Published online before print February 15, 2011, doi: 10.1177/1548512911398679
The Journal of Defense Modeling and Simulation: Applications, Methodology, Technology, October 2011 vol. 8 no. 4 225-244, http://dms.sagepub.com/content/8/4/225

Simulator-defined Radar Countermeasure System (Sim-dRCS) Proof of Concept for Deception in Air Defence at Sea

Theodoros G. Kostis
Dept. of Information & Communication Systems Engineering,
University of the Aegean, Karlovassi, Samos 83200, Greece.
{tkostis@iee.org, http://www.tkostis.gr}

Konstantinos G. Galanis
Services in Informatics and Organization,
Ethnodata S.A.,178 Kifisias Avenue, Halandri 15231, Greece.
{kgalanis@aegean.gr}

Nikitas V. Nikitakos
Dept. of Shipping Trade and Transport,
University of the Aegean, 2A Korai Street, Chios 82100, Greece.
{nnik@aegean.gr}

Ioannis A. Koukos
Dept. of Combat Systems, Electronics & Telecommunications
Hellenic Naval Academy, Hatzikiriakeio, Piraeus 18539, Greece.
{koukos@snd.edu.gr}

Keywords: Simulators, Inverse Synthetic Aperture Radar Countermeasures, Systems Engineering.

ABSTRACT

Modern air defence at sea doctrines need to consider the emerging technology of software-defined radar. In this manner the surveillance and tracking abilities of imaging radar are implemented in software. Concurrently there exists the need to forge the other side of the same coin. The devise of a Software-defined Radar Countermeasure System (S-dRCS) might be a solution for confusing adversary radar operators. In this spirit the current contribution is the proof of concept for an S-dRCS special case called Simulator-defined Radar Countermeasure System (Sim-dRCS). The simulator approach for imaging radar countermeasures is preferred because it provides a bespoke generation of the required signals valid for a diverse set of adversary observers which are considered to be Inverse Synthetic Aperture Radar (ISAR) systems. The simulator receives input from the sensors of the Sim-dRCS and then crafts false targets matched to the heading and velocity vectors of the threat. In this case the countermeasure output is a battleship-class false naval target. The achievement of verisimility enhancement is the main requirement in order to support this deceptive stratagem.

1.0 INTRODUCTION

In October 1942 *Operation Bertram* was the code name signifying the acts of deception practiced by the Commonwealth Forces in the waiting period before the second and final battle of El Alamein in North Africa. The stratagem consisted of confusing the *Axis High Command (Oberkommando der Wehrmacht)* about the exact time and place of the forthcoming conflict. Specifically plywood frames looking like tank turrets and upper chassis were placed over lorries so to constitute false tank targets in the southern theatre. And the actual tank force in the north was disguised as supply lorries by placing over again suitable sun-screen superstructures [1], as shown in **Figure 1**. The act that increased the verisimility of this ruse of war was that the lorry tracks were substituted for tank tracks by hauling a caterpillar tractor and that the tanks never left any traces because they were carried over lorries [2], as shown in **Figure 2**. Therefore increasing the verisimility of an act of deception is an integral factor in its mission to vanquish an adversary by stratagem.

Print ISSN: 1548-5129 - Online ISSN: 1557-380X

Yet another factor played a more important role that forged the final fate of the North African campaign. Since the *First World War* it was known that a ship is the most difficult man-made target to hide [3]. And the *Afrika Korps* relied on convoys from Italy in order to obtain their most needed supplies. Those *Axis* cargo ships could not easily hide and were primary targets for the *Royal Air Force (RAF)* which attacked from airports in Malta and Egypt. As a consequence those *RAF* attacks created an insurmountable logistics problem to *General E. J. Rommel* since more than half of his mostly needed oil, armoury and rations did not reach their destination at the port of Tripoli [4]. At the same time even the Allies did not remain unaffected by this issue, as was proven by the heavy losses incurred to the *Pedestal Convoy* bound to support the besieged island of Malta [5]. Therefore this influential factor was the problem of naval camouflage.

The introduction by the Allies of a new technology in 1941 named *RADAR*, for Radio Detection and Ranging, made *Axis* shipping even more vulnerable to attack [6]. The foundational technology of such a conventional radar system was its ability to see through night time, smoke screen and far distances. Nowadays radar has truly evolved. Advanced high range resolution radar systems, especially Inverse Synthetic Aperture Radars (ISAR), can provide extended information about a naval target [7]. But the most important quality is that ISAR systems cannot be barrage jammed like conventional radar [8]. Barrage jamming is when noise is indiscriminately broadcasted in the full spectrum of the complete frequency bandwidth. Therefore the task of preventing the clear reception of an ISAR system is very difficult. On the other hand a probable countermeasure route might be the task of interfering with the reception of such a system.

The deduction from the above discussion is that a naval target is one of the most difficult targets to hide and that ISAR systems are very difficult to be jammed. Nevertheless a solution for the disguise of naval targets from adversary imaging radars is still pending. Now stems the idea that the concept of verisimility might be employed in order to hide a naval target from those prying imaging radar eyes.

The operational theatre for this prospective application is the field of modern air defence at sea which will be analysed in the next chapter. This analysis will pave the road for understanding the application of verisimility enhancements for deception in ISAR imaging. This will result in the forging of the Simulator-defined Radar Countermeasure System (Sim-dRCS) concept which generates false ISAR images of naval assets in order to provide security by creating something out of nothing [9]. Then the main contribution of this paper will focus in the explanation of the relevant Sim-dRCS proof of concept that will display the foundations of operation for this device. Sample results will be depicted for two characteristic scenarios in air defence at sea. Overall the simulator approach is beneficial because it can provide these false ISAR images in a quick, bespoke and realistic manner to each particular threat in real time and this is the major operational requisite for this application.

2.0 AIR DEFENCE AT SEA AS AFFECTED BY ISAR TECHNOLOGY

The principal threat to a naval target is the subsonic or supersonic missile in air defence at sea. A naval platform is directly confronted with these formidable and lethal threats in the modern battlespace. Especially in the condensed littoral and archipelagos areas of the Aegean Sea a ship can be overwhelmed with saturation or barrage types of aerial attacks with highly catastrophic consequences [10]. Such a remarkable modern airborne aggressor platform equipped with an ISAR system is the *Sukhoi PAK FA T-50* fifth generation fighter aircraft, as can be seen at http://www.paralay.com/pakfasu.html, accessed on the 24th of February, 2010. Its on-board ISAR system is attached to an active electronically scanned array antenna that provides advanced surveillance abilities. Because there are no mechanical parts required in order to steer the radar beam into different areas of the target but all these tasks are performed electronically [11].

A fundamental ISAR imaging technique is called *Range-Doppler* and is capable of generating two-dimensional images of such a moving naval target. The method employed is the ability of the radar to distinguish superstructure features using many resolution cells that are shorter than the overall size of the naval target. When this happens a target is called *extended*. Moreover the extended target's angular movement ψ, as shown in **Figure 3a**, is a prerequisite for ISAR because this motion provides the advantageous ability of enhanced imaging. The dual of ISAR is called focused spotlight synthetic aperture radar [12]. In this mode the high resolution of the image corresponds to an antenna array of equal size to the travelling distance of the radar while its beam is always focused at the same location [13], as seen in **Figure 3b**. This duality is mentioned because it helps to explain the ISAR operational principle [14].

Technically ISAR systems employ the concept of coherence which means that the phase or frequency information of the return echoes are processed together with the amplitude of the return signal [15]. This enhanced reflectivity information is handled by a digital signal processor. In this manner classification and in some cases even identification information about a naval target can be provided. When such a naval target is accounted as hostile and the prevalent rules of engagement dictate that it must be fired upon this ISAR system can double as a fire control system. Then for example the *T-50* would direct multiple *Zvezda Kh-35 (NATO SS-N-25 Switchblade or Harpoonski)* subsonic anti-ship missiles to identified as hostile naval targets. Therefore ISAR systems provide accurate and timely enhanced knowledge about the position and movement of the opposing forces. And this task is necessary for effective air attacks at sea, as stated by [16].

In contrast conventional radar would see the same naval targets as point reflectors and simply depict spots on the radar screen. In other words no further information about the target's spatial extent would be available for a positive *IFF* (Identification Friend or Foe) decision. Efficient conventional countermeasures have already been developed for this point reflector technology. A well-known example is the cross eye method where a missile is slowly diverted from its course by gradually injecting a small amount of radar tracking error. Still the most important element in air defence at sea is the ability to hide the friendly naval target. Because when a naval target is discovered it may not be possible to effectively respond to a stealthy subsonic missile threat, as in the Argentinean *Exocet* missile against the *HMS Sheffield* destroyer incident in the Falklands War [17].

2.1 Jamming and False Targets as ISAR Countermeasures

Countermeasures developments for imaging radar are different than for conventional radar. For example [18] have researched the effects of ISAR jamming on an aircraft target. Although there is a considerable form of distortion the general form of the aircraft is evident. Then there is the concept of generating multiple false targets. This is a major building block in the field of modern electronic warfare. And a software architecture approach is a promising implementer for this type of application. For example [19] have implemented a false aircraft generator using an algorithm thus requiring less hardware in the form of supportive integrated circuits. Nevertheless the false targets appear in a regular horizontal form to each other having the same slant range coordinates in the ISAR image. This fact might induce suspicions to an adversary radar operator about the validity of this contact.

Nowadays miniaturized high resolution sensors are available and complete radar systems can be hosted on small footprint FPGA (Field-Programmable Gate Array) technology. For example such miniature sensors on board an UAV (Unmanned Airborne vehicle) and a missile platform could provide feedback to the adversary radar operator in real-time while keeping the overall cost low. The same technology is used for a small form factor decoy system. This battlespace scenario is depicted in **Figure 4** and will be further discussed in this paper. An example of this technology for ISAR countermeasures is the digital image synthesizer application-specific integrated circuit by [20]. However this approach is dependent on hardware therefore it might be difficult to add effects that

agree with the prevalent situational awareness conditions of a real encounter.

The ultimate effort is to achieve a flexible platform that can produce false targets that coincide with the real time or situational awareness actual parameters of the battlespace. And this review of technologies and strategies of modern warfare systems for air defence at sea paves the way for the exploration of ISAR deception based on verisimility levels using a simulator subsystem.

3.0 VERISIMILITY FOR DECEPTION IN ISAR IMAGING

The deception signal must be generated with several errors that are expected by the adversary radar. After all research is conducted in ISAR systems in order to combat these errors and produce a more focused image of the target. Moreover several verisimility details must exist in the signal, like angular glint and phase delays according to the distance between the decoy and the adversary sensors. For example an error emerges because the relative motion between the naval target and the ISAR instrument is generally not known and thus presents a fundamental problem [21]. Therefore the Sim-dRCS must be able to move the false target in time in order to incorporate the afore-mentioned translation errors. And another example is the addition of angular glint effects in the false target which dislocate scattering centres from the input mask again according to the distances between the involved parties.

Like having the advantage of solving a labyrinth from the end to the beginning the Sim-dRCS engineer can reuse the domain of ISAR simulators in order to realise this deception stratagem. Analytically the triptych of domain engineering, requirements engineering and software design, as stated by [22, p. 7], is employed in order to implement a proof of concept that can provide such ISAR images of a false naval target to multiple threats in different locations which means different phase delays.

3.1 False Naval Target Verisimility Domain Engineering

Domain engineering is the process of reusing domain knowledge in the spawning of new software systems [23]. Here we are reusing the advances that have been made in the domain of ISAR simulators. They are made to produce ISAR images either for academic purposes in order to increase the knowledge in the field or for industrial applications in order to make better radar systems. Here the novel idea is to reuse the domain of ISAR simulators in order to achieve a simulator defined radar countermeasure system. The principle of operation is that the simulator output can be crafted just-in-time and bespoke to each threat with a high or low verisimility level. The main effort is to conduct social engineering practices to adversary radar operators. Moreover this idea has serious possibilities of realisation due to advances in miniaturisation (FPGA technology) and parallel processing abilities (fast execution times of multiple software entities).

The domain description explains or describes the actual properties of a subject matter that can be partially or totally represented by a mathematical model and relevant computer code [22, p. 8]. Here the focus is in coherent jamming where the intention is to present many false yet plausible targets to the threat signal so the adversary radar-operator loop cannot differentiate between the friendly assets and artificial targets. For the current air defence at sea scenario the friendly asset is an extended target which means as was already mentioned that there are several points on the ship’s superstructure that backscatter the threat’s signal which in turn is received and processed by an Inverse Synthetic Aperture Radar (ISAR) system. It is only necessary to synthesize a false target that has almost the same radar cross section, or electromagnetic signature, to the protected friendly asset [24]. Therefore the false target must seem to be a collection of points dispersed in slant, cross and height ranges situated in a three-dimensional worldspace or 3D-space [8]. And to ensure correct geometrical properties and realistic false target velocities the range, velocity and heading of the threat signal must

be taken into account [25]. The false target entity properties must always be adjusted to the threat entity characteristics. And the simulator approach is fulfilling this requirement.

Towards the discussion of this subject matter an ISAR simulator is presented which is constructed as a complex system [26]. The input in this instance is simulated data representing the hijacked replica of a threat signal multiplied by the rest of the false target slant range components. The transfer function is composed of a distance calculator that provides line-of-sight (LOS) range measurements, an interferometer module that provides angle-of-arrival (AOA) angle measurements, a pace engine that provides roll, pitch, yaw and translations functions and the digital signal processing block that provides the standard time-frequency domains transformations usual to ISAR imaging. According to LOS and AOA the output of the simulator is a side view [27, 1996, 5.1.2.3 Roll Images, pp. 441-444 & 5.1.2.4 Pitch Images, pp. 444-446] of the target, a top view of the target [27, 1996, 5.1.2.2 Yaw images, pp. 437-440] or an in-between state [27, 1996, 5.1.2.5 Yaw/Pitch/Roll images, pp. 446-447]. Since a dominant characteristic of extended naval targets is the angular glint phenomenon as stated by [28, 2003, Section 3.4.2 Missile Noise Inputs, pp. 113-115], the overall design is easily extensible to provide such value added functions in the input stage [29]. According to the value of the interfering scatterer the dominant point scatterer in a resolution cell is displaced in the three dimensional worldspace by an amount that corresponds to a glint distance error.

Now the relationships between the inputs, transfer functions and outputs of the software system start to visualise. The corresponding software engineering draft product, code-named FB-16, is depicted in **Figure 5**. Moreover the '*create false radar & sonar targets'* block which is under the '*False Target'* column (or swim lane in Unified Modelling Language terms) is shaded because in this block the simulator subsystem contributes to the creation of the false target data. Then this data is further forwarded to the transmission subsystems of the Sim-dRCS concept. And in order to divide and conquer this paper deals only with the radar part. The underwater counterpart may be called Simulator-defined Sonar Countermeasure System (Sim-dSCS) and provides a deception synergy in the aerial and underwater communication mediums.

3.2 False Naval Target Verisimility Requirements Engineering

A requirement is defined as a property that must be exhibited in order to solve some real-world problem [30] In order to begin the software engineering process for the Sim-dRCS a verisimility requirements draft stage is essential. Therefore such a major requirement is that the simulator shall be able to generate targets of variable reality, as shown in **Table 1**.

Point of Interest	A	B	C	D	E
Credulous	100	0	0	0	0
Verisimilar	0	80	100	100	100
Credible	0	60	80	100	100
Veritable	0	0	0	20	100
Real	0	0	0	0	100

Table 1: Degrees of Persuasion

The conceptual model for those verisimility requirements is depicted in **Figure 6**. For example when the target output presented to the adversary radar operator is at point *A* then the opinion is that the target must be obviously false. At point *B* there is a high amount of verisimility but a low amount of credibility. At point *C* there is absolute verisimility to a real target with a high amount of credibility. An interesting point is depicted at point *D*. The absolute top values of verisimility and credibility are weighted against the disbelief of the human element. The adversary radar operator is presented with a very good candidate for a real contact but needs to be sure before giving a command to act against it.

Finally at point *E* the stratagem has succeeded. Any doubts by the adversary radar operator are cast away and now the opponent must either worry about the contact or expend resources for close-up identification and engagement purposes. Either way at this stage the adversary force is inflicted by an unnecessary cost in time and resources.

3.3 Software Design and Module Interconnection Language (MIL)

Proofs of concepts rely on rapid prototyping methods for the production of quick and reliable results. The software architectures of the proof of concept must be flexible because it may need to change as the project advances. Generally the backbone of software architectures is the module interconnection language which depicts the structural design of a system. In other words it shows the interconnection of the modules that comprise the software system. An important factor in this field is the form of the information that is exchanged between the modules. An example of the internal structure of an input packet of the Sim-dRCS is shown in **Figure 7(a)**.

The expectations of a model can be refined by a trial and error process, as stated by [31, p.13]. This statement is also true in the implementation of the structural design of the system. For example during the construction of this project it was found that by forming the output of any transfer function by the intact input packet plus the new output information there is a considerable speed and convenience in the realization of a functional proof of concept. All new information is always added to the left side of the output packet, as shown in **Figure 7(b)**.

Analytically the realisation of the proof of concept is speeded up because the packet structure is rich in elements that can be used by diverse transfer functions. For example suppose a subset of elements is used from packet A, as shown in **Figure 7(c)**. The subset that is used is marked in blue. This results in the output packet that is comprised by packet A and packet B. Packet A has emerged intact and packet B has been appended to the end.

Suppose that the project continuation required the partial use of elements from the newly crafted packet through transfer function 2, as shown in **Figure 7(d)**. The output packet is a superset of packets A, B and C with the elements of packet A and B at the same positions. The power of this MIL methodology is shown in **Figure 7(e)**. Here transfer function 2 was deemed not appropriate for the task at hand and the following actions needed to take place:

- More elements of the input packets needed to be engaged.
- The transfer function needed to be rewritten.

It may seem as a paradox to craft such large packets, but now it is evident that this methodology of reinserting the input packet to any output results in rapid implementation times. Because the designer is not distracted by the input structure in the case of a need to change any transfer function of the system. The locations of the input elements are fixed and this means that the existing locations of the transfer function input parameters do not change once recoding is required during the development period. And with this development approach the software engineering blueprint of the proposed false target generation simulator is realised and shown in **Figure 8**. The input to the simulator is the replication of the real-time situational awareness conditions. In other words a synthetic environment is created by the simulator that copies the battlespace spatial parameters. Then the position, heading and velocity vectors of the adversary and friendly forces are duplicated in this virtual environment. In order to generate the false target the simulator uses an abstraction degree which provides the required levels of accuracy and precision. In other words a false target can be a highly detailed battleship or a basic shape of the same dimensions without all the superstructure details. Then the distance between the threat and the false target is calculated. The false target abstraction is further made to look more realistic by adding glint effects. Moreover the reality degree is augmented by introducing phase delay

effects to the false target. Now the false target is ready to be translated in space with the help of affine transformations that provide for roll, pitch and velocity movements. The simulator can move the false target in the yaw direction but for ISAR this movement is usually taken as a change in aspect angle between the radar and the target. Therefore an appropriate velocity vector will suffice for this task. When the threat radar is recognized then the verisimility of the stratagem can be increased. Because the false target output can be forged to correspond directly to the operational parameters of the threat's radar system. Additionally all above generated data can be stored in a database system for further analysis and system development. In the output stage there are three categories of false targets that can be presented to the threat, which are the side-view type, the top-view type and a state of in-between type of imagery. This decision is primarily made according to the value of the depression angle between the threat and the false target.

4.0 METHODOLOGY OF SIM-DRCS PROOF OF CONCEPT

In this section the applied methodology in order to realise the Sim-dRCS proof of concept is described. First the geometrical space that defines the virtual battlespace is described. Then the method to create distances between the threats position and the false target is analysed. Then the method to inject the angle of arrival in the signal in order to increase the verisimility of the signal properties is presented. The false target must be able to move inside the virtual battlespace therefore the description of an appropriate pace engine comes next. A major verisimility enhancement follows which is the glint effects description. Finally the operational requirements are captured with a use-case as defined in the Unified Modelling Language (UML) software terminology.

4.1 Controlled Experiment Geometry Setup

The threat position heading and velocity is placed in a three dimensional synthetic worldspace that has origin the center of the false target. In this case the origin is declared when the center of gravity and the center of buoyancy are co-located on the *z-axis* [21, 2008, pp.11], in other words when the ship is upright, as shown in **Figure 9**.

4.2 Distance Calculation

The distance calculator module contributes to the estimation of the Line of Sight (LOS) vector duplication to the virtual battlespace, as shown in **Figure 10**.

4.3 Angle of Arrival Determination

A real interferometer in the decoy has determined that there are threats at a forty-five degree aspect angle to the protected naval asset, as shown in **Figure 11**. Then the radio frequency interferometer software module contributes to the duplication of the Angle of Arrival (AOA) of the threats in the virtual battlespace.

4.4 Pace engine for roll, pitch, yaw and translations transformations

Once the above parameters are locked then the pace engine module is injecting motion effects in the false target image. The collection of points that compose the false target are moved into space with realistic heading, course and angular velocity vectors, as shown in **Figure 12**. For example the sea state is observed and the false target is programmed to behave accordingly to the existing conditions. The mathematical praxis is conducted by the utilisation of affine transformations for roll, pitch, yaw and translations functions.

For the purpose of extracting results that validate the output of the simulator the following statements must be considered :

- the heading vector of the radar is at 45 degrees to the x-axis of the false target
- the false target is pitching or rolling resulting in a side-view image
- the Doppler resolution is the z-axis

The false naval target is considered to undergo a pure pitch or roll motion. In this manner side-view ISAR images can be produced of the false target. Pure pitch and roll motions provide good candidates for a controlled experiment environment because they produce side-view ISAR images which are easy to validate by visual inspection [32]. This setup produces a side-view of a real target; therefore the output of the simulator should be a side-view slant range profile and consequent ISAR image.

4.5 Glints Effects Injection

Angular glint is representative of extended naval targets. The inclusion of this effect increases the credibility factor of the decoy playback signal at the adversary radar-operator station. In order to keep the credibility quality of the experiment the interfering scatterer positions are placed at ninety degrees with respect to the aspect angle setup, as shown in **Figure 13**.

4.6 Digital Signal Processing Use-Case

The use-case resulting from the requirements study is shown in **Figure 14**. Team A tries to deceive Team B about the current locations and future headings of its naval assets. Also Team A tries to deceive Team B that real assets belonging to team A falsely exist at a location. So Team B would want to investigate this location and expend forces in vain or wrongly include this location as a potential strategic hazard. Generally these and similar use-case scenarios state the Sim-dRCS requirement which is the attempt to disorganize the plans and needlessly consume the resources of the opponent force. Moreover the verisimility attributes that are chosen to take part in the deception must take into account the real-time situational awareness of the battlespace. For example if the sea state is calm then a false naval target must not be made to roll like it would at rough seas.

An interesting case exists when the Sim-dRCS system is mounted on an autonomous decoy platform. Then should the platform be captured by a Team B Security Officer then the valuable software system must be protected by a strong encoding scheme. Furthermore attempts to remotely manipulate the platform must be dealt with a security measure. For example a proposal is the use of a set of preloaded authorization codes that must be matched to those received in order to execute an incoming command.

Abiding by these requirements the side view of a false naval target will next be presented to the adversary radar operator. In this manner Team B will deduct that an unidentified battleship-class target is located at forty-five degrees aspect angle and at almost zero depression angle to its sensors.

5.0 FALSE NAVAL TARGET GENERATION RESULTS

The wavelength permutations of an X-Band Fire Control Radar (XFC) at a wavelength of 0.03 to 0.04 m, as shown in [33] are now investigated. An advantage of the simulator is the easy and adaptable change of the operational parameters. For example the adaptation can easily change to a J band naval radar of 10 to 20 Ghz should that was the threat tracking the electronic countermeasure.

The aspect and depression angles between the threat and the target define the resulting scenario. In this case for an aspect angle close to forty-five (45) degrees and an aspect angle close to zero (0) the resulting ISAR image must be of a side-view type. The Slant Range Profile (SRP) which represent the energy of the reflected signal as a function of the slant range and its corresponding translation into the frequency domain as the ISAR image are arranged in **Table 2**.

Threat Type	Range [nmi]	Aspect Angle [degrees]	Depression Angle [degrees]	Height [m]	Slant Range Profile & ISAR [Figure Number]
M0 - Missile t=0	38	45	8.09	10000	15
M1 - Missile t=1	19	44.5	0.16	100	16
M2 - Missile t=2	5	45	0.25	40	17
M3 - Missile t=3	1	44.5	0.62	20	18
A0 - Aircraft t=0	38	45	8.09	10000	19
A1 - Aircraft t=1	42	44.5	7.33	10000	20
A2 - Aircraft t=2	46	45	6.69	10000	21
A3 - Aircraft t=3	50	44.5	6.16	10000	22

Table 2: Threat Assessment Parameters

where the terms that appear in Figures 15 to 22 are:

RC: Resolution Cell Number,

Reflectance Value: the squared magnitude of the signal as a function of the slant range of each resolution cell

Doppler: normalized to the highest value of the second Fourier Transform that produces the ISAR image that corresponds to the appropriate reflectance value (SRP)

Now in order to increase the verisimility of the results multiple layers that correspond to reflectivity coming from lower height coordinates are added to the final image. In this case one additional layer is presented. This layer is not injected with glint effects in order to demonstrate the presence and absence of the glint generator module.

In the modern battlespace it is possible to collect measurements from geographically dispersed sensors into a headquarters location for further strategic and tactical analyses. This is the concept of Network Centric Warfare [34]. In this case it is assumed that a *Team B* radar operator is able to receive measurement data from both a missile launched against the false naval target and its break-away aircraft. The expected requirement of the false target is that the *Team B* operator should not see absolutely the same ISAR images at different distance permutations. These scenarios and their respective results are presented in the next two subsections.

5.1 Approaching Missile Scenario

The scenario starts by considering that the adversary high resolution sensor mounted on a missile has acquired a target, which is false in this case, at 45 degrees aspect angle with half a degree change in order to achieve the required cross range resolution. From the set of **Figures 15, 16, 17 and 18** it is deduced that the output is slightly fluctuating with respect to the distance.

5.2 Stand-Off Aircraft Surveillance & Tracking Scenario

The scenario continues by considering that the aircraft, having fired the missile, is moving away from the threat still tracking it with an ISAR system. From the set of **Figures 19, 20, 21 and 22** it is deduced that the output again is slightly fluctuating with respect to the distance.

6.0 DISCUSSION

There are two main approaches in the construction of countermeasures in general. The first approach tries to provide an output that is particular in jamming or neutralizing an existing system. The other approach tries to generate an output that is close to the laws of physics so any sensor device is bound to pick up the false signal as recognized and valid. The effort in this paper is closer to the latter approach.

The explanation of the results can be demonstrated by the following key points:

- The simulator can easily create the appropriate permutations of diverse range, height, aspect angle and wavelength for the generation of the false target. The purpose of producing these results is the effort to make the false target more realistic to the adversary radar-operator (machine-human) system.
- The simulator can generate outputs that are valid or even non-valid. All these outputs are useful in the deception of the adversary. An on-board simulator may create non-plausible false targets thus driving the adversary operator to question the validity of the encounter at this area and directing opponent forces elsewhere. And a stand-off Sim-dRCS may create high validity targets in order to become a honeypot and lure the adversary radar operators to direct their efforts in that area. The ultimate goal is the deception of the opposite human element. Such examples are hiding valuable friendly forces into a false target set, creating ghost fleets, the further upsetting of adversary strategic plans and the initiation of ineffectual tactical actions by the opposition.

And the value of the results using a physics-compatible countermeasure system can be demonstrated by the following key points:

- The simulator can be seamlessly integrated to the context of a software-defined radar countermeasure system (S-dRCS). In this manner the simulator can support a decision making system that will produce the correct output according to an assessment made on the basis of the characteristics of the threat signal, leading to the special case of a Simulator-defined Radar Countermeasure System (Sim-dRCS).
- Countermeasure data can be created just-in-time thus eliminating the need for huge memory banks of playback false target data. By using miniaturised equipment, like FPGA’s, the simulator can be mounted into remote decoy systems. These decoy systems can be mounted on a platform that can simultaneously support underwater, sea-level and airborne functions. In this manner the software-defined countermeasure system can be augmented into providing better coverage and functionality. Also its survivability factor is highly increased.
- The Sim-dRCS can be hosted on a remote stand-off decoy platform acting as a front-line of defence electronic warfare system. This forward and tactically exposed position of the Sim-dRCS platform is justified because its pecuniary value is small compared to a conventional carrier like a destroyer vessel or a maritime patrol aircraft. In other words should the friendly decoy be found and destroyed the resulting loss to the friendly forces will be minimal. Moreover in case of capture such forwarded autonomous Sim-dRCS systems should protect

their code and data elements by using an encryption or self-destruction system.

Therefore the derivation of direct coherent countermeasures that hide the friendly naval assets from their opposing airborne counterparts by using obscurity and distraction principles are of paramount importance to air defence at sea operations. The main point is to be able to persuade an adversary radar operator that a false target is indeed a true contact or that a true target is indeed a false contact.

Moreover an important research aspect of high resolution systems are systems that could provide automatic classification and sometimes identification of a non-cooperative target [35]. We expect to further investigate the abilities of the Sim-dRCS system to deceive these types of systems in future research efforts.

7.0 CONCLUSIONS

Imaging radar makes a naval target extremely difficult to hide. Its ability to depict details of a ship's superstructure is a formidable surveillance and tracking asset for an airborne aggressor. In this paper we proposed the devise of a special case of a software-defined radar called Simulator-defined Radar Countermeasure System (Sim-dRCS). The main point is the employment of a simulator subsystem for the creation of false naval targets according to the stratagem of creating something out of nothing in order to confuse an adversary party about the location and type of the real friendly assets. Therefore we claimed that the Sim-dRCS is a valuable idea and a viable solution for confusing adversary imaging radar operators. Because it can create a virtual environment that duplicates the current situational awareness conditions around a protected asset and then add false targets to this theatre that have a high degree of verisimility to their real counterpart. This verisimility property is important because it imitates the electromagnetic signature of a real target that is exploited by an ISAR system, like phase delays and glint effects. Moreover the adversary radar operator can be deceived by increasing or even decreasing the verisimility levels of the false naval target. And this is the major argument that is raised on the usage of this software tool for actual obfuscation and deception actions for air defence at sea applications. All outputs are useful. Tactical and even strategic advantages can be gained over the adversary by adjusting the simulator output to high or low reality levels. This paper communicates a vision into the future of coherent countermeasures. Without Sim-dRCS knowledge and training an adversary radar operator will always wonder next time looking at the ISAR screen whether the depicted target is really there.

Acknowledgements

The authors would like to thank Prof. Chris Baker of the Australian National University and Prof. Hugh Griffiths of the Defence Academy of the United Kingdom for valuable guidance and support in the beginning of the simulator project. Also we would like to thank all anonymous referees of this work for their helpful and constructive comments and suggestions which improved the focus and coherence of this paper.

REFERENCES

1. Stokes R., 2010, *Maskelyne Magic*, http://www.maskelynemagic.com/alameinphotos.html.

2. War and Game blog, 2007, *Operation Bertram*, http://warandgame.blogspot.com/2008/06/operation-bertram-september-november.html, accessed at 15th February, 2010.

3. Wilkinson N., 1919, *The Dazzle Painting of Ships*, as reprinted in James Bustard, *Camouflage*, http://en.wikipedia.org/wiki/Norman_Wilkinson_(artist), accessed at 15th February, 2010.

4. Ford K., White J., 2008, *Gazala 1942: Rommel's Greatest Victory*, Osprey Publishing Ltd, Midland House, West Way, Botley, Oxford OX2 0PH, UK.

5. Nichols S., 2008, *Malta Spitfire Aces*, Osprey Publishing Ltd, p.64.

6. Marvin A., 2006, *How the cavity magnetron defeated the wolf pack*, IET Communications Engineer, April-May 2006.

7. Griffiths H. D., Baker C. J., 2005, *Fundamentals of Tomography and Radar*, University College London, UK.

8. Neri F. 2007, *Introduction to Electronic Defence Systems*, Artech House, Chapter 5-6-24, ISBN 9781580531795.

9. Cleveland K. E., 2001, *How to use the 36 Chinese Stratagems To Win*, Influence Marketing, LLC, http://www.maxpersuasion.com.

10. Hellenic Defence and Diplomacy, 2009, *AEGIS*, monthly journal publication in Hellenic, March, Issue 215, pp.64-65, Expansion Consulting, 20 Filikis Etairias Square, Athens 106 73, Greece.

11. Fenn A. J., Temme D. H., Delaney W. P., Courtney W. E., 2000, *The Development of Phased-Array Radar Technology*, Lincoln Laboratory Journal, Volume 12, Number 2, pp.321-340.

12. Pace, P.E. Fouts, D.J. Zulaica, D.P., 2004, *Digital Image Synthesizers: Are Enemy Sensors Really Seeing What's There?*, 72nd MORS Symposium, http://handle.dtic.mil/100.2/ADA428160.

13. Garnier J., Solna K., 2008, *Coherent Interferometric Imaging for Synthetic Aperture Radar in the Presence of Noise*, IOP Publishing, Inverse Problems, 24 (2008) 055001.

14. Lazarov A. D., Minchev Ch. N., 2007, *SAR Imaging of a Moving Target*, Constantinople, pp. 366-372.

15. Rzemien R., 1997, *Coherent Data Collectors; A Hardware Perspective*, Johns Hopkins APL Technical Digest, Vol. 18, No. 3.

16. Hill J. R., 1988, *Air Defence at Sea*, Ian Allan Ltd, Shepperton, Surrey.

17. Stavropoulos D. B., 2008, *San Carlos Bay, 21st May 1982: A Long Day for the British Navy in the Falklands Conflict*, Journal of Military History, Issue 148, pp.66-81, in Hellenic.

18. Rui C, Ming-liang XLL, 2006, *Research on Jamming Effect Evaluation Method of ISAR*,

IEEEXplore.

19. Yuan L. I., Xue-mei L. U. O., Gao-huan L. V., 2008, *The Study of Multi-False Targets Synthesizing Technology against Chirp ISAR*, Proc. ICMMT.

20. Fouts D. J., Pace P. E., Karow C., Ekestrom R. T., 2002, *A Single-Chip False Target Radar Image Generator for Countering Wideband Imaging Radars*, IEEE Jour. of Solid-State Circuits, Vol. 37, No. 6, June.

21. Doerry A. W., 2008, *Ship Dynamics for Maritime ISAR Imaging*, SAND2008-1020, Sandia National Laboratories.

22. Bjorner D., 2006, *Software Engineering I: Abstraction and Modelling*, Springer Verlag, Berlin Heidelberg.

23. Frakes W.B. and Kang K., 2005, *Software Reuse Research: Status and Future*, IEEE Trans. on Software Engineering, 31(7), July, pp. 529-536.

24. Baldwinson J., Antipov. I., 2008, *A Modelling and Simulation Tool for the Prediction of Electronic Attack Effectiveness*, Electronic Warfare & Radar Division, Defence Science and Technology Organisation, Bld. 205L, West Avenue, Edinburgh, SA, 5111, Australia.

25. Schleher C. D. 1999, *Electronic Warfare in the Information Age*, Artech House, ISBN 0-89006-526-8.

26. Kostis T.G., Baker C.J., Griffiths H.D., 2005, *Interferometric Inverse Synthetic Aperture Radar*, Proceedings of the London Communications Symposium 2005, London, England, pp. 1-4.

27. Rihaczek A. W., 1996, *Principles of High Resolution Radar*, Ch.5 Identification of Ships, pp.433-579, McGraw Hill, New York, ISBN 089006900X.

28. Siouris G. M., 2003, *Missile Guidance and Control Systems*, Springer-Verlag, ISBN 0-387-00726-1, 2003.

29. Kostis T. G., Galanis K. G., Katsikas S. K., 2009, *Angular Glint Effects Generation for False Naval Target Verisimility Requirements*, Institute of Physics, *Meas. Sci. Technol.* **20** 104016 (13pp) doi: 10.1088/0957-0233/20/10/104016, September, 2009.

30. Abran A., Bourque J-P., Dupuis R., Tripp L. L., Moore W., 2004, *SWEBOK : Guide to the Software Engineering Body of Knowledge*, IEEE Computer Society, Los Alamitos, CA.

31. Lieberman B. A., *The Art of Software Modelling*, Auerbach Publications, Taylor & Francis Group, LLC, Boca Raton, Florida.

32. Kostis T. G., Galanis K. G., Nikitakos N. V., 2009b, *Interferometric Inverse Synthetic Aperture Radar Software: Analysis for Air Defence at Sea*, NATO Sensors & Electronics Technology (SET-136) Software Radar Specialist's Meeting, June 23-25, Lisbon, Portugal.

33. Lynch D. 2004, *Introduction to RF Stealth*, Sci-Tech Publishing.

34. Alberts D. S., Garstka J. J., Stein F. P., 2000, *Network Centric Warafer; Developing and Leveraging Information Superiority*, CCRP Publication Series,

http://www.dodccrp.org/files/Alberts_NCW.pdf

35. Kostis T.G., Baker C.J., Griffiths H.D., 2006, *An Interferometric ISAR System Model for Automatic Target Identification*, EUSAR 2006, Proceedings of the European Conference on Synthetic Aperture Radar 2006, Dresden, Germany, no. 58.

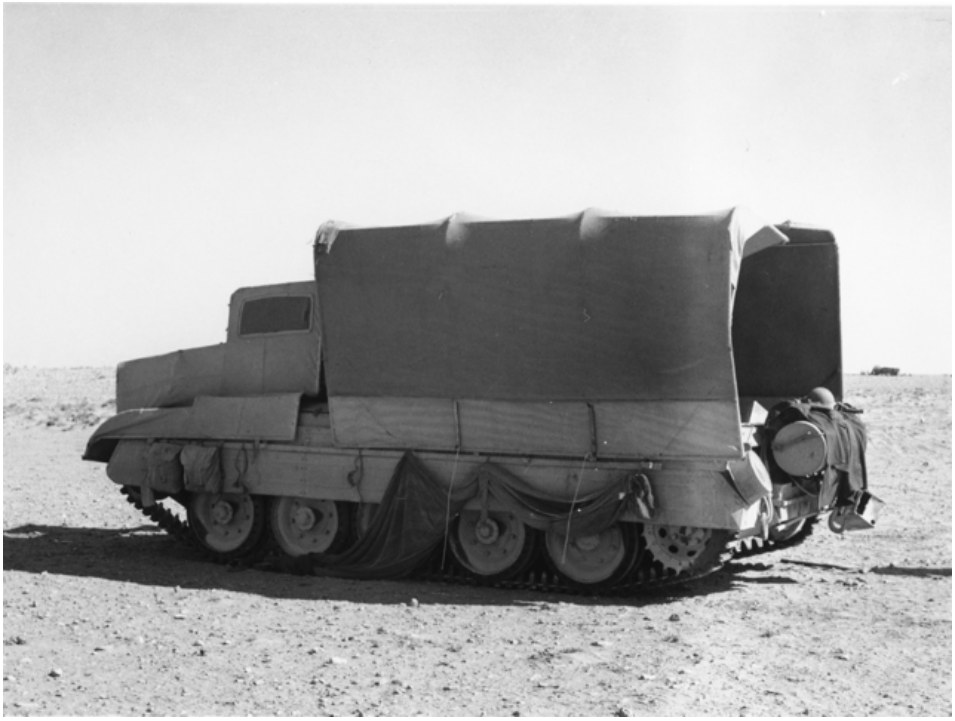

Figure 1: Stratagem where a tank is disguised as a truck with a sunshield cover.

Figure 2: Increasing the verisimility of the stratagem by leaving lorry tracks.

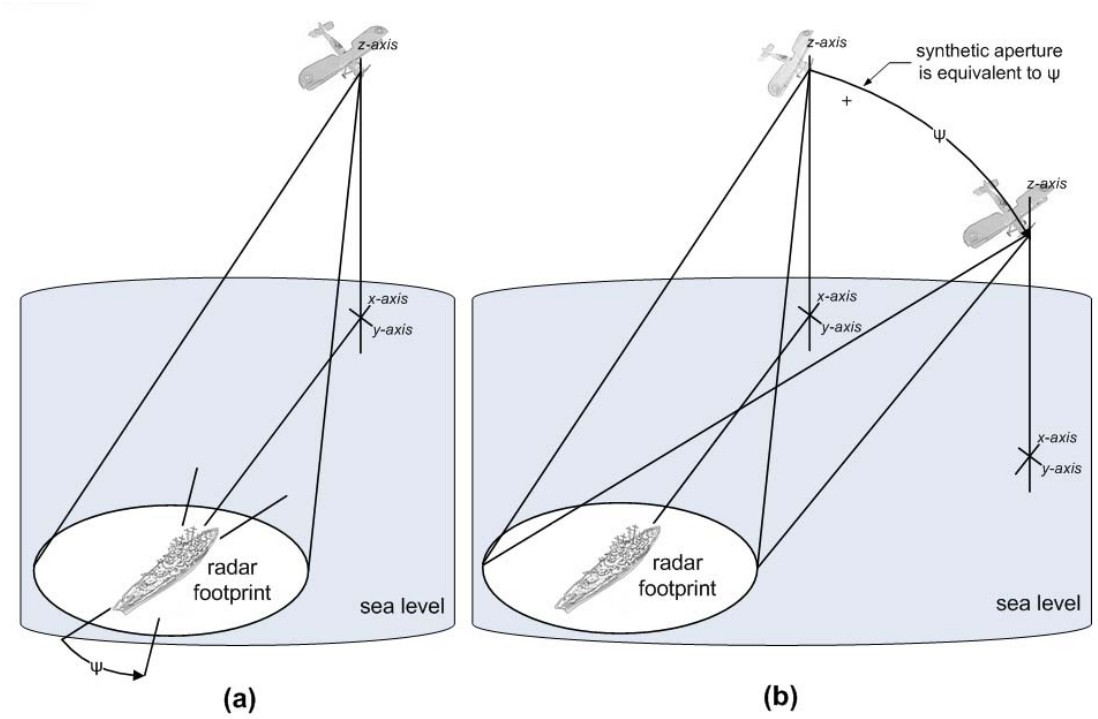

Figure 3: Foundational Principles of ISAR Operation

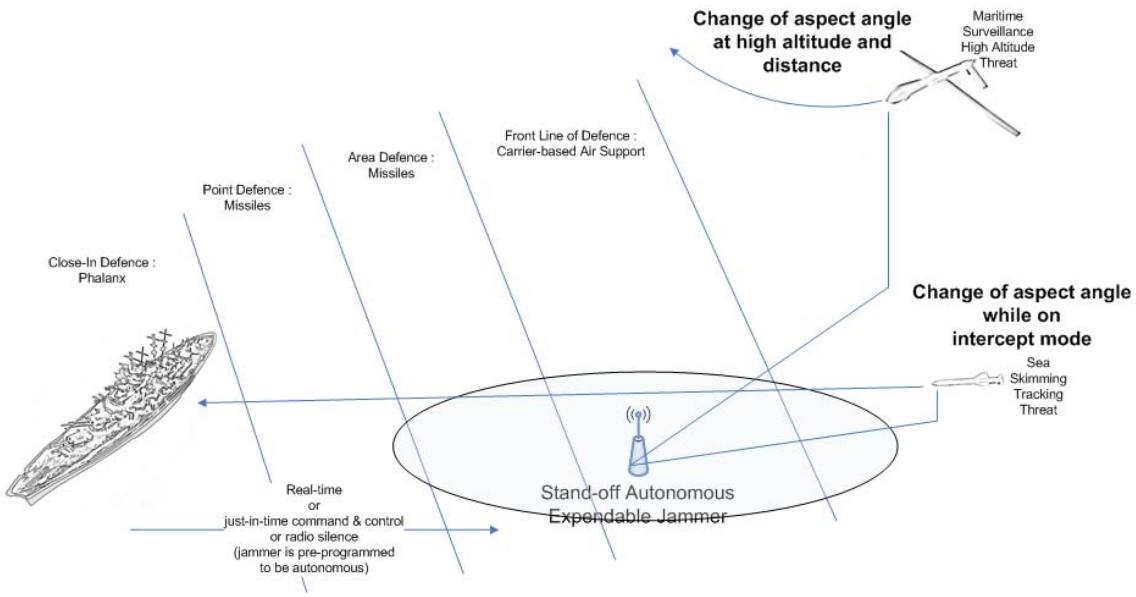

Figure 4: Battlespace scenario

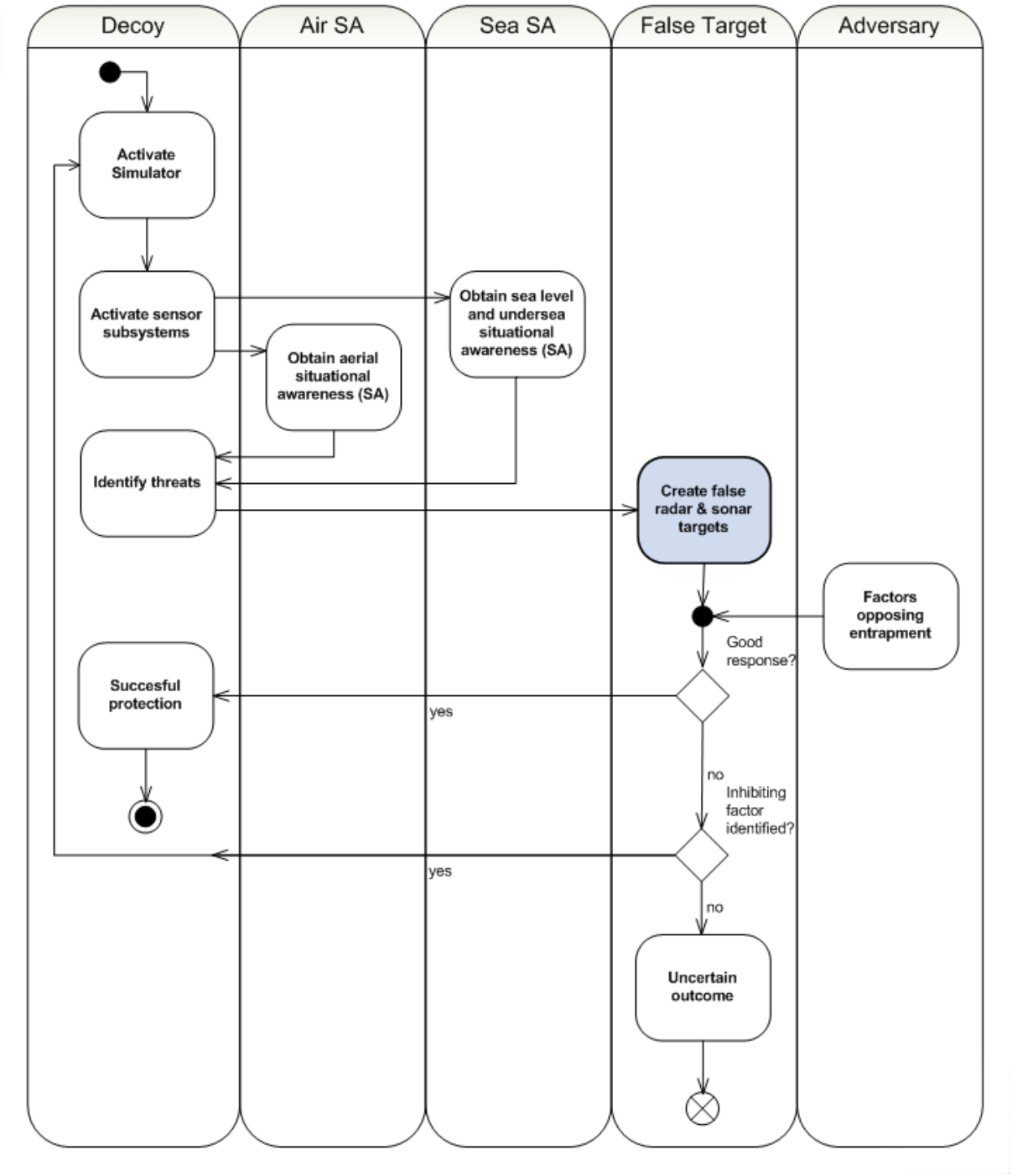

Figure 5: FB-16 Software-defined Radar & Sonar Countermeasure System (Sim-dRCS)

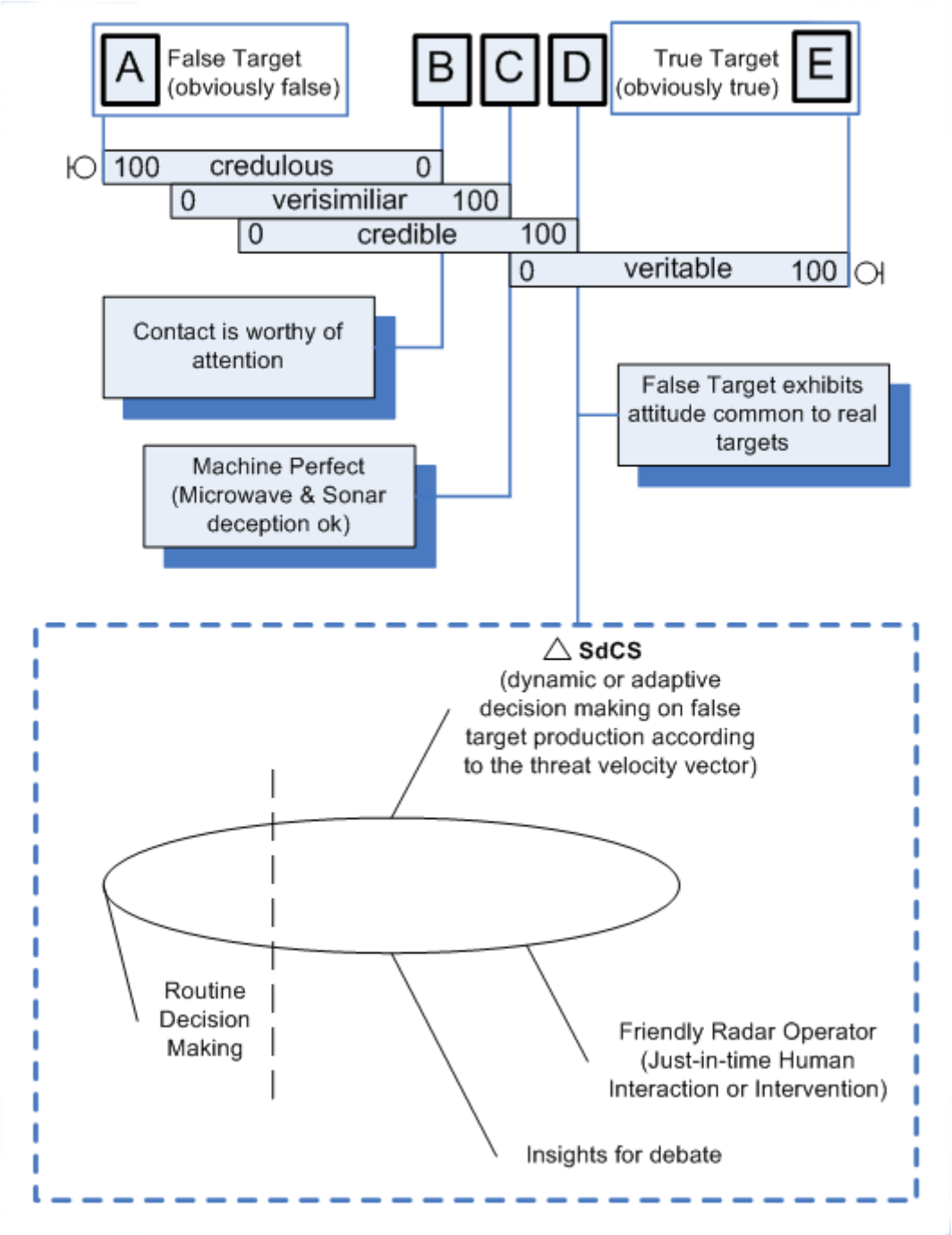

Figure 6: Conceptual Model for Verisimility Requirements.

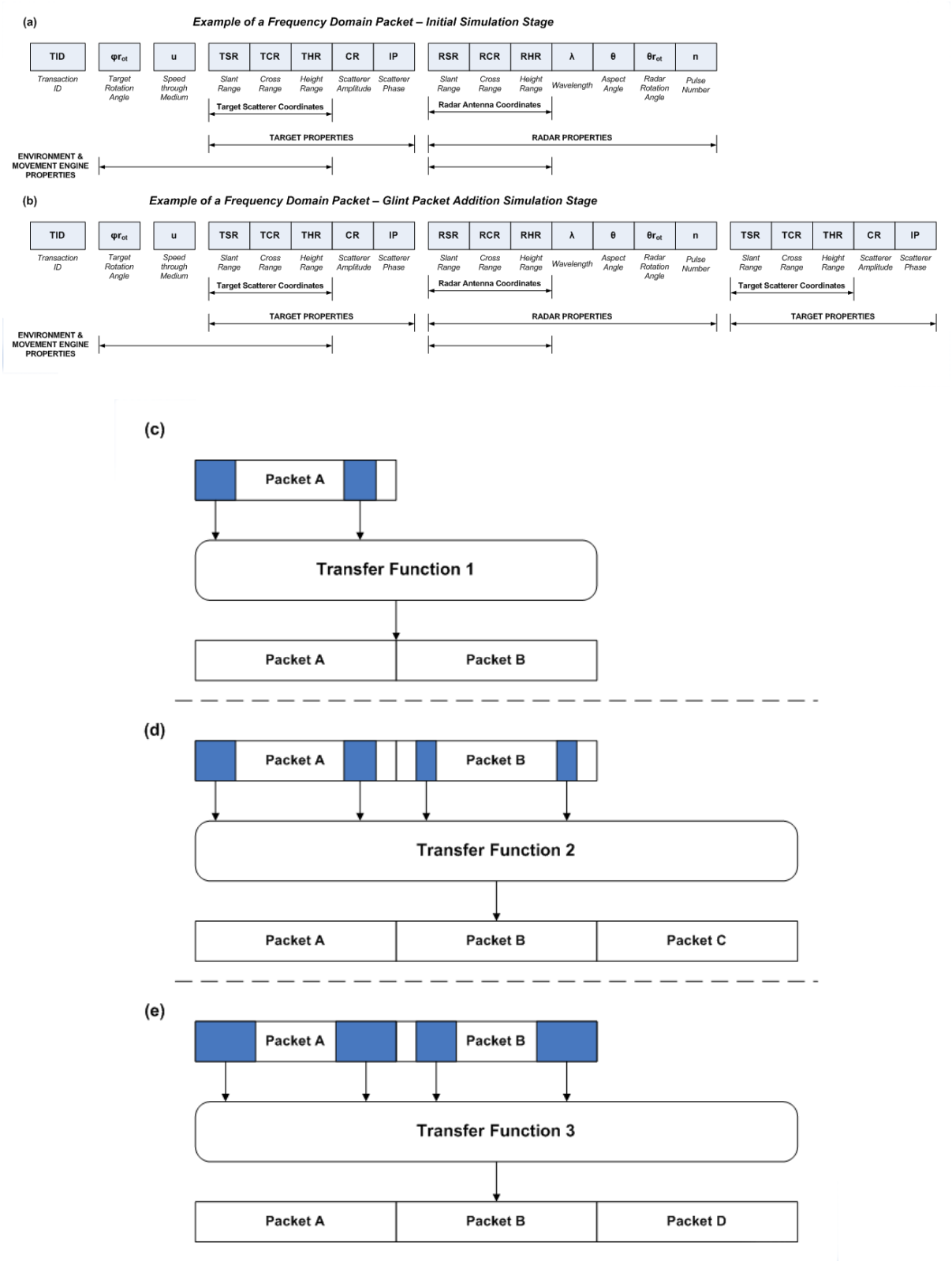

Figure 7: Packet structure and usage for quick proof of concept prototyping

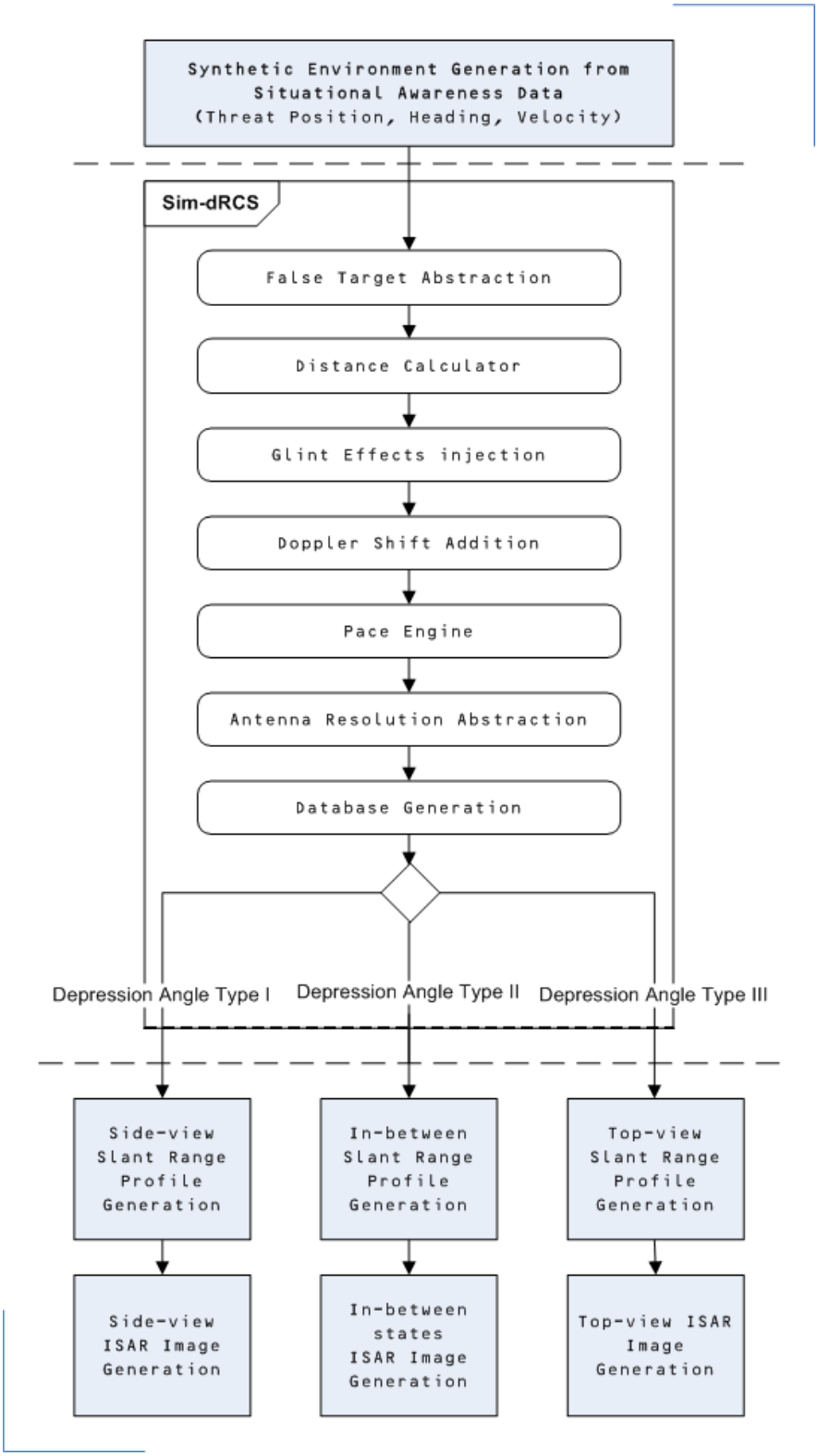

Figure 8: False target generation software modules.

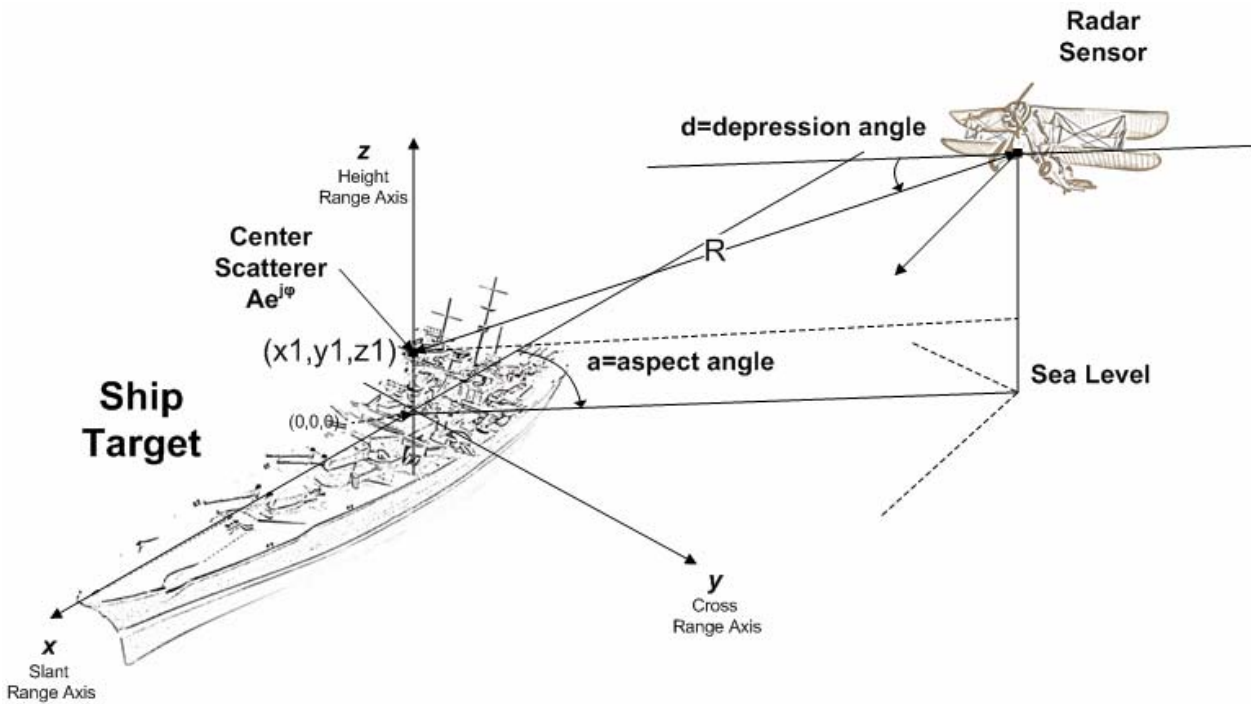

Figure 9: Simulator 3D-Space design

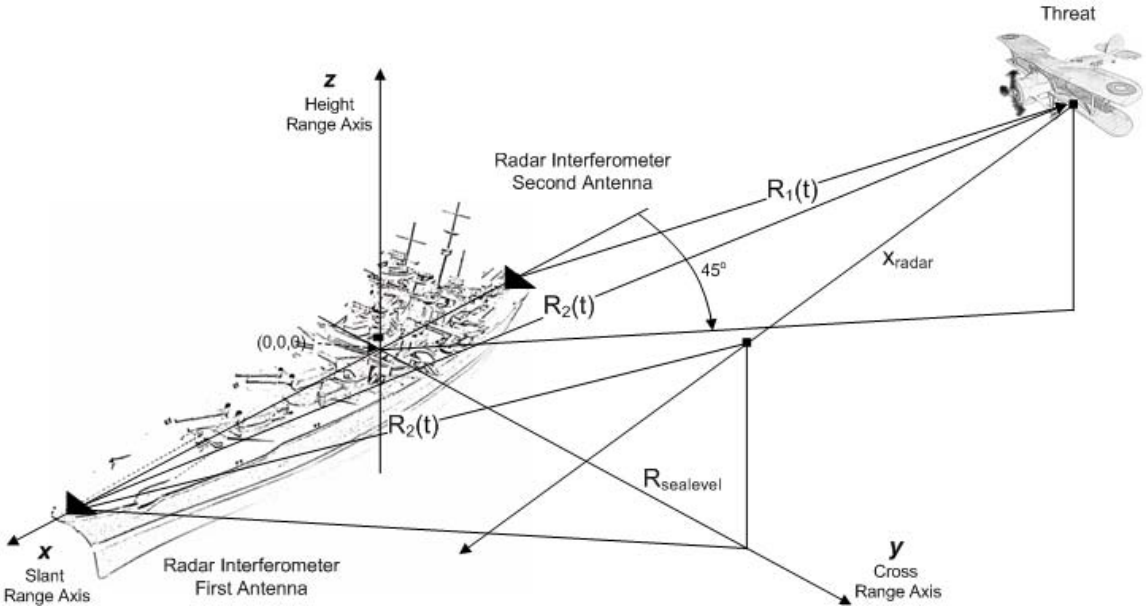

Figure 10: Distance proposed calculation

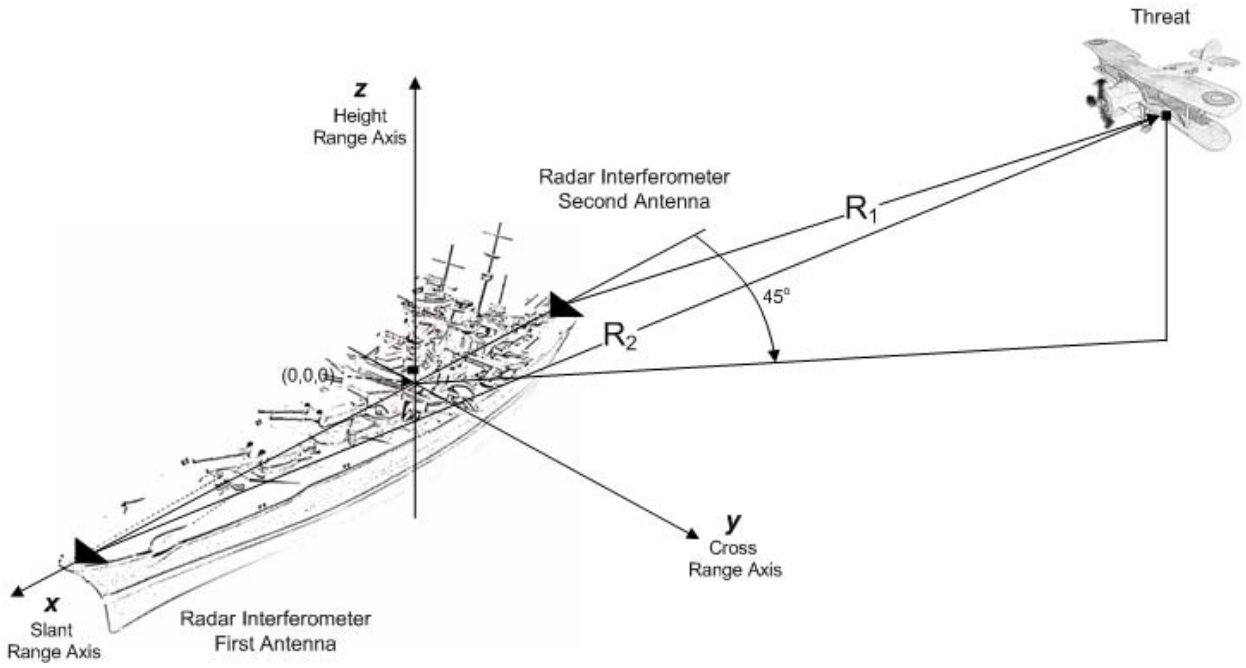

Figure 11: Interferometer proposed configuration

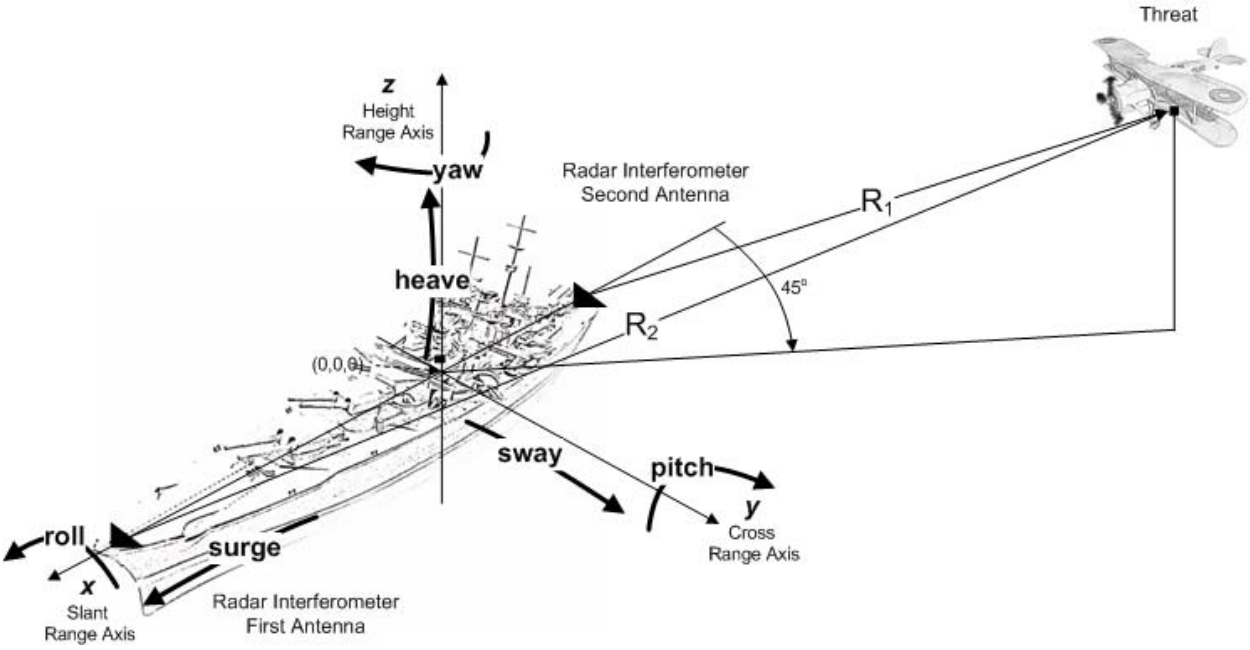

Figure 12: Movement of the false target

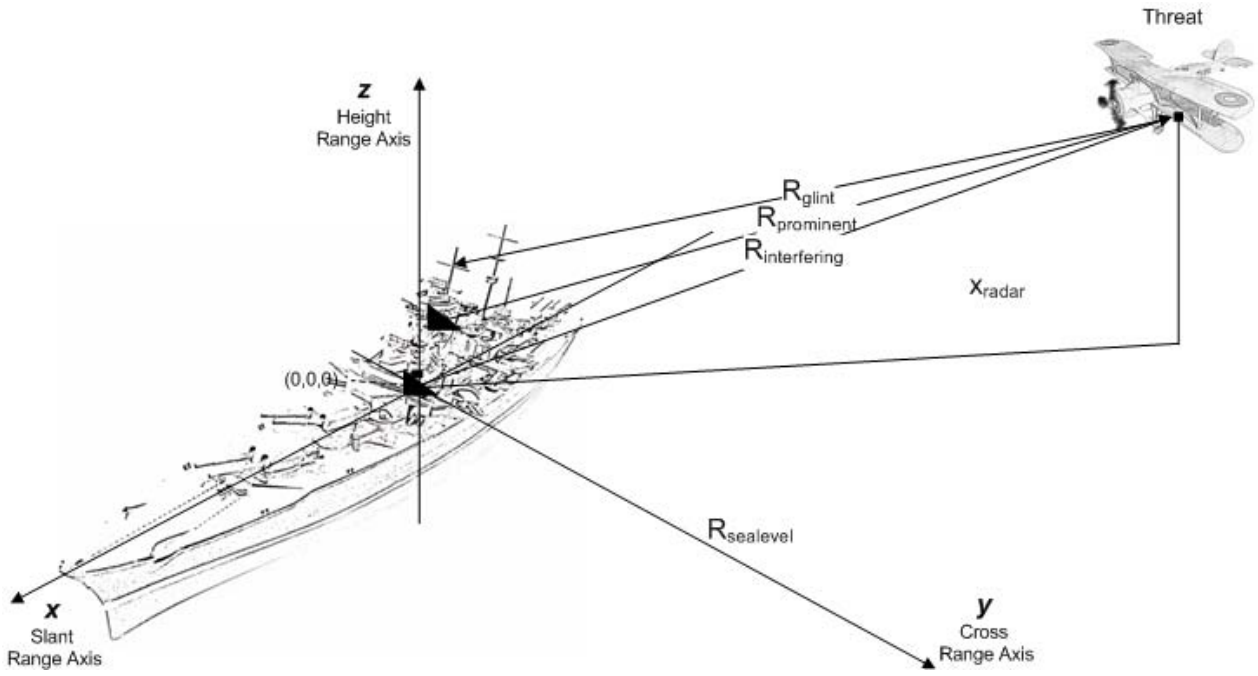

Figure 13: Prominent and interfering point scatterers

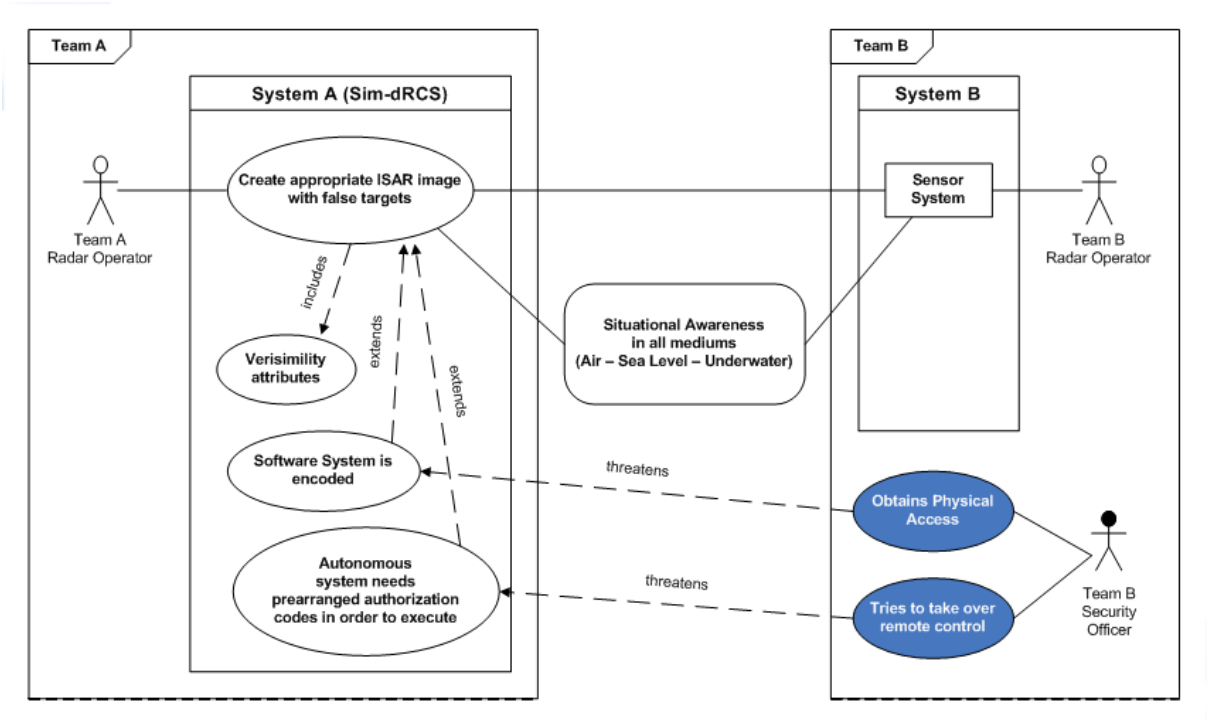

Figure 14: Use-Case diagram of the Simulator-defined Countermeasure System (Sim-dRCS).

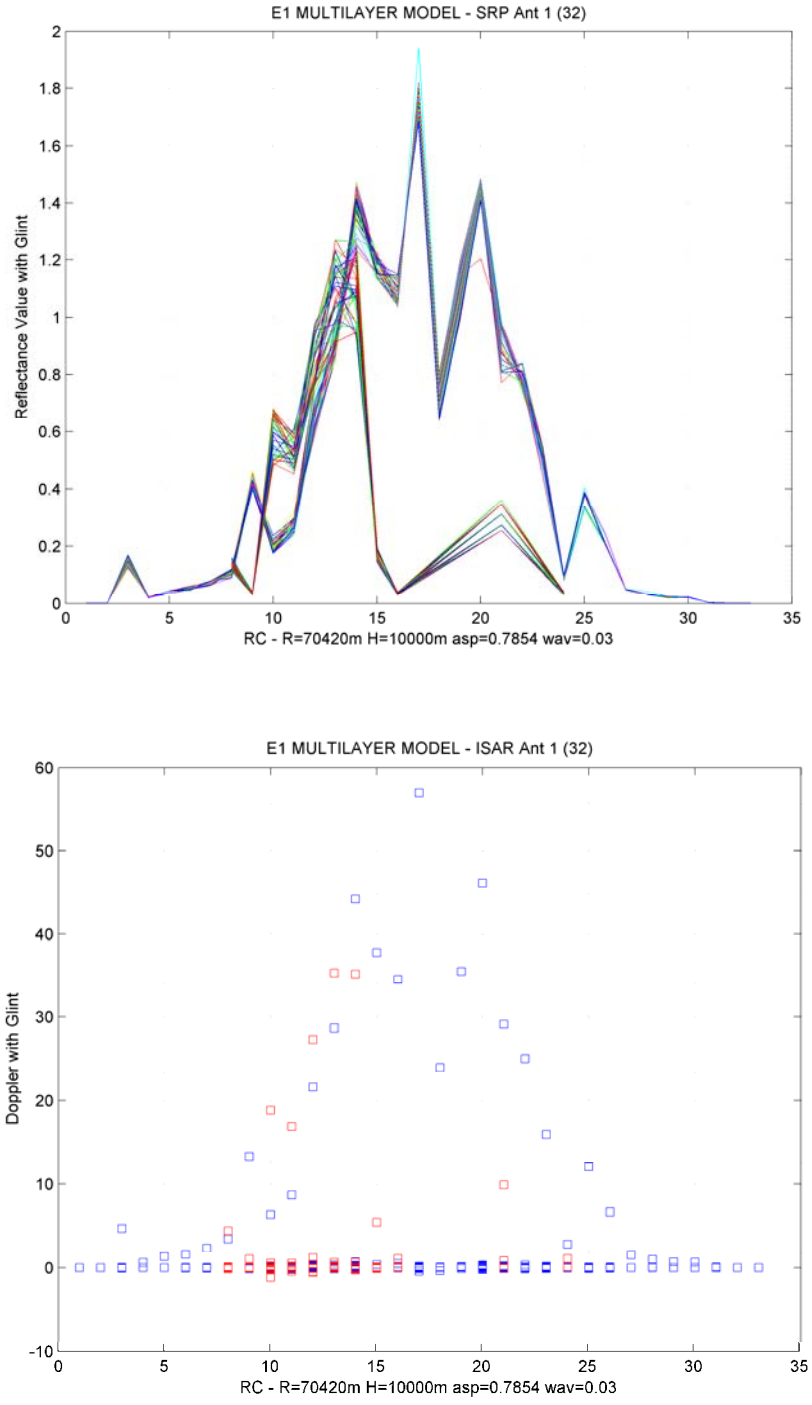

Figure 15: M(t_0), Missile at t=0, 38nmi, 45 aspect angle, 10000m.

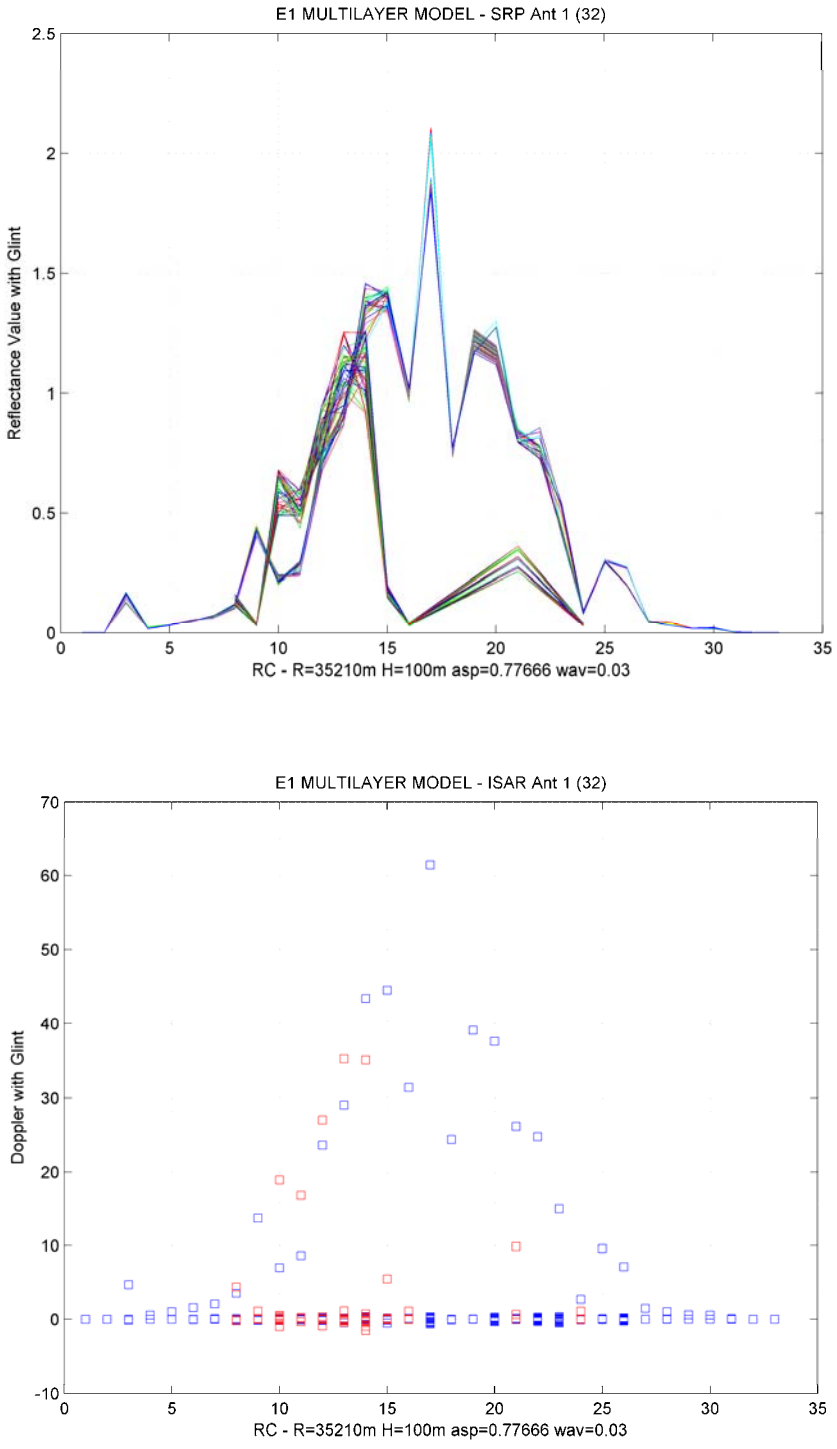

Figure 16: M(t_1), Missile at t=t_1, 19nmi, 44.5 aspect angle, 100m.

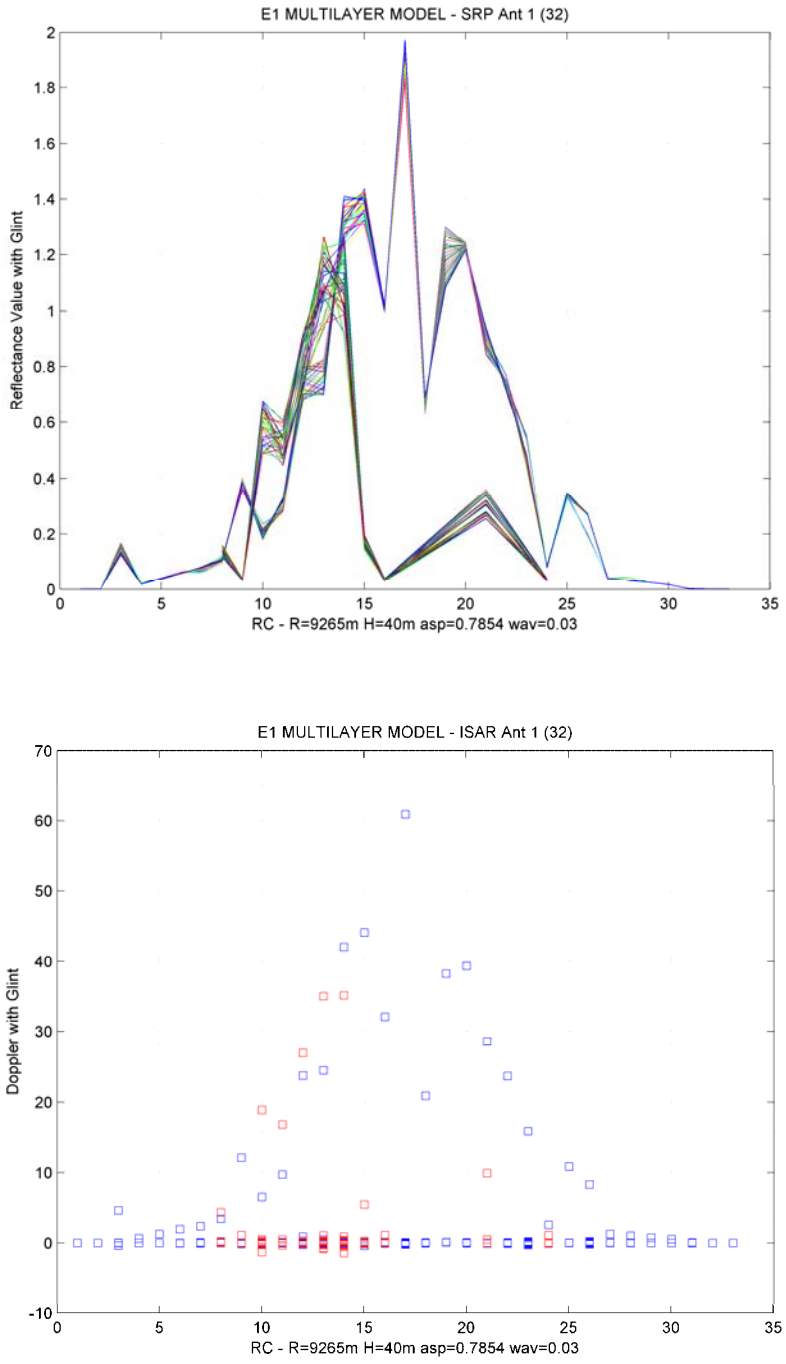

Figure 17: M(t_2), Missile at t=t_2, 5nmi, 45 aspect angle, 40m.

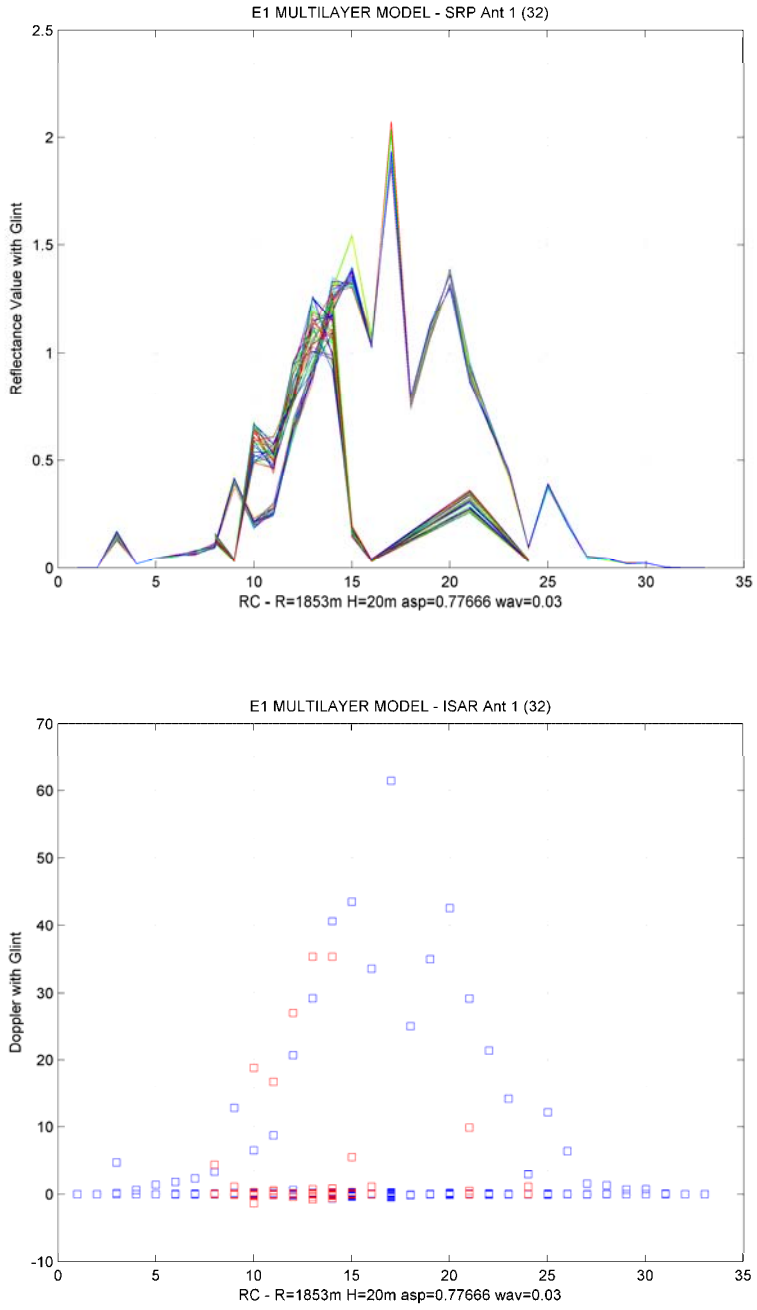

Figure 18: M(t_3), Missile at t=t_3, 1nmi, 44.5 aspect angle, 20m.

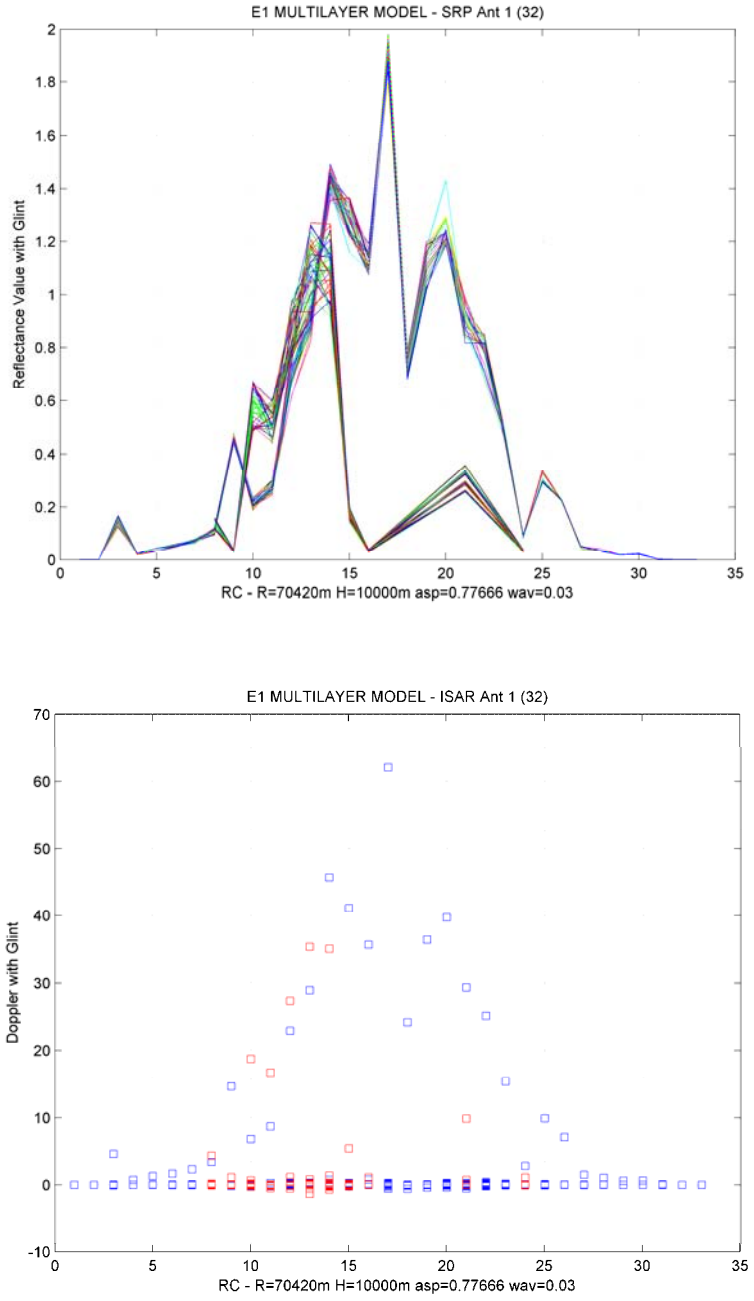

Figure 19: A(t_0), Aircraft at t=0, 38nmi, 44.5 aspect angle, 10000m.

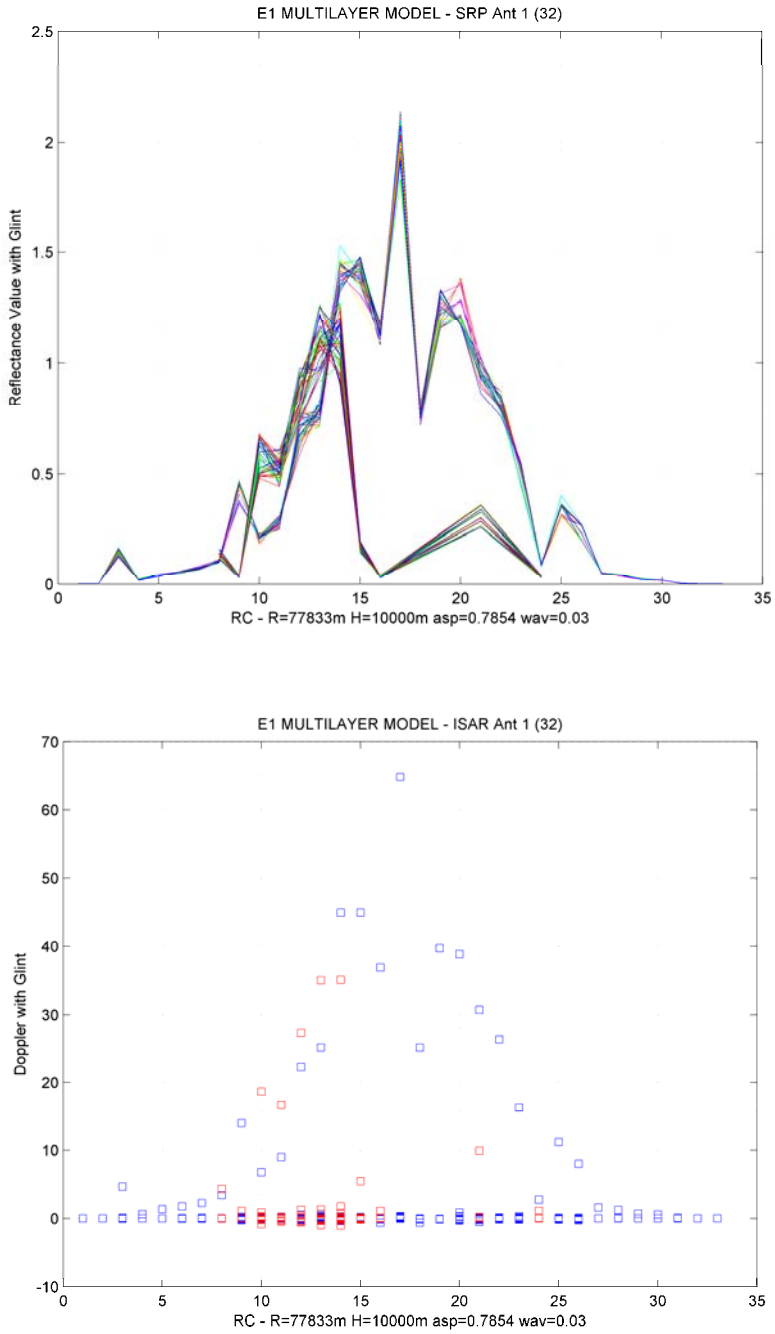

Figure 20: A(t_1), Aircraft at t=t_1, 42nmi, 45 aspect angle, 10000m.

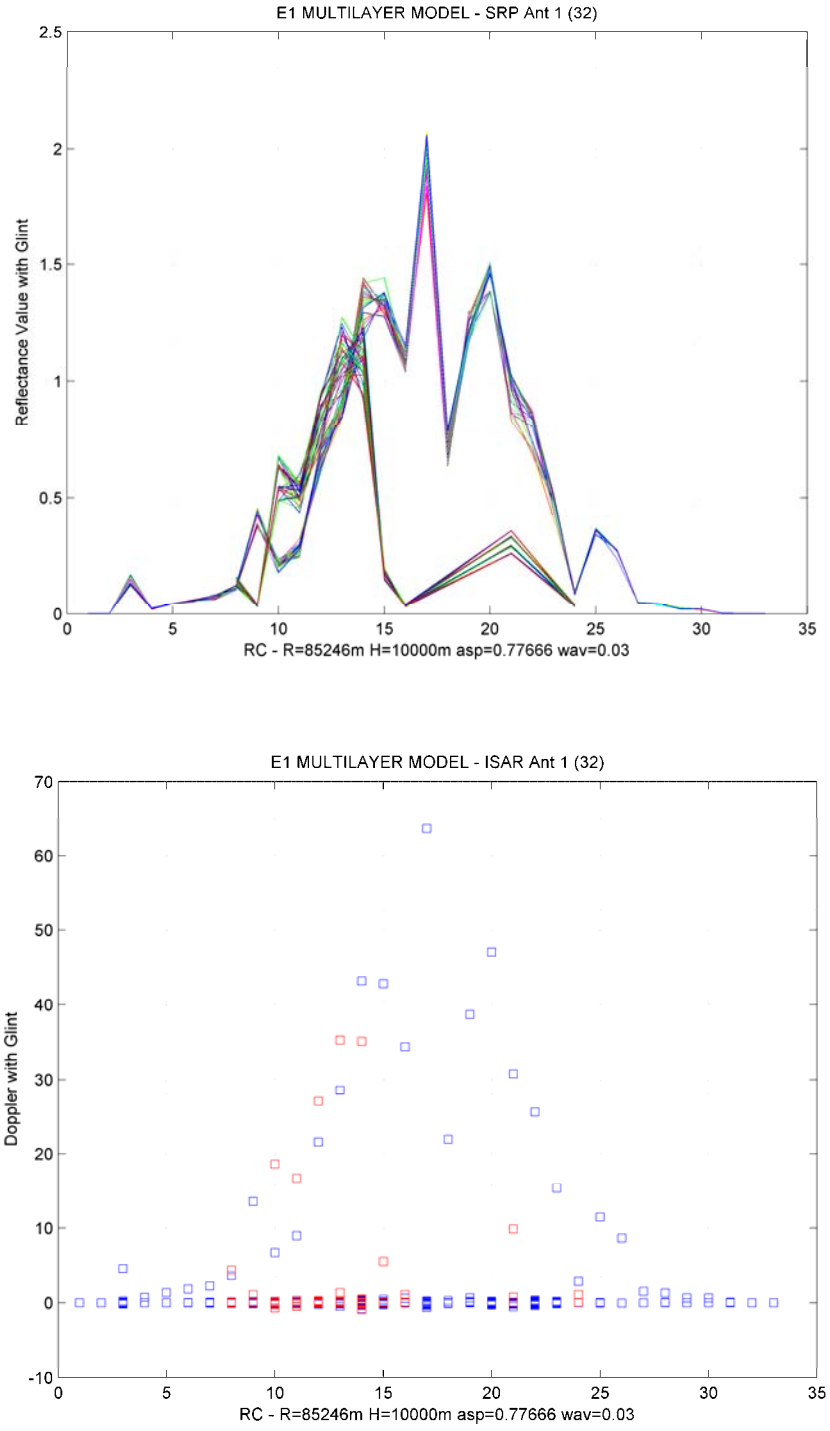

Figure 21: A(t_2), Aircraft at t=t_2, 46nmi, 44.5 aspect angle, 10000m.

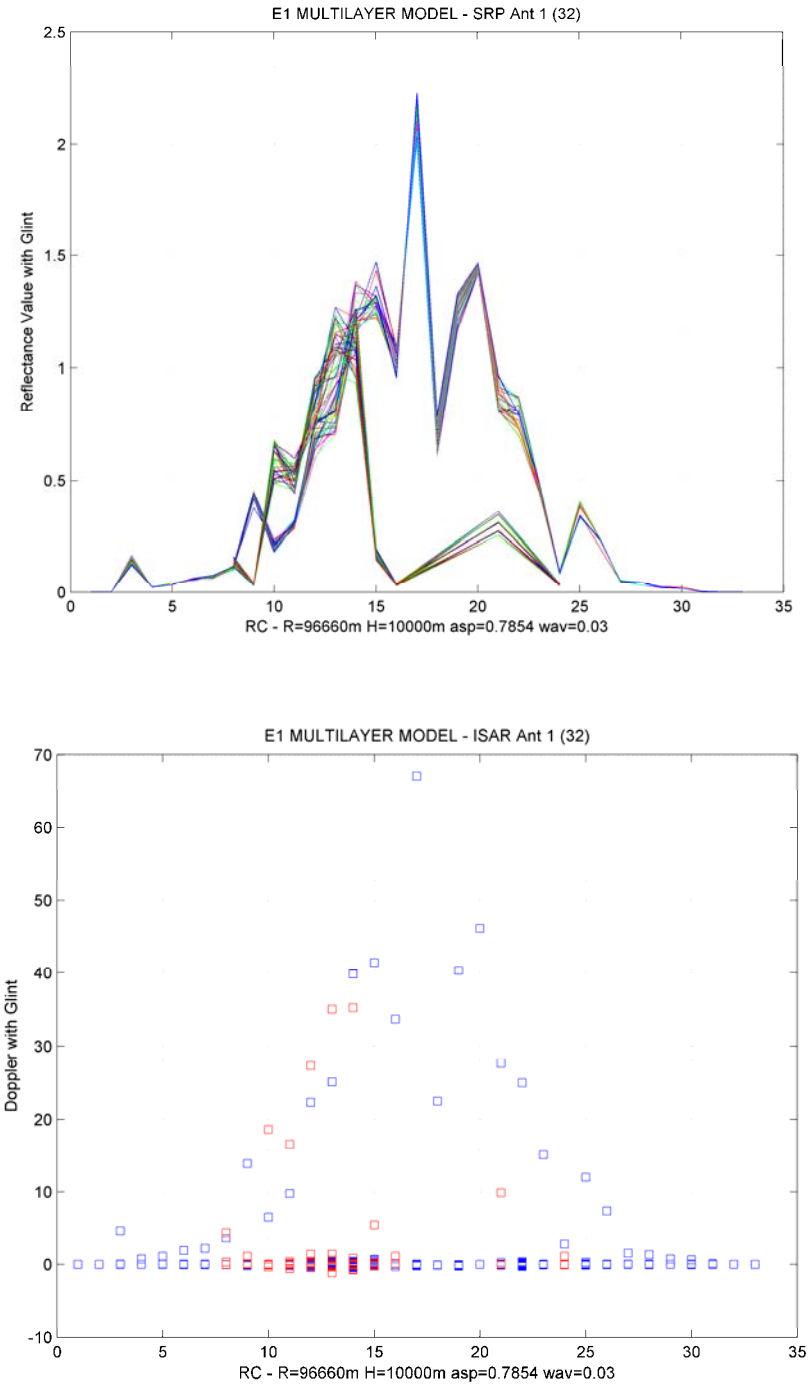

Figure 22: A(t_3), Aircraft at t=t_3, 50nmi, 45 aspect angle, 10000m.