Tracking the Asymmetric Threat -

Operational Requirements and Technical Solutions for Security Applications

Felix Opitz[1], Kaeye Dästner[2], Thomas Kausch[2]

[1] Defence and Communications Systems
EADS Deutschland GmbH
Wörthstr. 85
89077 Ulm, Germany
felix.opitz@eads.com

[2] Systems for Surface Ships
ATLAS-ELEKTRONIK GmbH
Wörthstr. 85
89077 Ulm, Germany
kaeye.daestner@atlas-elektronik.com
thomas.kausch@atlas-elektronik.com

Abstract: The asymmetric adversary poses a serious threat to civil and military facilities. Hence, the defence against such adversaries, the so-called anti asymmetric warfare, is of interest in various environments: air respectively maritime traffic, air defence, force protection in out of area missions, harbour protection, coastal surveillance, or the security of naval platforms operating in critical environments, like littoral. A vital factor in anti asymmetric warfare is to ensure own information superiority. This leads to new requirements and very new concepts for design, implementation and integration of the information fusion and the visualisation of the results.

1 Introduction

The classical situation of symmetric conflicts is determined by uniformed forces. The utilisation of weapons is assumed to comply with international treaties and conventions and with national laws. All targets one has to fight are assumed to comply with the principles of the laws of armed conflict, which implies requirements for any legal response, e.g.: military necessity, discrimination between civil environment and aggressor, proportionality of response, and minimization of unnecessary suffering.
The tactics are based on military superiority, e.g. high quantity of own entities, mobility, efficiency of weapon systems.

The asymmetric scenario is different to the classical battlefield, e.g. in the following aspects: Here, the objective of an adversary is to create instability using irregular forces. These may include prohibited weapons, improvised devices, the use of civilian facilities and equipment as weapons, or the use of legitimate weapons in an unlawful way. Civilian and protected targets (both inside the conflict area and elsewhere) may be attacked by the adversary if such actions serve his objectives.

The asymmetric adversary may utilise low cost platform and weapons: micro light planes, hang gliders, airliners, divers, mines, UAVs, UUVs, dinghies, car bombs,

bazookas, grenades, artillery fire or snipers. The asymmetric scenario is guided by the willingness to use to advantage irregular forces and unconventional weapons [SAS03].

For legal defence against asymmetric threats information superiority is a vital factor: In general one has to observe complicated situation with numerous involved civil or military entities over a long duration. Only by detection of critical situation at an early stage, one is able to reobtain the own escalation dominance and to fight off such threats by legal response.

Applications may be found in the civil and military area, like air defence systems, air traffic control, force protection in out of area missions, urban surveillance, combat management systems for naval ships, and coastal surveillance and harbour protection.

The answer to these threat scenarios is different. Both, operational concepts and technical solutions have to interlock. Technical solutions address the issues of information superiority and intervention capability by realising situation awareness and decision support even in situations where the operator is under stress [ODK07] .

2 Sources

The information about symmetric as well as asymmetric targets is collected by sensor systems or by other internal and external sources. These may be sensors like primary radar, passive radar, over-the-horizon radar (OTH), secondary radar (IFF), automatic identification system (AIS), electro optical sensors (EO), electronic support measures (ESM), acoustic sensors, seismic sensors, and chemical sensors.

Often it is only a sensor suite which is able to satisfy the information demand with respect to detection, accuracy, coverage, classification, diversity, etc.

3 Tracking

The requirements for target tracking in the anti asymmetric warfare, embracing data association and filtering, are similar to those of the known symmetric world.

Here one has to be able to track dense scenarios consisting of numerous and various participating objects. Asymmetric aggressors may use geographic constraints and civil shields to their own advantage. Further, anti asymmetric warfare has to deal with threats launched from the nearest neighbourhood. Hence short reaction times has to be considered. One has to cover the wide spectrum of possible platforms and weapons usable for asymmetric threats. However, this means that the advanced tracking algorithms which are applied in the symmetric warfare, are also required by the asymmetric one.

4 Classification and Automatic Target Recognition

A more detailed automatic classification of asymmetric platforms is required due to the possible large and different object spectrum. Very applicable for surveillance applications within anti asymmetric warfare is also the automatic detection of people.

Because it is not always possible to keep objects off distance, anti asymmetric warfare has to deal with scenarios consisting of multiple object in the nearest neighbourhood. So advanced recognition techniques may help to distinguish objects in dense scenarios typical for anti asymmetric warfare. Automatic target recognition based on image recognition methods is a benefit and can decrease the load of the operator and increase the situation awareness.

Often a more accurate classification is also necessary to ensure an optimal effector choice against the wide spectrum of asymmetric targets.

In other applications only the correct recognition of targets allows their detection and tracking because of the background clutter.

Hence the classification capability is a technical functionality addressing the requirements of a legal response, like proportionality and discrimination mentioned in the introduction.

Figure 1: Automatic target recognition for various applications.

5 Identification

Identification in anti asymmetric warfare has to ensure to distinguish between civil parties and the adversaries. This seems to be a bigger challenge as in the symmetric situation. Often the knowledge of the platform type doesn't contribute to the identity of the platform. Question and answer systems (IFF) are often not applicable and other identity sources usable in symmetric warfare are also not suitable [KO04].

Often the asymmetric adversary is identified by an assessment of the ongoing situation or by the prediction of this situation into the future. It is the interaction between objects, which characterises the object under observation as a potential origin for an asymmetric threat. Further, the own possibilities for countermeasures has to be taken into account. This means warning or the usage of non-lethal and lethal weapon systems bearing in mind the constraint of legal response. Hence, there is an interlock between the identification, and situation and threat assessment [St05].

However, there is no unique realisation, which automatically covers all aspects of situation and threat refinement. For example figure 2 shows one aspect of a situation refinement in the form of a traffic flow analysis, which studies the trajectories of the different vehicles within a surveillance area and tries to find potential suspect actions.

Figure 2: Traffic flow analysis.

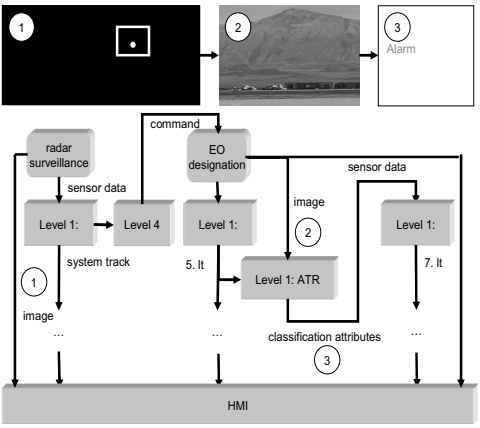

Figure 3: Sensor management.

6 Sensor Management

Another aspect of anti asymmetric warfare is the sensor management. An example specific for anti asymmetric warfare is the data acquisition with various sensor types and data processing techniques.

A possible applications in force protection is, the surveillance of a camp during out of area missions. Here, a radar and electro optical surveillance systems scan a large area around the camp. Whenever a suspicious detection is produced a camera system is used for cueing. Those contacts, which are confirmed by an automatic target recognitions system produce alarms, such that suitable counter measures may be taken (figure 3).

7 Visualisation

Very important for anti asymmetric warfare is the optimisation of the human machine interface and the cognitive refinement, such that operator interaction is supported in an optimal way. The cognitive refinement has to consider the following specifics: focus/defocus of attention, decision support, and representing ambiguous or uncertain data.

Asymmetric threats may happen during peace keeping operations, where the attention of the operator is decreased through long term missions. The asymmetric threat may happen spontaneously and may occur in a civil environment. Therefore, it is important to focus and also defocus the attention of the operator, especially in multi target scenarios.

Also the decision of an operator concerning effector usage may lead to consequences for the civil population, e.g. collateral damage has to be taken into account. Hence, it is difficult for the operator to predict all the consequences of his decisions. Here decision support tools are believed to be helpful.

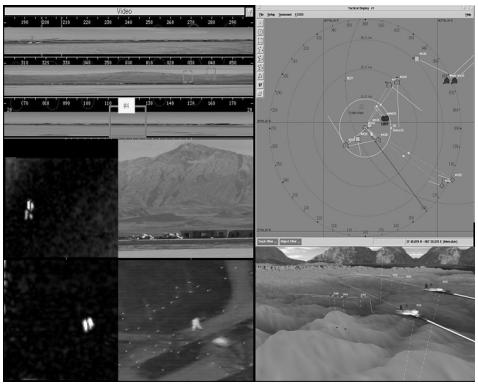

Figure 4: EO sensors and information fusion in force protection application.

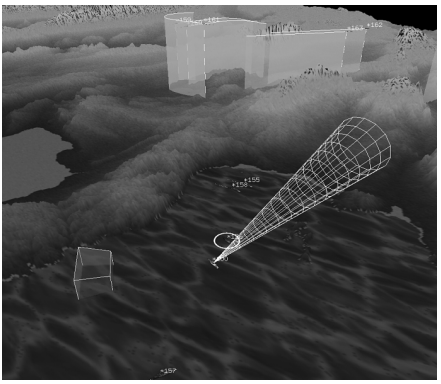

Figure 5: 3 dimensional visualisations with zones of potential collateral damage.

References

[ODK07] Felix Opitz, Kaeye Dästner, Thomas Kausch,: Information Fusion in Anti Asymmetric Warfare and Low Intensity Conflicts. Fusion2007, Quebec, Canada 2007.

[KO04] Thomas Kausch, Felix Opitz: Modern Principles of Identity Fusion, NATO RTA SCI-143 Workshop:Design Considerations and Technologies for Air Defense Systems, Istanbul, Turkey, 12 - 14 October 2004.

[St05] Alan Steinberg: Principles of Situation Assessment, NATO ASI: Multisensor Data and Information Processing for Rapid and Robust Situation and Threat Assessment, Albena, Bulgaria, 16-27 May 2005.

[SAS03] Non-Lethal Weapons and Future Peace Enforcement Operations, NATO RTO Technical Report TR-SAS-040, 2003.