Simulation Architecture for Network Centric Sensors and Electronic Warfare Engagements

Reeshen Reddy, Brian Burmeister, Solly Manamela, Ushik Mewalal, Umur Kathree
Council for Scientific and Industrial Research (CSIR), Defense Peace, Safety and Security (DPSS)
Pretoria, South Africa
rreddy@csir.co.za, bburmeister@csir.co.za,
smanamela@csir.co.za, umewalal@csir.co.za, ukathree@csir.co.za

ABSTRACT

Network Centric Operations describe the modern form of military action in the information age. Networked Sensors allow for information superiority acting as a force multiplier, greater lethality and increased survivability. The modern network centric battlefield requires advanced modelling and simulation (M&S) to predict performance of sensors and the effect of their performance on platform protection and weapon lethality in many-on-many scenarios.

This paper presents a novel M&S architecture for engagement scenarios in modern network centric operations involving sensors such as radar, communication and electronic receivers, effectors such as missiles, jammers, chaff and systems that combine inputs and outputs of sensors and effectors such as combat management suites (CMS), threat evaluation weapon assignment (TEWA), aircraft mission computers (AMC) and command and control (C2) systems.

The key differentiators between system centric, platform centric and network centric scenarios are described. Emergent properties of networked platforms and systems are analyzed to arrive at the emergent functions of sensor management, threat evaluation and effector assignment. General requirements for each of these functions are expanded upon by inferring from typical examples in the air, naval and ground domains and the conceptual modelling approach for each described.

The architecture presents a shift from traditional time line or scripted based simulation and requires a certain degree of autonomy where the simulated platforms and systems decide on an action depending on the scenario and pre-defined rules of operation. This fundamentally requires systems triggering actions or commands of other systems via the functions of sensor management, threat evaluation and effector assignment. The increased autonomy of the simulated platforms lends to modelling engagements with cognitive systems using artificial intelligence and machine learning.

This novel M&S architecture allows for a closer representation of Network Centric Operations for Sensors and Electronic Warfare Engagement Simulation (SEWES) and enables advanced tactics and doctrine development.

ABOUT THE AUTHORS

Reeshen Reddy is a Research Group Leader at the Council for Scientific and Industrial Research (CSIR) leading the Electronic Warfare Modelling Simulation and Training (EWMST) group in Pretoria, South Africa. He is a registered professional engineer with Engineering Council of South Africa (ECSA) (Pr.Eng), a senior member at the IEEE (SMIEEE). He holds a Masters of Engineering (distinction) from the University of Pretoria, a Bachelor of Engineering Honours (Microelectronics) from the University of Pretoria and a Bachelors of Engineering (Electronic Engineering) from the University of KwaZulu-Natal. He has chaired a number of technical and non-technical workgroups and developed technology demonstrators in the fields of Digital Radio Frequency Memories (DRFM), Radar Cross Section Measurement (RCS) Facilities, Advanced Digital Receivers, Radar Threat Simulators, Electronic Counter Measure (ECM) simulators and Reactive Jammers. He currently provides technical leadership and strategic direction in the field of Electronic Warfare (EW) Modelling Simulation and is responsible for product, engineering and strategy of advanced EW simulations including the Sensors and Electronic Warfare Engagement Simulator (SEWES) and Dynamic Scenario Planner (DSP). He is currently researching and developing in the fields of Phased Array EW, Cognitive EW, Cyber EW, EW Optimization, Spectrum Sharing and Next Generation EW simulation architectures.

Brian Burmeister graduated from the University of Pretoria in 1999 with a Bachelor in Electronic Engineering. In 2005 he received his Honors degree in Electronic Engineering and received his Masters degree in Electronic Engineering in 2009, both also from the University of Pretoria. He has been employed at the Council for Scientific and Industrial Research (CSIR) since 2000, and worked in the area of radar and EW research and application as a principle engineer until 2016. During this time he specialized in radar and EW signal processing, algorithm development as well as Modelling & Simulation. He led various international teams of development engineers in the establishment of engagement simulation facilities in support of military research and development, test, evaluation and training activities. Currently Brian manages International Business Development for the Radar and EW area within the CSIR.

Solly Manamela is a Software Engineer at the Council for Scientific and Industrial Research (CSIR) in the Electronic Warfare Modelling Simulation and Training (EWMST) research group in Pretoria, South Africa. He is a registered candidate engineer with the Engineering Council of South Africa (ECSA). He holds a Bachelor of Science in Electrical Engineering from the University of the Witwatersrand. He has worked in the fields of road traffic monitoring and load control for two and half years as an Integration Engineer. He is currently involved in the field of Electronic Warfare (EW) Modelling and Simulation, and is responsible for the development of advanced EW simulations including the Sensors and Electronic Warfare Engagement Simulator (SEWES) and Dynamic Scenario Planner (DSP). He is currently researching and developing in the fields of RF Propagation Modelling, Spectrum Sharing and Next Generation EW simulation architectures.

Ushik Mewalal is an Electronic Warfare Modelling and Simulation Software Engineer at the Council for Scientific and Industrial Research (CSIR) in Pretoria, South Africa. He is a registered candidate engineer with Engineering Council of South Africa (ECSA). He holds a Bachelor of Science in Electronic Engineering from the University of KwaZulu-Natal. He currently provides research and technical product development in the field of Electronic Warfare (EW) Modelling Simulation.

Umur Kathree is an Electronic Warfare Modelling and Simulation Software Engineer at the Council for Scientific and Industrial Research (CSIR) in Pretoria, South Africa and is part of the Electronic Warfare Modelling Simulation and Training (EWMST) group. He holds a Master of Science in Engineering (specializing in Radar and Electronic Warfare) as well as a Bachelor of Science in Engineering (specializing in Electrical and Electronic Engineering) from the University of Cape Town. He has worked in the fields of Radar Signal Processing, Radar Modelling and Simulation and Synthetic Aperture Radar (SAR) specifically in the areas of SAR Imagery Analysis, SAR Interferometry (InSAR) and SAR Polarimetry (PolSAR). He has also published papers in High Range Resolution (HRR) techniques and InSAR. He is currently involved in the field of Electronic Warfare (EW) Modelling and Simulation and is responsible for the development of advanced EW simulations including the Sensors and Electronic Warfare Engagement Simulator (SEWES) and Dynamic Scenario Planner (DSP). He is currently researching and developing in the fields of Next Generation EW simulation architectures.

Simulation Architecture for Network Centric Sensors and Electronic Warfare Engagements

Reeshen Reddy, Brian Burmeister, Solly Manamela, Ushik Mewalal, Umur Kathree
Council for Scientific and Industrial Research (CSIR), Defense Peace, Safety and Security (DPSS)
Pretoria, South Africa
rreddy@csir.co.za, bburmeister@csir.co.za,
smanamela@csir.co.za, umewalal@csir.co.za, ukathree@csir.co.za

MODERN NETWORK CENTRIC ENGAGEMENT SIMULATIONS

Electronics technology has played an increasingly important role in military operations. The invention of the radio, radio direction finder, radar and radar guided missiles (Neri, 2006) have made a dramatic increase in the sophistication, effectiveness and lethality of weapon systems. Electronic Warfare (EW) is any military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy typically using military electronics. EW has been employed in all war fighting domains to detect, intercept, classify, protect, counter and attack adversary's weapon systems that employ advanced sensors such as active electronically scanned phased array (AESA) radar.

The rise of electronic technology has given rise to the information age where data enabled by advanced communication networks has further increased the sophistication of weapon systems, sensors and the corresponding EW systems. Network Centric Operations describe the modern form of military action in the information age. Networked Sensors allow for information superiority acting as a force multiplier, greater lethality and increased survivability (Alberts, et al., 2000). Modern weapon systems and platforms seldom operate in isolation; but rather may be thought of as networks of connected platforms, sensors, weapons, effectors with complex data exchange that govern their behavior and performance.

The modern network centric battlefield requires advanced modelling and simulation (M&S) to predict performance of sensors and the effect of their performance on platform protection and weapon lethality in many-on-many scenarios. This paper will focus on sensors and EW engagement M&S i.e. fully constructive M&S that models the modern networked battlefield and the role sensors and EW play in outcome of tactical engagements. A novel M&S architecture shall be presented for a closer representation of Network Centric Operations for Sensors and Electronic Warfare Engagements and enables advanced tactics and doctrine development.

DEVELOPMENT APPROACH

The Council for Scientific and Industrial Research (CSIR) begun work during the early 2000's on EW engagement M&S software for the South African National Defense Force (SANDF) to better perform EW effectiveness evaluation, doctrine development and training. The CSIR created the Sensors and Electronic Warfare Engagement Simulator (SEWES) which is a few-on-few EW simulation environment. Any number of platforms, consisting of any number of sensors and EW systems, can engage each other in a simulated environment. The primary use of SEWES is to investigate the role of sensors and EW in platform survivability and weapon effectiveness.

Work prior to the advent of SEWES by the CSIR primarily focused on system centric M&S. A typical simulation would be a search radar against a noise jammer. During the early 2000's, a shift to platform centric simulation occurred leading to the development of SEWES which is a dynamic simulation environment that models time line behavior with multiple platforms carrying multiple sensors, effectors and weapons in a time-scripted, scalable, distributed and parallel simulation.

The CSIR interacts with a number of South African and International Defense Research Institutes collectively realizing the need to develop EW engagement software that can model network centric warfare. The modelling of not only the platforms and systems but the interactions, data exchange and communications between them underpin network centric M&S and represent the next-generation SEWES architecture.

TERMINOLOGY

The following are terminology as used in this paper. A “Platform” is a ground, naval or air body that has 3D movement and carries sensors, effectors and weapons. Typical platforms are aircraft, ships and vehicles. A “System” represents a sensor, effector or weapon that is on-board a platform. Typical systems are a radars, receivers, jammers and missiles.

In realizing an advanced network centric sensors and EW engagement simulator, there are various steps or phases that would occur. “Development Time” is the time at which a new platform or system model is being created and integrated into the simulation. “Plan Time” is the time at which an already created platform or system model may be used to plan a scenario with multiple platforms and systems and to configure their scenario specific parameters, command/controls and dynamic movements. “Build Time” is the time in which the already created platform or system models are used for the specific scenario and the entire simulation is built into an executable format. “Run Time” is the time at which the simulation is ran using the built scenario. Each model interacts with the environment and other models. Each model logs information and stores to files using the SEWES Run functionality. “Visualization and Analysis (VnA) Time” is the time at which results of simulations that have been ran may be visualized and analyzed.

A “local system” refers to a system model that resides on the same platform model as the system model of interest. A “local link” refers to a communication link for data exchange between system models residing on the same platform model.

A “global system” refers to a system model that resides on a different platform model as the system model of interest. A “global link” refers to a communication link for data exchange between system models residing on different platform models.

TAXONOMY OF REACTIVENESS IN ENGAGMENT SIMULATIONS

In order to develop a robust network centric architecture, a conceptual taxonomy of reactiveness in engagement simulations is developed. This conceptual framework defines three levels of reactiveness.

System Centric Simulations

System centric reactiveness is when a system’s behavior is governed by its own inputs/outputs and its own algorithms (see Figure 1). A typical example would be a tracking radar on a vehicle that reacts based on the pulses it transmits and receives. This level of simulation is adequate for one-on-one simulations

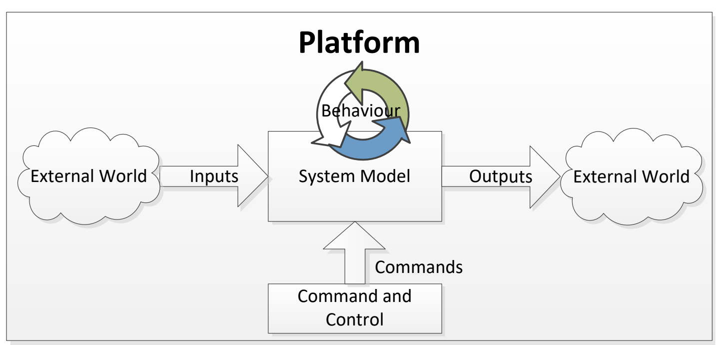

Figure 1. System Centric Reactive

Platform Centric Simulations

Platform centric reactiveness is when a system’s behavior is governed not only by its own inputs/outputs and its own algorithms but additionally other local systems inputs/outputs (see Figure 2). An example would be the tracking radar that is now coupled to a search radar which both resides on a vehicle. The detections from the search radar could be used to designate the tracking radar towards potential targets.

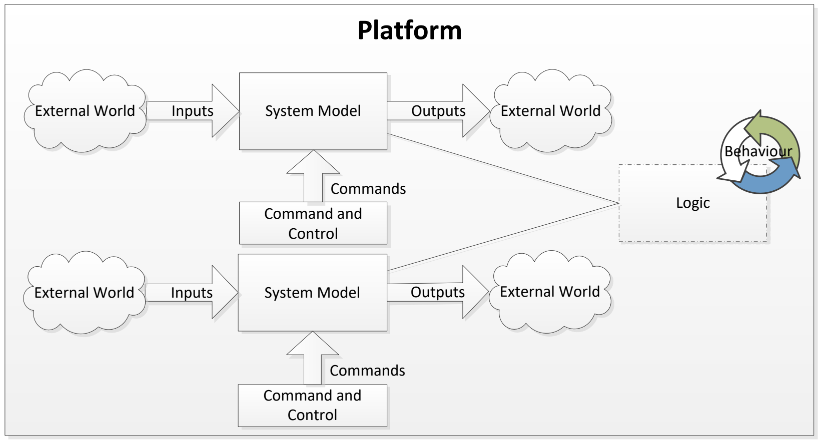

Figure 2. Platform Centric Reactive

Network Centric Simulations

Network centric reactiveness is when a system's behavior is governed not only by its own inputs/outputs and its own algorithms but additionally other local and global systems inputs/outputs (see Figure 3). An example could be a guided missile on an aircraft that is commanded to launch towards a target from a vehicle with a search and tracking radar on the ground providing detections and tracks on the target.

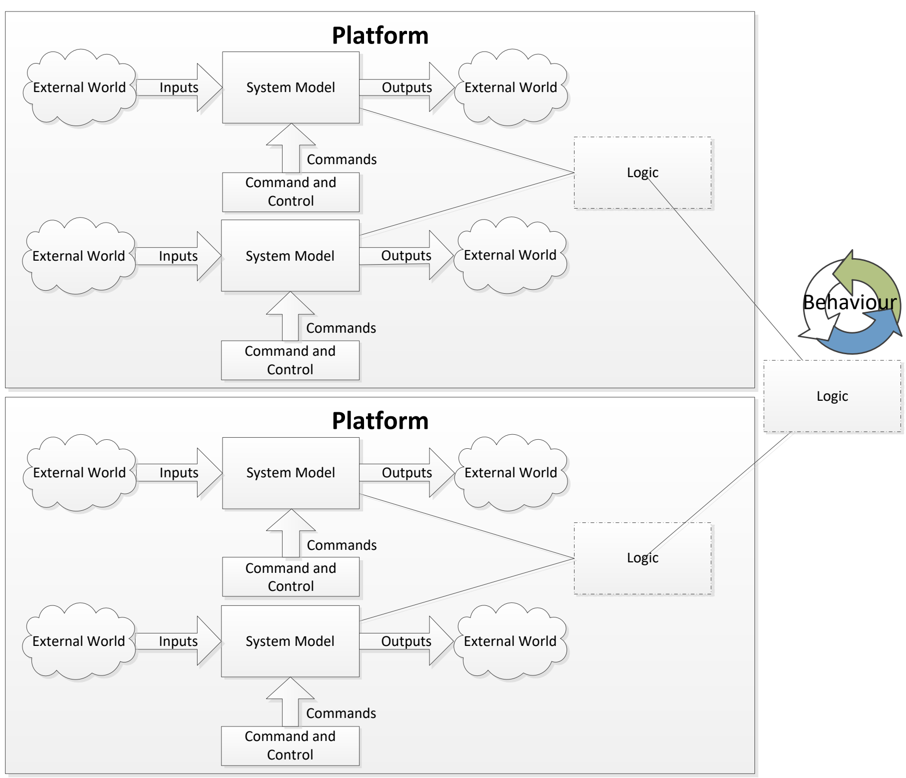

Figure 3. Network Centric Reactive

REAL-WORLD USE CASES AND REQUIRMENTS

Network centric SEWES has a large array of real world use cases. In order to realize a M&S architecture that is generic to support this large array of applications; a process of extracting the emergent functions required by way of inference from common use cases is applied. A common use case in the ground, naval and air domains is analyzed. While not exhaustive, these typical examples are illustrative of scenarios the architecture would be required to support.

Ground

A typical battlefield scenario encountered in the land domain is a Threat Evaluation Weapons Assignment (TEWA) system. The TEWA is typically used in Integrated Defense Systems for Ground Based Air Defense Systems (GBADS). The objective of a TEWA is to identify all threats, rank the threats and select the best weapon system to use against each threat. A TEWA is a closed-loop system in that after attempting to neutralize a threat, it evaluates if the threat was successfully neutralized and it takes further steps based on the success or lack thereof. Threats are constantly evaluated and weapons assigned based on the ever changing environment.

A typical TEWA would have an array of sensors such as radars and receivers connected to it. Furthermore, the TEWA would be aware of sensors state, type, priority and information they provide. Data fusion of the sensor information may also take place to improve the overall performance.

The TEWA would also be aware of friendly platforms and assets to defend. In order to realize this function, a threat library database would be used to classify all threats and their probable intent. The threats are then ranked; the ranking can be based on the threat capability index or threat intent. The TEWA would typically also employ different strategies or rules stipulating which threat to engage using which weapon. A threat-weapon correlation database may be utilized by this function to assist with the assignment of weapons to threats.

Naval

Modern naval vessels are outfitted with an array of sensors, weapons and countermeasures. The coordination of the systems is often achieved by a Combat Management Suite (CMS) on-board of naval vessels that integrates all the ship's sensors and information of other parties for real time situational awareness. The sensors on-board the ship are typically a multitude of radar such as 3D multifunction radar, 2D surface search radar, fire control radar, sonar and EW receivers. The CMS would need to integrate and fuse all of the sensor detections and tracks

The naval vessel would also typically be outfitted with an array of weapons such as cruise missiles, surface-to-air missiles, ballistic missiles, anti-ship missiles, guns and torpedoes. In order to defend against threats, active and passive EW are frequently employed including EW jammers, decoys, chaff and flares. The CMS would typically also perform threat evaluation based on a variety of models and modes. Some modes may be fully automatic, requiring no human intervention to counter certain fast approaching threats.

Air

Modern aircraft are designed to reduce pilot workload while simultaneously enhancing the overall mission effectiveness. Typical fighter aircraft are equipped with an aircraft mission computer (AMC) or similar computing system that is responsible for situational awareness and combat systems control. The AMC is typically responsible for control, coordination and management of sensors on board the aircraft and directing the information to the appropriate display unit or next functionality unit. In addition, the AMC is responsible for executive scheduling, initialization, and mode control of sensors.

The sensors on-board a modern aircraft are able to typically perform detection, tracking, classification and identification. The AMC combines multiple sensor inputs from the aircrafts various avionics and prepare data for various control panels and display surfaces in the cockpit. Aircraft still tend to rely on the pilot for weapons delivery however the AMC greatly simplifies this task by easing weapon selection and preparation, store selection, fire control algorithms and targeting.

Emergent Functions

Typical EW engagement simulations are specific to system, scenario or domain. While each domain and network centric engagement is unique with their own nuances, the following emergent properties are inferred requirements across all domains: Sensor Management, Threat Evaluation and Effector Assignment (SM-TE-EA). In addition, with many engagements requiring joint, interagency and multinational (JIM) operations, the impact of a simulation architecture generic enough to cater for multiple domains in the modern battlefield is enhanced. The network centric SEWES architecture is designed to realize the SM-TE-EA emergent functions in a scalable, distributed and parallel simulation.

NETWORK CENTRIC M&S ARCHITECTURE

Simulation Structure

The conceptual structure of network centric SEWES consists of any number of platforms, populated with any number of systems which can engage each other in a simulated engagement (see Figure 4). The specific platform can be a Naval, Air or Ground platform. Each platform has its own command and control center from where all interactions between the various system models are controlled and where the behavior of these systems can be observed. Each platform also has the emergent functions of Sensor Management, Threat Evaluation and Effector Assignment (SM-TE-EA) to achieve network centric behavior. The simulation architecture also provides components for simulation setup, simulation control, display, data logging and 3D visualization.

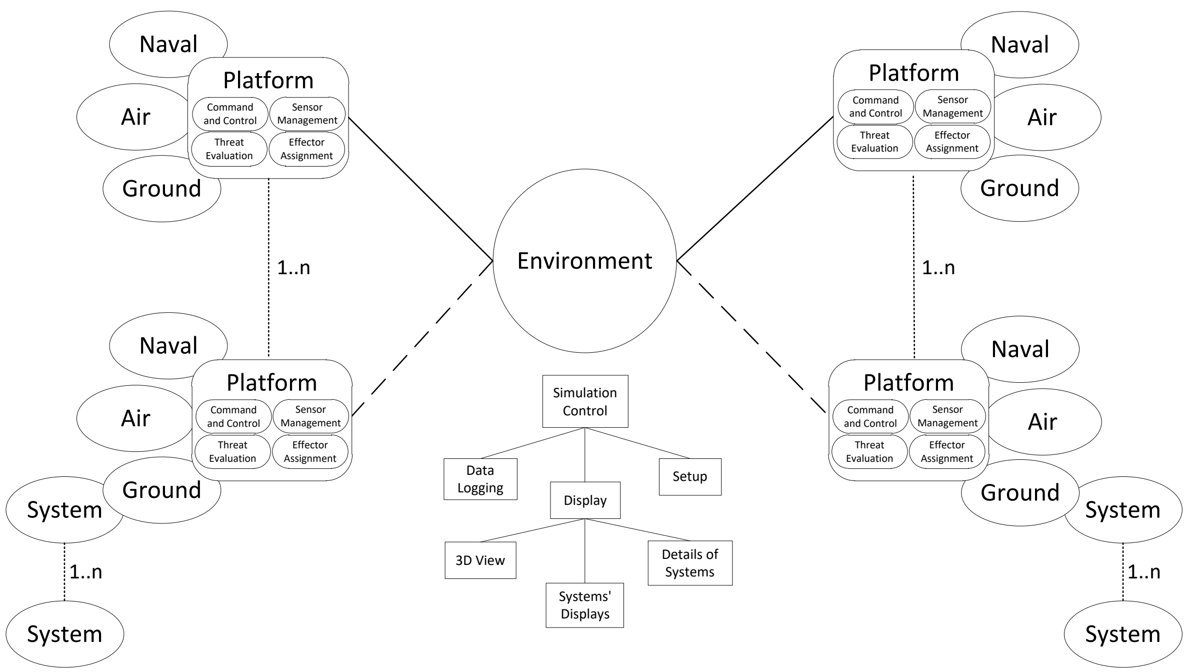

Figure 4. Conceptual Structure of network centric SEWES

Functional Design of Sensor Management

The Sensor Management module has the ability to be aware of all relevant emissions, and all sensors connected local to the platform. This includes their capability, mode, spatial position, type, state, priority and the information produced.

Using input from different sensors, the Sensor Management functionality is responsible for performing data fusion to obtain detailed information of the environment, and objects in the environment. It is also responsible for relaying information between the sensors, administering the coordinated usage of the sensors, and changing the states of the sensors as required. State, modes and designation of sensors are done through this module.

The output of the Sensor Management module is a list of all detected objects and their associated properties (e.g. spatial, tracks) which is then an input to the Threat Evaluation module (see Figure 5). Depending on the information generated from sensors, the Sensor Management module collects relevant data about object detections (e.g. from search radars), track information (e.g. from tracking radars) and Radio Frequency (RF) detections (e.g. from radar warning receivers).

The Sensor Management module also implements sensor priorities (e.g. a radar with higher tracking accuracy may be prioritized over a radar with lower tracking accuracy). Multiple sources of information from sensors may be combined using data fusion to produce more consistent, accurate, or useful information (e.g. multiple radar tracks may be fused to provide a more accurate track).

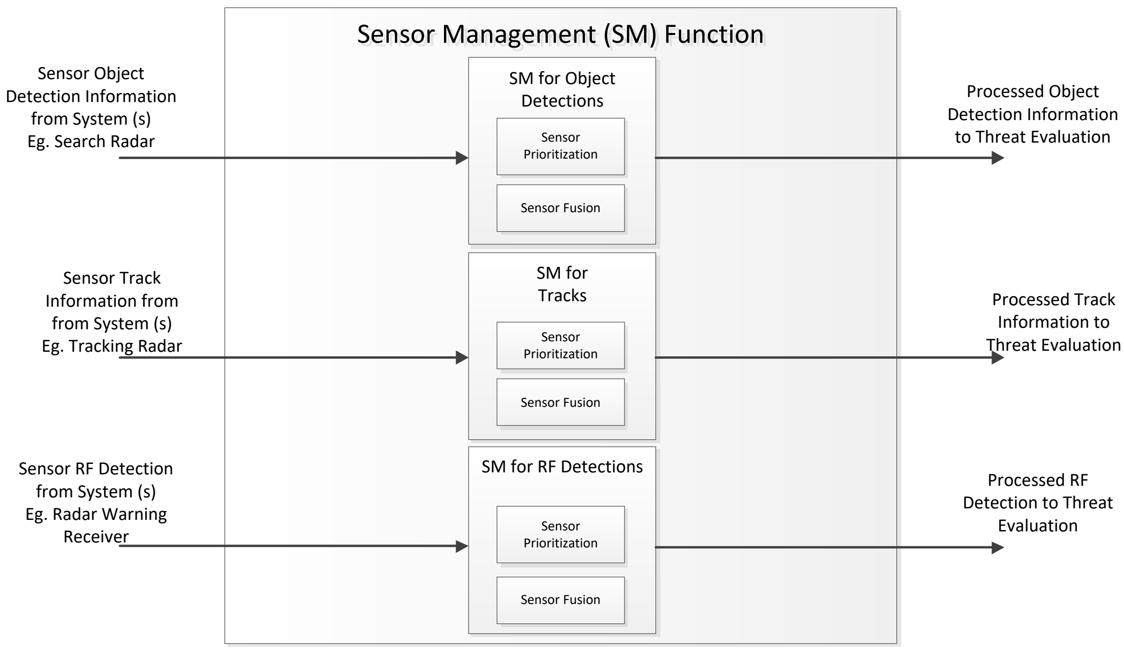

Figure 5. Sensor Management conceptual block diagram

Functional Design of Threat Evaluation

The Threat Evaluation module is responsible for evaluating and ranking information from the Sensor Management module and thereafter passing ranked threat information to the Effector Assignment module (see Figure 6). The association of target to threat information together with the identification and ranking of threat information is performed in this module. The threat ranking functionality could be achieved via a number of possible models including flagging, deterministic or probabilistic models. The threat evaluation function may use a traditional threat database or more advanced cognitive techniques using machine learning, artificial intelligence and optimization. A combination of different algorithms may also be used for threat evaluation of object detections (e.g. target feature analysis), track information (e.g. non-cooperative target recognition) and Radio Frequency (RF) detections (e.g. specific emitter identification).

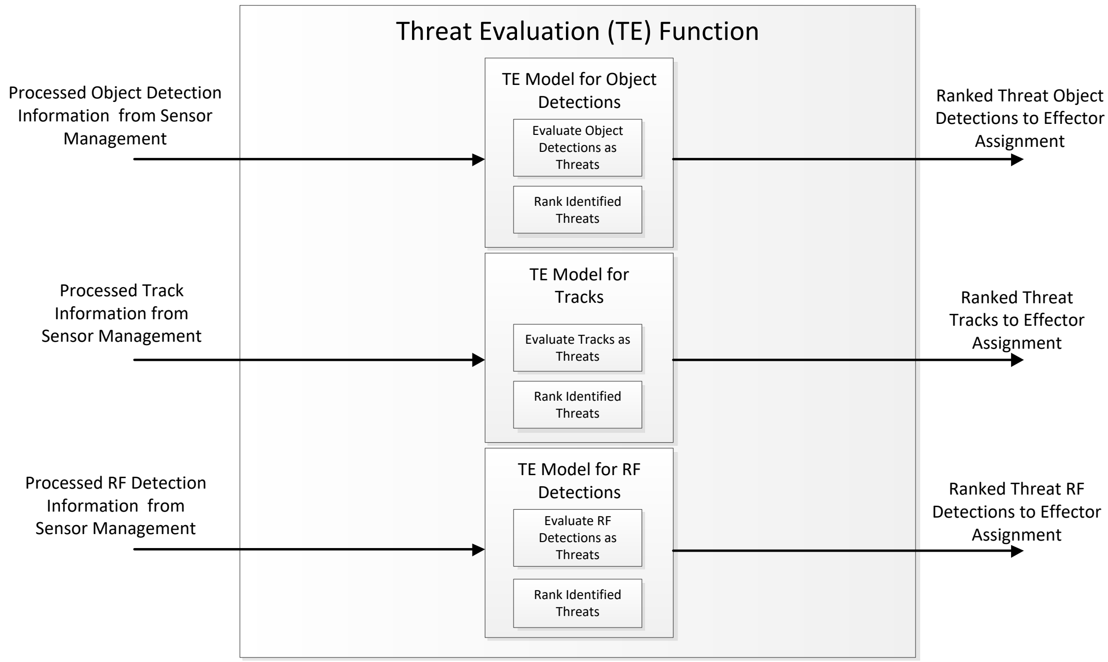

Figure 6. Threat Evaluation conceptual block diagram

Functional Design of Effector Assignment

The Effector Assignment module is responsible for determining which effector or combination of effectors to deploy to best address threats based on the ranked threat list from the Threat Evaluation module. The deployment of effectors against threats could employ various defense strategies such as preferential or subtractive.

Upon receiving ranked threat information from the Threat Evaluation module, various methods that may involve the use of fire control algorithms, threat weapon correlation databases and countermeasure correlation databases may be used to designate commands to effectors. Additionally, the output of the Effector Assignment module is the designation commands sent to systems on the platform to address ranked threat object detections, tracks, and RF detections according to their respective priorities. The respective command management blocks perform the evaluation of appropriate effector designations based on the ranked threats (see Figure 7).

In the event that the same effector is assigned to address their respective threats, the succeeding function will address the conflict based on the availability of effector type and threat with highest priority, and assigning the next available adequate effector.

The last stage of the Effector Assignment block determines designation commands based on the type of effector to be used. This output is sent to the appropriate effector on the platform for execution. Typical systems/effectors used to address threat object detections are tracking radar to track the object and EW receivers to determine if the detected objects have RF emissions. Typical systems/effectors used to address threat tracks are missiles, guns, bombs, chaff and flares to engage and counter the tracked target or missile. Typical systems/effectors used to address threat RF detections are jammers, chaff and anti-radiation missiles to counter detected radar.

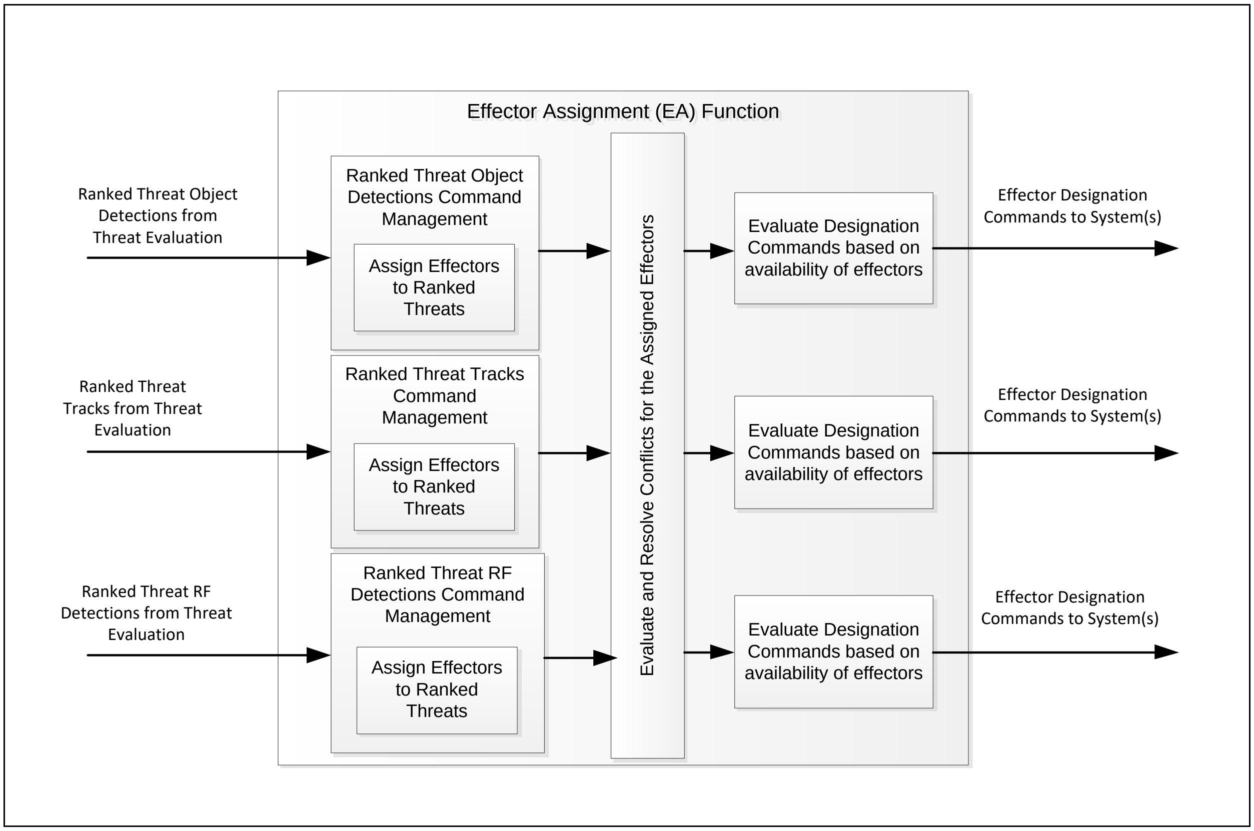

Figure 7. Effector Assignment conceptual block diagram

Sensor Management, Threat Evaluation and Weapon assignment for Network Centric SEWES

In a typical network centric SEWES, multiple platforms (Naval, Air or Ground) each populated with their own systems (e.g. radars, jammers, chaff, radar warning receivers, radios, and missiles) engage each other. Each platform is populated with a SM-TE-EA model that gives the platform the ability to achieve platform centric reactiveness.

Network centric reactiveness is achieved with the communication between platforms and their respective SM-TE-EA models via point-to-point, mesh, ring, star or hybrid topologies. An exhaustive list of communication topologies used in network centric warfare is beyond the scope of this paper; rather a few real-world use cases are shown.

RESULTS

Results of Architecture for Aircraft Strike Mission

In this result, a squadron of two aircraft is performing a strike mission against a ground target (see Figure 8). The ground target is defended by search radar and a command guided surface-to-air missile. The first aircraft maintains a stand-off position and performs jamming against the radar. The second aircraft carries chaff for self-protection the air-to-surface missile for the strike. Both aircraft are exchanging information via the SM-TE-EA modules in a network centric operation. In this result, the SM-TE-EA is configured to represent aircraft mission computers. The chaff on the strike aircraft and jammer on the stand-off aircraft are be coordinated via the SM-TE-EA modules to enhance the jamming effectiveness and improve the mission success.

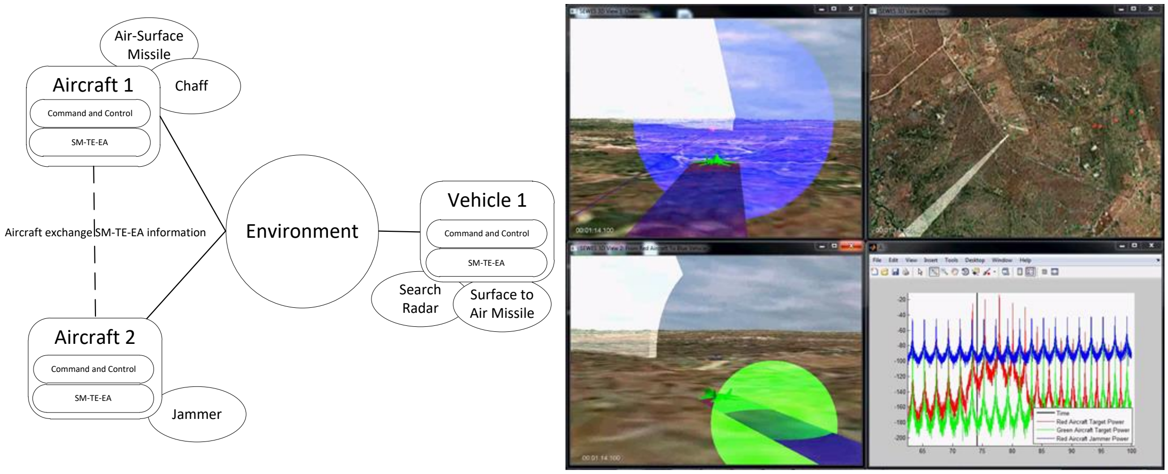

Figure 8. Results of Architecture for Aircraft Strike Mission

Results of Architecture for Ship Air Defense

In this result, two aircraft each fitted with anti-ship missiles are engaging a ship with active and passive countermeasures (see Figure 9). The aircraft perform a coordinated attack with the sensor management function on each radar exchanging data from the aircraft AESA radar. The effector assignment function on the aircraft performs a coordinated weapons delivery of an anti-ship missile from each aircraft with the aim of overloading the ships defenses.

The ship SM-TE-EA is configured to function as a CMS. The radar and receivers on the ship are used to scan for incoming missile threats. Sensor management fuses data from the ship sensors. The threat evaluation function of the ship is used to rank detected object information and prioritize fast incoming objects such as missiles. Once the ship detects two incoming anti-ship missiles; the ships effectors (jammers and chaff) and deployed to create a coordinated jamming technique to enhance the ships survivability.

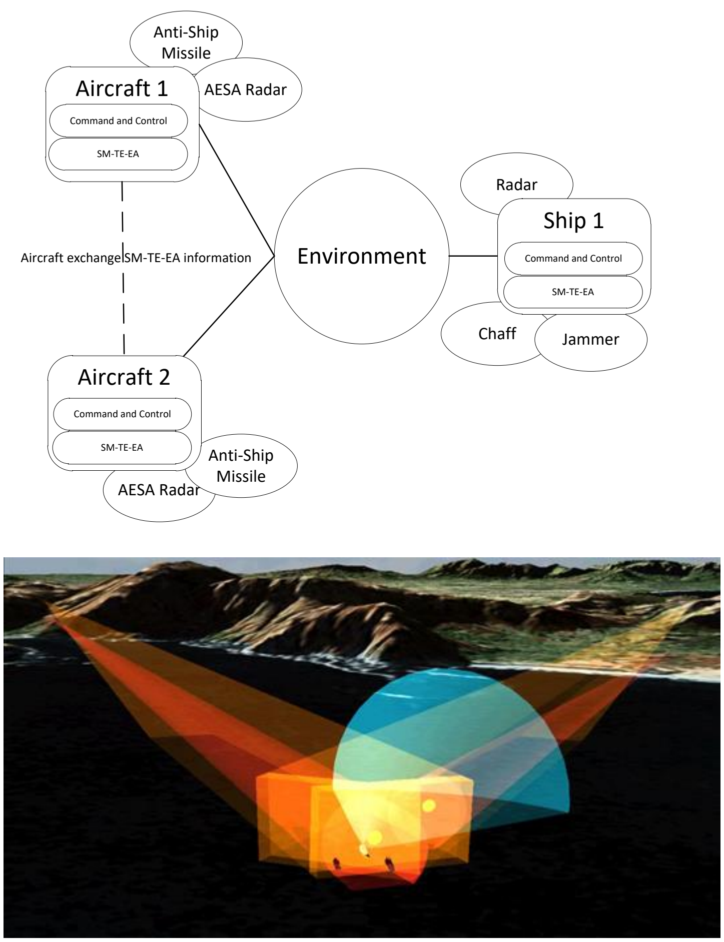

Figure 9. Results of Architecture for Ship Air Defense

CONCLUSION

This paper presented a novel M&S architecture for engagement scenarios in modern network centric operations involving sensors such as radar, communication and electronic receivers, effectors such as missiles, jammers, chaff and systems that combine inputs and outputs of sensors and effectors. A conceptual taxonomy of reactiveness in engagement simulations was developed highlighting key differentiators between system centric, platform centric and network centric scenarios. Emergent properties of networked platforms and systems were analyzed to arrive at the emergent functions of sensor management, threat evaluation and effector assignment.

The network centric SEWES architecture was presented with any number of platforms, populated with any number of systems which can engage each other in a simulated engagement. Each platform is populated with a SM-TE-EA module to realize network centric behavior. Results for the architecture using typical use cases were presented. The increased autonomy of the simulated platforms lends to modelling engagements with cognitive systems using artificial intelligence and machine learning. This novel M&S architecture allows for a closer representation of Network Centric Operations for SEWES and enables advanced tactics and doctrine development.

FUTURE WORK

The network centric SEWES architecture allows for the development of more complex and advanced doctrine and tactics in the modern battlefield. The development and evaluation of advanced network centric concept of operations in a fully constructive simulation is possible. The architecture is also conducive to perform research and development of cognitive EW that uses artificial intelligence, machine learning and mathematical optimization algorithms.

ACKNOWLEDGEMENTS

TBD

REFERENCES

Alberts, D.S., et. al. (2000), Network Centric Warfare: Developing and Leveraging Information Superiority, 2nd Edition (Revised), CCRP, 2000.

Filippo Neri “Introduction to Electronic Defense Systems” second edition, 2006.

D. C. Schleher, “Electronic Warfare in the Information Age”, 1999, *(Artech house radar library (hardcover))*. Artech House Publishers.

H. Naeem, A. Masood, M. Hussain and S. A. Khan, “A semi-automated dynamic approach to threat evaluation and optimal defensive resource allocation,” in *ICIC'09 Proceedings of the 5th international conference on Emerging intelligent computing technology and applications*, Ulsan, South Korea, 2009.

H. Naeem and A. Masood, “A two-stage dynamic decision support based optimal threat evaluation and defensive resource scheduling algorithm for multi air-borne threats: Asset-based dynamic weapon scheduling using artificial intelligence techinques,” in *2010 IEEE 9th International Conference on Cyberntic Intelligent Systems*, United Kingdom, 2010.

Z.-J. Lee, C.-Y. Lee and S.-F. Su, “An immunity-based ant colony optimization algorithm for solving weapon–target assignment problem,” in *Applied Soft Computing*, 2002.

J. Uchytil, “Assessing the operational value of situational awareness for aegis and ship self defense system (SSDS) platforms through the application of the knowledge value added (KVA) methodology,” The NPS Institutional Archive, Monterey, California, 2006.

America's Navy, “Americas Navy,” Office of Corporate Communication (SEA 00D), 18 Dec. 2013. [Online]. Available: http://www.navy.mil/navydata/fact_display.asp?cid=2100&tid=450&ct=2. [Accessed 15 Feb. 2017]

General Dynamics Mission Systems, 2017. [Online]. Available: https://gdmissionsystems.com/maritime-strategic/airborne-systems/advanced-mission-computer/