Proceedings of the 2014 ORSSA Annual Conference
pp. 54–61
www.orssa.org.za/wiki/uploads/Conf/2014ORSSAConferenceProceedings.pdf

ORSSA Proceedings
ISBN
978-1-86822-656-6
©2014

Prerequisites for the design of a threat evaluation and weapon assignment system evaluator

ML Truter* JH van Vuuren†

Abstract

In a military air-defence environment, ground weapon systems are responsible for defending assets against hostile aerial threats. To be able to fulfil this purpose, the *weapon systems* (WSs) are equipped with an array of sensors capable of detecting these threats. In this context, the purpose of a *threat evaluation and weapon assignment* (TEWA) system is to provide decision support to human operators tasked with WS assignment decisions, enabling them to make optimal use of the WSs. Such a TEWA system typically assigns appropriate threat values to the threats and then uses these threat values to generate a recommended list of WS assignments in such a way that the cumulative survival probability of the aerial threats is minimised. A large number of TEWA systems are already in use around the world, but due to the confidential nature of this research area, the workings of these systems are typically not available in the open literature. Despite the critical role of these systems in combat situations, there exist no standard methods in the open literature to evaluate the performance of TEWA systems. After briefly describing the subsystems of a TEWA system, various factors that potentially influence the effectiveness of a TEWA system are highlighted, and a methodology is proposed for evaluating the performance of a TEWA system within an integrated simulation modelling paradigm.

Key words: Performance Evaluation, Threat Evaluation and Weapon Assignment, Decision Support, Air-Defence, Simulation.

1 Introduction

On 22 May 2003, a *Royal Air Force* (RAF) Tornado jet was returning to its base when a *United States* (US) Patriot missile wrongly identified the fighter plane as an Iraqi anti-radiation missile. The blue-on-blue[1] confrontation which followed resulted in the US Patriot missile destroying the RAF Tornado [3].

During the build-up to this event, the Patriot battery crew were monitoring for Iraqi ballistic missiles when the Tornado plane was identified by their system. The symbol

*Department of Industrial Engineering, University of Stellenbosch, Private bag X1, Matieland, 7602, Republic of South Africa, email: 16057694@sun.ac.za

†**(Fellow of the Operations Research Society of South Africa)**, Department of Industrial Engineering, Stellenbosch University, Private Bag X1, Matieland, 7602, South Africa, email: vuuren@sun.ac.za

[1]Synonymous with friendly fire — an inadvertent firing toward one's own or otherwise friendly forces.

which appeared on the radar corresponded to that of an anti-radiation missile. To confirm the Patriot system's threat evaluation result, the radar track was interrogated for IFF[2], but no reply was received. After meeting all the criteria laid out by the specific rules of engagement, the Patriot crew engaged in self-defence action by destroying a friendly aircraft.

Several possible causes of this accident have subsequently been identified. The investigation board concluded that the rules of engagement were not robust enough to prevent blue-on-blue confrontations. In addition, the Patriot crews were trained to identify and react quickly, engage early and to trust the Patriot system. The problem with the training was that it focused on identifying generic threats rather than those specific to the Iraq conflict, and also not on identifying false alarms. After detailed investigations, the board concluded that both the operator training and the Patriot firing doctrine were factors contributing to the accident [3].

In this paper we advocate that perhaps the most effective way of preventing the reoccurrence of such a *threat evaluation and weapon assignment* (TEWA) decision support malfunction, is to develop a simulation model for testing the performance of the system with respect to different scenarios, thereby identifying potential system errors before commissioning the system. In the above accident, a scenario generation approach could have identified the flaws in the Patriot system's threat evaluation algorithms, making it possible to take corrective action. Since lives are at stake, it is clearly of critical importance that the performance of a TEWA system be thoroughly evaluated before commencing its industrialization phase.

This paper is structured as follows. A brief overview of the working of a TEWA system is given in §2, with a focus on the three core elements of the system: threat evaluation, weapon assignment and decision support. Thereafter, the importance of, and difficulties associated with, the performance evaluation of TEWA systems are elucidated in §3. Four TEWA performance metrics are proposed in §4. The paper concludes with some suggestions for possible further work related to the performance evaluation of TEWA systems. The research detailed in this paper is a report on work in progress. The methodology proposed forms part of an ongoing research project in which instances of a TEWA system will be simulated and evaluated, resulting in the identification of possible limitations and conflicts present in the algorithms employed by the system.

2 Current State of GBAD TEWA Systems

Several TEWA *decision support systems* (DSSs) are in use around the world, but the inner workings of these systems are typically classified [11]. The majority of TEWA systems are used on naval craft in a point-defence[3] role, while TEWA in a *ground-based air defence* (GBAD) environment requires the adoption of an area-defence[4] paradigm due

[2]Identification: Friend or Foe.

[3]Point-defence applied to the defence of a single entity; stationary or moving.

[4]Area-defence entails the protection of an area, possibly containing numerous DAs spread across the area.

to the potential spatial distribution of a number of prioritized *defended assets* (DAs) on the ground [11].

The *weapon assignment* (WA), *threat evaluation* (TE), and *human machine interface* (HMI) subsystems are three key constituents of any TEWA DSS. In order to simulate a complex TEWA system in detail, a model replicating all the formative elements (enemy aircraft, WSs, sensors, DAs and decision support modules) is required [10]. To further complicate matters, the environment in which a TEWA DSS operates, typically includes continual, dynamic and several non-linear interactions between the formative elements (feedback, looping and sudden changes are common). Furthermore, all these elements are influenced by one another, giving rise to various emergent properties of the system[5] and thus making it infeasible to test a TEWA DSS in a reductionistic manner.

2.1 The Threat Evaluation Subsystem

The TE process requires input data from ground radars and associated sensors. These sensors are responsible for detecting, tracking and identifying potential threatening aerial vehicles [4]. The TE subsystem utilizes the kinematic, tracking and attribute data collected from the sensors to estimate the level of threat posed by each aerial vehicle. During this process, a threat value is assigned to each threat-DA pair. Different measured attributes are taken into consideration when determining these threat values. These attributes can be subdivided into three classes:

Proximity parameters quantify the distance between a threat and a DA. Hence, a threat that is far away from a DA will not be classified as an imminent threat to that DA, when compared to threats that are close to the DA. A widely used example of such a parameter, is the range to the *closest point of approach* of a threat with respect to a DA [10].

Capability parameters attempt to quantify a threat's ability to cause damage to a DA. To calculate this value, it is required to know specific characteristics of the attacking aircraft. Examples of capability parameters include the threat type, its weapon envelope and its fuel capacity.

Intent parameters aim to quantify the will and determination of a threat to cause damage to a DA. Of these three parameter classes, intent is the most difficult type of parameter to estimate, but certain measured threat attributes can be used to estimate a threat's intent [11]. One method in which intent is estimated is through recognition of known attack manoeuvres from an aircraft's measured track.

A number of different algorithms of varying complexity and sophistication typically run concurrently in the TE subsystem, each assigning threat values to each threat-DA pair. This results in several threat values for each threat-DA pair. In the case where certain necessary sensor data are not available, the TE system will select scaled-down TE models

[5] *Emergent properties* are defined as those properties that derive from the interaction of the elements in the system, but cannot be reduced to them [2].

which are able to estimate threat values in the absence of very detailed threat data [8]. The different threat values for each threat-DA are then fused together to obtain a single prioritised list of threat values (*i.e.* a threat value for each threat-DA pair, typically found on a consensus basis, taking into account the results contributed by all the TE models) [8]. These threat values are used by the WA subsystem in a bid to optimise the utilization of available resources (WSs and ammunition) when weapon assignment decisions are made for engaging the aerial threats.

2.2 The Weapon Assignment Subsystem

Weapon assignment is the process of reactive allocation of weapon resources (ammunition and WSs) to counter identified threats [5]. The WA subsystem of a TEWA DSS is responsible for proposing high-quality assignment proposals of available ground-based WSs to engage aerial threats over some specified time frame [7].

Before high-quality assignments can be proposed by the WA subsystem, an operator is required to select a set of objectives that have to be optimised during weapon assignment. Lötter and Van Vuuren [7] have suggested a suite of objective functions that may be used in WA algorithms, including the minimisation of threat survivability, the minimisation of overall assignment cost and the maximisation of re-engagement opportunities (available ammunition after the engagement). Because of the typically short time frame over which decisions have to be made, the solutions generated by the WA subsystem are not always optimal; sometimes locally optimal solutions are generated. For this reason, meta-heuristic optimisation techniques are usually preferred over exact ones in a TEWA DSS [7].

The WA process usually employs different algorithms running concurrently, because certain algorithms may perform better than others under certain conditions [8]. The resulting algorithmic outputs are then fused together to obtain a single (approximately) Pareto-optimal solution front in the combined objective space. The operator can then select a specific solution from this front, depending on the situation and his/her preferences. The *fire control officer* (FCO) is presented with the Pareto-optimal solutions through an HMI, and can use this interface to interact with the WA suggestions in order to gain more clarity on the reasoning behind the WA decision suggested by the TEWA system.

2.3 Communicating Decision Support to the Operator

It is ultimately a human operator who decides whether and how each aerial threat should be engaged — not a fully automated system — because decision making in a GBAD environment can have severe (possibly catastrophic) consequences if inappropriate decisions are made, as described in the introduction. Hence, it is of utmost importance to ensure that the decision support information communicated to the human operator is as clear and uncluttered as possible. By so doing, the human operator is afforded the opportunity of effectively making use of the data for the purposes of analysis, interpretation and decision-making.

The form of decision making explained above is a highly complex task and requires the integration of various data sources [6]. To succeed in this highly stressful and dynamic decision making environment, it is required that the FCO should possess a high level of tactical expertise and knowledge of the type of threats, prevailing legal frameworks and assessment heuristics from experience [1]. Training and experience are, however, not enough to ensure tacit decision making. According to Morrison *et al.* [9], the importance of ensuring that information is meaningful, timely and easily accessible cannot be underestimated.

3 Performance Evaluation of TEWA Systems

Testing and evaluation is an iterative process of performance measurement, correction of deficiencies and remeasuring of the resulting performance. This testing process should commence as early as possible in the design process and should be conducted throughout system development [2]. The main purpose of testing a TEWA system is to identify general design deficiencies and specific conflicts present in the internal algorithms of the system, thereby highlighting required corrective action. By following this bottom-up testing approach, it is possible to reduce the risks associated with the final commissioned system. According to Sparrius [13], the only way to demonstrate risk reduction, as a prerequisite for an increase in resource commitment, is through testing and evaluation.

As is the case with many modern systems, the evaluation and design of a TEWA system is highly complex because of the magnitude of the system and the complexities of all the subsystems involved. A TEWA system's performance depends sensitively on the synergies between its subsystems, which gives rise to the emergent properties of the system (see §2). These emergent properties cannot be accounted for by individually testing the WA and TE subsystems, because such an approach will not enable one to assess whether the entire TEWA system will function as expected. To effectively test such a TEWA system, a *system-of-systems* (SoS) approach is required. Proper SoS engineering entails the allocation of functionality to components as well as inter-component interactions, rather than only focussing on the workings of individual components. SoS engineering is very powerful in terms of exploiting synergies between subsystems and in identifying capabilities that no standalone system testing can provide [12].

The preferred method of ensuring that a TEWA system is fully functional is through conducting full-scale flight tests. However, the complex nature of a TEWA system and the high cost of such an approach, makes it intractable to run flight tests for the purposes of system evaluation. In addition, flight tests alone do not provide insight into scenarios that were not actually tested. Because of the confidential nature of this research area, historical data on flight tests, from which system designers can gain insight into the performance characteristics of existing TEWA systems, are very rare. System designers are therefore forced to utilise modelling and simulation tools to evaluate the performance of TEWA systems.

4 Possible Performance Evaluation Metrics

In this section we propose the use of four performance metrics when evaluating the performance of a TEWA DSS within a simulation modelling paradigm. These metrics may serve as both *absolute* and *comparative* evaluation measures in the sense that the value of a metric may quantify the suitability of assignments proposed by a TEWA DSS in a specific scenario in absolute terms, but may also be used to identify limitations present in its constituent algorithms by comparing the metric values for different scenarios in a relative manner. By evaluating the metric values of different scenarios, it should be possible to determine the conditions under which the algorithms behave poorly. Finally, these metrics can be used to perform a sensitivity analysis with respect to the implemented algorithms, thereby providing valuable insight into the functioning and limitations of the TEWA system as a whole.

There is often a misconception about the term *performance metric*. A metric is a standard definition of any measurable quantity, while a performance metric goes further by gauging some aspect of a system's performance. For a performance metric to be successfully utilized, it must adhere to certain requirements — evaluating a performance metric should be achievable in a reliable, repeatable and consistent manner, independently of the pressure to drive performance.

The main role of the WSs in an air-defence scenario is to protect the DAs. Therefore, *survivability* is an important criterion for measuring the performance of a TEWA system. Johansson [5] suggested the use of the survivability metric

$$S = \frac{\sum_{j=1}^{D} \omega_j u_j}{\sum_{j=1}^{D} \omega_j}, \tag{1}$$

where D is the number of DAs in a simulation performance evaluation environment, ω_j is the importance value associated with DA j, and u_j is a binary variable which assumes the value 1 if DA j survives, and the value 0 if it is destroyed by an aerial threat. Hence, the survivability S is the ratio between the protection value of surviving assets to the total protection value of all the assets.

The metric in (1) does not penalise the engagement of superfluous aircraft as unnecessary engagements. The introduction of an *economy* metric may, however, account for the cost of engagement by each WS — thereby penalising unnecessary engagements. The economy metric

$$M = \sum_{i=1}^{W} \left(C_i \sum_{j=1}^{T} x_{ij} \right) \tag{2}$$

is proposed for this purpose, where C_i denotes the cost of one burst or round of ammunition for WS i, x_{ij} is the number of times WS i engages threat j, and W and T are respectively the number of WSs and threats. Hence, the economy metric M represents the total WS capital expenditure, based on ammunition used, associated with an engagement strategy.

It is preferable to destroy high-value aerial threats, especially in an ongoing conflict. In this context the value of an aerial threat may be interpreted as its ability to cause considerable damage to important classes of DAs. Our next metric, *engagement effectiveness*, is designed to reward the successful engagement of high-value threats. The value of a specific aerial threat may be determined during the pre-deployment phase of a mission and programmed into the TE subsystem. As stated above, it is desirable from an economic point of view not to engage superfluous targets. During an ongoing conflict, however, it may be beneficial to destroy these high-value threats even if they do not pose an imminent danger, in a bid to ensure that these threats do not return to attack DAs in the future.

Furthermore, a critical performance-related problem is the engagement of friendly and/or civilian aircraft (see §1). The engagement effectiveness metric may also be used to penalise friendly engagements by assigning a large negative importance value to friendly and commercial aircraft. In this way, friendly engagements can be heavily penalised. The engagement effectiveness metric is given by

$$E = \frac{\sum_{j=1}^{T} \nu_j e_j}{\sum_{j=1}^{T} \nu_j}, \tag{3}$$

where ν_j denotes the importance value associated with destroying threat j and e_j is a binary variable assuming the value 1 if threat j is destroyed, or the value 0 if the threat survives. The value of ν_j may be interpreted as the perceived value that the enemy is most likely to assign to an aircraft — the more important the aircraft, the higher the value. The engagement effectiveness E is the ratio of the importance value of destroyed threats to the total importance value associated with all threats encountered throughout the engagement.

Our final metric attempts to quantify the *adaptability* of a specific engagement strategy. This metric is given by

$$A = \min_i \left\{ A_i - \sum_{j=1}^{T} x_{ij} \right\}, \tag{4}$$

where A_i denotes the initial amount of ammunition available to WS i and the rest of the parameters have the same meanings as before.

The metric A is designed to measure the propensity of an engagement strategy to maximize the number of times that a WS is available for re-engagement after the proposed assignment, thereby ensuring that as many WSs as possible are reusable in future engagements. By using ammunition more effectively during an engagement, WSs on the ground will be more adaptable to changing conditions, such as responding to newly detected threats and performing follow-up engagements.

In addition to the above metrics, certain other parameters also need to be considered to ensure a successful TEWA system. These include the time required to generate WA allocation suggestions and the memory storage requirements of the internal algorithms of the system. Indeed, it is important to ensure that the FCO has enough time to utilize the results generated by the WA subsystem. Also, depending on the environment in which the TEWA system is implemented, there might be memory restrictions. There is often a trade-off between the time complexity and memory complexity of an internal TEWA algorithm — increased memory consumption normally leads to faster execution times, and *vice versa*.

5 Further Work

As stated in §1, the work detailed in this paper is a report on work in progress. The performance prerequisites detailed here will be used during the planned evaluation of a developed TEWA DSS as part of a larger, ongoing research project. Numerous scenarios will be generated by using commercially available simulation software, in order to test the performance of the system's internal algorithms under a variety of conditions. The metric values (1)–(4) will be calculated for each of these engagements in a bid to quantify the relative and absolute performance of the algorithms in each scenario. The results will make it possible to gain insight into the operation of the TE and WA processes and make it possible to identify limitations and internal conflicts, and to clarify possible improvements to the system.

References

[1] Cohen MS, Freeman JT & Thompson BB, 1997, *Integrated critical thinking training and decision support for tactical anti-air warfare*, Proceedings of the 1997 Command and Control research technology symposium, Arlington (VA).

[2] Danzig B, 2010, *Systems engineering handbook: A guide for system life cycle processes and activities*, 3rd Edition, International Council on Systems Engineering (INCOSE), San Diego (CA).

[3] Directorate of Air Staff, 2004, *Aircraft accident to royal air force tornado GR MK4A ZG710*, (Unpublished), Technical Report, Ministry of Defence, London.

[4] Heyns AM, 2008, *Measuring the threat value of fixed wing aircraft in a ground-based air defence environment*, MSc Thesis, Stellenbosch University, Stellenbosch.

[5] Johansson F, 2010, *Evaluating the performance of TEWA systems*, PhD Dissertation, Orebro University, Kållered.

[6] Liebhaber MJ & Feher B, 2002, *Air threat assessment: Research, model and display guidelines*, (Unpublished), Technical Report, DTIC Document.

[7] Lötter DP, Nieuwoudt I & van Vuuren JH, 2013, *A multiobjective approach towards weapon assignment in a ground-based air defence environment*, ORiON, **29(1)**, pp. 31–54.

[8] Lötter DP & van Vuuren JH, 2013, *Weapon assignment decision support in a surface-based air defence environment*, Military Operations Research, Submitted.

[9] Morrison JG, Kelly RT, Moore RA & Hutchins SG, 2012, *Tactical Decision Making Under Stress (TADMUS) Decision support system*, Proceedings of the 1997 IRIS National Symposium on Sensor and Data Fusion, MIT Lincoln Laboratory, Lexington (MI), p. 17.

[10] Roux JN & van Vuuren JH, 2008, *Real-time threat evaluation in a ground-based air defence environment*, ORiON, **24(1)**, pp. 75–101.

[11] Roux JN & van Vuuren JH, 2007, *Threat evaluation and weapon assignment decision support: A review of the state of the art*, ORiON, **23(2)**, pp. 151–187.

[12] Sommerer S, Guevara MD, Landis MA, Rizzuto JM, Sheppard JM & Grant CJ, 2012, *System-of-systems engineering in air and missile defence*, Johns Hopkins APL Technical Digest, **31(1)**, pp. 5–20.

[13] Sparrius A, 2014, Private Owner: Ad Sparrius System Engineering and Management (Pty) Ltd., [Personal Communication], Contactable at `ad_sparr@iafrica.com`.