Aircraft protection for complex threat platforms through integrated EWOS application

IOP Conf. Series: Materials Science and Engineering **610** (2019) 012078 doi:10.1088/1757-899X/610/1/012078

Aircraft protection for complex threat platforms through integrated EWOS application

R Rudd-Orthner, L S Mihaylova

Department of Automatic Control and Systems Engineering, The University of Sheffield, Mappin Street, Sheffield, S1 3JD, United Kingdom

Email: rruddorthner@mass.co.uk

Abstract. The advancement of threats is focusing commanders to consider how to combat these complex threats throughout the kill chain including prior to launch and Anti-Access Area Denial (A2AD). To match this technology race, modern platforms have been designed with integrated command and control systems and automated Defensive Aids Suites built on modular open system architectures incorporating less diverse but more complex software driven systems. The successful operation of these combat systems is reliant upon the availability of accurate, configured, harmonised and "time sensitive" mission data without which the systems may be ineffective. This paper explores the use of threat analysis diagramming techniques, and open architectures tightly integrated with a EWOS life-cycle; to develop countermeasures with a measured response beyond the traditional self-protection kill chain stages of self-protection. It introduces how threat analysis prepares understanding for simulation and how a countermeasure description language can be used to store and exchange countermeasures in a structured form. This level of intelligence data support and analysis coordinated and synchronised across multiple platforms thereby facilitating the complexities of force protection higher up the kill chain into an onion of protection mapped to a Venn diagram of countermeasure types (design intentions) with differing data needs.

1. Introduction

There is a trend for threat weapon systems to become more complex and this increased complexity could be argued to be at least in part due to: the evolution of tactics, the pace of technology development and digital modernisation, but also a trend for the broadening roles of threats with the reduction of human decision and response times. This is perhaps more so with the increased potency use of autonomous systems as well as the Integration of Air Defence Systems (IADS) and the construction of platforms with wider roles (Role Bandwidth). The rise of the autonomous system is developing in all domains: Land, Air, Sea, Space and Cyber. Autonomous systems do vary in scale from unattended gun systems to autonomous Air platforms. The roles in which these autonomous platforms operate in are also broadening and it follows that when combating Integrated Air Defence Systems (IADS), then a matching of complexity may be required in an "integrated Defensive Aids System". A traditional strategy for combating complex threat systems like IADS is with air-strikes. This paper embraces the IADS and A2AD problem with an alternative strategy of prior preparation analysis in EWOS extending higher up the kill chain to provide more complete simultaneous air protection at all levels within an extended kill chain. It is an alternative solution strategy to hard kill,

to counter IADS and A2AD solution alternatively using EWOS provisions, rather than Hard Kill air strikes [1] and this would be more applicable to UAS stealth missions.

The increased roles and capabilities of these complex platforms may cause a single platform to be less role specific and provide a "projection of protection" requirement to other platforms, but combined with this the stakeholder community is also more diverse and mechanisms for communication between scientists/engineers, crews and mission production programmers are also challenges such that they may all contribute meaningfully and complementary with values from their stakeholder groups. The Venn diagram [2] below shows "Spheres of Influence" of data availability: Protect Platform/Force, Threat or Weapon System and the Defensive Constraints are over laid with countermeasure design considerations Decoy, Deception etc. It may follow that different countermeasure considerations are coupled to different available data and form spheres of influence toward the countermeasure tactic design.

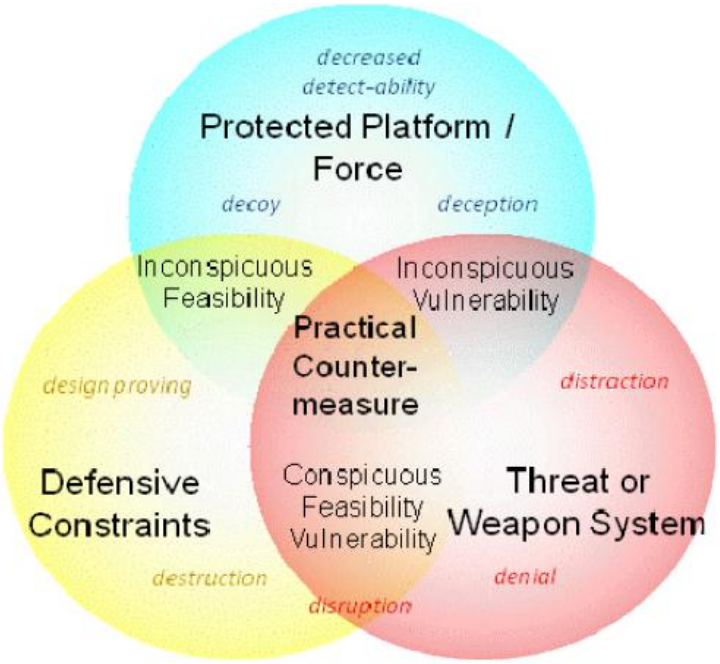

Figure 1. Venn diagram of CM design considerations and spheres of influence

It follows that consideration of a countermeasure that uses more information from the protected platform and less from the Defensive Constrains and Threat or Weapon System, may be a decoy or deception as it is using data to make a better more attractive target then the protected platform. Also it could be considered that countermeasures with specific information from that threat weapon system may be exploiting a weakness and could be more likely to be a disruption, distraction or denial. This may lead a consideration to the design intention and the kind of information available, and also that using some types of countermeasure could perhaps betray to the enemy the kind and detail of information available. To protect from this betrayal of information the use of some kinds of countermeasure design intentions could be reserved to layers lower in an onion of protection within a kill chain and are focused to be countered with a counter intention in that onion of protection. These threat intentions and countermeasure counter intention mappings leads to a consideration of the threat's complexity and a layered approach based on kill chain analysis, while providing a measured response at each layer of the onion of protection.

2. Engagement dynamics

Complex air platforms have the opportunity to both coordinate their countermeasure equipment and cooperate between platforms to form cooperative tactics. A lack of coordination and cooperation between platforms has historically caused some recorded losses notably in the naval domain, like the "Atlantic Conveyor" during the Falklands war between Britain and Argentina [4]. Within an engagement, dynamics can be considered in terms of the operator, software and how sensors are employed. In a countermeasure perspective this can change the order that modes or states that ELINT emissions appear in, coursing the consideration of understanding a threat and its intentions along a kill chain.

3. Understanding a threat and the discrimination view

For illustration purposes and for the de-classification obligation we can consider the S-75 SAM site as an example as there is much information available on-line and in literature. S-75 is a complex threat of subsystems working together and was a widely proliferated SAM. S-75 still remains a serious operational threat and illustrates some of the analysis mechanisms. The first part of any analysis is recognising patterns and discriminators for those patterns, this forms classifications and identities. Visually, as a land system S-75 could be recognised from the air or satellite by its classical distinctive star lay-down patterns with six single launchers around a radio locator (engagement radar). S-75 does not act alone but is part of a greater network of associated sensors and systems forming a kill chain. Some operating countries may see different associated systems employed in different regions. It may be argued that when preparing platform protection for a threat it is useful to prepare the specifics of what that system comprises, how they are linked and the sequences and concurrency of coordination for the kill chain. Ironically this causes a consideration of what the subsystem is, but also what the subsystem is not and therefore what are the subsystems tasks and intentions.

In the S-75 case as the new RF components were not ready from the outset of the development a crash programme to develop an extra S-75 variant that re-used S-25 RF components was started. This resulted in ELINT discriminators that can be observed to establish a class of variants of the S-75. The following rainbow spectrum diagram shows what parts of the system may be in-band of sensors. It can be additionally use with other axis or be decorated with other factors that may affect detection and intercept as well as jamming like power range, polarisation and other equipment limitations in sensing.

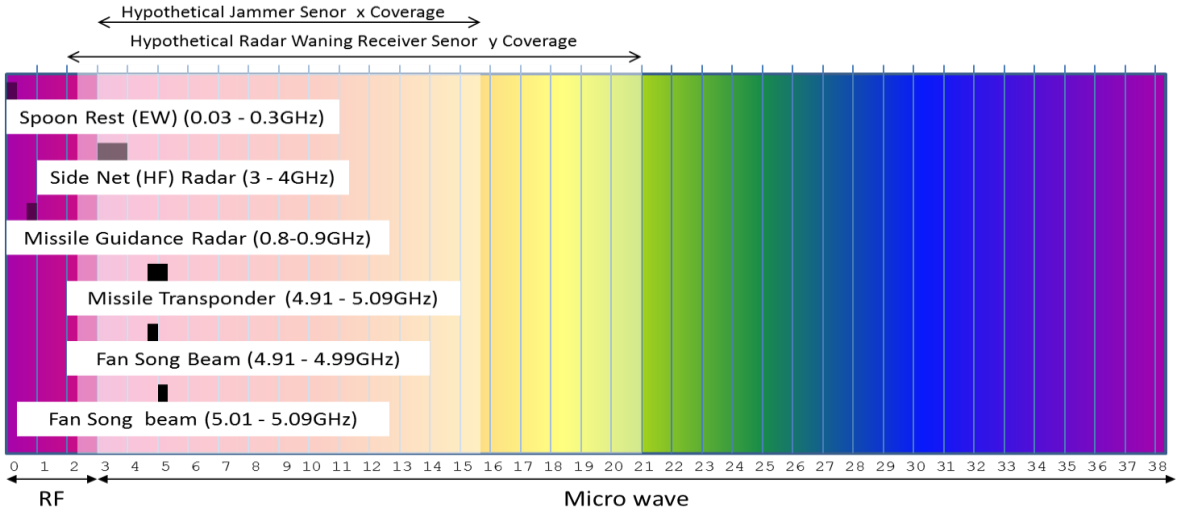

Figure 2. S-75 Rainbow spectrum

Also, helpfully the radar silhouette also reflects the ELINT discriminators allowing data convergence from imagery (IMINT) and (ELINT). During this paper the author is using a number of diagramming standards that he has formed to aid a threat analysis process to analyse the understanding

of a threat. In the example above the Sensor bandwidth are only illustrative and is not real specific equipment. Also, the bands of each of the sub-systems are taken from open sources and there is a list of references at the end of this paper.

As well as considering the ELINT discriminators S-75 also has IMINT and photographic discriminators (like the radar silhouette, shadow and aerial view lay-down).

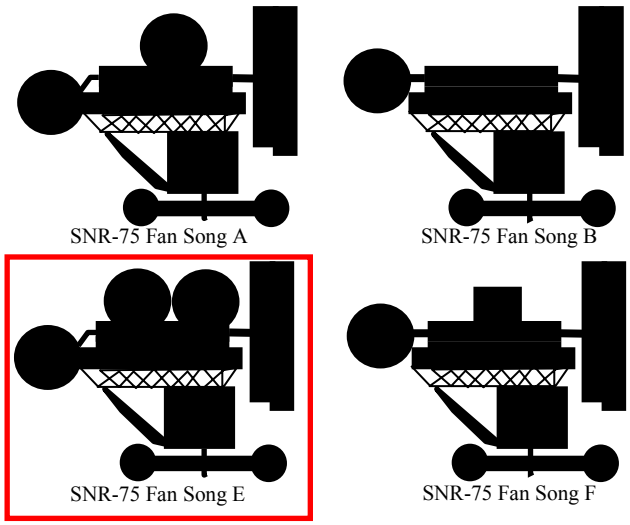

Figure 3. SNR-75 Lumps and bumps discriminators

Having defined the discriminators and classification of components, the analysis also looks from an operational view and this is a similar approach to MODAF [5].

4. The Operational View

The example diagramming technique shows relative search volumes of the systems used together with role designations: Early Warning (EW), Target Acquisition (TA), Height Finding (HF), Target Tracking Radar (TTR) and Missile or Weapon Engagement Zone (MEZ/WEZ). This presents an expectation of an order of encounter at differing block altitudes levels and operational vignettes scenarios, alternatively these diagrams can be 3D and use a multi system lay-downs with geographical terrain, thus embracing A2AD impact and the Integration of Air Defence Systems as IADS.

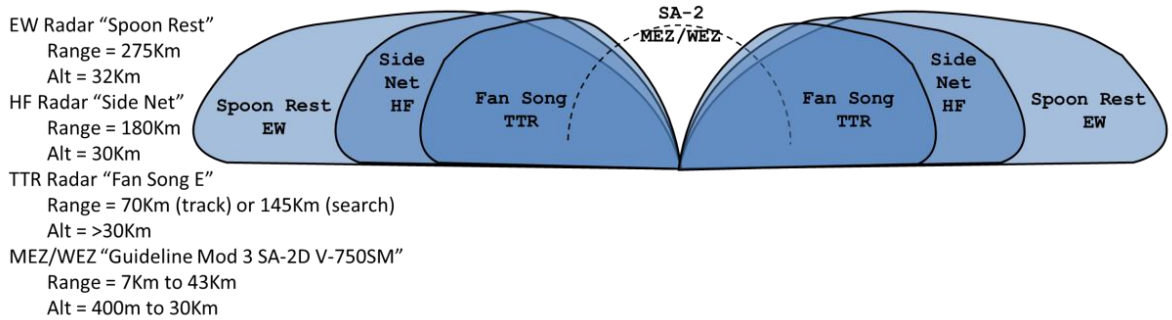

Figure 4. SAM System beam volumes and reaches

The way in which a SAM is employed may be in part driven by how data is handed off and what system capabilities are provided prior to the hand off. Knowledge of this may lead us to consider the SAM operators tasks that are trying to be conducted within the engagement and any observable discriminators we may expect in that engagement. This will form the SAM kill chain and extends from Find/Fix to Prosecute/Effect. The figure below is another example of the authors diagram

standards in a simplified form that has taken the ISTAR kill chain (Find, Fix, Recognise, Track, Engage and Effect) and applied it to the SAM operator point of view and over laid it with the different connection permutations through the connected subsystems.

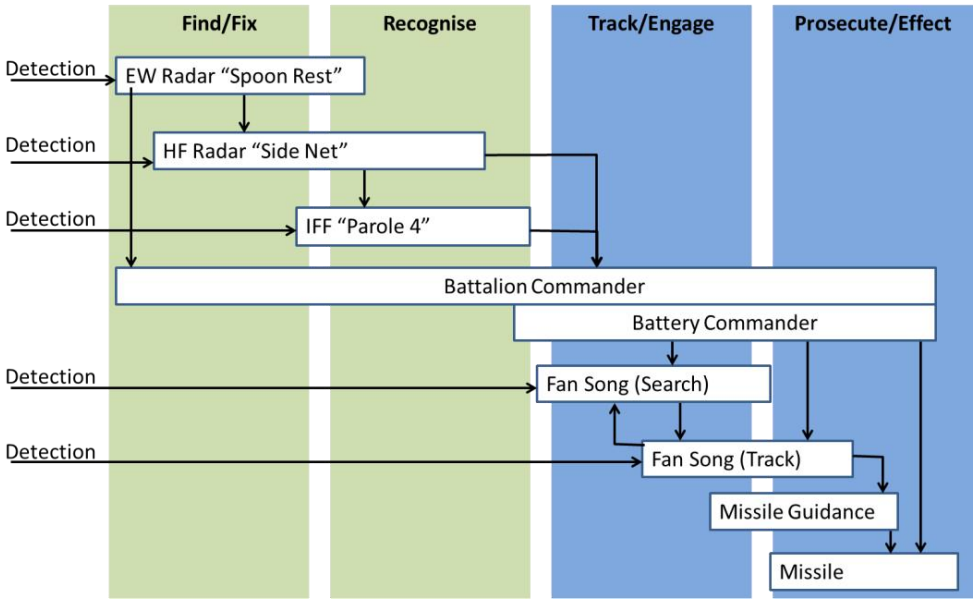

Figure 5. Extended kill chain

This is not the usual kill chain definition which might centre in only the blue area as "platform self-protection" and would centre on the primary threat stages of the fire control system, but instead extends the kill chain higher up the engagement to pre-engagement thus embracing the whole Air Defence System and its intentions. This embraces more of the integrated nature of an Air Defence System (IADS) as well as the concept of how different integrated systems are used as a concept of operation permutations. This is important for developing a countermeasure to interfere with those threat intentions directly, when combined with the previous diagrams we can see the connections sequences and what we may observe spatially and in the EM spectrum which allows the countermeasure effort to be focused on what can be affected and what threat intentions need to be focused on at each stage.

5. The system view

At this point the analysis has taken discriminators of components and operational view of employment, identifying intentions of the system in a kill chain and now moves to a Systems and Technology view point. When the say the SNR-75 Fan Song radar is considered alone it may cause the analysis of switches, displays and modes of operation to establish a state model of the components of the threat system. The diagram standard below is taken from UML and shows the system states and sub-states that are available. This is an important step on the way to creating specifications for a countermeasure to be effective and towards a computer simulation model in which to test it. It also maps how ELINT observables can be selected and the reason that they may be selected, further enhancing the operational view and kill chain analysis permutation and the reasoning for the intentions. Note that the H symbol in UML identifies that a state has a history and will be remembered if the state is re-entered and can be used for physical switch positions. The state motivations for state change can be identified as the intentions for that state change. Some of these states may have ELINT observables that may be used for trigger initiators for a countermeasure that are optimised for that state of the subsystem.

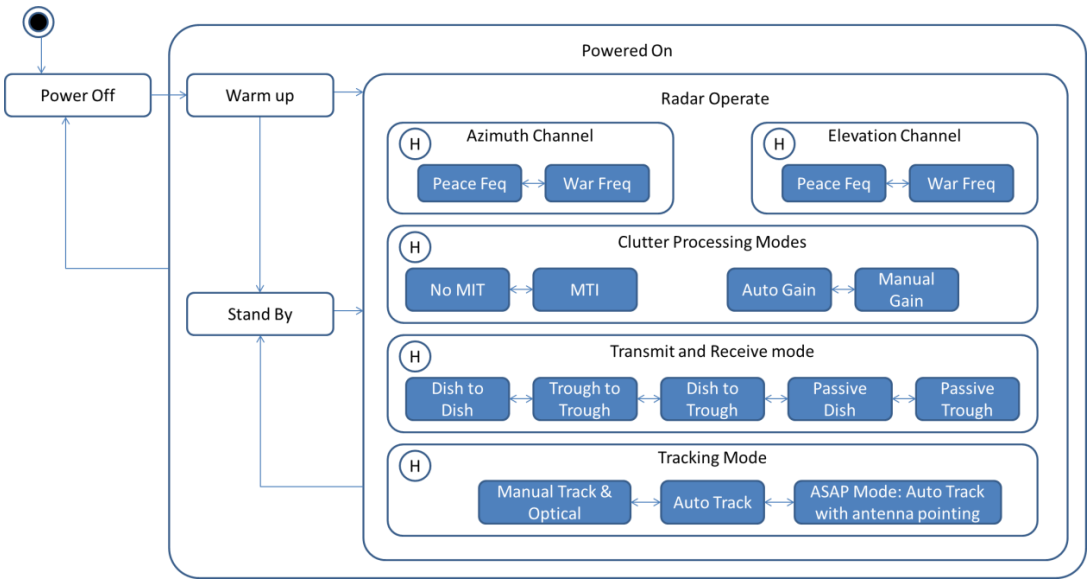

Figure 6. S-72 UML State diagram

From the above state diagram and aligned to ELINT observations a lower level subsystem version of a kill chain diagram is shown and is based on swim lane analysis and UML Interaction diagrams. It presents within a sub-system context of a component of an Air Defence System how the specific mode lines can be sequenced, with alternative permutations with the motivation indicated by ELINT observables called mode lines and how they move between the different swim lane intents. The "sub-intention" kill chain shows how ELINT observables may indicate operator selections and progress in the engagement or reaction to your countermeasure; these can be used for triggering optimised countermeasures that are optimised to switch positions and the engagement progresses through intentions.

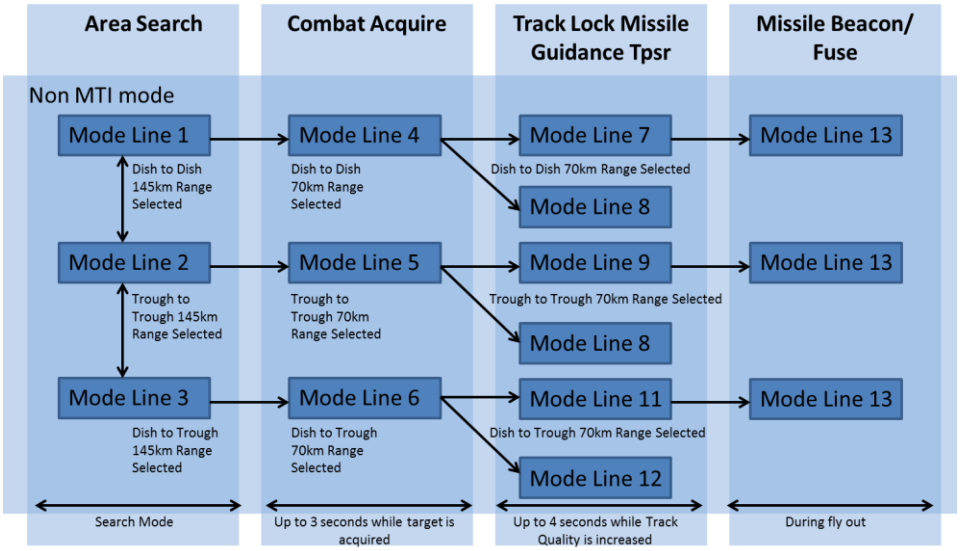

Figure 7. Swim lane: Mode line permutation diagram for auto track

It also may be noted that some indication of an expectation of the duration of the mode lines observation may be shown, and are implying performance requirements for a countermeasure system and for a countermeasure to be effective. Understanding the mode-lines and the possible order in which they can be observed helps to align countermeasure tactics and map onto the ELINT discriminators. While also improving understanding of the operator intent of specific permutation

through that chain. Also, for a temporal assessment for when the countermeasure needs to be effective an illustration of the "Phases of Flight" depiction can be shown, that may highlight when and how the effector / projectile in the engagement is guided under separate "phases of flight". This again implies performance and timing synchronisation requirements of countermeasure elements against equipment and programming capabilities.

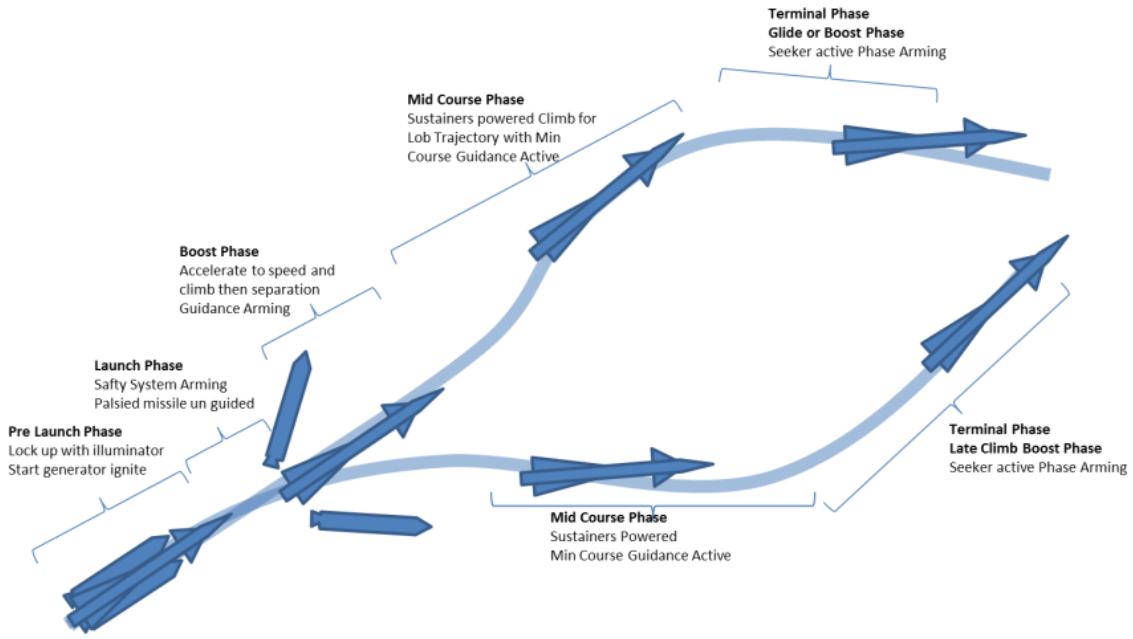

Figure 8. "Phases of flight" illustration

In this illustration we used a generic SAM instead for the Phases of flight as S-75 is command guided only. This diagram demonstrates how a software model for assessment will be configured and the timing and events that a countermeasure may need to be effective against the guiding radar or the seeker with perhaps guidance laws and type in each phase. This means a number of countermeasures can be used that are designed for different intentions to effect different parts of the flight. These might be attached to different mode-line sequence triggers initiator such that the countermeasure becomes re-active to the operator and phases of flight or are simultaneous against many aspects of the guidance of the SAM missile. When considering the states and modes it is also useful to consider a system block diagram that represents the order and precedence of processing within the radar and seeker. Again this is not an S-75 example, but instead is part of a Mono pulse Doppler system.

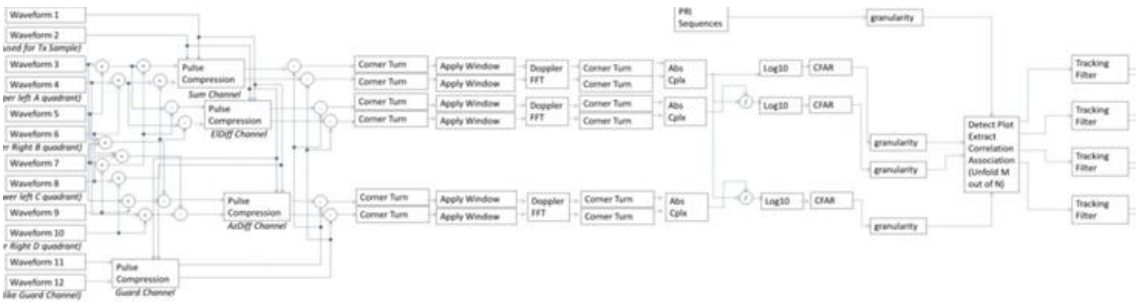

Figure 9. Signal and processing block diagram

The processing block diagram is particularly important as many of a threat system: Strengths, Capabilities, Weaknesses and Opportunities are exposed from vulnerabilities and hardenings in the system design. This analysis can be tested when capabilities and observations of the system are combined and implemented within a Simulation and Modelling environment such as CounterWorX-

PROTECT. Representation of the signal processing chain allows for targeting of vulnerabilities within the signal processing to be exploited.

6. Countermeasure simulation and modelling

The use of a single software model for threat analysis and countermeasures assessment gives consistency from the Weapon System Analysis to countermeasure development processes and takes advantage of a common software model representation of the system understanding. It should be noted that the: state model, phases of flight, kill chain, mode line sequences and signal and processing chain block diagrams presented here and their information is represent-able into the CounterWorX-PROTECT Simulation and Modelling system making for a low abstraction of the threat analysis into the model. This is useful for validation while not compromising the original threat analysis when fitted to a model. The combination of diagramming information provides a representation of the complete complex system to prepare a software model in a synthetic engagement environment that simulates the complete engagement possibilities and permutations of use. It therefore may follow that some sequences can be completely deterministically repeatable unlike live trials, or control asynchronous events such as the lack of synchronisation of equipment or accuracy and uncertainty in human operators using stochastic analysis.

7. Countermeasure tactic

The author's earlier presented work in 2012 in episodic (state-full) Countermeasure and Common Countermeasure Communication Language (C3L) [6] [7] presented as a framework for Reactive and Adaptive countermeasure specifications and its aim for autonomous system's self-protection. This work was furthered in the University of Lincoln in an MSc degree [2]. The nature of that work abstracted the textual countermeasure mark-up language into a graphical Model Driven Architecture (MDA) with the view to aiding the bridge of terminology and the view points from three key stakeholder groups: Scientists and engineers, Operational crews and mission data programming professionals. The MSc MDA research had literature reviewed and comparatively studied the application of established software development diagramming and system engineering methodologies. It is also noted that within the MSc's "Further Research" chapter 12 that: an extension to the C3L language could allow the emitter mode-line sequences to be described in a reactive and adaptive way and this is a feature of a PhD research project within the University of Sheffield.

8. The onion of protection mapping

Applying the multi-view threat analysis diagramming techniques, which was based on discriminators, operational and system views, the Venn diagram of countermeasure design consideration and Spheres of Influence can be applied to an onion of protection. It should be pointed out that when we describe a countermeasure design consideration in the Venn diagram it depicts the countermeasure's design intention and not an ECM jammer technique capability. For example, in some literature a deception countermeasure is a range or velocity gate steal, but it should be noted that the design consideration is deception and the ECM techniques are the gate steal as the design consideration may sequence a number of ECM techniques into Smart techniques. The countermeasure design consideration indicates the counter intention of a tactic in this case. Shown in the table below is the Onion of protection's Layer Levels (layer 1 is the outer most) and the countermeasure design consideration, Sphere of Influence mapped with the kill chain intentions:

Table 1. Onion of protection layers

Onion Layer Kill Chain Intention	Spheres of Influence (Dominate Data need)	CM Design Considerations	Comment
Layer 1 Find	Protected Platform	Decreased Detectability	Counter the detection or the behaviours that would make the protected platform standout as a threat this could be by an Early Warning, Air Search or Ground Control Intercept radar. Tactic is directed directly at the kill chain intention and is inconspicuous. Using knowledge of own strengths and weaknesses.
Layer 2 Fix	Protected Platform	Decreased Detectability Decoy & Deception	Counter Target Acquisition or Height Finding radars with deception and decoying could be used to degrade information or counter an altitude fix.
Layer 3 Recognise	Protected Platform Weapon System	Decreased Detectability Decoy & Deception Distraction Denial Disruption	Counter recognition with measures directed at causing confusion to delaying the assessment of your classification or identity, Recognition can be based on behaviour or use special radar modes like NCI.
Layer 4 Track	Protected Platform Weapon System	Decreased Detectability Decoy & Deception Distraction Denial Disruption	Counter threat track convergence with disruption, distraction and denials, could be a Target Acquisition radar or higher data rate search mode.
Layer 5 Engage	Defensive Constraints Weapon System Protected Platform	Decreased Detectability Decoy & Deception Distraction Denial Disruption Destruction	Defeat threat using all capabilities available hard and soft kill dependant of ROE and is traditional platform self-protection. May use Break Lock and Signal Processing and Tracking targeted tactics.
Layer 6 Prosecute / Effect	Defensive Constraints Weapon System Protected Platform	Decreased Detectability Decoy & Deception Distraction Denial Disruption Destruction	Defeat threat using all capabilities available hard and soft kill and is traditional platform self-protection. May use Break Lock and Signal and Track Processing targeted tactics and may have simultaneous techniques employed against seeker and radars.

9. Summary and conclusions

This paper presented some simplified forms of the diagramming techniques for use in analysis of complex threats and started with discriminators and associations of complex system components, the next set of diagramming techniques centre on the operational view and moved into the System view specification that would be used to create a software model, finally the C3L countermeasure description language described the countermeasures in a reactive adaptive and re-useable form. These representations and the facilities they provide for a mapping to the countermeasures based on data needs defined in the Venn diagram onto an onion or protection based on the mapping of countermeasure design considerations for a measured response such that the countermeasures are provided at higher levels up the kill chain in pre-engagement and help to reserve advertising knowledge of classified Weapon system information in the outer layers of the onion of protection.

This paper provides a backbone spine for analysis when considering complex air platforms, how to counter them incrementally while focused on countering the intention at each incremental layer. It also highlights a collaborative environment in diagramming allowing different stakeholders from different views to contribute meaningfully. Finally, the facility of the analysis as part of an EWOS provision are applicable to IADS and A2AD problems analysis.

References

[1] Brig. Gen. Alex Grynkewich (2017), The Future of Air Superiority, Part III: Defeating A2/AD, [Online], WarOnTheRocks, Available from https://warontherocks.com/2017/01/the-future-of-air-superiority-part-iii-defeating-a2ad [Accessed 24 September 2018].
[2] Rudd-Orthner, R N M. (2015) To investigate a collaborative environment enabling stakeholders, engineers, scientists and mission dataset technicians to cooperate effectively over disciplined boundaries in the field of countermeasures and platform self-protection.. MSc Thesis University of Lincoln.
[3] Wikipedia (2008): OODA Loop. [Online], Wikipedia Available from http://en.wikipedia.org/wiki/OODA_loop [Accessed 21 December 2013].
[4] Kenneth L Privratsky (2014), Logistics in the Falklands War, Pen and Sward Ltd Military Barnsley, P 123.
[5] Dickerson, C Mavris, D. (2010), Architecture and principles of systems engineering, CRC Press, London, P 179
[6] AOC EW Saudi Arabia (3rd): EW Saudi Arabia (3rd) (2013), [Online], TangentLinks Available from http://tangentlink.com/wp-content/uploads/2014/07/6.-A-Formal- Countermeasure-Language-a-Common-Generic-Architectu-Richard-Rudd-Orthner.pdf [Accessed 5 December 2014].
[7] Rudd-Orthner, R. (2013) A Formal Countermeasures Language: A Common Generic Architecture as a Technology Enabler for Future Electronic Warfare Capability. [AOC Page 105 EW Saudi Arabia], EW Analysis and Countermeasures Training, Association of the Old Crews Saudi Arabia Chapter, 12 November 2013.

Open Source Internet Links used in the S-75 example:

[8] commons.wikimedia.org/wiki/File:Fan_Song_fire_control_radar_of_the_SA-2_SAMsystem. JPEG Available from 17 June 2014
[9] en.citizendium.org/wiki/FAN_SONG_(radar) Available from 5 Dec 2008 at 17:50
[10] en.wikipedia.org/wiki/Fan_Song 16 April 2015 at 17:14
[11] en.wikipedia.org/wiki/S-75_Dvina Available from 19 May 2015 at 11:57
[12] fas.org/nuke/guide/russia/airdefv-75.htm Available from 23 June 2000 at 14:29
[13] www.armyrecognition.com/russia_russian_missile_system_vehicle_uk/sa-2_guideline_s-75_dvina_desna_vol...system_technical_data_sheet_specification.
[14] www.ausairpower.net/APA-Engagement-Fire-Control.html Available from 27 Jan 2014 at 11:18
[15] www.ausairpower.net/APA-S-75-Volkhov.html Available from 27 Jan 2014 at 11:18
[16] www.ausairpower.net/APA-SNR-75-Fan-Song.html Available from 27 Jan 2014 at 11:18
[17] www.globalsecurity.org/military/world/russia/fan-song.htm Available from 11 July 2011 at 15:48
[18] www.militaryfactory.com/armor/detail.asp?armor_id=133 Available from 2015
[19] www.nationalelectronicsmuseum.org/fansong.shtml Available from 2012
[20] www.nationalmuseum.af.mil/factsheets/factsheet.asp?id=1884 Available from 23 Oct 2009
[21] www.nationalmuseum.af.mil/factsheets/factshee.asp?id=334 Available from 03 April 2015
[22] www.radartutorial.eu/19/kartei/karte406.en.html Available from 2015More references