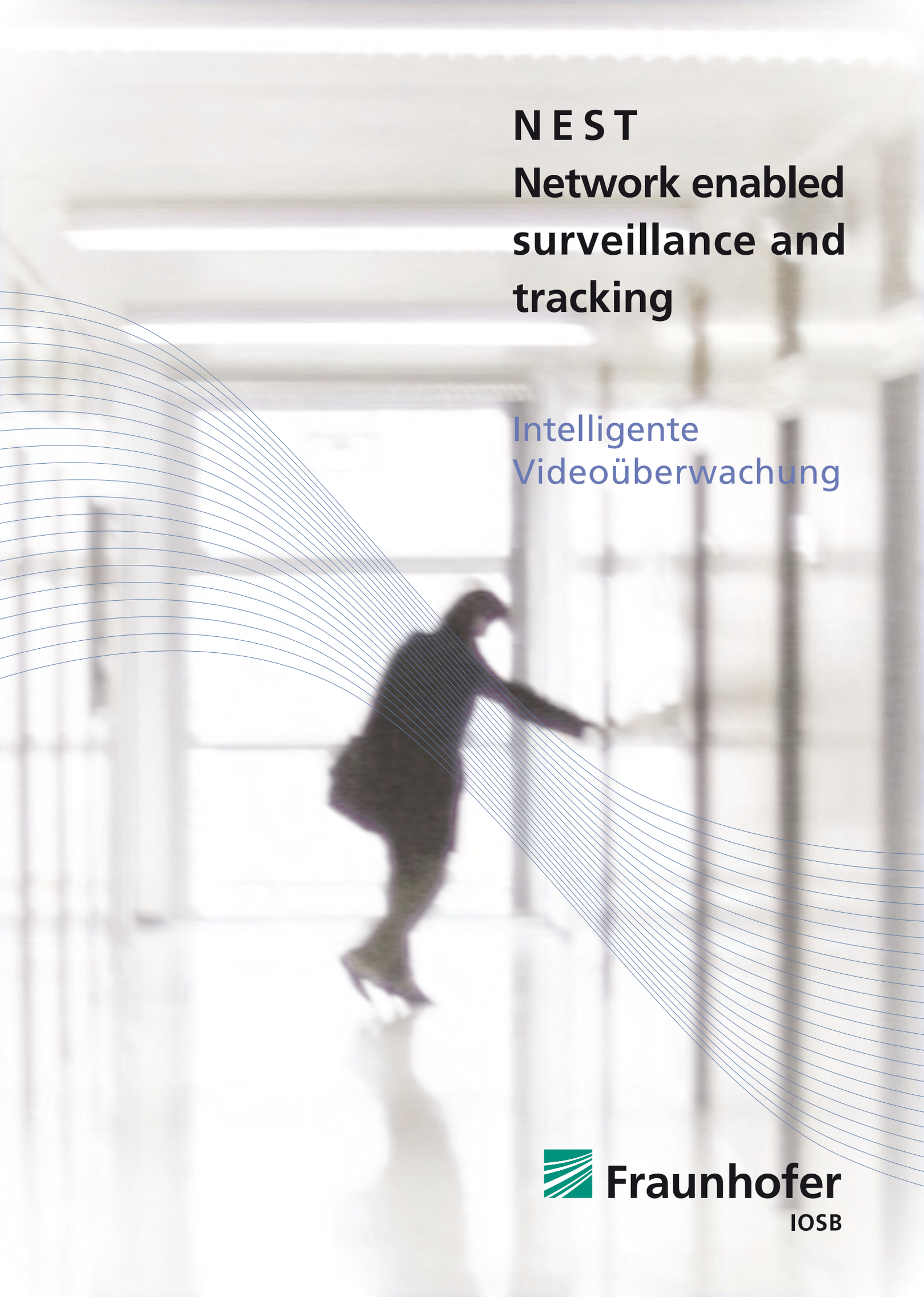


NEST
Network enabled surveillance and tracking

Intelligente Videoüberwachung

Fraunhofer
IOSB

SZENARIO I: PERSONENÜBERWACHUNG

Karlsruhe, Montagmorgen im Fraunhofer IOSB. Ein Gast betritt das Foyer des IOSB und meldet seinen Besuch bei Dr. Mustermann am Empfang. Das Sicherheitspersonal am Empfang trägt Name und Ziel des Besuchs in der NEST-Bedienersoftware ein. Dann wird der Gast gebeten, in die Kamera über der Empfangstheke zu schauen, und Sekunden später wird ein Besucherausweis mit Lichtbild ausgedruckt. Der Besucher macht sich auf den Weg zu Dr. Mustermann und das NEST-System nimmt im Hintergrund die Assistenztätigkeit auf. Ein Routenplaner berechnet automatisch die möglichen Wege vom Foyer zum Büro von Dr. Mustermann. Kameras behalten den Gast im Blick. Ein NEST-Dienst prüft zyklisch, ob der Gast sich auf dem korrekten Weg bzw. in zulässigen Bereichen des IOSB-Gebäudes aufhält, wenn nicht – und nur in diesem Fall – wird das Personal am Empfang benachrichtigt. Ist der Gast bei Dr. Mustermann angekommen, wird die Überwachungsaufgabe mit einer Meldung an das Sicherheitspersonal quittiert.

Intelligente videogestützte Sicherheits- und Monitoringsysteme finden in Forschung und Entwicklung große Aufmerksamkeit. Neue technologische Möglichkeiten, verbunden mit einer in der öffentlichen Wahrnehmung zugespitzten Gefahrenlage und der stetigen Forderung nach höherer Effizienz, lassen eine steigende Nachfrage nach innovativen Lösungen erwarten. Sowohl zur Kriminalitätsprävention in öffentlichen Räumen, zur Aufdeckung von Industriespionage in Unternehmen als auch für die Unterstützung polizeilicher Ermittlungen nach Delikten werden intelligente Videoüberwachungssysteme vermehrt zum Einsatz kommen.

Die meisten derzeit im Einsatz befindlichen Videoüberwachungssysteme haben eines gemeinsam: Die Überwachungsaufgabe wird von einem menschlichen *Operator* (z. B. Mitarbeitern eines Sicherheitsdiensts) übernommen (Abb. 1). Dieser muss eine gewisse Anzahl von Monitoren im Auge behalten und über Stunden hinweg Auffälligkeiten detektieren. Dies führt in der Regel zu einer reduzierten Effektivität. Zum einen ist die Aufmerksamkeit des Menschen über die Zeit nicht konstant und zum anderen ist durch die geringe Anzahl der Sicherheits-Mitarbeiter die Anzahl der Sensoren ebenfalls begrenzt, da ein einzelner Operator nur wenige Monitore verwalten kann.

Eine Möglichkeit diese Problematik zu umgehen, ist der Einsatz von automatischen Sensorauswertungsverfahren. Automatische Überwachungssysteme sind in der Lage, rund um die Uhr mit konstanter Leistung eine hohe Anzahl an Sensoren zu verwalten und auszuwerten.

Der menschliche Operator erhält dadurch die Möglichkeit, auf verarbeitete Daten zuzugreifen und sich somit auf höherwertige Aufgaben wie die Lageeinschätzung (Situation Awareness) zu konzentrieren (Abb. 2).

Abb. 1: Veraltetes CCTV Überwachungssystem nach dem Sensor-Monitoring-Prinzip.

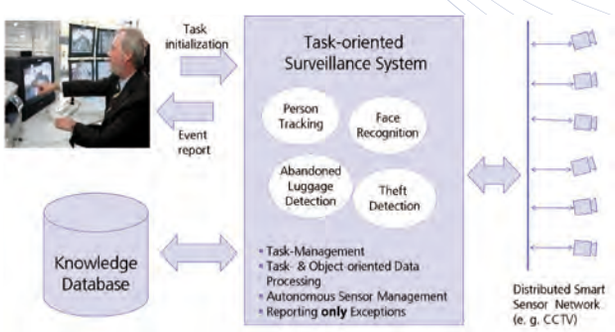


Abb. 2: Struktur eines auftragsorientierten Überwachungssystems.

Eine der meistgefragten, jedoch bisher weitgehend ungelösten, Aufgaben ist die Detektion von „verdächtigem Verhalten“ oder das sensor-übergreifende Verfolgen von verdächtigen Personen oder Fahrzeugen in großen Sensornetzwerken. Durch die komplexen und vielfältigen Umgebungsbedingungen sind hierbei extrem hohe Anforderungen an die Videoanalyse- und Sensorauswerteverfahren gegeben. Während die derzeit kommerziell zur Verfügung stehenden Videoüberwachungssysteme erste Schritte in Richtung automatischer Videoanalyse gehen, wobei primär einfache Videoauswerteverfahren auf einzelne Kameras angewendet werden, beschäftigt sich die Wissenschaft heute mit der Erforschung neuer Verfahren und Methoden zur Auswertung von Videodaten in Sensorverbünden (z. B. Kamera-Netzwerken) und der auf Sensorinformationen aufbauenden Situationsanalyse. Das Fraunhofer IOSB gehört auf diesem Feld zu den führenden Instituten.

Die kameraübergreifende Verfolgung und Wiedererkennung von bewegten Objekten (z. B. Personen) ist ein Schwerpunktthema im Forschungsprojekt NEST. Der „Person Tracking Service“ ist ein Standarddienst im System.

Im Forschungsprojekt NEST (Network Enabled Surveillance and Tracking) wurde am Fraunhofer IOSB eine generische und offene Architektur entwickelt, die sensor- und herstellerunabhängig eine Infrastruktur zur Informationsgewinnung, -aufbereitung und -analyse bereitstellt. Die Architektur ist so konzipiert, dass man durch modulare Verknüpfung von Schlüsselkomponenten das System für unterschiedlichste Systemanforderungen und Anwendungsmöglichkeiten konfigurieren kann.

NEST konzentriert sich hierbei auf die Untersuchung und exemplarische Umsetzung von drei innovativen Konzepten im Bereich von Sicherheitssystemen: Der in NEST realisierte *Plug & Protect-Ansatz,* die *auftrags-* und *aufgabenorientierte Datenauswertung* und der NEST *Modellwelt-Ansatz.*

Durch das NEST *Plug & Protect-Prinzip* soll erreicht werden, dass Sensoren (insbesondere Sensoren mit integrierter Signalauswertung, sogenannte Smart Sensors) sich nach Ankopplung im Sensornetzwerk automatisch im NEST-System authentifizieren und registrieren. Wird ein neuer Sensor als NEST kompatibel erkannt, kann dieser ab sofort von bereits in Betrieb genommenen Analysekomponenten ausgewertet werden. Die „Plug & Protect“-Fähigkeit soll dazu führen, dass die Erweiterung des Sensornetzwerkes effektiv, schnell und ohne Expertenwissen vonstatten gehen kann. Seitens der Sensorkonzeption und der Sensordatenverarbeitung fokussieren sich die Forschungsaktivitäten am IOSB auf die Entwicklung neuer Methoden zur Selbstkalibrierung, -konfiguration

SZENARIO II: FAHRZEUGÜBERWACHUNG

Flughafengelände. Ein weißer Transporter fährt zum Wareneingang des Flughafengeländes. Der Fahrer meldet sich beim Sicherheitspersonal, nennt seinen Namen und seinen Besuchszweck. Er ist von einem Handwerksbetrieb und soll im Hangar 15A Reparaturarbeiten vornehmen. Das Empfangspersonal trägt Name und Ziel des Besuchs in der NEST-Bedienersoftware ein. Dann wird dem Fahrer die Route zum Hangar 15A erklärt. Bevor der Transporter losfährt, wird in der NEST-Bedienersoftware noch das Fahrzeug markiert – der Überwachungsauftrag wird nun gestartet. Der weiße Transporter fährt ein und das NEST-System nimmt im Hintergrund die Assistenztätigkeit auf. Ein Routenplaner berechnet automatisch die möglichen Wege vom Wareneingang zum Hangar. Kameras behalten den Transporter im Blick. Sollte das Fahrzeug von der vorgeschriebenen Route abkommen, wird das Sicherheitspersonal alarmiert.

und -parametrisierung von Sensorsystemen. Die NEST-Architektur stellt hierfür die nötige Infrastruktur für die Detektion, Registrierung, Verwaltung und Steuerung von „Plug & Protect"-fähigen Sensoren zur Verfügung.

Die *auftrags- und aufgabenorientierte Datenauswertung* ist einer der wichtigsten Leitgedanken im NEST-Konzept, insbesondere bei der Sensordatenauswertung und -speicherung. Hierbei ist die Idee, nur auftrags- und / oder aufgabenrelevante Informationen von den intelligenten Sensoren anzufragen, auszuwerten, zu visualisieren oder zu archivieren. Am IOSB werden hierfür gezielt Algorithmen zur auftragsorientierten Sensor-Selektion entwickelt, mit Hilfe derer lediglich Daten von relevanten Sensoren angefordert, fusioniert und dem Bediener bereitgestellt werden. Dadurch soll das Datenaufkommen in großen Sensornetzen, aber auch die erforderliche Speicherkapazität von Archiv-Servern bezüglich der aktiven Überwachungsaufgaben optimiert werden. Weiter werden durch die auftrags- und aufgabenorientierte Auswertung keine Daten und Informationen visualisiert und archiviert, die als sicherheitsirrelevant angesehen werden, was dem „Privacy"-Aspekt zugute kommt.

Die Modellwelt

Der *Modellwelt-Ansatz* stellt ebenfalls eine Innovation im Bereich von Sicherheitssystemen dar. Eine zentrale Komponente der modularen NEST Architektur fungiert als virtuelle Informationsdrehscheibe zwischen einzelnen Auswerte- und Analysediensten. Die Informationsdrehscheibe kann sowohl als Knotenpunkt für Informationssammlung, -verdichtung und -fusion als auch als gemeinsames Gedächtnis und Wissensrepräsentation im Überwachungssystem angesehen werden (Abb. 3). Gewonnene Daten über relevante Objekte, Zustände oder Ereignisse sollen von den intelligenten Sensoren lediglich in geeigneter Form vorverarbeitet und in der *Modellwelt* abgebildet bzw. aktualisiert werden.

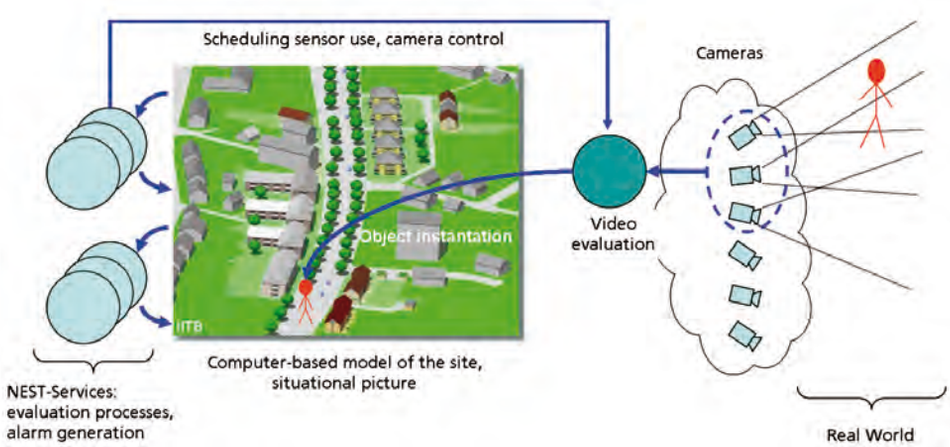


Abb. 3: Der *Modellwelt-Ansatz* dient sowohl als Entkopplung von Informationsgewinnung (rechts) und Analyse durch „NEST-Dienste" (links), als auch als Informationsdrehscheibe zwischen den auftragsorientierten Analyse-Diensten.

Unabhängig von der Daten- und Informationsgewinnung durch Sensoren greifen nun beliebige Situationsanalysedienste auf die Modellwelt zu, um eine Aussage über den aktuellen Auftragszustand zu treffen. Dadurch ergeben sich eine Reihe von Vorteilen: Zum einen sind die auftragsorientierten Instanzen von Situationsanalysediensten (z. B. Verfolgung von Personen, Diebstahlsicherung, etc.) unabhängig von den eigentlichen Informationsquellen (videobasiertes Tracking, RFID, etc.). Zum anderen wird durch diese Entkopplung vermieden, dass ein mehrfacher Bedarf an einer Information zu einer mehrfachen Rohdatenauswertung führt. Beobachtungen aus einem einzigen Sensor stehen in der Modellwelt einer Vielzahl an Analysediensten zur Verfügung.

Die NEST-Architektur

Um die Flexibilität, Generik und Erweiterbarkeit für unterschiedlichste Anwendungen zu gewährleisten, wurde als Basis eine *serviceorientierte Architektur* gewählt (SOA). Die SOA stellt ein ausreichendes Abstraktionsniveau zur Verfügung, welches für ein offenes und beliebig erweiterbares System notwendig ist.

Einzelne selbständige Dienste (Services) werden hier durch eine auftragsorientierte Steuerungsinstanz (den sogenannten „Task Execution Service“) so koordiniert, dass die Überwachungsaufgabe mit minimaler Interaktion seitens des Benutzers durchgeführt werden kann. Abb. 4 zeigt hierfür exemplarisch die benötigten Dienste zur Erfüllung der Personenverfolgungsaufgabe (siehe „Szenario I Personenüberwachung“). Die Kommunikation erfolgt über zwei logisch getrennte Busse, den „Service Control & Communication Bus“ und den „Result Bus“. Auf dem „Service Control & Communication Bus“ findet primär der Austausch von Steuerbefehlen und auftragsbezogenen Initialisierungsparametern statt.

Um dies zu realisieren wurden alle Dienste in einer einheitlichen Beschreibungssprache spezifiziert (WSDL) und über ein passendes Interface eingebunden. Die WSDL-Schnittstelle übernimmt hierbei die komplette Übersetzung vom spezifizierten Service-Befehl in proprietäre serviceinterne Kommandos. Dies ermöglicht somit auch die Einbindung beliebiger Verfahren von Drittanbietern in das NEST-System.

Der „Result Bus“, ist auf die Übermittlung hochfrequenter Daten wie Alarm-Meldungen, Positionsdaten und Beobachtungsinformationen ausgelegt. Spezifizierte Nachrichten (basierend auf dem OGC Standard) werden hierbei von Auswerte- und Analysediensten mittels JMS (Java Message Service) bandbreiteneffektiv transferiert und an anfragende Dienste (z. B. weitere Analysedienste, HMI, Archivierungsdienst, etc.) automatisch verteilt.

Zusätzlich ist ein dritter Datenkanal, der „Streaming Bus“, vorgesehen, der speziell für hochfrequente Daten mit hoher Bandbreite ausgelegt sein soll. Dies betrifft vor allem Videoströme, die in Echtzeit dem Bediener (zur Visualisierung) oder einem Archivierungsdienst (zur Videospeicherung) zur Verfügung gestellt werden müssen.

SZENARIO III – DIEBSTAHLSICHERUNG

München, Mittwochmorgen im Konferenzhotel Primus. Die Besprechungsräume sind komplett ausgebucht – sieben an der Zahl. Im Erdgeschoss ist der große Saal für eine wissenschaftliche Konferenz mit 200 Gästen belegt. Um 12:30 Uhr ist das Mittagessen für die Gäste angesetzt. Kurz davor schaltet ein Sicherheitsmitarbeiter eine der im Saal installierten Kameras auf den Bildschirm und wartet, bis der letzte Gast den Saal in Richtung Hotelrestaurant verlassen hat. Dann selektiert er mit der Computermaus alle Laptops und Taschen, die im Saal gelassen wurden, startet die automatische Diebstahlsicherung des NEST-Systems und widmet sich wieder anderen Tätigkeiten. Zehn Minuten später ertönt eine Alarmmeldung vom NEST-System. Mit nur einem Mausklick auf die Meldung wird eine Kamera vom großen Saal auf den Bildschirm geschaltet. Eine Person scheint einen Laptop einzupacken. Der Sicherheitsmitarbeiter macht sich sofort auf den Weg zum großen Saal…

Zur Infrastruktur der NEST-Architektur gehören jedoch nicht nur die Diensteschnittstellen und die logischen Datenkanäle, sondern speziell auch die auftragsorientierte Steuerungseinheit des Systems. Der „Task Execution Service" ist hierbei ein spezieller Dienst, der im System die Orchestrierung auftragsrelevanter Dienste übernimmt. Der „Task Execution Service" erzeugt für jede Überwachungsaufgabe eine neue Instanz, die einen zum Auftragstyp definierten Ablaufprozess ausführt. Die Überwachungsaufgabe wurde hierbei mit BPEL (Business Process Execution Language) als Geschäftsprozess modelliert. Beim Durchlaufen des Prozesses werden zugehörige Dienste über den „Service Bus" entsprechend gestartet, initialisiert, angefragt und freigegeben. Eine Besonderheit bei der Abarbeitung des Auftrags ist die Einbindung eines gemeinsamen Gedächtnisses (oder der Wissensrepräsentation) des Systems – die NEST- Modellwelt.

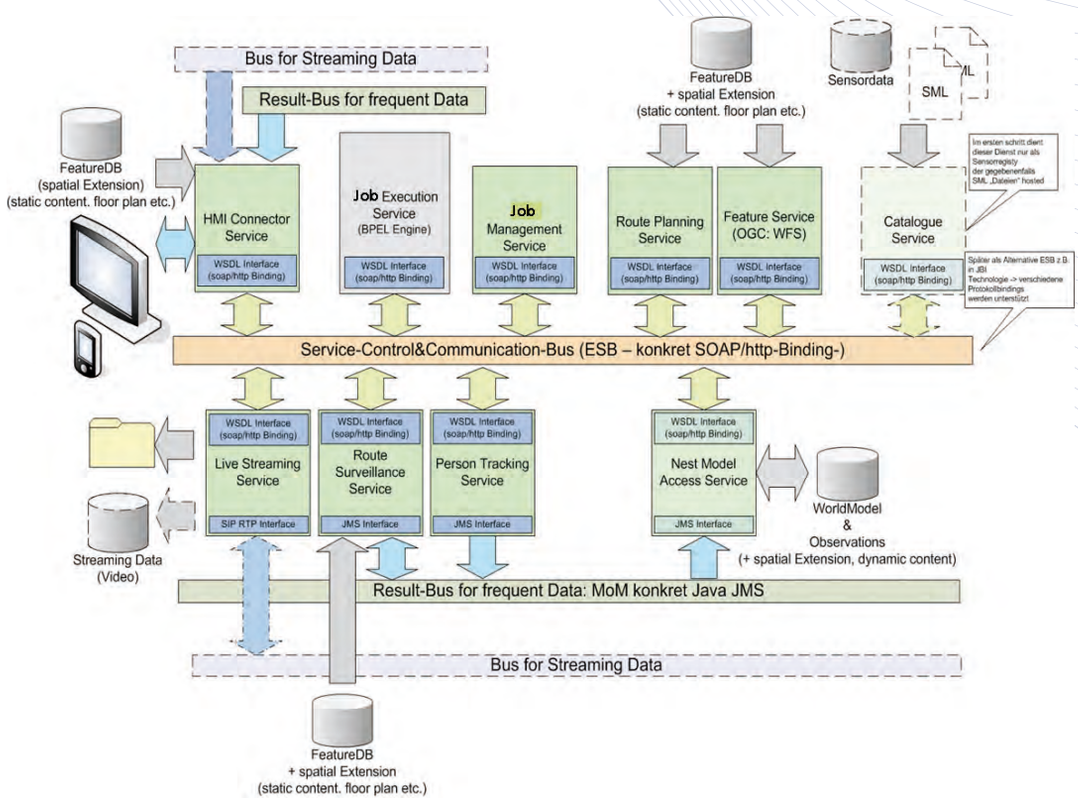


Abb. 4: Architektur des NEST-Demonstrators mit den integrierten Diensten zum Szenario „Personenüberwachung".

Alle aktivierten Überwachungsaufträge und zugehörigen Ablaufprozesse beinhalten den „Model Access Service“ als festen Bestandteil. Somit werden neue statische oder dynamische Informationen (z. B. neue Beobachtungen) über deren Abbildung in die Modellwelt auftragsübergreifend allen Diensten zur Verfügung gestellt.

Das NEST-Demonstrationssystem am IOSB

Am Fraunhofer IOSB wurde die hier vorgestellte Architektur für ein exemplarisches videobasiertes Überwachungssystem realisiert. Das verteilte Sensornetzwerk besteht aus 25 statischen und beweglichen Kameras, verteilt auf drei Etagen. Als Demonstrationsszenarien wurden drei sicherheitsrelevante Applikationen gewählt: *Sensorübergreifende Personenüberwachung, Sensorübergreifende Fahrzeugüberwachung und Interaktive Diebstahlsicherung.*

Das erste Szenario wurde bereits komplett realisiert und steht am Fraunhofer IOSB als Demonstrationssystem zur Verfügung. Alle benötigten Komponenten, von der Bedienoberfläche über die Datenverwaltung, serviceorientierter Prozesssteuerung, bis hin zu Situationsanalyse- und Videoauswertungsalgorithmen gehören zu den Kernkompetenzen des IOSB und wurden im Haus entwickelt.

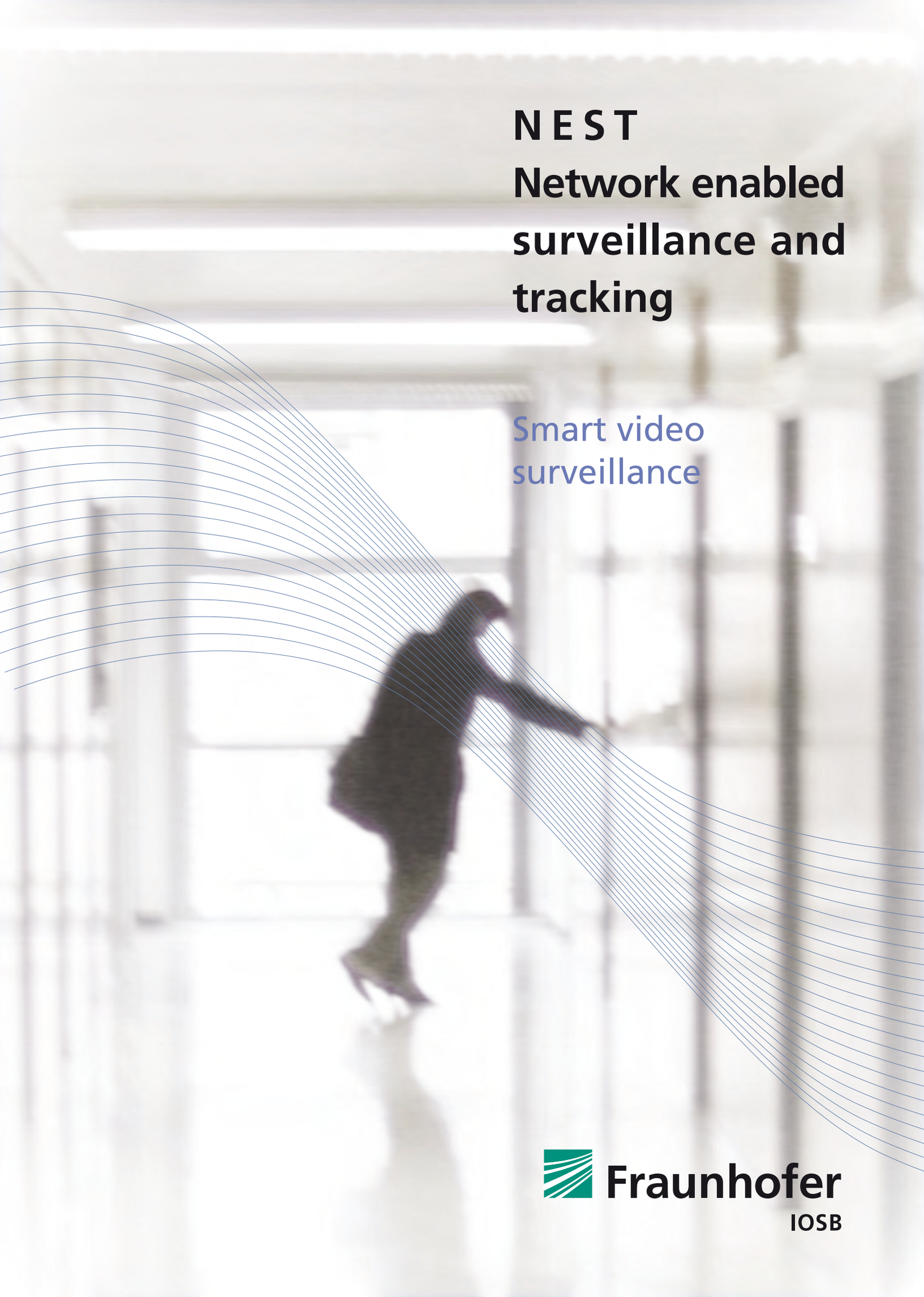
Das hier vorgestellte Konzept und die entworfene Architektur stellen einen bedeutenden Schritt in Richtung *Sicherheitssysteme der nächsten Generation* dar. Die heutige „Sensor-Monitoring“-Sichtweise wird hierbei durch eine auftragsorientierte semi-automatische Unterstützung des Sicherheitspersonals abgelöst. Der Benutzer interagiert nicht länger mit den Sensoren direkt, sondern überträgt dem System definierte Überwachungsaufgaben und lässt die Informationsgewinnung, -filterung und -fusion teilautomatisiert von NEST-Diensten durchführen.

Das hohe Automatisierungsniveau spiegelt sich in hohen Anforderungen an die Systemkomponenten: Von der Datengewinnung und -auswertung (Videoanalyse, Merkmalsextraktion) über die Situationsanalyse (Erkennung von sicherheitsrelevanten Ereignissen), den performanten Datenaustausch zwischen Diensten und die Archivierung hochfrequenter Daten, bis hin zu geeigneter Mensch-Maschine-Interaktion für optimale Aufmerksamkeitssteuerung des Sicherheitspersonals leistet NEST wichtige Beiträge an der Schwelle von aktueller Forschung zum praktischen Einsatz.

[1] J. Moßgraber, E. Monari, F. Reinert, S. Eckel, A. Bauer, T. Emter und A. Laubenheimer. N.E.S.T. – Network Enabled Surveillance and Tracking. Future Security - 3rd Security Research Conference, Karlsruhe, 2008.

[2] I. Gheta, T. Emter und J. Beyerer. Object Oriented Environment Model for Video Surveillance Systems. Future Security - 3rd Security Research Conference, Karlsruhe, 2008.

[3] E. Monari, S. Voth, K. Kroschel. An Object- and Task-Oriented Architecture for Automated Video Surveillance in Distributed Sensor Networks. 5th IEEE International Conference On Advanced Video and Signal Based Surveillance (AVSS). Santa Fe, New Mexico, USA,. 2008.



NEST
Network enabled surveillance and tracking

Smart video surveillance

Fraunhofer
IOSB

SCENARIO I: PERSON MONITORING

Karlsruhe, Monday morning in Fraunhofer IOSB. A visitor enters the foyer of the IOSB and reports to reception as a visitor to Dr. Joe Bloggs. The security employee at the reception enters the name and destination of the visitor in the NEST user software. The visitor is then asked to look into the camera above the reception desk, and seconds later a visitor pass with photograph is printed out. The visitor sets off for Dr. Bloggs' office and the NEST system begins its support activity in the background. A route planner automatically calculates the possible routes from the foyer to Dr. Bloggs' office. Cameras keep the visitor in sight. A NEST service checks periodically whether the visitor is keeping to the correct path, or to permitted areas of the IOSB building; if not – and only in this case – the staff at reception is informed. Once the visitor arrives at Dr. Bloggs' office, the monitoring task is terminated with a message to the security staff.

Intelligent video-assisted security and monitoring systems are attracting a good deal of attention in research and development. New technological opportunities, associated with a sharpened level of threat as perceived by the public and with the constant demand for higher efficiency, are raising expectations of a growing demand for innovative solutions.

Intelligent video monitoring systems are being deployed in increasingly large numbers for crime prevention in public spaces, detecting industrial espionage within businesses as well as supporting criminal investigations by the police.

Most of the video monitoring systems currently in use have one thing in common: the monitoring task is controlled by a human operator (e. g. security staff) (Fig. 1). The operator must pay attention to a certain number of monitors and detect unusual events for several hours at a stretch. This generally leads to reduced effectiveness, for two reasons. Firstly, the attention span of a human being is not constant over time, and secondly, due to the small number of security staff the number of sensors is likewise limited, since a single operator can only manage a few monitors.

One possibility of eliminating this problem is the use of automatic sensor evaluation methods. Automatic monitoring systems are capable of managing and analysing a large number of sensors while maintaining a constant level performance, round the clock. This means that the human operator is given the opportunity to access processed data and therefore to concentrate on higher-level tasks such as situation awareness (Fig. 2).

One of the most commonly encountered, but so far largely unsolved, problems is the detection of suspicious

Fig. 1: Outdated CCTV-Surveillance system using the sensor monitoring concept.

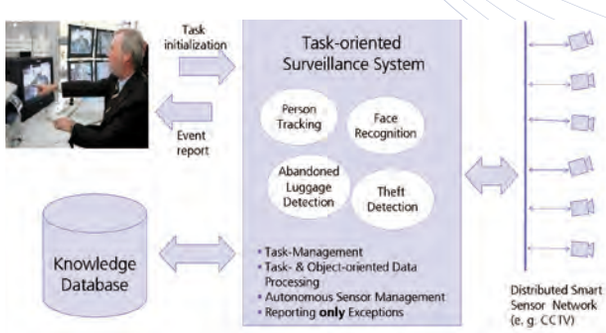
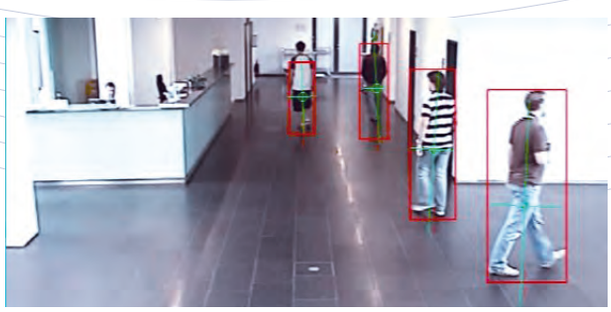


Fig. 2: Structure of a command-oriented monitoring system.

behaviour or the tracking of suspicious persons or vehicles by multiple sensors in large sensor networks. Owing to the complex and varied environment conditions associated with this task, extremely high requirements are placed on the video analysis and sensor analysis methods. While the currently commercially available video-monitoring systems are in the earliest stages of automatic video analysis, with mainly simple video analysis methods being applied to single cameras, researchers are investigating new approaches and methods for the analysis of video data in sensor arrays (e.g. camera networks), and the situational analysis based on the sensor information. Fraunhofer IOSB is one of the leading institutions working in this field.

In the research project known as NEST (Network Enabled Surveillance and Tracking) at Fraunhofer IOSB, a generic and open architecture has been developed that provides an infrastructure for the gathering, processing and analysis of information, independently of sensors and manufacturers. The architecture is designed in such a way that the target system can be configured to meet the most diverse system requirements and application possibilities by the modular interconnection of key components.



The multi-camera tracking and recognition of moving objects (e.g. people) is a central topic in the NEST research project. The "Person Tracking Service" is a standard service in the system.

NEST concentrates on the investigation and sample implementation of three innovative concepts in the field of security systems: the *Plug & Protect approach, which is realized in NEST, the job- and task-oriented data analysis and the model world approach.*

The *Plug & Protect* principle is intended to allow sensors (in particular sensors with integrated signal analysis, so-called smart sensors) to automatically authenticate and register themselves in the NEST system after connection to the sensor network. If a new sensor is detected as compatible with NEST, this can immediately be analysed by analysis components that are already in operation.

The *Plug & Protect* capability is meant to allow the sensor network to be extended effectively, rapidly and without expert knowledge. In terms of the sensor design and sensor data processing, the research activities at IOSB are focused on the development of new methods for the self-calibration, configuration and parameterisation of sensor systems. The NEST architecture provides the necessary infrastructure for the detection, registration, management and control of Plug & Protect capable sensors.

SCENARIO II: VEHICLE MONITORING

Airport terminal. A white delivery van drives up to the goods-in entrance of the airport terminal. The driver reports to the security personnel, gives his name and the purpose of his visit. He is from a building company and is assigned to undertake repair works in hangar 15A. The receptionist enters the name and destination of the visit in the NEST user software. The route to hangar 15A is explained to the driver. Before the delivery van drives off, the vehicle is first selected in the NEST user software – the monitoring command is started. The white delivery van enters the site and the NEST system begins its support activity in the background. A route-planner automatically calculates the possible routes from goods to hangar 15. Cameras keep the delivery van in sight. If the vehicle should deviate from the prescribed route, the security staff is alerted.

The *job and task-oriented data analysis* is one of the most important leading ideas in the NEST concept, in particular in the area of sensor data evaluation and storage. The idea behind this is to request and analyse only the information from the (intelligent) sensors that is relevant to the job and/or task, and then to display or archive it.

At IOSB algorithms are being specifically developed for task-oriented sensor selection, which will be used to ensure that only data from relevant sensors is requested, combined and provided to the operator. This is intended to optimise both the volume of data collected in large sensor networks, but also the required storage capacity of archive servers with respect to the active monitoring tasks. In addition, when using job and task-oriented analysis no data or information is displayed or archived that is considered irrelevant to security, which is beneficial from the privacy point of view.

The Model World

The *model world* approach also represents an innovation in the field of security systems. A central component of the modular NEST architecture functions as a virtual information hub between individual evaluation and analysis services. The information hub can be regarded as both a node point for information gathering, compression and fusion as well as a common memory and knowledge representation component within the monitoring system (Fig. 3).

Data acquired about relevant objects, conditions or events must only be pre-processed in a suitable form by the intelligent sensors, and mapped or displayed in the *model world*, as appropriate. Independently of the data and information gathering process (by sensors), any desired situation analysis services now access the *model world*, in order to provide a summary of the current state of the surveillance task.

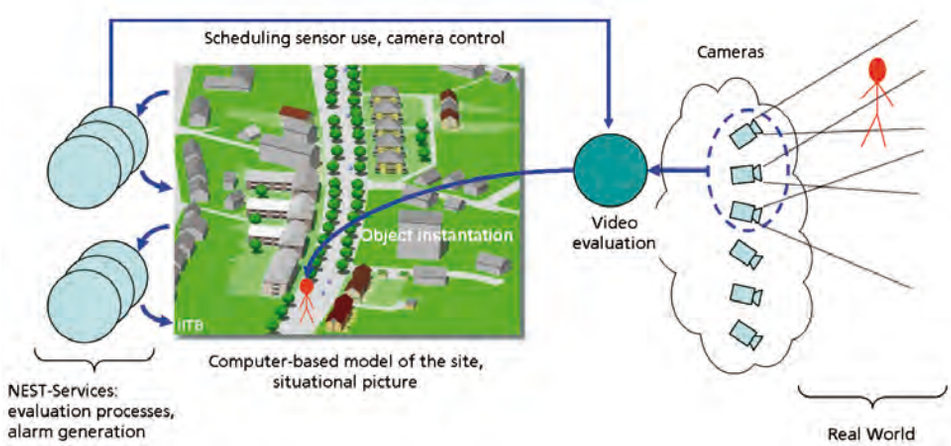


Fig. 3: The *model world* approach functions both as a means of decoupling information gathering (right) and analysis by NEST services (left), and as an information hub between the command-oriented analysis services.

This provides a range of advantages: firstly the task-oriented instances of situation analysis services (e. g. tracking of people, anti-theft protection, etc.) are independent of the actual information sources (video-based tracking, RFID, etc.). Secondly this decoupling avoids a situation in which repeated demands for a certain piece of information leads to repeated evaluation of raw data. Observations from a single sensor are at the disposal of a range of analysis services in the model world.

The NEST Architecture

In order to guarantee flexibility, genericity and extensibility for widely differing applications, a *service-oriented architecture* (SOA) was chosen as the basis of the system. The SOA provides a sufficient level of abstraction, which is necessary for an open and arbitrarily extensible system. Individual autonomous services are coordinated here by a task-oriented control instance (the so-called „Task Execution Service“) in such a way that the monitoring task can be performed with minimal interaction of the user. Fig. 4 shows an example of the necessary services for fulfilling the person tracking task (see „Scenario I - Person Monitoring“).

The communication takes place via two logically separated buses, the „Service Control & Communication Bus“ and the „Result Bus“. The type of event taking place on the „Service Control & Communication Bus“ is primarily the exchange of control commands and command-related initialisation parameters. In order to implement this, all services are specified in a uniform description language (WSDL) and linked in via a suitable interface. The WSDL interface takes control of the complete translation process from the specific service command into proprietary command-internal commands. This therefore enables any desired processes from third-party providers to be linked into the NEST system.

The „Result Bus“ is designed for transmitting high-frequency data such as alarm signals, position data (tracks) and observation information. This involves specified messages (based on the OGC standard) being transferred in a bandwidth efficient way by the evaluation and analysis services using JMS (Java Message Service) and automatically distributed to requesting services (e.g. other analysis services, HMI, archiving service, etc.).

In addition, a third data channel, the „Streaming Bus“, is provided, which is to be specially designed for high-frequency data with high bandwidth. This relates mainly to video streams which must be made available in real time to the operator (for display purposes) or to an archiving service (for video storage).

The infrastructure of the NEST architecture however not only includes the service interfaces and the logical data channels, but also specifically the task-oriented control unit of the system. The „Task Execution Service“ involved here is a special service, which is responsible for the orchestration of services relevant to performing the surveillance job in the system. The „Task Execution Service“ generates a new instance for

SCENARIO III: ANTI-THEFT PROTECTION

Munich, Wednesday morning in the Primus Conference Hotel. The meeting rooms – seven in total – are fully booked. On the ground floor the large hall is being used for a scientific conference with 200 guests. At 12:30 pm lunch is served for the guests. Shortly before this, a member of security staff links one of the cameras installed in the hall to the screen and waits until the last guest has left the hall for the hotel restaurant. Then, using the computer mouse he selects all laptops and bags that were left in the hall, starts the automatic anti-theft protection service of the NEST system and gets on with other activities. Ten minutes later an alarm signal from the NEST system sounds. With a single click on the signal, a camera from the large hall is switched through to the screen. A person seems to be putting a laptop in a bag. The security guard immediately sets off for the large hall.

each monitoring task which executes a sequential process specific to the job type. The monitoring task is modelled with BPEL (Business Process Execution Language) as a business process. During the execution of the process, associated services are started, initialised, queried and enabled via the „Service Bus“ as appropriate. A special feature of the processing of the job is the incorporation of a common memory (or knowledge representation scheme) of the system – the NEST model world. All active monitoring commands and associated sequential processes include the „Model Access Service“ as a fixed component. New static or dynamic information (e.g. new observations) are therefore made available to all services across all commands via their representation in the model world.

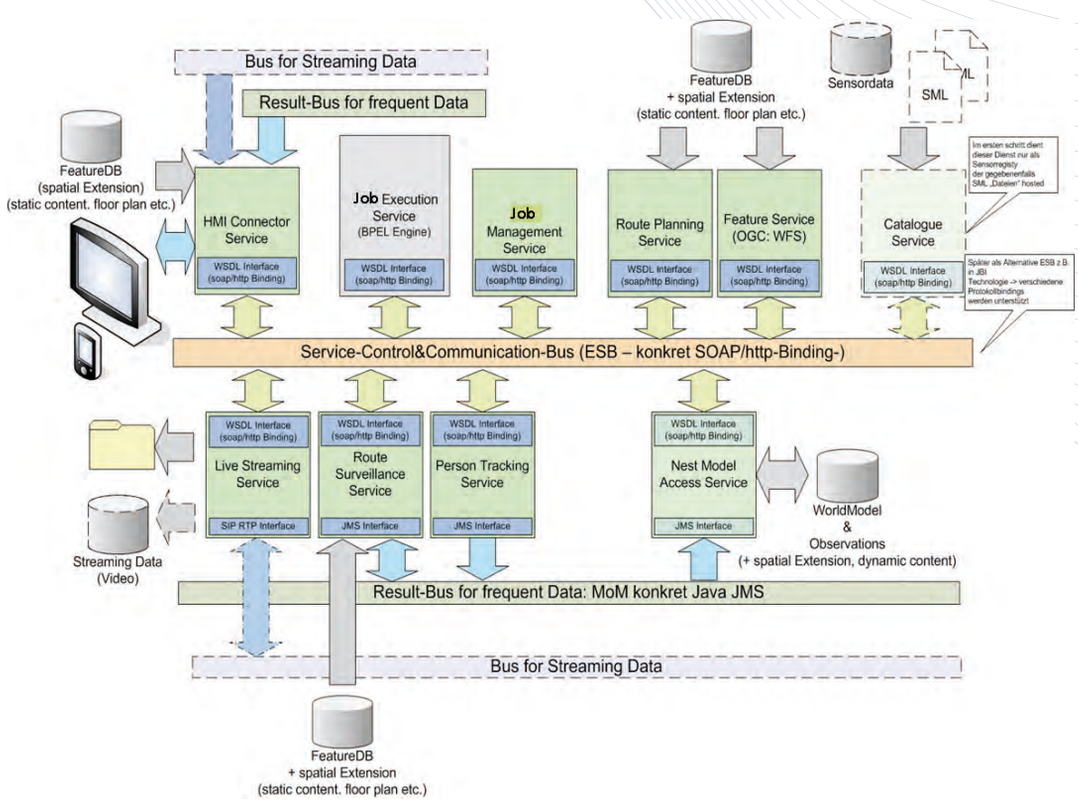


Fig. 4: Architecture of the NEST demonstrator with the integrated services used in the „Scenario I - Person Monitoring“.

The NEST Demonstration System at IOSB

At Fraunhofer IOSB the architecture presented here has been implemented as an example of a video-based monitoring system. The distributed sensor network consists of 25 static and mobile cameras, distributed over three floors of the IOSB. Three security-related applications were chosen as demonstration scenarios: *Multi-sensor person monitoring, multi-sensor vehicle monitoring and interactive anti-theft protection.*

The first scenario has already been fully implemented and is available as a demonstration system at Fraunhofer IOSB. All the necessary components, from the operator interface via data management, service-oriented process control, right up to the algorithms for situation analysis and video evaluation, form part of the core expertise of IOSB and have been developed in-house.

The concept and the architectural design presented here represent an important step towards *next generation security systems*. The „sensor-monitoring" concept used today is thus superseded by a system of job-oriented semi-automatic support for the security personnel.

The user no longer interacts directly with the sensors, but rather hands over specific monitoring tasks to the system, allowing the information gathering, filtering and fusion processes to be carried out in a partly automated way by NEST services. The high level of automation is reflected in high requirements on the system components. From data gathering and evaluation (video analysis, feature extraction), through situation analysis (detection of security-related events), the high-performance data transfer between services and the archiving of high-frequency data, right up to suitable man-machine interaction for optimal attention guidance for the security personnel, NEST makes important contributions to the practical use of technology at the forefront of current research.

[1] J. Moßgraber, E. Monari, F. Reinert, S. Eckel, A. Bauer, T. Emter und A. Laubenheimer. NEST – Network Enabled Surveillance and Tracking. Future Security - 3rd Security Research Conference, Karlsruhe, 2008.

[2] I. Gheta, T. Emter und J. Beyerer. Object Oriented Environment Model for Video Surveillance Systems. Future Security - 3rd Security Research Conference, Karlsruhe, 2008.

[3] E. Monari, S. Voth, K. Kroschel. An Object- and Task-Oriented Architecture for Automated Video Surveillance in Distributed Sensor Networks. 5th IEEE International Conference On Advanced Video and Signal Based Surveillance (AVSS). Santa Fe, New Mexico, USA, 2008.

Fraunhofer-Institut für Optronik,
Systemtechnik und Bildauswertung IOSB
Fraunhofer Institute of Optronics,
System Technologies and Image Exploitation IOSB
Standort Karlsruhe
Fraunhoferstraße 1
76131 Karlsruhe
Telefon / Phone +49 721 6091-0
Fax +49 721 6091-413
www.iosb.fraunhofer.de
info@iosb.fraunhofer.de

Your contacts:
Dr. Andreas Meissner
Leiter Geschäftsfeldentwicklung
Zivile Sicherheit
Civil Security
Telefon / Phone +49 721 6091-402
Fax +49 721 6091-413
andreas.meissner@iosb.fraunhofer.de

M. Eng. Eduardo Monari
Autonome Systeme und
Maschinensehen
Autonomous Systems and Machine Vision
Telefon / Phone +49 721 6091-583
Fax +49 721 6091-233
eduardo.monari@iosb.fraunhofer.de

Editorial notes:
Text Eduardo Monari
Layout Sibylle Wirth
English Edition
SciTech Communications GmbH
Heidelberg

Printing MeinDruckportal.de

Photo acknowledgments
page 5
invisiblekilla / pixelio.de
Sturm / pixelio.de
page 16 pixelio.de
Fraunhofer IOSB

Fraunhofer
IOSB