FP7-SEC-2011-284725

SURVEILLE

Surveillance: Ethical Issues, Legal Limitations, and Efficiency

Collaborative Project

SURVEILLE Deliverable 2.7: Update of D2.1 on the basis of input of other partners

Due date of deliverable: 31.01.2014

Actual submission date: 31.01.2014

Start date of project: 1.2.2012 Duration: 39 months

SURVEILLE Work Package number and lead: WP02 Prof. Tom Sorell

Author(s):

Dr. Bert-Jan Kooij and Dr. Coen van Gulijk

SURVEILLE: Project co-funded by the European Commission within the Seventh Framework Programme		
Dissemination Level		
PU	Public	X
PP	Restricted to other programme participants (including the Commission Services)	
RE	Restricted to a group specified by the consortium (including the Commission Services)	
CO	Confidential, only for members of the consortium (including the Commission Services)	

§0 Executive summary

This document updates deliverable D2.1 ‘Survey of Surveillance Technologies’. D2.1 provided an initial survey of surveillance technologies for the SURVEILLE project. This document contains generic descriptions of the technologies: how they work, technical possibilities and shortcomings.

The authors imagine that there are two types of readers for this document: those with a technical background and those without a technical background. The authors have written the report for non-technical readers. They tried to explain some basic technical concepts without sinking into a myriad of technical details. Since the authors have a technological background themselves, the non-technical reader may still feel that this report is already crammed with technocratic slang. However, we think that the right balance is struck for use in the SURVEILLE project.

This report does not have a conclusion; it is simply a list of technology descriptions of surveillance technologies. If anything could be concluded from the list of descriptions, it would be that there is nothing simple about surveillance technologies.

Table of contents

§1 Introduction

This document updates deliverable D2.1 ‘Survey of Surveillance Technologies’. D2.1 provided an initial survey of surveillance technologies for the SURVEILLE project. This document contains additions to the technological research of D2.1 that are relevant for the SURVEILLE project as a whole. Following a note on the technical categorization of surveillance technologies in §2, there is a more comprehensive description of all the technologies surveyed thus far as part of WP02 in §3, and a technological assessment of these in §4. The descriptions are more comprehensive in the sense that the technologies are grouped into classes. Also, a textual description is provided in addition to the concise information in the tables of D2.1. These tables are enclosed as annex 1.

Since Snowden’s revelations on NSA spying practices a considerable effort on technology analysis was aimed at NSA technologies. These efforts are not reported in this deliverable but are forthcoming in deliverable D2.8.

§2 Technical description of surveillance technologies

In the security context, ‘surveillance’ amounts to the targeted or systematic monitoring, of persons, places, items, infrastructures (including means of transport) or flows of information, in order to identify criminal conduct and other hazards, manage risk and typically enable a preventive, protective or reactive response, or the collection of data for preparing such a response in the future.

The added value of surveillance *technologies* is that they expand human capabilities. Some technologies observe what is hidden from human senses. Some reach points that are difficult or impossible to reach for humans. Some enable continuous monitoring. Some multiply the work that a single person can do.

Surveillance technologies for serious crime and terrorism serve a specific purpose. They contribute to effective and efficient observation and monitoring of crime and terrorism. Any technology that can contribute to that aim may qualify as a surveillance technology. This makes it hard to construct a simple technical taxonomy for surveillance technologies. Nonetheless, several types of technologies are frequently associated with surveillance. They are (amongst others) closed circuit television (CCTV), unmanned aerial vehicles (UAVs), and data analysis.

§3 Inventory of Surveillance Technologies

This section lists data technology sheets that were developed as part of deliverable D2.1. They were derived primarily from technologies mentioned in the ESRAB report of 2006;[1] the ESRIF report of 2009;[2] an overview of EU-funded security research projects;[3] and research projects within the technical partners of the SURVEILLE project (Fraunhofer Institute, University of Freiburg, and TU Delft). The focus on novel and future technologies is deliberate: the results from the SURVEILLE project will be used in the future. All information has been gathered from publicly available documentation.

The technology data sheets list basic information describing the technologies (name, description and a weblink to additional information); classification of the functionality (description of the function, and function in the Bow-Tie structure); elementary technical features (e.g. dimensions and weight); and operational features (such as personnel and maintenance requirements). The basic description can be limited in these sheets because in-depth scientific discussion of the underlying engineering is of limited importance to the decision maker. Additional information can be found through the weblinks but much detailed information is not readily available through publicly available information.

Currently, the list of technologies is grouped according to categories that identify a group of technologies, e.g. CCTV, RADAR, and X-RAY. The list is given below. A more detailed technical description of these groups is presented in chapter 3.

BIO - airborne IMS BIO-PROTECT

BIO - continuous bio monitoring system TWOBIAS

CCTV - visual semi-automated camera Guppy_F036C

CCTV - visual spectrum dome-fixed

CCTV - visual spectrum dome-zoom tilt and rotate

CCTV - visual spectrum fixed

CCTV & ACTIVITY DETECTION - IPS Activity Detection

[1] Krunes H & Hellenthal M (2006) *Meeting the challenge: The European Security Research Agenda*. European Commission, Luxembourg.

[2] Mate D (2009) *ESRIF final report*, ESRIF project, Brussels.

[3]http://ec.europa.eu/enterprise/newsroom/cf/itemdetail.cfm?item_id=5405&lang=en&tpa_id=168&title=Investing%20into%20security%20research%20for%20the%20benefits%20of%20european%20citizens (accessed August 2012).

CCTV & INFRARED - near-field

CCTV & INFRARED - wide-area

CHEM - explosives detection by antibody SALIENT

CHEM - explosives detection near harbours UNCOS

CHEM - gas chromatography drugs detector DIRAC

CHEM - novel detection techniques COMMONSENSE

CHEM - precursor and drugs detection CUSTOM

CHEM - standoff explosives detection and identification OPTIX

DATA - mobile phone tap PTS

DATA ANALISIS - Omnifind

DATA ANALYSIS - detection of money laundering HEMOLIA

DATA ANALYSIS - networked data analysis SCIIMS

DATA TRANSFER ANALYSIS - name recognition

DNA - rapid DNA analysis MiDAS

GPS - car tracker SN

IMAGE PROCESSING - crowd and riot

IMAGE PROCESSING - people counting and density

INFRARED - motion detector

MM-WAVE - whole body scanner EQO

NETWORK - AIS ship location detection and identification

NETWORK - SIRIUS 3RK3

NETWORK - UGM 2040

NETWORK & INTERFACE - AMFIS data fusion for ground control

RADAR - Marine Radar (ARPA, automatic radar plotting aid)

RADAR - short range radar for intrusion detection

RADIOACTIVE - Compton detector COCAE

SOUND - ECM8000 microphone

SOUND - sound processing FIREFACE400

SOUND - sound recording bug AU046

SPACE - spy satellite

UAV - platform helikite balloon

UAV - platform micro helicopter

X-RAY - luggage screening

§4 Technical Assessment of Surveillance Technologies

§4.1 Assessment of Bio Surveillance Technology

Associated technology sheets:

- BIO - airborne IMS BIO-PROTECT
- BIO - continuous bio monitoring system TWOBIAS

Biological surveillance is of importance to the detection of biological toxins in the event of either accidents or terrorist attacks. Biological agents could be disseminated in the following ways:

- *Aerosol dissemination* is the dispersal of a biological toxin with the use of sprayers or other spreading devices. In the case of a biological terrorist attack the agent is processed to maximize human infection. Attacks could take place outdoors in populated areas or indoors using the ventilation system. Continuous monitoring of the air is needed, in order to take adequate action in the event of accidents or terrorist attacks. The installation of monitoring devices should be carried out on the basis of a thorough risk analysis. For example, one could take the case of the installation of biological detectors in the neighborhood of a plant that produces biological toxins or at a site that is particularly vulnerable to a terrorist attack. Gas-chromatography ion spectroscopy is very effective at detecting aerosol pathogens. And for continuous monitoring this technology could be incorporated into the TWOBIAS continuous bio monitoring system.

- *Food or water* can be contaminated with biological toxins. Contaminations could occur via natural causes (i.e. aflatoxin B contamination in peanuts), accidentally during production (i.e. agricultural contamination) or could be contaminated intentionally with biological toxins as part of a terrorist attack. However, the public water supply is less vulnerable, since dilution, filtration, and the addition of chlorine annihilate most biological pathogens. Regular testing of food and water quality is needed in order to detect contamination with biological pathogens. In most countries in the developed world we have institutionalized agencies that prevent contamination of the food and water supply by thoroughly testing samples on toxic agents. At locations where there is an increased risk of biological toxic contamination due to accident, production error or biological terrorist attack, special measures for extra testing of food and water can be taken. Fluid-chromatography spectroscopy is a very effective technology for detection of pathogens in fluids. Also in this case the technology could be incorporated into the TWOBIAS continuous bio monitoring system.

- *Human carriers* are able to spread transmissible toxic biological agents by coughing, body fluids or by means of contaminated surfaces. At this moment it is still extremely difficult to detect people who have been contaminated with a transmissible agent. However, most of these agents become contagious after people have become ill or incapacitated, thereby reducing risks of disease transmission. The most critical stage in transmission occurs where the disease has become contagious but the person has not yet become incapacitated. At this stage the screening for people that have a raised body temperature with an infrared screening device is the only thing that may prevent an outbreak of the disease.

- *Infected animals* can also be carriers of a biological toxic agent. However, in most developed countries these animals live in a controlled environment, enabling continuous monitoring for toxic pathogens.

- *Insects* spread a number of toxic pathogens. Pathogens that cause diseases like Dengue fever, Malaria and the Plague are examples. Pathogens spread by insects could potentially be used by terrorists to force an outbreak of the disease. At this time, there are no technological devices that could detect a contamination by pathogens in insects on a regular basis. Contamination in insects is often discovered at a late stage, long after the contamination took place, at the moment people in a certain area fall ill on a large scale.

- *Physically distributed* through the mail or other means. Sites that are at risk could be screened to detect pathogens before they spread to humans.

Diseases and pathogens that are listed by the CDC (United States Center for Disease Control) as potential bioterror agents are subdivided in different categories of hazardousness.

- *Category A:* Easily disseminated and/or contagious; high mortality rates; might disrupt society; requires special action for public health preparedness. *Bacteria:* Anthrax, Plague and Tularemia. *Viruses:* Smallpox, Ebola, Marburg, Lassa and Machupo. *Biotoxins:* Botulism.

- *Category B:* Moderately easy to disseminate; moderate illness rates, low mortality; requires enhanced diagnostic capacity, surveillance. *Bacteria:* Brucellosis, Glanders, Melioidosis, Psittacosis. Food safety threats (Salmonella, E-Coli), water safety threats (i.e. Cholerae). *Viruses:* Viral encephalitis. *Rickettsia:* Q-fever, Typhus fever. *Biotoxins:* Ricin, Aflatoxin B, Epsilon toxin.

- *Category C:* Emerging infectious diseases that could be a future threat. *Viruses:* Nipah virus and Hanta virus.

The use of Anthrax spores on civilians in late 2001 has shown the necessity of protecting civilians from the terrorist use of toxic biological substances and viruses. The threat of a sophisticated large-scale attack using these substances has to be taken seriously. The success of a large-scale attack depends mainly on spreading a sufficient quantity of pathogens with an adequate concentration over a highly populated area. The protection of such an area against the threat of biological attack requires a safeguarding system that is able to detect and classify toxic pathogens and trigger a short-term alarm. The concept of the BIO-PROTECT project is the development of a fast-alert, easy-to-use device to be applied, for detection and identification of airborne bacteria, spores, viruses and toxins. Its technology is based on bio-aerosol detection by fluorescence, scattering and background aerosol measurement followed by ionization of air flow and analysis of the spectrum of relative speed of passage, which, in turn, enables identification of harmful biological agents. In the TWOBIAS project a modular system was developed of a stationary, reliable, vehicle-portable, low false alarm rate Two Stage Rapid Biological Surveillance and Alarm System for Airborne Threats (TWOBIAS) for use at indoor or outdoor public sites regarded as targets for bioterrorist attacks. The biological surveillance alarm system aims at reliability and calibrates and analyses the airborne biological particle content in the air at the site-of-use, and distinguishes between the natural air content and a release of biological threat agents.

§4.2 Assessment of CCTV Surveillance Technology

Associated technology sheets:

- CCTV - visual semi-automated camera Guppy_F036C
- CCTV - visual spectrum dome-fixed
- CCTV - visual spectrum dome-zoom tilt and rotate
- CCTV - visual spectrum fixed
- CCTV & ACTIVITY DETECTION - IPS Activity Detection
- CCTV & INFRARED - near-field
- CCTV & INFRARED - wide-area

Closed-circuit television (CCTV) is a setup of video cameras to transmit a signal from a specific place to a limited set of monitors. The signal is not openly transmitted though it may employ point-to-point (P2P), point to multipoint, or mesh wireless links. CCTV technology is most often used for surveillance in areas that may need monitoring to prevent or register crimes.

The images in a CCTV system are captured through the lens of the camera and projected onto a high resolution CCD chip that converts the image into a large collection of digital data that is stored and transmitted along the interconnects (wired or wireless) of the CCTV system to television monitors or a storage server.

CCTV surveillance cameras generally have the following features:

- Analog or digital CCTV cameras. The capturing of the image is nowadays done in most cameras with a digital CCD device, however we refer to a camera as being analog if the signal from the camera is an analog signal. The signal from a real digital camera is digital.

- Networked CCTV cameras. These cameras often have an IP address and are connected to other cameras via a server. The data of the image that is exchanged to the server via a LAN or WLAN system can be secured by encryption, such that the information cannot be hacked from outside.

- Night vision cameras. For low light conditions, some cameras are equipped with CCD sensors that are very sensitive to light. Other cameras are equipped with infrared sensors, which provides thermographic sensing of the environment under low-light conditions. The infrared camera enhances the camera input by detecting the infrared radiation emitted by objects and people.

- Image resolution determined by the number of pixels available on the CCD sensor in the camera. Video formats that are available are PAL (768 x 576 pixels), NTSC (720 x 480 pixels), VGA (640 x480 pixels), SVGA (800 x 600 pixels), SXGA (1200 x 1024 pixels) and HD (1920 x 1080). Nowadays, megapixel cameras of 10 to 20 megapixels for pictures and the HD video camera have become the standard resolution. However, the higher the resolution of the image, the larger the accompanying data package, thereby increasing the processing time of the images.

- Mounting varieties of the camera. Dome-shaped cameras can be mounted on a ceiling and have the capability to rotate within the dome. Bullet-shaped boxes that contain the camera or very small cameras that can be incorporated into objects, such that they are not visible by the naked eye.

- Pan-Tilt-Zoom cameras. These cameras have the ability to get better camera vision, by eliminating dead angles and by deploying a zooming functionality.

Today’s high-definition CCTV cameras have many computer-controlled technologies that allow them to identify, track, and categorize objects in their field of view.[4]

Video Content Analysis (VCA) technology enables the automatic analysis of video content that is not based on a single image, but detects and determines events as a function of time. A system using VCA can recognize changes in the environment and identify and compare objects related to a database based on pre-defined classifiers. VCA analytics can also be used to detect unusual patterns in an environment, such as anomalies in a crowd of people. A camera like the visual semi-automated camera Guppy_F036C, which is a high-resolution camera with automatic trigger is able to detect suspect objects and is used for areal clearance control and other surveillance operations. In order to enhance the capabilities of CCTV cameras, other sensors are incorporated into the camera system. For example, motion sensors that can easily detect motion without the use of advanced image analysis software to detect motion in images. For surveillance in dark areas, CCTV cameras are often equipped with an additional infrared sensor that

[4] The use of CCTV raises a number of ethical issues – for a SURVEILLE discussion of these in relation to technical assessment see SURVEILLE Deliverable D2.6. ‘Matrix of Surveillance Technologies’ pages 8, 36-43
http://www.surveille.eu/PDFs/D2.6%20Matrix%20of%20Surveillance%20Technologies.pdf

detects the body heat of a person or the heat of fire. Some of these cameras are equipped with a CCD that is able to detect infrared images. These cameras are suitable for detecting images of persons or other heat sources in the dark.

CCTV technology as a Facial Recognition System is a computer application that is able to automatically identify an individual from a video source. So far, only facial recognition in relation to a facial database with a limited number of persons and facial features has been effective with a low number of false positives. Facial recognition systems based on the interpretation of facial expression to determine a person's intention have so far not been very effective. Computerized monitoring of CCTV images is under development, allowing CCTV operators to observe many CCTV cameras simultaneously. These systems do not observe people directly but analyze the image on the basis of certain pre-defined classifiers like bodily behavior or certain types of baggage.

The data obtained with CCTV cameras is often stored on a digital video recorder or a computer server. In order to limit the amount of data, these images are compressed and often kept for a preset amount of time before they become automatically archived.

Closed-circuit digital photography (CCDP) is often combined with CCTV to capture and save high-resolution images for applications where a detailed image is required. Modern day CCTV cameras are able to take images in a digital still mode that has a much higher resolution than the images captured in the video mode.

A growing development in CCTV technology is the application of Internet protocol (IP) cameras. These cameras are equipped with an IP interface, enabling the incorporation of the camera in a Local Area Network (LAN) to transmit digital video data across. Optionally, the CCTV digital video data can be transmitted via the public Internet, enabling users to view their cameras through any Internet connection available. For professional secure applications IP video is restricted to within a private network or is recorded onto a secured remote server. IP cameras can be wired (LAN) or wireless (WLAN).

Vulnerability of CCTV cameras:

- CCTV cameras are usually visible and therefore often vulnerable to vandalism. Some CCTV cameras come in dust-tight, explosion-proof housing.
- The lens of the camera is vulnerable to sprayed substances that make the image blurry.
- Lasers can blind or damage the cameras.
- CCTV systems are vulnerable to hostile intrusion. Wireless IP cameras are in this respect much more vulnerable to hostile intrusion than wired cameras.

§4.3 Assessment of Chemical Surveillance Technology

Associated technology sheets:

- CHEM - explosives detection by antibody SALIENT
- CHEM - explosives detection near harbors UNCOS
- CHEM - gas chromatography drugs detector DIRAC
- CHEM - novel detection techniques COMMONSENSE
- CHEM - precursor and drugs detection CUSTOM
- CHEM - standoff explosives detection and identification OPTIX

The detection of hazardous chemical materials is the core goal of most chemical surveillance technology. Hazardous chemical materials may be used in terrorist attacks or spilled in chemical accidents near chemical plants. Common chemicals used for terrorist attacks include blister agents (mustard gas), nerve agents (Sarin and VX), blood agents (hydrogen cyanide, cyanogens chloride, arsine) and choking agents (chloropicrin, chlorine and phosgene). Chemical agents are less difficult to detect than biological agents. However, current detection systems are not yet capable of detecting chemical agents in a civilian environment. Most of the systems suffer from a lack of sensitivity and mobility, and require a trained operator. Currently, Gas Chromatography (GS) combined with Mass Spectrometry (MS) is the standard method of identification and quantification of chemical substances. Mass Spectroscopy together with Gas Chromatography is based on breaking apart a molecule before accelerating the charged fragments and bending their paths inside a magnetic field. This surveillance technology has a very high sensitivity for a variety of mixed samples but cannot achieve the same results in a mobile system. Furthermore, the technology is expensive and requires sample calibration before testing, which can only be carried out by trained personnel.

A chemical surveillance technology based on Colorimetric indicators, which is an enzymatic detection technique, is a very basic chemical detection technique. The detectors contain an acid based indicator that changes color as soon as it is exposed to a specific agent or aerosol. They are cheap and easy to use. However, colorimetric indicators are not only sensitive to the substance for which they were designed but are also sensitive to a wide variety of other substances, giving rise to false positives. The surveillance technology can serve as a cheap and simple early warning system, especially in an area where the risk of the release of a certain agent is high.

Ion Mobility Spectrometry is a mobile chemical surveillance technology that uses an electric field to distinguish differences in the velocity of ions. The technology is cheap and has a short response time, but is dependent on the agent's concentration. The technology is combined with surveillance technologies based on Surface Acoustic Wave devices that use a piezoelectric quartz crystal coated with polymers that absorbs particular chemicals. The technology can detect multiple substances simultaneously. The combined technology leads to a higher sensitivity and lower false alarm rate.

Another chemical surveillance technique employs infrared radiation to detect various chemical substances. It uses the fact that chemical agents have a unique infrared fingerprint that is related to their vibrational wavelength within the substance. By measuring the amount of radiation with a certain wavelength that is absorbed within a substance, one is able to identify the concentration of a particular chemical agent inside the substance.

Recently, several European projects have been set up in order to develop new chemical surveillance technologies that are especially suitable for civilian purposes. These projects are:

- DIRAC: A portable system for rapid detection of illicit drugs and key precursors by infrared absorption spectroscopy and gas chromatography. The goal of this project is to develop an advanced sensor system, that combines miniaturized Gas Chromatography (GC) as its key chemical separation tool, and Hollow-Fiber-based Infra Red Absorption Spectroscopy (HF-IRAS) as its key analytical tool to recognize and detect illicit drugs, key precursors and potential derivatives. For controls at EU external frontiers and intra-community checks, customs officers and law enforcement personnel will use the DIRAC sensor as a hand-held device to perform rapid detection of key chemicals, together with advanced data analysis and with low false positive rates.

- CUSTOM: Aims to perform chemical identification in contexts such as custom offices, inspection of trucks, cars, containers, as well as people and baggage. The device developed has to be used by field operators with no specific skills. Only established detection techniques are used in order to get an unambiguous response from the incorporated software tool that processes the roughly measured data. The system will be able to detect a large number of compounds with a low false alarm rate and high sensitivity.

- OPTIX: Optical Technologies for Identification of Explosives. OPTIX enhances the security of citizens by developing a transportable system for standoff detection and identification of explosives in real life scenarios at distances of around 20 meters, using alternative or simultaneous analysis by three different complementary optical technologies (LIBS, RAMAN and IR).

- COMMONSENSE: Creates a network of sensors through the simultaneous and parallel development of novel materials, portable sensors and wireless communications network, which use chemometric data-processing algorithms to “learn” to recognize trace amounts of explosives, and differentiate them from interferents. In COMMONSENSE a variety of sensor technologies are used, such that no substance can act as an interferent to all sensors, thus reducing the risk of false positives and negatives. Chemometric algorithms that learn to recognize the fingerprint sensor response to distinct explosives types and at the same time ignore interfering compounds achieve elimination of the remaining false readings. The COMMONSENSE network uses low-cost sensor modules in wireless communication in combination with a central server, which manages remote access, control, operation and readout from the network.

- SALIANT: The development of a hand-held device for real-time analysis of explosives, chemicals and drugs at trace level. The SALIANT detection system is an immuno-array based technology for the detection of small molecular weight analytes relevant to the needs of specific end users targeting explosives and chemical toxins. It is a mobile, hand-held system for sampling, detection, read-out, display, storage, retrieval and secure communication of results. It enables first responders and forensic scientists at major crime scenes to use real-time technology that supports risk assessment, evidence collection and information guided investigation.

- UnCoSS: The main objective of UnCoSS (Underwater Coastal Sea Surveyor) is to provide tools for the non-destructive inspection of underwater objects mainly based on the application of a neutron sensor. It develops a technology for protecting vulnerable naval infrastructures, especially against the threat of underwater IEDs (Improvised Explosive Device).

§4.4 Assessment of Data Surveillance Technology

Associated technology sheets:

- DATA - mobile phone tap PTS
- DATA ANALISIS - Omnifind
- DATA ANALYSIS - detection of money laundering HEMOLIA
- DATA ANALYSIS - networked data analysis SCIIMS
- DATA TRANSFER ANALYSIS - name recognition

Data analysis tools that examine large data sets on the Internet or in data communications to find particular pre-defined classifiers are widely used in crime fighting and anti-terrorism surveillance.[5]

Usually intelligence information from the Internet or other data communications has to be interpreted, integrated, analyzed, and evaluated if it is to provide useful information that can add to contextual awareness, with the use of situational and threat assessment methods.

Social Network Analysis (SNA) is a method of statistical investigation of the patterns of communication within groups. The basic concept of the method is the hypothesis that the way members of a group communicate with each other and members of other groups reveals important information about the group itself. The investigations are performed via the method of structural analysis, based on a mathematical graph model consisting of nodes and edges that model actors and communication, respectively, within the group. In addition all kinds of weights can be introduced in the model, which represents the probability of an event taking place in the model. The use of Bayesian belief networks (BBN) is one such uncertainty modeling and information fusion methodology to exploit uncertain causal relationships between large collections of variables.

Data analysis tools are widely used crime fighting tools in law enforcement. However, not much is known about their effectiveness. The effectiveness of the tools depends

[5] The use of data surveillance technologies raises a number of ethical issues – for a SURVEILLE discussion of these in relation to technical assessment see SURVEILLE Deliverable D2.6. 'Matrix of Surveillance Technologies' pages 8, 32-36
http://www.surveille.eu/PDFs/D2.6%20Matrix%20of%20Surveillance%20Technologies.pdf

heavily on the quality of the pre-defined classifiers, which in the end have a large impact on the final outcome of the researched data. If used in an appropriate way, data analysis tools have the potential to help police decision makers and front-line police officers reduce crime, prevent further offending, and apprehend criminals.

A number of significant data analysis tools are included in this report:

- HEMOLIA is a new generation Anti-Money Laundering intelligent multi-agent alert and investigation system, which in addition to the traditional financial data also makes extensive use of telecoms data, thereby opening up a new dimension of capabilities to all money laundering investigators and financial institutes. The technology consists of data collection and data mining from the Financial-and Telecom-plane, which is analyzed and creates enhanced alerts.

- OmniFind is an IBM software product that provides a high-quality enterprise search capability that is both scalable and secure. It can crawl and index documents stored in more than 25 different enterprise repositories and more than 250 document file types. The results that are returned from a search are highly relevant and can be further filtered easily using faceted navigation for many languages. The system can be scaled to millions of documents and thousands of users, since the system can be configured in flexible manner. The system is an open platform for processing unstructured information to enable semantic queries. Together with the Fraunhofer Research Institute, IBM has incorporated the search technology of Smart Semantics, which enables the user to obtain the essence of the contents from unstructured data. The technology recognizes the contents of websites and documents on the basis of a model-based contents analysis. To the contrary of recognizing contents with the aid of token words, Smart Semantics is a self-learning technology that improves its performance in time by gaining experience. The user saves time, since the software does the filtering rather than the user.

- SCIIMS is a European project directed at people trafficking and people smuggling as part of the fight against organized crime. The project deals with the development and application of information management techniques that enable information to be shared and fused nationally and internationally within a secure information infrastructure in accordance with European agencies information needs. Tools to assist decision making in order to predict events, and analyze likely consequences and effects to the security of citizens, have been developed. The technology is built around state-of-the art products and incorporates new capabilities that are vital to the improvement of information management and exploitation techniques.

E-mail surveillance is a technology where software tools screen each data packet that passes through. During the screening the contents of the mail can be filtered or altered. Deep Packet Inspection (DPI) is an e-mail screening technology where all the layers of a data packet are screened. The DPI engine that does the deep packet inspection is built around a set of pattern-recognizing algorithms that need permanent updating for effective screening over time.

Social Network Surveillance is a technology in which Deep Packet Inspection technology is combined with data mining for screening social media like Facebook and Google. Special filtering techniques are used to filter out atypical behavioral patterns and illegal content.

§4.5 Assessment of GPS Surveillance Technology

Associated technology sheets:

- GPS - car tracker SN

GPS surveillance technology is used to track a person, vehicle or a piece of property. In recent years the technology has become highly accessible to the general public. The Global Positioning System (GPS) is based around a constellation of 31 satellites that provide the GPS signal all around the world. By capturing the signal from three or more satellites, GPS receivers are able to calculate their position with an accuracy of about 10 meters. The GPS system is controlled from the ground by a series of ground stations used to interpret and relay satellite signals to various receivers. To reach the satellites, the GPS devices need to have access to the open sky, which means that GPS devices cannot be operated indoors. The GPS technology is prone to the following errors:

- Clock error: The accuracy of the clock of GPS receiver is in most cases not as accurate as the atomic clock of the GPS satellite, which leads to positioning errors.
- Orbital error: Errors in the determination of the orbit of a GPS satellite also lead to errors in the positioning calculations.
- Position error: Inaccurate GPS signals due to signal interference from reflections of buildings or other objects can lead to inaccurate data and positioning errors.

Together with computing devices, data storage and road maps, GPS devices are capable of transforming location, speed and time information into a format that can be displayed or fed via a data network to a server for further processing.

GPS tracking is a technology that is commonly used in surveillance operations to gather, analyze and store location data from GPS satellites to track or locate suspicious persons or shipments. Nowadays most available smartphones are equipped with a GPS receiver. The GPS receiver that is located in a smartphone can be exploited for surveillance purposes. By installing special software or apps on a smartphone it is possible to track and trace persons without their awareness. Already a lot of apps that are commercially available make use of GPS tracking information beyond the knowledge of the smartphone user for commercial purposes.

The widespread availability and use of GPS receivers in smartphones and navigation devices enables an easy application of the GPS technology for surveillance purposes. Most users of GPS technology are not aware that they are already tracked and traced by apps made available from commercial parties to investigate their customer behavior. The GPS information obtained for surveillance from these devices can be transferred easily from the device via the GSM network or a WiFi network (WLAN) to a custom server for data collection and further processing.

The positioning and timing function of GPS are vulnerable to manipulation and attacks. GPS jammers are devices that can disrupt the data submitted from the satellite by transmitting interfering noise, such that any receiver within reach can no longer connect with the satellite. Also GPS spoofing attacks may directly target a receiver by feeding it with altered input data, producing a faulty location. Due to these vulnerabilities GPS remains a surveillance tracking technology that can be easily scrambled by suspects that know they are being tracked.

§4.6 Assessment of Image Processing Surveillance Technology

Associated technology sheets:

- IMAGE PROCESSING - crowd and riot
- IMAGE PROCESSING - people counting and density

Since the cost of digital image processors and digital storage has fallen dramatically, the storage of analog storage for surveillance applications has changed to digital storage. This introduced all kinds of digital image processing techniques and applications into the field of image surveillance technology.

Movement detection, and many more sophisticated techniques in image analysis can be equipped with advanced sensor technology leading to proactive systems that allow sophisticated monitoring. Advanced software applications able to pick out a region of interest in an image have enhanced digital image processing for surveillance purposes dramatically. It enables the recognition of persons in crowds, showing sufficient details to recognize a person, whilst not permitting enough detail to allow the viewer to see every detail. However, when it is clear that the person in the image is a serious suspect, the images can be processed using digital image processing tools like contrast, detail and edge enhancing tools in order to reveal more detail in the image.

The requirements for high-quality images for stored evidence have been raised and the fear that evidence could be tampered with or fabricated has been taken more seriously. Digital images are very vulnerable to tampering and fabrication as it is very easy to change subtle or complete aspects of a digital image. The need for data protection has introduced encryption and watermarking technology within the digital image surveillance technology to help to protect against this risk. Well-accepted media management systems have been developed that use trusted third party crypto-technology and that take care that evidence is not segmented to avoid the risks of misinformation.

The JPEG 2000 system has many of the following aspects that are needed in image processing surveillance technology:

- The Motion JPEG 2000 system has features that allow catching sequences of actions, where the initial view could be at low resolution, switching under the monitor’s control to higher resolutions, faster frame rates, and including more metadata and regions of interest.

- The JPEG 2000 file formats allow both standardized and user metadata to be stored with the image data.

- The JPEG 2000 features sophisticated security support, effective client server communications, and an ability to link its features into an error-prone wireless infrastructure.

- The JPEG 2000 system standard has a low cost of implementation.

Digital image processing for surveillance applications also features facial recognition and suspicious behavior recognition software tools. Image processing control techniques have been developed that maintain processing accuracy and adjust video analysis based on its content. In this way, image-processing frequency can be customized to focus on video featuring human subjects, maximizing the amount of processing per server and thereby extending the area that can be covered for image analysis.

§4.7 Assessment of Infrared Surveillance Technology

Associated technology sheet:

- INFRARED - motion detector

The infrared band of the electromagnetic spectrum lies between the wavelengths of 0.7µm and 1 mm. The human body itself radiates infrared radiation with a wavelength between 3 - 14 µm, hence both active and passive infrared surveillance technologies can be used.

Infrared surveillance technology is used extensively as it uses light that is not visible to the naked eye. Further, due to the reduced Rayleigh scattering of infrared light in a haze, mist, rain and fog, it produces high contrast images of good quality under these circumstances. The technology is also used on a large scale for motion detection (PIR sensor), since the infrared sensor is sensitive to the infrared radiation that living animals and humans produce, making it an ideal sensor for the detection of moving living animals or humans.

Many biometric detection technologies have been developed using infrared radiation. Face and hand vein pattern recognition are the most commonly applied biometric modalities in this frequency band.

Nowadays more and more people use thermal (infrared) imagers to overcome many of the imaging challenges that plague other effective video surveillance technologies. As the cost of thermal imagers have been dropping steadily and the incorporation of the imagers in remote transmission systems over IP for monitoring applications has been growing, their use in video surveillance systems has become a standard feature.

The decision to use IR illuminated technology, thermal imaging technology or some combination of the two, depends on a number of factors. If the surveillance technology is used for detection, assessment, classification or identification purposes or a combination of these objectives, then the choice of the type of imagers is of importance, since it will provide a suitable solution with the appropriate field of view, resolution and placement of the imagers. Thermal imagers should be used where detection and general assessment is the main objective of surveillance, as they maximize detection capabilities by providing enhanced contrast, with less noise and clutter, regardless of the lighting conditions. The problem with thermal cameras is that they do not provide color information and are not able to give facial information. In general, infrared imagers and motion sensors should be used in combination with other imaging surveillance technologies in order to cover all the features that are needed for efficient monitoring, especially in monitoring systems that are connected via IP and that provide intelligent video analytics and digital image processing capabilities.

§4.8 Assessment of mm-Wave Surveillance Technology

Associated technology sheet:

- MM-WAVE - whole body scanner EQO

Millimeter and sub-millimeter wave surveillance technology fills in the gap between infrared and microwave surveillance technologies. Specifically, millimeter waves are located in the frequency band of 30-300 GHz, which is a wavelength of 10 – 1 mm, and the sub-millimeter regime is located in the range of 0.3 – 3 THz, which is a wavelength of 1 – 0.1 mm. These types of radiation can easily penetrate nonpolar dielectric materials such as plastic, wood and thin dry walls with little attenuation. The water content in these materials has a high influence on the attenuation properties of these materials for millimeter and sub-millimeter waves. The attenuation increases when the wavelength of the radiation decreases.

Applications of millimeter waves in surveillance technology systems include security screening and biometrics imaging[6]. We can distinguish between passive millimeter waves and active millimeter waves for the application in surveillance technology. Passive millimeter waves are emitted naturally by the body and scattered by the surrounding objects. The amount of passive radiation that is emitted by a body is very low. Hence, images produced from passive millimeter waves are often fuzzy and of low quality. With active millimeter waves the body is illuminated by an external source that emits radio waves in the range of millimeter waves. The created images with active millimeter waves have a good quality, showing the surface of the body in detail.

The detection of concealed weapons has been the most developed application of millimeter waves so far[7]. Millimeter-wavelength surveillance technology has much potential for contributing to overall aviation security, but its limitations need to be recognized[8]. The technology will be most effective, if it is used in conjunction with other sensor technologies that provide detection capabilities in additional wavelength regions. Millimeter-wavelength imaging is of a similar quality as x-ray imaging technology.

[6] Oka S, Togo H, Kukutsu N, Nagatsuma T, (2008), Latest trends in millimeter-wave imaging, Progress in Electromagnetics Research Letters, Vol. 1, 197-204 .

[7] Stanko s, Notel D, Huck J, Wirtz S, Kloppel F, Essen H, (2008), Millimeter Wave Imaging for Concealed Weapon Detection and Surveillance at up to 220GHz, Passive Millimeter-Wave Imaging Technology XI, Proc. of SPIE Vol. 6948.

[8] Peichl M, Suss H, Dill S, (2003), High resolution passive millimeter-wave imaging technologies for reconnaissance and surveillance, SPIE Vol. 5077, 0277-786X/03/.

However, millimeter-wavelength technology has the benefit of being non-ionizing radiation, which is not hazardous to human health. In contrast to x-ray radiation, millimeter-wavelength radiation cannot penetrate metal objects. This property can be advantageous for the detection of metal objects, but it can also be a problem when objects are hidden inside a metal object.

The application of millimeter-wavelength surveillance technologies poses a problem for the personal privacy of the people being screened[9]. Since millimeter-wavelength imaging technology produces good quality images of the human body without the presence of clothing, the surveillance technology has raised protests from the general public for offending their personal privacy.

To perform an accurate assessment of the applicability of millimeter-wavelength based surveillance technology for the detection of explosives and concealed weapons, the following issues should be considered:

- Decide on the range of materials that need to be detected.
- Assess the state of knowledge of what chemical structures or features of the scope of materials lend themselves to detection by millimeter-wavelength radiation.
- Assess the presence of these features in other common materials in order to determine the uncertainty in the detection of the material.
- Assess the contribution of additives to explosives in their response in a millimeter-wavelength detection system.

[9] Appleby R, Anderton RN, (2007), Millimeter-Wave and Submillimeter-Wave Imaging for Security and Surveillance, Proceedings of the IEEE, Vol. 95, No. 8.

§4.9 Assessment of Digital Network Surveillance Technology

Associated technology sheets:

- NETWORK - AIS ship location detection and identification
- NETWORK - SIRIUS 3RK3
- NETWORK - UGM 2040
- NETWORK & INTERFACE - AMFIS data fusion for ground control

Digital network surveillance technology is used to interconnect numerous sensors of the same type to collect data from distinct locations or to interconnect sensors of different types to collect additional data that supplements the data from other sensors. Numerous data management systems have been developed that manage and collect the output of each sensor in order to manage a surveillance control system. The AMFIS system which was developed by the Fraunhofer Institute for Optical Solutions and System Technology, is a generic mobile ground station, that controls, analyses and guards information inside a sensor network and serves as an assistant system of an application system. Tasks that can be carried out in connection with the AMFIS system are:

- Control of roads and sceneries.
- Detection of persons and objects.
- Classification and recognition of the relation between persons or vehicles,
- Securing of evidence.

AMFIS is a generic system that can be adapted to distinct surveillance applications. Generic systems that collect and process the data within a sensor network are adaptable and provide opportunities for security systems to combine data from different sensor types in order to enlarge effectiveness.

In general, all surveillance systems that consist of a network of sensors managed by a server can be referred to as a digital network surveillance system. Networked CCTV systems and networked fire detection systems that are managed via a server also fall into this category of surveillance systems. A person can operate these systems or they can be sophisticated self-learning systems that control and manage the system without external guidance. Systems that are operated by a human are vulnerable to human error, while systems that are fully automated are vulnerable to software bugs and intrusion from the outside world. Nowadays, more and more surveillance systems are fully automated and regulated, since the complexity of surveillance systems requires more operators, which enlarges the risk of human error and increases the fixed costs dramatically.

By linking digital network surveillance systems, a large network of such systems is established. This provides a huge amount of data collected from an enormous amount of sensors.

§4.10 Assessment of Radar Surveillance Technology

Associated technology sheets:

- RADAR - Marine Radar (ARPA, automatic radar plotting aid)
- RADAR - short range radar for intrusion detection

Radar surveillance technology has been developed specifically for reliable detection and tracking of vehicles and persons in an environment where scanning with other types of electromagnetic radiation yields poor imaging results. Radar surveillance technology can be used for airspace, marine and ground security applications to monitor a wide range of targets like aircrafts, vehicles, ships and persons. Multifunctional surveillance radars are available that provide surveillance coverage from ground level to 700 meter altitude with simultaneous air, marine and ground detection[10]. These multifunctional radars are capable of providing the following surveillance tasks:

- Airspace monitoring and surveillance.
- Marine and coastal surveillance.
- Border intrusion detection.
- Perimeter air, marine and ground security.
- Shoreline protection.

By combining the data from acoustic, vibration and radar sensors, it is possible to increase the accuracy of the speed and location estimate. Furthermore, combining the sensor modalities enlarges the set of features used for object classification.

Another application of radar for surveillance purposes is motion detection radar that is not limited by the line-of-sight and is able to detect moving objects and persons that are located behind concrete walls[11]. This tool is very useful for the tracking of suspects that

[10] Kozma R, Wang L, Iftekharuddin K, McCracken E, Kahn M, Islam K, Bhurtil SR, Demirer RM, (2012), A Radar-Enabled Collaborative Sensor Network Integrating COTS Technology for Surveillance and Tracking, Sensors 2012, 12, 1336-1351.

[11] Frazier LM, (1997), Radar Surveillance through Solid Materials, SPIE Vol. 2938, 0-8194-2340-8/97/.

are located in another room, with the advantage that no devices have to be placed inside the room where the suspect is located.

Ground surveillance radars provide wide area surveillance and tracking over a large, 360-degree area. There are two primary technologies:

- Pulsed Doppler radar technology.
- Frequency Modulated Continuous Wave (FMCW) radar technology.

FMCW radars are able to detect small objects and persons and operate on the imaging principle. The background is divided into small segments. The changes in the reflection of the signals from each segment are measured, enabling detection of small objects within the segment. Long-range FMCW radar have typical resolutions of 1 meter in range and 1 degree in azimuth. Nowadays, FMCW radars are capable of detecting people that are even moving at near zero speed and are walking in any direction with respect to the radar.

Pulsed Doppler radars are radars that make use of the Doppler principle to detect motion. The Doppler principle states that all moving objects exhibit a frequency shift in the signal from the transmitter to the receiver. This frequency shift is proportional to the speed with which the object is moving towards the radar. However, Pulse Doppler radars have large areas where slowly moving objects will not be detected. This is due to a velocity threshold that is taken into account in order to avoid the influence of so-called clutter (the influence of other moving objects in the radar image due to the blowing of the wind).

The advantages of FMCW radar over other technologies such as pulsed Doppler radar are:

- FMCW radar is more robust, simpler in design, safer and lower cost than Doppler radar.
- The number of false alarm rates with FMCW radar is lower.
- FMCW radar is able to detect more valid targets.

To circumvent radar detection, there are many ways to counter a radar probe. Persons who are being probed can use radar-reflecting barricades or radar-absorbent materials, disturbing radar scattering points, or generate a radar-jamming signal in order to disturb the radar image.

§4.11 Assessment of UAV Surveillance Technology

Associated technology sheet:

- UAV - platform helikite balloon

Unmanned Aerial Vehicles are becoming a very important part of surveillance technology, since a wide variety of commercial aerial vehicles have entered the market, which has lead to a large drop in price. The availability of cheap and good navigation technology has accelerated the development of UAVs significantly. The total system that is required for the UAV to operate consists of the Unmanned Aerial Vehicle, a (mobile) ground control unit and wireless data connections. UAVs are also commonly referred to as Drones. The drone types that are used for surveillance include:

- Drones designed for logistics in surveillance operations.
- Law-enforcement drones that carry out surveillance and tracking operations.
- Commercial drones for surveillance operations for property protection.
- Micro-drones for surveillance operations where the drone itself must be invisible.

Drones can be equipped with all kinds of surveillance tools, such as CCTV equipment, infrared and thermal cameras, audio recording devices, radar equipment, Wi-Fi interception technology and chemical and radiation detection devices. However, in order to use most of these tools, extra measures have to be taken in the processing of the acquired data, to compensate for the motion of the drone. CCTV, infrared, thermal and radar images can become blurry due to the rapid movements of the drone, especially if it is a medium or small sized drone. Another issue is that often the weight of these extra surveillance tools is a problem, since most of the drones that are commercially available are able to carry an extra weight of only 10 Kg. Most drones are equipped with a gasoline engine, which provide a large action radius, however these make a lot of noise. Small drones are equipped with electric motors, which have the advantage that they are very silent, allowing surveillance operations with sound-recording or operations where the drone itself stays unnoticed. However, electric drones only have a small action radius and the batteries are heavy, limiting the amount of weight the drone can carry during an operation. Finally, drones are exceptionally vulnerable to the weather conditions. In windy weather conditions the movements of the drone will disrupt the effective surveillance operation, and in some cases may lead to crashes.

Suspects targeted by a surveillance drone have a number ways to circumvent detection, thereby reducing the effectiveness of the surveillance:

- The drone can be shot down.
- The GPS signal of the drone can be jammed, which results in navigation errors and eventually to the crash of the drone.
- Real-time images that are transmitted to a ground system via a satellite connection can have large latency. This latency can be used by the suspect to avoid direct action against him by moving around rapidly.

§4.12 Assessment of Audio Surveillance Technology

Associated technology sheets:

- SOUND - ECM8000 microphone
- SOUND - sound processing FIREFACE400
- SOUND - sound recording bug AU046

The widespread application of audio surveillance technology has been thriving, as it is almost undetectable to the naked eye and it can be hidden in almost any location.

Audio surveillance devices, like phone bugs, distant audio recorders or cell-phone audio bugs can be assembled into a very small device and incorporated into almost any object we use in our everyday life. Audio surveillance devices capture the audio with a microphone (audio sensor), which converts the audio signal to an electric signal. This analog electric signal is converted via an analog to digital converter to binary data, which can be stored and distributed wired or wireless to a receiver, where the signal is converted from a digital to an analog audio signal. Due to modern day chip technology, these audio surveillance devices consists of very few electronic components, assembled on a very small printed circuit board, making it possible to incorporate the device in almost any object available. Most of the present day audio chips that are used have also a DSP (Digital Signal Processor) incorporated, allowing onboard digital audio signal processing to enhance the quality of the sound.

Sound bugs can be hidden almost anywhere. Their vulnerability to detection results from the way the sound bugs communicate the received digital audio signal to the receiver. Wireless communication involves the sound bug transmitting an electromagnetic wave within a certain frequency band, which can be detected with a device that can locate these electromagnetic sources.

Audio surveillance can also be carried out by measuring the vibrations of windows with the aid of a laser-monitoring device or by a sound bug hidden in an adhesive substance on the window.

Phone sound bugs are probably the most common audio surveillance devices. A phone sound bug is simply a small audio spying device that is usually attached to the inside of the phone and for audio surveillance. It transmits digital audio signals during a conversation to another location to stream the voice of the suspect and the contacted person to a monitoring device.

Cell-phone audio surveillance is a technology that uses a normal cell phone, which is equipped with a device that enables an external connection and tracking of all conversations made over that cell phone. Together with the installed GPS system the location of the caller can also be monitored. Smart phones may even be infected with spy software that copies all information and communication and sends it through normal communication networks (Cellular or WiFi) to an investigator.

§4.13 Assessment of Radioactive Detection Surveillance Technology

Associated technology sheet:

- RADIOACTIVE - Compton detector COCAE

Nuclear radiation can only be detected with the aid of special equipment since it cannot be detected by human or animal senses. The first device that was able to detect x-ray radiation was invented in 1908 by Hans Geiger and was called the Geiger counter. In recent years many more devices have been developed that are able to detect nuclear radiation over a much broader range than solely x-ray radiation.

There are a number of factors that limit radiation surveillance devices to detect nuclear material:

- The amount of radioactive content.
- The capacity and size of the detection device.
- The proximity of the surveillance device to nuclear material.
- Shielding of the nuclear materials from surveillance detection.

In many cases it is very difficult to detect, for instance, the illegal transport of nuclear material, particularly if the transport contains low radiation-enriched uranium[12][13]. In order to detect materials that emit low levels of nuclear radiation, sensitive detection devices are needed.

Most modern detection devices for surveillance purposes use spectrometers based on scintillation crystals. These crystals react to nuclear radiation by emitting a flash of light proportional to the energy of the photon captured by the crystal. These solid-state devices often contain a wide range of materials such as germanium, silicon, mercuric iodide, cadmium telluride and cadmium zinc telluride. Detectors that contain these materials transform incident photons emitted by nuclear materials directly into electrical pulses.

[12] Leidholdt EM, Williams GA, McGuire EL, (2003), A Reassessment of Radioactive Material security in Health Care and Biomedical Research, Operational Radiation Safety, S15-S19.

[13] International Atomic Energy Agency. (2003), IAEA-TECDOC-1355, Security of radioactive sources

Nowadays, radiation surveillance devices contain a high Z semiconductor operating at room temperature with high efficiency.

Radiation surveillance equipment is widely employed by Homeland security agencies, emergency response groups and the nuclear industry all over the world. The threat of terrorist attack with so called “dirty bombs” containing nuclear radioactive material has been regarded as a particularly important threat, with government agencies investing heavily in the development of portable and efficient radiation surveillance equipment. These surveillance devices are devoted to preventing terrorists from obtaining suitable radioactive material for the fabrication of a “dirty bomb”.

§4.14 Assessment of X-Ray Surveillance Technology

Associated technology sheet:

- X-RAY - luggage screening

X-ray surveillance technology is a surveillance technology widely used in airports to detect explosive materials and weapons in luggage[14][15]. The devices that are located at the gates of airports for the screening of hand luggage are devices with one x-ray source and an x-ray detector, which provide traditional x-ray images, enhanced with software to distinguish different objects more clearly, and evaluated by a trained operator. For the screening of the other baggage, special explosive detection systems (EDS) are used, which are belt-fed machines used to scan un-opened checked luggage for explosive materials. The luggage is scanned in a Computed Tomography (CT) x-ray machine, which uses special software to interpret the data from multiple x-ray sensors. The performance of such a system is about 300 bags per hour. In order to increase the performance, manufacturers have introduced systems that are capable of screening about 1200 bags per hour. These systems are called Real Time Tomography systems. Instead of rotating the detectors in a scanner with 11 detectors, the RTT system relies on 400 stationary detectors, avoiding the time consuming rotation of the detectors.

Passenger screening is also evolving to keep up with the changing threats of terrorists exploring new ways to circumvent airport security. Threats now include liquid explosives, radioactive materials and toxic pathogens. However, in the screening of humans, people cannot be subjected to the same type of radiation used for baggage screening, as it is hazardous to health.

In most airports full-body imaging devices have been installed, which use backscatter x-ray or millimeter radio wave technology. X-ray backscatter technology is based on the x-ray Compton scattering effect of x-rays. Unlike traditional x-ray equipment, which relies on the transmission of x-rays through the object, backscatter x-ray technology detects the x-ray radiation that is reflected from the object. The backscatter technology requires a very low power x-ray source, since the detection only relies on the reflected x-ray

[14] Chalmers A, (2005), Three applications of backscatter X-ray imaging technology to homeland defense, Proc. of SPIE, Vol. 5778, No. 1, pp. 989-93

[15] Bossi RH et al, (1988), Backscatter X-ray imaging, Materials Evaluation, Vol. 46, No. 11, pp. 1462-7

radiation, which is hardly attenuated from the x-ray source to detector, while transmission based x-ray technology involves most of the energy being absorbed into the body. Backscatter x-ray technology only needs to generate a very low dose of only 10 microREM of radiation (100 milliREM a year is the threshold). The technology relies on the same technology as radar, where the device projects energy onto an object and the incorporated software interprets the reflected energy detected by numerous detectors around the object to display an image. However, the x-ray backscatter screening technique has run into the same opposition based on privacy concerns as the millimeter radio wave backscatter screening devices. The public views the screening as violating the dignity of passengers, as during the screening process a person's naked body is made visible.

The effectiveness of backscatter x-ray equipment has been investigated by numerous research groups all over the world. Multiple reports document the failure of existing equipment deployed at airports. Problems that were encountered during the survey were:

- The scanners are inaccurate and inconvenient.
- The scanners lead to big delays in the boarding of passengers.
- The scanners were ineffective and could be easily thwarted.
- For airport screening the European Union only authorizes the use of scanners that do not use ionising radiation.[16]

[16] COMMISSION REGULATION (EU) No 185/2010 of 4 March 2010 laying down detailed measures for the implementation of the common basic standards on aviation security (as amended); ANNEX para. 4.1.1.2

Annex 1: Equipment fact sheets

EQUIPMENT FACT SHEET

Surveillance technology survey sheet
V1.1

EQUIPMENT IDENTIFICATION	
name	BIO - airborne ims BIO-PROTECT
description of equipment	Ionisation based mass spectroscpy for detecting ions
group	BIO
type	bio-agent detector
other	
Sources	fp7-bioprotect.eu

CLASSIFICATION OF FUNCTIONALITY	
Function description	gas-chromatography ion mass spectroscopy
hazard (bow-tie left) **(to be controlled)**	
events (bow-tie event) **(unwanted activities)**	attack with airborn pathogens
consequence (bow-tie righ **(of failure)**	
bow-tie functionality	rapid biological threat detection

TECHNICAL FEATURES		
dimensions		[m/m/m]
weight		[Kg]
power consumption		[W]
control range (functional		[m]
autonomous operation		[yes/no]
automated operation		
system embedding		

OPERATIONAL FEATURES		
personnel requred	yes	[%]
maintenance	na	[days/year]
ballpark cost	na	[Eur]

EQUIPMENT FACT SHEET

Surveillance technology survey sheet
V1.1

EQUIPMENT IDENTIFICATION		
name	BIO - continuous bio monitoring system TWOBIAS	
description of equipment	unspecified detection technology, integrated system	
group	BIO	
type	bio detectors and network	
other		
Sources	www.twobias.info	

CLASSIFICATION OF FUNCTIONALITY	
Function description	continuously operating Bio detector system
hazard (bow-tie left) **(to be controlled)**	early detection of pathogens early identification of pathogens, possible prophylaxi
events (bow-tie event) **(unwanted activities)**	identification of pathogens
consequence (bow-tie rigl **(of failure)**	identification of pathogens for medicine programme
bow-tie functionality	identification to prevent disease and help fight disea

TECHNICAL FEATURES		
dimensions		[m/m/m]
weight		[Kg]
power consumption		[W]
control range (functional		[m]
autonomous operation	yes	[yes/no]
automated operation	yes	
system embedding	system	

OPERATIONAL FEATURES		
personnel requred	na	[%]
maintenance	na	[days/year]
ballpark cost	na	[Eur]

EQUIPMENT FACT SHEET

Surveillance technology survey sheet
V1.1

EQUIPMENT IDENTIFICATION	
name	CCTV - visual semi-automated camera Guppy_F036C
description of equipment	high resolution digital camera with automatic trigger
group	CCTV
type	MARLIN F-146
other	
Sources	http://www.alliedvisiontec.com/us/products/camera

CLASSIFICATION OF FUNCTIONALITY	
Function description	image sensor for object detection
hazard (bow-tie left) **(to be controlled)**	area clearance control, object detection detection of suspect objects
events (bow-tie event) **(unwanted activities)**	detection of area intrusion
consequence (bow-tie right) **(of failure)**	record of event data retrieving
bow-tie functionality	visual information of new threats visual information about events unfolding visual evidence of crime or terorism after the event

TECHNICAL FEATURES		
dimensions	0.072/0.044/0.029	[m/m/m]
weight	0.12	[Kg]
power consumption	< 3	[W]
control range (functional space)	depends on mounted lens	[m]
autonomous operation	no	[yes/no]
automated operation	partly: camera activation triggering	
system embedding	required	

OPERATIONAL FEATURES		
personnel requred	na	[%]
maintenance	na	[days/year]
ballpark cost	na	[Eur]

EQUIPMENT FACT SHEET

Surveillance technology survey sheet
V1.1

EQUIPMENT IDENTIFICATION	
name	CCTV - visual spectrum dome-fixed
description of equipment	Network Camera
group	CCTV
type	dome-fixed
other	
Sources	http://www.axis.com/products/video/camera/fixed

CLASSIFICATION OF FUNCTIONALITY	
Function description	detection of events in large and distant areas
hazard (bow-tie left) **(to be controlled)**	area clearance control, object detection detection of suspect objects
events (bow-tie event) **(unwanted activities)**	detection of area intrusion
consequence (bow-tie rigl **(of failure)**	record of event data retrieving
bow-tie functionality	visual information of new threats visual information about events unfolding visual evidence of crime or terorism after the event

TECHNICAL FEATURES		
dimensions	0,1 x 0,04	[m/m]
weight	1 kg	[Kg]
power consumption	10	[W]
control range (functional	fixed field of view (cone-shaped)	[m * m]
autonomous operation	no	[yes/no]
automated operation	no	
system embedding	part of modular system	

OPERATIONAL FEATURES		
personnel requred	yes	[%]
maintenance	na	[days/year]
ballpark cost	500€/instance	[Eur]

EQUIPMENT FACT SHEET

Surveillance technology survey sheet
V1.1

EQUIPMENT IDENTIFICATION	
name	CCTV - visual spectrum dome - zoom tilt and rotate
description of equipment	Network Camera
group	CCTV
type	dome-ptz
other	
Sources	http://www.axis.com/products/video/camera/ptz/in

CLASSIFICATION OF FUNCTIONALITY	
Function description	detection of events in large and distant areas
hazard (bow-tie left) **(to be controlled)**	area clearance control, object detection detection of suspect objects
events (bow-tie event) **(unwanted activities)**	detection of area intrusion
consequence (bow-tie rigl **(of failure)**	record of event data retrieving
bow-tie functionality	visual information of new threats visual information about events unfolding visual evidence of crime or terorism after the event

TECHNICAL FEATURES		
dimensions	0,20 x 0,30	[m/m]
weight	2 kg	[Kg]
power consumption	20	[W]
control range (functional	pan/tilt and zoomable field of view (cone-shaped)	[m * m]
autonomous operation	no	[yes/no]
automated operation	no	
system embedding	part of modular system	

OPERATIONAL FEATURES		
personnel requred	yes	[%]
maintenance	na	[days/year]
ballpark cost	900€/instance	[Eur]

EQUIPMENT FACT SHEET

Surveillance technology survey sheet
V1.1

EQUIPMENT IDENTIFICATION	
name	CCTV - visual spectrum fixed
description of equipment	Network Camera
group	CCTV
type	fixed
other	
Sources	http://www.axis.com/products/video/camera/fixed/

CLASSIFICATION OF FUNCTIONALITY	
Function description	detection of events in large and distant areas
hazard (bow-tie left) **(to be controlled)**	area clearance control, object detection detection of suspect objects
events (bow-tie event) **(unwanted activities)**	detection of area intrusion
consequence (bow-tie rigl **(of failure)**	record of event data retrieving
bow-tie functionality	visual information of new threats visual information about events unfolding visual evidence of crime or terorism after the event

TECHNICAL FEATURES		
dimensions	0,30 x 0,1 x 0,05	[m/m/m]
weight	1 kg	[Kg]
power consumption	10	[W]
control range (functional	fixed field of view (cone-shaped)	[m * m]
autonomous operation	no	[yes/no]
automated operation	no	
system embedding	part of modular system	

OPERATIONAL FEATURES		
personnel requred	yes	[%]
maintenance	na	[days/year]
ballpark cost	500€/instance	[Eur]

EQUIPMENT FACT SHEET

Surveillance technology survey sheet
V1.1

EQUIPMENT IDENTIFICATION	
name	CCTV & ACTIVITY DETECTION - IPS activity detection
description of equipment	single functionality motion detecor
group	CCTV
type	motion detector
other	
Sources	http://www.ips-analytics.com/produkte/ips-videoan

CLASSIFICATION OF FUNCTIONALITY	
Function description	detection of motion in video scenes
hazard (bow-tie left) **(to be controlled)**	identification of motion in wrong areas motion out of wrong areas
events (bow-tie event) **(unwanted activities)**	evidence of events unfolding
consequence (bow-tie rig **(of failure)**	record of event data retrieving
bow-tie functionality	visual information of new threats visual information about events unfolding visual evidence of crime or terorism after the event

TECHNICAL FEATURES		
dimensions	s/w	[m/m/m]
weight	na	[Kg]
power consumption	na	[W]
control range (functional	na	[m]
autonomous operation	no	[yes/no]
automated operation	yes, automated motion detection software	
system embedding	part of modular system	

OPERATIONAL FEATURES		
personnel requred	na	[%]
maintenance	na	[days/year]
ballpark cost	na	[Eur]

EQUIPMENT FACT SHEET

Surveillance technology survey sheet
V1.1

EQUIPMENT IDENTIFICATION	
name	CCTV & INFRA RED - near-field
description of equipment	IR-Cam
group	CCTV & INFRA RED
type	near-field
other	
Sources	http://www.axis.com/products/video/camera/therm http://www.drs.com/Products/RSTA/WatchMasterIP

CLASSIFICATION OF FUNCTIONALITY	
Function description	detection of events in large and distant areas
hazard (bow-tie left) **(to be controlled)**	area clearance control, object detection detection of suspect objects
events (bow-tie event) **(unwanted activities)**	detection of area intrusion
consequence (bow-tie rigl **(of failure)**	record of event
bow-tie functionality	visual information of new threats visual information about events unfolding

TECHNICAL FEATURES		
dimensions	0,20 x 0,30	[m/m]
weight	2 kg	[Kg]
power consumption	15	[W]
control range (functional	pan/tilt and zoomable field of view (cone-shaped) ne	[m * m]
autonomous operation	no	[yes/no]
automated operation	no	
system embedding	part of modular system	

OPERATIONAL FEATURES		
personnel requred	yes	[%]
maintenance	na	[days/year]
ballpark cost	2500€/instance	[Eur]

EQUIPMENT FACT SHEET

Surveillance technology survey sheet
V1.1

EQUIPMENT IDENTIFICATION		
name	CCTV & INFRA RED - wide-area	
description of equipment	IR-Cam	
group	CCTV & INFRA RED	
type	wide-area	
other		
Sources	http://www.zeiss.de/C1257088004A3F3C/EmbedTite http://www.flir.com/cs/emea/de/view/?id=42061	

CLASSIFICATION OF FUNCTIONALITY	
Function description	detection of person in wide area (border control)
hazard (bow-tie left) **(to be controlled)**	area clearance control, object detection detection of suspect objects
events (bow-tie event) **(unwanted activities)**	detection of area intrusion
consequence (bow-tie rigl **(of failure)**	
bow-tie functionality	visual information of new threats visual information about events unfolding

TECHNICAL FEATURES		
dimensions	0,50 x 0,30	[m/m]
weight	10 kg	[Kg]
power consumption	40 (<125 when max. heating is requiered)	[W]
control range (functional	pan/tilt and zoomable field of view (cone-shaped) wi	[m * m]
autonomous operation	no	[yes/no]
automated operation	no	
system embedding	part of modular system	

OPERATIONAL FEATURES		
personnel requred	yes	[%]
maintenance	na	[days/year]
ballpark cost	20000€/instance	[Eur]

EQUIPMENT FACT SHEET

Surveillance technology survey sheet
V1.1

EQUIPMENT IDENTIFICATION	
name	CHEM - explosives detection by antibody SALIENT
description of equipment	hand-held device to analyze explosives, toxic chemicals
group	CHEM
type	explosives, chemicals and drugs detector
other	
Sources	www.saliant.eu

CLASSIFICATION OF FUNCTIONALITY	
Function description	selective antibodies detection of chemicals
hazard (bow-tie left) **(to be controlled)**	trace detection of illegal goods
events (bow-tie event) **(unwanted activities)**	rapid identification of illegal goods rapid identification of explosives
consequence (bow-tie right) **(of failure)**	
bow-tie functionality	First Responders at crime scenes and terrorist incidents crime prevention and community safety

TECHNICAL FEATURES		
dimensions	10cm*10cm	[m/m/m]
weight	<1kg	[Kg]
power consumption		[W]
control range (functional space)		[m]
autonomous operation	no	[yes/no]
automated operation		
system embedding		

OPERATIONAL FEATURES		
personnel requred	yes	[%]
maintenance	yes	[days/year]
ballpark cost	na	[Eur]

EQUIPMENT FACT SHEET

Surveillance technology survey sheet
V1.1

EQUIPMENT IDENTIFICATION		
name	CHEM - explosives detection near harbours UNCOS	
description of equipment	unmanned ROV explosive detection by neutron dete	
group	CHEM	
type	ROV	
other		
Sources	www.uncoss-project.org	

CLASSIFICATION OF FUNCTIONALITY	
Function description	detection of explosives and IEDs in harbors
hazard (bow-tie left) **(to be controlled)**	detection of explosives and IED's
events (bow-tie event) **(unwanted activities)**	
consequence (bow-tie rig **(of failure)**	
bow-tie functionality	prevention of IED attack on harbor.

TECHNICAL FEATURES		
dimensions	2 x 0,85 x 1,3 m	[m/m/m]
weight	na	[Kg]
power consumption	na	[W]
control range (functional	na	[m]
autonomous operation	no	[yes/no]
automated operation	no	
system embedding	part of modular system	

OPERATIONAL FEATURES		
personnel requred	na	[%]
maintenance	na	[days/year]
ballpark cost	na	[Eur]

EQUIPMENT FACT SHEET

Surveillance technology survey sheet
V1.1

EQUIPMENT IDENTIFICATION	
name	CHEM - gas chromatography drugs detector DIRAC
description of equipment	IR absorption spectroscopy and gas chromatography
group	CHEM
type	hand held rapid detector
other	
Sources	http://www.consorziocreo.it http://www.fp7-dirac.eu

CLASSIFICATION OF FUNCTIONALITY	
Function description	rapidly recognize and detect illicit drugs and precursors
hazard (bow-tie left) **(to be controlled)**	
events (bow-tie event) **(unwanted activities)**	Capture drug traffickers
consequence (bow-tie right) **(of failure)**	
bow-tie functionality	daily fight (hand portable, fast response, good

TECHNICAL FEATURES		
dimensions		[m/m/m]
weight		[Kg]
power consumption		[W]
control range (functional space)		[m]
autonomous operation	no	[yes/no]
automated operation	no	
system embedding	no	

OPERATIONAL FEATURES		
personnel requred	yes	[%]
maintenance	na	[days/year]
ballpark cost	na	[Eur]

EQUIPMENT FACT SHEET

Surveillance technology survey sheet
V1.1

EQUIPMENT IDENTIFICATION		
name	CHEM - novel detection techniques COMMONSENSE	
description of equipment	water phase sensor for explosives detection	
group	CHEM	
type	water phase decector	
other		
Sources	http://www.fp7projectcommonsense.eu	

CLASSIFICATION OF FUNCTIONALITY		
Function description	sensor for explosives in waste water outlets	
hazard (bow-tie left) **(to be controlled)**	explosives in water phase to capture bomb-makers bef radionucleides in water phase to capture dirty bomb makers	
events (bow-tie event) **(unwanted activities)**	Chemical trace detection to find drugs laboratories	
consequence (bow-tie right) **(of failure)**		
bow-tie functionality	prevention of deployment of explosives identifying drugs labs in operation	

TECHNICAL FEATURES		
dimensions		[m/m/m]
weight		[Kg]
power consumption		[W]
control range (functional space)		[m]
autonomous operation	yes	[yes/no]
automated operation	yes	
system embedding	yes	

OPERATIONAL FEATURES		
personnel requred	yes	[%]
maintenance	na	[days/year]
ballpark cost	na	[Eur]

EQUIPMENT FACT SHEET

Surveillance technology survey sheet
V1.1

EQUIPMENT IDENTIFICATION		
name	CHEM - precursor and drugs detection CUSTOM	
description of equipment	laser photo acoustic spectroscopy and UV fluorescer	
group	CHEM	
type	drugs and precursors for drugs	
other		
Sources	www.custom-project.eu	

CLASSIFICATION OF FUNCTIONALITY		
Function description	detection of motion in video scenes	
hazard (bow-tie left) **(to be controlled)**	detection of precursors for drug production	
events (bow-tie event) **(unwanted activities)**	detection of drug production detection of drug trafficking	
consequence (bow-tie rig **(of failure)**		
bow-tie functionality	prevention of drug prevention identificatio of drug production	

TECHNICAL FEATURES		
dimensions		[m/m/m]
weight		[Kg]
power consumption		[W]
control range (functional	meters	[m]
autonomous operation	no	[yes/no]
automated operation	no	
system embedding	yes	

OPERATIONAL FEATURES		
personnel requred	na	[%]
maintenance	na	[days/year]
ballpark cost	na	[Eur]

EQUIPMENT FACT SHEET

Surveillance technology survey sheet
V1.1

EQUIPMENT IDENTIFICATION		
name	CHEM - standoff optical detection of explosives OPTIX	
description of equipment	optical sensor (LIBS, RAMAN, IR absorption)	
group	CHEM	
type	car-transportable	
other		
Sources	www.fp7-optix.eu http://www.fotonica-evenement.nl/assets/Fotonica-2(	

CLASSIFICATION OF FUNCTIONALITY		
Function description	stand off detection and identification of explosives in r	
hazard (bow-tie left) **(to be controlled)**	detection/identification of explosives in the vicinity	
events (bow-tie event) **(unwanted activities)**		
consequence (bow-tie right) **(of failure)**		
bow-tie functionality	prevention of explosion damage	

TECHNICAL FEATURES		
dimensions		[m/m/m]
weight		[Kg]
power consumption		[W]
control range (functional space)	20meter	[m]
autonomous operation	no	[yes/no]
automated operation	yes	
system embedding	yes	

OPERATIONAL FEATURES		
personnel requred	yes	[%]
maintenance	yes	[days/year]
ballpark cost	na	[Eur]

EQUIPMENT FACT SHEET

Surveillance technology survey sheet
V1.1

EQUIPMENT IDENTIFICATION		
name	DATA - mobile phone tap PTS	
description of equipment	software to record phone use and data	
group	DATA	
type	phone-based software	
other		
Sources	http://phonetappingsoftware.net/iphone-tapping/	

CLASSIFICATION OF FUNCTIONALITY	
Function description	data gathering from mobile phone
hazard (bow-tie left) **(to be controlled)**	identification of criminal plans or networks
events (bow-tie event) **(unwanted activities)**	intercept signals for commencing crimes
consequence (bow-tie right) **(of failure)**	evidence gathering
bow-tie functionality	evidence of crime to prevent crime evidence for conviction intercept crimes in action

TECHNICAL FEATURES		
	embedded in phone	
dimensions	computer software	[m/m/m]
weight	na	[Kg]
power consumption	na	[W]
control range (functional space)	phone	[m]
autonomous operation	no	[yes/no]
automated operation	yes	
system embedding	in mobile phone	

OPERATIONAL FEATURES		
personnel requred	1	[%]
maintenance	na	[days/year]
ballpark cost	na	[Eur]

EQUIPMENT FACT SHEET

Surveillance technology survey sheet
V1.1

EQUIPMENT IDENTIFICATION	
name	DATA ANALYSIS - Omnifind
description of equipment	Computer program searching for identifying entities
group	DATA ANALYSIS
type	Data Fusion/Data Information Management
other	
Sources	Fraunhofer

CLASSIFICATION OF FUNCTIONALITY	
Function description	mapping synonyms and different terms to the real physical entitie
hazard (bow-tie left) **(to be controlled)**	identification of relevant entities in huge databases intelligence gathering identification of entities is missing/incorrect
events (bow-tie event) **(unwanted activities)**	attackers not detected due to scattered information sources
consequence (bow-tie rigl **(of failure)**	any consequence an attack might have
bow-tie functionality	Left-hand side: intelligence gathering and control of current event after event: localisation of victims and aggressors

TECHNICAL FEATURES		
dimensions	computer program	[m/m/m]
weight	na	[Kg]
power consumption	na	[W]
control range (functional	huge databases	[m]
autonomous operation	partly: in producing alerts	[yes/no]
automated operation	yes	
system embedding	na	

OPERATIONAL FEATURES		
personnel requred	na	[%]
maintenance	na	[days/year]
ballpark cost	na	[Eur]

EQUIPMENT FACT SHEET

Surveillance technology survey sheet
V1.1

EQUIPMENT IDENTIFICATION		
name	DATA ANALYSIS - detection of money laundering HEMOLIA	
description of equipment	searching, analyzing and fusing financial data	
group	DATA ANALYSIS	
type	financial and telecom multi-agent alert and investigatic	
other		
Sources	www.hemolia.eu	

CLASSIFICATION OF FUNCTIONALITY		
Function description	detect, and dismantle criminal financing networks and financing of te	
hazard (bow-tie left) **(to be controlled)**	detect criminal/terrorist financing	
events (bow-tie event) **(unwanted activities)**	impede criminal/terrorist activity	
consequence (bow-tie right) **(of failure)**		
bow-tie functionality	money laundering prevention detection of financing of crime & terrorism	

TECHNICAL FEATURES		
	networked datasystem	
dimensions	computer program	[m/m/m]
weight	n/a	[Kg]
power consumption	n/a	[W]
control range (functional space)		[m]
autonomous operation	?	[yes/no]
automated operation	yes	
system embedding	yes	

OPERATIONAL FEATURES		
personnel requred	na	[%]
maintenance	na	[days/year]
ballpark cost	na	[Eur]

EQUIPMENT FACT SHEET

Surveillance technology survey sheet
V1.1

EQUIPMENT IDENTIFICATION	
name	DATA ANALYSIS - networked data analysis SCIIMS
description of equipment	strategic crime and immigration information management system
group	DATA ANALYSIS
type	informtaion management for combating immigration crime
other	
Sources	www.sciims.co.uk/index.html

CLASSIFICATION OF FUNCTIONALITY	
Function description	predict and analyse likely people trafficking and people smuggling sou
hazard (bow-tie left) **(to be controlled)**	detect organized crime detect individuals that perform crimes
events (bow-tie event) **(unwanted activities)**	capture suspects in the act
consequence (bow-tie right) **(of failure)**	trace victims of crime
bow-tie functionality	Primarily identification of crime and criminals (left hand

TECHNICAL FEATURES		
dimensions	computer system	[m/m/m]
weight	n/a	[Kg]
power consumption		[W]
control range (functional space)	data systems	[m]
autonomous operation		[yes/no]
automated operation		
system embedding		

OPERATIONAL FEATURES		
personnel requred	yes	[%]
maintenance	yes	[days/year]
ballpark cost	na	[Eur]

EQUIPMENT FACT SHEET

Surveillance technology survey sheet
V1.1

EQUIPMENT IDENTIFICATION		
name	DATA TRANSFER ANALYSIS - name recognition	
description of equipment	computer program identifying people according to th	
group	DATA TRANSFER ANALYSIS	
type	intelligence gathering	
other		
Sources	Fraunhofer	

CLASSIFICATION OF FUNCTIONALITY		
Function description	resolution of different transcription schemes and evaluation of pro	
hazard (bow-tie left) **(to be controlled)**	known attackers not identified	
events (bow-tie event) **(unwanted activities)**	attack by known malicious people	
consequence (bow-tie rig **(of failure)**	any consequence an attack might have	
bow-tie functionality	Left-hand side: barrier and control of current event	

TECHNICAL FEATURES		
dimensions	na	[m/m/m]
weight	na	[Kg]
power consumption	na	[W]
control range (functional	data flows through digital networks	[m]
autonomous operation	partly: in producing alerts	[yes/no]
automated operation	yes	
system embedding	na	

OPERATIONAL FEATURES		
personnel requred	na	[%]
maintenance	na	[days/year]
ballpark cost	na	[Eur]

EQUIPMENT FACT SHEET

Surveillance technology survey sheet
V1.1

EQUIPMENT IDENTIFICATION	
name	DNA - rapid dna analysis MiDAS
description of equipment	rapid millifludic DNA analysis sytsem
group	DNA
type	portable instrument
other	
Sources	http://www.forensic.gov.uk/html/company/partnersh

CLASSIFICATION OF FUNCTIONALITY	
Function description	produce DNA database compatible results from crime
hazard (bow-tie left) **(to be controlled)**	
events (bow-tie event) **(unwanted activities)**	
consequence (bow-tie right) **(of failure)**	identify DNA from crime scenes to capture offenders
bow-tie functionality	provide information about offenders from DNA found

TECHNICAL FEATURES		
dimensions	0.3 x 0.3 x 0.3 (?)	[m/m/m]
weight	na	[Kg]
power consumption	na	[W]
control range (functional space)	DNA sample	[m]
autonomous operation	no	[yes/no]
automated operation	yes	
system embedding	no	

OPERATIONAL FEATURES		
personnel requred	yes	[%]
maintenance	na	[days/year]
ballpark cost	na	[Eur]

EQUIPMENT FACT SHEET

Surveillance technology survey sheet
V1.1

EQUIPMENT IDENTIFICATION		
name	GPS - car tracker SN	
description of equipment	GPS locator	
group	GPS	
type	candy-bar size device	
other		
Sources	www.skymall.com/shopping/detail.htm?pid= 204198015&c=102002	

CLASSIFICATION OF FUNCTIONALITY		
Function description	GPS tracking device	
hazard (bow-tie left) **(to be controlled)**	track whereabouts of cars	
events (bow-tie event) **(unwanted activities)**		
consequence (bow-tie right) **(of failure)**	localisation of suspect cars after event	
bow-tie functionality	follow suspect cars	

TECHNICAL FEATURES		
	palm-size device for GPS tracking	
dimensions	palm size	[m/m/m]
weight	na	[Kg]
power consumption	na	[W]
control range (functional space)	earth surface	[m]
autonomous operation	yes	[yes/no]
automated operation	yes	
system embedding	depends on phone network	

OPERATIONAL FEATURES		
personnel requred	na	[%]
maintenance	na	[days/year]
ballpark cost	na	[Eur]

EQUIPMENT FACT SHEET

Surveillance technology survey sheet
V1.1

EQUIPMENT IDENTIFICATION	
name	IMAGE PROCESSING - crowd_and_riot
description of equipment	software module (Windows); from VGA
group	IMAGE PROCESSING
type	people tracking
other	
Sources	developed by IOSB

CLASSIFICATION OF FUNCTIONALITY	
Function description	
hazard (bow-tie left) **(to be controlled)**	identification of crowd movement that poses threat
events (bow-tie event) **(unwanted activities)**	info about events during crowd movement
consequence (bow-tie rigl **(of failure)**	regaining control
bow-tie functionality	early threat warning regaining control after intial loss of control

TECHNICAL FEATURES		
dimensions	computer program	[m/m/m]
weight	na	[Kg]
power consumption	na	[W]
control range (functional :		[m]
autonomous operation	yes	[yes/no]
automated operation	yes	
system embedding	no	

OPERATIONAL FEATURES		
personnel requred	na	[%]
maintenance	na	[days/year]
ballpark cost	na	[Eur]

EQUIPMENT FACT SHEET

Surveillance technology survey sheet
V1.1

EQUIPMENT IDENTIFICATION	
name	IMAGE PROCESSING - people counting_and_density
description of equipment	Crowd density analisis
group	IMAGE PROCESSING
type	crowd analysis/people counting
other	
Sources	developed by OSB

CLASSIFICATION OF FUNCTIONALITY	
Function description	image processing
hazard (bow-tie left) **(to be controlled)**	determinatin of crowd density determining threats and hazards from crowd density
events (bow-tie event) **(unwanted activities)**	study unwanted activites of crowds during mass ever
consequence (bow-tie rigl **(of failure)**	regain control over the crowd identifiy spots where injuries took place
bow-tie functionality	early warning, coordinate precautions event control assisting first responders after the event

TECHNICAL FEATURES		
dimensions	computer program	[m/m/m]
weight		[Kg]
power consumption		[W]
control range (functional :		[m]
autonomous operation	no	[yes/no]
automated operation	yes	
system embedding	no	

OPERATIONAL FEATURES		
personnel requred	1	[%]
maintenance	na	[days/year]
ballpark cost	na	[Eur]

EQUIPMENT FACT SHEET

Surveillance technology survey sheet
V1.1

EQUIPMENT IDENTIFICATION	
name	INFRA RED - motion detector
description of equipment	infra red motion detector
group	INFRA-RED
type	motion sensor for alarm systems
other	
Sources	www.ladyada.net/learn/sensors/pir.html

CLASSIFICATION OF FUNCTIONALITY	
Function description	detect people
hazard (bow-tie left) **(to be controlled)**	illicit entry detection
events (bow-tie event) **(unwanted activities)**	
consequence (bow-tie right) **(of failure)**	
bow-tie functionality	illicit entry

TECHNICAL FEATURES		
	infrared detector	
dimensions	0,1 x 0.05 x 0,05	[m/m/m]
weight	0,005	[Kg]
power consumption	na	[W]
control range (functional space)	room	[m]
autonomous operation	no	[yes/no]
automated operation	yes	
system embedding	possible	

OPERATIONAL FEATURES		
personnel requred	0	[%]
maintenance	na	[days/year]
ballpark cost	10 E	[Eur]

EQUIPMENT FACT SHEET

Surveillance technology survey sheet
V1.1

EQUIPMENT IDENTIFICATION	
name	MM-WAVE - whole body scanner EQO
description of equipment	Whole body scanner for security
group	MM - WAVE
type	body scanner
other	
Sources	www.smithisdetection.com/eqo.php

CLASSIFICATION OF FUNCTIONALITY	
Function description	body scan to reveal weapons
hazard (bow-tie left) **(to be controlled)**	detect illegal weapons on person detect illegal goods on person
events (bow-tie event) **(unwanted activities)**	
consequence (bow-tie right) **(of failure)**	
bow-tie functionality	detect illegal weapons before entering secure space

TECHNICAL FEATURES		
	body scanner	
dimensions	1,1 x 1 x 2	[m/m/m]
weight	na	[Kg]
power consumption	na	[W]
control range (functional space)	person	[m]
autonomous operation	yes	[yes/no]
automated operation	yes	
system embedding	possible	

OPERATIONAL FEATURES		
personnel requred	1	[%]
maintenance	na	[days/year]
ballpark cost	na	[Eur]

EQUIPMENT FACT SHEET

Surveillance technology survey sheet
V1.1

EQUIPMENT IDENTIFICATION	
name	NETWORK - AIS ship location detection and identification
number	
description of equipment	AIS VHF antenna/receiver (active System)
group	NETWORK
type	ship localisation and database
other	
Sources	http://www.imo.org/ourwork/safety/navigation/pag http://www.imo.org/OurWork/Safety/Navigation/Do http://www.profilant.net/de/maritim/44070250

CLASSIFICATION OF FUNCTIONALITY	
Function description	providing information about the whearbouts of ships
hazard (bow-tie left)	proximity detection
(to be controlled)	illegal crossing of territorial waters
events (bow-tie event)	interception of illigal shipping
(unwanted activities)	
consequence (bow-tie rig	evidence gathering of illegal shipping
(of failure)	
bow-tie functionality	identification of ships
	interceptio of illegal shipping

TECHNICAL FEATURES		
dimensions	0,1 x 0,1 x 1,35 m	[m/m/m]
weight	400 kg	[Kg]
power consumption	na	[W]
control range (functional		[m]
autonomous operation	yes	[yes/no]
automated operation	yes	
system embedding	AIS system sends only the own information to next s	
	No routing of received information	
	auto	

OPERATIONAL FEATURES		
personnel requred	na	[%]
maintenance	na	[days/year]
ballpark cost	na	[Eur]

EQUIPMENT FACT SHEET

Surveillance technology survey sheet
V1.1

EQUIPMENT IDENTIFICATION	
name	NETWORK - SIRIUS 3RK3
description of equipment	multi functional circuitry for safety and security
group	NETWORK
type	digital network system
other	
Sources	www.automation.siemens.com/mcms/industrial-con

CLASSIFICATION OF FUNCTIONALITY	
Function description	detection of intrusion & fire
hazard (bow-tie left) **(to be controlled)**	early warning of intrusion or fire
events (bow-tie event) **(unwanted activities)**	localisation of intrusion or fire during event
consequence (bow-tie rigl **(of failure)**	
bow-tie functionality	detection, alarm, activation of barriers cameras or ot

TECHNICAL FEATURES		
dimensions	s/w	[m/m/m]
weight	na	[Kg]
power consumption	na	[W]
control range (functional	na	[m]
autonomous operation	enabler for autonomous operation	[yes/no]
automated operation	enabler of autmation	
system embedding	part of modular system	

OPERATIONAL FEATURES		
personnel requred	na	[%]
maintenance	na	[days/year]
ballpark cost	na	[Eur]

EQUIPMENT FACT SHEET

Surveillance technology survey sheet
V1.1

EQUIPMENT IDENTIFICATION		
name	NETWORK - UGM 2040	
description of equipment	multi functional circuitry for safety and security	
group	NETWORK	
type	network system	
other		
Sources	www.bosch-sicherheitssysteme.de/UGM2040/	

CLASSIFICATION OF FUNCTIONALITY	
Function description	detection of intrusion & fire
hazard (bow-tie left) **(to be controlled)**	early detedtion of intrusion and fire
events (bow-tie event) **(unwanted activities)**	localisation of intrusion or fire during event
consequence (bow-tie rigl **(of failure)**	
bow-tie functionality	detection, alarm, activation of barriers cameras or ot

TECHNICAL FEATURES		
dimensions	s/w	[m/m/m]
weight	na	[Kg]
power consumption	na	[W]
control range (functional	na	[m]
autonomous operation	enabler for autonomous operation	[yes/no]
automated operation	enabler for automated operation	
system embedding	part of modular system	

OPERATIONAL FEATURES		
personnel requred	na	[%]
maintenance	na	[days/year]
ballpark cost	na	[Eur]

EQUIPMENT FACT SHEET

Surveillance technology survey sheet
V1.1

EQUIPMENT IDENTIFICATION	
name	NETWORK & INTERFACE _ AMFIS data fusion for ground control
description of equipment	heterogeneous ground control station
group	NETWORK & INTERFACE
type	ground control station fir data analysis
other	
Sources	http://www.iosb.fraunhofer.de/servlet/is/5045/

CLASSIFICATION OF FUNCTIONALITY	
Function description	Monitor data from heterogeneous sensor carriers / Control of het
hazard (bow-tie left) **(to be controlled)**	reconaissance for threat detection Status analysis of barriers
events (bow-tie event) **(unwanted activities)**	monitoring of crimes or accidents in progress attatching new statonary or mobile detectors to increase coverage
consequence (bow-tie rigl **(of failure)**	evidence gathering damage assessment
bow-tie functionality	detection/intelligence

TECHNICAL FEATURES		
	Computer system/data fusion system	
dimensions	na	[m/m/m]
weight	na	[Kg]
power consumption	na	[W]
control range (functional	na	[m]
autonomous operation	na	[yes/no]
automated operation	yes	
system embedding	na	

OPERATIONAL FEATURES		
personnel required	na	[%]
maintenance	na	[days/year]
ballpark cost	na	[Eur]

EQUIPMENT FACT SHEET

Surveillance technology survey sheet
V1.1

EQUIPMENT IDENTIFICATION	
name	Digital Situation Table
number	1
description of equipment	Interactive Visualisation of a Common Operational Pi
group	Advanced Image and geo-spatial analysis technologie
type	geodata visualisation
other	
Sources	http://spie.org/x14499.xml?ArticleID=x14499

CLASSIFICATION OF FUNCTIONALITY	
Function description	understanding data scattered in space and time
hazard (bow-tie left) **(to be controlled)**	analysis of destruction area wounded and desoriented people, major events
events (bow-tie event) **(unwanted activities)**	crowd control increase of harmed people crowd panic
consequence (bow-tie right) **(of failure)**	control crowd behaviour loss of life ineffective mission of security staff
bow-tie functionality	Stake holder organisation fully integrates INSPIRE ruled data

TECHNICAL FEATURES		
dimensions	2 x 2 x 1,3 m	[m/m/m]
weight	220 kg	[Kg]
power consumption	2500	[W]
control range (functional space)	infinite	[m]
autonomous operation	yes	[yes/no]
automated operation	no	
system embedding	can be part of modular system	

OPERATIONAL FEATURES		
personnel requred	na	[%]
maintenance	na	[days/year]
ballpark cost	na	[Eur]

EQUIPMENT FACT SHEET

Surveillance technology survey sheet
V1.1

EQUIPMENT IDENTIFICATION	
name	RADAR - Marine radar
number	
description of equipment	transceiver/Scanner/Console
group	RADAR
type	X-band (10GHz) and S-band (3GHz)
other	
Sources	http://www.riceelectronics.com/marine-radar.html http://www.km.kongsberg.com/ks/web/nokbg0240.nsf/0/FAD5EE http://www.jrc.co.jp/eng/product/marine/product/j http://www.furuno.com/en/business_product/merc

CLASSIFICATION OF FUNCTIONALITY	
Function description	acquisition and tracking of ships
hazard (bow-tie left) **(to be controlled)**	collision detection intrusion detection
events (bow-tie event) **(unwanted activities)**	direct action to stop intrusion or collision
consequence (bow-tie rig **(of failure)**	
bow-tie functionality	acquitition and tracking of illegal ships

TECHNICAL FEATURES		
dimensions	0,65 x 1,1 x 1,2 m	[m/m/m]
weight	65 kg	[Kg]
power consumption	na	[W]
control range (functional		[m]
autonomous operation	yes	[yes/no]
automated operation	yes	
system embedding	standalone/integrated	

OPERATIONAL FEATURES		
personnel requred	na	[%]
maintenance	na	[days/year]
ballpark cost	na	[Eur]

EQUIPMENT FACT SHEET

Surveillance technology survey sheet
V1.1

EQUIPMENT IDENTIFICATION	
name	RADAR - short range for intrusion detection
description of equipment	perimeter security
group	RADAR
type	intrusion detection radar
other	
Sources	http://www.smartmicro.de/index.php?option=com

CLASSIFICATION OF FUNCTIONALITY	
Function description	detection, position tracking and classification of hum
hazard (bow-tie left) **(to be controlled)**	Early identification of perimiter intrusion
events (bow-tie event) **(unwanted activities)**	localisation of intruder during event
consequence (bow-tie rig **(of failure)**	evidence of untrusion
bow-tie functionality	identification of intrusion

TECHNICAL FEATURES		
dimensions	sensor: 10 x 20 x 20	[m/m/m]
weight	na	[Kg]
power consumption	na	[W]
control range (functional	depends on environment	[m]
autonomous operation	partly, automous identification possible	[yes/no]
automated operation	yes	
system embedding	yes	

OPERATIONAL FEATURES		
personnel requred	none	[%]
maintenance	low	[days/year]
ballpark cost	low	[Eur]

EQUIPMENT FACT SHEET

Surveillance technology survey sheet
V1.1

EQUIPMENT IDENTIFICATION	
name	RADIOACTIVE - compton detector COCAE
description of equipment	radiation strength and source detection
group	RADIOACTIVE
type	detector
other	
Sources	www.cocae.eu

CLASSIFICATION OF FUNCTIONALITY	
Function description	radioactive radiation detection by compton effect in Cd(Te)Zn crys
hazard (bow-tie left) **(to be controlled)**	identification of radioactive radiation
events (bow-tie event) **(unwanted activities)**	rapid detection of radioactive radiation
consequence (bow-tie rigl **(of failure)**	
bow-tie functionality	detection of preparation actions or deployment of radioactie sources.

TECHNICAL FEATURES		
dimensions		[m/m/m]
weight		[Kg]
power consumption		[W]
control range (functional		[m]
autonomous operation		[yes/no]
automated operation		
system embedding		

OPERATIONAL FEATURES		
personnel requred	na	[%]
maintenance	na	[days/year]
ballpark cost	na	[Eur]

EQUIPMENT FACT SHEET

Surveillance technology survey sheet
V1.1

EQUIPMENT IDENTIFICATION		
name	SOUND - ECM8000 microphone	
description of equipment	audible sound microphone	
group	SOUND	
type	microphone	
other		
Sources	http://www.behringer.com/de/Products/ECM8000.aspx	

CLASSIFICATION OF FUNCTIONALITY	
Function description	acoustic sensor for shot detection and bearing
hazard (bow-tie left) **(to be controlled)**	
events (bow-tie event) **(unwanted activities)**	sniper attack threat detection via acoustic signal analysis
consequence (bow-tie right) **(of failure)**	
bow-tie functionality	event recording, prompt reaction

TECHNICAL FEATURES		
dimensions	app. 0.2/0.01/0.01	[m/m/m]
weight	0.12	[Kg]
power consumption	na	[W]
control range (functional space)	depends on environment	[m]
autonomous operation	na	[yes/no]
automated operation	na	
system embedding	na	

OPERATIONAL FEATURES		
personnel requred	na	[%]
maintenance	na	[days/year]
ballpark cost	na	[Eur]

EQUIPMENT FACT SHEET

Surveillance technology survey sheet
V1.1

EQUIPMENT IDENTIFICATION	
name	SOUND - sound processing FIREFACE400
description of equipment	FireWire Audio Interface
group	SOUND
type	processing and interpreting sound recordings
other	
Sources	www.rme-audio.de/products_fireface_400.php

CLASSIFICATION OF FUNCTIONALITY	
Function description	audio AD-DA interface
hazard (bow-tie left) **(to be controlled)**	
events (bow-tie event) **(unwanted activities)**	sniper attack threat detection via acoustic signal analysis
consequence (bow-tie right) **(of failure)**	
bow-tie functionality	event recording, prompt reaction

TECHNICAL FEATURES		
dimensions	app. 0.2/0.05/0.1 and computer program	[m/m/m]
weight	0.4	[Kg]
power consumption	na	[W]
control range (functional space)	depends on environment	[m]
autonomous operation	na	[yes/no]
automated operation	yes	
system embedding	sound system enabler	

OPERATIONAL FEATURES		
personnel requred	na	[%]
maintenance	na	[days/year]
ballpark cost	na	[Eur]

EQUIPMENT FACT SHEET

Surveillance technology survey sheet
V1.1

EQUIPMENT IDENTIFICATION	
name	SOUND - sound recording bug AU046
description of equipment	sound recorder
group	SOUND
type	mini-integrated microphone
other	
Sources	http://www.spy.th.com/audio.html#!au046

CLASSIFICATION OF FUNCTIONALITY	
Function description	sound recording
hazard (bow-tie left) **(to be controlled)**	identification of criminals identification and description of plans
events (bow-tie event) **(unwanted activities)**	
consequence (bow-tie right) **(of failure)**	evidence gathering
bow-tie functionality	evidence of crime to prevent crime evidence for conviction

TECHNICAL FEATURES		
dimensions	0,01 x 0,015 x 0,025	[m/m/m]
weight	0,001	[Kg]
power consumption	na	[W]
control range (functional space)	room	[m]
autonomous operation	no	[yes/no]
automated operation	no	
system embedding	Telephone network	

OPERATIONAL FEATURES		
personnel requred	1	[%]
maintenance	recharghe 48 hours	[days/year]
ballpark cost	300 E	[Eur]

EQUIPMENT FACT SHEET

Surveillance technology survey sheet
V1.1

EQUIPMENT IDENTIFICATION	
name	SPACE - spy sattelites
description of equipment	Earth observing sattelites based on photographs
group	SPACE
type	processing and interpreting sound recordings
other	
Sources	http://www.mscbc.msn.com/id/44568418/ns/technology_and_science-space/t/declassified-us-spy-sattelites-reveal-rare-look-cold-war-space-program/#.UDiI5UJLfcA

CLASSIFICATION OF FUNCTIONALITY	
Function description	Monitoring surface activites
hazard (bow-tie left) **(to be controlled)**	detection of training camps detection of surface conditions
events (bow-tie event) **(unwanted activities)**	
consequence (bow-tie right) **(of failure)**	
bow-tie functionality	detection of large-scale illegal activities

TECHNICAL FEATURES		
dimensions	1 x 1 x 5	[m/m/m]
weight	500-3000 kg	[Kg]
power consumption	na	[W]
control range (functional space)	earth surface	[m]
autonomous operation	yes	[yes/no]
automated operation	yes	
system embedding	ground and launch site	

OPERATIONAL FEATURES		
personnel requred	vast	[%]
maintenance	na	[days/year]
ballpark cost	na	[Eur]

EQUIPMENT FACT SHEET

Surveillance technology survey sheet
V1.1

EQUIPMENT IDENTIFICATION	
name	UAV - platform helikite balloon
description of equipment	Helium Balloon – Aerostate
group	UAV
type	sensor-carrier
other	
Sources	http://www.iosb.fraunhofer.de/servlet/is/5045/

CLASSIFICATION OF FUNCTIONALITY	
Function description	Long-time surveillance of large area
hazard (bow-tie left) **(to be controlled)**	detect critical situation in big open-air events prevent communication loss with relay functionality detect intrusion
events (bow-tie event) **(unwanted activities)**	intrusion in security areas mass panic
consequence (bow-tie rig **(of failure)**	disruption of operation loss of life loss of communication
bow-tie functionality	

TECHNICAL FEATURES		
dimensions	na	[m/m/m]
weight	5 – 8kg	[Kg]
power consumption	na	[W]
control range (functional	na	[m]
autonomous operation	No	[yes/no]
automated operation	no	
system embedding	part of modular system	

OPERATIONAL FEATURES		
personnel required	na	[%]
maintenance	na	[days/year]
ballpark cost	na	[Eur]

EQUIPMENT FACT SHEET

Surveillance technology survey sheet
V1.1

EQUIPMENT IDENTIFICATION	
name	UAV - platform micro helicpter
description of equipment	Small VTOL UAV for close range
group	UAV
type	sensorcarrier
other	
Sources	http://www.iosb.fraunhofer.de/servlet/is/5045/

CLASSIFICATION OF FUNCTIONALITY	
Function description	reconnoissance of complex / urban terrain
hazard (bow-tie left)	reconnoissance of target areas
(to be controlled)	Detect crtitical gas concentrations in the air e.g. after
	detect unwanted movement
events (bow-tie event)	ambush of tactical teams
(unwanted activities)	harm to civil population from fire gases
consequence (bow-tie rig	disruption of operation
(of failure)	loss of life
bow-tie functionality	mostly identification of threats

TECHNICAL FEATURES		
dimensions	na	[m/m/m]
weight	1.5 – 5.0 kg	[Kg]
power consumption	na	[W]
control range (functional	Approx 1 km²	[m]
autonomous operation	No (legal reasons)	[yes/no]
automated operation	yes	
system embedding	part of modular system	

OPERATIONAL FEATURES		
personnel requred	na	[%]
maintenance	na	[days/year]
ballpark cost	na	[Eur]

EQUIPMENT FACT SHEET

Surveillance technology survey sheet
V1.1

EQUIPMENT IDENTIFICATION	
name	X-RAY - luggage screening
description of equipment	single functionality luggage/parcel x-ray scanner
group	X-RAY - luggage screening
type	parcel/hand luggage
other	
Sources	http://www.smithsdetection.com/HI-SCAN_6040i.ph

CLASSIFICATION OF FUNCTIONALITY	
Function description	detection of illicit goods without opening parcels/hand luggage
hazard (bow-tie left) **(to be controlled)**	detection of illicit weapons in parcels/hand luggage detection of illicit goods in parcels/hand luggage
events (bow-tie event) **(unwanted activities)**	prevent access to weapon while processed
consequence (bow-tie rigl **(of failure)**	after the event: evidence
bow-tie functionality	primarily prevention: left hand side

TECHNICAL FEATURES		
dimensions	2 x 0,85 x 1,3 m	[m/m/m]
weight	400 kg	[Kg]
power consumption	na	[W]
control range (functional	0,62 x 0,41 m tunnel opening	[m]
autonomous operation	no	[yes/no]
automated operation	no	
system embedding	part of modular system	

OPERATIONAL FEATURES		
personnel requred	na	[%]
maintenance	na	[days/year]
ballpark cost	na	[Eur]