Bayesian Target Identification and Classification: Application of AIS, GMTI and BFT in Command and Control Systems

Albert Bodenmüller(✉)

Airbus Defence and Space GmbH, 89077 Ulm, Germany
albert.bodenmueller@airbus.com

Abstract. The Identification and classification of targets is one of the key capabilities of Ground based C4ISR systems, military Command and Control Systems and Combat Management Systems. It is a precondition for situational awareness and supports operational users in decision making. A correct identification is an important prerequisite to prevent fratricide and civilian collateral damages and to complete the Situational Awareness. Modern Combat Management and Surveillance systems deal with thousands of tracked objects and such an operator is unable to handle the huge amount of targets and data in an operationally acceptable timeline. Therefore an automated identification and classification process is integrated in such military systems. Typical sensors used for this task are radars, IFF and ESM sensors complemented by sources like Tactical Data Links, civil and military Airspace Control Means and flight plans.

In today's naval combat ships and surveillance systems various additional sensors and sources like Automatic Identification System (AIS), Automatic Target Recognition (ATR), GMTI Radar and Blue Force Tracking system are available to support identification, classification and decision making. This paper gives an overview of our solution for the extension of the Bayesian identification process.

Keywords: Military target identification and classification · Situation Awareness · Bayes decision theory · AIS · GMTI · NFFI

1 Introduction

In the first section of this paper the current existing military standard of target identification and classification will be described. This standard fusion process uses Bayes decision theory as described by [1, 2]. It has already been implemented in airborne reconnaissance systems and different naval and ground based Air Defense Systems, but it is not limited to military systems; it may be used for any identification and categorization problem.

Future systems will use the principle also for renegade detection and more granular rating of various kinds of suspicious behaviour. The implementation of this standardized fusion process ensures the comparability of results and the exchange of source data in future.

C. Benavente-Peces et al. (Eds.): SENSORNETS 2017/2018, CCIS 1074, pp. 135–150, 2019.
https://doi.org/10.1007/978-3-030-30110-1_8

Section 2 will give an overview of the principles of Bayesian Fusion for target identification and classification, Sect. 3 will detail the proposed source processing of some non-standardised sensors and sources in a Command and Control (C2) system. The paper describes our approach for some additional sensors which were not yet considered in the identification standard. For each of the described sources the sensor's provided source information and the required data for the processing is indicated.

2 Principles of Bayes Fusion

2.1 Source Processing

The identification process consists of two main processing parts: The first step is a source processing component, which provides the source specific processing, which is unique for each source type (Fig. 1), and the second step is the fusion component, which has the task to combine and fuse all contributing sources of information and to assign the final decision for the identification and classification. Such multiple instances of source processing are implemented (e.g. for each type of sensor or source), whereas one fusion process is sufficient for identification or classification.

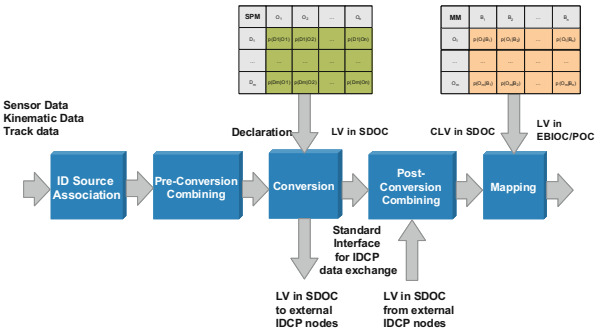

Fig. 1. Identification source processing (from [13]).

Following the flow of information the initial step is to establish an unique association between a sensor or source information and a system track. When no related existing system track can be found, a new track based on the kinematic data of the sensor will be initiated. This will be performed for those sensors or sources, which provide positional and/or kinematic data, e.g. a Blue Force Tracking/Friend Force Information system will normally provide the actual own position information. During this process the results of sensors like Electronic Support Measure (ESM) or Ground Moving Target Indicator (GMTI) Radar including the contributing collateral data is assigned to a track. For many sensors the association process and the pre-conversion combining are an integrated process making a final hard decision, if a source declaration is made or not.

In some cases the periodical association match analysis is input into a pre-conversion combining step, which uses a hysteresis or stochastic mean of several association attempts to make the final declaration hard decision. Also combinations of an integrated process making the association attempts based on a hysteresis function and stochastic output of the result are applied in some systems. The stochastic output finally has to be compared with a threshold for a final hard decision.

The source processing is specific for each kind of sensor and such the determined declarations are not in a form which is appropriate for fusion. Hence they are converted into a Likelihood Vector (LV), which is a set of probabilities related to appropriate types of object classes. The standard proposes for this conversion the application of a Source Probability Matrix, which represents the probability of the source to make these source specific declarations given a known object type. The Source Probability Matrix (SPM) contains for each possible declaration, which can be made by a source, the related likelihoods. Different qualities or confidences related to the association process are considered by different SPMs.

Given a determined source declaration and a priori determined source probabilities in the SPM the conversion step is performed by selection of the related row of the source specific SPM. The result of the conversion step is a Likelihood Vector (LV) in the Source Discrimination Object Class (named LV in SDOC) to which additional collateral information, which is required for the mapping stage, is attached.

The result of this conversion of a declaration D_i is a source specific Likelihood Vector LV_i which can be written in the following way:

$$LV_i = \left(p(D_i|O_1),\ p(D_i|O_2),\ \ldots,\ p\left(D_i|O_j\right)\right) \tag{1}$$

where $p(D_i|O_j)$ denotes the probability of declaration D_i given Object property O_j (from [13]).

The LV in SDOC expresses the performance of that particular source to make this declaration.

There exist also types of sources where the application of pre-calculated SPMs is not suitable. In such cases a dynamic determination of the LV in SDOC may be applied. For instance the dynamic evaluation of Electronic Support Measure sensors (ESM) requires for each emitter and emitter mode an emitter related SPM. This is not feasible in that way. One possibility is to calculate dynamically from the emitter characteristics and comparison with an emitter database the SPM values.

Also for very dynamic sources where the kinematic behaviour of target is compared with extreme kinematic characteristics, a dynamic SPM calculation is the better solution. For instance when the actual target kinematics is compared with operator defined extreme kinematic thresholds the a priori SPM values cannot be pre-calculated, because they change depending on the criteria and target characteristic. This kind of processing requires a specific database and collateral data.

There are different possibilities to exchange identification information between different identifying and classifying systems or nodes. One possibility is to exchange final identification and classification results as this is performed via Tactical Data Links e.g. Link-16 or Link-22. The disadvantage is that only the final result is available such that receiving nodes are not able to assess what the basis of this assessment had been.

Several surveillance systems also use the Variable Message Format (VMF) to exchange tactical data and the situational picture. These systems also have to deal with the disadvantage that only the final decision is available.

So the comparability of final results is often a problem when different systems interact in a joint combined mission. Therefore the exchange of identification source data is preferred. The exchange of Likelihood Vectors or references on harmonized predefined LVs enables a standardized identity information exchange between fusion nodes. By this way the source information and the confidence of the information is transferred, but the information has not yet been interpreted, i.e. the allegiance, the distinction of civil/military targets or the platform data has not been derived.

When more than one sensor or source of the same type (i.e. using the identical SDOC) of either several own sensors or by receiving data from other identification nodes contribute to one track, the combination of these LVs is performed by column wise multiplication in the Post Conversion Combination step according the following formula:

$$CLV = \left(\prod_{i=1}^{N} p(D_i|O_j) \right)_{j=1,\ldots,M} \tag{2}$$

with CLV $= (p(D_{1,\ldots,}D_N|O_1), \ldots, p(D_{1,\ldots,}D_N|O_M))$ (from [13]).

The Combined Likelihood Vector (CLV) is determined by a column multiplication of the single contributing LVs, and is still in form of the source specific SDOC. Such a CLV in SDOC contains the complete information of one source type which contributes to the final result of the identification/classification. But still this first combination/fusion step is in a format which is not suitable for fusion with other source specific information.

2.2 Mapping Processing

A Likelihood Vector or Combined Likelihood Vector in SDOC is a source specific representation of information and such different LVs in SDOC cannot be fused directly without a conversion into a common format. In the Mapping stage the LVs/CLVs in SDOC are mapped in such a common information representation which allows for fusion.

This common information format is called Output Object Class (OOC). The OOC shall be defined according the operational needs to distinguish object categories, e.g. when only a distinction of civil and military targets is needed, the OOC may contain only the members:

- Military Target;
- Civil Target.

When a distinction of basic allegiances is needed the OOC contains for example the members:

- Own Forces (OF);
- Enemy Forces (EF);
- Non-Aligned (NA).

And a basic distinction of air platform categories can be defined for example as:

- FIGHTER;
- BOMBER;
- HELICOPTER;
- UAV;
- AEW AIRCRAFT;
- SAR AIRCRAFT;
- PATROL AIRCRAFT;
- FREIGHT AIRCRAFT;
- GLIDER;
- BALLOON;
- MISSILE;
- OTHER AIR TARGET.

Also combinations of basic OOC for certain applications are reasonable and hence an OOC using members like friendly fighter, hostile fighter, own forces civil helicopter etc. may be used. A very common composite OOC is the Extended Basic Object Class (EBIOC) using the combinations of basic allegiances and civil/military targets, e.g. Own Forces Civil (OFC) and Own Forces Military (OFM). Depending on the discriminating capabilities of the contributing sensors/sources and the user's operational requirements any kind of Platform Object Class (POC) can be defined as OOC for target classification applications. In any case the OOC members shall be mutually exclusive and the OOC has to be exhaustive.

The mapping is calculated according the formula:

$$p_{OOC}\left(D_i|B_j\right) = \sum_{k=1}^{M} p(D_i|O_k) \cdot P_{MM}\left(O_k|B_j\right) \tag{3}$$

where $p(D_i \mid O_k)$ denotes the CLV in SDOC and $P_{MM}(O_k \mid B_j)$ denotes the Mapping Matrix (MM) (from [13]).

The mapping values are stored in a source specific Mapping Matrix, which is defined specifically for each corresponding source type and SDOC. In cases where different operational facts or constraints have to be considered (e.g. a radar may be currently jammed) different MMs can consider such circumstances by different mapping values. After the mapping stage the LV in OOC is normalized and then passed to the conflict detection and fusion process.

2.3 Conflict Recognition on Basis of Source Information

The next step now is to check if there exist source inconsistencies and contradictions. The identification source information after the mapping step is available in a common normalized format which enables the recognition of potentially contradicting information. The inconsistency/conflict recognition is performed in the following way:

When an element of a LV in OOC indicates that one object class is very likely and the same element of the compared second LV in OOC indicates that this object class is very unlikely, this test indicates a possible information inconsistency/conflict.

When an element of a LV in OOC indicates that one object class is very likely and another element of the compared second LV in OOC indicates that this different object class is very likely, this test indicates a further possible information inconsistency/conflict.

Finally an information content distance measure between two LVs indicates a possible information inconsistency when the distance exceeds a certain threshold:

$$d = \sum_{i=1}^{M} |x_i - y_i| \tag{4}$$

where x and y represent the two LVs to be tested (from [13]).

This test makes sense particular for large LVs with many elements. The statistical information distance between two LVs is a measure for inconsistency.

The inconsistency/conflict recognition tests are performed for each combination of two contributing LVs in OOC and the results are summarized for display purposes to the operational user.

Figure 2 illustrates the following processing steps including conflict detection, fusion and final category decision.

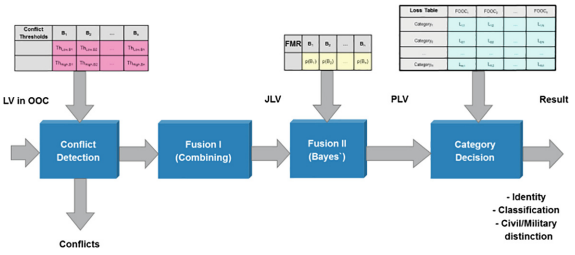

Fig. 2. Bayesian identification fusion and decision (from [13]).

2.4 Fusion

In the first step of the fusion process a combination of all determined contributing LVs/CLVs in OOC is calculated by a component wise multiplication of all contributing LVs, building the Joint Likelihood Vector (JLV). The JLV is a probability distribution over all members of the OOC. The elements of the calculated JLV contain the

probability that a target may have these associated declarations given that the target belongs to that respective OOC (from [13]):

$$JLV = \left(\prod_{i=1}^{N} p_{OOC}(D_i|B_j) \right)_{j=1,\ldots,M} \tag{5}$$

In the second step the Posterior Likelihood Vector (PLV) is calculated from the JLV by application of Bayes' Theorem according the following formula:

$$p(B_j|D_i) = \frac{p(D_i|B_j) \cdot p(B_j)}{\sum_{j=1}^{N} p(D_i|B_j) \cdot p(B_j)} \tag{6}$$

where $p(B_j \mid D_i)$ denotes the PLV, $p(D_i \mid B_j)$ denotes the JLV and $p(B_j)$ denotes the required a priori information called Force Mix Ratio (FMR) (from [13]).

The FMR is a priori information and it quantifies the relative expectation that a member of that object class could be found in the area of interest. When using this processing for target classification analogously a Platform Mix Ratio is required. The elements of the calculated PLV contain the posterior probability that the target belongs to that respective OOC given the considered declarations.

2.5 Conflict Recognition on Basis of Combination/Fusion Result

The declaration combination result JLV can be used additionally to detect possible information inconsistencies.

When an element of the JLV indicates that one object class is very likely and the same element of the a priori FMR indicates that this object class is very unlikely this test indicates a possible information inconsistency.

When an element of a JLV indicates that one object class is very likely and another element of the a priori FMR indicates that this different object class is very likely this test indicates a further possible information inconsistency.

The inconsistency/conflict recognition is performed on each update of the JLV and the result is used for display purposes or alerting the operational user.

Generally it depends on the operational application and required depth of information level, which inconsistency information shall be indicated to an operational user, and if such consistency tests are performed. In larger C2 systems (e.g. frigates) or Command and Reporting Centers (CRC) normally the operator has more time to investigate problematic targets for inconsistencies and his operational task requires as detailed information from the automatic system as possible. But if a similar identification software is running in a small tank or shelter with minimum staff (e.g. 1 to 2 persons) there is no need for such detail of information nor the capability to investigate such cases. Possibly he has only few seconds to decide to execute an engagement of a target and any detail of information delays the decision process.

2.6 Final Identity Decision Process

The PLV contains the fusion result and such it can be displayed to operators to support the further decision process. A final identity decision could be realized by a simple thresholding function based on the most likely element. But usually this result is translated into a recommendation, which regards the user's needs and operational aspects [3]. In the domain of target identification the operational user expects an identity category according to NATO STANAG 1241 or MIL-STD 6016 and a civil/military target assessment. In the case of target classification a platform type or platform specific type according to military Data Link standards STANAG 5516 or STANAG 5522 is required.

The decision process is based on a loss function which uses a set of loss values (see Fig. 3), which define the operational risk when making a wrong decision.

Loss Table	OFC	OFM	EFC	EFM	NAC	NAM
UNKNOWN	$L_{1,1}$	$L_{1,2}$	$L_{1,3}$	$L_{1,4}$	$L_{1,5}$	$L_{1,6}$
ASSUMED FRIEND	$L_{2,1}$	$L_{2,2}$	$L_{2,3}$	$L_{2,4}$	$L_{2,5}$	$L_{2,6}$
FRIEND	$L_{3,1}$	$L_{3,2}$	$L_{3,3}$	$L_{3,4}$	$L_{3,5}$	$L_{3,6}$
NEUTRAL	$L_{4,1}$	$L_{4,2}$	$L_{4,3}$	$L_{4,4}$	$L_{4,5}$	$L_{4,6}$
SUSPECT	$L_{5,1}$	$L_{5,2}$	$L_{5,3}$	$L_{5,4}$	$L_{5,5}$	$L_{5,6}$
HOSTILE	$L_{6,1}$	$L_{6,2}$	$L_{6,3}$	$L_{6,4}$	$L_{6,5}$	$L_{6,6}$
...	...	...	...	...	...	...
KILO	$L_{M,1}$	$L_{M,2}$	$L_{M,3}$	$L_{M,4}$	$L_{M,5}$	$L_{M,6}$

Fig. 3. Identification loss table (from [13]).

The decision process determines for each decision alternative a specific risk value by weighting the loss values of that category (decision alternative) by the posterior probabilities of the fusion result:

$$\text{Risk} = p(OOC_1) * L_{ID,1} + p(OOC_2) * L_{ID,2} + \ldots + p(OOC_N) * L_{ID,N} \quad (7)$$

where $p(OOC_n)$ represents the n^{th} element of the PLV, $L_{ID,m}$ the loss value related to that evaluated identity (ID) and OOC element m (from [13]).

The decision alternative comprising the lowest risk is proposed as final decision result. In those cases were ambiguous risk values prohibit a decision based on the risk values a final decision applying a rule based approach is advised.

If during the identification process additional operationally important information is attained, which is not suitable for fusion but relevant for the decision, this information is incorporated in the decision process. For instance when the operational alert state changes from peace to tension or a target violates a self-defence safety zone this has to be considered for the identity decision. For all these cases a set of dedicated loss tables has to be provided, which contain modified loss values regarding operational facts and target relevant criteria.

3 Novel Source Types for Identification and Classification

The following section describes our solution for some additional sources and sensors which were not yet covered by the identification standard. Hence we enhanced the standard and introduced capabilities like Automatic Identification System (AIS), Automatic Target Recognition (ATR), Ground Moving Target Indicator (GMTI) Radar and Blue Force Tracking systems. For some of these the implemented solution is presented in the following sections. Normally only the source processing has to be extended for new sources, i.e. further SDOCs have to be introduced and additional a priori conditioning data (SPMs, MMs) have to be designed and implemented. The generic approach of combining, fusion, and final category decision is not affected and keeps unchanged as described in the previous chapter.

3.1 Automatic Identification System

The Automatic Identification System (AIS) is originally a radio-based collision avoidance system for ships. AIS has the main requirements to

- Support the avoidance of collisions by enabling an efficient navigation of vessels;
- Support the protection of the environment by providing information about the ship's cargo;
- Actively support Vessel Traffic Systems (VTS) by providing static, dynamic and voyage data.

Besides that port authorities use AIS to warn ships about hazards, low tides and shoals that are commonly found at sea. In open sea AIS-enabled distress beacons are used to signal and locate men who have fallen overboard [5].

Several state-of-the-art surveillance satellites are now equipped with AIS [6], thus the fused information from dual sensors Radar and AIS contributes to global maritime surveillance. But also naval ships like corvettes and frigates are going to exploit received AIS data for the improvement of the maritime picture and tactical situation in real-time. The information extracted from AIS radio broadcast data includes:

- Static ship data: Maritime Mobile Service Identity (MMSI), i.e. the vessels unique identification number, International Maritime Organization (IMO) ship identification number, radio call sign, name of the vessel, type of ship;
- Dynamic ship data: navigation status, position of the vessel, time of position, course over ground, speed over ground, true heading, rate of turn;
- Further voyage data: current maximum draught of ship, hazardous cargo, destination, estimated time of arrival (ETA) at destination.

In a first step the received positional data of a vessel are used for the association of the AIS data with existing system tracks, which is part of the source data association. If no matching system track is available a new AIS based system track will be initiated and the track is updated with the AIS position data.

For the evaluation of AIS data for military target purposes it is important to recognize that AIS message content can be spoofed easily, so that the manipulated result of the data association process or from the information exploitation may be erroneous. Besides the intentional manipulation also any kinds of intentional and unintentional

interference of the AIS signals or the improper setup of AIS devices may cause problems in the evaluation.

The AIS is a civilian system, hence no primary military information is transmitted by default. For military purposes also dedicated variants (NATO STANAG 4668 WARSHIP - AUTOMATIC IDENTIFICATION SYSTEM (W-AIS) and NATO STANAG 4669 - AUTOMATIC IDENTIFICATION SYSTEM (AIS) ON WARSHIPS) exists, which are not handled here in this paper. In order to use the civilian AIS data for military identification and classification purposes a further processing is necessary. In the optimal case a database providing military and intelligence information is available, such that the received AIS data can be compared with it and the stored (military) information can be retrieved to support the tactical interpretation. The database content provides information like ship type, specific type, platform class and platform name, allegiance, civil/military information and of course data like sensor equipment, weapon systems and further tactical intelligence information.

But usually on board of a ship this intelligence database is not available and such a more pragmatic solution was additionally necessary. In this case the broadcasted MMSI number is exploited, because the MMSI number uniquely identifies a vessel. The MMSI is not an identity in the military sense, where a distinction between civil and military objects and the membership to either a friendly, neutral or hostile allegiance is required. Thus the Identification Digit (MID), which is part of the MMSI number, is extracted from the MMSI. The MID is a 3 digit number and defines uniquely the country, where the vessel is registered.

A simple repository then is used to determine the allegiance of the country. A civilian/military distinction is determined from a simple MMSI repository. When this repository information is not available for a received MMSI, the civilian/military distinction is derived from the AIS message content “type of ship”.

AIS is handled as a new source type and hence a new AIS specific SDOC definition and related SPM and MMs were introduced:

- Surface vessel with an operating AIS transponder is sending data ‘x’;
- Surface vessel with an operating AIS transponder is sending data different from ‘x’;
- Surface vessel is not fitted with a transponder or the surface vessel is fitted with an AIS transponder and the transponder is not operating.

The source type AIS provides the following declarations:

- AIS (data) received;
- AIS (data) not received.

The related SPM has therefore the following format as given in Table 1.

Table 1. AIS Source Probability Matrix (from [13]).

AIS SPM	AIS SDOC		
	Fitted and operating sending data x	*Fitted and operating, sending data different x*	*Fitted and NOT operating or NOT Fitted*
AIS received	A	B	C
AIS not received	1-A	1-B	1-C

Such the related Mapping matrices have the following format as indicated in Fig. 4.

AIS MM SDOC → EBIOC	OFC	OFM	EFC	EFM	NAC	NAM
Fitted and operating sending data x	A_1	A_2	A_3	A_4	A_5	A_6
Fitted and operating, sending data different x	B_1	B_2	B_3	B_4	B_5	B_6
Fitted and NOT operating or NOT Fitted	$1-A_1-B_1$	$1-A_2-B_2$	$1-A_3-B_3$	$1-A_4-B_4$	$1-A_5-B_5$	$1-A_6-B_6$

Fig. 4. AIS Mapping Matrix (from [13]).

One problem in the military identification using AIS data arises from the ability to manipulate the transmitted AIS data easily. Additional threats arise from triggering SAR alerts to lure ships into navigating to hostile, attacker-controlled sea space or spoofing collisions to possibly bring a ship off course. Hence a possibility to detect spoofing targets is required [7].

Evaluation of historic satellite AIS data worldwide showed, that more than 30% of AIS data are not quite correct; either due to operating failures, problems with the handling the AIS devices or spoofing.

In our system we implemented a multitude of consistency checks for the AIS data, were we compare the received data with repository and intelligence information for plausibility. When this check indicates a sufficient discrepancy the operator is alerted and he has the possibility either to suppress the generation of a declaration and the usage of the AIS data or to declare this vessel as a spoofing target. This knowledge is then used in the mapping process for the selection of dedicated mapping values for the spoofing case or in the final identity decision processing to assign special identity categories respectively.

3.2 Automatic Target Recognition

For our naval and ground based Command and Control Systems (C2 Systems) we are using (different types of) Daylight/Infra-Red cameras with Automatic Target Recognition (ATR).

ATR has become increasingly important in modern defense systems, because it permits precision strikes against certain tactical targets with reduced risk and increased efficiency [8]. ATR helps to minimize collateral damages to civilian persons and objects (like cars, vessels, planes and buildings). The main advantage is that ATR systems connected and fed by sensors can detect and recognize targets automatically so that the workload of an operator can be reduced and the accuracy and efficiency of the complete C2 System can be improved.

For the detection and recognition of tactical relevant objects and their more or less coarse classification different algorithms are known, e.g.:

- Pattern recognition;
- Detection theory;
- Artificial Neural Network;

- Model-based target recognition;
- Artificial intelligence and model-based methods.

In our system we implemented a combination of model-based target recognition and Artificial Neural Network for detection and classification of target objects. The result of this processing is already in the form of a probability distribution over the discriminated object attributes (object classes), so it can be processed and fused directly in our identification and classification processing.

An interface for sensors and sources, which provide results in a form which is suitable for fusion, has been introduced and allows for the fusion of the image processing result, because the ATR result is already a probability distribution over platform categories, which correspond to a LV in POC (see Fig. 5). The detection of conflicts with other sensor results, the combining, Bayes' processing and final category decision are performed as described in Sect. 2.

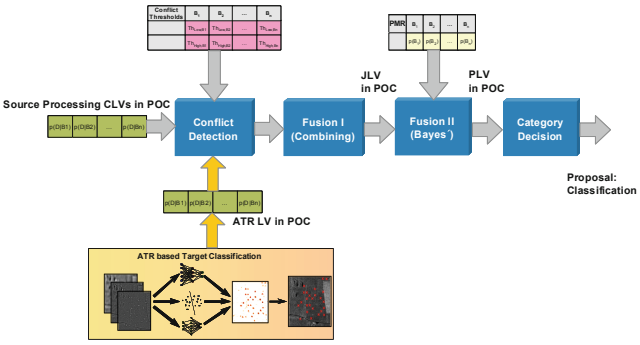

Fig. 5. Extension of Bayesian classification fusion with ATR interface (from [13]).

3.3 Ground Moving Target Indicator (GMTI) Radar

Usually GMTI Radars are mounted on reconnaissance aircrafts and UAV which operate in high altitudes above the normal height of civil aircrafts. The observed area has a large extend and allows for the observation of many ground and maritime moving targets [9].

The NATO Standard Agreement [10] provides a generic and complex GMTI radar interface standard which describes the data encoding. Sometimes problems occur by different interpretation and implementation of the format description and such a robust interface connection is necessary [11].

STANAG 4607 GMTI target reports provide an enumeration field denoting the classification of the target. The classification types include e.g. wheeled vehicles, non-wheeled vehicles, helicopters, fixed-wing air targets, rotating antenna, maritime etc., for both live and simulated targets. Additionally an optional Target Classification Probability (TCP) may be transmitted.

The classification result set is relative coarsely, but it is sufficient to perform a target classification based on it. In order to achieve a good classification result the

interpretation of STANAG 4607 GMTI target report classification and probability results shall be clarified with the vendor such that the GMTI source processing can be optimized for that sensor and the related mapping values can be adapted accordingly.

A pre-conversion is not necessary when the GMTI radar provides the result of the most actual integrated assessment. Otherwise a temporal integration using adequate methods like a hysteresis function or a probabilistic logic using a running mean $p = \Sigma TCP_i/n$, where TCP_i is the received Target Classification Probability, and a threshold function are used to make a declaration.

The integrated assessment is converted into a proper related normalized LV in OOC using the Target Classification Probability for the proper OOC element, the residual R (R = 1-TCP) is equally distributed on the remaining OOC components. The normalized vector is then input into the fusion process analogously to ATR (Fig. 5). In cases where no TCP is transmitted a proxy LV in OOC is determined using experience or analytic measures.

3.4 Blue Force Tracking/Friend Force Tracking Information

For multi-national operations with forces of coalition partners a state-of-the-art Combat Management System requires Network Enabled Capabilities (NEC) for exchange of blue force information to avoid possible blue-on-blue situations. Several incidents during the past NATO missions are pointing out the importance of a positive friend identification and classification to prevent fratricide and fatal collateral damages. Therefore NATO has specified a format for exchange of Friendly Force Tracking (FFT) information of ground targets called NATO Friendly Force Information (NFFI). The specification includes an XML schema to allow the exchange of blue force tracking information using a Web service [12].

The participants in a NFFI network report their position and further information to other units via NFFI message information. The self-generated messages are either encrypted or sent via a secure network, so they are a cooperative source of high confidence.

The information extracted from NFFI data includes as relevant data:

- Positional Data: position coordinates in latitude/longitude/altitude including accuracy data, target speed, bearing, time of measurement, source identifier, reliability;
- Identification Data: identity, classification category encoded as military symbol.

It is important to note, that there are currently specific restrictions and constraints concerning the usage of NFFI, which have to be regarded in the system design and implementation/integration of NFFI:

- Military allegiance: the provided affiliation code, which contains information about the object's hostility, is normally fixed to indication of "friendly" targets, because the usage of NFFI is specified for friendly forces. But there exists no hard restriction thus principally any military allegiance can be derived from NFFI;
- Tactical environment information: the provided Battle Dimension code is usually restricted to ground, since NFFI tracks usually identify mobile objects, in particular land-based objects;

- The track data received by NFFI are non-real-time track data and thus special care has to be taken in the association process.

For association of the extracted FFT data with existing tracks the included positional data and time of measurement is used. Further non-kinematical criteria support the association process.

The military unit symbol code is the main identification and classification information content of FFT.

Taking the specific characteristic of NFFI into account a new FFT specific SDOC definition and a related SPM and MMs were introduced. The SDOC consists of the following elements:

- object is generating this FFT message;
- object is not generating this FFT message (no knowledge, intent or capability).

The source type provides the following declarations:

- FFT message received;
- FFT message not received.

The related SPM has therefore the following format as indicated in Table 2.

Table 2. FFT Source Probability Matrix.

FFT SPM	FFT SDOC	
	Object is generating this FFT message	*Object is not generating this FFT message*
FFT message received	A	B
FFT message not received	1-A	1-B

For each encoded affiliation in the military unit symbol code one related Identification MM is necessary for mapping into the identification related Output Object Class. Such the related Mapping matrices have the following format as indicated in Fig. 6.

FFT MM SDOC → EBIOC	OFC	OFM	EFC	EFM	NAC	NAM
object is generating this FFT message	A_1	A_2	A_3	A_4	A_5	A_6
object is not generating this FFT message	$1 - A_1$	$1 - A_2$	$1 - A_3$	$1 - A_4$	$1 - A_5$	$1 - A_6$

Fig. 6. FFT identification Mapping Matrix.

Analogously for each relevant encoded target category one related Classification MM is needed to map from the SDOC into the POC. The classification related Mapping matrices have the following principal format, depending on the applied Platform Object Class, as illustrated by example in Fig. 7.

FFT MM SDOC → POC	Car	Armoured vehicle	…	Tank	Truck	Train
object is generating this FFT message	M_1	M_2	…	M_{n-2}	M_{n-1}	M_n
object is not generating this FFT message	$1 - M_1$	$1 - M_2$	…	$1 – M_{n-2}$	$1 – M_{n-1}$	$1 - M_n$

Fig. 7. FFT classification Mapping Matrix.

4 Conclusions

In Sect. 2 an overview on the principles of Bayesian identification and classification information fusion has been given. The necessary processing steps like association, conversion, mapping, combining, fusion, Bayesian inference and risk assessment have been detailed.

In Sect. 3 this paper explained further sensor and sensor-like sources which complete the Situation Awareness of Combat Management Systems today. The data provided by AIS is not only a very important source for Vessel Traffic Systems and maritime surveillance but can also be evaluated for an enhanced identification and classification. Also the processing of daylight or infra-red pictures and video applying ATR algorithms supports the object classification. A quite novel information source for Situation Awareness and classification of ground objects is provided by GMTI Radars, which are mounted on reconnaissance aircrafts and UAV operating in high altitudes above the normal height of civil aircrafts. Finally the information provided by Blue Force Tracking/Friend Force Tracking Information system, which may be received via radio communication means or secure networks, is a very valuable cooperative source for identification and classification and means to prevent fratricide.

In our implemented systems we could prove that the identification results were complying with the expectations of the military operators and the adherence of identification doctrines and operational rules succeeds very well. Significant simulation or just real results cannot be published without disclosure of restricted information.

References

1. Desbois, M.: Sensor data fusion & sensor management in the NATO AIR C2 SYSTEM (ACCS). In: RADAR 2009 International Radar Conference, Bordeaux, France, 12–16 October 2009 (2009)
2. Stroscher, C., Schneider, F.: Comprehensive approach to improve identification capabilities. In: RTO IST Symposium on ‘New Information Processing Techniques for Military Systems’, Istanbul, Turkey, 9–11 October 2000, ser. RTO Meeting Proceedings RTO-MP-049. NATO Research & Technology Organization, April 2001 (2000)
3. Krüger, M., Kratzke, N.: Monitoring of reliability in Bayesian identification. In: 12th International Conference on Information Fusion, Seattle, WA, USA, 6–9 July 2009 (2009)
4. Bodenmüller, A.: Method and device for monitoring target objects. Patent application European Patent Office, Pub. No. EP2322949, Publication Date: 09.11.2010, EADS Deutschland GmbH (2010)

5. Balduzzi, M., Wilhoit, K.: A security evaluation of AIS. Trend Micro Forward-Looking Threat Research Team, A Trend Micro Research Paper (2014). https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp-a-security-evaluation-of-ais.pdf
6. Høye, G.K., Eriksen, T., Meland, B.J., Narheim, B.T.: Space-based AIS for Global Maritime Traffic Monitoring. Norwegian Defence Research Establishment (FFI), NO-2027 Kjeller, Norway (2007)
7. Katsilieris, F., Braca, P., Coraluppi, S.: Detection of malicious AIS position spoofing by exploiting radar information. NATO STO Centre for Maritime, Research and Experimentation, La Spezia, Italy (2013)
8. Dudgeon, D.E., Lacoss, R.T.: An overview of automatic target recognition. Linc. Lab. J. **6**(1) (1993). https://www.ll.mit.edu/publications/journal/pdf/vol06_no1/6.1.1.targetrecognition.pdf
9. Austin, R.: Unmanned Aircraft Systems. UAVS Design, Development and Deployment. Wiley, Chichester (2010)
10. NATO STANAG 4607: NATO Ground Moving Target Indicator Format (GMTIF) STANAG 4607 Implementation Guide (2013). http://nso.nato.int/nso/zPublic/ap/aedp-7(2).pdf
11. Dästner, K., von Hassler zu Roseneckh-Köhler, B., Opitz, F.: GMTI radar data analysis and simulation. In: 19th International Conference on Information Fusion, Heidelberg, Germany, 5–8 July 2016 (2016)
12. Porta, R.: Friendly force information sharing, lessons learned and way towards NNEC. In: 7th NATO CIS Symposium, Prague, CZE, 15 October 2008 (2008)
13. Bodenmüller, A.: Bayesian multi-sensor data fusion for target identification. In: 7th International Conference on Sensor Networks, Funchal, Madeira, Portugal, 22–24 January 2018 (2018)