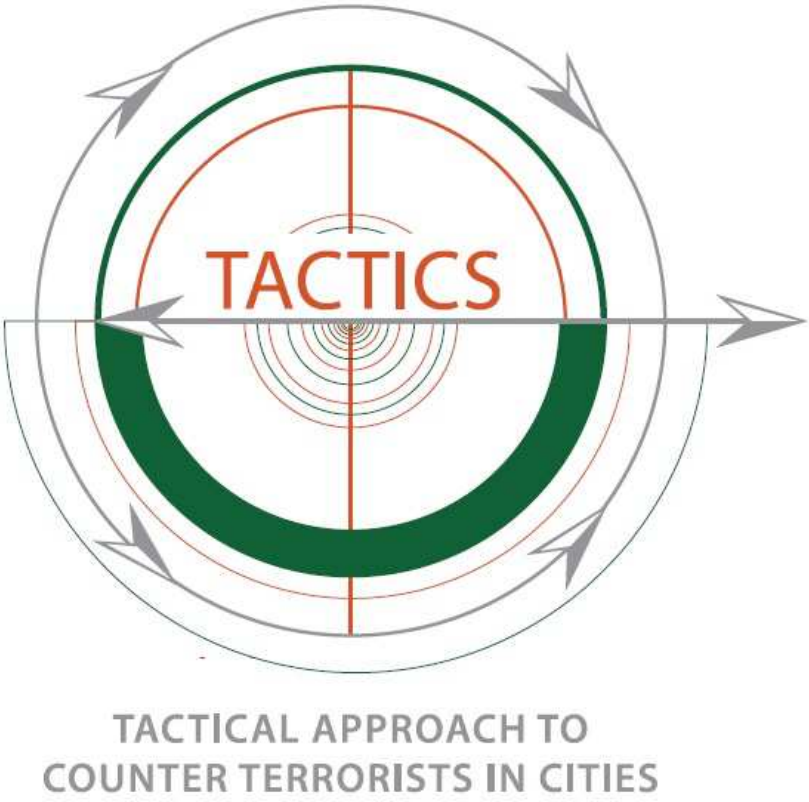
SEVENTH FRAMEWORK PROGRAMME

Collaborative project
Small or medium-scale focused research project
FP7-SEC-2011-1
Grant Agreement no. 285533



TACTICS

Tactical Approach to Counter Terrorists in Cities

Deliverable details	
Deliverable number	D3.2
Title	System Architecture
Author(s)	TNO, UPV, RAND, ITTI, Fraunhofer
Due date	31-03-2013
Delivered date	28-03-2013 (update 11-12-2013)
Dissemination level	Public
Contact person EC	PO

Cooperative Partners	
1.	ITTI Sp. z o.o.
2.	Nederlandse Organisatie voor toegepast natuur-wetenschappelijk onderzoek TNO
3.	Peace Research Institute Oslo
4.	Rand Europe
5	Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
6	Universidad Politécnica de Valencia (UPVLC)
7	Fraunhofer Gesellschaft zur Förderung der angewandten Forschung e.V.
8	Koninklijke Marechaussee
9	Morpho

Table of Contents

Executive Summary

The purpose of this report D3.2 is:

- To present a system design of the TACTICS validation system in order to guide the development of that validation system in the TACTICS project.

The purpose of the TACTICS validation system is to assist in validating key components of the TACTICS research project, which focuses on managing a terrorist threat in an urban environment.

D3.1 describes the generic architecture of a hypothetical future TACTICS type of system. Such a hypothetical system will not be built in the TACTICS project.

Problem

Over the years the threat of terrorism in European urban environments has become an important issue, first because of campaigns of organisations like IRA and ETA, and more recently by several successfully carried out terrorist attacks by Islamic terrorist groups (New York, Madrid, London) and “lone wolves” (Oslo, Boston). Also failed attempts reported in the global media have served to keep the perception of a terrorist threat alive, such as the failed attempt by the ‘underwear bomber’ Umar Farouk.

Terrorists focus on different types of locations, many of them typically in an urban environment. Examples are the attacks in Mumbai in 2008 - where a hotel, hospital, a movie theatre, a café and other locations were hit - or the initial bombing in Oslo by Breivik. Urban environments are characterized by higher population density and vast metropolitan features as compared to their surrounding areas. Urban areas may be cities, towns or urban agglomerations. These areas are very “attractive” to terrorists since attacking them has a strong impact: high numbers of victims, high emotional and in some cases cultural value. If the Eiffel Tower would be attacked successfully, it would probably result in many victims, but it would also strike many French citizens, and Europeans, in their hearts.

When a specific threat or an actual terrorist attack occurs, security forces must answer several questions. These questions are relevant to any kind of threat, but are even more difficult to answer when dealing with urban environments:

- What are the signs of an impending attack?
- How can these signs be detected by humans or technological tools?
- How can the detected signs be fully understood?
- What actions do the signs imply?
- How to know what capabilities are at security forces’ disposal that can be used to prevent or react to an attack?
- How to decide upon the right actions in case of an actual attack?

Security forces have difficulties in answering these questions for two major reasons. First of all, most security forces in Europe do not have sufficient experience with regard to specific terrorist behaviour. Without sufficient knowledge on this behaviour it is impossible to know what the signs of an impending attack are in an urban location, how the signs can be recognised by humans or technological tools, how they can be understood and what actions the signs imply. Secondly, security forces cannot assess quickly enough what capabilities are at their disposal and what other capabilities might be necessary to deal with a specific threat or terrorist attack. They will have to be able to make this assessment quickly to decide upon the right actions, not only to prevent a terrorist attack but also to minimise the impact in terms of casualties, injuries, shock, fear and damages.

The problem of determining and detecting of terrorist behaviour can be decomposed into a set of smaller problems. We separate three aspects of this problem:

1. How can we better understand a terrorist threat? (speed, cost, quality of prediction)
2. How can we better detect precursors?
3. How can we better support decisions, while avoiding biases?

The TACTICS project goals are:

1. to make security forces capable of responding quicker, without being biased in decision making and to be more precise in the kind of information they request and the orders they send out by providing expert knowledge at the fingertips of the professionals of the security services at the time of an actual threat in urban environments (threat management);
2. to improve preparedness of security forces by decomposing threats into observable terrorist behaviours specific for urban environments (threat decomposition);
3. to improve the capabilities at security forces' disposal by improving their management, efficiency and their cooperation in urban environments (capability management);
4. to facilitate a cross-European approach by offering a 3-levelled strategy on the tactical, operational and strategic level.

Design Principles

In deliverable D3.1, considerations are given for design principles that should be used when developing a TACTICS system:

- Design process
- User centred design
- Privace-by-design

The choice for design process is mostly guided by earlier choices in defining the project, and by the fact that a future operational implementation of a TACTICS system will require a complete redesign. The purpose of this design is to validate several key design patterns. The Waterfall process is therefore suitable for the TACTICS project, and the main components of that process map directly on TACTICS work packages.

Gulliksen et al [13] have described twelve principles of user-centred design. Within the TACTICS project, we apply most of them, as discussed in section 3.3. For example, user focus is obtained by putting three users as central main actors in the design. End users are active members in the project.

The seven foundational principles of Privacy-by-design are addressed (see section 3.4). Important issues involving the use of the system during validation will be met, by only observing subjects that gave their consent, and not storing personal data longer than useful in the project, and not exceeding the duration of the project. Validation of the TACTICS project is further described in report D7.1.

System architecture description

The system architecture of the TATICS system described in this report is based on the conceptual design of a generic TACTICS system as described in report D3.1. Figure 1.1 shows a view of the system, showing the three main users (managers), three tools with which the users interact, and external information resources.

The system is further described, by describing the main actors, the use cases of these actors with the tools, the functional description of the tools and the definition of interfaces, including human-machine-interfaces, where the users interact with the tools.

Main actors

TACTICS introduces three roles: the Threat Manager (TM), the Threat Decomposition Manager (TDM) and the Capabilities Manager (CM). They work as a team to prevent or mitigate terrorist attacks during the development of a threat:

- The TM is responsible for making decisions based on the complete operational picture;
- The TDM is responsible for providing knowledge on terrorism, terrorist groups and modus operandi;
- The CM is responsible for providing knowledge on the current capabilities that security forces have at their disposal at the threat locations(s).

One final roll is that of information resource, which can for example be a sensor providing data, an officer on the street providing observations, or a combination of a sensor and an operator providing observations.

Use cases

For each user interacting with the corresponding tool, use cases are described. The TM, with as general use case managing of the threat, for example should be able to view information, be able to select reources based on information exchanged with Capabality Management, and obtain information from Threat

Decomposition based on provided information about the threat. The TDM interacts with the Threat Decomposition tool to assist in finding relevant threat indicators. The CM uses the Capability Management tool to enable it to provide the TM with possible resources to observe those indicators. Uses cases are provided in more detail in section 4.3.

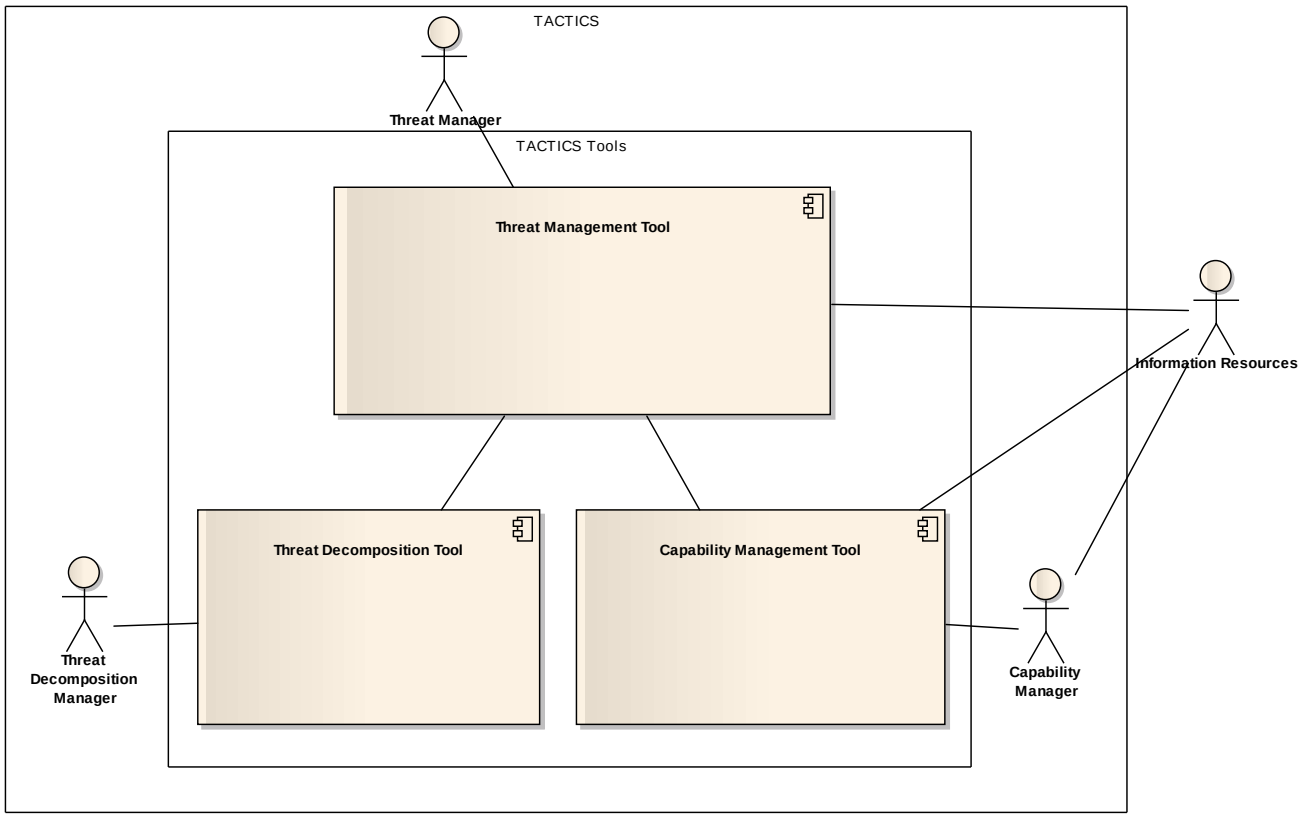


Figure 1.1 System view with main actors and three sub-components

Functional descriptions

The purpose of the Threat Decomposition process is to improve preparedness of security forces by decomposing threats into observable terrorist behaviours specific for urban environments. Expert and historic information about terrorist attacks relevant for the scenario for which the system will be validated, will be structured and stored in a database. The *Threat Decomposition Tool* allows obtaining indicators of a threat from this database, based on known indicators, and assists in communicating this information back to Threat Management.

The purpose of the Capability Management (CM) is to improve the knowledge on the available capabilities at security forces' disposal by improving (1) awareness about the general availability of capabilities most appropriate in a given situation, (2) access to capabilities, and (3) management of capabilities. The *Capability Management Tool* helps the Capability Manager to keep track of capabilities, and match them to required information needs of Threat Management.

The purpose of the Threat Management process is to make security forces capable of responding quicker, without being biased in decision making and to be more precise in the kind of information they request and the orders they send out by providing expert knowledge at the fingertips of the professionals of the security services at the time of an actual threat in urban environments.The Threat Management Tool assists in this process, by providing obtained information in a more useful way, and enabling clearer interaction with Threat Decomposition and Capability management.

Interfaces between the tools are defined to enable further development of the tools within the different workpackages. Human-Machine-Interfaces for the different tools are described, including general guide lines, such as simplicity of use.

1 Introduction

The FP7 research project TACTICS is concerned with improving terrorist threat mitigation in an urban environment. These are the project goals:

1. to make security forces capable of responding quicker, without being biased in decision making and to be more precise in the kind of information they request and the orders they send out by providing expert knowledge at the fingertips of the professionals of the security services at the time of an actual threat in urban environments;
2. to improve preparedness of security forces by decomposing threats into observable terrorist behaviours specific for urban environments;
3. to improve the capabilities at security forces' disposal by improving their management, efficiency and their cooperation in urban environments;
4. to facilitate a cross-European approach by offering a 3-levelled strategy on the tactical, operational and strategic level.

After this project, the knowledge built is available for future initiatives[1]. The challenges involved in mitigating a terrorist threat in an urban environment are described in deliverable D2.1 [1]. In report D3.1 [7] (addressing goals 1-3) a conceptual solution description is given, presenting an integral yet generic approach to a managing a terrorist threat in an urban environment.

TACTICS is an FP7 Specific Targeted Research Project (STReP)[2] [11] of which key aspects have been selected to be validated in a simulated laboratory environment (TRL 5 [3]). This report D3.2 will focus on that approach. This document describes the design of such a system, describing functional parts and interfaces, in order to allow further development of its components during the project. As such, it describes functionality in enough detail to make sure all needed functionality is divided over the components, and making interfaces clear, but leaving implementation decisions to corresponding work packages where possible.

The TACTICS validation system is a loosely coupled collection of three tools. The integration is kept as light as possible to reflect the relative high level of autonomy and the diversity of the respective three managers and their tasks. Aspects which concern all three tools are covered in this document. The implementation of the integration is done iteratively, and starts as early as possible in WP4-6.

The "TACTICS system" has a double meaning:

(1) a hypothetical class of operational systems which in some way or form resemble the TACTICS approach to mitigating terrorist threats in an urban environment. (Focus of D3.1)
(2) the concrete result of the TACTICS project; (Focus of D3.2)

In this report we use the term "TACTICS system" in the second meaning, i.e. as the concrete result of the TACTICS project.This implemented system will assist in the validation of specific hypotheses at a later stage in the project, therefore another name for this system is "the validation system".

Section 2 describes the terminology used in D3.1 and D3.2. In section 3, TACTICS system design principles are discussed. In section 4, the system architecture is giving, including a description of the system and its context, actors and use cases. The system design in section 5 and interface definitions in section 6 provide the functional descriptions needed for further development and implementation of the system towards its final validation. Although part of the systems functionality may be performed by humans, an important part of the system will be tools in software. In section 7, the human-machine-interfaces for these tools are described. Section 8 describes the origins of information flows during the validation of the TACTICS system.

---

[1] Goal 4 –the 3-levelled strategy- will be described in project deliverables D8.1 and D8.2

[2] STRePs are multipartner research, demonstration or innovation projects. Their purpose is to support activities of a more limited scope and ambition than Integration Projects.

[3] Technology maturity is the degree to which a technology has been proven in a realistic operational setting [20]. TRL 5 means that fidelity breadboard technology increases significantly. The basic technological components are integrated with reasonably realistic supporting elements so they can be tested in a simulated environment. Examples include "high-fidelity" laboratory integration of components.

D3.1 and D3.2 are design documents of similar systems which mainly differ in their maturity level, so they cover roughly the same topics. However, they should be readable as stand-alone documents, so they contain several very similar or even identical segments. This introduces the risk of inconsistency between D3.1 and D3.2.

1.1 The risks of using system engineering in a research project

Using a system engineering approach for a scientific project has risks in the perception of the scientific work. For example, the software built during the project can be seen as (a preliminary version of) an operational system. Allthough this is strictly not one of the goals of the TACTICS project, TACTICS does work on dessimination and exploitation of the results. It must be noted however that the EC is not the organisation to commission the building of such a system (for a TACTICS system this would probably be a police or defense force), nor is the FP7 research framework suitable as an ICT procurement tool.

In fact, the consortium has been formed in order to achieve and validate scientific progress. In the opinion of the consortium the progress in this topic is in e.g.:

- Design methodologies (e.g. privacy by design applied to system of systems);
- Definitions of deviant behaviour and corresponding methodologies;
- Use cases for emerging technologies in the TACTICS context (face recognition and behaviour analytics);
- Work processes for counter terrorism (TM, CM and TDM);
- Prevention of biases;

The progress is not in (the development of) ICT, which can be done by regular software developers.

Another potential risk is the perception that all formulated requirements are requirements for a concrete system which is being built. Some of the requirements (D2.2 and D3.1) are intended for a hypothetical TACTICS class of systems. Other requirements (D3.2, D4.4, D5.5 and D6.4) are intended for the TACTICS Validation System. In fact, work package 7 – validation will probably generate new requirements and / or alter existing requirements for the hypothetical class of TACTICS systems.

2 Terminology

Shared understanding of relevant terminology is a precondition to fruitful research and design. In the domains of police, surveillance and system engineering there are several concepts which are notoriously difficult to define. The aim of this chapter is to give the definitions which are used in D3.1 and D3.2. The definitions that were used in section 1 are included here too.

Term	Definition
Behaviour	The reaction of a cognitive agent to a stimulus, expressed in elements of his environment.
Behaviour profiling	The extrapolation of information about a cognitive agent, based on its behaviour.
Bias	Bias is a systematic flaw in judgment, caused by a distorted image of reality. Biases are common to all humans and can pertain to attention, information processing, attribution, categorization of groups, patterns, and contextual factors such as fatigue and noise. Prevalent examples of cognitive biases are the confirmation bias, which is the tendency to seek information that corresponds with pre-existing ideas or to interpret information in such a way that it verifies pre-existing ideas [18], and stereotypering, which involves describing a person in terms of (often negative) characteristics of the group this person belongs to [8]. For an overview of cognitive biases see Baron [1].
Capability	An ability that an organization, person, or system possesses. Capabilities are typically expressed in general and high-level terms and typically require a combination of organization, people, processes, and technology (i.e. *resources*) to achieve [23]. This would be for TACTICS something like “Person Identification”, “Object Observation”, or “Area Surveillance”. In TACTICS, external (additional) cooperative capabilities are not enabled by default: based on their effectiveness against an actual threat, they may be temporarily dynamically linked to the TACTICS system, and removed again when the threat is gone.
Cognition	The ability to solve problems.
Context	The context of a surveillance system consists of the factors that influence the system and necessarily includes the environment, including people in the environment. Typical examples of surveillance context are the local culture, the level of terror threat, and the weather conditions. Additionally, world knowledge as prior probability, and known correlations between events and actions, are also a part of a surveillance system’s context.
Decision Support System	An information system that supports business or organizational decision-making activities. A TACTICS system is a decision support system for counter-terrorism purposes.
Design pattern	A design pattern is an abstraction of a design, in the sense that it is not concerned with implementation details. A *surveillance (design) pattern* is a design construct which is considered ‘good practice’ in certain application areas of surveillance. There are several surveillance patterns with similar purposes: to create situational awareness. Their structure is therefore also similar: input is raw data (video, sound, tweets, etc.), the output is a hit (alarm) or a no-hit. All require a suitable physical infrastructure and information about the context in which they are applied. Several design patterns are already prevalent in the surveillance domain –which is why we call them surveillance patterns- such as threshold alarm, behaviour profiling and concentric circles of protection. Other surveillance patterns are still emerging. Since these surveillance

	patterns are only concerned with structuring and analysing data, they can be applied by both machine and human. However, a human professional can shift seamlessly between these patterns, while machines must be explicitly designed to apply them. In both cases, the underlying information structure has its own strengths and weaknesses. Therefore, there is no perfect surveillance pattern: each pattern has to fit requirements such as efficiency, efficacy and lack of invasiveness, all of which depend on the local situation.
Deviant behaviour	(1) A reaction which does not fit to the stimulus if the intent were benign. (2) Behaviour which is not part of any of the regular processes which occur at the respective location. (3) Socially abnormal behaviour (4) Behaviour which falls outside the normal distribution of behaviour at the respective location. (5) Behaviour which is part of the modus operandi of a criminal act. (6) Behaviour which may lead to a dangerous situation. (7) Behaviour which "leaks" because the cognitive load is high when a person attempts to hide an intention.
Environment	The environment of a system is the system's surrounding that could interact with the system. The typical environment for a surveillance system is the area under surveillance including the people under surveillance and the location(s) of the system components (including storage, data transport, monitoring room etc.).
Information Fusion	Information fusion is the merging of information from disparate sources with differing conceptual, contextual and typographical representations. There are many definitions [24] and several related concepts: **Data fusion** is the merging of data representing the same real world object. **Sensor fusion** is the combining of sensory data or data derived from sensory data from disparate sources such that the resulting information is in some sense better than would be possible when these sources were used individually. The purpose of fusion is typically to have a more accurate, more complete, or more dependable result, or refer to the result of an emerging view.
Invasiveness / intrusiveness	There is no common definition of the invasiveness of a surveillance capability. This frustrates answering questions such as "how invasive is a particular surveillance capability?", or "which is the least invasive manner of detecting a specific modus operandi?" TACTICS uses a mix of two aspects of invasiveness: the degree of autonomy which is taken from the data subject, and the level of detail of data which is observed on the data subject. Both are subjective measures. In concrete capabilities these two aspects are typically correlated: the more detailed aspect is observed, the more cooperation you need from the data subject. Technological advances allow for observing more detail at a lower level of cooperation.
Privacy	The definition of privacy –in relation to data protection- is not settled. Privacy is the ability to control and limit physical, social, psychological and informational access to the self or one's group [14]. Gutwirth writes that privacy is the safeguard of personal freedom--the safeguard of the individual's freedom to decide who she or he is, what she or he does, and who knows about it [22]. Langheinrich gives a short history of the concept of privacy by design [15], and illustrates as part of that history the origination of five specific categories of privacy that together appear to encapsulate all previous definitions: • Privacy of personal behaviour (media privacy); • Privacy of territory (territorial privacy); • Privacy of the person (bodily privacy); • Privacy of personal communications (interception privacy), and • Privacy of personal data (data or information privacy).
Privacy by Design (Data protection by	The principle of 'Privacy by Design' means that privacy and data protection are embedded throughout the entire life cycle of technologies, from the early design

design)	stage to their deployment, use and ultimate disposal [10].
Privacy invading activities	Activities that potentially interfere with one's privacy [3].
Profiling	The extrapolation of information about something, based on known qualities. It leads to the identification of patterns in data of the past which can develop into probabilistic knowledge about individuals, groups of humans and non-humans in the present and in the future [22]. In the security domain, profiling means determining information about a (potential) (group of) offender(s), based on other information about the offender. Predictive profiling does this before a crime has happened. Offender profiling does this after the crime has happened, when forensic tools and methods are involved then offender profiling becomes forensic profiling. A lesser used classification is to use the type of crime as label, e.g. cyber-crime profiling. A classification which is more often used, is by type of information which is used as input (ethic or behavioural profiling) or as output (geographic profiling). TACTICS focusses on predictive behavioural profiling against terrorist attacks. Rubinstein et al give seven elements of a generally accepted framework for government data mining [21].
Resource	A physical asset, an organizational resource or a functional resource that can contribute towards fulfilling a capability. Within TACTICS this could be a type of sensor (including a human) or a database which potentially provides data and/or information to a TACTICS system, and would be combined to create *capabilities*. Examples of resources in the context of TACTICS are CCTV cameras, police officers, permit databases and private security personnel.
Scope creep	The unmanaged change of system purpose. TACTICS aims to prevent scope creep by supporting the use of the proper procedures and legislation. Re-using systems –and effectively changing their purpose(s)- generates chances for efficiency and speed. This is one of the main starting points for the TACTICS concept.
Sensor	A device which converts one energy to another, usually an electric signal, e.g. microphone, CCTV camera, pressure sensor and also the human eye. There are several closely related concepts: An active sensor sends a signal which is reflected by the subject, and/or which triggers a response from the subject, e.g. radar, sonar and lidar. An intelligent sensor applies some form of knowledge to either improve the output signal or to interpret the signal to a higher level of abstraction, e.g. a face recognition system, video content analysis and also a human. A probing sensor is a sensor with a probing mechanism with the function of bringing a stimulus to the observed subject. The response to the stimulus is measured by the sensor. Human surveillance professionals do this e.g. in Search Detect React ® [12].
Surveillance	The focused, systematic and routine attention to personal details for purpose of influence, management, protection or direction [16].
System	A construct or collection of different elements that together produce results not obtainable by the elements alone [23]. Within TACTICS the term system is a hybrid collection of machine and human components, i.e. a socio-technical system.
System of systems	The system-of-systems is composed of cooperative systems which are independent, useful and used in their own right [17]. From the point of view of managerial control, a TACTICS system-of-systems is a group of cooperative systems in that the central management organization does not have coercive power to run the system. The component systems must, more or less, voluntarily collaborate to fulfill the agreed upon central purposes.

Systems Engineering	Systems Engineering is an interdisciplinary approach and means to enable the realization of successful systems. It focuses on defining customer needs and required functionality early in the development cycle, documenting requirements, then proceeding with design synthesis and system validation while considering the complete problem [23].
Technology maturity	The degree to which a technology has been proven in a realistic operational setting. Not to be confused with a system's life cycle [20]. (1) Technology Readiness Level is a technology-neutral metric to assess the risk associated with technology development. (2) Integration Readiness Level is the maturity of the links between individual components (TRL); (3) System Readiness Level is a function of individual TRLs and the maturities of the links between them (IRL).
User centred design	User centred design (UCD) is a type of user interface design and a process in which the needs, wants, and limitations of end users of a product are given extensive attention at each stage of the design process. UCD can be characterized as a multi-stage problem solving process that not only requires designers to analyse and foresee how users are likely to use a product, but also to test the validity of their assumptions with regards to user behaviour in real world tests with actual users [13].

3 Design principles

In deliverable D3.1[7], considerations are given for design principles that should be used when developing a TACTICS system. Figure 3.1 shows a view of the project with its work packages. In workpackage 2 scenarios and requirements are defined. In workpackage 3 the design of a TACTICS system is given. Where D3.1 offers a wider view, which includes concepts for maturity levels beyond this project, D3.2 focusses on the design of a system within the project, as supporting process and framework for research activities and validation of what a TACTICS system would do.

In the next sections some design principles, as introduced in D3.1, are considered for application to the system design in this project:

- Scoping
- Design process
- User centred design
- Privacy-by-design
- Data security

3.1 Scoping of the TACTICS Validation system

The TACTICS validation system is a system-of-systems. Therefore there are multiple scopes:

1. The TACTICS Validation core system, which internally consists of three loosely coupled tools.
2. The TACTICS Validation system with connected (friendly) capabilities.
3. The TACTICS Validation system with connected (friendly) capabilities, surrounded by not (yet) connected friendly capabilities.

3.2 Design process

The design of an operational TACTICS system requires a professional design methodology as is motivated in D3.1. The TACTICS consortium has proposed a particular solution direction in competition with other proposals, which eliminates the need for a design process in the TACTICS project which facilitates alternative parallel designs. In addition, a future operational implementation of a TACTICS system will require a complete redesign and rewrite from scratch. The purpose of our design and validation is to validate several key design patterns, not to start the actual implementation of them. The Waterfall process is therefore suitable for the TACTICS project, and the main components of that process map directly on TACTICS work packages.

The *requirement specification* is performed in WP2. The *system design* is done in WP3, with D3.1 describing the generic concepts and this document describing the specific design of the validation system developed within the project. Implementation and integration of a system is divided over work packages 4 to 6, each regarding one of the defined functional components, using the results from work packages 2 and 3. The system will be validated in work package 7. A maintenance phase is not part of this research project.

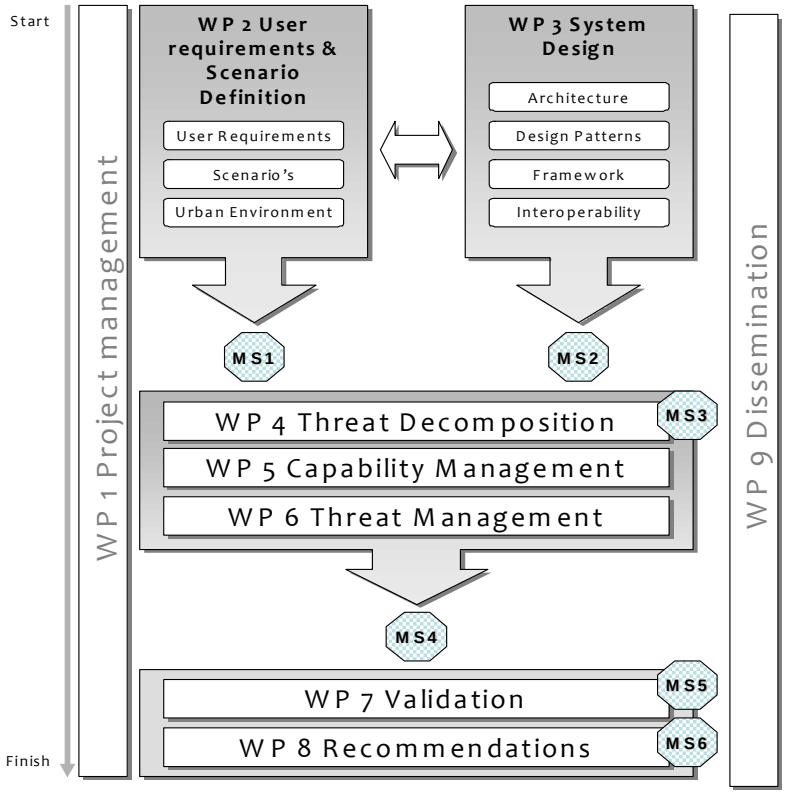


Figure 3.1 View of the TACTICS project by Work Package.

This approach is common for a research project such as a STReP and has several consequences:
- It garantees an external oriented focus with high interaction with end users;
- It garantees a high level of control over budget, result and timing;

3.3 User centred design

Gulliksen et al [13] have described twelve principles of user-centred design which can be applied both the TACTICS project and in the design of a TACTICS-class operational system. Within the TACTICS project, we apply most of them (see also Figure 3.1 for a view of the project and its work packages):

Principles	TACTICS project
User focus	The TACTICS project has defined three archetypical users which guide the system design: the threat manager, the threat decomposition manager and the capability manager. For these three users an overview of system-level scenarios is included in Annex A.
Active user involvement	Two end users are active project members. In addition, the user workshop was used to play a serious game of a simulation of the TACTICS system.
Evolutionary systems development	TACTICS project has one design cycle, although iterative cycles may be used in implementing the system in WP4-6.
Simple design representations	D3.1 and D3.2.
Prototyping	Prototypes of tools are the deliverables of WP4-6.
Evaluate use in context	An validation will be done in WP7
Explicit and conscious	WP2-7.

design activities	
A professional attitude	Consortium has extensive experience and professional attitude.
Usability champion	None
Holistic Design	Deliberated in D3.1. The consortium is aware of multiple dimensions such as technical, organizational, human, ethical, legal, etc.
Processes customization	Section 2.3 of D3.1.
A user-centered attitude	Yes, mixed with a scientific and holistic attitude

3.4 Privacy by Design

The TACTICS project will operate within the limits of current law. Specifically, the laws of the nation where the validation will take place. Within work package 7 (Validation) it is possible that TACTICS will observe people, since the validation covers aspects such as face recognition, human surveillance and behaviour video analytics. The validation will also be carried out in accordance with EU Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data, as well as with the European Data Protection Supervisor's 2010 video surveillance guidelines. In addition to this, TACTICS will apply Privacy-by-Design. The seven foundational principles [2] will be addressed as follows:

- **Proactive not Reactive; Preventative not Remedial**: By having an ethics specialist responsible for ethical relevant issues, TACTICS creates a working environment where issues regarding privacy can be pro-actively worked on, instead of in a reactive manner with an external ethical board. The section on ethics and privacy in deliverable D2.2 is a direct result of this approach.
- **Privacy as the Default**: Data subjects will only participate in any validation activities on an opt-in basis. This is sufficient for the TACTICS validation system because the TRL level is not higher than 5, and because none of the TACTICS project goals require actual surveillance to be done.
- **Privacy Embedded into Design**: Every work package of TACTICS has a task embedded regarding privacy, ethics and human rights. In addition, the ethical requirements from D2.2 are direct input for the system design of the TACTICS validation system.
- **Full Functionality – Positive-Sum, not Zero-Sum**: The TACTICS project does research for security while ensuring the privacy of data subjects which were needed for the project.
- **End-to-End Security – Lifecycle Protection**: Any personal data that is gathered during the project phase will be deleted when it is not needed anymore for the project.
- **Visibility / Transparency**: Data subjects participating in any testing and validation activities will be explained in full detail what happens with their personal data. In addition, the general (D3.1) and specific (D3.2) approaches of the TACTICS project are described in public deliverables. However, due to the sensitive nature of this project not all deliverables can be made public. For many restricted deliverables a public version is made available where the security-sensitive material is removed. The TACTICS project has a public email address for any additional questions.
- **Respect for Users**: In the context of this project, respect for users should be interpreted as respect for data subjects in any testing and validation activities. TACTICS will recommend to use the least invasive surveillance capability as possible. The next section describes how the TACTICS validation system will interpret invasiveness.

3.4.1 Invasiveness / intrusiveness

The TACTICS validation system will recommend the least invasive surveillance capabilities given a certain information request, and will inform relevant end users of the invasiveness of surveillance measures that they employ. D3.1 contains a more elaborate section on the definition of invasiveness. Table 1 describes the four- and nine levels of invasiveness that the TACTICS Validation System will use.

Table 1 - Four- and nine level scales of invasiveness

Invasiveness (4 point)		Invasiveness (9 point)		Description
A	None	0	None	There is no surveillance
B	Slight	1	Knowing	The subject knows that he is being monitored, but does not see, have to carry or do anything special (e.g. you assume that a certain fraction of the subjects carries mobile phones which you can monitor);
		2	Seeing	The subject sees the devices monitoring him around him, but he does not have to carry something or act in a special way;
C	Moderate	3	Carrying	The subject carries a device which is being monitored. The device does not require any special acts in order to be monitored, e.g. a GPS tracking device;
		4	Acting	Acting (i.e. cooperation): the subject regularly has to act in a certain way in order to be monitored, e.g. have biometrics taken in a controlled environment, or offer an RFID card to a reader;
		5	Possibly interrupting	The monitoring agent (device, etc.) has the option to interrupt when he sees fit, but this is not certain, e.g. a police officer standing next to a people flow;
D	Strong	6	Interrupting	The subject knows he will actually be interrupted in his normal behaviour in order to respond to a probe or an information-request, e.g. a reception desk at a secured object;
		7	Bodily	The subject has to give physical access to (a part of) his body, e.g. a pat down at an airport.
		8	Full transparancy	The subject hands over control over his body and allows monitoring of his internal physiological factors

These scales will be used in the communication to and from the end users of the TACTICS system to make them aware of the invasiveness of their choices.

3.5 Data security

TACTICS as a research project does not focus especially on data security because, as the end users are typically defence and police organisations, they will already have appropriate data security policies and measurements in place.

The TACTICS validation system faces several data security threats:

- Data breach of personal data of actors for scenario's (either in role of end users, terrorist, citizen or resource);
- Intellectual property theft (of designs, source code, scenario's, scientific papers and patents);
- Corruption of test data (by inserting false test data or stealing test data).

The TACTICS Validation system will apply appropriate data security measurements by relying on the data security measures of the consortium partners. These are speratately validated by the EC and are among the strongest in their kind. The TACTICS validation system will only be run in a secure environment.

4 System architecture description

This section describes the main actors of the TACTICS validation system, the system decomposition and the use cases and information flows.

4.1 Main Actors

The TACTICS validation system serves three managers, and has interaction with several kinds of resources. The managers are the Threat Manager (TM), Threat Decomposition Manager (TDM) and Capability Manager (CM). In the next sections, these three managers are described as personas. As external users, there are the resources managed by the capability management, and used as information sources by threat management. These resources can be sensors (possibly combined with automated processing), persons (such as police officers), data/information sources (e.g. databases) or combinations (e.g., a person looking at a video screen, reporting information). Section 4.2 describes the three tools which in a loose integration form the TACTICS validation system. In section 4.3 a short description of the use cases is given. A more complete description of the personas, including additional personas of relevant actors such as the terrorist (who are not direct users of the system), is provided in D3.1.

4.1.1 Threat manager

The TM is responsible for making decisions based on the complete operational picture. He is in charge of the operation. He has information on a specific threat. He asks the TDM to decompose the threat into observable terrorist behaviour that can be detected at the threat location. He asks the CM to give him “eyes and ears” on the relevant locations. He hears from the TDM what the threat is, and what he should look out for. He hears from the CM what his options are, and where his blind spots are. He combines this information with human intelligence. Based on the outcome the TM must take decisions.

The TM has to have an overview of the entire situation in order to make the right decision. Therefore it is important that he can prioritize information and focus on the most essential decisions that have to be made. Also he must oversee the consequences of decisions that are made.

The TM will be assisted by a Threat Management Tool (TMT) which provides up-to-date information and reduces the work load, especially in stressful situations. This is done by:

- enabling clear communication: help creating clear, understandable messages to other managers and resource
- provide prioritized information: allow the TM to make decisions based on the information shown and also his/her experience, also allowing to find what made information have a higher priority.

The design in D3.1 contains both a threat manager decision maker and a threat manager (analyst level). In this TACTICS validation design (D3.2) these two roles are combined into one role to reduce unnecessary complexity: the threat manager.

4.1.2 Capability manager

The CM is responsible for providing knowledge on the current capabilities that security forces have at their disposal.

The CM will analyze the possible capabilities with regard to their appropriateness and availability for detecting signs of a threat as specified by the TM. The CM will advise the threat manager what capabilities are required given a certain situation.

The CM is assisted by a Capability Management Tool (CMT) by having information about all capabilities, and by matching relevant capabilities to the information needed by Threat Management.

4.1.3 Threat decomposition manager

The Threat Decomposition Manager (TDM) is responsible for providing knowledge on terrorism, terrorist groups and modus operandi. The TDM has access to historical examples of similar threats, with specific threats, modus operandi and behaviour.

He must also be able to think of possible variations of modus operandi. A certain degree of creativity is also an important requirement with regards to possible new (and realistic) modus operandi.

The TDM is assisted by a Threat Decomposition Tool (TDT) by providing relevant threat knowledge matching the known threat information, and reporting this information in a non-biased way.

4.2 System

The main aim of the TACTICS system is to provide important information about a threat more quickly and efficiently. This is done by using information of previous threats to obtain threat indicators, efficiently match capabilities to focus on these indicators, and combine and filter information to provide relevant information. To do this, this process is executed by three users, who are supported with three loosely coupled tools. The tools also support the communication between the users, as shown in Figure 4.1.

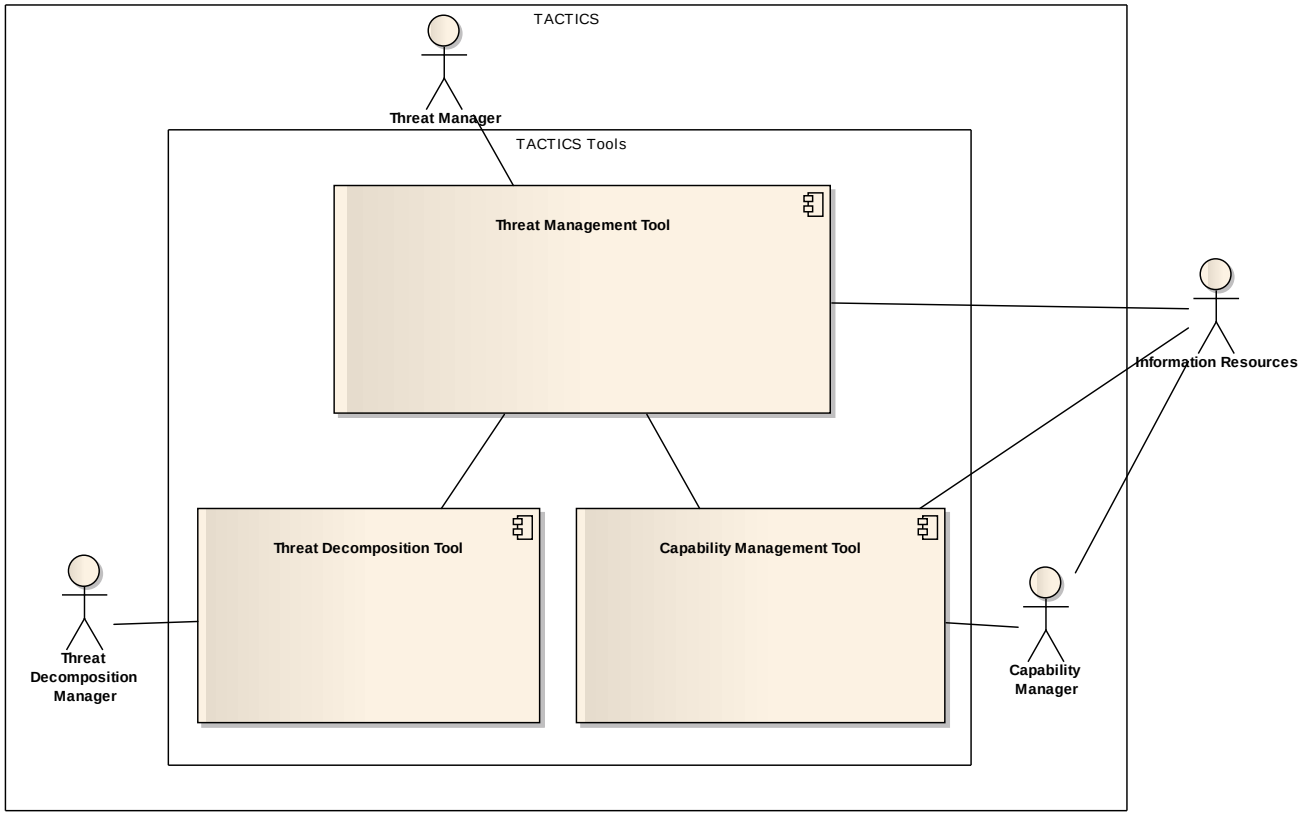


Figure 4.1 System view with main actors and three sub-components

Although no direct links are shown between actors, they will communicate directly with each other and with other people. A technical link will also be provided by the tools, for example allowing a threat manager to communicate directly with a resource like a technical sensor or a human observer.

The validation design is described in more detail in Figure 2. The figure is followed by three sections with descriptions of the internal modules per tool.

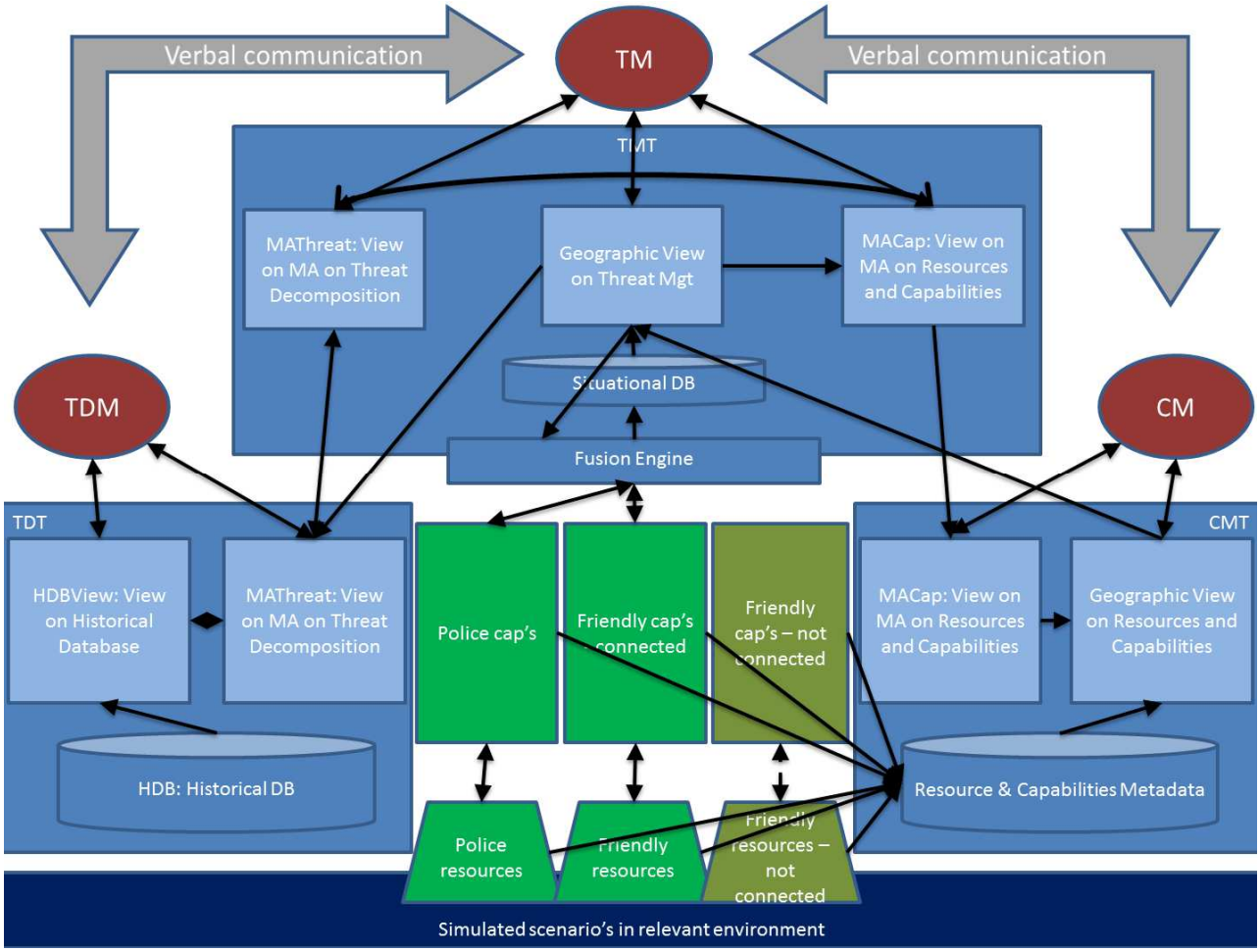


Figure 2 - TACTICS Validation Design: structural decomposition. The blue elements TMT, CMT and TDT are the core TACICS system, the dark blue rectangle is the environment of the TACTICS system-of-systems. Internal light blue blocks are the respective GUI elements., Black arrows are technical interfaces, human users are shown in dark red, including verbal communication in grey. Resources and capabilities are in green, where two distinctions are made: police capabilities versus non-police capabilities, and connected capabilities versus not (yet) connected capabilities.

In the next sections, the system will be described further. Use cases are provided for these actors for the different components. An example is then provided of how information may flow through the system and between components. These use cases and information flow are indicative for the functional description of the components and their interfaces in the later chapters.

4.2.1 Components of the TMT

The TMT has three GUI elements and contains all elements w.r.t. situational awareness, data fusion and links to (TACTICS-)resources which are actually in use.

Table 2 - Components of the TMT

Name	Function	Detail
TMT	Give an overview of the actual situation, the threat and possible prevention or response actions	Three separate GUI's (screens)
TMT:Geo	Give situational awareness to TM	
TMT:SitDB	Store actual situation in metadata and data	Contains video, tracks, detections, etc.
TMT:Fusion	Fuse data and information from both TACTICS and non-TACTICS capabilities	
TMT:MACap	Input screen for TM to request capabilities	Morfological analysis view
TMT:MAThreat	Output screen to TM to get unbiased threat information	Morfological analysis view
TACTICS capabilities and Resources	Supply object metadata	Behaviour detection, person recognition, identification, tracking
Friendly capabilities and resources	Supply object metadata	Simulated

4.2.2 Components of the TDT

The TDT contains two GUI elements and contains all data and functionality for analysing threat information.

Name	Function	Detail
TDT	To support TDM to generate unbiased threat information and supply this to TM (via link to TMT)	Two separate GUI's (screens)
TDT:HDB	Store historical incident metadata	Nice to have
TDT:HDBView	Show and search historical metadata	relate to configurations
TDT:MAThreat	Described unbiased threat information	Morfological analysis view; using input from HDB and TM

4.2.3 Components of the CMT

The CMT has two GUI elements and contains all metadata about the fitness-for-purpose, availability, accessibility, location and costs of local surveillance capabilities.

Name	Function	Detail
CMT	To support the CM to generate actual references to capability and resources	Two separate GUI's (screens);
CMT:Geo	Show geographic view on availability, location and QoS parameters of capabilities and resources	
CMT:MACap	Show TM requests	Morfological analysis view
CMT:RCDB	Collect and store actual resource and capability metadata	using input from both TACTICS and friendly resources and capabilities

4.3 Use Cases

In this section, we describe how the TACTICS system will be used by means of use cases. A use case describes the interaction of a user with the system. An indicated connection of a user to a use case does not imply on which side the use is initiated, although in many cases this is obvious. For example, the capabilities of external information resources have to be known, but it is not defined whether the information resources themselves make their capabilities known, or that the system requests this information from these users, just that the functionality of getting the capabilities known in the system should be present, and involves the information resources. Use cases in this section are based on requirements from D2.2 [5] but may not correspond one-to-one.

4.3.1 Threat Management Use Cases

In Figure 4.3 the use cases for Threat Management are shown, indicating the users that interact with the Threat Management Tool. The use cases for the Threat Manager are further described in Table 3.

The Threat Manager uses the system to make the threat more clear in order to make better decisions to obtain information about the threat, and finally to act on the threat. These use cases (on the left of Figure 4.3) will in part be handled within the Threat Management Component (either by Threat Managers themselves, other operators, or tools such as a fusion engine and information display), and in part delegated to the Threat Decomposition Tool and Capability Management Tool. The dotted lines indicate a direct link to use cases of the Threat Managers to those of the other Tools and the information resources. These need not be unique, for example, communication of a Threat Manager with a resource is not the only control of resources. Use cases of the other tools are described for the respective tools below the respective figures. Not all use cases are described in detail.

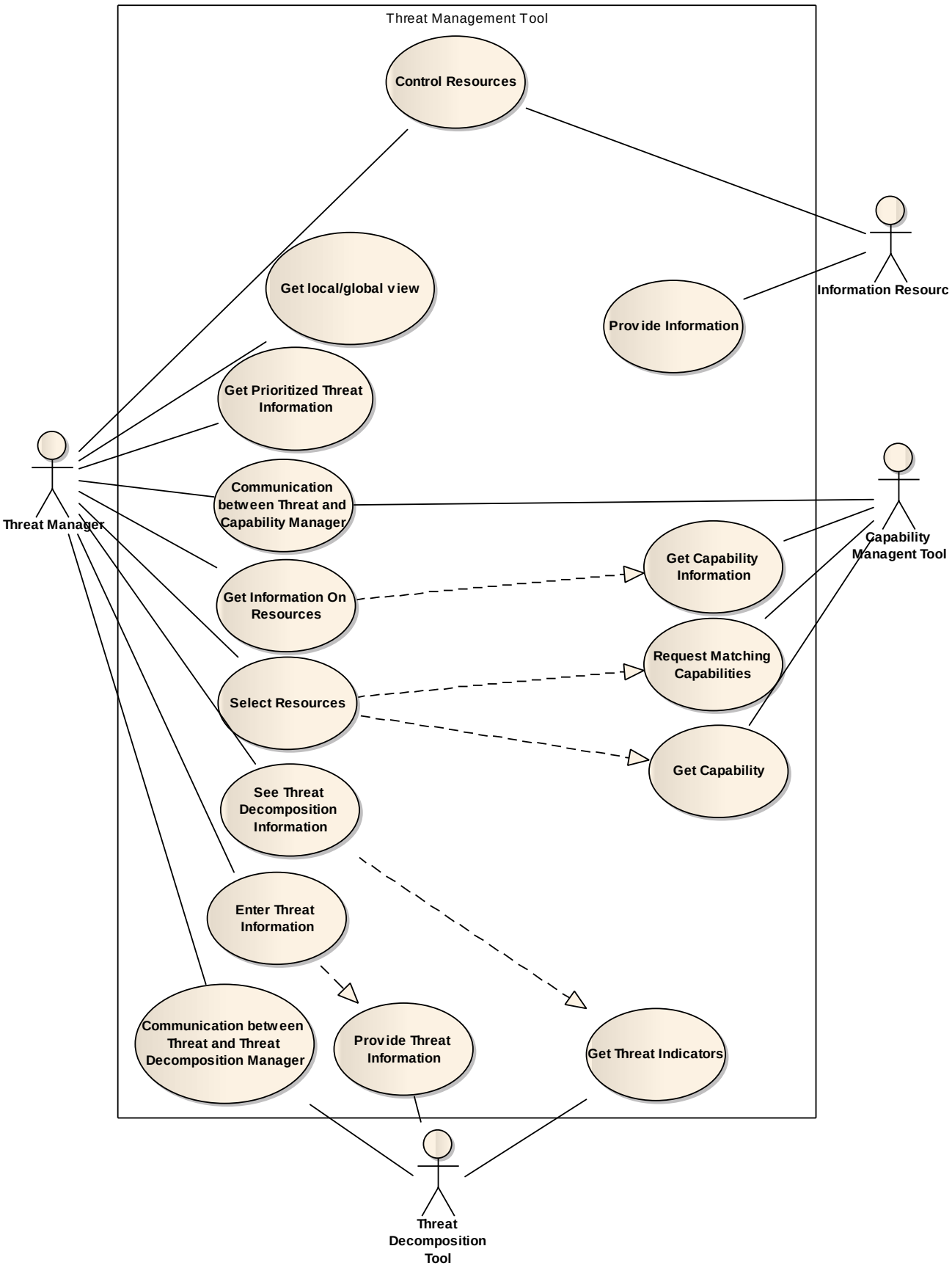


Figure 4.3 Threat Management use cases

Table 3. Details for the use cases for the Threat Management Tool

Use cases of the Threat Management Tool
UC1 Get local/global view
The Threat Manager ask the Threat Management Tool to filter displayed information (e.g., resource locations, threat information) by location, or display information from all locations (global).
UC2 Get Prioritized Threat Information
The Threat Manager is shown information on (possible) threats, with a priority by which information can for example be filtered. Underlying information on why information has a certain priority can be requested, for example, that a certain object is of interest because it is in a certain location, and therefor fits a key indicator as specified by Threat Decomposition.
UC3 Communication between Threat and Capability Manager
The Threat Manager is helped in communicating with the Capability Manager by the tool facilitating communication, e.g., by setting up a connection and/or allowing pre-formatted messages.
UC4 Get Information on Resources
The Threat Manager can get information displayed of resources (as obtained from Capability Management).
UC5 Select Resources
Based on threat descriptors (e.g., behaviours, or possible targets, or locations) resources are selected that may supply this information. (This links to capability management, where matching to capabilities of resources is done). Selected resources will start to provide information (See later use cases)
UC6 Enter Threat Information
The Threat Manager can enter threat information (for example after looking at other information), to be used by threat decomposition (if it was not automatically generated and passed on).
UC7 See Threat Decomposition Information
The Threat Manager can see the Threat Decomposition Information provided by TDM (i.e., key indicators, modus operandi, etc.).
UC8 Communication between Threat and Threat Decomposition Manager
The Threat Manager is helped in communicating with the Threat Decomposition Manager by the tool facilitating communication, e.g., by setting up a connection and/or allowing pre-formatted messages.

UC9 Control Resources
The resources in use can provide information autonomically, i.e., after requesting information, no interaction takes place until information (such as intell) is provided. However, it may be necessary to control resources. For example, an officer on the street may be given a task to specifically look for something, or a camera (when viewed by an operator) may have to be pointed somewhere.
UC10 Provide Information
This use case has the Information Resources as user, providing information to the Threat Management Tool (for display, filtering, processing, etc.) in different ways.

4.3.2 Threat Decomposition Tool Use Cases

Threat Decomposition provides threat information to Threat Management, which is a user via the Threat Management Tool. The Threat Decomposition Manager is a direct user of the Threat Management Tool, as shown in Figure 4.4.

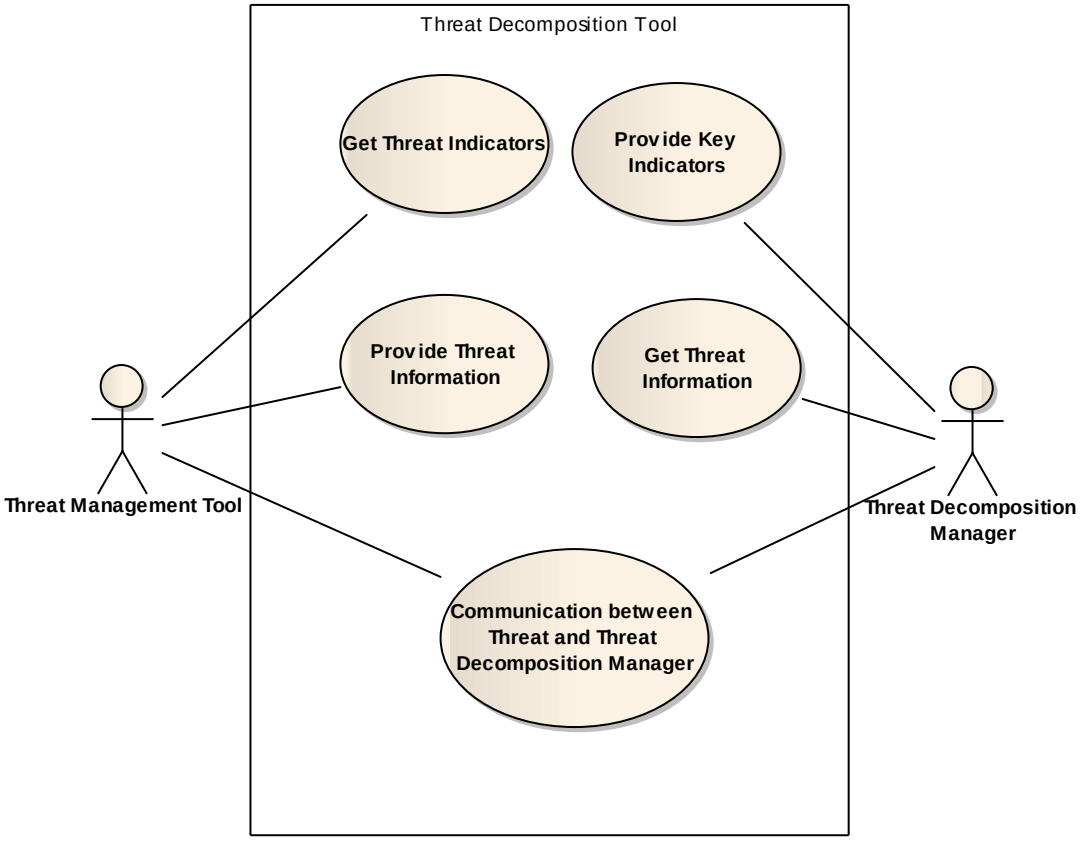


Figure 4.4 Use cases of Threat Decomposition

The Threat Decomposition Component provides four use cases for Threat management (here worded as seen from Threat Management). These can either be fulfilled internally, for example by automatic use of a database, or helped by the Threat Decomposition Manager as an expert (or by contacting other experts). In these cases, there is a direct link between the use cases delegated from the Threat Management, and the (sub-)use cases of the Threat Decomposition Manager. The threat Decomposition Manager can see the information about the threat provided by Threat Management, as indicated by the last three use cases.

Table 4. Details for the use cases for the Threat Decomposition Management Tool

Use cases of the Threat Decomposition Management Tool
UC11 Provide Threat Information
Information about a threat is provided from Threat Management, for example that a threat is from a certain terrorist group.
UC12 Get Threat Indicators
Threat decomposition provides relevant related key indicators, i.e., possible targets, possible resources, possible (deviant) behaviour and Modus Operandi
UC13 Get Threat Information
The Threat Decomposition Manager can see what Threat Information is provided from Threat Management.
UC14 Provide Threat Indicators
The Threat Decomposition Manager can enter Threat Indicators to be provided to Threat Management

4.3.3 Capability Management Use Cases

The Capability Management Tool (see Figure 4.5) has three users: The Information Resources as external user, the Capability Manager, as internal user who together with the Capability Management Tool provides the Capability Management, and the Threat Management Tool, who delegates functionality from Threat Management (i.e., the Threat Manager as user of the Threat Management Tool is connected to Capability Management via this internal user).

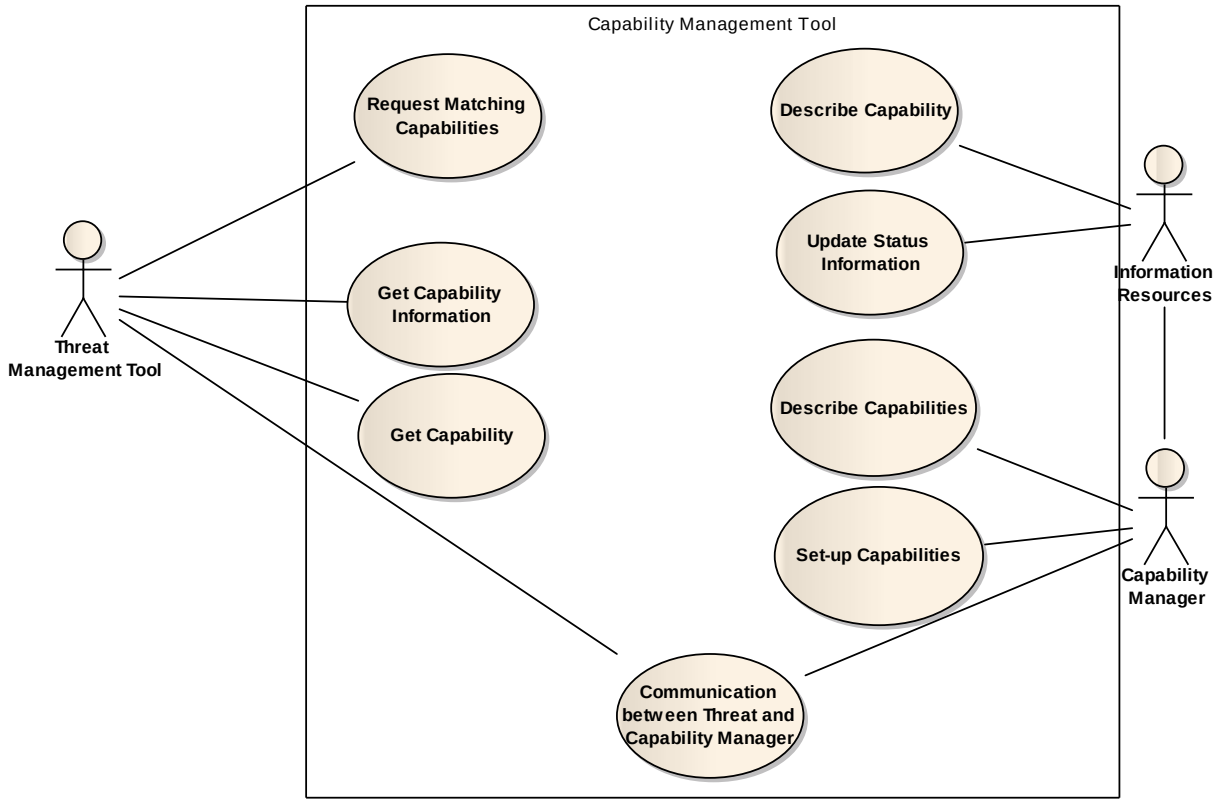


Figure 4.5 Use cases for Capability Management

Use cases for the Capability Management Tool are shown in the table below. Capability Management is delegated four use cases from Threat Management, worded here (in the first four use cases) as seen from Threat Management. Capability Management needs to know the capabilities of available resources. This may be automated or done by the Capability Manager, and is described by the last four use cases.

Table 5. Details for the use cases for the Capability Management Tool

Use cases of the Capability Management Tool
UC15 Request Matching Capabilities
Threat Management indicates an information need, for example observing certain objects, or surveilling a certain geographical area, and requests information on resources that might provide this information.
UC16 Get Capability Information
Capability Management provides a list of resources that match this need. This may be a full list of capabilities if no focus was requested. Capabilities should include information on reliability (how well can it supply the information), cost and time of deployment. For example, the following high-level categories can be used for the attributes: • Technical • Financial • Geo-spacial • Quality-of-service • Ethical General appropriateness for detecting certain signs should be indicated as well.
UC17 Get Capability
When threat management selects a resource, it should get a link to this resource.
UC18 Communication between Threat and Capability Manager
Direct communication should be possible between the Threat and Capability Managers, facilitated by the tools, or directly. Either may initiate this communication.
UC19 Describe Capability
For matching descriptors to resources, the capabilities of the resources should be known by the system, in a defined form. In this use case, this information is either provided by the capabilities, or obtained automatically by the tool from the resources.
UC20 Update Status Information
Some resources may have changing status, such as the direction a camera is looking, or the location of an officer in the field. The first is needed to use the information, the latter could be part of describing the capability (i.e., is the officer near).
UC21 Describe Capabilities
The capability manager may input known capabilities of resources that do not communicate with the system automatically, for example officers on the street, a security firm, or an information system to which a connection is not always present.
UC22 Set-up Capabilities
For resources that are not always connected, a connection needs to be set-up that can be passed to threat management. This can be communication information to a security officer, or a url to information

4.4 Information Flows

A real operational system will be started after a decision to manage a threat is made, based on intell information suggesting a likely threat. The system developed within the project will be validated in a realistic but controlled setting, as described in section 8 As such, information flow starts after starting the system, with an initialisation process, initialising its components (including both tools and managers). The Capability Management will at this point need to get a list of capabilities of (available) information sources.

Threat management is the central part of the system, and communicates with the other parts. From Threat Management, the threat information is communicated to Threat Decomposition Management, in order to get Threat Decomposition information back, such as indicators of possible ways the (fake) threat may evolve.

These indicators could be resources that will be used by the terrorists (e.g., a van, explosives) and possible targets (e.g., events, certain buildings). Threat Management can decide where the focus should be and ask Capability Management for available capabilities that can provide information about these indicators. Capability Management provides information about available capabilities, combined with a concrete link to obtain this information. For example, a camera can be listed as capability for observing a certain building, with a link to a camera feed. Another possibility is an officer that is nearby, and a way to contact him, together with information that it will take some time for him to get to the building. The Threat Manager decides what resources to use and requests and receives information from the information sources. This information (possibly) improves the knowledge about the threat, after which the cycle starts again towards Threat Decomposition Management.

5 System design

The design described in this chapter describes the functionality and its internal components in sufficient detail to make clear what it needs from other components, and what it will produce in return. These last two will be described in more detail in the interfaces section. In the next sections the functionality of each component is described, as well as an indication of its internal implementation. This section is not intended to fully define the internals of the components (which will be done in respective work packages).

5.1 Threat Decomposition

The Threat Decomposition tool will help the Threat Decomposition Manager (TDT) provide information from historical and expert knowledge, to the Threat Management, related to possible threats. For this, historical and expert knowledge has to be made accessible. Therefore, WP4 contributes to two different work processes:

1. The preparation against a certain terrorist threat, collecting and processing relevant information, and providing it in a processable form
2. The understanding of an actual terrorist threat, during the use of the system, accessing the information.

For the first work process, i.e. in the preparation for possible terrorist threats during validation, project partners and end users determine the key indicators (including indicators describing parts of Modus Operandi), their possible values, and combinations of such indicators, based on logical, empirical and normative grounds. This is done based on their professional experience, and on available collections of historical incidents. This process in formalizing the form of information, is done by performing a morphological analysis [19], as one of possible methods for this process. This results in a database with for example, a table with a list of the indicators, a table with the possible values and a table with combinations of values, in a form that can be accessed by the tool.

For the second work process, i.e. during a terrorist threat, the TDT receives from the Threat Manager (TM) potential indicators. These indicators should be of the same type that were determined in the Morphological Analysis, or should be transformed in those MA-indicators. Using the tables in the database, the TDT returns complimentary indicators to the TM. The TM should look out for those indicators. Based on the current set (or a user-specified subset) of indicators, the TDT also shows historical incidents which match those indicators.

5.2 Capability Management

The Capability Management Tool helps the Capability Manager to keep track of capabilities, and match them to required information needs of Threat Management. It should keep an overview of all available capabilities, up-to-date for example for resources that are changing location, or may not always be available due to other use. CM should be able to provide Threat Management with an overview of capabilities, if required only those matching the request. Capabilities shown to Threat Management should include the information needed to access the capability, for example a URL of a camera stream, or the phone number of an officer on the street. If special access rights are required, these should be set, based on the current restrictions. For example, because of privacy, use of private CCTV may be restricted, but these restrictions may be lifted under higher threat alert levels.

The CMT assists the capability manager by describing capabilities and resources in a standardized way, keeping track of resources, and helping to find resources that provide capabilities and thus deliver required information.

We envisage the CMT to support the following capabilities:

- Identify Person
- Observe Object
- Observe Area/Area Surveillance
- Recognize Number Plate
- Detect Abandoned Luggage

- Determine co-located events

We envisage the CMT to support the following types of resources

- Databases for number plates, events, work schedules
- Datalink/communication
- Cameras (CCTV, mobile/stationary cameras)
- Human sensors (SDR trained actors)
- Camera Operator

The logical view in Figure 5.1 presents the CMT as a packaging module pooling functional components that contribute to four major functional areas/packages/layers.

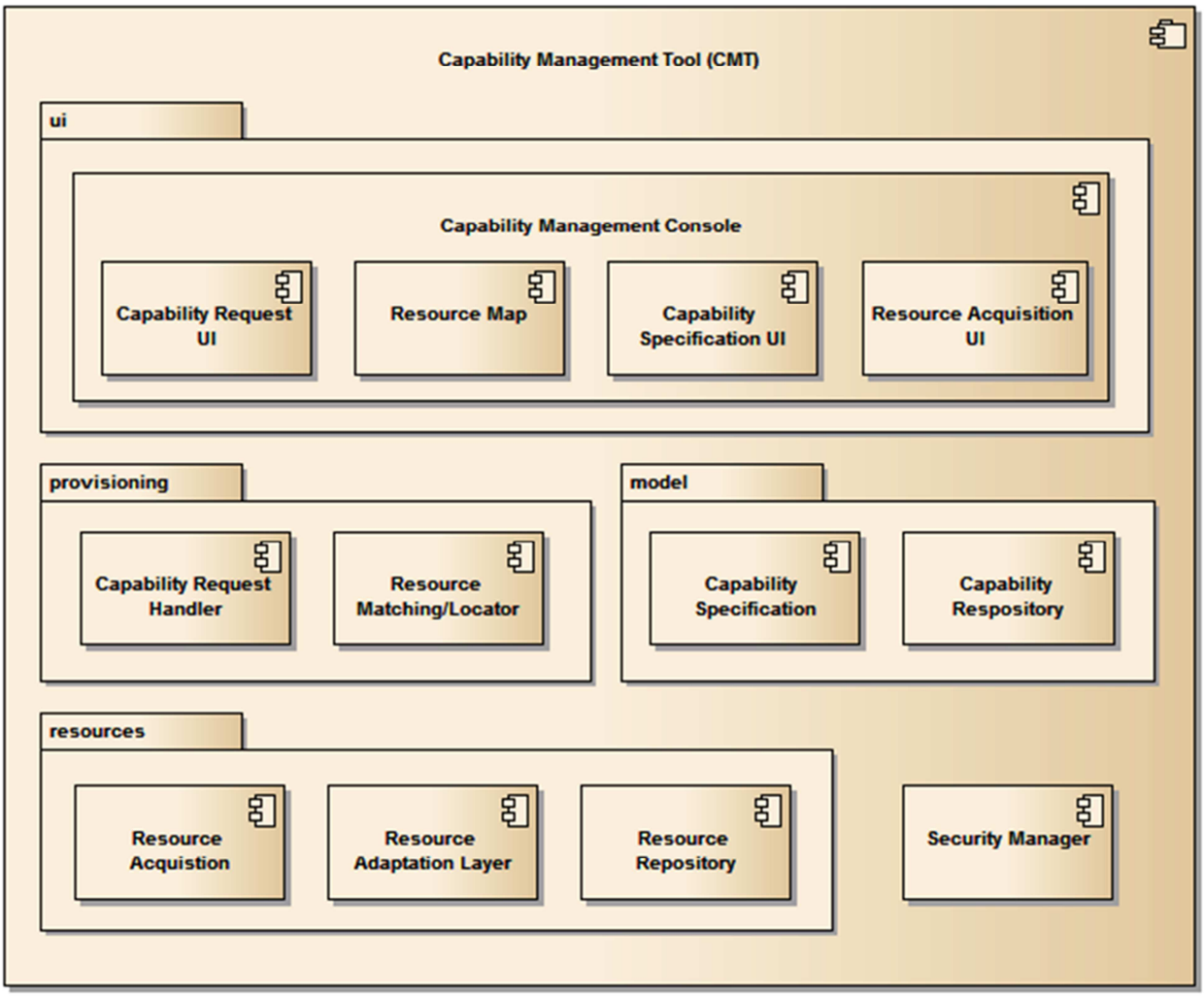


Figure 5.1 Capability Management Tool – Logical View

Resources layer

The Resources layer manages resources. Its components provide means to acquire, describe, persistently store, technically integrate, and monitor resources. The Resources layer decomposes into the following functional components:

Resource acquisition

- Maintains/manages the acquisition of resources, which are available to the TACTICS system
- Allows for automated, semi-automated acquisition of resources (e.g. crawl for IP cameras)
- Is capable of monitoring a resource' status (availability) during runtime
- Restricts access to/integration of resources according to security/privacy rules and the operational context (threat level)
- Provides an external service interface (WS-SOAP)
- The service interface allows for adding, removing, modifying, and tracking status of resources at runtime

Resource adaptation

- Represents an abstraction layer hiding technical specifics of concrete resources
- Provides unified interfaces to resources of the same resource type
- Provides connectors/drivers for resources
- Is capable of redirecting/optimizing resources (if a concrete resource technically allows for that)
- Provides an external service interface (WS-SOAP)

Resource Repository

- Imposes a unified way of describing resources. A unified resource model will be considered as discussed in chapter 6.3.3
- Persistently stores information on resources, which are permanently available to the TACTICS systems across several execution cycles of the TACTICS system (static resources)
- Establishes a runtime repository of static and dynamic resources that allows for fast/performant-querying
- Automatically releases resources that are only available until a threat is mitigated.
- Synchronizes access from the resource adaptation, resource acquisition and resource matching component
- At this point, the technical solutions for both the persistent store (e.g. SQL DBMS) as well as the runtime repository (e.g. in-memory database) are open

Model layer

The model layer imposes a common capability model that defines in a generic way how to leverage/utilize (abstract) resources (resource types) or a combination of resources to obtain certain capabilities. For that it provides means to define and persistently store (abstract) capabilities. The Model layer decomposes into the following functional components:

Capability specification

- Maintains/manages an abstract model of capability specifications
- A specification consists of potential resource sets, which in combination deliver a certain capability to a quantifiable or qualitative extent
- A specification considers also the estimated (a priori) support to a capability of resource sets as for example in terms of precision, accuracy, or coverage

- The model is not refering to concrete resources (instances) but rather abstract types of resources
- Provides an external service interface (WS-SOAP)
- The service interface allows for dynamically adding, removing, and modifying capabilities

Capability repository

- Persistently stores capability specifications across several execution cycles of the TACTICS system
- Synchronizes access from the capability specification and the resource matching component
- Establishes a runtime repository of capability specifications that allows for fast/performant-querying
- At this point, the technical solutions for both the persistent store (e.g. SQL DBMS) as well as the runtime repository (e.g. in-memory database) are open. Both might be co-located with the equivalent store/repository of the resource repository component

Provisioning layer

The provisioning layer is the CMT's main service layer. It handles incoming requests for certain capabilities and determines available utilizing resources based on the common capability model. The Provisioning layer decomposes into the following functional components:

Capability request handler

- Guides through/processes a requests for certain capabilities
- Is capable of handling multiple parallel requests, especially with respect to synchronization and performance
- Provides an external service interface (WS-SOAP) supporting synchronous and asynchronous communication (WS-Callbacks may be passed or some kind registration/subscription will be provided to be able to notify clients on successful matches in case of long running matching procedures)

Capability matching/locator

- Finds resources or resource sets supporting a specific capability (request parameter are detailed in chapter 6.3.3)
- Returns a ranked list of matching resource sets partially/fully fulfilling the requested capability
- Restricts access to/integration of resources according to security/privacy rules and the operational context (threat level)
- At this point, the technical solution is open (e.g. a business rule engine)

UI layer

The UI layer provides graphical frontends for the CMT's different resource and capability management components. Chapter 7.2 introduces the modules the UI layer is composed of.

Security Manager

As security and privacy aspects are considered to be crosscutting concerns of all logical functional CMT components, these are addressed with the security manager as central component.

- Enforces security/privacy regulations and restrictions in all components and sub-components
- Dynamically considers context changes (e.g. threat level changes)

5.3 Threat Management

The Threat Management Tool (TMT) will help the Threat Manager (TM) and his/her team to achieve a Common Operational Picture (COP) and increase their situation awareness (SA) during the threat facing/neutralization tasks.

The TMT will show to the TM fused and filtered information from different sources: the Threat Decomposition Tool (TDC), the Capability Management Tool (CMT) and the different information sources (including units deployed in the field) integrated in the TACTICS system. With this information the TM will be able to take more accurate decision for neutralizing the threat or mitigating the effects of the attack.

The main functionalities of the TMT will be the following:

- To show the location of the units in the field: the location of the units (persons and vehicles) will be shown in a GIS of the hot spot area. In addition, indoor locations will be shown depending on the building digital maps availability.
- To show information from both sensors deployed in the field (e.g. CCTV cameras) and from the deployed units portable sensors (especially video/infrared cameras). These cameras could be head-mounted, fixed, deployed and/or installed in vehicles (terrestrial, maritime and aerial).
- To show potential threats in the field: Different potential threats (e.g., suspicious vehicles or persons) can be introduced into the system in order to be reviewed by the units in the field.
- To show sensors location on the GIS: the location of the different sensors available in TACTICS will be shown to the TM in order to select the more suitable ones at each moment.
- To show fused sensor information: the TMT will show on the screen the information (Video, text, coordinates, etc.) from the different sensors integrated in TACTICS.
- To allow messaging (chat) and preformatted messages (such as key indicators to look for), providing different communication channels with the units in the field for sending orders and receiving updated information.
- To show information from the Threat Decomposition Tool (TDT) regarding deviant behaviours and potential modus operandi according to the type of threat provided by the intelligence.
- To allow communication with the TDT in order to ask for updated information.
- To show information from the Capability Management Tool (CMT) regarding available capabilities (including capabilities attributes). With this information the TM will be able to select/access the most suitable capability at each moment.
- To allow communication with the CMT in order to ask for updated information.
- To provide a portable version of the TMT for being used for the units deployed in the field. This application will be included in mobile phones or PDAs in order to allow the units to send and receive information to/from the control room (e.g. video, potential threat, preformatted messages, pictures, etc.).

6 Interface definition

In this section, the technical interfaces to communicate among the tools themselves are described. In the current design phase, these descriptions should be complete enough at a functional level, for each component and user to know what it is requested to provide, and to know that input it needs from other components will be provided.

TACTICS as a research project does focus on syntactic or semantic interoperability but is not in a position to dictate or build a complete metadata standard. We do recommend nine specific requirements for applied metadata languages for surveillance applications [25]. For the TACTICS Validation System a pragmatic approach is taken which leads to a limited notion of “plug and play”. The TACTICS validation system uses existing standards (ONVIF, REST, etc) where possible, which will be encapsulated in a simple abstraction layer.

In the following sections, the interfaces of the three components are described, assuming the interfacing will be through the tools. Although direct communication between for example the Threat Manager and the Threat Decomposition Manager (for example by phone or in person) is not excluded in the system, this communication is not described here. Interfaces from the tools to the Managers using the tools is described separately in the next chapter, where the human-machine-interfaces are considered.

The exact form at lower levels is left to be decided in the implementation phase, which can be done if interfaces are implemented in a single step. Some general considerations about choices for the lower levels of communication are given in the next section.

6.1 Open standards for data communication

For the exchange of information among systems in TACTICS, which includes TMT-to-TDT and TMT-to-CMT, the use of open standards is encouraged, at each level of the communication architecture. The universally extended TCP/IP stack is a useful communications framework, which can be used with different communication technologies such as: Ethernet, optics fibre, WIFI, WiMAX, satellite links, trunking networks as TETRA, GSM/GPRS, etc, in a transparent way. At level 4 (transport) of the ISO/OSI [27] layered architecture, both TCP and UDP can be used, depending on the criticality of the information to be exchanged. It is further proposed to use a mechanism of data exchange based on the interchange of XML messages, which will transport both requests and data. This mechanism could be one of the commonly used SOAP web services [26] that require HTTP on top of TCP transport.

Benefits from this approach are:

- Its high level of standardization
- Wide usage in the internet community, existence of tools and resources
- Ease of maintenance

However, we consider that the system has not to limit itself to only this approach. It can be useful to pay attention to other approaches more particularized to possible scenarios in TACTICS such as harsh, tactical communication environments where very limited bandwidth and high interference is present. In these cases, soft real time communications, with very narrow and reduced data exchange are a must. This leads to the usage of non-connection oriented, non-reliable transport protocols such as UDP.

6.2 Identification, purpose and data description of technical interfaces

Building upon the structural decomposition of Figure 2, this section identifies each technical interface in a new Figure 2. The figure is followed by a table describing each technical interface on a functional level.

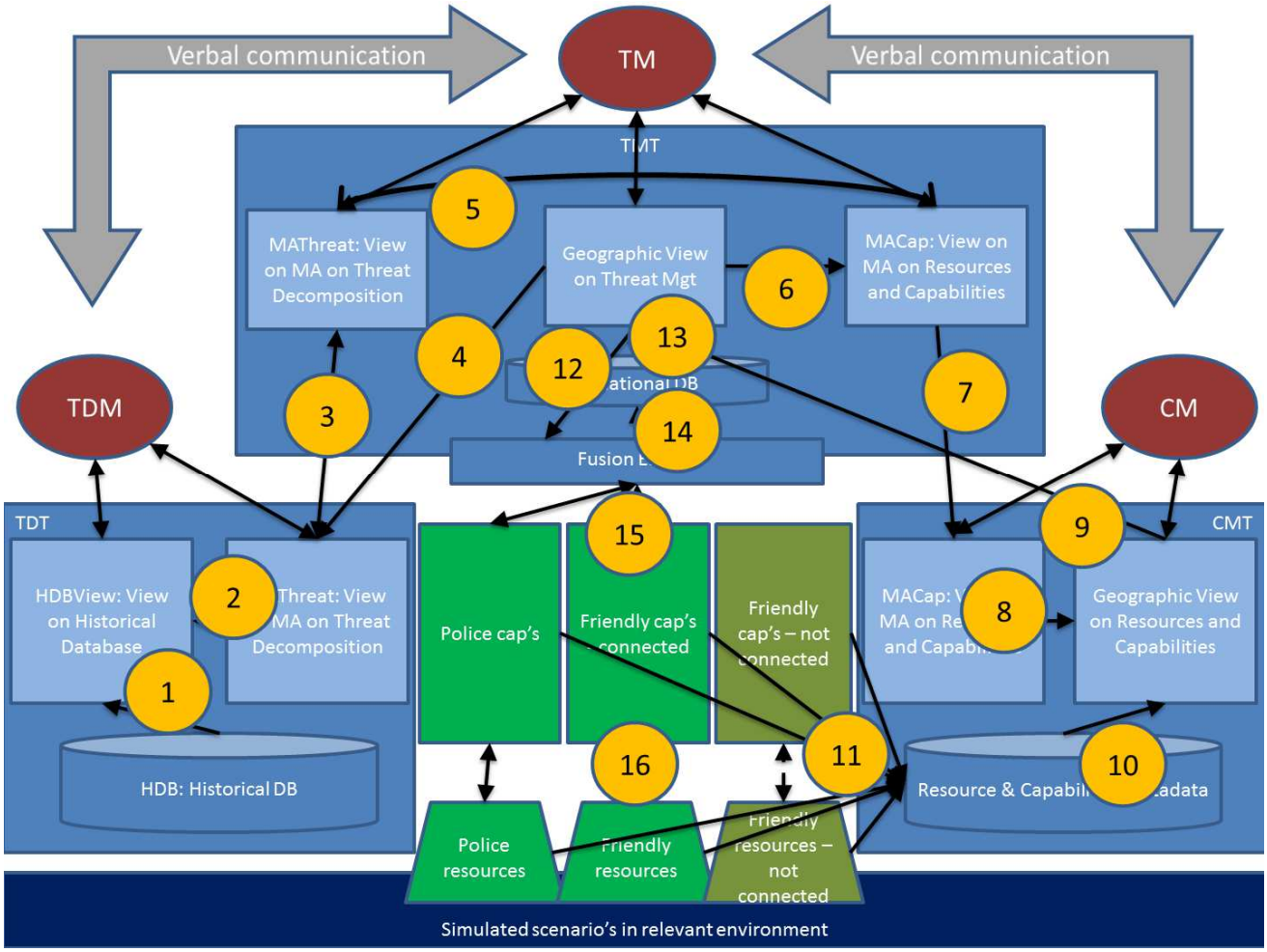


Figure 2- Identification of technical interfaces

Four technical interfaces involve two-way communication: 3, 5, 15 and 16. These take up 2 rows in Table 6 with identical id's.

Table 6 - List of technical interfaces

Id	Sender	Receiver	Information	Datatype
1	TDT:HDB	TDT:HDBView	Descriptions of historical incidents	texts / keywords
2	TDT: HDBView	TDT:MAThreat	Links between (partial) configurations and historical incidents	Keywords + partial configurations
3	TDT:MAThreat	TMT:MAThreat	Decomposed threat information	(partial) configurations
3	TMT:MAThreat	TDT:MAThreat	Suggestions to decompose	(partial) configurations
4	TMT:Geo	TDT:MAThreat	More detailed threat information	Free text (for logging)
5	TMT:MAThreat	TMT:MACap	Threats to find capabilities for	(partial) configurations
5	TMT:MACap	TMT:MAThreat	Capabilities to address threats	(partial) configurations
6	TMT:Geo	TMT:MACap	Area selection for capabilities	Area
7	TMT:MACap	CMT:MACap	Request for capabilities, including area	(partial) configurations + area
8	CMT:MACap	CMT:Geo	Request for capabilities, including area	(partial configurations + area)
9	CMT:Geo	TMT:Geo	Ranked list of available capabilities and resources	List of capabilities + resources (URL, configuration)
10	CMT:CapDB	CMT:Geo	Resource and capability metadata	Keywords + partial configurations

11	TMT:Fusion / Resources	CMT:CapDB	Dynamic metadata per resource / capability (availability, location)	ONVIF? SensorWebEnablement?
12	TMT:Geo	TMT:Fusion	Data request / configuration based on suggestions from CMT	(Capability, resources, area, parameters)
13	TMT:SitDB	TMT:Geo	View on actual situational awareness according to TM wishes	Situational awareness
14	TMT:Fusion	TMT:SitDB	Situation updates (tracks, recognition, detection of behaviour)	Object metadata
15	Capabilities	TMT:Fusion	Fusion	Object metadata
15	TMT:Fusion	Capabilities	Data requests / configuration updates	(Capability, resources, area, parameters)
16	Capabilities	Resources	Data requests / configuration updates	(Resources, area, parameters)
16	Resources	Capabilities	Raw data	Video / audio / text / …

6.3 Threat Management

6.3.1 TM – External resources interface

The TMT will gather information from heterogeneous external data sources, mainly three-fold: sensors, people as sensors and external information resources such as databases. Due to that heterogeneity an abstraction layer is required to encapsulate such an amount of different objects and associated data structures.

Most of the external data sources will be provided by CMT to TMT, so CMT will provide TMT the location of the resource and the means to access it. For instance, for a given video source, CMT will provide the location of the video (which can be, but not limited to, it's URL) and the means to access it which can include type of transport (TCP or UDP), kind of coding (MPEG, etc.) and so on. Besides video sources, CMT can provide a capability to TMT that can be the IP address of the policeman in the fields PDA, in order to send/receive messages from them. This where the heterogeneity is relevant and an abstraction layer has to be used to have a uniform access to resources, hiding each resource peculiarities.

6.3.2 TM - Threat Decomposition

These tools will communicate among themselves by means of exchanging (automated) messages. The overall process will be, most of the time, driven by the TMT which will request information from the TDT and processing. On the other hand, TDT can advise the TMT, asynchronously, when new data or processing is found to be relevant by the TDT managers.

Information to be exchanged can be divided in requests and information itself. Most of the information flow will be requests from TMT to TDT which will send data to TMT. Then, both TMT and TDT will send/receive requests and plain information.

In the latter case, the tools will exchange the following data:

- Information from the database about threats
- Information from the database about modus operandi
- Information from the database about behaviours and key indicators
- Information from the database about attack profiles
- Information from the database about current urban environment features
- Information from the database about current urban environment features matched to current threat
- Information from the database about privacy, ethics and human rights restrictions

6.3.3 TM - Capability Management

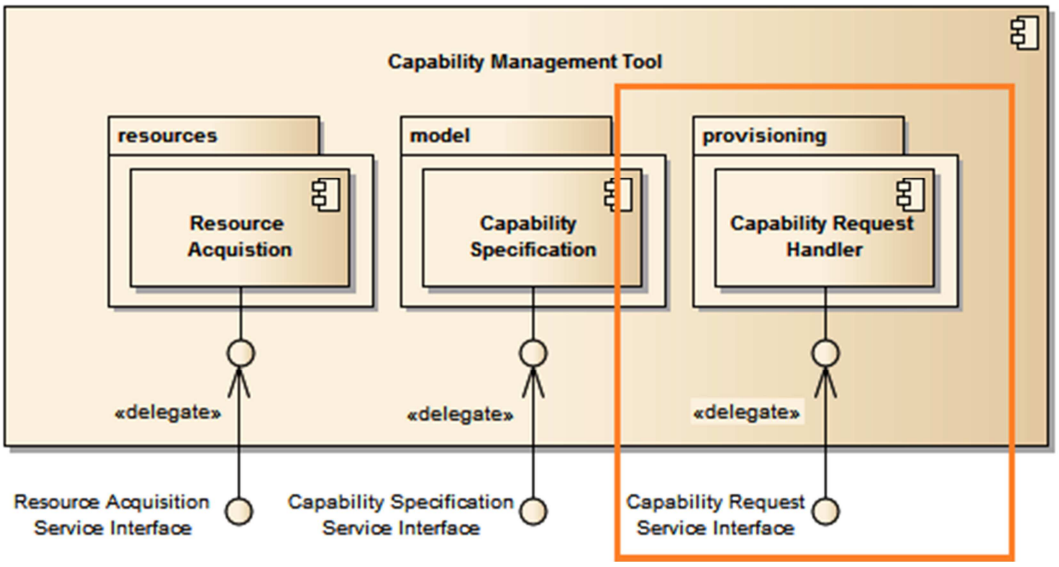


Figure 6.3 Capability Management Tool - Service View

In this particular case, the TMT communicates with the CMT by requesting capabilities through the CMT's service interface highlighted in Figure 6.3. In this context two kinds of information are exchanged between TMT and CMT:

- When TMT sends requests regarding certain capabilities required to mitigating a particular threat to CMT, a request considers the following request parameters:
  - Identifier of the required capability
  - Envisioned operating area, where the capability is needed
  - Envisioned geo position, where the capability is needed
  - Envisioned operational time frame, when (and how long) a capability is needed
  - QoS parameters (e.g. cost limit, minimum precision, minimum coverage)
  - Information on the operational context (e.g. threat level or about privacy, ethics and human rights restrictions)
- When CMT sends responses on previous requests to the TMT it returns a ranked list of matching single resources and/or resource sets, which partially/fully support the requested capability. Partial matches may require Threat and Capability Managers to redirect/optimize resources at their disposal in the field. Matching resources are detailed with their meta-data:
  - Supported modalities (e.g. audio, video)
  - Covered operating area
  - Geo position
  - Availability (e.g. a duty roster for police units)
  - Technical requirements (e.g. dependencies to other resources, prerequisitary resources)
  - Access information (depending on the type of resource for example a data link, URI, radio channel, or phone number)

6.4 Capability Management - External resources

One of the main challenges capability management faces is the integration of both technical and non-technical (human) resources.

In addition, new (technical) resource types, networking technologies, and communication protocols are evolving. Thus, resources employed in the field are constantly changing. Conceptually, CMT takes that into

account by providing a flexible and modular approach for the coordination of automatic discovery and integration of existing resources with different types.

Resource acquisition in CMT allows for three different discovery approaches:

- *Automated* – resources are discovered and integrated without the support of capability managers (e.g. a crawler for IP cameras within a certain area)
- *Semi-automated* – resources are discovered and integrated with support of a capability manager (e.g. automated crawling for cameras, but manual filtering of resources on certain criteria or manual redirection of resources)
- *Manual* – resources are integrated directly by capability managers (e.g. capability manager adds mobile cameras placed by on-site units)

Resource adaptation in CMT is not designed as one concrete software component. It rather formulates an architectural style how resources should be technically integrated into the system and how information received from (or send to a resource) should be represented in a uniform way.

It allows to access resources from multiple levels of abstraction and it decouples interfaces of a resource (which information is provided) from where and how it is attached (e.g. communication technology and protocols).

The high-level component diagram in Figure 6.4illustrates the core components involved in resource adaptation.

- *Resource Acquisition Manager* – A component that controls the discovery process
- *Resource Adaptation Manager* – A component that controls the initiation of the attachment process
- *Resource Type* – Defines how a Driver service and a Resource service can cooperate.
- *Driver* – Competes for attaching Resource services of its recognized resource type
- *Resource* – A representation of a physical resource or other entity that can be attached by a Driver service
- *Factory* – Discovers external resources and instantiates representing Resource services

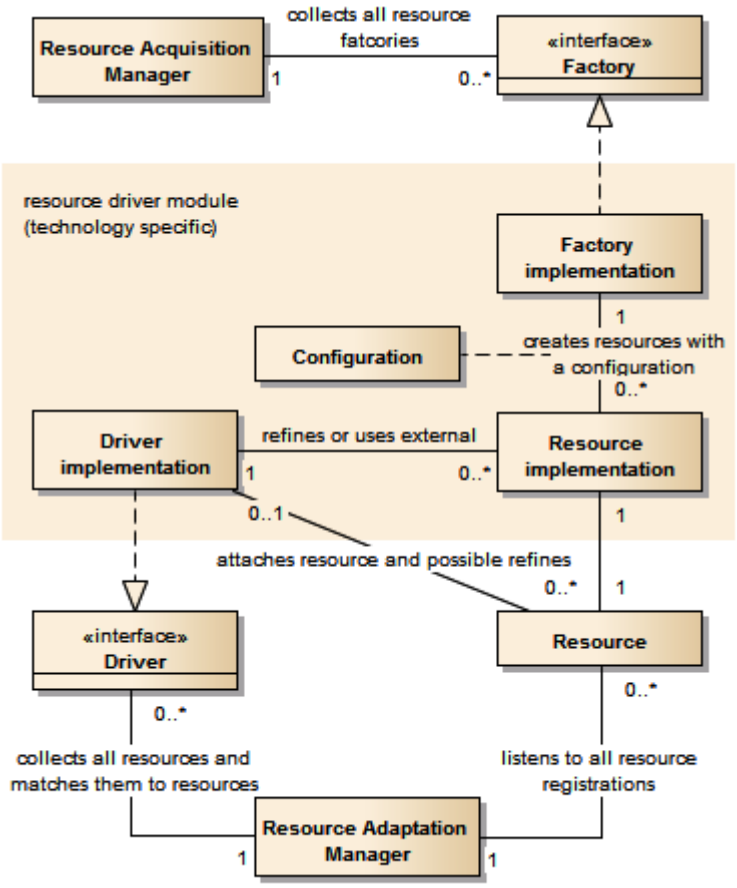


Figure 6.4 Capability Management Tool - Resource Adaptation

Resource services may differ widely: some represent individual physical resources and others represent for example complete networks or databases. Several Resource services can even simultaneously represent the same physical resource at different levels of abstraction. For example:

- A resource discovered on the Ethernet using salutation.
- The same resource identified as simple video camera
- The same camera refined as camera with integrated recorder

6.5 Data Model and tools interoperability

The full interoperability between the Threat Management Tool (TMT) and the Threat Decomposition tool (TDT), as well as between the TMT and the Capability Management Tool is a key design issue in the TACTICS system. Besides functional and physical interoperability, as discussed in previous sections, data models are needed to ensure that both sides of an interface understand both form and meaning of information. The data interoperability TMT-TDT and TMT-CMT will be performed through a precise design of the data models of each tool along with well defined interfaces between the different tools. The data model interoperability schema is shown in Figure 6.5.

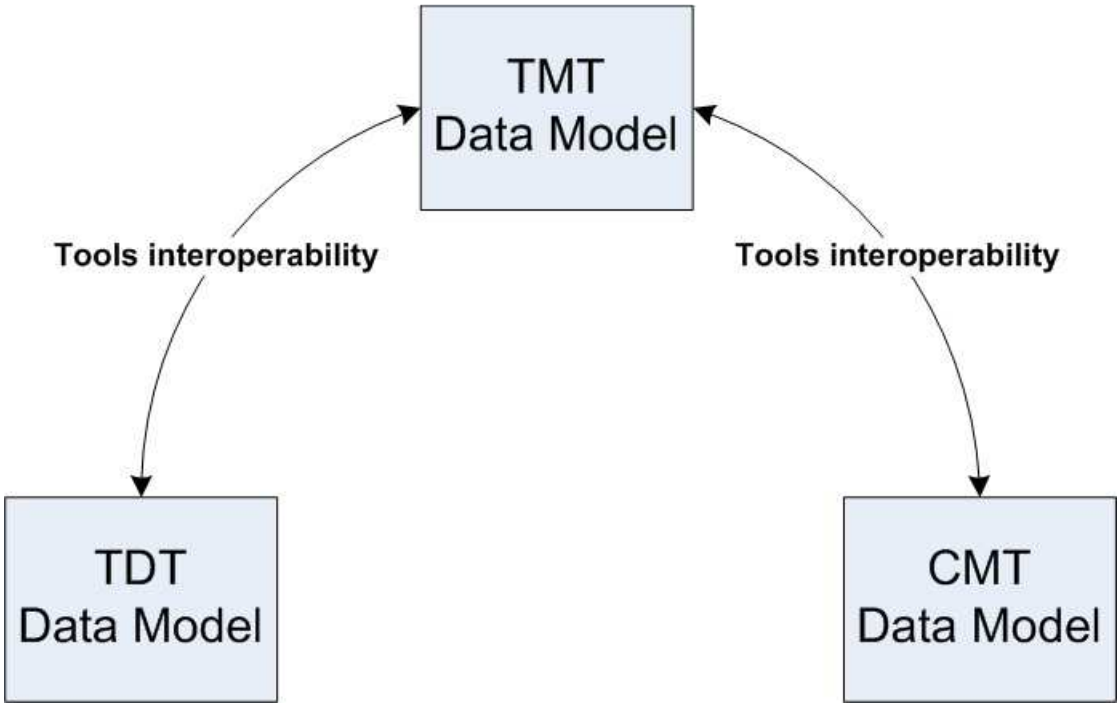


Figure 6.5 Relation between Data Models used in the different tools.

It is critical that the logical description of the data (entities and its attributes), which are susceptible to be exchanged between the different tools, will be the same in the respective data models of each tool.

During the data models developments in WP4, WP5 and WP6, focus will be put on the correct definition of the data that will be exchanged, and the necessary interoperability mechanism for performing the correct data transmission and storage in the different databases of the tools that form the TACTICS system.

7 Human Machine Interface

In this chapter, the human-machine-interfaces of the three tools to the corresponding Managers are described. There are some general considerations about the design of HMIs that are valid for all interfaces. All interfaces have to be:

- Intuitive
- Extremely simple
- Only few clicks to perform tasks

In addition, HMIs can include features to mitigate worries about privacy related issues, for example by providing a pop-up warning when a user is about to do an action or use information that would cause privacy issues under normal circumstances, or by providing visual cues (e.g., a red border, or flashing) when use of certain information sources is allowed, that would not be under other circumstances. The three tools will also have a common look and feel.

7.1 TMT HMI

The TMT will provide an HMI for the TM as manager in charge of the operation.

During the threat facing tasks, the commanders will be cognitively loaded, and under stress and high pressure. Most information shown will be geolocated. Therefore, the main item in the HMI will be a GIS (Geographical Information System) display where relevant items and events in the operation are displayed. Clicking on relevant items shown on the map (for instance a capability such as a video source or a unit in the field) will lead to an extra information display (a small window or a form) to gather information from or to interact with. The user will have access to some function buttons (that can be removed from screen on demand to have a full map view) that will provide access to capabilities such as:

- A module to communicate with units in the field (preformatted messages)
- A module to communicate/interact with TDT and its manager
- A module to communicate/interact with CMT and its manager
- HMI configuration and management
- Filtering of information to be shown: for instance, selection of a subset of some kind of information on file, filtered by some parameter

On the other hand, information from information sources such as units in the field have to be ranked regarding Key Indicators, and this information has to be shown to managers in a very intuitive way. For instance, a possibility is to use colour coding in the GIS, as potential threat representation.

There must be an extremely simple interface for managers to state to the system things like: from now on, I want all the information regarding capabilities ranked (and shown consequently) by cost or by time to deploy.

7.2 CMT HMI

CMT provides with the Capability Management Console an HMI to the Threat Manager and the Capability Managers acting on behalf of the Threat Manager. It's a threefold interface hosting UI components that interface with the core business logic components of the CMT that support managers in finding resources supporting a certain capability, managing and interacting with a resource, and defining capabilities. It consists of the following UI components:

Capability Request UI

- Query interface for defining requests for certain capabilities
- Maintains a request/response cache that allows for asynchronous updates
- Its functionality corresponds to the request-side of the Capability Request Handler service component

Resource Map

- Presents operational resources on a map

- Uses layering for focusing (showing/hiding) on resources of a certain type or that enable a certain capability
- Allows for directly executing actions on resources (e.g. redirection)
- Its functionality corresponds to the response-side of the capability request handler service component

Capability Specification UI

- Administrational interface for defining capabilities with respect to their supposed/expected characteristics
- Its functionality corresponds to the functionality of the capability specification service component

Resource Acquisition UI

- Administrational interface for manually, semi-automatically, automatically integrating resources with the TACTICS system
- Its functionality corresponds to the functionality of the resource acquisition service component

7.3 TDT HMI

The TDT will provide an HMI for managers in charge of threat analysis and decomposition. It has to be a simple tool providing quick access to relevant information, letting managers define queries on the system to refine their analysis.

Therefore, given a particular threat, it has to show all the historical information regarding past events such as other attacks and threats. Basically, it has to show information regarding modus operandi of terrorist groups in similar circumstances and key indicators in the form of (deviant) behaviours that should be detected by the police in order to be able to mitigate the threat. Both sets of information should refer to historical data as well as information processed from the current threat.

In order to achieve this goal, the HMI will provide an interface to require that information and to show it in a textual way. Queries will be inserted in a search bar or form, where the user will insert key words regarding what he is looking for. The HMI will provide users with textual information about their queries on modus operandi and behaviours.

A messaging module will be included in order to provide the interaction and communication with the Threat Manager.

8 Validation data

The validation of the TACTICS system is as realistic as possible. There are however several constraints. Validating a research project with or in the context of a real terrorist threat would lead to security risks. The validation phase of a research project also takes a significant amount of time and effort, which simply cannot be aligned with a real life terrorist threat. In addition, the TACTICS measures are invasive from a privacy point of view, so it should be avoided to test them on innocent bystanders. Finally, a real terrorist threat is unpredictable. TACTICS proposes several innovations with a varying usefulness with regard to a specific terrorist threat. The validation of the TACTICS project should be done with scenario's that are guaranteed to test all relevant contributions from TACTICS.

This leads to several consequences:

1) We cannot use live data from an actual terrorist threat. We can however use historical data from past threats and (mitigated) attacks.
2) We cannot use personal data from innocent bystanders. We can however use personal data from people (staff / actors) in an opt-in setting.
3) We have to create our own scenarios which test all relevant contributions from TACTICS. (D2.3). This starts with a fake intelligence message. (e.g. D3.1 - Appendix B)
4) We cannot use a real city because it would interfere too much with regular urban life. We can however use training-villages in police and defence property.

9 References

[1] Baron, J. (2007). Thinking and deciding (4th ed.). New York, NY: Cambridge University Press.
[2] Cavoukian, Privacy by Design – The 7 foundational principles (August 2009, revised January 2011)
[3] D. J. Solove, "A Taxonomy of Privacy," University of Pennsylvania Law Review, vol. 154, no. 3, pp. 477-564 (Jan. 2006)
[4] D2.1 Urban Factors Overview, 2013, TACTICS Consortium
[5] D2.2 Requirements, 2013, TACTICS Consortium
[6] D2.3 Scenario's, 2013, TACTICS Consortium
[7] D3.1 Conceptual Solution Description, 2013, TACTICS Consortium
[8] Devine, P.G. (1989). Stereotypes and prejudice: their automatic and controlled components. Journal of Personality and Social Psychology, 56, 5-18.
[9] EC, COM(2010) 609 (final), A comprehensive approach on personal data protection in the European Union (November 4th 2010)
[10] EC, COM(2010) 609 (final), A comprehensive approach on personal data protection in the European Union (November 4th 2010)
[11] EC, FP7 Funding Schemes, http://cordis.europa.eu/fp7/ict/future-networks/funding-schemes_en.html
[12] ISCA Company website, Search Detect React®, http://www.isca.org.il/, Accessed February 27th 2013
[13] J Gulliksen, B Göransson, I Boivie, S Blomkvist, J Persson, Å Cajander, Key principles for user-centred systems design, Behaviour and Information Technology 22 (6), 397-409;
[14] K. Burgoon, R. Parrott, B. A. Le Poire, D. L. Kelley, J. B. Walther, and D. Perry, "Maintaining and Restoring Privacy through Communication in Different Types of Relationships," Journal of Social and Personal Relationships, vol. 6, no. 2, pp. 131 -158 (May. 1989)
[15] Langheinrich, Privacy by design—principles of privacy-aware ubiquitous systems, UbiComp2001 (2001)
[16] Lyon, David. 2007. Surveillance Studies: An Overview. Cambridge: Polity Press.
[17] Maier, Mark W. "Architecting principles for systems-of-systems." Systems Engineering 1.4 (1998): 267-284.
[18] Oswald, M. E., & Grosjean, S. (2004), Confirmation Bias, in Pohl, Rüdiger F. (Ed.), Cognitive Illusions: A Handbook on Fallacies and Biases in Thinking, Judgement and Memory (pp. 79–96), Hove, UK: Psychology Press.
[19] Ritchey, Tom. "General morphological analysis." 16th EURO Conference on Operational Analysis. 1998.
[20] Sauser, B., Verma, D., Ramirez-Marquez, J., & Gove, R. (2006). From TRL to SRL: The concept of systems readiness levels. In Proceedings of the Conference on Systems Engineering Research. Los Angeles, CA: CSER.
[21] Schwartz, Paul M.; Lee, Ronald D.; & Rubinstein, Ira. (2008). Data Mining and Internet Profiling: Emerging Regulatory and Technological Approaches.
[22] Serge Gutwirth. *Privacy and the information age*. Lanham/Boulder/New York/Oxford: Rowman & Littlefield Publishers, 2002.
[23] The Open Group Architecture Framework (TOGAF 9.1), Introduction , Section 3: Definitions
[24] University of Bonn – Institute of Computer Science – Communication and Networked Systems, *Definitions of Sensor Data Fusion in the Literature* http://net.cs.uni-bonn.de/wg/sensor-data-and-information-fusion/what-is-it/sdf-definitions/, Accessed January 23rd 2013
[25] Van Rest et al, Requirements for multimedia metadata schemes in surveillance applications for security, Journal of Multimedia Tools and Applications, 2013
[26] W3C consortium website, SOAP definition, http://www.w3.org/TR/soap12-part1
[27] Zimmermann, H., "OSI Reference Model--The ISO Model of Architecture for Open Systems Interconnection," Communications, IEEE Transactions on , vol.28, no.4, pp.425,432, Apr 1980

Annex A – Scenarios

The actual scenario's to be validated will be constructed in WP7. These scenario's serve only as illustration to help guide the design of the TACTICS validation system.

Each scenario has a unique name, and includes a set of preconditions. Scenario's can run in parallel unless they result in an undetermined state for the TACTICS system. All steps in this scenario's are logged for the respective legal investigation. This annex contains these scenario's:

1. Initiating the TACTICS system by the TM
2. Stopping the TACTICS system by the TM
3. The TDM generates new relevant information about the threat
4. The CM responds to a request for capabilities from the TM
5. The TM releases friendly capabilities
6. The TM connects to friendly capabilities
7. The TM receives information from the fusion engine

Scenario 1: Initiating the TACTICS system by the TM
Precondition: TACTICS is not running. The TM has received information about a specific terrorist threat in his urban environment. No attack has happened yet.

1. The TM designates the roles of CM and TDM to two colleagues. He relays the information about the threat verbally to the CM and the TDM and receives first feedback and ideas.
2. Based on this first assessment by the TM, CM and TM, the TM decides to instantiate the TACTICS system. The TMT, CMT and TDT are initiated and filled with the default configurations for the particular city.
3. Based on this first assessment by the TM, CM and TM, using the TMT, the TM does a first request to the CM for specific capabilities.

Scenario 2: Stopping the TACTICS system by the TM
Precondition: TACTICS is running. The relevant authorities have decided that the specific threat is over and / or was based on incorrect information.

1. The TM secures –or lets secure- any data which may be relevant for the respective investigation, including data captured by friendly capabilities, police capabilities and TACTICS system data, including communication logs.
2. The TM releases external friendly capabilities.
3. The TM releaves the CM and TDM from their roles w.r.t. the TACTICS system.
4. The TM shuts down the TACTICS system, which means that the TMT, CMT and TDT are shut down.

Scenario 3: The TDM generates new relevant information about the threat

1. The TDM models the (new) information received from the TM about the specific threat in a morphological analysis (MA). Future updates on this information are also updated in this MA.
2. Based on this analysis an unbiased view emerges of the threat. The TDT generates new hypotheses with links to relevant historical sources.
3. The TDM verifies some sources, and models the new hypotheses in an extended MA.
4. The extended MA is sent to the TMT.

Scenario 4: The CM responds to a request for capabilities from the TM
Precondition: TACTICS is running. The TM decides he needs more capabilities.

1. The TM uses the TMT to formulate a request to the CM for additional (friendly) capabilities.
2. The CM analyses the request using an MA to generate a longlist of hypothetical capabilities which would be fit for the respective purpose.
3. The CM uses the longlist as a search query in the local friendly capabilities. This generates a list with concrete capabilities and respective resources.
4. Based on factors like costs, actual availability, actual location and invasiveness, a filtering and ranking is done on that list. This generates a shortlist.
5. The CM sends the shortlist with capabilities accompagnied with access details (e.g. URL, credentials) and a suggestion for a configuration of the respective resources to the TM using the CMT.

Scenario 5: The TM releases friendly capabilities
Precondition: TACTICS is running. Some friendly capabilities are connected. The TM decides he does not need specific friendly capabilties anymore.

1. The TM uses the TMT to release one or more friendly capabilities.
2. The capabiltiies are released.

Scenario 6: The TM connects to friendly capabilities
Precondition: TACTICS is running. The CM has sent a shortlist with capabilities accompagnied with access details (e.g. URL, credentials) and a suggestion for a configuration of the respective resources to the TM based on an earlier request from the TM.
1. The TM assesses the suggestions from the CM, and decides upon a final configuration of resources.
2. The TM uses the TMT to link to required friendly capabilities.

Scenario 7: The TM receives information from the environment
Precondition: TACTICS is running. One or more capabilities are connected and running.
1. The resources send data or updates of data to the TMT, effectively supporting a capability. This is done through the fusion engine.
2. The TM uses the data to mitigate the threat, which may include give new information to the TDM or changing connected capabilities with the help of the CM.