameras with visible imagery. A related contributions in regards to vehicle classification appeared in [7].
- A new tracking algorithm has been developed especially for thermal imagery and clearly outperforms previously published methods. Two methods have been invented for reducing background contami-

nation the effects of detection noise that are called *background-weighted distribution field tracking* and *adaptive object region distribution field tracking*, which are independent of each other and can this easily be combined. The resulting tracker, called ABCD (Adaptive object region + Background-weighted Channel coded Distribution field tracking). Moreover, foreground-background segmentation algorithms have been evaluated and a multi-target tracker been implemented. These and other related contributions and innovations are published in [11-16].

- The work on detection and tracking of UAVs from visible and infrared images has also been undertaken. First, background-subtraction-based detection is performed. Next, the track-before-detect paradigm, which combines target detection and estimation by removing the detection algorithm and supplying the sensor data directly to the tracker, is applied. For tracking of high manoeuvring targets, an Interacting Multi Model (IMM) framework is applied, which is well suited for low-cost embedded real-time application, using also some scene contextual knowledge as well as potential trajectories of the airborne objects.
- The algorithms on ground object detection and tracking with both thermal and visual images have been embedded on an AXIS camera that supports the execution third party applications. The CPU of the AXIS camera presents some restrictions, and efforts have been made on code optimization for object detection and tracking applications to be able to run in real time. Different image features have been investigated (KLT and Harris corner features; FAST) and evaluated for the task. FAST has proved to behave well, except when the object has very low contrast with the background where KLT works better.

Likewise, the key contributions and innovations for the work done under 'Privacy enhancing technology' are briefly described below.

- The growing use of surveillance applications around the world has led to an increasing need of protecting privacy of individuals. Here, the privacy protection refers to replacing the original content in an image region (that may reveal object identity) with a new (less intrusive) content generated as a result of transforming the original content (by means of image processing and filtering operations) or applying a perturbation on it or using a different imaging modality. Indeed the development of privacy protection techniques needs also to be complemented with an established objective evaluation method in order to facilitate their assessment and comparison. Generally, the existing evaluation methods rely on the use of subjective judgements or assume the presence of a specific target type in the image data and use target detection and recognition accuracies to measure privacy protection. To this end an annotation-free evaluation method [5, 10] was proposed that is neither subjective nor assumes a specific target type. It is aimed at assessing the two key aspects of privacy protection: protection and utility. Protection is quantified as an appearance similarity and utility is measured as a structural similarity between original and privacy-protected image regions. An extensive experimentation was performed using several challenging datasets (including P5 and existing ones) that contains visible and thermal imagery.
- The ethical and legal aspects associated with the technology developed under 'Thermal and visual solutions' was also studied [1, 2].

Thermal and visual solutions and the principle of privacy-by-Design

The first half of the project involved defining user requirements for P5 future system where legal aspects were taken into account in the requirements mining process. We used the EU directive 95/46/EC for analysing the legal requirements for personal data usage and processing. The ethical studies were also conducted in order to have the view from people who may be affected by the system when it is deployed. Based on the defined user requirements, those requirements were translated into system requirements and then a complete P5 system architecture was proposed. Privacy-by-design approach was developed for P5 system where the privacy protection issues are taken into account for every step of data processing and the privacy protection modules were introduced in the system architecture level. To ensure a proper privacy protection, in P5

architecture, three modules we introduced: Privacy-filter, Privacy-aware access control module (PACM) [2] and Trusted Third Party (TTP). Privacy filter is responsible for filtering the privacy-related information (e.g. if an object is a physical person, it hides the face of that person). PACM is responsible for controlling the access to raw data generated from sensor. It decides who can or cannot access raw data based on the access control policies defined by TTP administrator. TTP is responsible for controlling the processing of personal information in P5. These include, defining access control policies, defining user account and tracking user activities in the system.

While the first period of the project focused mostly on the requirements analysis and design, the second period of the project started from the month 19 to the end of the project has been focusing on the implementation of the privacy protection modules and integration of such modules into P5 system. Below is given a description of different modules.

1. Authentication and authorisation module: this module is responsible for controlling who can use the P5 application through which user can access data generated from sensors installed in the protected facility. User is authenticated with an account representing by his username and password. The authentication server is developed as Java package connecting to P5 player, which is used to view data from visual or thermal camera. The secure username and password storage and processing is also developed and integrated into the authentication server. Hashing function (MD5) is used to transform the plaintext password into human unreadable text before storing it into Mysql database. Authentication and authorisation server were also integrated with P5 player module. Such integration was presented in the first final demonstration that took place on Wednesday 20th April 2016 in CAST (UK).
2. Privacy-aware access control module: once user is authenticated, he can access data from different sensors installed in the facility when needed, by default he can access only filtered data. Access to raw data from visual or thermal sensors are subjected to another level of control by a module called “privacy-aware access control module”. This module controls access to such data, like who can access under which conditions, based on the predefined access control policy, which is generally defined by authorised trusted third party (TTP administrator). Since raw data from visual or thermal sensor bears privacy-related information, it is necessary to control who have accessed to such data in which circumstances. This kind of control allows us to limit unnecessary access to raw data. Other role of privacy-aware access control module is to record all the access activities of users in the system for auditing purpose. Authorised trusted third party performs the auditing of users’ past activities. Privacy-aware access control module was implemented in Java with the support of standard XACML engine. The privacy-aware access control module was successfully integrated with P5 Player module developed in Python with the help of ZMQ. The integrated modules were presented in the first final demonstration that took place on Wednesday 20th April 2016 in CAST (UK).
3. Trusted Third Party: to ensure the accountability of personal data usage in P5, the use of an entity called “Trusted Third Party” was proposed. This entity can be inside or outside protected facility. A “trusted third party” system was developed, which is responsible for creating users, defining the access control policy for every user in the system and auditing users’ activities. Trusted Third Party is developed in Java where Mysql database was used for storing users’ activities. This module has been tested and validated. It has also been integrated with P5 system and presented in the first final demonstration that took place on Wednesday 20th April 2016 in CAST (UK).
4. Privacy filtering module: Privacy filtering refers to replacing the original content of an image (or a region thereof) with a new content that is less intrusive on the privacy of individuals. The new content may be a result of (i) transforming the original content, or (ii) perturbing the original content, or (iii) using a different image capturing modality. The first case may involve hiding image regions (that would otherwise reveal object identity) by applying different image processing and filtering operations to provide a different level of identity protection. In the second case, perturbations may be added to the original content in the form of displacing the state of the image patch thus obscuring

object's identification by motion. The third case involves employing a different imaging device that is assumed to be privacy protecting. For example, it could be thermal infrared (TIR) camera that has been considered privacy preserving for years due to low resolution, high noise levels, and difficulty for a human to interpret thermal imagery and identify objects. Overall, several privacy filtering techniques have been implemented (including blurring, pixelating, cartooning, blanking, motion perturbation and TIR) followed by their comprehensive assessment and comparison using a new objective evaluation method [4, 10] proposed under the 'P5 Thermal and Visual Solutions' work.

Radar Solutions

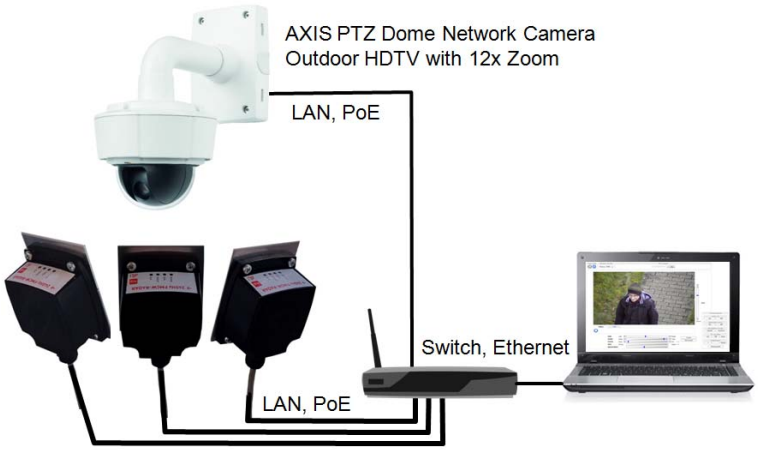
At the beginning of the P5 Project a small radar module was available operating in the 24 GHz ISM-band and applying an SPI interface for digital communication. A first firmware allowed some FFT processing and simple signal processing to measure targets in distances and angles. Based on this module an extensive development in hardware, firmware and PC-software was carried out in the P5 Project to achieve these results in summary:

1. 24 GHz FMCW radar module in IP65 housing with CAN-bus and Ethernet (Power-over-Ethernet) interfaces (module name: sR-1200c for CAN-bus and sR-1200e for PoE).
2. Firmware for sR-1200c and sR-1200e with intruder detection and tracking algorithms.
3. PC software tool with Graphical User Interface (GUI) for radar parameter settings and radar signal visualisation.
4. Modified (in hardware and firmware) 24 GHz radar module to enable μ-Doppler measurements for target classification.
5. Radar Network Controller (RNC) with LINUX computer and interface board to connect up to 4 radar modules with CAN-bus interface to Local Area Network (LAN).
6. PC software to evaluate the extended observation area by 4 radar modules (-90° to +90°, 0 to 30m) including enhanced intruder tracking, target visualisation in a diagram and camera control to direct a Pan-Tilt-Zoom camera to the main target.

All these developments were accompanied and verified with a number of test campaigns carried out at locations of individual partners or in cooperation at one partner's site. One fixed test installation was made at IMST's company building with surveillance of the backyard and car park. The Radar Network Controller, 4 radar modules and a PTZ camera were mounted at the building and long term intruder measurements were carried out and evaluated. Partner FOI recorded and evaluated the μ-Doppler radar signals of a large number of different target classes like human, animal, and man-made object, with the man-made object class containing cars and a drone. The huge amount of data was evaluated with a Support Vector Machine (SVM), which achieved 77% of correct classification. All measurement campaigns could either improve the radar hardware and software development or verify the achievements.

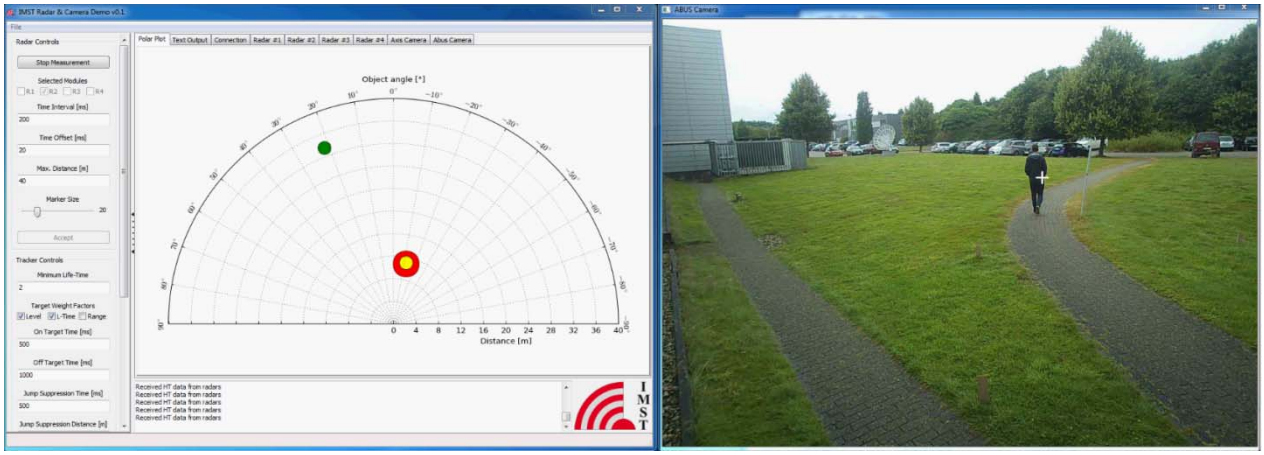
Achievements and results

The final radar developments and setup in the P5 project could be summarised in the following graphical overview. The picture shows three radar modules of type sR-1200e with PoE interface. These modules are connected directly with a LAN or via a switch, which delivers the 48 V power supply, to any Ethernet. The radar network controller is implemented on a PC with GUI software. This program allows the use of up to 4 radar modules, one AXIS PTZ camera and a standard surveillance video camera from ABUS (IR HD 720p network outdoor camera). For each connected device (radar modules and cameras) the installation coordinates (height and orientation) can be inserted as parameters for a transformation into world coordinates. This ensures that the intruder coordinates can be matched with the camera view and zoom. Furthermore the network controller software combines the different observation sectors of each radar module to one common surveillance area.



A typical screen shot of the radar network controller is demonstrated in the following picture. The left window shows a polar plot with coloured targets in distance and angle. The red circle indicates the main target, which will be determined from parameters like reflection magnitude and live time. The white cross in the video marks this target. Furthermore radar and tracker control parameters can be modified in the left menu of the GUI. Setting for interface “Connection”, “Radar 1” to “Radar 4”, “Axis Camera”, and “Abus Camera” can be made by opening register cards above the object plot. A couple of test campaigns were successfully made with this setup by installing 1 to 3 radar module and both camera types in different configuration and mounting position. The proper functionality could be proven. Extended tests should show the false alarm rate in future test campaigns.

Due to advanced developments of sensor technology and autonomous systems in recent years, security applications used in critical infrastructures received much attention in the world. Usually video and thermal cameras are used for the surveillance of critical areas.

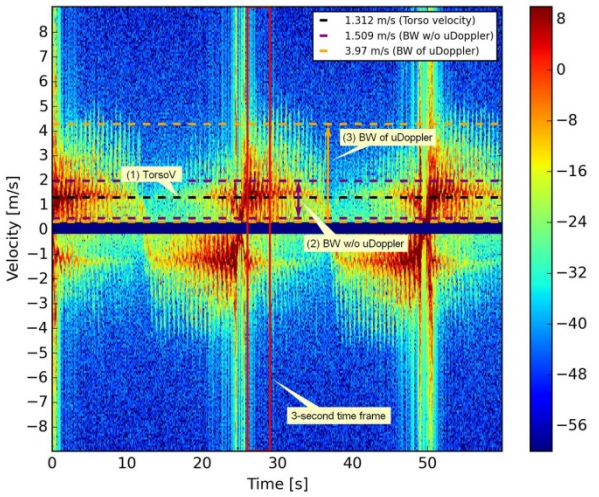


However, video detection would degrade or even fail in case of fog, darkness, backlight or heavy rain. Furthermore, in cases where the observation is extended to public areas, video and photograph recording would be in conflict with the right to privacy and data protection. Radar is therefore a gainful complement to video observation and could also be used as the primary and sole detection sensor, see [19, 21].

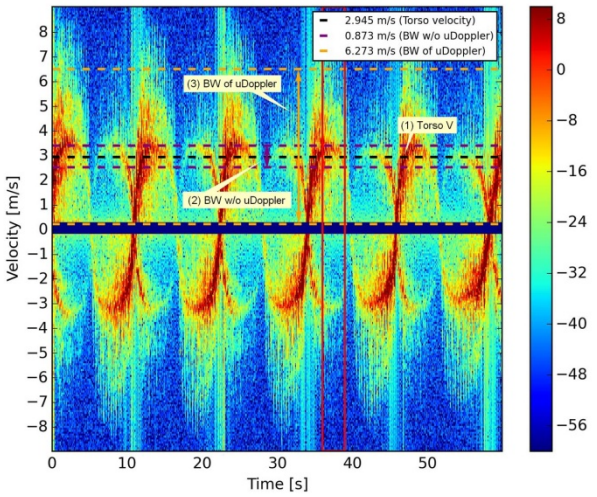
The radar capabilities could be enhanced further, if classification of targets would be possible. Comprehensive researches in the P5 project indicate that radar can be used for classification of moving targets through observing the μ-Doppler signatures of the reflected signal. Therefore, using radar as a security application can provide ground surveillance under a wide range of weather and lighting conditions, high privacy standards and low false alarm rate.

The 24 GHz FMCW radar sR-1200 was modified to enable μ-Doppler measurements in CW mode. A positive velocity represents targets, which move away from the radar, while targets with negative travelling speed are

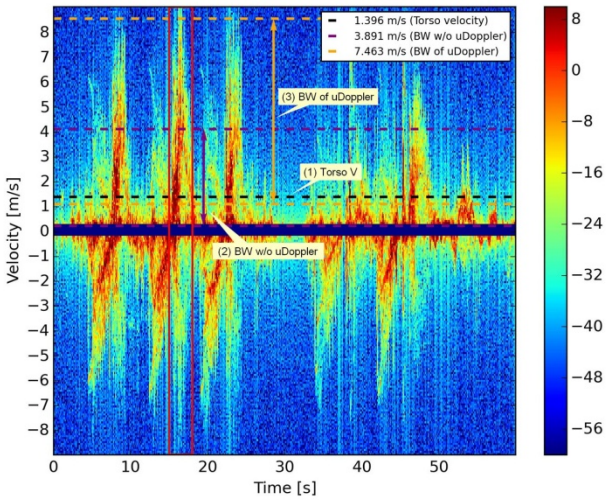
approaching the radar. Furthermore, the micro-Doppler signature includes characteristic movements from the target like the oscillating arms, legs and torso of a walking person. In case of vehicles it would be the rotating wheels of a car or the revolving blades of a multicopter. The different signatures become obvious from time-velocity diagrams, see the figures below. P5 partners carried out a number of µ-Doppler measurements with the modified radar. The objective of these campaigns was to analyse the micro-Doppler signatures in order to classify different moving targets: human, vehicle, UAV and animal. By analysing the µ-Doppler signatures (e.g. with a Support Vector Machine), the potential of using radar as a remote sensor for security and perimeter protection applications could be demonstrated, see [17, 18, 20]. It is also shown that I/Q sampling during the signal processing preserves the direction of the targets' motions, which provides additional information on top of the micro-Doppler signatures. This information can then be used as a parameter during the danger assessment of ground surveillance. Examples for µ-Doppler TV diagrams are plotted in the following four graphs with the extraction of three features: (1) mean torso velocity, (2) bandwidth without micro-Doppler and (3) bandwidth of micro-Doppler.



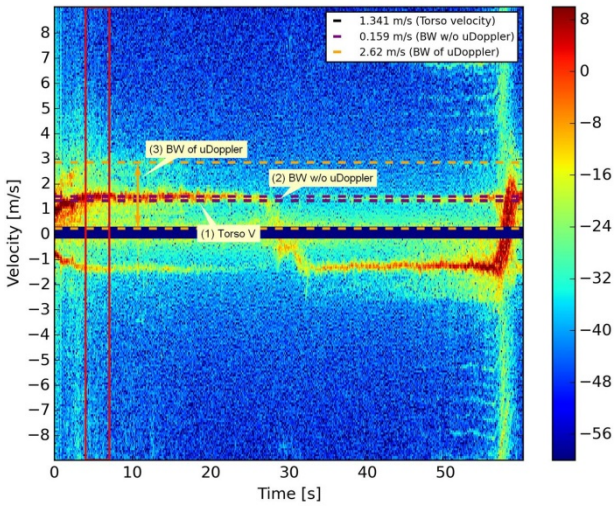
Walking person.



Running person.



Walking dog.



4-wheels grass mowing vehicle.

Radar Solutions and the principle of Privacy-by-Design

Compared to visual camera sensors, radar does not record personal or private attributes. A radar measures the distance and directions to the target, and only if the reflection amplitude is above a predefined level, regardless if it is a person, an animal or a vehicle. Even in case of μ-Doppler measurements, only a classification (as a human, animal, vehicle or other) of different targets can be made. An identification of an individual is not possible with the radar technology at hand. This property of privacy preservation makes radar specifically interesting for perimeter protection, where privacy should be preserved. With radar in combination with visual cameras it becomes possible to activate the visual camera only when radar detects a significant intrusion into a defined area and when a threat becomes probable, which also can be used as a privacy preserving feature.

Early Warning Solutions

Two aspects of a proactive, early warning capability are considered here; on one hand the ability to discover or detect persons that approach the protected facility at a great distance, and on the other hand the ability to among a relatively large number of people discover one or a few with a deviating behaviour, of which a subset of behavioural patterns are atypical indicators recognised before-hand to precede actions of violence or crime. Possibly attributable to two rather diverse surveillance contexts, both cases are relevant to consider from a capability perspective, and both should engage the operator into inspection and final assessment of the severity; if actions are required to meet a security threat or not. Indeed, proactivity in the present context should be understood as the ability to predict an intrusion attempt, an event of violence, or possibly some other form of security breach, before it actually takes place, and thereby giving security staff an early warning and valuable time to implement safety procedures aimed at minimising damage, loss or injury.

Detection at great distance pose minimal technical problem in a dessert-like environment, where a central sharp-eyed sensor can scan beyond the perimeter with little or no occlusion. However, we must also be prepared to protect facilities located in more complex environments where settlements or terrain features vastly restrict sensor sightlines, thus calling for an often large number of sensors to cover every corner around the site. Possibly, this is a more typical case for the critical buildings in Europe. The ability to recognise behavioural patterns also relies on a multitude of sensors to overcome crowd occlusion, and to cover a range target angles. Apart from the coverage aspect, requirements on robustness against weather variations P5 meets by the use of complementary sensors modalities (radar, thermal, visual), which increases the system sensors count even more. In the end, the number of sensors needed to achieve a reliable early warning capability – say 100-1000 sensors – could easily overwhelm the operator, pushing the cognitive load way beyond what a person reliably can handle, at least in the long run. In essence, this motivates the envisioned multi-sensor system with a high level of autonomy regarding the detection and tracking of persons, and to that end the automatic classification of certain behaviours as precursors of violence and crime.

Calibration

Before sensors can collaboratively contribute to a common state-of-matter, they need to be calibrated to stand on a common geometrical footing. This initial step identifies how the sensor response relates to stimuli at different positions in the surveillance area, where position coordinates are given in a common coordinate system. In the case with a camera, a map between each image pixel (picture element) in the camera view needs to be mapped to the origin and orientation of the field in space that stimulate the corresponding pixel. In P5 a framework for manual camera calibration has been described that makes subpixel mapping accuracy achievable in realistic environments. It is based on known camera calibration methods and software libraries, but the methodology has been perfected in P5 to the benefit of data quality in the data sets produced, used and delivered in P5.

The manual calibration gives good accuracy and good control of the calibration errors, but consists of multiple steps, it is time consuming, and it usually requires expert performance. Therefore more practical methods to automate the calibration has been pursued. These methods may perhaps not always give the accuracy needed in academic situations, but are aimed to give sufficient accuracy for practical use. First, a graphical

software calibration tools has been developed that based on four or more landmarks in two overlapping camera views (or a camera view and a map of the area) finds the homography between the two views (or the view and the area map.) The homography maps coordinates between the views, and can be used to associate objects to improve and enhance target tracking. In P5 we have also applied a rather new method that automatically identify a correspondence map between two images. The method only requires two sensors with overlapping view. The sensor positions need not be known. In P5 we have verified that the method can be used to identify correspondences also between a camera and a radar.

Sensor Fusion

The role of sensor fusion is to automatically combine data from all sensors into a system-common estimate of the state-of-matter. This estimate includes the coordinates and classification of detected objects/threats/targets. In the P5 architecture, the input to sensor fusion comes from detection algorithms at the sensor level described in the section on Visual and Thermal Solutions. A detection in a camera defines a region in the image where a (potential) target has been discovered bundled with metadata such as time stamp and the spatial calibration parameters. A radar detection consist of the direction and distance to the potential target, bundled with metadata. The output from sensor fusion is made available to the user via the human machine interface, but also subject to further analysis by a function that detects behaviour indicative of violence, see below.

An important research challenge that we have addressed in P5 is the target (detection) association between distributed sensor views. In P5 the association function is handled by a state-of-the-art multi-hypothesis tracker based on the FOI tracking framework for target tracking research. The tracker software has been adapted to the P5 architecture so that it interfaces with the adjacent processing modules. The tracker has been demonstrated on P5 scenario data, but also thoroughly evaluated on other relevant and well annotated data sets with various sensor constellations. Tracker performance measures include track start delay, ability to maintain continuous tracks for prolonged periods and also comparisons with ground truth. It has been shown that visual and thermal cameras can be consistently fused, facilitating reliable and accurate surveillance both night and day. The achieved tracking performance, in the evaluated scenarios, have proved promising results of high quality, which we published in [23]. Promising attempts to fuse the 24 GHz IMST radar data with visual data on relevant surveillance data are also part of the positive results of P5.

Another important research challenge that has been addressed in P5 is to assess the quality or reliability of detections made at the local sensor level. This assessment is particularly important when fusing sensors of different types, so that at all times the momentarily best sensors can be prioritised. Although more work remain to fully test and utilise this assessment performance, we have described assessment methods for both image sensors and radar, that are implemented in P5 integration platform and quality measures are propagated to the fusion node.

Classification

In the P5 architecture, part of the classification function is located at the local sensor level where each detection is classified, part at the fusion node, where associated detection are aggregated into a final classification. The classifier determines whether a target is an animal, a human, a vehicle or something else (four classes.) For the radar, the classification is based on micro Doppler features as described earlier. For cameras, the classification is based on the image content in the image region defined by the detection. In P5 a specialized algorithm for image-based object classification has been described and evaluated. The algorithm is based on multi-class boosting, a machine learning technique. Algorithm parameters are learnt from a set of training examples obtained in a data collection effort involving multiple humans, animals and vehicles recorded by a set of thermal infrared and visual video cameras. While performance on validation data from the same data recording is excellent, performance on test data from recordings at a different site is less than perfect, but understandably so given the differences in viewpoint and object appearance. It is likely that a more diverse training data set would result in significantly better performance.

A method for combining classification results from multiple sensors at the fusion node has also been presented. The algorithm produces a weighted average of class membership probability estimates from a set of sensor-specific classifiers, where the weights are functions of sensor data features. In simulations a possible application is demonstrated where the weights are functions of the current sensor noise levels. The results are encouraging, with a significantly improved performance compared to sensor-specific classifications and a simple averaging of class probability estimates, but more work is required to fully understand all aspects of the proposed method.

Detection of indicative behaviour

Considerable effort has been paid to the development of a high-level methodology to decide when to issue a threat-related early warning based on indicative behaviour. Indicative behaviour is a behavioural pattern that a priori is known to be associated or correlated with situations that escalates to violence or crime, and that motivate an alert to the operator. We have addressed the detection of single-actor and group behaviours that can account for a threat. We have established an approach based on the analysis of trajectories from detected mobile objects such that input trajectories are the fusion result from a set of heterogeneous sensors.

Behaviour characterisation is achieved by relating the mobile trajectory to automatically learned activity zones of the observed scene. Automatically learning the context of the scene (activity zones) allows first extracting knowledge on the occupancy of the different areas of the scene. Further, the activity of a person can be characterised as the series of zones that the person has visited. Broadly speaking the proposed methodology contains the following steps:

1. Multi-resolution analysis of the mobile speed profile to extract speed-changing points.
2. Speed changing points are the input to a fast clustering algorithm. The clustering results in an initial set of zones {Zn}.
3. The partition of clusters is corrected by merging similar zones, Zn, employing soft-computing relationships
4. Mobile behaviour is summarised as the series of zones that the person has visited.

For single-actor behaviours, we have developed trajectory-based algorithms for detection of the following behaviours: Speed change (Sudden acceleration) and Direction change (Sudden change of trajectory). For group behaviours, we have targeted Meet (two individuals come close to each other and interact); Split/Leave (an individual departs from a group); Detach (Sudden departure from a group); Catch up (Pursuit to meet/attack an individual); Loitering (Long stay of a person in the same area). We have tested the approach on public datasets such as CAVIAR obtaining 60% Precision and 100% Recall measures on threat detection. The system has been fully integrated into the P5 platform and performed live at CAST demo on 20th April 2016.

Early warning solutions and the principle of privacy-by-design

From a research-ethical viewpoint, developing a machine that automatically can follow people, how they move over extended areas, and to that end also determine their behaviour raise concerns. In P5 it has also been concluded that the use of such a machine today would raise legal issues in many European countries. In P5 we propose how to use the new sensor technology in order to preserve privacy. First, the highly automated early warning system may be used to isolate the users from sensor data that can compromise privacy, for instance the ability to recognise individuals in the surveillance views. In other words, the automation allows the user to interact with the surveillance system on an abstract cognitive level using anonymous symbolic markers for individuals and their behaviour. Secondly, the system has strict control of data streams and storage, and unlocking sensitive data can only be done in extreme cases or by the admittance of a prosecutor or other entrusted authority, as explained to the detail in the Privacy sections at the beginning of the project summary. This is what we propose in P5, although today we are not entirely sure if and in which surveillance contexts such a system may gain legal and ethical acceptance.

Integration and Validation

Integration of components is a key part in a software project. It involves understanding the communication and the coordination between different elements and should be done effectively to be able to demonstrate the whole system capabilities. There are different strategies to perform the integration, in P5 we decided to pursue an incremental integration approach. In a non-incremental integration approach, the different parts of the system are tested separately and at the end of the project they are joined. The non-incremental integration methodology is commonly used in both commercial and research projects, but it has some drawbacks. Due to the fact that the integration is left for the last moment, when the deadline to deliver the software is approaching, this approach leads commonly to unexpected problems when there is a lack of time to recover. The strategy used in the P5 integration of prototypes is an incremental integration. This means, basically, that at first stages the data scheme is created and the modules are integrated and validated, once those modules are verified a new module is also aggregated, until all of the modules of the system are finally working together. This second strategy becomes very useful having in mind that the periodic and early integration of work was beneficial in the sense that we learnt from the coordination of the modules and we were able to rectify on time.

Regarding validation, we wanted not only validate but to evaluate the approach. In the sense of determining if our approach was useful from a technical perspective. In order to achieve this an evaluation process and a validation template were developed. The P5 technical validation and evaluation process includes the definition of individual and common success criteria, and assessment criteria of the project and the validation of the fundamental requirements. It also provides details on the project innovations and two tables: One for a SWOT analysis of the overall approach and the other one to link the P5 achievements with the initial objectives of the project.

P5 had five main challenges

1. To detect and classify objects in varying environments
2. To reduce the number and impact of false alarms towards optimised decision making
3. To investigate and handle privacy issues regarding the technology and its implications
4. To provide a demonstration of automated threat detection
5. To evaluate the modules and the approach

The integration and validation is somehow related to all of them. In order to take up the challenge of providing a demonstration (challenge 4), it was necessary to develop the different detection and classification components (challenge 1) and fuse the data and provide and early warning system in order to reduce the false alarms (challenge 2). Privacy (challenge 3) was taken into account in different modules which were also integrate with the sensors and user interfaces. Finally in order to evaluate the P5 approach an evaluation process and a validation were produced. More details on the approach followed for taking up the challenges are provided in the “Integration Approach” and “Validation Approach” sections.

Integration approach

As it was mentioned previously, it was a must to include modules and sensors components integrated into a common platform. We wanted a solution which was compatible with an incremental integration approach but was modular enough, so that each component can be compiled separately and also be evaluated on a stand-alone basis.

During the architecture design we agreed on having a scalable solution with a loosely coupled components. For this reason we choose a published/subscriber approach and we thought on ZeroMQ as messaging middleware. It allowed data publishing and subscribing and was compatible with the programming languages used by the different partners. (C++, python, Java, MATLAB). For data structure, we followed a similar approach. We wanted something that was compatible with C++, Python, Java and which had a structured and extensible IDL. We choose ProtoBuf data interchange format. Apart from these tools, and in order to help in

the integration some tools were developed for P5. We wanted a tool for recording the results of the modules with the ability of replaying the data simulating a module. A kind of sniffer/spoofer software allowing the publishing/subscribing of the data and the individual testing of the modules with real data. This tool together with some tools for synchronization and manipulation of the data were an important part of the integration.

In summary, thanks to the idea of incremental integration, the integration tools and ZeroMQ + ProtoBuf, we were able to integrate partners from different backgrounds, working in different environments and developed modules which could be later exploited independently if required.

Integration and the principle of privacy-by-Design

In the integration of the forensics pipeline, privacy was taken into account. This pipeline dealt with the video replay. The idea behind this pipeline was to have a method for retrieving the video data of a certain moment in time. The operation is similar to a digital video recorder with the difference that it follows the same publisher/subscriber approach of the rest of the system. In this pipeline, the video replay modules access to the video storage database and publish the selected video. This video goes through the privacy filters to the forensics UI. The privacy filters are managed by PACM module which enables or disables them.

Validation approach

As it was mentioned before, we wanted to determine if our approach was useful from a technical perspective. For this reason, we developed an ad-hoc evaluation methodology for P5. This methodology starts with the description of all the prototypes, modules and demos developed in the project. This description involved not only what was the objective of each of the prototypes but also the partners involved. After this initial description, the first step was to know the expected result for each of the prototypes, this was recorded together the success criteria. Information on the assessment criteria and contingency plans was also recorded at this stage. The second step was to evaluate that the fundamental requirements were taken into account each application fulfilled a template for tracking the requirements. Next, we wanted to track not only the requirements but also the technologies. For this the leaders of the prototypes were asked for providing a summary of the main technologies used.

For finalising the evaluation three important sections were developed: First a common success criteria description, including the common success criteria of all the prototypes. Second a SWOT tables, in which each of the partners provided their subjective opinion on the approach. Last, a table linking the achievements of each prototype together with the objectives of the project. This approach helped us to find commonalities in the criteria, technologies and requirements and gave us a vision on the usability of the approach from a technical perspective.

Results and conclusion

As it is mentioned, we think that the integration approach we followed was a good choice for dealing with this type of the project with modules from different entities with different backgrounds. We believe that this strategy based on incremental integrations using a simple framework allowed the partners to focus more in the modules and less in the communication and integration. Regarding the validation, the approach was validated by ten demonstrators, from detectors, to fusion modules, early warning modules and user interfaces. The demonstration was not only made with recording data but also in realistic field trials in different domains.

Dissemination and Exploitation

The P5 dissemination and exploitation tasks encompass a set of drastically dissimilar activities. Highlights are the organisation of several well-attended workshops, the showcases at AVSS, exploitation in existing and coming products, and the final demonstrations.

Scientific dissemination

Five of the P5 partners have been actively pursuing scientific publication of P5 results. That is, not only the universities, but also the research agency and two of the SMEs. So far, 4 journal and 11 conference contributions have been published, and a few more submitted. Also, one licentiate thesis has been presented. The objective of this task was never quantified as a specific number of publications, but nevertheless, the scientific output is without doubt a success.

Industrial exploitation

Commercial exploitation of the foreground created in the project is the task of the four industrial partners. All four have exploited P5 results, in different ways: Visual Tools has improved its video monitoring softwares *SupervisorX* and *PeopleCounter*; Sagem has consolidated a new demonstrator including video sensors, detection and tracking algorithms with multiple cameras; Termisk Systemteknik has included tracking algorithms developed in P5 in three coming products; and IMST will exploit the project results in a new radar module and a radar network controller.

Industrial and academic visibility

The P5 project has been disseminated in presentations and demonstrations. In particular, during the AVSS[1] conference in Karlsruhe in August 2015, P5 exposed a series of posters, rollups and live demonstrations in the Industrial Surveillance Day, and the project as a whole was presented in the main conference track. Moreover, the industrial partners have been active in industrial events and exhibitions, such as SICUR, Axis Solution Conference and InnoSecure.

Workshop organization and links to other projects

The P5 project has been organizing several workshops devoted technology as well as ethical and legal issues. The IEEE International Workshop on Performance Evaluation of Tracking and Surveillance was organized by the University of Reading; the University of Namur was in charge of a panel ("Ethics of the security researcher") at the CDPD[2] conference; and a joint P5-PARIS-IPATCH workshop was organized to engage legislation and policy makers, researchers in the fields of sociology, psychology and law, and experts in surveillance technologies.

Demonstrations

P5 ends with two demonstrations. One in the UK in April 2016 and one in Sweden in October 2016.

References

[1] A. T. Rath, Protecting Personal Data: Access Control for Privacy Preserving Perimeter Protection System, 29th Annual IFIP WG 11.3 Working Conference on Data and Applications Security and Privacy, 29th July 2015, Fairfax, VA.

[2] A. T. Rath, J.-N. Colin, Protecting Personal Data in Privacy Preserving Perimeter Protection System: From Legal to Technical Requirements and Implementation, AVSS'2015 [Poster presentation]

[3] E. Jungert, N. Hallberg and N. Wadströmer, A System Design for Surveillance Systems Protecting Critical Infrastructures, Journal of Visual Languages and Computing 25 (2014) 650–657.

[4] E. Jungert, N. Hallberg and N. Wadströmer, A System Design for Surveillance Systems Protecting Critical Infrastructures, Proceedings of the 20th International Conference on Distributed Multimedia Systems Journal of Visual Languages and Computing 25 (2014) 650–657.

[5] T. Nawaz, J. Ferryman, An annotation-free method for evaluating privacy protection techniques in videos, AVSS'2015.

[1] IEEE International Conference on Advanced Video- and Signal-based Surveillance.
[2] International Conference on Computers, Privacy and Data Protection.

[6] L. Li et. Al., On fusion for robust motion segmentation, AVSS'2015

[7] J. N. Boyle, J. Ferryman, Vehicle subtype, make and model classification from side profile video, AVSS'2015

[8] T. Nawaz et al., Tracking performance evaluation on PETS 2015 Challenge datasets, AVSS'2015

[9] L. Li, T. Nawaz, J. Ferryman, PETS 2015: Datasets and Challenge, AVSS'2015

[10] T. Nawaz et al., Effective evaluation of privacy protection techniques in visible and thermal imagery, IEEE Trans. on Info. Foren. and Sec., Submitted 2016

[11] J. Ahlberg et al., Multi-person fever screening using a thermal and a visual camera, SSBA, Ystad, Sweden, March 2015.

[12] A. Berg et al., A Thermal Object Tracking Benchmark, 12th IEEE AVSS'2015

[13] J. Ahlberg and A. Berg, Evaluating Template Rescaling in Short-Term Single-Object Tracking, AVSS'2015.

[14] A. Berg et al., Detecting rails and obstacles using a train-mounted thermal camera, SCIA 2015

[15] A. Berg et al., An Overview of the Thermal Infrared Visual Object Tracking VOT-TIR2015 Challenge, SSBA 2016.

[16] A. Berg et al., Channel Coded Distribution Field Tracking for Thermal Infrared Imagery, PETS'2016.

[17] S. Björklund, *Target Classification in Perimeter Protection with a Micro-Doppler Radar*, International Radar Symposium (IRS) 2016, Krakow, Poland, May 2016

[18] S. Björklund, *Features for Micro-Doppler Based Activity Classification*, IET Radar, Sonar & Navigation, Vol. 9, No 9, December 2015

[19] R. Kulke, K. Maulwurf-Just, R. Jetten: *Sensorfusion aus FMCW-Radar- und Videoüberwachung zur Erkennung und Verfolgung von Personen*, innosecure, Kongress für Innovation in den Sicherheit-stechnologien, S. 249-252, Velbert Heiligenhaus, Germany, April 22-23, 2015

[20] O. Lam, R. Kulke, M. Hägelen, G. Möllenbeck: *Classification of Moving Targets Using Micro-Doppler Radar*, IRS – 17th International Radar Symposium, Krakow, Poland, May 10-12, 2016

[21] M. Hägelen, R. Kulke, R. Jetten, G. Möllenbeck: *Perimeter Surveillance Using a Combination of Radar and Optical Sensors*, 13th European Radar Conference at European Microwave Week, London, UK, October 3 -7, 2016

[22] G. Hendeby, Target Tracking for Efficient Perimeter Protection, National Symposium on Technology and Methodology for Security and Crisis Management (TAMSEC), 2015, Stockholm, Sweden.

Potential Impact

Impact on security and society

The P5 project has demonstrated how surveillance systems respecting privacy can be built and how various sensors (cameras, thermal, radar) can be used for this task. These results have been disseminated not only to the project's stakeholders, but to a wider audience of legislation and policy makers, to the scientific communities, and to the potential customers of the industrial project partners.

Impact on research and development

Five of the P5 partners have been actively pursuing scientific publication of P5 results. That is, not only the universities, but also the research agency and two of the SMEs. So far, 4 journal and 11 conference contributions have been published, and a few more submitted. Also, one licentiate thesis[3] has been presented. The P5 project has pushed the state-of-the-art in *privacy and data protection*, in *algorithms and methods* for detection and tracking using individual sensors as well as sensor networks, and in *sensor development*. These advances have been communicated to audiences from legislation, academia and industry, as briefly described below.

The P5 project has also made an impact on *benchmarking* and *de facto standards* by organizing or contributing to open dataset and benchmarks for the evaluation of tracking and surveillance methods. In conjunction with the PETS workshop (see below), an open dataset was published including annotated surveillance imagery and benchmarking measures. Moreover, AP5 also contributed to the Visual Object Tracking Challenge (VOT), by providing a thermal object tracking benchmark used as a sub-challenge (VOT-TIR).

Impact on industry and the exploitation of results

The results of P5 have been exploited by the four industrial partners, in different ways. Products have been improved, several new products are being released or planned, two patents are pending, and one new company created.

Visual Tools has adapted a video monitoring software to support new types of cameras and video sources (includes ZeroMQ-based streams, as used in P5). This has been demonstrated at the first of the two P5 demos and will be part of the *SupervisorX* software.

Visual Tools' current video management system is highly valued in the video surveillance sector, but there are a few things that could be improved in order to gain a bigger market share. One is the dependence on Windows machines and the other is that the current software is mainly linked to a specific camera manufacturer. During the development of the forensics UI support for other data sources was developed, this is being included in the current video management software and probably will be part of the product at the end of 2016. This together a possible port to cloud (end of 2017) or at least a redesign in order to support different platforms (such as android devices) and operating systems will allow VT to have a more powerful video management system.

Moreover, Visual Tools have exploited P5 results and been able to improve the performance of their *PeopleCounter*.

Work on P5 allowed **Sagem** to consolidate a new demonstrator including video sensors, detection and tracking algorithms with multiple cameras. This has already been extended to include acoustic sensors, and will, in the near future, also be combined with a radar system. All these technical results will directly be exploited and integrated, after a product development phase in projects with security customers in France and abroad. Today, Sagem participates in the French seminars about security and defence to improve the level of protection of critical assets towards new threats.

At **Termisk Systemteknik**, tracking algorithms from P5 are integrated in three coming products:

[3] The licentiate degree is a Swedish degree half way between M.Sc. and Ph.D.

- The intrusion detection function developed as an add-on to *TST Fire Outdoors*, a newly developed system for monitoring of biofuel storage.
- The fever screening system developed for TST's new daughter company Imafor. The prototype will be demonstrated at the two P5 demos, and the product is planned to be tested at customer sites even before the end of the P5 project.
- The pedestrian/vehicle/animal warning system *Argos*.

These products are based on three detection and tracking algorithms developed in P5:

- Object tracking algorithm for thermal imagery CCFBS (Channel coded foreground/background separation).
- Object tracking algorithm for thermal imagery ABCD (Adaptive background-weighted channel coded distribution field tracking).
- Multi-target multi-sensor algorithm MTMST used for demonstrating radar/thermal tracking in the P5 final demonstrations.

Tracking techniques from TST are also components in two pending patents.

IMST will exploit the following technical advances made during the P5 project:

- Radar hardware improvements especially in frontend and antenna design and digital interfaces.
- Radar hardware modifications to enable micro-Doppler measurements.
- New features for radar GUI including micro-Doppler functions.
- Implementation of radar network controller with four radar modules.
- Improvement of intruder detection and tracking algorithms for radar firmware.
- Fusion of radar with PTZ camera.

These advances will be exploited in the form of three new products: First, a 24 GHz FMCW Radar module for detection and tracking of intruders that will become two products in the form of the Radar Module sR-1200e and the Developer Kit (DK-sR-1200e). Each product includes manual, data sheet, application notes and technical support. They will be marketed through a specific web site (www.radar-sensor.com), exhibitions, and demonstrations.

The third product is a controller hardware and software to combine up to 4 radar modules to enlarge the observation area for intruder detection and tracking with radar. This will become a product of IMST as Radar Network Controller (RNC).

Main dissemination activities

The main dissemination activities of the project are the demonstrations and presentations at AVSS, the three organized workshops, the project's final demonstrations, and the individual activities of the industrial partners.

AVSS Industrial Surveillance Day

At the AVSS[4] conference in Karlsruhe in August 2015, P5 exposed a series of posters, rollups and live demonstrations in the Industrial Surveillance Day, and the project as a whole was presented in the main conference track.

P5 posters, roll-ups and demonstrations at the Industrial Surveillance Day at AVSS 2015.

Jörgen Ahlberg from P5 partner TST presents the P5 project in the main conference track at AVSS 2015.

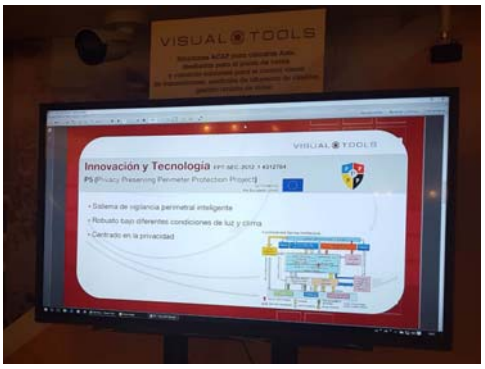
Industrial exhibitions

P5 partners have been active at industrial events and exhibitions, for example:

- Visual Tools participated in the Axis Solution Conference 2015, showing demos of algorithms inside Axis Cameras.

[4] IEEE International Conference on Advanced Video- and Signal-based Surveillance.

- Visual Tools exhibited at SICUR 2016, the biggest security fair in Spain. The pictures below show the VT exhibition stand under preparation, and one screen explaining the P5 project.



- Termisk Systemteknik presented the product TST Fire Outdoors, with P5-based intrusion detection as an add-on, at the SSBA conferences and directly to potential customers.

- Termisk Systemteknik demostrated a coming product developed in cooperation with Visage Technologies and that will be marketed through new daughter company Imafor at the SSBA conferences and at Venture Arena 2015.

- IMST presented their products at, e.g. Innosecure in Velbert, Germany, in April 2015, at the International Radar Symposium (IRS) in Krakow, Poland, in May 2016, and is planning to exhibit at EurRAD in London, UK, in October 2016.

- 

  In addition to these separate market efforts, the combined radar/thermal tracker demonstrated in the P5 demos is planned as a joint marketing effort.

Performance evaluation workshop

The workshop IEEE International Workshop on Performance Evaluation of Tracking and Surveillance (PETS) was organized by P5 in conjunction of the AVSS conference in Karlsruhe, Germany, in August 2015. Peer-reviewed papers were presented and the workshop also featured an invited speaker.

Tahir Nawaz from P5 partner University of Reading giving the introduction at the PETS 2015 workshop.

Workshops on ethical and legal issues

CDDP

The University of Namur was in charge of a panel ("Ethics of the security researcher") at the international conference Computers, Privacy and Data Protection Conference in Brussels dedicated to the P5 project to-

gether with the IPATCH one as the main partners are the same. The CPDP conference is one of the major events in Europe on this area.

Joint P5, PARIS and IPATCH workshop

A dedicated workshop was organised to engage legislation and policy makers, researchers in the fields of sociology, psychology and law, and experts in surveillance technologies, with the aim of discussing and reviewing the ethical and legal issues surrounding the use of different countermeasures and privacy issues. Representatives from the P5 consortium were joined by members of the IPATCH[5] and PARIS[6] project consortia. These projects raise similar legal and ethical concerns and cross-fertilisation of the different experiences was an interesting dimension of the discussion.

Since the 1990s, a new dimension has been included in European Research & Development projects. This refers in this context to the need to address the ethical, legal and social issues raised by technological innovation and scientific research. It is of course the case of surveillance and security technologies projects. Human scientists are involved in these projects in order to examine its "social acceptability". However, this mandate can be understood in different ways.

Very different approaches can be developed to assess the social acceptability of surveillance technologies. The objective of the workshop was to better define the mandate and role of ethics and humanities in surveillance and security technologies projects. The workshop was divided into 3 parts. In a first theoretical step, the aim was to identify different paradigms of the evaluation of social acceptability of surveillance technology and identify strengths and weaknesses of each of these paradigms. In a second step, a round table was organized around the question of the expectations of political and industrial actors about the ethics of surveillance technologies. Finally, the last part was devoted to the consideration of particular ethical issues raised by surveillance technologies. The questions addressed are summarised as follows:

1. **What means assessing the social acceptability of surveillance technologies?** What are the different paradigms of the evaluation of the social acceptability of surveillance technologies? Evolution and criticism of the paradigms
2. **The issue of expectations of political and industrial actors.** What political and industrial actors expect from the intervention of ethics and humanities? Are these expectations the same as those of Human Scientists and legal researchers?
3. **Cases studies.** What are the major ethical issues raised in each of the three projects? How to address these issues?

The workshop was organized jointly with the P5, PARIS and IPATCH projects and held on 13th March 2015 in Namur, Belgium. The sub-title of the workshop was "Deepening the reflection on ethical, legal and social issues in security surveillance technology projects." The motivation to organize a joint workshop was to enable cross-fertilization and mutual learning between ethical research in these projects. The workshop was able to carry a reflective perspective on the ethics work already done in these projects.

Final demonstrations

Two demonstrations are planned. At the time of writing, the first has been successfully executed at the CAST site in the UK in April 2016. The second demonstration is planned to be held in Sweden in October 2016.

The first demonstration event featured presentations as well as live demonstrations. In short:

- The P5 project, scenarios, and privacy preserving work were presented.

[5] Intelligent Piracy Avoidance using Threat detection and Countermeasure Heuristics, www.ipatchproject.eu.
[6] PrivAcy pReserving Infrastructure for Surveillance, www.paris-project.org.

- Live demonstrations were given of multi-sensor tracking, with video cameras, thermal cameras, and radar.
- Demonstrations on behaviour analysis from the scenarios recorded at the second data acquisition campaign at OKG were given.

A similar agenda and setup is planned for the 2nd demonstration in Sweden in October 2016.

Presentations and demonstrations at the first P5 demonstration event in April 2016.


Thermal cameras, visual cameras and radar moutned on mobile poles at the demo site at CAST.

Public Web Site

The P5 public web site has the address

http://www.p5-fp7.eu