

DSIA JOURNAL

A Quarterly Publication of the Defense Systems Information Analysis Center

Volume 7 • Number 3 • Summer 2020

CHARACTERIZATION OF

COMPOSITE

SPACED ARMOR PERFORMANCE

page 49

PAGE 4

PREDICTING HYDRODYNAMIC RAM
DAMAGE IN BONDED COMPOSITE
TANKS USING PROGRESSIVE
DAMAGE FAILURE

PAGE 17

DETECTION AND CLASSIFICATION
OF SMALL UAS FOR THREAT
NEUTRALIZATION

PAGE 23

PASSIVE COHERENT LOCATION
RADAR - THE SILENT THREAT

PAGE 29

SYSTEMS ENGINEERING OF
AUTONOMY: FRAMEWORKS FOR
MUM-T ARCHITECTURE

PAGE 42

DAUNTING CHALLENGE OF DRONE
DEFENSE

PAGE 56

INVESTIGATING SURFACE
STRUCTURES FOR INFRARED
SIGNATURE MANAGEMENT



Distribution Statement A: Approved for
public release; distribution is unlimited.



JOURNAL

VOLUME 7 | NUMBER 3 | SUMMER 2020

Editor-in-Chief: Brian Benesch

Copy Editor: Maria Brady

Art Director: Melissa Gestido

On the Cover:

(Photo Source: 123rf.com)

The *DSIAC Journal* is a quarterly publication of the Defense Systems Information Analysis Center (DSIAC). DSIAC is a DoD Information Analysis Center (IAC) sponsored by the Defense Technical Information Center (DTIC) with policy oversight provided by the Office of the Under Secretary of Defense (OUSD) for Research and Engineering (R&E). DSIAC is operated by the SURVICE Engineering Company with support from Georgia Tech Research Institute, Texas Research Institute/Austin, and The Johns Hopkins University.

Copyright © 2020 by the SURVICE Engineering Company. This journal was developed by SURVICE under DSIAC contract FA8075-14-D-0001. The Government has unlimited free use of and access to this publication and its contents, in both print and electronic versions. Subject to the rights of the Government, this document (print and electronic versions) and the contents contained within it are protected by U.S. copyright law and may not be copied, automated, resold, or redistributed to multiple users without the written permission of DSIAC. If automation of the technical content for other than personal use, or for multiple simultaneous user access to the journal, is desired, please contact DSIAC at 443.360.4600 for written approval.

Reference herein to any specific commercial products, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or DSIAC. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or DSIAC and shall not be used for advertising or product endorsement purposes.

Distribution Statement A: Approved for public release; distribution is unlimited.

ISSN 2471-3392 (Print)
ISSN 2471-3406 (Online)



ABOUT DSIAC

PURPOSE

The purpose of DSIAC is to provide information research and analysis for DoD and federal government users to stimulate innovation, foster collaboration, and eliminate redundancy.

MISSION

The mission of DSIAC is to generate, collect, analyze, synthesize, and disseminate scientific and technical information (STI) to DoD and federal government users and industry contractors.

VISION

DSIAC will be the premier information research partner and curator of technology advancements and trends for the defense systems community.

PRODUCTS & SERVICES

TECHNICAL INQUIRIES (TIs)

We offer 4 hours of information research (free to the client) in response to TIs on any of the DSIAC subject areas. TI response efforts generally include literature searches, document requests, answers to technical questions, and expert referrals.

CORE ANALYSIS TASKS (CATs)

We conduct customer-funded CATs that expand the limits of the free TI service. Each CAT is limited to a \$1M ceiling and can be incrementally funded.

STI UPLOAD

We collect STI, adding it to the DTIC collection, and ensuring that the body of information is available to share with the DoD community.

TRAINING/EVENTS

We participate, host, and promote key technical conferences and forums to engage and network with the science and technology (S&T) community.

PROMOTION

We publicize events, technologies, information research products, and more to our +75,000 members.

INFORMATION RESEARCH PRODUCTS

We publish the DSIAC Journal, Defense Systems Digest, State-of-the-Art Reports (SOARs), and many other information products available for free electronic download on our website.

HOW TO CONTACT DSIAC

Ted Welsh
DSIAC Director

Brian Benesch
DSIAC Technical Project Lead

DSIAC HEADQUARTERS

4695 Millennium Drive
Belcamp, MD 21017-1505
Office: 443.360.4600
Fax: 410.272.6763
Email: contact@dsiac.org ▶

WPAFB SATELLITE OFFICE

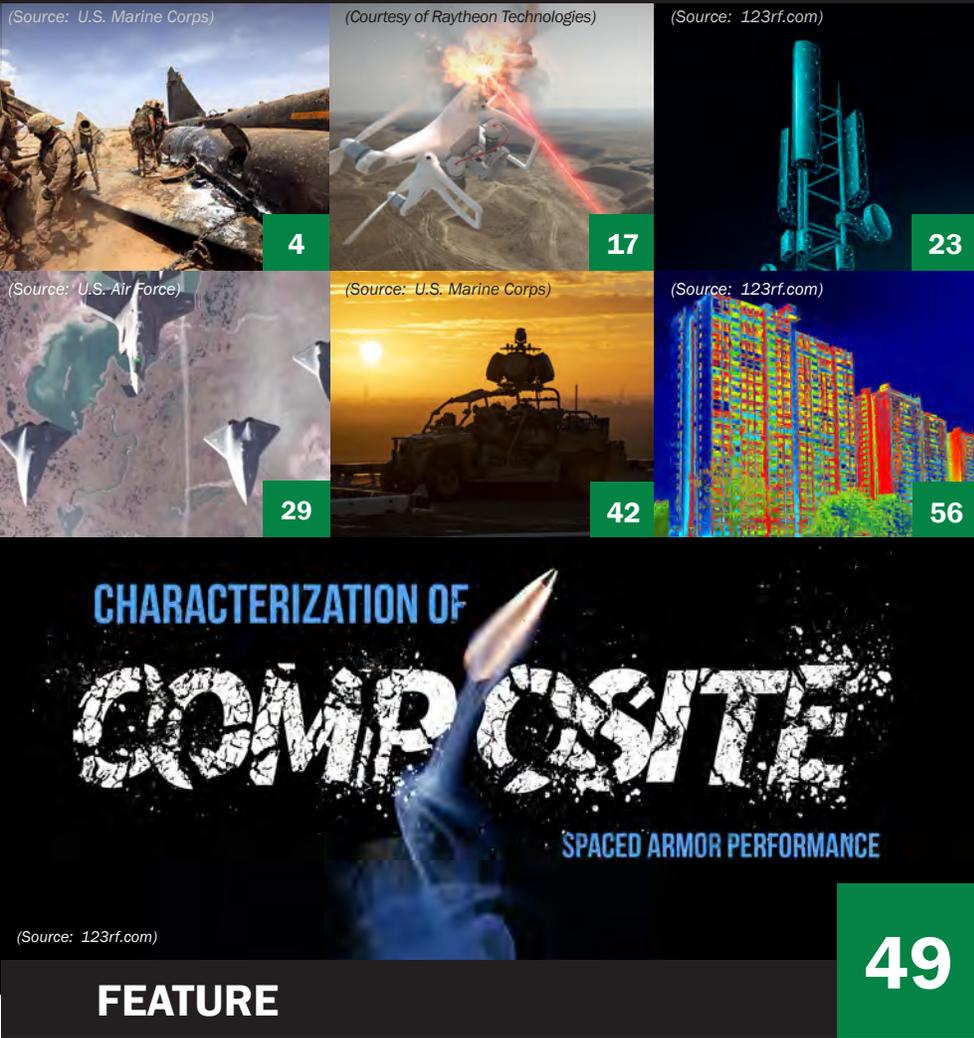
704 TG/OL-AC/DSIAC
2700 D Street, Building 1661
Wright-Patterson AFB, OH 45433-7403
Office: 937.255.3828
DSN: 785.3828
Fax: 937.255.9673

DSIAC TECHNICAL CONTRACTING OFFICER REPRESENTATIVE (TCOR)

Peggy M. Wagner
704 TG/OL-AC
2700 D Street, Building 1661
Wright-Patterson AFB, OH 45433-7403
Office: 937.255.4126

DSIAC COR/PROGRAM MANAGEMENT ANALYST

Emese Horvath
IAC Program Management Office (DTIC-I)
8725 John J. Kingman Road
Fort Belvoir, VA 22060
Office: 571.448.9753



CONTENTS

- 4**
SV

Predicting Hydrodynamic Ram Damage in Bonded Composite Tanks Using Progressive Damage Failure
By Teddy Sedalor and David Fleming
- 17**
MS

Detection and Classification of Small UAS for Threat Neutralization
By Matthew Henderson
- 23**
MS

Passive Coherent Location Radar - The Silent Threat
By Ronald Mathis
- 29**
AS

Systems Engineering of Autonomy: Frameworks for MUM-T Architecture
By Michael Woudenberg, Mark Waltensperger, Troy Shideler, and Jerry Franke
- 42**
AS

Daunting Challenge of Drone Defense
By Kyle Carnahan and Darrel Zeh
- 56**
MS

Investigating Surface Structures for Infrared Signature Management
By Dennis Metz

Characterization of Composite Spaced Armor Performance

By Sierra I. Semel, Daniel V. Camp, John T. Hailer, and Delaney M. Jordan

AM SV Advanced Materials/Survivability and Vulnerability

Composite spaced armor is an unconventional armor system capable of stopping armor-piercing (AP) projectiles at lower areal density than possible with traditional metallic and ceramic armor systems, which makes it especially attractive for weight-sensitive applications. Prior testing of this armor system at normal obliquity has shown that it has great potential to reduce weight in aircraft systems while providing improved ballistics protection. The anisotropic nature of this composite spaced armor further differentiates it from traditional metallic and ceramic systems because its directionally-dependent mechanical properties cause performance to vary with obliquity. Ballistics testing evaluated normal and oblique angle impacts to quantify performance at a range of shot lines. Results indicate that for a limited range of oblique shot lines, the tumble of the bullet is reduced, resulting in degraded performance of the armor. However, this can be mitigated through system-level design and careful integration or eliminated with technology solutions.

Focus Area Key:

<p>AM Advanced Materials</p> <p>AS Autonomous Systems</p> <p>DE Directed Energy</p> <p>SF Special Feature</p>	<p>EN Energetics</p> <p>MS Military Systems</p> <p>NW Non-lethal Weapons</p>	<p>RQ RMQSI</p> <p>SV Survivability & Vulnerability</p> <p>WS Weapon Systems</p>
---	---	---

NOTE TO OUR READERS:

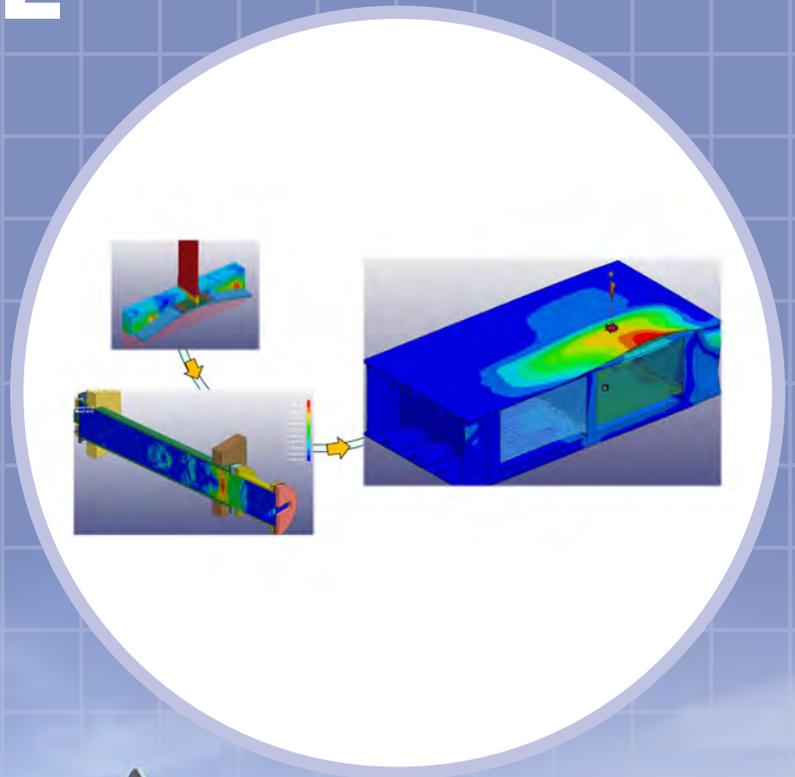
This will be the last edition of the *DSIAC Journal*. Please check our website for future articles and publications on featured scientific and technical information.

(Source: U.S. Marine Corps)

PREDICTING HYDRODYNAMIC RAM DAMAGE

in Bonded Composite
Tanks Using Progressive
Damage Failure

By Teddy Sedalor and David Fleming



INTRODUCTION

Hydrodynamic ram (HRAM) occurs when a fluid-filled enclosure is penetrated with a high-velocity projectile. A classic case, and common occurrence, is when an aircraft with fuel in the wings is impacted with a fast-moving projectile, which could be foreign object debris or a ballistic projectile. The projectile will, in turn, transfer its energy to the fluid, creating a very high pressure, which is then imparted onto the structure. The pressure is very high near the projectile, on the order of 10 ksi [1], and decreases exponentially away from the projectile but may still carry enough energy to cause catastrophic damage. The structural damage can range from complete structural failure to damage of critical internal components. There is also damage at the projectile entry and sometimes exit locations. The nature of this damage will vary based on the nature of the material (e.g., whether it is metallic or composite). HRAM occurs in four distant phases, with each phase accompanied by its own pressure distribution [1]. The phases are shock, drag, cavitation, and exit [1].

The shock phase describes the introduction of the projectile into the medium. The structure and fluid will be impulsively-loaded upon impact, creating a hemispherical shock wave in the fluid that travels at the speed of sound. The effect of this shock is dispersive and encountered by most of the structure in its path and cone of the wave. Depending on the scenario, this phase may exhibit the highest pressure.

The next phase is the drag phase. During this phase, the stagnation pressure generated from the projectile slows it down in the fluid, transferring its energy to the fluid. The pressure generated in this stage tends to be lower than in the shock phase.

The most complicated stage, known as cavitation, occurs next. At this stage, the projectile creates a cavity behind it by violently moving the fluid, creating a low-pressure region, which causes some of the fluid to vaporize or cavitate to establish equilibrium. A combination of high pressure and gravity causes the cavity to collapse, which sends a strong pressure pulse through the fluid and to the structure. This will usually result in oscillations with subsequent smaller pressure pulses.

The final stage is the exit stage. This stage is similar to impact damage when the projectile first hits the projectile except the wall at the exit is prestressed from the previous stage, which will magnify the damage. Based on the composition of the material and projectile characteristic, the critical damage from HRAM will focus around the projectile exit and/or the joints of the enclosure.

During aircraft design, the effect of HRAM must be accounted, usually through testing, to ensure that catastrophic damage does not result from an HRAM event (or damage from HRAM is manageable) [2]. To achieve this, two main tests methods are utilized. In one method, joints are isolated and tested to understand their HRAM resistance using a RamGun or universal testing machine. The other method is a complete test of the article of interest to an HRAM event. This is very effective, albeit expensive, which tends to limit the amount of testing that can be conducted.

Numerical methods have been used to understand and complement HRAM testing. This provides a cost-effective method for studying the event and reducing the testing scope. Numerical methods for HRAM analysis started from using the piston theory and went through iterations where the continuum

equations were finally incorporated. The current state of the art is combining an algorithm that can account for the drastic fluid movement without distortions and, at the same time, account for deformation of the structure [1]. The leading methods are arbitrary Lagrangian-Euler (ALE) and smooth particle hydrodynamics (SPH). Both methods have shown promise and are used by several researchers to study the event. While SPH tends to have more resolution, ALE seems to be the better option for larger articles [1].

A continuing trend in the aerospace industry is the increasing usage of composites, from about 1% in the 1960s to over 50% by weight currently, and with even higher percentages projected in the future [3]. As the industry builds confidence in composites, their use has transitioned to structural parts like the wings.

A recent trend accompanying composites is bonding structural composites instead of fastening them. This approach eliminates weight and bearing failure [4]. It also produces a better stress distribution around fasteners that is favorable for composites. Various analytical techniques are used to study bonded joints, including those developed by Hart-Smith and the Volkersen method. These methods can limit utility for analyzing complex structures and loading that would be experienced in a primary structure. Hence, finite-element analysis is used to assess bonded joints for primary structure, with cohesive zone modeling (CZM) at the forefront. CZM is a fracture mechanics technique that can track crack initiation and growth using an idealized representation of joint failure in terms of disbond and delamination [5, 6]. With the current trajectory of the aerospace industry, it is imperative to understand the effect of

HRAM on bonded-composite fuel tanks. This research aims to study HRAM in bonded composites and propose a numerical method to accurately assess damage. This approach will potentially save money on costly testing and provide insight into aircraft vulnerability early in the design process. The proposed method will combine ALE fluid-structure interaction (FSI) and CZM in LS-DNVA to predict damage using a building block approach.

ANALYSIS APPROACH

Penetration damage at the inlet and exit of a fuel tank can be modeled numerically with relative ease [1, 6]. The biggest challenge is damage prediction at the seams or joints of the fuel tank. Joint damage from HRAM is one of the critical modes of failure for both fastened and bonded structures; it can be even more catastrophic in bonded joints due to the threat of continuous delamination and disbond. A building block approach is used to build the numerical model for assessing tank damage in a bonded composite tank. The building block in Figure 1 is based on damage characterization at the joint level by using a local breakout model conducive for calibrating joint CZM properties. The calibrated model is then verified in a full-scale RamGun model [7]. Finally, the joint model is extrapolated to the complete fuel tank model.

A few different high strain rate test methods can be utilized to perform a joint-level test. One method is using a high-rate, universal testing machine. Heimbs et al. [8] used this method to test joints at a rate of 5 m/s. A more realistic method is using a RamGun or ram simulator to create HRAM fluid pressure in the presence of a joint. To operate the RamGun, a puck is shot with a gas gun at a cylindrical fluid chamber containing the test joint. Contact of

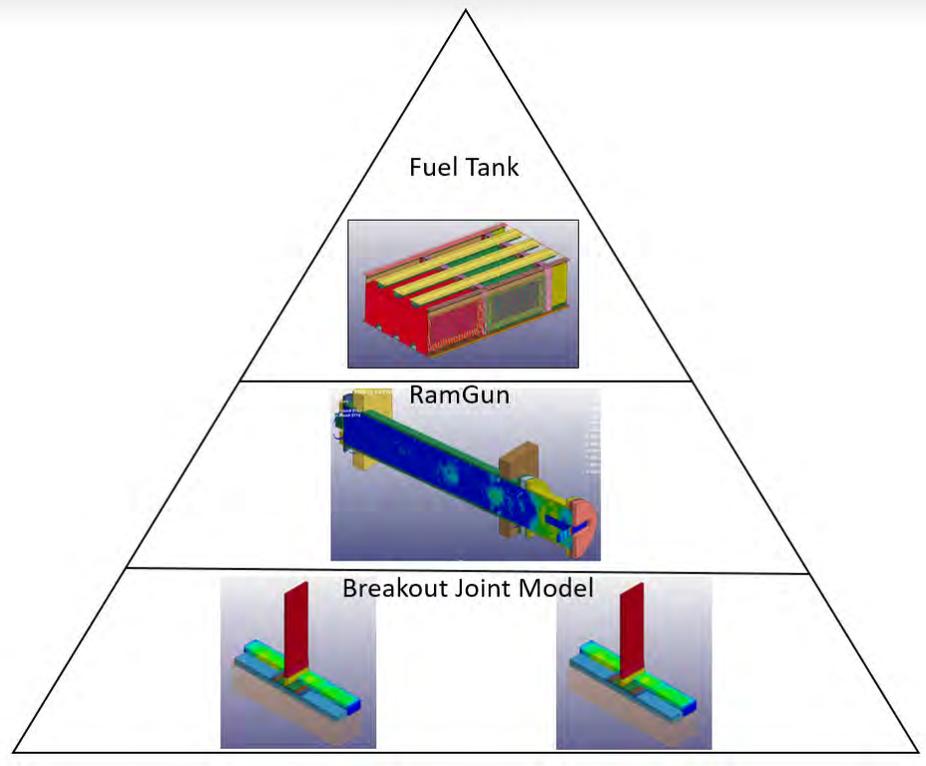


Figure 1: Building Block Approach Used for Numerical Model (Source: Northrup Grumman Corporation [NGC]).

the puck with the chamber end plate generates the high-pressure wave needed to load the joint. A RamGun was used in this study to test various joint configurations with variable skin thickness and total bonded area [9]. Previous methods, both using RamGun and a universal testing machine, usually tested at a single failure strain rate and thus did not provide much insight on the damage characteristics of a particular joint regarding different pressures (strain rates) [8, 9]. To provide a more refined perspective into the damage,

the V_{50} ballistic testing approach was utilized [9]. To create the bounds of the test [10], the up/down V_{50} approach is utilized by first testing to a pressure where the joint is expected to fail and then testing at a pressure where the joint is expected to survive. The pressure is then moved inwards from the bounds until a failure transition pressure is identified. An example of a pressure spectrum from RamGun testing is shown in Figure 2 [9]. Failure and survival pressure regions can be identified, as well as a transition region.

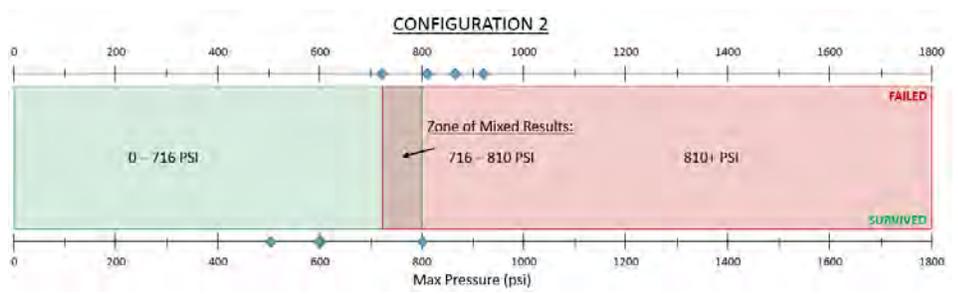


Figure 2: Sample Pressure Spectrum Showing Failure, Nonfailure, and Region of Mixed Results (Source: NGC).

Based on the RamGun results, previous research showed that increasing the base thickness of a joint tends to increase its strength and, hence, HRAM resistance [9]. More significant is the effect of increasing the total bonded area [9]. Increasing the bonded area to about 40% by adding extra plies at the interface of the Pi preform and the base resulted in an increase of about 70% in bond strength [4]. In a previous study, the joint numerical model, when calibrated to empirical failure data, was able to accurately predict joint failure across a range of pressures [7]. The greatest disagreements between the model and the experiments were RamGun pressures in the inflexion region (see Figure 2), where there is also the greatest uncertainty in the experimental results. Table 1 shows the summary of the numerical failure prediction results.

In this research, the calibrated CZM joint model was transposed to the complete tank model, as shown in Figure 3. The joint in the tank numerical model was modeled with the appropriate CZM parameters and joint area based on the desired configuration. The coarse mesh model of the joint enables the fuel tank, which is a large structure, to be modeled and used to accurately predict progressive damage in the tank.

MODEL AND SIMULATION

A finite-element model of a representative fuel tank is modeled in LS-DYNA to predict failure of a bonded composite fuel tank subjected to HRAM caused by impacting the tank with a projectile. The critical structural connection of interest, the spar-to-skin joint, is modeled as a bonded joint representative of the T-joint tested in the RamGun. The tank FEM is divided into Lagrangian and Eulerian components. The Lagrangian components consist of

Table 1: Summary of Failure Prediction Accuracy

Joint Cohesive Zone Models	Thin Base Baseline Area	Thin Base Increased Area	Thick Base Baseline Area	Thick Base Increased Area
Failure Prediction Accuracy	84%	82%	98%	87%

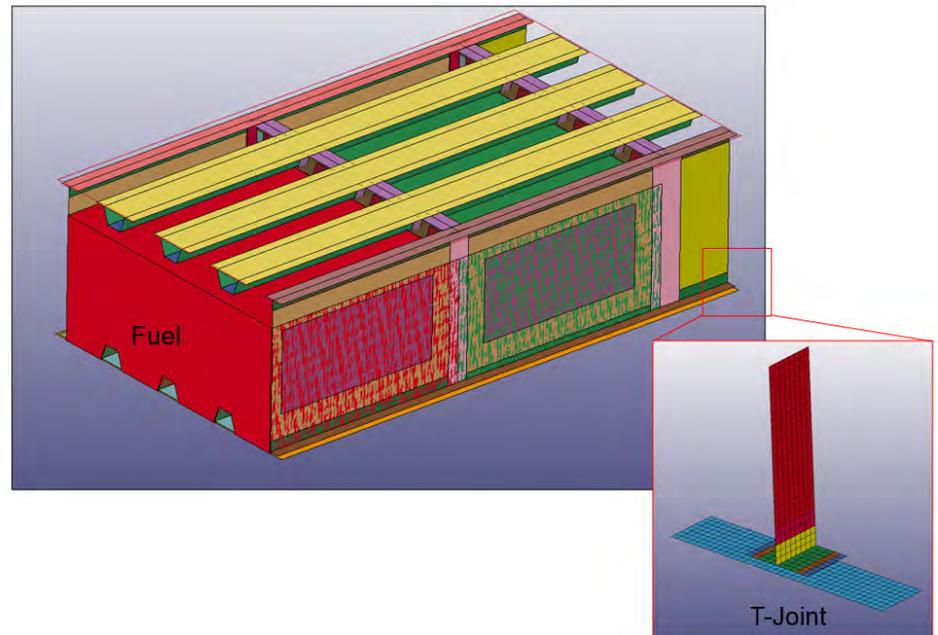


Figure 3: Extrapolating Joint Failure to Fuel Tank Failure (Source: NGC).

the tank and the projectile. The Eulerian components consist of air and water. The model measures 92 inches x 42 inches x 30 inches and contains about 7.3 million elements.

A 150-grain cubic projectile, which weighs about 0.0214 lbf, is used in this simulation. The projectile is modeled with Lagrangian solid hexahedron elements. It is modeled as a rigid material since stress and strain data for the projectile are not essential to the simulation and its deformations are not significant at this fidelity. This technique saves on total simulation time.

The tank was modeled with hat-reinforced top and bottom skins, stiffened forward and aft spars, and

three stiffened ribs resulting in two fuel bays. The bay where the projectile impacts is dubbed the primary bay. The tank components are modeled with shell elements. An average element size of 0.25 inches is used, which resulted in 311,264 elements for the Lagrangian model designed as a composite material. The main failure of interest is the joints. The same bonded joint design used in the RamGun models is implemented in the box-level analysis. A cohesive zone modeling approach is used to model the joints.

The initial projectile velocity applied to initiate the simulation did not simply match the preimpact velocity but was modified to ensure that correct conditions were obtained following initial

impact. For efficiency, the tank was modelled with shell elements. These elements are unable to accurately reduce the energy of the projectile as it penetrates the wall. To accurately model the energy imparted into the system, the initial velocity is adjusted to compensate for this effect. Other researchers [1, 6] address this problem by solid elements, but that approach is prohibitive for a realistic tank due to size. To use the current approach, a study of residual velocity was conducted.

Various panels similar to the skin, with different thickness, were shot with the intended projectile. The reduction in the projectile velocity was recorded. After a sufficient sample size was obtained, the average velocity reduction was observed to be about 13% for the skin thicknesses used in this analysis. The residual velocity was calculated using this factor as input in the simulations. Contact between the projectile and the skin was ignored; the projectile just passed straight through the skin and directly impacted the fluid with the required residual velocity. This approach eliminated a step from the analysis and replaced it with empirical data while providing consistent results in projectile energy.

To ensure accurate fluid-structure interaction analysis, the mesh needs to be fine enough to transfer the energy

To ensure accurate fluid-structure interaction analysis, the mesh needs to be fine enough to transfer the energy from the projectile effectively.

from the projectile effectively, which will dictate the stopping distance of the projectile distance in the fluid and the resulting pressure. Some researchers use an estimate of stopping distance, based on projectile shape and density of fluid, to determine the appropriate mesh density for the analysis [11]. Others calculate the stagnation pressure or use pressure data, if available, to determine the mesh size. To accurately track the pressure, these methods usually result

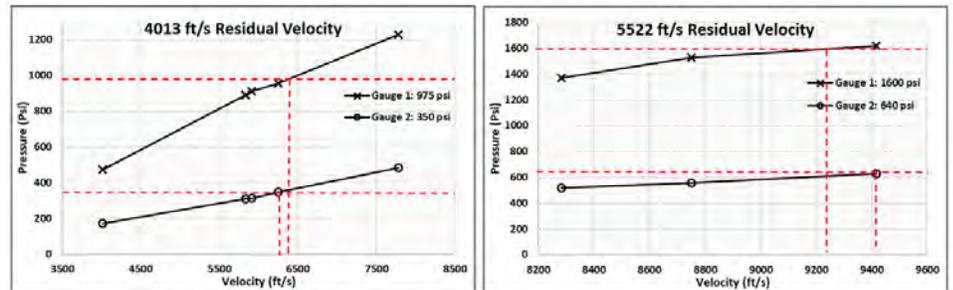


Figure 4: Velocity Calibration (Source: NGC).

in mesh sizes of about 0.0625 inches. That mesh size is impractical to use for a large article like the one analyzed or for larger fuel tanks. A plan was devised to obtain accurate pressure distribution while maintaining a relatively coarse mesh to reduce the size of the overall model and hence the solution time.

A test was conducted where a 150-grain cubic projectile was shot into an instrumented tank. The tank contained pressure transducers (PTs) at different locations to capture the pressure during the event. The projectile velocity was varied to provide a variety of data. An FSI model was created similar to the one used for the fuel tanks. The projectile velocity in the numerical model was modified for each run until the pressure predicted by the numerical model matched the pressure recorded by the pressure transducers during the

test. The hydrocode used in LS-DYNA is dissipative in terms of pressure, so it is difficult to match pressure far from the source. A linear relationship was developed that increased the residual velocity to make up for the coarse mesh and replicate pressure recorded by the PT in an actual experiment. A linear relationship was then applied to the numerical model for the fuel tank. Figure 4 shows the calibration process for the mesh and pressure.

Two baseline velocities were analyzed—4,013 ft/s and 5,522 ft/s. The pressure readings from near- and far-field gages—gauge 1 and gauge 2, respectively, were recorded for reference. The analysis pressure seems to have a linear relationship with velocity. It was found that the experimental velocity had to be increased by a factor of 1.6–1.8 to match the pressure data.

The main parameter used to track and assess failure capability is pressure. Pressure also provides a measure of analysis accuracy when compared with experimental results. In this research, since the box-level analysis is built up from the RamGun models, pressure from both tests provides a way to assess how well they track. This can lead to future RamGun studies to make joint-to-complete tank analysis seamless. LS-DYNA provides tracers in the ALE

simulation, which act like pressure transducers.

The tracer elements are illustrated in Figure 5, where 20 tracers are used. Based on the proposed methodology, four distinct models are created to provide correlations from the RamGun models and test. The models were thin skin, thick skin, and a model with an increase in bonded area for both base thicknesses, thus resulting in four models.

RESULTS AND DISCUSSION

To build confidence in the numerical model and its ability to accurately predict HRAM damage in a composite fuel tank, the fluid mechanics of the HRAM event is checked to make sure it follows the HRAM evolution and conservation laws. Figures 6 and 7 show the progression of the HRAM process as captured by the numerical model.

The projectile impulsively loads the fluid and creates a high-pressure, hemispherical shock wave. This is the HRAM shock phase, which can be seen explicitly in Figure 6. The drag phase follows as the projectile slows down and transfers its energy to the fluid. The pressure has a radial shape and stays in front of the projectile and moves with it. Since the initial shock pressure moves at speed of sound in the fluid, it is faster than the drag pressure pulse and stays ahead of it. The cavitation phase is also evident, as shown in Figure 7. The cavity grows behind the projectile, and the projectile slowly comes to a standstill as it transfers all its energy to the fluid. The cavity continues to grow to its maximum size and then collapses due to the pressure difference and gravity. There was no exit stage since the fluid depth and projectile velocity ensured complete transfer of the projectile energy to the

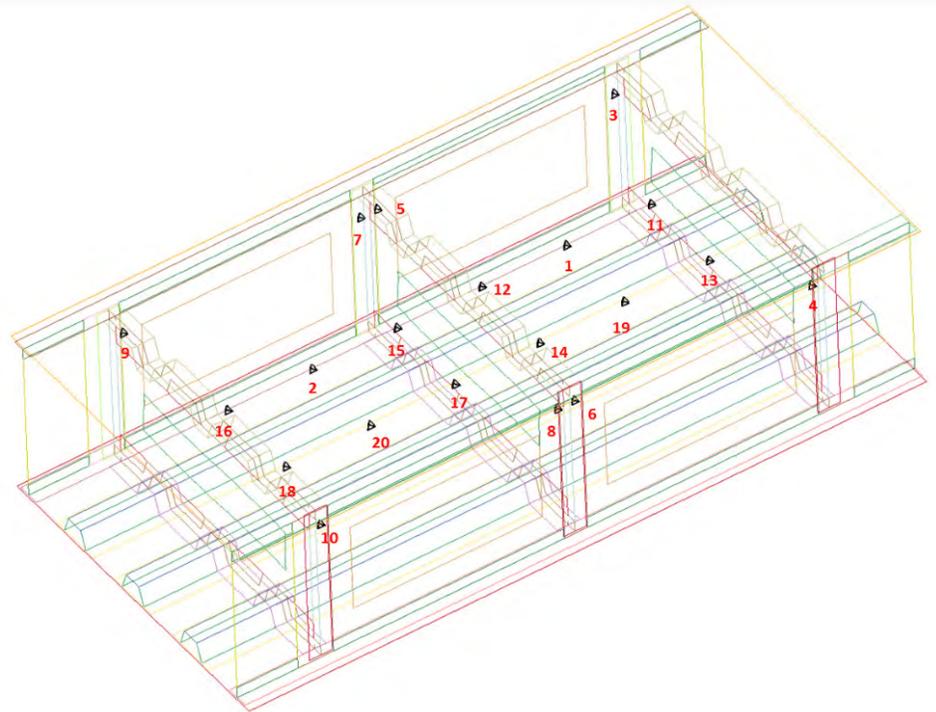


Figure 5: Number of Tracer Elements in the Model (Source: NGC).

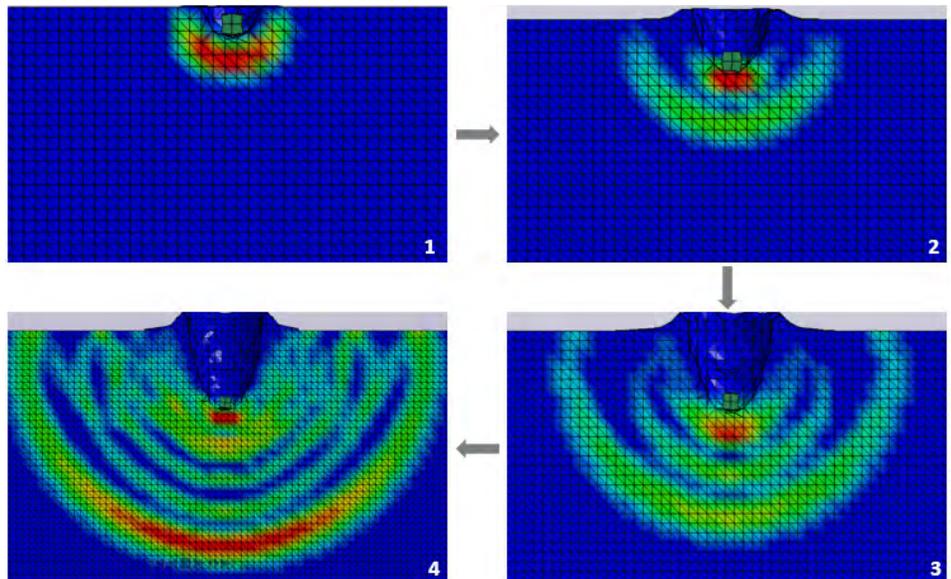


Figure 6: Shock Created During HRAM (Source: NGC).

fluid before the projectile reached the wall. Therefore, it did not have any energy to exit the structure.

The tracers were used to monitor the pressure inside the tank to provide more

insight on the event. Figure 8 highlights a few tracer nodes to provide insight into the pressure distribution. The tracers closest to the projectile were about 7 inches away and recorded the highest pressure of 8.2 ksi x 0.5 ms, dissipating

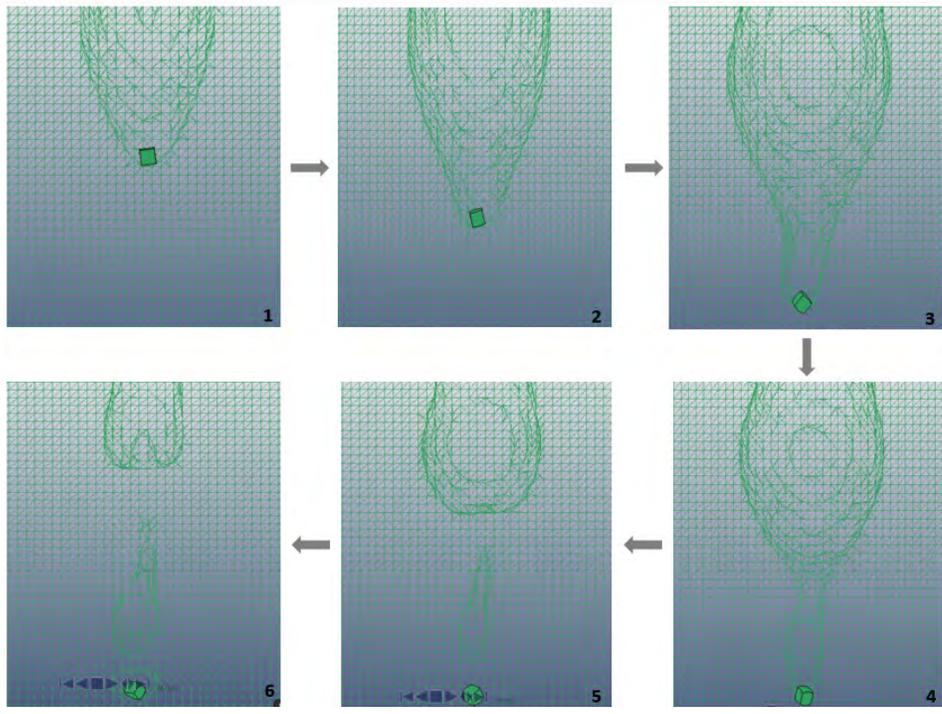


Figure 7: Cavity Evolution (Source: NGC).

is testament to the fact that the shock pulse dissipates very quickly, almost exponentially. Even though the pressure pulse has reduced magnitude, it may still have enough energy to cause damage.

There are also tracer nodes placed before (tracer 6) and after (tracer 8) the mid rib to provide information on how much the middle rib dissipates the pressure. As expected, there was significant pressure drop of about 200 psi across the rib. A model using solid elements for the skins might have yielded slightly different results for this pressure drop since solid elements better capture energy absorption and transfer. For our purposes, however, the shell element model provided an appreciable pressure drop to predict overall tank failure while still remaining computationally viable.

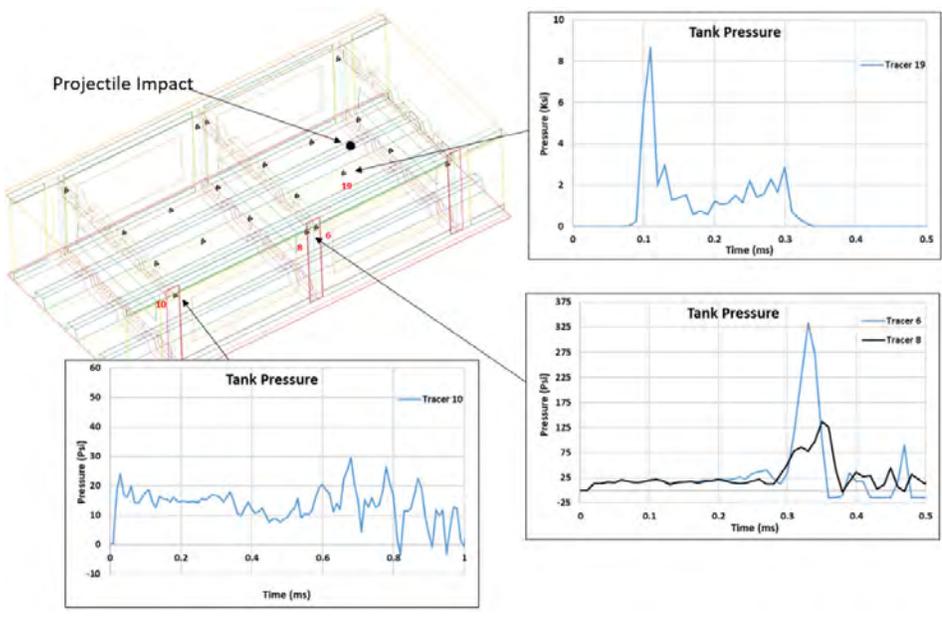


Figure 8: Recorded Tracer Pressure (Source: NGC).

The tracer (tracer 10) in the secondary bay (bay without impact) recorded a very low pressure, close to ambient pressure, much later in the simulation. The damaging capacity of HRAM seems to be local but can create inertia, which propagates failure in the structure since the far-field pressure is usually not enough to cause failure.

A baseline projectile velocity of 4,000 ft/s was used in initial studies of the HRAM effect in the tank. A baseline spar distance of 13 inches (spar distance 1) from the closest spar was also used. This means the projectile is located 13 inches from the spar. Figure 9 shows the baseline impact location and an example of the HRAM cavity evolution based on impact location. The baseline impact location places the projectile over skin and avoids the hats. This was done to simplify the analysis and reduce the complexity of the event. The previously-discussed 13% reduction in velocity to correct skin penetration losses has already been determined for

quickly thereafter. The highest pressure pulse recorded was during the shock phase. The drag phase also produces a high-pressure pulse soon after, as shown in tracer 19. The tracers next to the spar, about 14 inches away, pick

up the pressure pulse later, depending on the impact location. These pressures are usually at least an order of magnitude lower than the pressure recorded near entry. For example, only 333 psi is recorded by tracer 6. This

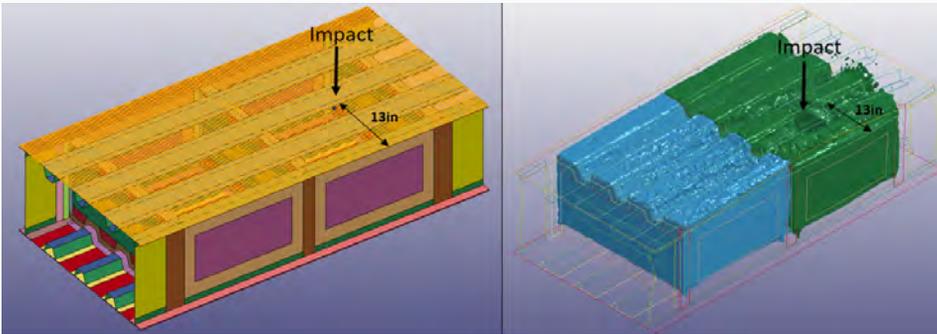


Figure 9: Nominal Impact Location and Its Effects (Source: NGC).

a projectile going through the skin (see Model and Simulation section) and is used to determine the residual velocity.

For different impact locations, there will be changes in the pressure distribution within the tank that determine the energy transfer and magnitude of pressure experienced within the tank. The structure will react to these pressure distributions, with deformations and possibly failure based on its composition and structural design.

The first tank assessed to determine the effects of different impact locations was based on the thin-base model. In this model, the tank skin is 0.2 inches thick. From the RamGun test, this resulted in the weakest joint, which tends to fail at a pressure range between 400 and 483 psi. At the tank level, the damage predicted for the nominal impact location was extensive. The main damage occurred at the interface between the skin and spar closest to the projectile impact. Damage propagated from the primary bay to the secondary bay, completely disbonding the whole base close to the location of impact.

The other three spar-to-skin joint locations were also severely compromised. Figure 10 shows the damage caused in the thin-base model. The image to the left shows the overall displacement of the model highlighting the disbond. The skin closest to impact

had a maximum deformation of 5.68 inches. The image to the right shows the same deformation state, with the model rotated 180 degrees and hiding the skins for better interior structure visualization. The colors in the figure show the binary failure flag for the CZM surfaces. Red indicates that cohesive zone failure has occurred. It is apparent that the disbond extends all the way from the first rib to the last rib.

The thick-base tank was investigated

next using the same baseline parameters. The skin thickness on this tank was 0.5 inches. The pressure experienced by the closest spar-to-skin joint was comparable to the pressure distribution that occurred in the thin-base tank mode. As illustrated in Figure 11, however, the extent of damage is very different. From the RamGun test, the thick-base model failed at a pressure range of 692–707 psi, indicating that the thick-base tank model should be able to resist more than the thin-base model.

The displacement model to the left in Figure 11 shows a slight damage in the primary bay where the projectile made impact. The skin displayed a maximum deformation of 0.54 inches. The rotated CZM failure model to the right shows the failure/disbond more vividly. Skin-to-spar failure was contained to one bay (the primary bay), and the other skin-to-spar joints remained intact.

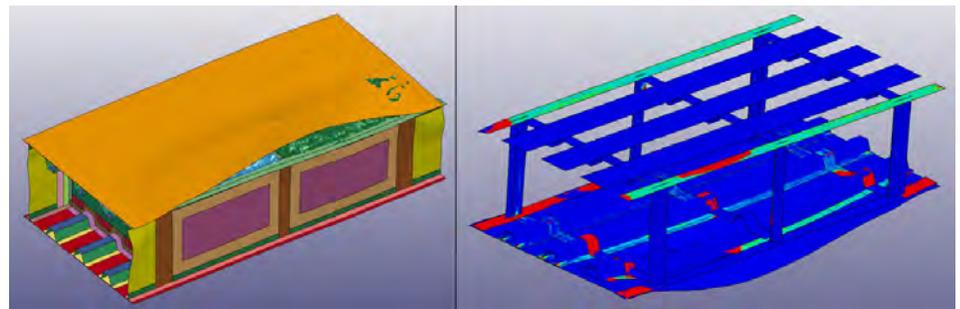


Figure 10: Thin-Base Model Predicted Damage (Source: NGC).

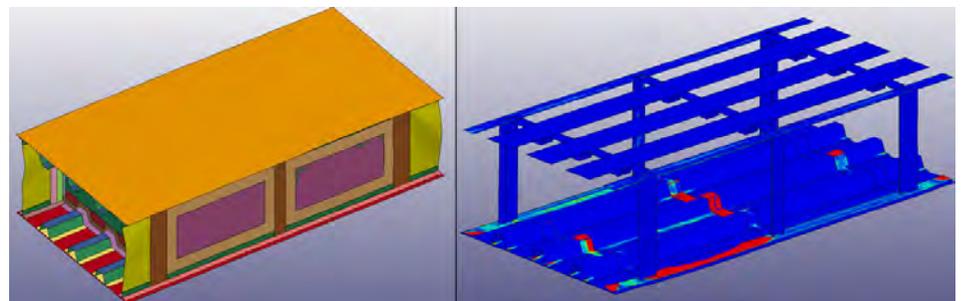


Figure 11: Thick-Base Model Predicted Damage (Source: NGC).

Parametric Study – Projectile Velocity

To understand the effect of projectile velocity on the damage, a different projectile velocity was used while maintaining the same impact location (spar distance of 13 inches). A projectile velocity of 5,000 ft/s was used on the thick-base model. Figure 12 compares

the pressures generated from the 4,000-ft/s models and the 5,000-ft/s models.

For the higher-velocity projectile, the maximum pressure closest to the projectile increased by 65% to a pressure of 14.5 ksi. The pressure recorded by the tracer nodes next to the closest skin-to-spar interface

increased by 40% to a pressure of 460 psi. There was also about a 40% increase in the pressure recorded by the tracers located directly behind the mid rib in the secondary bay. The farthest tracers in the secondary bay were not significantly affected by the change in projectile velocity, remaining close to ambient in each case. Irrespective of the magnitude of initial pressure, the pressure decays rapidly to ambient after a certain travel distance. The skin deformation increased to 3.15 inches from 0.54 inches for the higher-velocity projectile. The higher velocity tremendously increases the kinetic energy introduced by the projectile into the system, resulting in much higher pressure and energy. Figure 13 compares the cavity size of the 4,000- and 5,000-ft/s models. Cavity size has a direct relation to the energy introduced into the system.

Figure 14 shows the damage that occurred with the higher-velocity projectile. Because the pressure recorded at the joint location was much higher than the joint strength pressure determined with the RamGun test, it is expected that the damage state was more severe than in the simulation using the 4,000-ft/s projectile. In the high-velocity simulation, the damage was extensive and spread across both the primary and secondary bays. However,

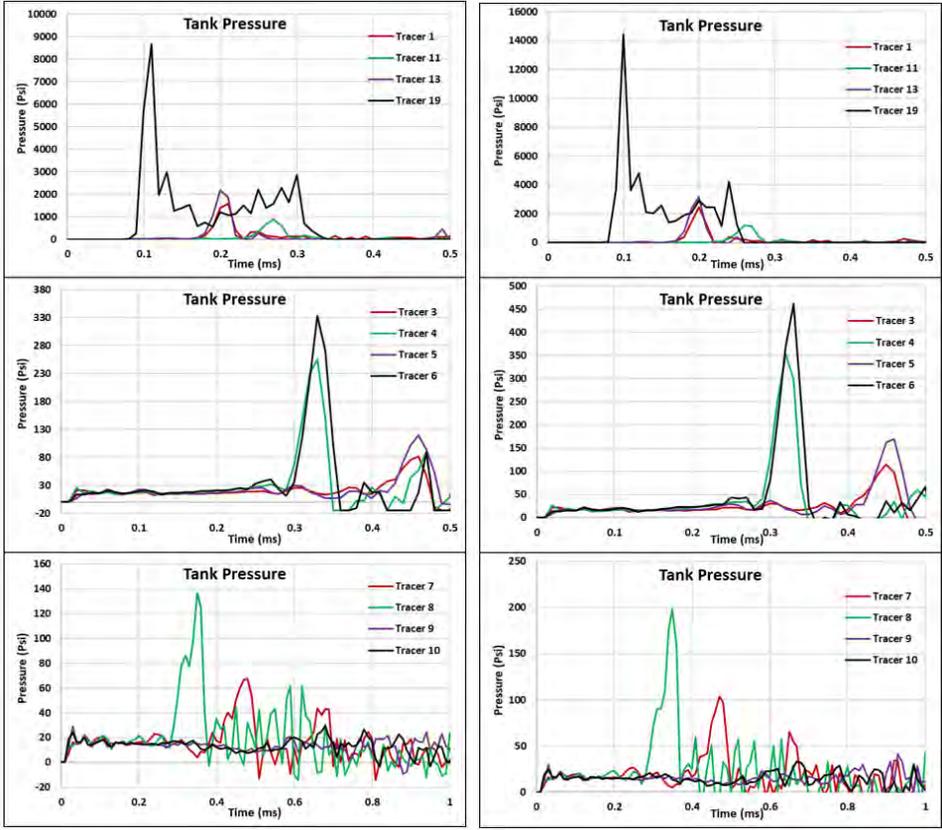


Figure 12: Tracer Pressure Distribution Comparison—(Left) 4,000 ft/s and (Right) 5,000 ft/s (Source: NGC).

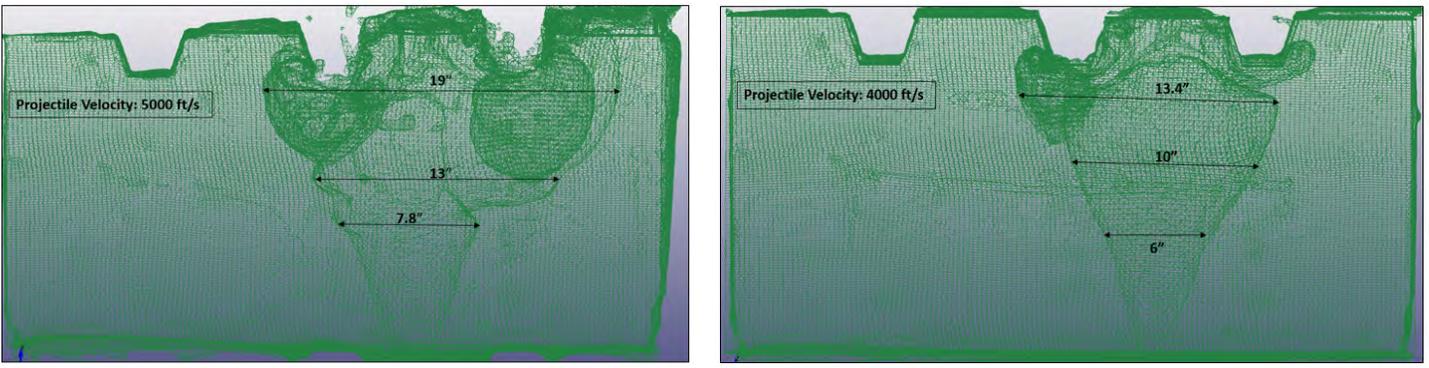


Figure 13: Cavity Size Based on Projectile Velocity (Source: NGC).

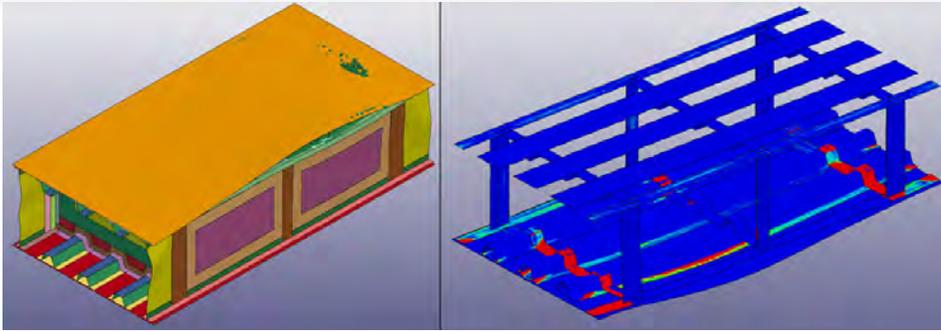


Figure 14: Thick-Base Model Predicted Damage for 5,000-ft/s Projectile Velocity (Source: NGC).

the damage was contained to only the spar-to-skin joint closest to the projectile impact. The other spar-to-skin joints were intact.

Parametric Study – Distance to Spar

Another variable was assessed to study its effect on tank damage—the location of the projectile impact. Changing the impact location changes the pressure distribution and cavity formation within the tank. The projectile impact-to-spar distance changed from 13 inches to 3 inches (spar distance 2), which brought the projectile closer to the spar/skin interface that experienced the most damage in previous simulations. A 0.5-inch skin thickness was maintained for this model, corresponding to the thick-base model used in the RamGun model. Based on the RamGun test and simulation, the failure pressure for this joint configuration was estimated to be in the 692–707 psi range. Figure 15 shows the new projectile location and increased proximity of the formed cavity to the spar and skin.

Due to the proximity of the projectile impact location to the spar, the high pressure from the projectile will not be significantly dissipated before it is experienced by the spar. The magnitude of the pressure recorded close to the spar was as high as 500 psi, which is about 50% higher than the pressure recorded for the original spar location.

The high pressure resulted in the damage state displayed in Figure 16.

The displacement image showed in the left of Figure 16 reveals a maximum skin displacement of 1.7 inches. Visually, it looks like the damage extended into the secondary bay, completely disbonding both bays. The CZM failure image to the right confirms this. There also seems to be significant damage to the joint located at opposite skin in the primary bay. The other skin-to-spar joints seem to be intact, further demonstrating

During the RamGun joint studies, it was found that increasing the total bonded area of a joint drastically increased the joint strength.

the local nature of the damage and dissipation of the pressure pulse with distance.

Effect of Total Bonded Area

During the RamGun joint studies, it was found that increasing the total bonded area of a joint drastically increased the joint strength. (Similar results were also shown by previous researchers [12].) Both thin- and thick-base models were analyzed, which yielded failure pressure increases of 73% and 79%, respectively. This concept was investigated at the

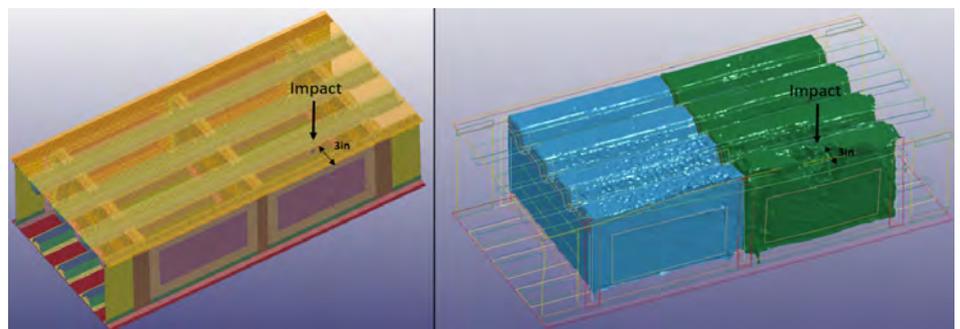


Figure 15: Alternate Impact Location and Its Effects on Cavity Formation (Source: NGC).

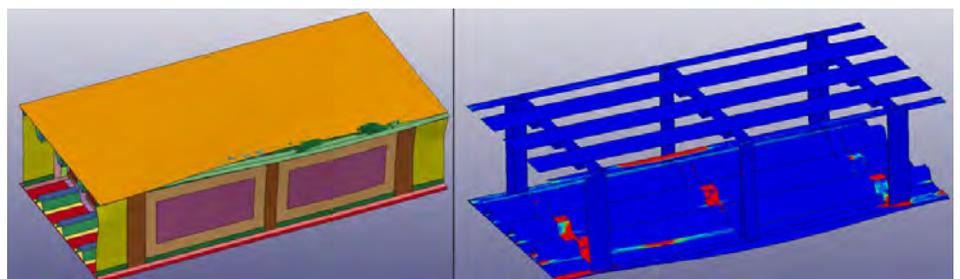


Figure 16: Thick-Base Model Predicted Damage for Spar Location 2 (Source: NGC).

tank level for both thin- and thick-base configurations to determine whether the trend carries over to the fuel tank since this is a promising method for reducing the extent of disbond and damage in a bonded fuel tank. The baseline velocity of 4,000 ft/s and projectile spar distance of 13 inches (spar distance 1) was maintained to produce approximately the same pressure distribution as previous models. The damage found in the augmented thin-base model is displayed in Figure 17. From the RamGun model and test, the failure pressure for this model was in the 716–810 psi range compared to 400–483 psi for the model without the bonded area extension.

From the displacement image in the left of Figure 17, the maximum skin deformation was about 1.8 inches. The damage seemed to be contained to only the primary bay. The CZM failure image in the right agrees with this failure assessment. Damage was reduced drastically from the original joint configuration, which showed a complete disbond of both bays with other joints also being potentially compromised.

The effect of the increased, bonded area was also checked with the thick-base model. According to the RamGun test,

the failure pressure range increased from 692 to 707 psi to 1,212 to 1,292 psi. Figure 18 shows the damage experienced by the thick-base model with the increased, bonded area.

The maximum skin displacement, seen in the left of Figure 18, reduced to 0.31 inches. The displacement model shows

no apparent damage. The CZM model in the right confirms this observation; no binary failure is indicated. This is a great improvement from the baseline model, which had a complete disbond in the primary bay. Table 2 summarizes the predicted damage for the different configurations and variations.

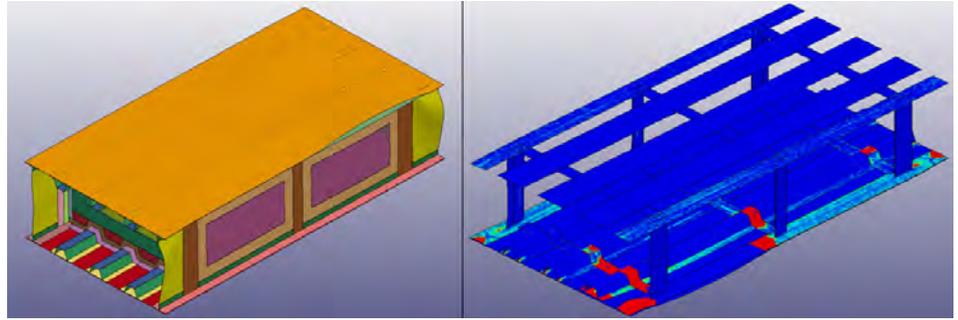


Figure 17: Thin-Base Model With Extended, Bonded Area Predicted Damage (Source: NGC).

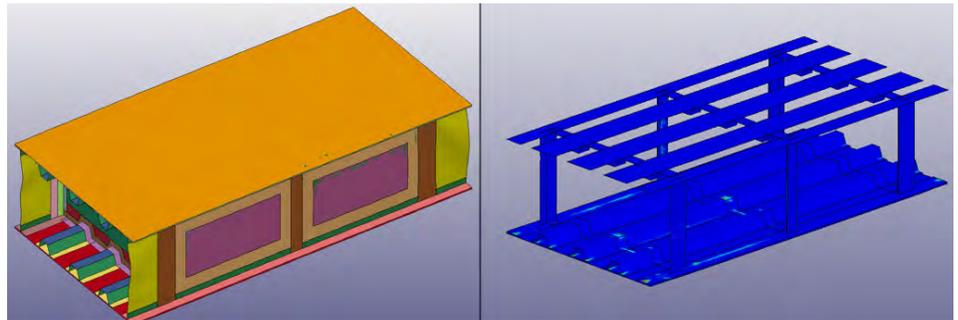


Figure 18: Thick-Base Model With Extended, Bonded Area Predicted Damage (Source: NGC).

Table 2: Summary of Predicted Damage

Tank Model	Projectile Velocity (ft/s)	Spar Distance (in)	Max Joint Pressure (psi)	Max Skin Displacement (in)	Predicted Damage	RamGun Failure Pressure Range (psi)
Thin Base	4,000	13	333	5.68	2 Bays	400-483
Thick Base	4,000	13	333	0.54	1 Bay	692-707
Thick Base	5,000	13	460	3.15	2 Bays	692-707
Thick Base	4,000	3	500	1.7	2 Bays	692-707
Thin Base, Increased Area	4,000	13	333	1.8	1 Bay	716-810
Thick Base, Increase Area	4,000	13	333	0.31	No Damage	1,212-1,292

CONCLUSIONS

HRAM damage remains a critical failure mode and kill mechanism for military aircraft due to susceptibility of fuel tanks to hostile fire. Unfortunately, testing for HRAM can be cumbersome and expensive. This research sought to provide a numerical analysis method to accurately capture HRAM damage in a bonded-composite fuel tank. The method combined ALE and CZM in a building block approach to model and predict tank failure. A calibrated, coarse CZM model for various T-joints was created based on a RamGun test that utilized the V_{50} approach to characterize failure pressure. The calibrated model was extrapolated from the joint model to produce a fuel tank model. The model was comparable to an actual fuel tank, complete with skin stiffeners and multiple bays. Tracer nodes were incorporated to track fluid pressures. Four distinct models were created based on the four joint configurations tested in the RamGun—thin base, thick base, and extended joint area for both thin- and thick-base cases.

The models were checked for accuracy by studying the pressure pulses and evolution of the cavity, which proved to match the observed HRAM hydrodynamics. For consistency in comparing the various models, a projectile velocity of 4,000 ft/s was used in conjunction with a projectile-to-spar distance of 13 inches. The thin-base models showed extensive damage. The spar-to-skin joint closest to the projectile impact location exhibited a complete disbond of both bays, and other spar joints were also compromised.

The thick-base model, on the other hand, exhibited much less damage under the same modeling parameters. The primary bay exhibited disbond, but that was the extent of the damage. All

HRAM damage remains a critical failure mode and kill mechanism for military aircraft due to susceptibility of fuel tanks to hostile fire.

the other spar-to-skin joints remained intact. This result reinforces the notion that a thicker base tends to make the overall joint stronger in terms of HRAM resistance. A similar trend was exhibited at the RamGun joint testing level.

Parametric studies were performed on the thick-base model. The first was a study of the effect of projectile velocity. The velocity was increased from 4,000 ft/s to 5,000 ft/s. This resulted in many changes—most notably, a general increase in pressure. The cavity created in the cavitation stage was also much larger due to the higher kinetic energy introduced. The damage increased from being contained only in one bay, as in the 4,000-ft/s model, to include joint disbond in both primary and secondary bays. The other skin-to-spar joint interfaces remained intact and uncompromised.

The second parameter that was studied was the effect of projectile impact distance from the spar. This study was also performed using the thick-base model. The original velocity of 4,000 ft/s was maintained, but the projectile spar distance was altered from 13 inches to 3 inches, moving it closer to the spar. This change resulted in a higher-pressure distribution near the spar since the pressure is higher close to the projectile. The closest spar-to-skin

joint experienced a complete disbond in both the primary and secondary bays. The joint at the opposite skin also showed some damage in the primary bay. The other skin-to-spar joints remained intact.

Finally, the other two configurations using increased joint areas for both the thick- and thin-base models were analyzed to assess their resistance to HRAM. The same projectile velocity of 4,000 ft/s and spar distance of 13 inches was maintained for these models. The RamGun test predicted increased strength for the models with increased bond area. For the thin-base model, the prediction was reduced from catastrophic damages to disbond within the primary bay only. The same trend was realized for the thick-base model with the increased joint area. The modified thick-base model showed no damage compared to the baseline line model, which experienced a disbond in the primary bay. In line with the RamGun results, increasing the total bonded area greatly improves HRAM joint resistance and can be used as an HRAM mitigating technique.

Using a combination of empirical data and analytical techniques, we have been able to predict overall joint failure in bonded composite fuel tanks as well as investigate a very promising HRAM mitigation technique. The effects of projectile velocity and impact location on HRAM were also ascertained. This technique employed a coarse mesh in the numerical model, making it computationally viable to study HRAM in large items like fuel tanks and beyond. ■

ACKNOWLEDGMENTS

The authors want to thank Ron Hinrichsen of Skyward Ltd., who is an industry expert on HRAM simulation, for providing modeling guidance based on his numerous years of experience and Frank Compton of Northrop Grumman Corporation, who continuously provided invaluable insight on HRAM based on his long, live-fire industry experience over multiple platforms.

NOTE: This article was previously presented at the 2020 American Institute for Aeronautics and Astronautics (AIAA) SciTech Forum in Orlando, FL.

REFERENCES

- [1] Varas, D., J. Lopez-Puente, and R. Zaera. "Numerical Analysis of Hydrodynamic Ram Phenomenon in Aircraft Fuel Tanks." *AIAA Journal*, vol. 50, no. 7, pp. 1621–1630, 2012.
- [2] Selvarathinam, A. S., M. W. Stewart, S. P. Engelstad, and B. Eby. "Application of Progressive Damage Failure Analysis to Large Aircraft Composite Structures." The 2018 AIAA/ASCE/AHS/ASC Structures, Structural Dynamics, and Materials Conference, July 2018.

[3] Adams, R. D. *Structural Adhesive Joints in Engineering*. London: Chapman & Hall, 1997.

[4] Sedalor, T., and D. Fleming. "Effect of Total Bonded Area on Hydrodynamic Ram Resistance of a T-Joint." Proceedings of the American Society for Composites 34th Technical Conference, Atlanta, GA, 23–25 September 2019.

[5] Noorman, D. C. "Cohesive Zone Modelling in Adhesively Bonded Joints: Analysis on Crack Propagation in Adhesives and Adherends." M.S. thesis, Delft University of Technology, 2014.

[6] Turon, A., C. G. Davila, and P. P. Camanho. "An Engineering Solution for Using Coarse Meshes in the Simulation of Delamination With Cohesive Zone Modeling." Technical report NASA/TM-2005-213547, National Aeronautics and Space Administration (NASA) Langley Research Center, Hampton, VA, March 2005.

[7] Sedalor, T., and D. C. Fleming. "Numerical Analysis of a Bonded Composite T Joint Subjected to Hydrodynamic Ram Pressures in a RamGun." AIAA SciTech 2019 Forum, January 2019.

[8] Heimbs, S., T. Duwensee, A. C. Nogueira, and J. Wolfrum. "Hydrodynamic Ram Analysis of Aircraft Fuel Tank with Different Composite T-Joint Designs." *Structures Under Shock and Impact VIII*, pp. 279–288, 2014.

[9] Hinrichsen, R., S. Stratton, A. Moussa, and G. Zhang. "Hydrodynamic Ram Simulator." JASPO-V-07-06-001 AAC-TR-08-17, Joint Aircraft Survivability Program Office, September 2008.

[10] Hull, B. T., T. Sedalor, and T. Mifsud. "Utilization of Hydrodynamic Ram Simulator to Determine the Dynamic Strength Thresholds of Structural Joints." AIAA SciTech 2019 Forum, January 2019.

[11] Mansoori, H., and H. Zarei. "FSI Simulation of Hydrodynamic Ram Event Using LS-DYNA Software." *Thin-Walled Structures*, vol. 134, pp. 310–318, 2019.

[12] Li, J., Y. Yan, Z. Liang, and T. Zhang. "Experimental and Numerical Study of Adhesively Bonded CFRP Scarf-Lap Joints Subjected to Tensile Loads." *The Journal of Adhesion*, vol. 92, pp. 1–17, 2014.

BIOGRAPHIES

TEDDY SEDALOR is a lead systems test engineer at NGC, where he performs dynamic simulations to supplement and complement various structural aircraft tests, including live-fire test. He is the company's subject matter expert for FSI analysis, focusing on HRAM analysis, and possesses broad experience in analyzing and testing aircrafts and large subsea machines. He is a member of the AIAA Survivability Technical Committee. Dr. Sedalor holds a Ph.D. from Florida Institute of Technology and an M.S. from Virginia Polytechnic and State Institute.

DAVID FLEMING is an associate professor of aerospace engineering and Aerospace Engineering Program Chair at the Florida Institute of Technology in Melbourne, FL. His primary research interests are in composite structures and the crashworthy design of aircraft. He is an Associate Fellow of AIAA. Dr. Fleming holds a B.S. in aeronautics in astronautics from MIT and an M.S. and Ph.D. in aerospace engineering from the University of Maryland, College Park.

(Courtesy of Raytheon Technologies)



Detection and Classification of

SMALL UAS FOR THREAT NEUTRALIZATION

By Matthew Henderson

INTRODUCTION

The recent emergence of small unmanned aerial systems (sUAS) into a broad sphere of commercialized applications has caused proliferation of easily, accessible platforms that can be operated and modified with relatively little training. Because they are cheap, effective, and disposable, sUAS are an attractive option for state and nonstate actors alike to conduct surveillance or directly apply force. They are threatening because they are small and fast. If an sUAS payload poses a direct threat, the timeline to neutralize it is critical (Figure 1). This timeline is extremely severe, requiring defeat of an sUAS that will be effective within 40 s from 1 km out. Consequently, the military, intelligence community, and security firms have been working on methods to counter the unmanned aerial vehicle (UAV) threat, with many initiatives launched in the United States and overseas. This article will focus on detecting and classifying UAS threats, with a brief overview of mitigation or kill solutions.

DETECTION AND CLASSIFICATION PROBLEMS

Detection and classification of an sUAS threat to successfully engage a kill solution has two primary problems. The first is detection and classification of a class of very small objects that may move at very fast or slow speeds (or hover). sUAS may present different characteristics in their phenomenology because they can be different types (e.g., rotary or fixed wing, with a wide range of material structures, optical emissions, reflectivity characteristics, and radar cross sections [RCS]). Their variability across size and profiles means that, generally, no single system addresses the whole problem from detection to neutralization but rather a system of systems is required to address the necessary tasks (see Figure 2). The elements in the detection and classification parts of this system are guided by the key detectable elements of an sUAS—shape, size, material structure, velocity, communication

Because they are cheap, effective, and disposable, sUAS are an attractive option to conduct surveillance or directly apply force.

signals, and high-frequency propeller and rotor blade movement/acoustics.

DETECTION

As opposed to classification, detection refers simply to establishing that an object is present as distinct from its background and surroundings. UAS detection methods consist of those modalities likely to discriminate a UAS from its background but not necessarily, specifically classify it apart from similar objects. The typical multisensor approach is to use one wide-area modality to detect a possible UAS and then have that sensor cue an additional, narrower field-of-view (FOV) asset to examine the possible UAS and classify it from other similar objects (e.g., birds) or other confusers and signal noise.

Radar

The primary detection modality against sUAS is radar because of its range and sensitivity detection capabilities in all-weather conditions. Generally, radar systems have coarse resolution and cannot fully profile possible targets for classification and location with sufficient precision for targeting. Low-speed, slow Class 1/Class 2 UAS would be missed by the same radar systems that track larger class airframes at longer distances. Radar signals are also subject to obscuration and clutter by terrain features in settings such as forest and

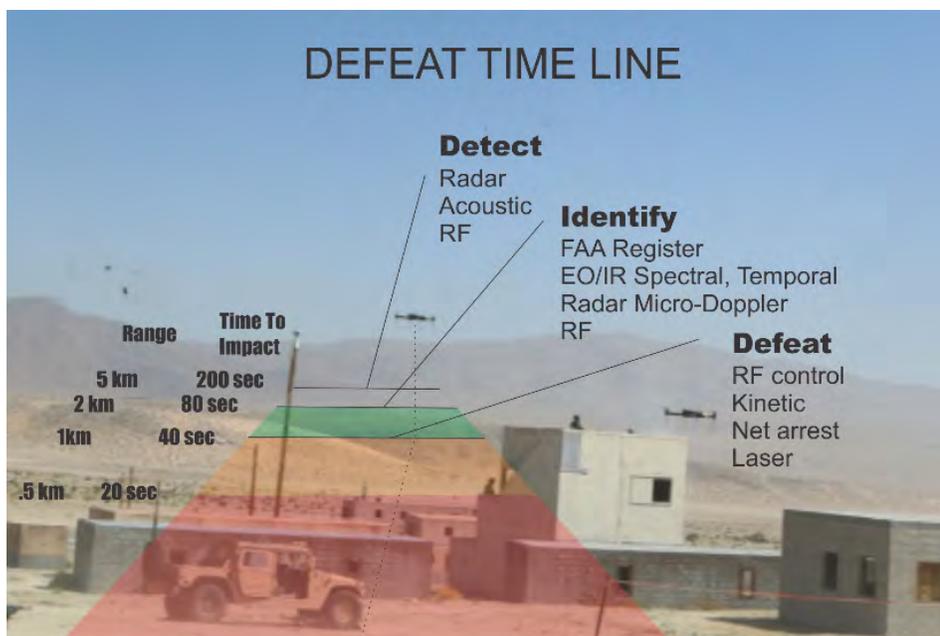


Figure 1: Defeat Timeline (Source: QinetiQ).

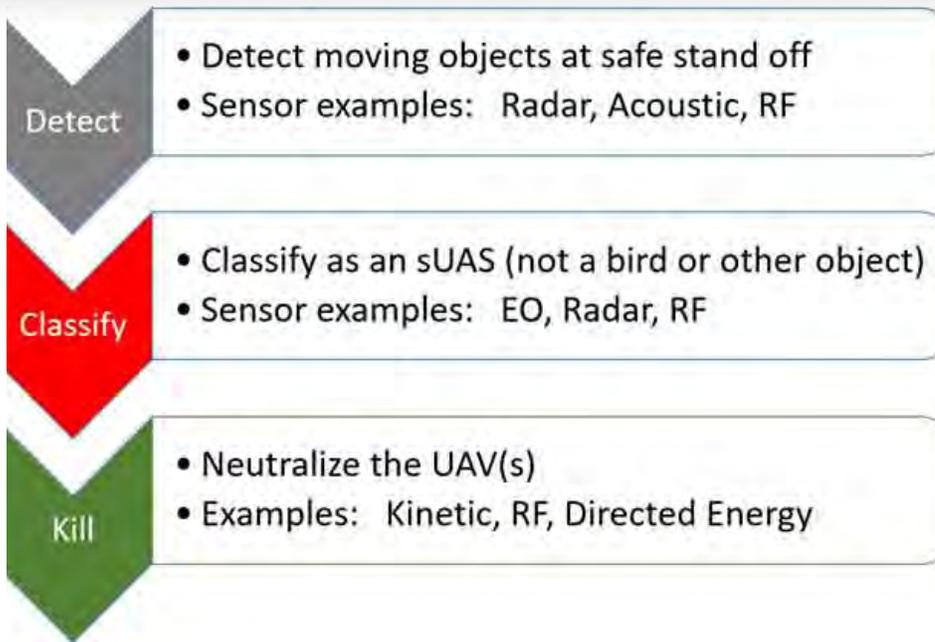


Figure 2: Top-Level Sequence of Events Necessary for Prosecuting Counter-UAV Missions (Source: QinetiQ).

urban environments. Low-cost, low-SWAP active electronic scanned array (AESA), or staring array antennas, or three-dimensional (3-D) radars have been developed that serve the counter-UAS (C-UAS) mission well. Multiple AESA panels or 3-D radars can be structured to cover full 360° FOV in the entire upper hemisphere. These radars can detect sUAS at ranges of 1–3 km based on RF power and sUAS RCS. A separate, smaller class of RF detection systems can be used for close-range objectives.

Because detection of sUAS threats occurs at shorter ranges, higher-frequency radars are preferred for this task. Ku- and Ka-bands (12–18 GHz and 26.5–40 GHz, respectively) are ideal. This is a difference from most military-grade, fire control radars, which operate in the X-band (8–12 GHz) [1]. Experiments are conducted also in millimeter-wave frequencies and even in terahertz frequencies to enable detection of very small objects with low RCS signatures. Further radio frequency (RF) processing using linear frequency modulation

techniques, chip pulse Doppler, or ubiquitous frequency-modulated continuous waves could enable detection of very low RCS objects and high-frequency rotary movement in high-clutter conditions.

A number of theoretical studies have been carried out to evaluate RF performance in terms of target detection probability. RCS of an sUAS, such as DJI-Phantom 4, was estimated to be ~0.02 m². Radar modeling assuming AESA-based, 3-D radar operating at Ka-band with 10-W output power predicts detection at a range up to 2 km, with reasonable false alarm probability. Tracking algorithms can extract the drone plots from noise, so sUAS detection and track could be accomplished.

The phenomenology of sUAS poses significant challenges to radar. Because RCS of target sUAS may vary significantly, multiband radars may be necessary. Further, the shorter bands used to detect sUAS are more susceptible to interference from weather [1].

Frequently, radar must operate in staring mode, where it can survey the entire area to be protected. Its ability to track multiple objects at once using electronic beamsteering is key to holding multiple, possible UAS in memory, prioritizing them, and cueing EO/infrared (IR) assets to classify the objects in question.

Radio Frequency

RF detection of sUAS is based on locating the direction of the signals from communication with the UAV or interrogate it to identify its type. Once this is known, an RF system can double as a kill solution, as it can also be used to take control of the sUAS and land or disable it using further electronic warfare techniques. The key RF system characteristics for successful detection are power sensitivity, directional accuracy, and bands covered. RF detection is also a key alternative to radar in settings where radar transmissions and returns may be obscured.

Both active and passive approaches to RF detection have been demonstrated [2]. Active RF detection is possible by emitting a Wi-Fi signal and measuring its returns. However, we will focus on passive sensing because it is generally better for military application where possible. Most drones communicate with their controller ~30 times per second, giving ample opportunities to be sensed. They also have distinct signatures that allow them to be separated from the clutter of other wireless signals. This is key for operating in urban environments [2].

While both military and commercial UAS attempt to use secure communications, these are still susceptible to attack that exposes their base signatures. Frequency hopping spread spectrum (FHSS) is a technique where carrier frequency is changed to prevent

RF detection of sUAS is based on locating the direction of the signals from communication with the UAV or interrogate it to identify its type.

jamming or sniffing. Korean experiments in academia have shown it to be vulnerable when attacked using software-defined radio [3]. This experiment was specifically performed against an sUAS and its controller. Once the activeness of the channel used is detected (there is a widely established field of techniques for doing this), the period in the hopping sequence is extracted by looking for repetitions from the sequence. Using pattern-matching algorithms can help. Baseband extraction can then provide further information for signal analysis [3].

Acoustic

Acoustic detection is another viable means for detecting possible sUAS. These can operate using single microphones or arrays. In combination, microphone arrays can triangulate a target's location and velocity and track it. Beamforming algorithms are a common method for detecting and tracking targets in this case. They can be augmented with additional processing techniques, such as a Kalman filter [4]. The U.S. Army Research Laboratory has demonstrated that while a UAS as small as Class 1 can be detected and tracked with a portable, inexpensive microphone, acoustic signals are easily interfered with by noise from other sources (e.g., aircraft) [4].

CLASSIFICATION

EO/IR and Spectral

Once a possible sUAS is detected, a sensor must be cued that can hone in on the detected track and verify what it is. EO/IR imaging systems discriminate sUAS based on their shape. While they can serve as detection systems, they are most adept at classification. Full, 360° monitoring, with sufficient resolution to detect a UAS using cameras, would be prohibitively expensive. The key performance parameters for an EO/IR sensing system in this capacity are range and resolution. Because the UAS is extremely small and must be examined at sufficient range so that a kill system can be engaged in time to eliminate the threat before it approaches, imagers used for this purpose must have good optical magnification and fast frame rates. The magnification of an optical assembly is determined mostly by its "f" number, which is calculated by dividing its focal length by the diameter of its aperture. This enables the camera to see the target UAS from far away by having a long optical system and a smaller opening, creating a narrow FOV. A good FOV for a dedicated C-UAS camera would be ~20°.

With magnification achieved, the imager's sensor core must provide high enough spatial resolution that the small object can be suitably distinguished in the image for classification. The number of pixels in the camera's focal plane array (FPA), which is its core photoreactive component, is the most important physical element in providing high resolution. Small FPAs with more pixels (but where each pixel is smaller in size) are worth additional cost when the size of the system needs to be small. Because of the short timeline available to defeat the threat, automated classification based upon imagery is

optimal.

The most effective imaging systems for most classification tasks employ multiple spectral bands. Visible, near-IR, and short-wave IR cameras have distinct advantages in achieving the large number of pixels required for spatial resolution because the materials used to create their FPAs are simpler. This makes their sensors lower cost and more reliable. They also do not require the extensive cooling as long-wave IR (LWIR) sensors, giving them a size advantage.

However, mid-wave IR and LWIR provide additional advantages for nighttime operation and seeing through obscurants like smoke, dust, and fog. A key characteristic in determining the sensitivity of these sensors is their noise equivalent temperature difference. A typical sensitivity suitable for the C-UAS classification mission is 40 mK. Their intricate materials make them more costly and typically lead to more dead pixels on their FPA. They also require some design study to choose a cooled vs. an uncooled sensor (the former is larger and more expensive). Nevertheless, the added functionality they bring in dealing with any sort of environmental degradation makes them worthwhile.

Radar

Specific radar techniques can also contribute to classification using analysis based on micro-Doppler signatures. Micro-Doppler analysis is capable of detecting high-frequency, moving components within an object, such as rotor or propeller blades of the target UAS. sUAS present additional challenges to micro-Doppler analysis because of their low mass and small inertia. Wind impacts their flight significantly, which, coupled with their active stabilization measures, creates

highly variable trajectories. This is problematic because high-Doppler frequency resolution measurement requires extended, coherent data.

PROCESSING

Because of the short timeline available to defeat the sUAS, at-sensor processing is critical. A human must not be in the loop between the radar or RF detection system and a camera, for example. This opens up several architecture trades that vary greatly, depending on whether the C-UAS solution must function for a small group of soldiers operating where they might not have access to higher-order, command and control (C2) assets.

In the case of an all-in-one solution where a vehicle is travelling with a small group or a ground-based portable system, the detection system must be able to process its information and cue the EO/IR sensor for classification. The EO/IR system, in turn, must determine reliably that the object in question is an sUAS in order to engage a kill solution. This requires advanced, small-format processors, such as the NVIDIA Jetson line, which can be small and power efficient but run advanced algorithms quickly.

Radar-tracking, micro-Doppler analysis, image-segmentation, and material-identification algorithms are extremely complex, power- and processing-hungry processes that must factor into any C-UAS system design and go hand-in-hand with the choice of the sensors themselves. Even in the case of a C-UAS asset intended to function with access to higher C2 systems, at-sensor processing is critical because of the short defeat timeline against a threat sUAS. A vast amount of data cannot be related to the C2 system, processed for detection or classification, and returned to the C-UAS system for prosecution. Linking to the C2 system, in this case, gives situational awareness of the drone threat but does

not actually contribute to detecting, classifying, or defeating the target.

DEFEAT

Once the sUAS has been detected and classified, a defeat mechanism must be engaged. There are a number of means being used and evaluated for this task. Any of the following might be cued once a spectral system has made a classification.

RF-based drone takeover is ideal when an sUAS must be defeated in the presence of people or high-value infrastructure. In this case, electronic techniques are used to control a drone and either force it to land at a given safe zone or, by jamming communication to its controller, make it return to its point of origin on its own. D-FEND is a current industry solution offering detection and location capabilities that take over an sUAS and land it in a prechosen, safe zone [5].

Another technique is to leverage a purpose-built drone to engage in an intercept collision path. The interceptor is itself an sUAS; some work by colliding with their target, such as Anduril's new interceptor [6]. This interceptor is heavy

sUAS present additional challenges to micro-Doppler analysis because of their low mass and small inertia.

and designed to survive the collision. Others, like the Skylord Hunter, use a C-UAS net payload to disable their targets [7].

Kinetic destruction uses appropriately-sized munitions aimed at the sUAS to defeat it. Proximity triggers may help destroy sUAS. Ground-based nets and latex cloud deployments can also be launched.

Directed energy is an additional means to defeat oncoming UAS. It has recently been the focus of extensive military interest. Raytheon delivered their first High-Energy Laser Weapon System (HELWS) to the U.S. Air Force in 2019 for year-long field evaluation [8] (Figure 3). This system, which leverages



Figure 3: Raytheon's HELWS (Source: U.S. Air Force).

a multispectral system for targeting, is a significant step forward in directed energy application; its results will help define future efforts.

THE SWARM sUAS THREAT

We have so far focused on a single UAS. This applies to security and counterinsurgency contexts. The far more difficult problem, but one that must be solved if we are to compete against near-peer adversaries in the future battlespace, is defeating swarms of UAS. Already the subject of offensive research in the Defense Advanced Research Projects Agency Offensive Swarm Enabled Tactics program [9], Russia declared in 2019 its intent to create “Flock-93,” an operational concept where warhead-equipped drones numbering upwards of a hundred are equipped with explosive payloads to attack convoys [10].

Against swarms, at-sensor processing is even more essential. Communicating data and video streams back to a C2 post for centralized processing and coordination would jam communication channels and create a single point of failure. Swarm offenses could easily overwhelm a centralized processing architecture as part of the C2 capability. Fortunately, industry advances can meet this challenge. Compact, low-cost processors have evolved into high-performance, embedded computing solutions. Each sensor can dedicate processing for tracking or video, with specific function to distill information into target attributes and significantly reducing information bandwidth back to the C2 center.

With specific target attributes, the C2 processor is responsible for collecting all measurements from individual sensors into track vectors, with classification, prioritization, and a filter for false detects from clutter. Candidate threats working through the processing filter achieve a threat classification and assigned target identifications, tracked with realistic motion gating, and further locked in to maintain observation and tracking.

CONCLUSIONS

The engagement with UAS detection, classification, and mitigation is a current problem that will continue to advance in both the threat and antithreat missions in the coming years. UAS continue to increase in use and decrease in cost. Current research shows individual success capabilities, but it is in combining the systems where a greater impact is likely by leveraging the benefits of each system. On-sensor processing and automated algorithms will continue to be very important. ■

ACKNOWLEDGMENTS

The author thanks Chris Sheppard, Wes Procino, and Abraham Isser (all QinetiQ, Inc.) for their technical assistance.

REFERENCES

- [1] Wilson, B., S. Tierney, B. Toland, R. M. Burns, C. P. Steiner, C. S. Adams, M. Nixon, M. D. Ziegler, J. Osburg, and I. Chang. “Small Unmanned Aerial System Adversary Capabilities.” Homeland Security Operational Analysis Center, 2020.
- [2] Nguyen, P., M. Ravindranathan, R. Han, and T. Vu. “Investigating Cost-Effective RF-based Detection of Drones.” DroNet '16: Proceedings of the 2nd Workshop on Micro Aerial Vehicle Networks, Systems, and Applications for Civilian Use, pp. 17–22, June 2016.

[3] Shin, H., K. Choi, Y. Park, J. Choi, and Y. Kim. “Security Analysis of FHSS-type Drone Controller.” In: Information Security Applications, Springer: *Lecture Notes in Computer Science*, vol. 9503, 2015.

[4] Benyamin, M., and G. H. Goldman. “Acoustic Detection and Tracking of a Class I UAS With a Small Tetrahedral Microphone Array.” ARL-TR-7086, U.S. Army Research Laboratory, pp. 16–17, September 2014.

[5] “D-Fend Solutions’ EnforceAir selected by the U.S. DIU during ‘Counter Drone 2.’” *Military Press Releases*, <https://www.militarypressreleases.com/2020/02/04/d-fend-solutions-enforceair-selected-by-the-u-s-diu-during-counter-drone-2/>, accessed 23 April 2020.

[6] Ward, J., and C. Sotile. “Inside Anduril, the Startup That Is Building AI-powered Military Technology.” *NBC News*, <https://www.nbcnews.com/tech/security/inside-anduril-startup-building-ai-powered-military-technology-n1061771>, 3 October 2019.

[7] Skylord Hunter Short. <https://vimeo.com/390202512/67b3c4d5cc>, accessed 15 May 2020.

[8] Keller, J. “Raytheon Delivers First Laser Counter-UAV System.” *Military and Aerospace Electronics*, <https://www.militaryaerospace.com/power/article/14069489/laser-weapon-counteruav-directedenergy>, accessed 23 April 2020.

[9] Defense Advanced Research Projects Agency (DARPA). “Offensive Swarm-Enabled Tactics (OFFSET).” <https://www.darpa.mil/work-with-us/offensive-swarm-enabled-tactics>, accessed 23 April 2020.

[10] Atherton, K. D. “Flock 93 Is Russia’s Dream of a 100-Strong Drone Swarm for War.” *C4ISR News*, <https://www.c4isrnet.com/unmanned/2019/11/05/flock-93-is-russias-dream-of-a-100-strong-drone-swarm-for-war/>, accessed 23 April 2020.

BIOGRAPHY

MATTHEW HENDERSON has 5 years of experience working for QinetiQ in sensing systems, with a focus in spectral modalities. He has worked with industry technical solution developers to identify and present hyper- and multispectral systems in response to U.S. government needs. He has also participated in creating test plans for hyperspectral sensing systems, as well as multiple technology research deliverables for government customers. Mr. Henderson holds a master’s degree from Kent State.

(Source: 123rf.com)

PASSIVE COHERENT LOCATION RADAR

THE SILENT THREAT

By Ronald Mathis

INTRODUCTION

The future battlefield will be highly complex and congested. The electromagnetic (EM) environment will consist of a complicated mix of signals, both threats and friendlies. Figure 1 is a simplified illustration of some of the potential players. Passive coherent location (PCL) radars represent an emerging threat that differs from typical radar threats in that no radar signal is transmitted. Rather, the radar signals consist of signals of opportunity, such as radio or TV stations, enabling PCL radars to operate covertly. In other words, they can actively track targets of interest without alerting the target to their presence.

The Electronic Warfare Integrated Laboratories (EWIL) at the U.S. Naval Air Warfare Center Weapons Division (NAWCWD) provides a simulation of contested environments enabling the testing of new and emerging systems against realistic threats and threat scenarios. A key element of this test environment is the Testing Theater Operations Using Real-time Networks Achieving Multiple Interconnected Nodal Tactics (T²OURNAMINT) system, which serves as the hub of a digital electronic warfare (EW) environment.

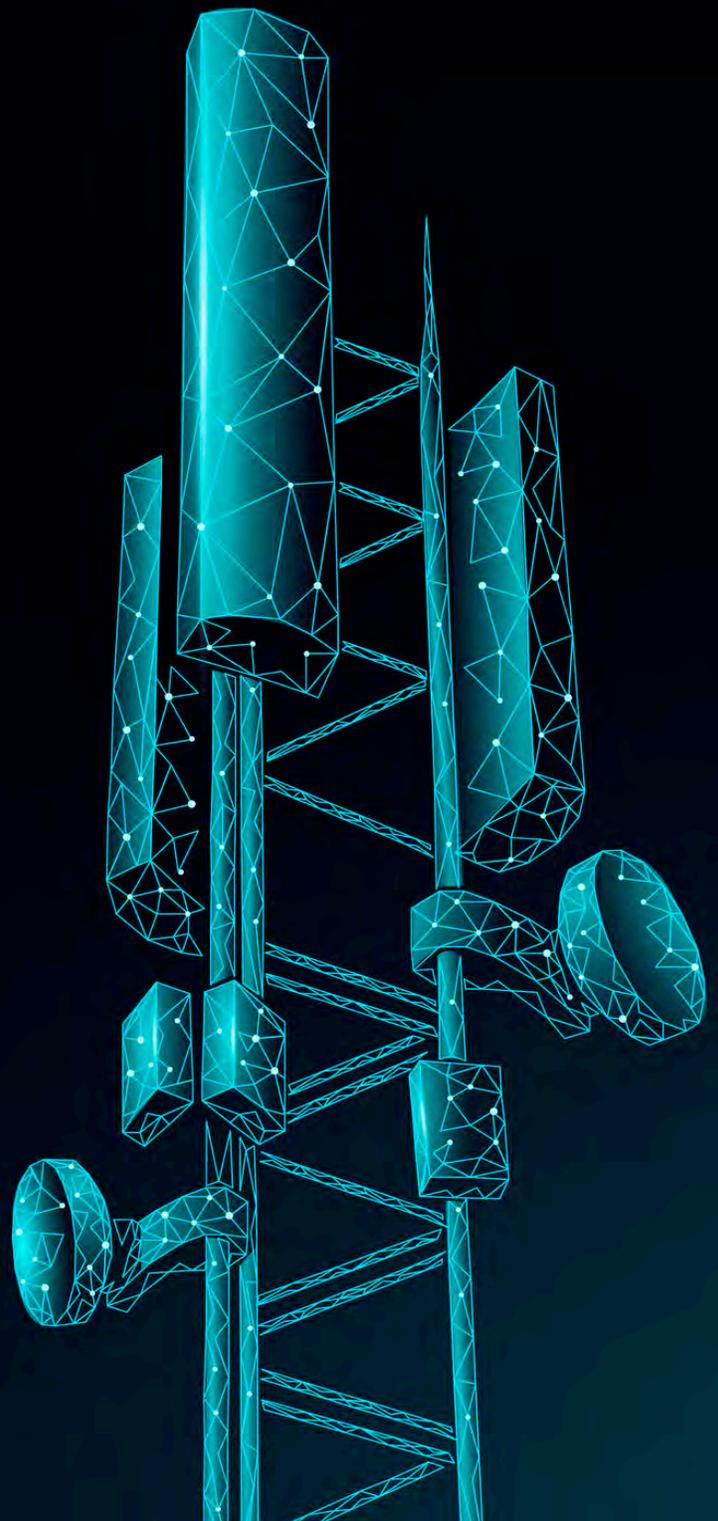




Figure 1: Contested Environment Illustration (Source: NAWCWD).

Adding a PCL radar to the T²OURNAMINT test environment will enable the development of countermeasures to this unique, emerging PCL radar threat.

PCL RADAR OVERVIEW

PCL radars are a variation of bistatic radars, which are radars in which the transmitter and receiver are not colocated. This is in contrast to the more common monostatic radars having a transmitter that is colocated with or near the receiver. The unique feature of PCL radars is their use of signals of opportunity.

Signals of opportunity can be radio or TV broadcasts, including both analog and digital TV, mobile telephone networks, local area networks, and even satellite transmissions. The most common transmitters used in existing PCL systems are FM radio stations. They are available worldwide, and the signal bandwidth (50–100 kHz) and power (typically, 100–250 kW) are adequate.

Digital TV signals are also commonly used in areas where they are available.

Figure 2 illustrates the elements of a PCL radar, where R_t is the transmitter-to-target distance and R_r is the target-to-receiver distance. The direct path distance from the transmitter to the receiver can vary from a few kilometers to 100 km. The location of each transmitter and its distance to the receiver are known by the receiver,

which must have a separate, dedicated receive channel for each transmitter.

The PCL receiver detects a target by first collecting and digitizing a sample of the direct path transmission. The sample is then used to form a matched filter, which the receiver uses to search for the same signal reflected from targets of interest. The peak of a matched filter response is used to determine the differential time between the two paths. Since the

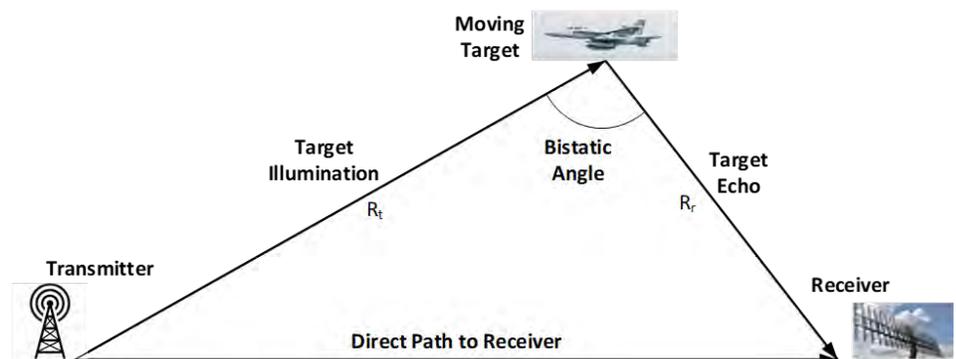


Figure 2: Key Elements in a PCL Radar (Source: NAWCWD).

transmitter position is known, the propagation time from the transmitter to the target to the receiver can be computed. Knowing this time delay enables the computation of an ellipsoid with foci at the known transmitter and receiver positions. The target is located on the ellipsoid surface. Finally, the intersection point of at least three such ellipsoids locates the target in three dimensions (illustrated in Figure 3). Of course, this computation assumes that three different transmitter-receiver pairs are available. With just two transmitter-receiver pairs, the azimuth angle of the target can be determined, with no knowledge of the altitude.

A variety of configurations is possible. In general, a minimum of three transmitter-receiver pairs is required to locate a target in three dimensions. That could be three receivers and one transmitter, three transmitters and one receiver, or any other combination forming three pairs. When more than one receiver is used, one of the receivers is designated as the master and the others must be time synchronized to that master receiver.

Alternatively, PCL receivers can use directional antennas to reduce the required number of receiver-transmitter

pairs. When the receiver can locate and track the direction of the target, then the range to the target is provided by the point where the target direction intersects a single ellipsoid. Although this approach is simpler, it is usually less accurate because of uncertainty in the true target direction.

PCL ADVANTAGES

There are several advantages PCL radars have over conventional monostatic radars—one being that they are inherently covert. That is, unlike conventional monostatic radars, PCL radars have no transmitted beam to give away their position. That allows them to covertly acquire and track targets and pass the target position to other platforms. It is difficult for an adversary to apply countermeasures when they do not know that they are being tracked.

PCL radars can also be considered antistealth. Stealth technologies have been developed from L-band to X-band (1 to 12 GHz). However, FM radio operates in the VHF band (from about 80 to 108 MHz), where stealth materials and methods are not as effective. Therefore, stealth aircraft will have much larger cross sections (be less stealthy) against PCL radars using FM radio stations as their signal of opportunity.

The benefits of not having a transmitter also include smaller size, weight, system complexity, and reduced maintenance. This leads to lower cost of operation and simplifies implementation on mobile platforms. Mobility also contributes to PCL radars' ability to operate covertly.

Another benefit of not having a transmitter is that a PCL radar adds no additional demand on spectrum resources. The EM spectrum is extremely crowded. Each radio or TV station, cell tower, microwave oven, etc., must license its piece of the spectrum with stiff penalties for spilling energy into adjacent frequency bands. This is also a problem for new monostatic radars because they must get approval to operate at a particular frequency with a particular bandwidth. However, since PCL radars use existing signals, this is not a barrier to fielding new systems.

PCL CHALLENGES

PCL radars have several unique challenges. One is the operator's lack of control over the transmitter. The PCL radar operator has no control over the location, signal type, transmission power, transmission content, and other parameters—all which affect the radar performance. For example, FM radio is a commonly-used signal of opportunity, but the radar operator has no control over the type of programming from any particular station, yet the programming significantly affects radar performance. The worst format is voice because of pauses during which there is no signal. One of the better formats is rock music because it is more continuous, with fewer pauses or gaps.

Another significant challenge is isolation between the reference signal (direct path to receiver in Figure 2) and the much smaller target echo. The direct-path signal is typically many orders of

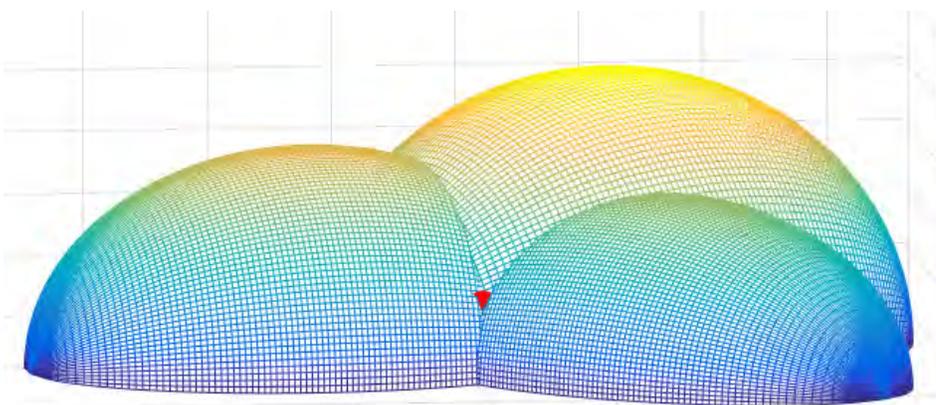


Figure 3: Intersection of Ellipsoids Locates Target at the Red Dot (Source: NAWCWD).

magnitude stronger than the target echo. If even a very small component of the reference signal is received by the target receiver, it can degrade or even prevent target detection.

Some of the methods used to isolate the signals include the following:

- Physically blocking the signal antenna with a building or hill. This is most appropriate with fixed-site PCL radars rather than mobile.
- Using a signal canceler that coherently cancels the reference in the receiver prior to signal detection. The process is similar to that used in noise-cancelling headphones except that it operates at microwave frequencies rather than audio frequencies.
- Using a null-steering antenna. (This is described in more detail in the Antennas section of this article.)
- Using filtering to isolate a Doppler-shifted target signal from the nonshifted reference signal. The signal from moving targets will be shifted in frequency, which can allow using a bandpass filter to isolate it from the reference signal.

Generally, a combination of methods must be used because no single method will provide the necessary isolation.

Another issue is that the coverage area of a PCL radar is more complex than the coverage area of a monostatic radar. The maximum range of a conventional monostatic radar is given by the well-known radar range equation. The coverage area is nominally circular, the same in any direction, within the constraints of the antenna and the terrain.

The maximum range contour of a PCL radar is more complex. Instead of a circle, there is a range of shapes (illustrated in Figure 4) that depends on

Computer-based methods have been developed to decide which radio stations to use for optimum performance in a given application.

the radar range and L , the transmitter-to-receiver distance. We designate the radius of an equivalent monostatic radar range as R_m . This is the range a particular PCL radar would have if the transmitter and receiver were collocated.

The relationship between R_m and the two ranges defined in Figure 2 is given by $R_m^2 = R_t \times R_r$. The shape of the maximum range contours in this case, instead of circular, is described by the ovals of Cassini with respect to the transmitter and receiver points. The focal points in the ovals are the transmitter and receiver locations. When the detection range, R_m , is large compared to L , the detection area is similar to a conventional monostatic radar (Figure 4 [a] and [b]). However, when the detection range is small compared with the transmitter-to-receiver distance, then the detection areas can look like Figure 4 (c) and (d). In the extreme case (Figure 4 [d]), the PCL radar can only see targets that are close to the transmitter or the receiver.

Therefore, we can say that the relative locations of the transmitter(s), the target, and the receiver will significantly affect the ability to accurately locate and track the target. In another extreme case, when the target is near the line between the transmitter and the receiver, the effective cross section is

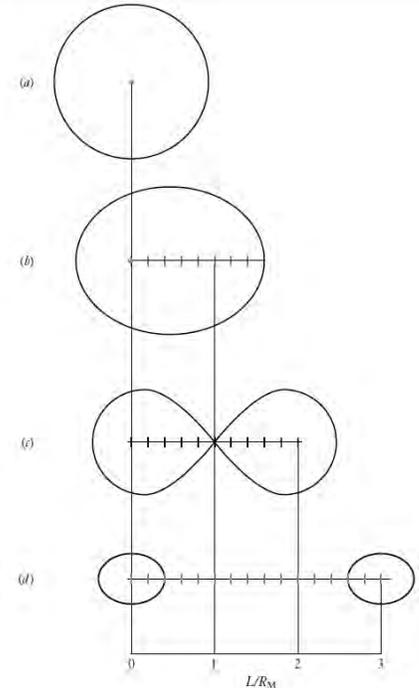


Figure 4: Ovals of Cassini Determine Detection Area (Source: Willis [1]).

significantly enhanced, but the ability to determine its location is greatly diminished (i.e., the target can be seen but not located).

In practice, the location of PCL receivers and the particular transmitters of opportunity used must be carefully chosen to optimize radar performance. In recent studies of PCL radar operation in areas with a high density of stations, methods for selecting the best radio stations for a given receiver location and expected target locations have been used. Computer-based methods have been developed to decide which radio stations to use for optimum performance in a given application [2].

ANTENNAS

PCL radars typically use antenna arrays rather than a single-element antenna. Figure 5 shows an example of a commercially-available PCL radar. Notice that the antenna consists of a circular



Figure 5: Commercial PCL Radar Example (Source: Hensoldt [3]).

array of eight dipole antennas. A review of PCL radars shows that this antenna arrangement is common. The details of the implementation will change, but the eight-element, circular array is often seen.

When the phase of the individual elements can be separately controlled, this becomes a phased array. The processing complexity is increased, but it can perform null steering. That is, it can place a null on the strong reference signal while simultaneously forming a beam in the direction of the much smaller target signal. Null steering can provide much of the needed isolation between the reference signal and the target echo.

It is also possible to use larger antennas to detect the target signal. A larger antenna provides higher gain and better angular resolution in the target direction, potentially increasing the distance the radar can see. The tradeoff is that a larger antenna is easier to observe, making the PCL radar less covert.

PCL Radar Challenge

Although we have just given a brief overview of PCL radars, it should be evident that they represent a unique threat unlike any other radar. Furthermore, it is unlikely that a PCL radar would be used in isolation. Rather, it seems most useful when integrated with other platforms, including conventional radars. To use Figure 1 as an illustration, it seems likely that PCL radars would be added to the environment, making it even more complex. The challenge is to develop countermeasures to an invisible threat in a complex environment.

T²OURNAMINT

Future battlefield engagements will occur in congested EM environments where radar and communication systems encounter intentional and unintentional interference from many sources simultaneously, including both adversarial- and friendly-force transmissions. The complex array of signals will cover a broad spectral

range from communications bands to X-band radar and above. Furthermore, the signals are constantly changing in response to the changing EM environment and adversarial responses.

With a few exceptions, new weapons systems are typically tested one on one against specific threat systems. While such testing provides useful information, it does not provide insight into performance in a highly complex, dynamic battlefield with multiple, simultaneous, constantly-changing threats.

The T²OURNAMINT system at NAWCWD EWIL resides in the Electronic Combat Simulation Environment Laboratory. T²OURNAMINT brings a new level of fidelity to many-on-many, hardware-in-the-loop (HWIL) EW testing. It can be described as the hub of a digital electronic warfare (EW) arena. It provides a digital, high-fidelity threat environment into which multiple systems and systems of systems can be connected and interact at a signal-processing level. An overview illustration is shown in Figure 6.

The T²OURNAMINT system is driven by a scenario generator that provides a single, all-inclusive mission scenario. In response to scenario details, T²OURNAMINT adds independent Doppler, range attenuation, and time-delay effects across all relevant frequencies. Closed-loop operation provides a dynamic, simulated battlespace environment in which systems interact in real time as they would in the field.

Other T²OURNAMINT features include the following:

- A frame generator maintains strict real-time operation to keep control over hardware devices and is synchronized to radar-coherent

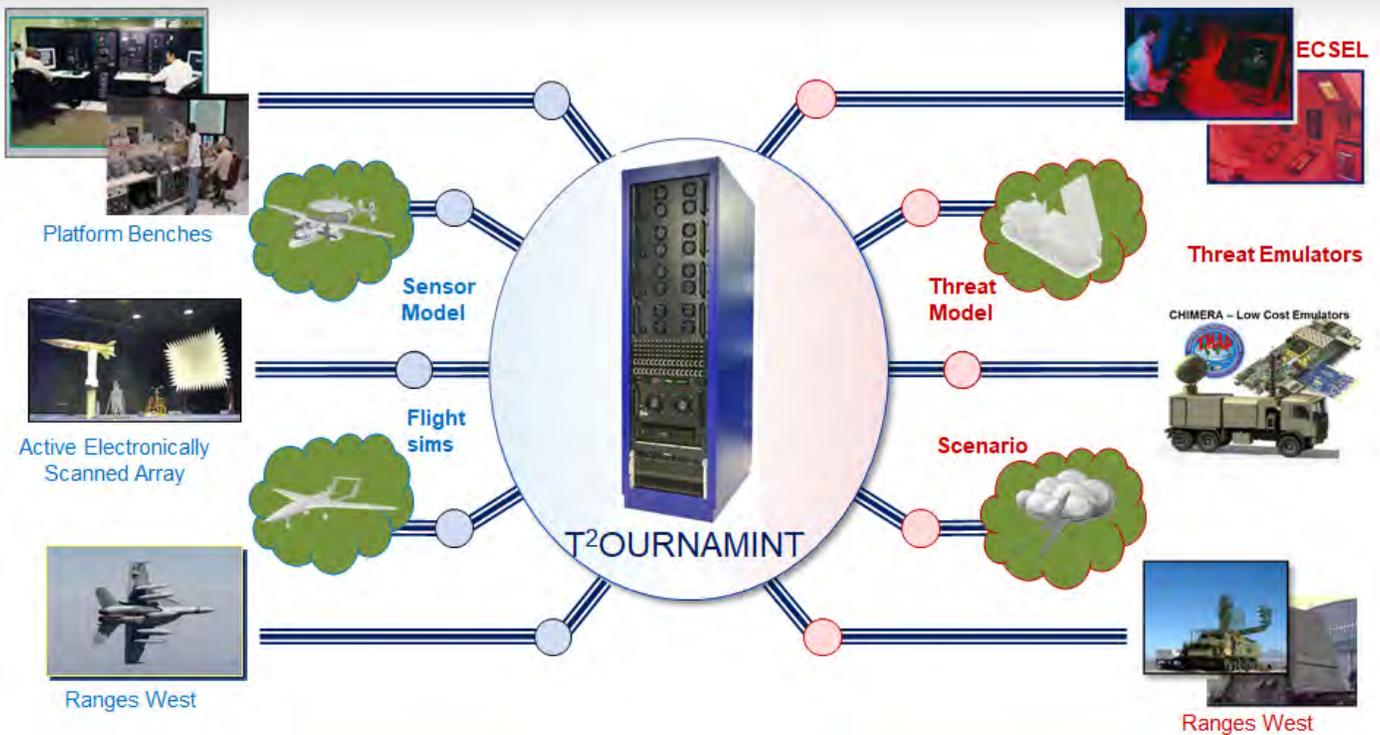


Figure 6: Connected Elements See Realistic Signals From All Other Nodes (Source: NAWCWD).

processing intervals to ensure simulation accuracy.

- T²OURNAMINT interacts at the real radio frequency (RF) and signal-processing level, and all input/output occurs at RF.
- Signal reflection from each object skin return caused by the PCL transmitted waveform is accounted for.

The T²OURNAMINT system is an ideally-suited testbed for developing strategies to counter the PCL threat. Therefore, a generic, easily reconfigurable, PCL radar is being developed to operate with the T²OURNAMINT system. This will enable the development of counter PCL radar strategies for new and emerging PCL radar threats.

CONCLUSIONS

PCL radars differ from typical radar threats in that they are bistatic radars in which no radar signal is transmitted. Instead, they rely on signals of

opportunity, such as radio or TV stations, enabling them to operate covertly. This means that they can actively track targets of interest without alerting the target of their presence. Their relative simplicity also means that they are lower cost and can readily operate from a mobile platform.

The T²OURNAMINT system in the NAWCWD EWIL is an ideal platform for testing emerging anti-PCL strategies. As new strategies are developed, they can be tested in a realistic, closed-loop, many-on-many HWIL environment provided by the T²OURNAMINT system. ■

ACKNOWLEDGMENTS

The author wishes to acknowledge helpful comments and edits from his colleagues Ethan Julius, John Rice, and Ernie Rodriguez and insights gained from discussions with Duane Roth and Omar Ramos.

REFERENCES

- [1] Willis, N. *Bistatic Radar*. Raleigh: SciTech Publishing Inc., 2007.
- [2] Johnson, N. "Method for Real-Time Signal Selection for Passive Coherent Location Systems." Ph.D. dissertation, University of Central Florida Orlando, FL, 2017.
- [3] Hensoldt. "TwInvis - Passive Radar," https://www.hensoldt.net/fileadmin/HENSOLDT_2019/Products/Radar_IFF_Datalink/18-04-28_Hensoldt_TwInvis_Passive_Radar_Flyer_v2d_highres.pdf, accessed March 2020.

BIOGRAPHY

RONALD MATHIS is a physicist for EWIL at NAWCWD, Point Mugu, where he researches and develops advanced technologies supporting the EW domain. He supports technology for RF and microwave sensing, signal processing, identification, detection, tracking, and geolocation of emitters, including the ALQ-218 receiver used within the EA-18G Growler. He is a primary contributor in digital signal processing, systems development, and hardware integration and tests. He authored and coauthored 19 patents, some which are related to RF signal processing, including EW applications and photonics and fiber optics signal processing. Dr. Mathis holds a Ph.D. in physics from the Missouri University of Science and Technology.



(Photo Source: U.S. Air Force)

SYSTEMS ENGINEERING OF AUTONOMY:

Frameworks for MUM-T Architecture

By Michael Woudenberg, George “Mark” Waltensperger, Troy Shideler, and Jerry Franke

SUMMARY

Do we design autonomous systems or systems with autonomy? This question will be explored and developed by first understanding the perspective of autonomy, deconflicting the buzzwords from the reality, and applying a robust and simple framework. This will encapsulate and begin to decompose autonomy, autonomous behaviors, artificial intelligence (AI), and collaborative Manned-Unmanned Teaming (MUM-T) systems for the U.S. Department of Defense (DoD) customer.

This article will progress from conceptualizing autonomy to introducing frameworks to analyzing autonomy and conclude with a synthesized approach to designing autonomy into a system-of-systems (SoS) solution.

INTRODUCTION

Warfighters will find themselves operating in complex battlespaces against highly adaptive, multi-dimensional, and fully automated SoS. Joint all-domain warfare environments and the nascent mosaic warfare concept

from the Defense Advanced Research Projects Agency (DARPA) demand system behaviors never experienced before. In these environments, there will be complex, adaptive, emergent, and highly unpredictable interactions, where future conflicts will be data driven, with extremely large numbers of manned and unmanned platforms in the mix. This will make human decision makers highly susceptible to information overload but stressed with vastly-shortened kill chains and decision timelines.

Autonomy-enabled teams of manned and unmanned systems will be a disruptive game changer under these conditions for both the threat and as a force multiplier for U.S. forces and their allies. As with other complex adaptive systems, MUM-T will not just be greater than the sum of their parts, it will be *different* than the sum of its parts and should be treated as such. The MUM-T combinations and permutations will greatly exceed the performance capabilities of manned platforms alone. Warfare will be transformed and disrupted if the characteristic asymmetries of MUM-T are planned and exploited wisely.

Lockheed Martin established a MUM-T, integrated product team (IPT) of subject matter experts organized to tease apart the collaborative autonomy/ MUM-T problem. The team was tasked with identifying techniques, tools, and methods of operations analysis to show the benefits of MUM-T. They were challenged with the difficult problem of identifying how Warfighters, technologists, and engineers communicate regarding these new and extraordinary capabilities, with a common language and discriminating the technology exhibiting unique operational behaviors that distinguish one autonomous approach over another.

To achieve these revolutionary capabilities, the systems' designer must first step back and baseline, deconflict, and understand the complex environment of autonomous systems.

CONCEPTUALIZING AUTONOMY

The first obstacle to overcome was to establish a common foundation of autonomy. This required the team establish first principles for autonomy to align definitions, create an ontology, and agree on appropriate semantics to fully conceptualize the problem space.

Warfare will be transformed and disrupted if the characteristic asymmetries of MUM-T are planned and exploited wisely.

In "Autonomous Horizons – The Way Forward," the chief scientist of the U.S. Air Force and team captured the complex relationships of the underlying functions and behaviors that autonomous systems achieve. Their graphic, as captured in Figure 1 [1], identifies that the solution space for autonomous systems is, by nature, polymathic, i.e., requiring knowledge that spans a significant number of subjects and the need to draw on complex bodies of knowledge to solve the problems.

The multi-disciplinary problem was addressed in three ways. First the team looked at consolidating an executable definition for autonomy. Next, the problem space was analyzed from a systems engineering perspective. Last, the conceptualization of autonomy had

to be modular and composable into modeling and simulation and MUM-T configurations.

Defining Autonomy

A cursory look at defining autonomy was exacerbated from the perspective of the U.S. government customer, where 10 major organizations (the U.S. Army, Navy, and Air Force; Secretary of Defense; DARPA; National Aeronautics and Space Administration; DoD Joint Procurement Office; National Institute of Standards and Technology [NIST]; Center for Naval Analysis; and the Defense Science Board) identified that not only do they have different definitions of autonomy, but these definitions shifted from year to year.

To begin reducing this problem space, the team performed an analysis on these definitions, visions, and mission statements of those organizations to distill a definition in this environment. This analysis looked for key, encapsulating elements which, by removing, would change the nature of those statements. These elements established a taxonomy of characteristics and a common lexicon for discussion. The team then began mapping the semantic ontology of those characteristics across the different definitions to identify critical elements

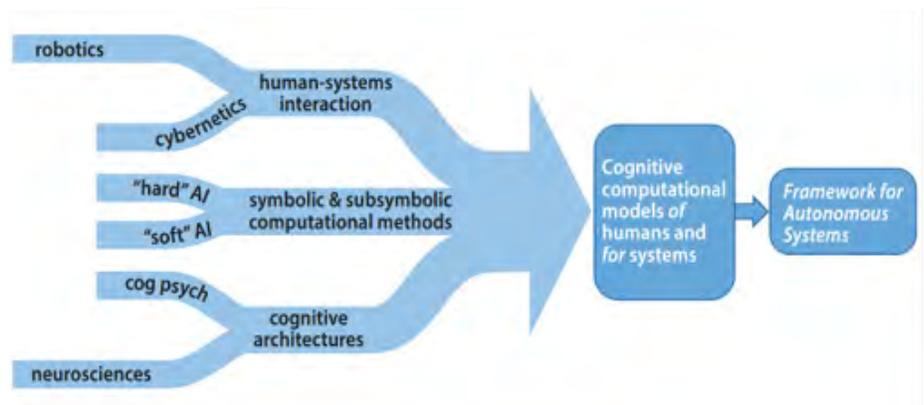


Figure 1: Research and Development (R&D) Streams Supporting Autonomous Systems (Source: *Autonomous Horizons*).

that maximized alignment to all the stakeholders. This distillation resulted in the following definition of autonomy:

Autonomy is a capability whereby an entity can sense and operate in its environment with some level of independence. An autonomous system may be comprised of automated functions with varying levels of decision making, and it may have adaptive capabilities, but these features are not required for a system to be autonomous.

The team found this definition aligned with a simple heuristic used to conceptualize autonomy:

Autonomy is a gradient capability enabling the separation of human involvement from systems performance.

This corollary, not exclusive of supporting technologies such as AI, reduces the complexity from many of the academic pitfalls the team refers to as the “No True Autonomy Fallacy,” which is based on the No True Scotsman Fallacy.

Conceptualizing autonomy as a capability enabling the separation of human involvement from systems performance transitions autonomy from being the end state to an enabler of an end state. This end state focuses more on improved warfighting capabilities where the human in the loop is a limiting factor. This enabling baseline led the team to the next consideration—systems layers of autonomy.

SoS Approach to Autonomy

The Defense Science Board 2012 Autonomy Task Force Report identified a concern: “Autonomy is often misunderstood as occurring at the vehicle scale of granularity rather than at different scales and degrees of sophistication depending on the

requirements” [2]. This insight is critical to the broader concept of autonomy.

A self-driving car is a challenging problem to solve with complex sensing, decision analysis, and heavy data processing in a dynamic environment. Imagine, however, if you were to move requirements into the super-system roads. Now, instead of machine vision to identify and contextualize a stop sign, what if the stop sign announced itself and its context with a vision of broader, current conditions in mind? Intersections could control traffic flow, and the system requirements for the vehicle system could be substantially reduced.

The team considered the SoS approach and identified three layers for consideration—the entity, integrated system, and system security layers (see Figure 2).

The entity is the vehicular scale. It is the “thing” being produced and focuses on making a system smarter, networked, and collaborative, with improved AI, etc. This level is discrete.

In this example, the integrated system is focused on collapsing the kill chain, where one can achieve highly complex AI mission planning and integration of the kill chain from detection through mission planning to weapon engagement.

System security is considered as technologies become more interconnected. Additional cyberattack surfaces emerge with collaborative weapons, networked sensors, and remote kill chains, with new connections added to legacy equipment. The system security layer is critical to conceptualization. Autonomous technologies create both unique

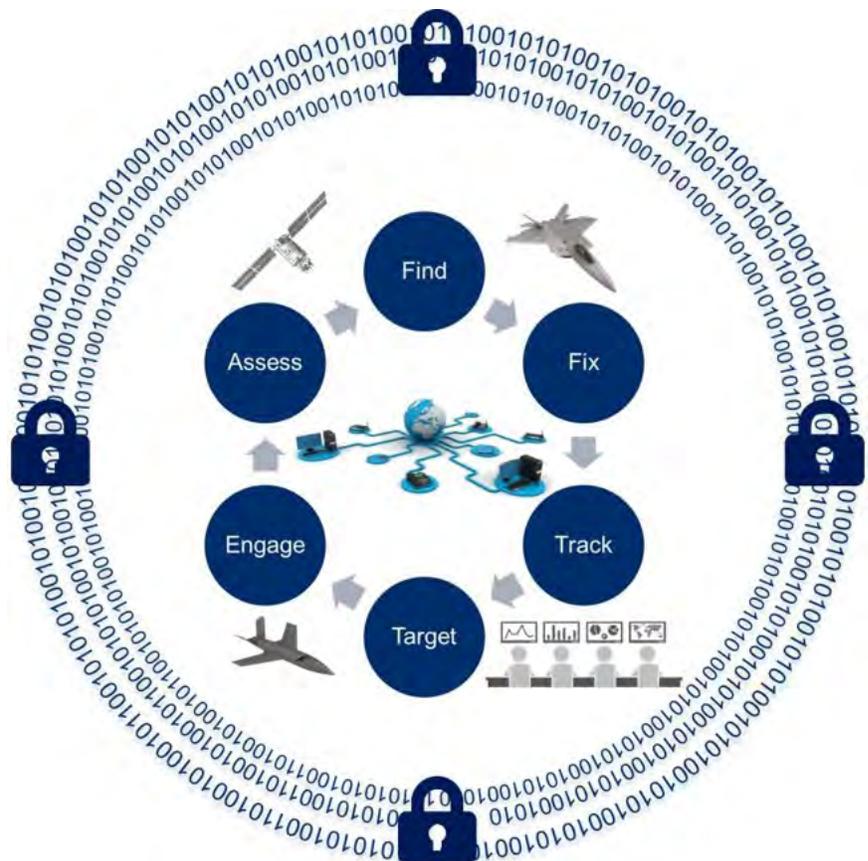


Figure 2: Autonomy Layers (Source: Lockheed Martin).

cybersecurity implications and opportunities to apply autonomous technologies to solve the system security concerns, such as real-time monitoring and resilient security through AI-based cyberdefense. This layer focuses on improving trust in autonomous system integrity.

These three SoS layers push beyond the vehicular scale and include the larger implications of the integrated systems and systems security. They become crucial in considering how to measure autonomy in systems design.

The Dimensions of Autonomy

The final consideration for conceptualizing autonomy is tying the definition with the SoS views into a method to measure the autonomy implications of MUM-T. The team initially struggled with identifying the critical concepts to measure to craft systems' interactions before three axes emerge (see Figure 3).

The first axis is Independent Operation, which captures the degree to which a system relies on human interaction and measures the separation of human involvement from systems performance. This scale can include completely-manual to completely-autonomous systems. It is on this scale that the independence of action of the entity or platform is measured.

The second axis is System Intelligence, which identifies the degree to which a system can process the environment to compose, select, and execute decisions. This also includes concepts referred to as AI and methods like machine learning (ML) that allow a system to perform complex computations and behaviors aligned with cognitive science.

Measures of System Intelligence against Independent Operation can capture ideas like autonomy at rest (high intelligence and low independence) and autonomy in motion (variable intelligence with higher independence).

This X/Y scale also captures automated functions (low intelligence and high independence) and allows comparing automation vs. autonomy.

The third and final axis is System Collaboration, which is the degree to which a system partners with humans and other systems. This axis identifies MUM-T behavior considerations and identifies interrelationships between systems and within an SoS view. Key in the development of these dimensions is the ability to map both human and machines on the axes.

Conceptualizing Autonomy Summary

To summarize conceptualizing autonomy, the team applied a definition of autonomy as a gradient capability enabling the separation of human involvement from systems performance. This capability can be applied to an entity, integrated systems, and systems security layering to ensure a holistic, SoS autonomy perspective. This SoS view can be mapped along three dimensions of Independent Operation, System Intelligence, and System Collaboration for further analyses and to design autonomous systems.

ANALYZING AUTONOMY

Based on the foundations established in conceptualizing autonomy, the team developed frameworks to analyze autonomy. This activity was born out of a need for a framework, taxonomy, or structure to study MUM-T operationally. What was needed could not be found in the literature and, apparently, had not been previously done or at least not published. With little theoretic basis on which to formulate and analyze the unique considerations of MUM-T, the team set off to build the structure itself. The goal was to establish the first

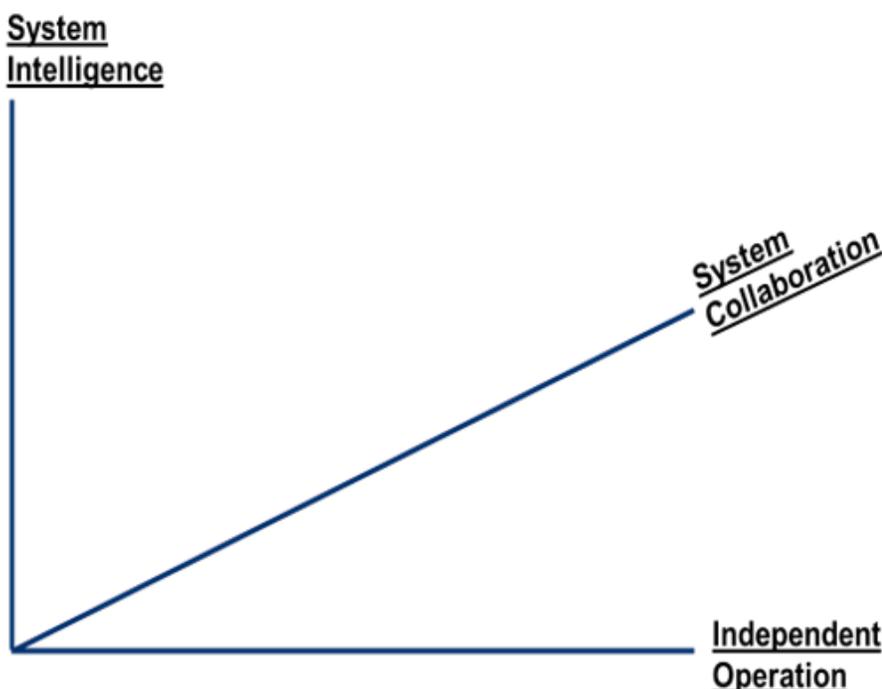


Figure 3: Three Dimensions of Autonomy (Source: Lockheed Martin).

principles of autonomy and a taxonomy of elements related to all autonomous systems. The structure is scalable and flexible to meet the needs of operational researchers, engineers, and Warfighters seeking to qualify and quantify solutions to problems concerning autonomous development, MUM-T.

The following four frameworks were developed:

1. Autonomous behavior characteristics (ABCs): capabilities organic to the autonomous system.
2. Operational: visually represents how the system is organized.
3. Environmental: captures the context/environment the system operates in.
4. Trust: assures autonomy.

The next sections will further detail these frameworks for analysis, their origins, and alignment with the conceptualization of autonomy.

Framework 1: ABCs

ABCs capture mission architecture considerations for how a system processes, interacts, and teams in an environment. These characteristics and associated scales are intended to be used as a heuristic approach vs. an explicitly-quantified relationship. They work to describe the relationships between entities, outcomes of teaming, and intelligence required to achieve customer requirements. These characteristics and associated maturities simplify complex design space inherent in MUM-T.

The overall autonomy maturity level, shown in Figure 4, establishes the format for each of the dimensions of autonomy dimensions. The autonomy maturity level is on an ordinal scale where each higher level subsumes and



Figure 4: Autonomous Behavior Characteristics for Independent Operation (Source: Lockheed Martin).

ABCs capture mission architecture considerations for how a system processes, interacts, and teams in an environment.

expands upon the capabilities of the level below it. That is, level 1 (manual) where 100% of operations are controlled by a human, has the least autonomous capability, while level 10 (full autonomy) reflects the most. A system having a higher-level number than another system implies that it has more autonomous capability.

The colors of the bullets at each level estimate the maturity of implementations of systems at the time of publication—as items mature, the method still applies. Green bullets indicate levels of capability that most fielded systems have demonstrated in general. Blue bullets indicate levels of capability that have not been fielded in most systems in a general way. However, some systems exhibiting that capability have been fielded, and/or fielded systems have exhibited that capability but in a limited or constrained way. Purple bullets indicate levels of capability that have not been widely fielded, but the technology for that level of capability

is under development, and the basic principles have been explored and understood. Red bullets reflect levels of capability that have currently not been achieved in a generalized way and whose constituent properties, including behaviors, are not yet fully understood. These levels can generally be compared to technology readiness levels (TRLs).

The ABCs align with the three dimensions of autonomy of Independent Operations, System Intelligence, and System Collaboration (see Figure 5).

Independent Operations

At the top level, the framework establishes an autonomy maturity level. This top-level view is derived from the Levels of Robotic Autonomy scale developed by Dr. Jenay Beer at University of Georgia and is based on a synthesis of ideas that combines aspects of many previous scales, including the original autonomy levels for unmanned systems (ALFUS) work [3]. This autonomy maturity-level model captures the system's overall ability to perform tasks in the world without explicit external control.

System Intelligence

System Intelligence contains four behavior characteristics—Situation Understanding, Planning and Control, Contingency Management, and System Adaptation.

Situation Understanding encompasses the sensing, perception, and processing to create a semantic and cognitive

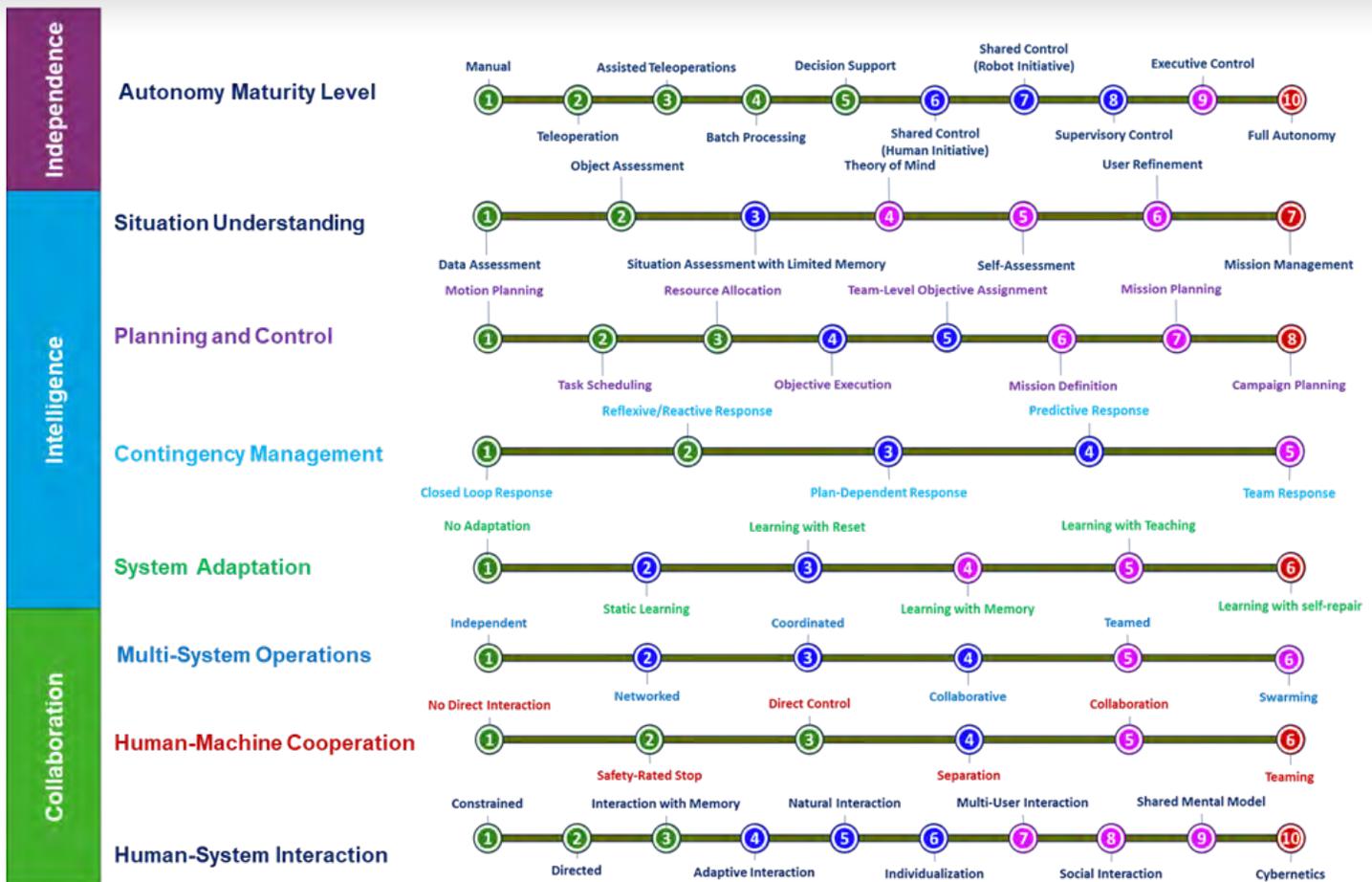


Figure 5: Autonomous Behavior Characteristics (Source: Lockheed Martin).

representation of the environment, mission, the system itself, and its teammates and adversaries. Situation Understanding goes beyond situational awareness in that it enables action to be taken. This measure reflects the observe and orient components of the observe, orient, decide, act (OODA) loop.

Situation Understanding is the synthesis of two existing models—the data fusion information group’s levels of data fusion [4] and Mica Endsley’s [5] levels of situation awareness.

Planning and Control provides the ability to plan and manage the execution of autonomous actions within a mission implementing the decide and act portions of the OODA loop.

Contingency Management adds the detection and reaction capability to unplanned events that affect mission success. Contingency Management works in parallel with the Mission Planning component to generate an effective response to contingencies either known and anticipated to some degree or unknown altogether. This scale was derived from Franke et al. in 2005 [6], which described the first-developed, holistic approach to contingency management for autonomous systems, referred to as the Lockheed Martin Mission Effectiveness and Safety Assessment [7].

System Adaptation is tightly integrated with the Contingency Management and Planning and Control functions. An autonomous system with adaptive

capability responds to environmental changes or changes in its internal functioning and modifies its structure of functionality appropriately to its circumstances. A major assumption in system adaptation is that the system can make the necessary adaptations needed.

In analyzing the ABCs for orthogonality, the team was unable to explicitly separate these behaviors and consolidate or split the behaviors while still retaining a common ontology with the research and academic environments. To that end, there is a natural relationship between the System Intelligence ABCs:

- Situation Understanding can exist on its own.

- Planning and Control must inherit Situation Understanding to develop a plan.
- Contingency Management requires a plan to identify a contingency.
- System Adaptation occurs when contingencies are managed more than the original plan requiring an adaptation down the relationship chain.

System Collaboration

Multi-System Operation measures multi-agent and distributed interactions between unmanned machines, electronic agents, and platforms, such as multiple unmanned and AI systems, including autonomy-at-rest systems. This characteristic measures machine-to-machine collaboration, where autonomous systems can operate together in many ways and seeks to provide a scaling of those interactive capabilities. While an unusual source for a scale related to autonomous systems working together, this scale is adapted from literature produced by the Oregon Center for Community Leadership and later adopted by the Amazon Web Services group, which defined levels 1-5 [8].

Human-System Interaction captures the complexity of direct communication and other interactions between an autonomous system and the human(s) controlling, supervising, or teaming with it. At least three domains contribute to human-system interaction (cognitive science, systems engineering, and human factors engineering), and the scale reflects contributions of each in terms of capability. The IPT derived this scale after determining no scale in the literature captured the depth and breadth of interaction that autonomous systems might support.

Human-Machine Cooperation measures the degree to which the human and

unmanned system work together in the same environment. This reflects not only the relationship between the system and the person controlling it, but also between the system and other people in its environment. This scale is adapted from one published by the Nachi Robotic Systems Corporation [9]. At its lowest level, humans and systems do not directly interact, except possibly through a remote interface. At each successive level, the richness increases how the system and humans coexist.

Tying these ABCs together along the three dimensions of autonomy provides the analyst a measurement of SoS implications, interactions, and relationships and allows the autonomy's analysis to be viewed beyond only the vehicular scale, as shown in Figure 6.

In this example, a highly independent, yet low-intelligence sensor system achieves Situation Understanding and passes it to a less-independent, more-intelligent battle management system to achieve Planning and Control. High-fidelity mission plans are collaboratively communicated to a weapon system, which is balanced on Intelligence and Independence and empowered for Contingency Management. System Adaptation is achieved by closing the

loop from the weapon system back to the integrated system, allowing updates to the data set for later analysis and system configuration modification to current operational and/or environmental conditions. The System Collaboration dimension measures and analyzes the relationship arrows between these three assets from the Multi-System Operation, Human-System Interaction, and Human-Machine Cooperation perspectives.

Our ABCs, layered on the three dimensions of autonomy, create the first, and most important, framework for analyzing customer requirements across a SoS view, with autonomy as an enabler.

Framework 2: Operational

The Operational framework for autonomy provides a tool with which to depict MUM-T configurations assigned to complex warfighting tasks. The Operational framework tool provides the means to build a visual representation of any MUM-T configuration and clearly identify key differences between autonomous systems. The objective with the Operational framework is to provide a method to identify common elements of autonomous system mission

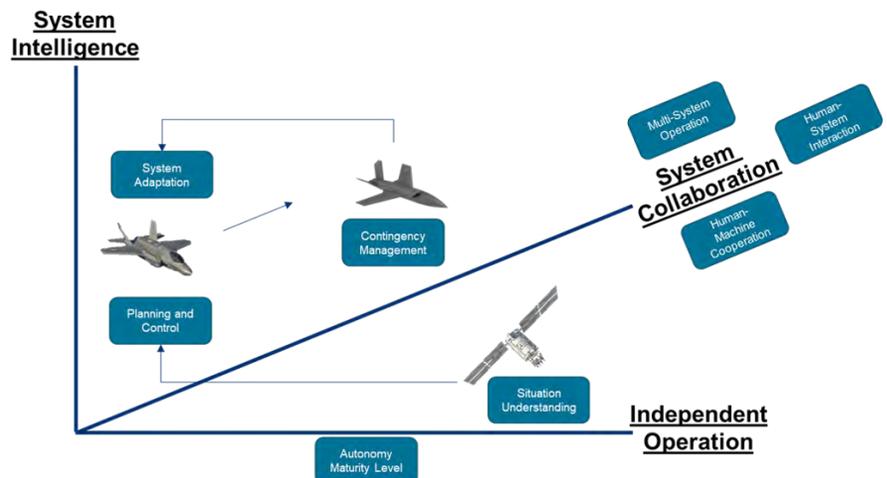


Figure 6: ABCs Along the Three Dimensions of Autonomy (Source: Lockheed Martin).

configurations and how the parts can be combined to create different operational effects; describe common operational approaches, techniques, and technology requirements of MUM-T; and develop an autonomous systems view that clearly identifies the degree of autonomous operations and where the human decision marker resides in the overall scheme of the mission.

Control elements are represented as color-coordinated squares as human (HUM) or autonomous program (AP). System elements are represented as color-coordinated circles, and command and control (C2) elements are color-coordinated triangles. Vehicles are depicted as control elements enclosed in a black hexagon. Information transfer elements are either solid or dashed, directional arrows with a number for autonomy level. A solid line indicates that a direct link exists between team members representing a common command and control relationship. A dashed line indicates an indirect link exists between team members; while they may be able to share information, they are unable to influence their team members' operational or tactical orders. Four examples of Operational views are displayed in Figures 7–10.

In Figure 7, members plan and execute separately against separate goals and objectives but coordinate to resolve conflicts. In Figure 8, members plan against common sets of goals but execute against separate objectives. Goals are separated by time or space. Objectives can be transferred from one team member to another but never simultaneously shared. In Figure 9, members belong to one system interdependently. Except for platform control, autonomy exists at the swarm level rather than the individual level. Individual plans do not exist. Decision making is shared and typically by

consensus. In Figure 10, members plan and act in a coordinated fashion throughout the mission and can perform tightly coordinated actions together.

In addition to modeling specific use cases, the Operational framework also allows users to combine elements to represent complex autonomous designs at two or more levels. The macro level view shows a depiction of the high-level interactions between team members. This view simplifies many of the underlying autonomous elements to focus on the interactions between manned and unmanned platforms and their control stations (see Figure 11).

The system-level view, on the other hand, provides a more comprehensive and detailed look of the autonomous teams to represent how autonomy is used at the system level within a specific platform and how the subsystems are integrated in the overall configuration scheme.

The Operational framework simplifies discussion with customers. It builds off the autonomous behavior characteristics and visualizes and clarifies the SoS considerations of MUM-T configurations. This framework is scalable from the integrated system down into subsystem considerations and quickly communicates basic

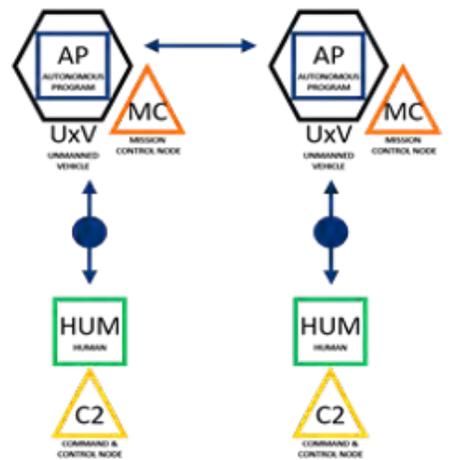


Figure 7: Coordinated (Source: Lockheed Martin).

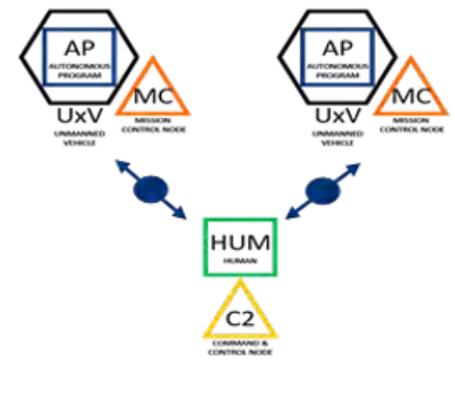


Figure 8: Collaborative (Source: Lockheed Martin).

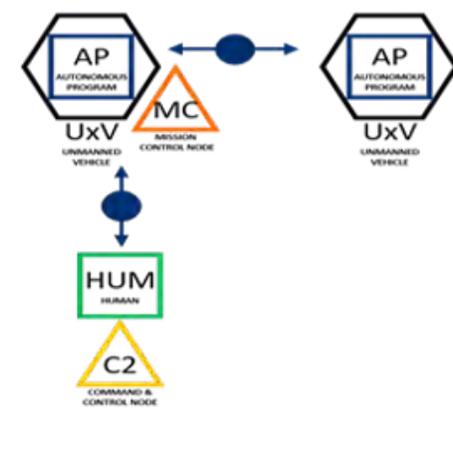


Figure 9: Swarming (Source: Lockheed Martin).

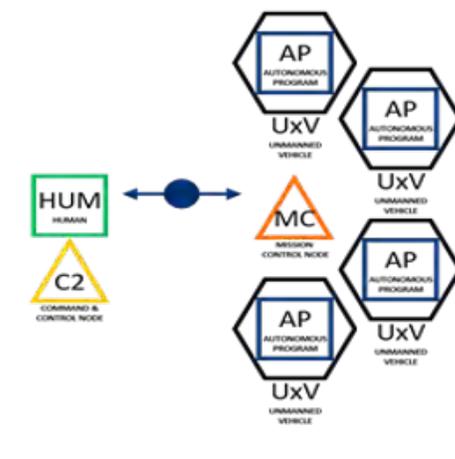


Figure 10: Teamed (Source: Lockheed Martin).

functional architecture for determining requirements.

Framework 3: Environmental

The Environmental framework addresses the use of autonomy under multiple environmental conditions, such as weather, location, threats, domains, C2, communications, etc. This framework helps identify the

capabilities, constraints, and limitations of specific capabilities across multiple implementations and sets the analysis boundary to successfully determine subsystem characteristics (see Figure 12). It aligns along the DoD’s mission, enemy, terrain, troops, time, and civilian considerations concept and intends to capture the spectrum of activities that have influence to the MUM-T

environment.

In concert with the ABC framework, environmental considerations can add complexity to the behaviors needed to achieve system needs. For example, a system traveling less than 2 km on maintained, rural roads in a logistics support region is much less complicated than traveling 50 km on off-road, mixed terrain at the forward edge of battle.

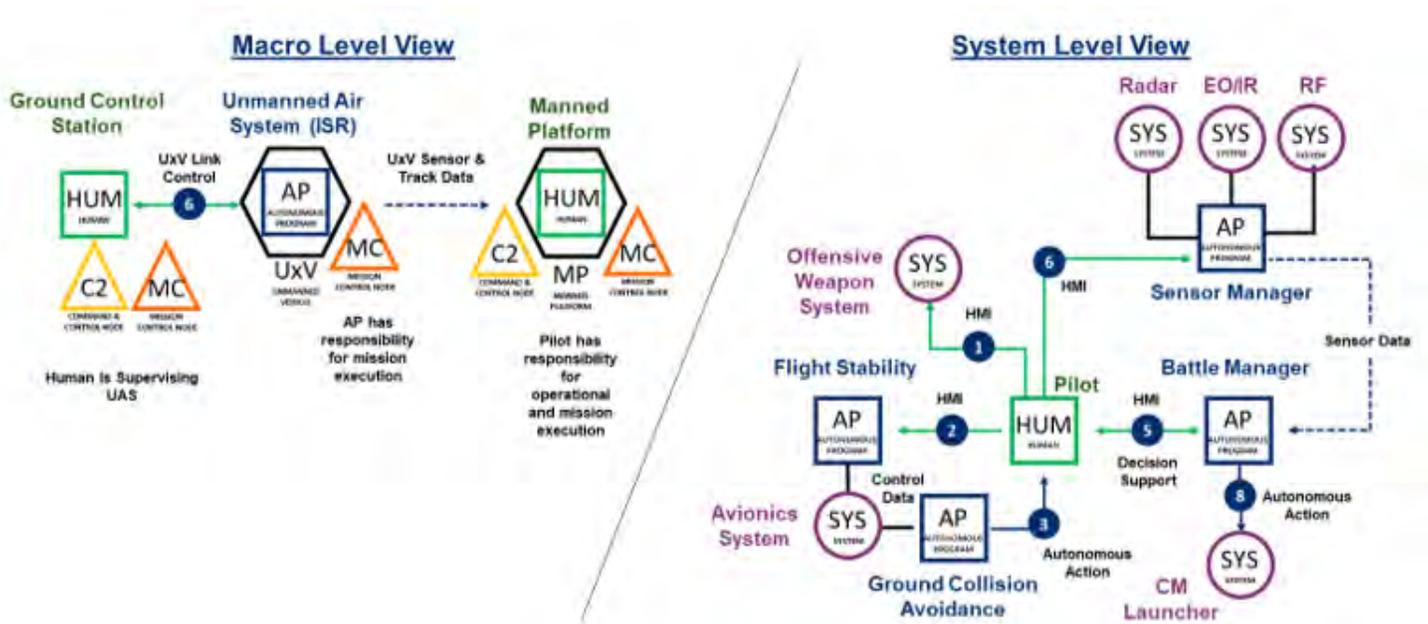


Figure 11: Macro vs. Systems Views (Source: Lockheed Martin).

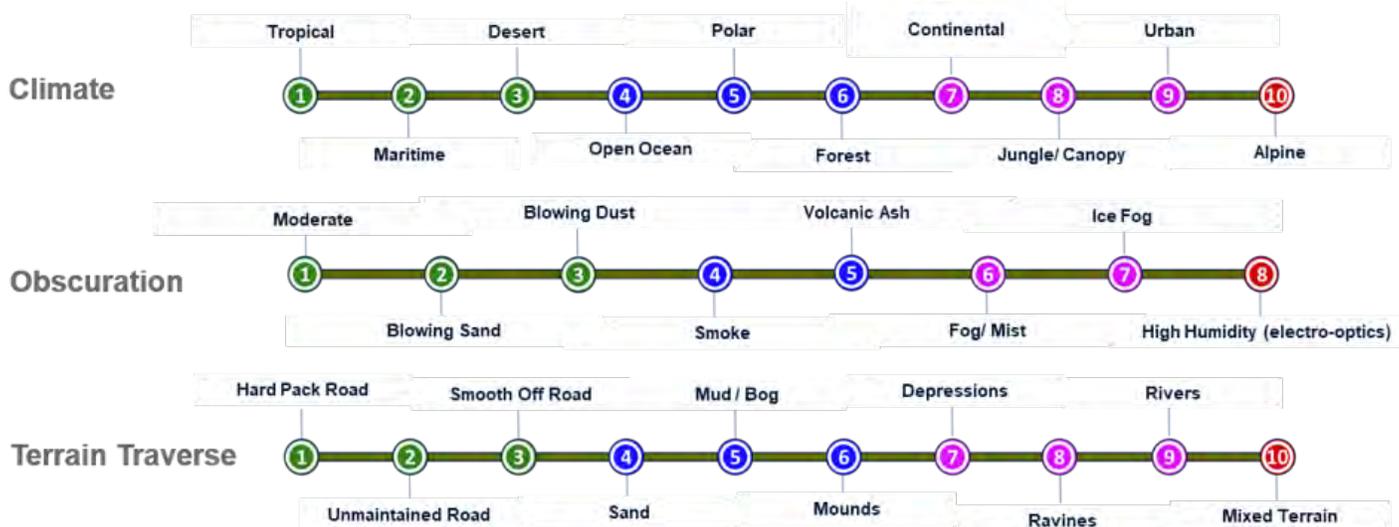


Figure 12: Environmental Framework Examples (Source: Lockheed Martin).

These environmental considerations are consistent with traditional systems analysis but help clarify substantial autonomous systems complexity when paired with the ABC and Operational frameworks.

Framework 4: Trust

The Trust framework allows tailoring for each autonomy design application, drives analysis of the unique stakeholder considerations for design, and supports data capture to identify trust trends and consensus between stakeholders. Five major stakeholder groups to consider with this framework emerged—Development, User, Cybersecurity, Acquisition, and Regulatory (see Figure 13). They are as follows:

1. Development:
 - Does the system do what it was designed to do (verification measures)?
2. User:
 - Will the system do what is expected (transparency/explanation/usability measures)?
3. Cybersecurity:
 - What are the unique cybersecurity risks with autonomy (system assurance and security)?
4. Acquisition:
 - Does the system do what was requested (validation measures)?
5. Regulatory:
 - Will the system become a menace (ethics/reliability/resilience measures)?

The Trust framework allows the autonomy space to be constrained by what is allowable, desirable, and usable by stakeholders. This framework analyzes trust from multiple perspectives to understand design, test, and implementation trade spaces and captures stakeholder expectations and assumptions. The Trust framework focuses on balancing regulatory, human factors, and performance considerations and ties existing trust considerations together, such as the recently-proposed DoD principles for AI of being responsible, equitable, traceable, reliable, and governable [10].

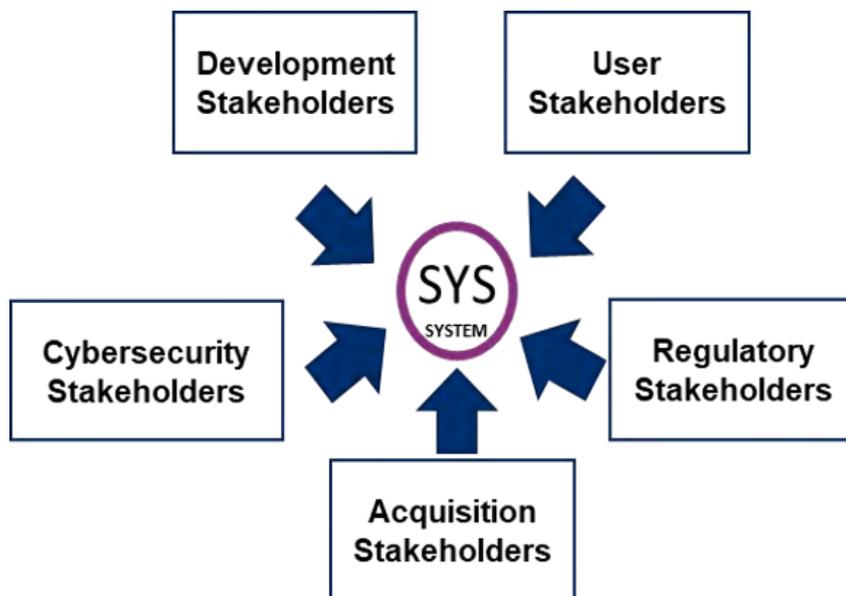


Figure 13: Trust Framework (Source: Lockheed Martin).

Considering all four frameworks together supports a holistic architecture for structuring future systems engineering of autonomous capabilities.

Analyzing Autonomy Summary

The four frameworks reviewed allow the analysis of autonomy to govern systems design beginning with the conceptualization of autonomy as an enabler for improved systems performance. The Trust and Environmental frameworks provide additional context for analyzing the design trade space created through applying different applications of the ABCs and Operational framework. Considering all four frameworks together supports a holistic architecture for structuring future systems engineering of autonomous capabilities.

The team developed these frameworks within the same timeframe as the chief scientist of the Office of the U.S. Air Force [1]. Comparing the two frameworks finds comfortable synergy and identifies that the major tenets do not conflict. The consistency between the frameworks of two independent efforts confirms the validity of the approach and identifies that tailoring for an organization's structure and culture is achievable without losing context in the complex and cross-discipline field of autonomous systems.

SYSTEMS ENGINEERING FOR AUTONOMY

Systems engineering for autonomy begins only when a solid conceptualization and analysis capability is established. Too often, engineering begins before a full understanding of the situation is established. Figure 14 identifies the systems engineering flow, beginning with understanding the customer needs in terms of performance, cost, etc. It moves through the systems architecture, after which time, the actual autonomous capabilities aligning into the enabling technologies are determined.

Ensuring this flow connection allows balancing TRLs and identifying discriminators and future investments. The flow back to customer requirements occurs when enabling technologies are out of sync with customer requirements—like schedule and cost—and ensures a balanced, aligned, and deliverable solution.

Executing this flow aligns the four autonomy frameworks, as captured in Figure 15. Starting with the customer requirements, we can bracket the design space by understanding the environment the system is expected to operate in against what the stakeholders will trust the system to do in that environment. Once that space is defined, the SoS analysis of the ABCs against the three dimensions of autonomy allows identifying the initial concepts of operations, systems architecture, and subsystem considerations. Capturing these relationships in the Operational framework allows easy systems and subsystems trades to align technology, reduce complexity, and support initiatives, such as Modular Open Systems Architecture.

A last benefit of this design flow is the ability to easily translate the Operational

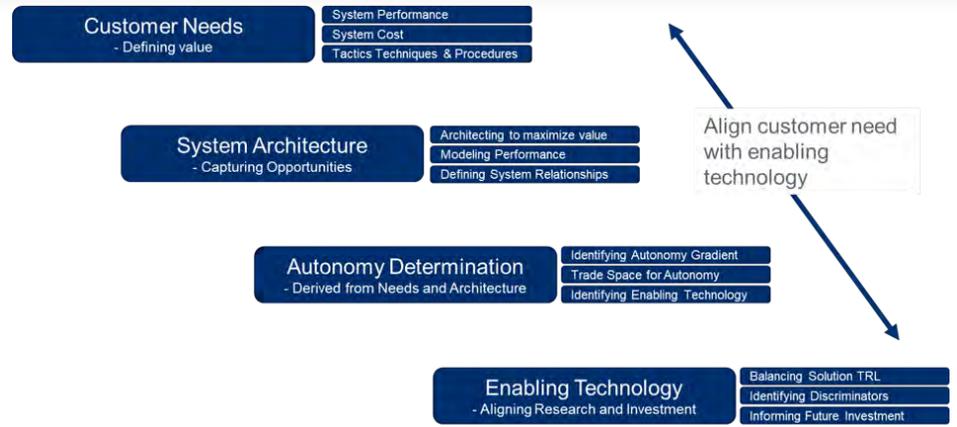


Figure 14: Aligning From Customer Need to Enabling Technology (Source: Lockheed Martin).

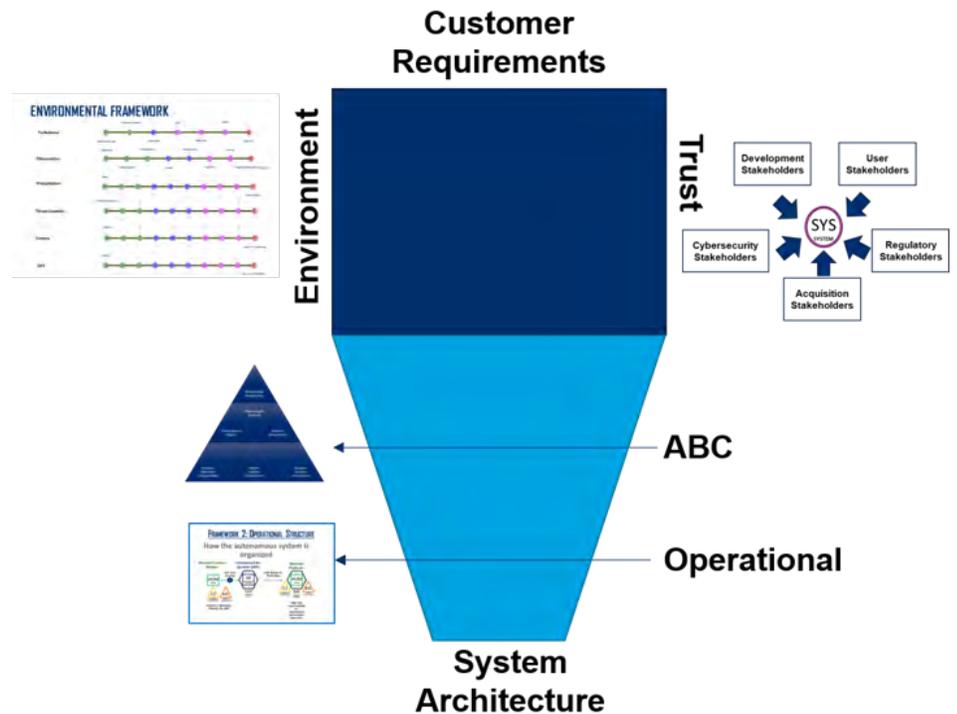


Figure 15: Systems Engineering of Autonomy Interrelationships (Source: Lockheed Martin).

configurations into mission-level modeling environments, such as Advanced Framework for Simulation, Integrations, and Modeling (AFSIM), and also into systems modeling languages, such as SYSML, UML, etc. (see Figure 16). By using the Operational framework and leveraging the ABCs levels as trade space brackets, experiments can be conducted where trades between

environment, trust, and architecture can be quantified and modeling of enabling technologies can validate design assumptions. Further, these frameworks foster proactive verification and validation (V&V) engagement in the modeling and simulation environment that informs subsequent detailed design, integration, and test.

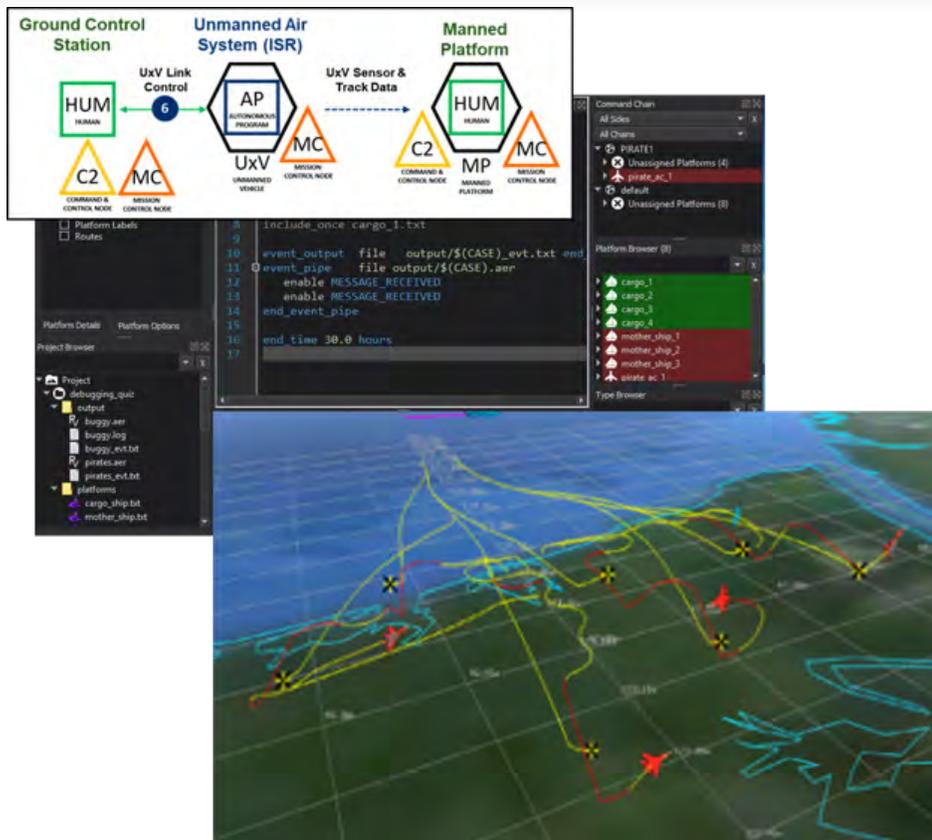


Figure 16: Operational Framework to AFSIM (Source: Lockheed Martin).

The frameworks and design process outlined here provides a rich set of tools for describing the autonomy of a system. Together, the artifacts produced could establish a potential ninth viewpoint to serve as an adjunct to the DoD Architecture Framework [11]. Current experiments with the design process have defined an autonomy viewpoint (AUV) consisting of the following:

- AUV-1: Intelligence, collaboration, and independence diagram. A three-dimensional view of autonomy configurations in cartesian space reflecting system intelligence, system collaboration, and independent operation (the three dimensions of autonomy). This view can be used to compare canonical examples as a way to measure complexity and relationships.

- AUV-2: Operational framework system view. A top-level operational configuration view showing interaction between platforms, autonomous program(s), humans, and C2/mission control functions.
- AUV-3: Authority allocation. A table listing allocation of task responsibilities between humans and autonomous systems.
- AUV-4: ABC diagram. The eight ABCs describing the level of behavior in each dimension for system mission requirements.
- AUV-5: Operational framework expanded view. A detailed operational configuration showing interaction among subcomponents of the platform, autonomous programs, humans, and C2/mission control functions.

- AUV-6: Environmental view. The N-dimensional environment characteristics that capture environmental context for the system's operations.
- AUV-7: Trust view. The five-dimensional trust characteristics that describe the level of trust required by each major stakeholder.

These potential autonomy views further demonstrate the applicability of these frameworks to standard systems architecture and systems engineering processes, templates, and tools.

The autonomy systems' architecture frameworks are designed to be an iterative approach where customer requirements, trust, and environment provide trade space dimensions and the autonomous behavior characteristics and operational framework provide design opportunities. Modeling of the architectures against the requirements, environment, and trust provide feedback for design improvements. Multiple iterations are expected to trade within these frameworks to best balance customer expectations, schedule, scope, and budget of systems designs.

CONCLUSIONS

A clear, concise, and applicable foundation for analysis of autonomous systems emerged, starting with conceptualizing autonomy as a gradient capability enabling the separation of human involvement from systems performance. Building from there, autonomous designs centered on a SoS approach and focused on system security ensured optimal designs. Lastly, collaborative trades can be achieved through the three dimensions of intelligence, independence, and collaboration. From this foundation, the following three analysis steps emerged:

Collaborative trades can be achieved through the three dimensions of intelligence, independence, and collaboration.

1. Applying the four Analysis frameworks for autonomy from the Trust and Environmental to the ABCs and then visualizing it with the Operational framework demonstrates a holistic and exhaustive structure to view the unique interactions and complexities of autonomous relationships.
2. Aligning the Conceptualization and Analysis frameworks to the systems engineering process, iterative designs with clarified trade spaces empower analysts to quickly translate design architectures into modeling and simulation programs to perform quantified analysis.
3. Leveraging the autonomous system conceptualization, analysis, and design capabilities strengthens the systems engineering toolkit to achieve revolutionary capabilities through stepping back and baselining, deconflicting, and understanding the complex environment of autonomous systems and applying a synthesized approach to designing autonomy into an SoS solution.

Lockheed Martin continues to mature this structure for conceptualizing, analyzing, and designing autonomy into a systems solution. Continued collaboration with the DoD, industry partners, and academic institutions

provides opportunities for spiral development of MUM-T solutions to create disruptive game changers for U.S. forces and their allies. ■

REFERENCES

- [1] Zacharias, G. L. "Autonomous Horizons – The Way Forward." Office of the U.S. Air Force Chief Scientist. *Air University Press*, p. 27, March 2019.
- [2] Defense Science Board. "Task Force Report: The Role of Autonomy in DoD Systems." Office of the Under Secretary of Defense for Acquisition, Technology and Logistics, Washington, DC, p. 21, July 2012.
- [3] National Institute of Standards and Technology. "Autonomy Levels for Unmanned Systems (ALFUS) Framework." *NIST Special Publication 1011-1-2.0*, Gaithersburg, MD, 2008.
- [4] Blash, E. "One Decade of the Data Fusion Information Group (DFIG) Model." U.S. Air Force Research Laboratory, Rome, NY, https://www.researchgate.net/publication/300791820_One_decade_of_the_Data_Fusion_Information_Group_DFIG_model, accessed 5 April 2020.
- [5] Wickens, C. "Situation Awareness: Review of Mica Endsley's 1995 Articles on Situation Awareness Theory and Measurement." *Human Factors*, vol. 50, no. 3, pp. 397–403, 2008.
- [6] Franke, J., et al. "Collaborative Autonomy for Manned/Unmanned Teams." Paper presented at the American Helicopter Society 61st Annual Forum, Grapevine, TX, June 2005.
- [7] Franke J., B. Satterfield, and M. Czajkowski. "Self-Awareness for Vehicle Safety and Mission Success." Unmanned Vehicle Systems Technology Conference, Brussels, Belgium, December 2002.
- [8] Hogue, T. "Community-Based Collaborations – Wellness Multiplied." Oregon Center for Community Leadership, Corvallis, OR, 1994.
- [9] Nachi Robotic Systems Corporation. <https://www.nachirobotics.com/collaborative-robots/>, accessed 8 April 2020.
- [10] Defense Innovation Board. "AI Principles: Recommendations on the Ethical Use of Artificial Intelligence by the Department of Defense." Washington, DC, https://media.defense.gov/2019/Oct/31/2002204458/-1/-1/0/DIB_AI_PRINCIPLES_PRIMARY_DOCUMENT.PDF, accessed 3 April 2020.
- [11] U.S. DoD. "DoD Architecture Framework Version 2.0." https://dodcio.defense.gov/Portals/0/Documents/DODAF/DoDAF_v2-02_web.pdf, accessed 6 April 2020.

BIOGRAPHIES

MICHAEL WOUDEBERG is a senior staff operations research analyst for Lockheed Martin and an applied research lead for autonomy, AI, and ML. Prior to joining Lockheed, he was a program manager for cyber, electronic warfare, and directed-energy R&D portfolios at Raytheon and advanced avionics at Honeywell Aerospace. He is a veteran of the U.S. Army, where he served as an Airborne and Ranger qualified Field Artillery Officer. Mr. Woudeberg holds an M.S. in systems engineering from Johns Hopkins University and a B.S. in information systems from Michigan Technological University.

GEORGE "MARK" WALTENSBERGER is the chief analyst for Lockheed Martin's Missiles and Fire Control Operations Analysis department in Orlando, FL. He retired from the U.S. Air Force in 2000 as a scientific analyst and member of the DoD Acquisition Corps. He currently leads a cross-corporation integrated product team on

MUM-T and represents Lockheed Martin as a member of the International Organization for Standardization Joint Technical Committee on AI. Dr. Waltensperger holds a B.S. in biology, an M.S. in command, control, and communications from the Naval Postgraduate School, and a Ph.D. in operations research from the University of Oklahoma.

TROY SHIDELER is a senior operations analyst for Lockheed Martin, where he leads cross-functional analytical studies on future technology and employment concepts (MUM-T and multidomain operations). Prior to joining Lockheed Martin, he supported a variety of DoD customers focusing on employing future technology at Systems Planning and Analysis. He is a former Navy Surface Warfare Officer and instructor of antisubmarine warfare tactics. Mr. Shideler holds a B.S. in political science from the U.S. Naval Academy and an M.A. in national security studies from Georgetown University.

JERRY FRANKE is a Lockheed Martin fellow, acting chief technology officer at the Advanced Technology Laboratories, and chief scientist for Lockheed Martin's Intelligent Systems Works. He has 22 years of experience providing technical vision and project leadership related to technologies for command and control and autonomous operation of unmanned vehicles. He has two patents awarded in autonomous mission management and contingency management and authored more than 20 publications on unmanned collaborative autonomy, human-system interaction, and MUM-T. Mr. Franke holds a B.S. and M.S. in computer science (specialization: AI) from Florida State University.

(Source: U.S. Marine Corps)

Daunting Challenge of

DRONE DEFENSE

By Kyle Carnahan and Darrel Zeh

INTRODUCTION

The proliferation of an unmanned aircraft/aerial system (UAS) spreads beyond military and remote control (R/C) hobbyist markets in the last decade, spearheaded by the Chinese company DJI beginning with the release of the DJI Phantom 1 in early 2013 [1]. As the capability of these aircraft has increased to meet the needs of new users, these platforms have been repurposed in unintended ways.

Nefarious use of drones raises concerns for several key reasons—drones' ability to circumvent the billions of dollars' worth of physical security barriers installed around the world; their ability to carry malicious payloads, spy devices, or just innate mass; and their ability to allow the operator to deliver this payload remotely and pseudo-anonymously. Even more concerning is that this capability can be obtained instantly with commercial-off-the-shelf technology

under \$1,000 (e.g., a DJI Mavic Pro rigged with an improvised bomb in Turkey [2]). These systems have been designed to eliminate the learning curve, enabling nearly anybody to fly them with little-to-no previous experience. This article will discuss the means by which security entities are attempting to protect assets against malicious drones.

NOTE: For the purposes of this article, the terms drones and unmanned aircraft are considered interchangeable.



The focus of this article is on small unmanned aircraft, regardless of the level of autonomy involved, that are becoming ubiquitous in recreational, commercial, and military zones. These aircraft can span consumer products, home-built R/C aircraft, and small military systems, such as those developed by AeroVironment (United States) and Aeronautics (Israel). The term UAS will be used to encompass not only the drone but additional hardware, including the ground control station, software, payloads, and supporting equipment.

CONCERNS

A major domestic concern is the intentional or careless interference with general and commercial aviation. For instance, the shutdown that occurred at Gatwick Airport in December 2018, where a small UAS flying over airport property suspended all flight operations for 33 hours, resulted in an economic cost of \$64.5M [3]. The drone disturbance caused the airport to be steeped in chaos, confusion, and helplessness but was a relatively small threat to life and property; one could argue the stress caused by interrupting travel of thousands of people over the holidays was far more devastating than the physical damage the drone might have done except in an absolute worst-case scenario.

Other drone concerns include potential terroristic acts from protesters. In 2015, a protestor against the Japanese government's nuclear energy policy flew a drone carrying radioactive sand onto the roof of the Japanese prime minister's office. The drone was not discovered until 13 days after it was initially flown onto the roof. The radiation levels of the cesium source were low enough to not be harmful; however, the clandestine nature of the operation is disconcerting [4].

Although there are no successful cases of domestic terrorism with drones, one can wonder if a case such as the Austin, TX, serial bombings in 2018 would have led to more destruction if the suspect used drones rather than trip wires and FedEx to attack his targets [5]. The destructive potential for terrorist or militia use of small, commercially-available drones has been demonstrated throughout the world, from Syria [6] to Ukraine [7] and Venezuela [8] to the Philippines [9], and has been well documented in other press reports on the topic [10].

In addition to the threat of modified consumer drones for nefarious purposes, smaller UAS's developed by defense industries are also rapidly increasing in capability and proliferation at levels of both peer competitors (the People's Liberation Army reportedly recently acquired the CH-901 armed UAS [11]) and rogue regimes and their proxies (such as attacks on Saudi and Emirati civilian facilities by Iran and Ansar Allah [12]). For the foreseeable future, security forces across the globe should plan, in advance, on how to respond to a UAS threat, whether they are protecting assets on a battlefield or a civilian center.

FRIEND OR FOE?

One of the most significant issues with defense against a UAS is determining intent. This is, in part, due to the anonymity of the operator. Security forces responding to a situation like that at Gatwick Airport have little awareness whether the perpetrators are kids pulling a prank, a hobbyist hoping to upload exciting close-up aerial videos of commercial airliners during takeoff and landing, or someone nefarious, like the Austin serial bomber or an internet extremist trying to wreak havoc with a live audience [13]. Security forces must weigh the risks of overreaction vs.

Security forces must weigh the risks of overreaction vs. underreaction to a drone incident, as both can lead to loss of life or property.

underreaction to a drone incident, as both can lead to loss of life or property.

Determining the intent of a UAS is challenging to do proactively. In the United States, the Federal Aviation Administration's (FAA's) response to the issue of ambiguity is focused around mandating remote identification and development of unmanned traffic management standards. This would help address the reckless and careless operators using UAS's as long as they have properly configured the UAS to those security standards, a "papers, please" approach to interrogating drones and ground stations flying in public zones. (Note: there has been significant pushback against the FAA's planned implementation of remote identification from industry and hobbyist groups, but this article will not address those issues.)

These efforts would allow security forces to detect, monitor, and, if needed, interdict some UAS's interfering with public safety. More importantly, security forces will be quicker to respond to UAS's flying without proper remote identification certifications [14]. With the careless and reckless operators thus handled, all other UAS's can be treated as nefarious, akin to driving a car with no license plate, and therefore cue security forces to react more quickly with additional means of response.

Security operators are typically left with analyzing the behavior of a drone to determine its intent, such as evaluating its track history and current trajectory. Tracking solutions typically involve radar systems that require continuous operation and constant monitoring. The operator would have to interrogate whether a given track was indeed a UAS and then analyze the target trajectory to make an informed decision as to whether it was hostile. This capability does provide situational awareness of threats in the area, even if the threat UAS is not interdicted.

FALSE ALARM FATIGUE

Even with all means of response authorized, defense against drones is far from an easy task. Security forces responsible for detecting and responding to malicious drones suffer the same issues of fatigue and vigilance and boredom and paranoia as all sentries. A security officer could go weeks, months, years, or even a career without encountering a malicious drone; meanwhile, the security officer may be bombarded with false or nuisance alarms in that same time frame. Security organizations are left choosing between highly-sensitive (and expensive) drone defense systems that can cause hundreds of false alarms per week vs. less-sensitive systems that may miss the very threats they are supposed to detect.

The most significant impact that can be made to current systems is including operator-assisting algorithms to aid the operator in interpreting the system data presented to them. Significant investment into automated sensor processing is necessary to accurately parse the data to minimize the false alarms or nuisance alarms presented to the operator. Further investment into human systems integration can focus on minimizing operator workload by efficiently presenting the data to the

operator. For example, radar displays can be overwhelmed by nuisance alarms, especially when small UAS's can have similar radar cross-section values as large birds, to an extent that obfuscates the presence of a UAS on the radar display. While difficult for an operator to sift through in the required time, automated intelligent processing to neglect these nuisance alarms would alleviate this issue. All other sensors have similar nuisance alarms or background noise issues.

Optic sensors can have nuisance alarms from birds and background noise from clouds or terrain, while electronic detection sensors can be cluttered by extraneous signals or must overcome a high ambient noise floor, and acoustic systems can easily be saturated by background noise. Advancements to shift away from operator dependence and put the burden on automated processing to detect low signal-to-noise ratio signals and reduce the number of notifications from nuisance alarms will simplify the problem to something the

Significant investment into automated sensor processing is necessary to minimize the false alarms or nuisance alarms presented to the operator.

operator can easily manage.

NO SILVER BULLET

Once detected and assessed to be a threat, security forces must then employ a defeat mechanism similar to the one shown in Figure 1. The most prevalent is electronic interference/attack (barrage jamming) of the UAS command and control signals to disrupt the operator control and initiate a fail-safe mode. The emission of radio frequency (RF) energy by the counter



Figure 1: U.S. Department of Defense (DoD) Personnel Training With the Flex Force Dronebuster (Source: Joint Base McGuire-Dix-Lakehurst [15]).

(C)-UAS system raises the RF noise floor in the surrounding area, causing the UAS command signals to be lost in the noise. This results in the UAS entering a hover/loiter, landing, returning to its takeoff location, or continuing its flight path with a significant capability handicap, much like when a UAS flies too far away from the ground station transmitter. In some cases, the Global Positioning System (GPS) link may be jammed and cause the aircraft to enter an attitude hold in which it maintains current trajectory, attempts to use less-reliable navigation sensors, or hovers in place, depending on the selected fail-safe.

A more precise mitigation technique can be used to avoid electronic fratricide, which is narrowband jamming. This technique relies on jamming the precise frequencies on which the command and control signal will hop. To achieve this, the C-UAS system needs to have a threat library, which includes information on these hopping signals.

There are issues relying on a threat library for UAS detection and interdiction. Constant reverse engineering on datalinks is required to maintain a current library, which involves cost and effort. The evolution of the DJI datalink is a paradigm of why threat libraries are difficult to maintain. The early DJI Phantom models relied on Lightbridge technology, which was a hybrid between hardware and software for the transmission system. However, newer models utilize OcuSync, which is strictly software-defined radio (SDR) based [16]. OcuSync 2.0 firmware is upgradable through patches and can automatically switch between multiple bands for communication (2.4 GHz or 5.8 GHz industrial, scientific, and medical bands). The agility at which newer SDR-based systems can alter their frequency band and hopping pattern will cause difficulty in keeping a consistent library. The constant evolution and development

A more effective and surgical means of counter-drone defense is to try to hijack the drone by hacking its control system.

to make more robust datalinks for UAS by the commercial industry will require constant efforts to update the threat libraries by the counter-drone industry.

Barrage jamming and narrowband C-UAS systems can be a promising mitigation tool against UAS flying by command and control links. But what happens when RF links are not present? UAS researchers are making flight operations more autonomous, less reliant on active datalinks, and more reliant on GPS-based or vision-based navigation. Additional efforts have explored the utilizing long-term evolution networks as the backbone for the communications link [17]. In both cases, jamming these frequencies will have either no effect or effects with significant, unintended consequences of electronic fratricide (i.e., blocking cellular, Wi-Fi, and GPS service) to the nearby population. The FAA has testified to Congress their hesitation for many security forces to be given the ability to jam the command and control and GPS signals of a drone, as the solution (jamming) is worse than the problem (presence of an unauthorized drone) in many scenarios [18].

HACKIN' AIN'T EASY

A more effective and surgical means of counter-drone defense is to try to hijack the drone by hacking its control system, thereby allowing the security responder

to land the drone in a safe area, with minimal risk of disrupting bystanders. However, this methodology has legal issues. The Fourth Amendment of the U.S. Constitution; U.S. Code: Title 18 Electronic Communications Interception; and U.S. Code: Title 50 Collections, Stipulations, and Limitations of the Preventing Emerging Threats Act of 2018 suggest this methodology in U.S. jurisdictions is applicable only after other methodologies fail [19]. There are also technical hurdles to overcome. Just as the efficacy of a flu vaccine is dependent on the strain of flu, a cyber-based countermeasure system is highly dependent on the strain (software and firmware version) of the drone and whether counter-drone engineers have amply developed an effective attack for that drone. Rapid improvements toward more resilient command and control protocols made by drone manufacturers compound this problem.

DJI, the leading UAS manufacturer that dominates ~70% of the commercial UAS market [20], has developed its own cyber-based drone defense system, Aeroscope. This system exploits back doors in the communications and flight control system to allow security officials to hijack nearby DJI drones. Future collaboration between security and regulatory officials and drone manufacturers can provide more thorough portfolios of hackable drones, although it is unlikely counter-drone systems will be loaded with hacks to attack every potential threat, and particularly drone-savvy individuals are able to build and program custom UAS that have no communication systems to hack at all.

SHOOT TO KILL?

When electronic interference or hacking the command protocol fail to disrupt an unauthorized drone, security forces then require a "hard kill," such as nets,

bullets, missiles (including drone-to-drone intercepts akin to the one shown in Figure 2), lasers, and high-power microwave bursts (shown in Figure 3). Hard-kill systems, if they hit the target, are less discriminating than the barrage-jamming and cyber techniques mentioned previously. However, they come with other issues, such as collateral damage, environmental interference, and range to target, that can degrade or negate their suitability. Hard-kill defenses have their own safety risks that must be mitigated and do not guarantee an optimistic outcome. Those safety risks—hitting something other than the target or bringing down a drone in an uncontrolled, destructive crash—have restricted fielding of hard-kill systems primarily to conflict zones [21].

YOU GET WHAT YOU PAY FOR

The best approach is to use a combination of sensors—radars, cameras, and signals intelligence devices—to increase the odds of detecting and defeating a UAS. Using a system-of-systems approach can leverage capabilities inherent in each modality while mitigating weaknesses. Sensors can correlate information to weed out false alarms and maximize probability of an effective defense. Similarly, a layered defense approach can use a combination of defeat options—jammers and interceptors—to improve probability of UAS interdiction. A perimeter defense solution can be employed with a network of sensors

and efforts to maximize the coverage of the protected area. An example of a system of systems is as follows: an electronic support node can be used to detect a nearby threat UAS emitting a signal early. A radar system can work with an optic for slew to cue to achieve positive threat identification, then an electronic attack system can attempt to jam to the UAS datalinks. If this proves unsuccessful, then a kinetic solution can be used to interdict the aircraft. The overlap of sensors ensures that the limitations of any given sensor are mitigated by the capabilities of the others.

The difficulties with a system of systems approach are two-fold. First, the monetary cost of fielding radars and cameras and net guns and jammers will strain budgets. Second, security officers armed with an arsenal of sensors and effectors may be overwhelmed with data and engagement decisions. However, decisions related to selecting engagement options, threat assessment, and potential collateral damage must be made in less than a minute.

Being able to successfully detect and defeat a worst-case drone threat will necessitate that much of the decision making in the engagement be automated via the C-UAS system. This ultimately means risks of overreaction or underreaction to drone incidents are left to system developers and parameters set by each security unit rather than a security officer.

WHAT'S THE SOLUTION?

Each scenario or operation will have a different optimal C-UAS solution. As such, numerous C-UAS systems have been developed based on specific missions and operational needs from DoD commanders over the last several years. Depending on the mission or



Figure 2: Raytheon Coyote Multipurpose, Disposable UAS (Source: 433rd Airlift Wing, USAF [22]).



Figure 3: Raytheon Phaser High-Powered Microwave (Source: Raytheon [23]).

protected area, the appropriate C-UAS system will have an optimal size, weight, and power (SWaP). Systems can be segregated into dismounted, mobile, and fixed-site configurations.

Dismounted systems might include electronic detection and attack capabilities for point defense but must be light enough to be carried in a backpack for long periods. Electronic detection and attack systems offer the only low SWaP solutions feasible. Optic systems could meet SWaP considerations but have not yet been proven useful in dismounted operations; identification and targeting issues would only be compounded by a moving operator. Similarly, acoustic systems (consisting of a few microphones) could be worn by an operator. Although some dismounted solutions for acoustic-based gunshot detection have been developed, there has not been adequate exploration of this capability for a C-UAS to determine operational feasibility.

Mobile systems, such as the one shown in Figure 4, must be small enough to mount onto a vehicle, rugged enough to sustain shock and vibration loads, and able to operate off of generator power. However, there is more flexibility in the types of systems that can be applied toward the problem compared to dismounted systems. Electronic detection systems can be present and used for early warning systems. Electronic attack systems can radiate more power because they can operate off generator power instead of batteries. Smaller radar systems can be utilized on mobile vehicles [24]. Depending on the rules of engagement, visual identification may be required before engagement. As a result, optics should be integrated with any radar systems on a mobile solution. Acoustic systems still have not made much headway when it comes to mobile operations, as the noise floor caused by generator noise or



Figure 4: L-MADIS Light Marine Air Defense Integrated System (Source: PM GBAD, USMC [25]).

vehicle movement will mask the target signal.

Lastly, kinetic defeat solutions can be present on mobile platforms. Interceptors have become more common, both in the form of multirotor UAS and tube-launched systems, such as AeroVironment's Switchblade and Raytheon's Coyote, which use onboard sensors for guidance to the threat UAS. Laser systems have also made recent advancements to find their way into the battlespace. There are deconfliction

Laser systems have also made recent advancements to find their way into the battlespace.

issues using high-energy lasers (HELs) in the battlespace; however, systems like MEHEL and CLaWS are overcoming these and provide a mobile HEL solution [26, 27].

All the same sensors and effectors applicable to mobile operations can also be employed for fixed sites, with the added benefit of extra space, infrastructure for installation, and use of shore power, thus eliminating many SWaP concerns. Detection nodes can be dispersed around the perimeter of the defended area and placed so the electronic or acoustic detection nodes are isolated from interference. Effectors can be dispersed or centralized, depending on the defended area, and lines of fire can be cleared during the planning process. Command and control systems are critical because networked sensors and effectors need to communicate with each other in a timely manner to enable the kill chain and provide a common operational picture.

In December 2019, the Undersecretary of Defense for Acquisition and Sustainment designated a Joint C-UAS Office and selected the Army as the lead Executive Agent in charge of assessing currently-fielded C-UAS programs for the DoD [28]. Assessments of several C-UAS systems are ongoing to determine the best-of-breed systems for use in various operational conditions. The Joint Office aims to leverage the efforts and expertise of each Service to improve current C-UAS capabilities. However, while the DoD is becoming more organized to develop, test, and field C-UAS systems, the rest of the federal government and state and local entities will have a far more piecemeal approach. One can easily imagine police departments in neighboring jurisdictions having completely different C-UAS equipment, training, and policies.

CONCLUSIONS

Protecting assets or personnel from nefarious UAS is an ever-increasing problem due to capability improvements and unhindered proliferation. Whether the drone operator is a terrorist, foreign intelligence agent, or a kid innocently flying a toy, security forces must be prepared to identify and proportionally respond to the threat. There is no silver bullet for the drone defense problem set, so continued investment, testing, and improvements to counter-drone technologies are necessary. The complexities and trade-offs of this problem must be carefully navigated to effectively manage policy, technical challenges, and funding restrictions to ensure adequate defense capabilities. ■

REFERENCES

- [1] DrDrone.ca. "Timeline of DJI Drones: From the Phantom 1 to the Mavic Air." <https://www.drdrone.ca/blogs/drone-news-drone-help-blog/timeline-of-dji-drones>, accessed 1 April 2020.
- [2] Acar, C. "3 Types of Pkk 'Armed' Drones Downed by Security Forces in Turkey's SE Areas." <https://twitter.com/Acemal71/status/934788399441088512>, accessed 1 April 2020.
- [3] Calder, S. "Gatwick Drone Disruption Over Christmas Cost £50m." <https://www.independent.co.uk/travel/news-and-advice/gatwick-drone-airport-cost-easyjet-runway-security-passenger-cancellation-a8739841.html>, accessed 1 April 2020.
- [4] Murai, S. "Man Who Landed Drone on Roof of Japanese Prime Minister's Office Gets Suspended Sentence." <https://www.japantimes.com.jp/news/2016/02/16/national/crime-legal/man-landed-drone-roof-japanese-prime-ministers-office-gets-suspended-sentence/#.XsLVu3d-FymQ>, accessed 1 April 2020.
- [5] Weber, P. J., and W. J. Weissert. "Fear Mounting in Austin as Serial Bomber Uses Tripwire Along a Street." <https://www.denverpost.com/2018/03/19/austin-bombing-spree/>, accessed 1 April 2020.
- [6] PressTV. "Russian Military Eliminates Militants Behind Syria Air Base Attack: Video." <http://french.presstv.com/Detail/2018/01/12/548707/Russian-military-eliminates-militants-behind-Syria-air-base-attack>, accessed 1 April 2020.
- [7] Mizokami, K. "Another Ukrainian Ammo Dump Goes Up in Massive Explosion." <https://www.popularmechanics.com/military/weapons/news/a28412/ukrainian-ammo-dump-explosion/>, accessed 1 April 2020.
- [8] Koettl, C., and B. Marcolini. "A Closer Look at the Drone Attack on Maduro in Venezuela." <https://www.nytimes.com/2018/08/10/world/americas/venezuela-video-analysis.html>, accessed 1 April 2020.
- [9] Tima, R. "Marawi, The Drone War." <https://www.gmanetwork.com/news/news/specialreports/632793/marawi-the-drone-war/story/>, accessed 1 April 2020.
- [10] Rassler, D. "The Islamic State and Drones: Supply Scale, and Future Threats." <https://ctc.usma.edu/wp-content/uploads/2018/07/Islamic-State-and-Drones-Release-Version.pdf>, accessed 1 April 2020.
- [11] DefenseWorld.net. "China to Buy 2 Types of Loitering Munitions." https://www.defenseworld.net/news/26507/China_to_Buy_2_Types_of_Loitering_Munitions#.XsLbTndFymQ, accessed 1 April 2020.
- [12] Hubbard, B., P. Karasz, and S. Reed. "Two Major Saudi Oil Installations Hit by Drone Strike, and U.S. Blames Iran." <https://www.nytimes.com/2019/09/14/world/middleeast/saudi-arabia-refineries-drone-attack.html>, accessed 1 April 2020.
- [13] Boot, M. "Why Social Media and Terrorism Make a Perfect Fit." <https://www.washingtonpost.com/opinions/2019/03/16/why-social-media-terrorism-make-perfect-fit/>, accessed 1 April 2020.
- [14] Stubblefield, A. "Drone Security: Enhancing Innovation and Mitigating Supply Chain Risks." <https://www.transportation.gov/testimony/drone-security-enhancing-innovation-and-mitigating-supply-chain-risks>, accessed 1 April 2020.
- [15] Carter, J. "Joint Base MDL Implements New Dronebuster Technology to Deter Evolving." <https://www.jbmdl.jb.mil/News/Article-Display/Article/2076897/joint-base-mdl-implements-new-dronebuster-technology-to-deter-evolving-threat/>, accessed 27 March 2020.
- [16] djibestdrones.com. "dJI OcuSync 2.0: What You Need to Know About This FPV Transmission System." <http://djibestdrones.com/dji-ocusync-2-0/>, accessed 1 April 2020.
- [17] Kannan, K. "Nokia Showcases LTE Technology for the Use of Drones in Smart Cities." <https://www.nokia.com/about-us/news/releases/2016/02/04/nokia-showcases-lte-technology-for-the-use-of-drones-in-smart-cities/>, accessed 1 April 2020.
- [18] National Cable Satellite Corporation. "Federal Aviation Administration Oversight Hearing." <https://www.c-span.org/video/?463129-1/federal-aviation-administration-oversight-hearing>, accessed 1 April 2020.
- [19] Rupprecht Law P.A. "7 Big Problems with Counter Drone Technology." <https://jrupprechtlaw.com/drone-jammer-gun-defender-legal-problems/>, accessed 1 April 2020.
- [20] Business Insider Intelligence. "Commercial Unmanned Aerial Vehicle (UAV) Market Analysis - Industry Trends, Forecasts and Companies." <https://www.businessinsider.com/commercial-uav-market-analysis>, accessed 1 April 2020.
- [21] Pappalardo, J. "The Air Force Is Deploying Its First Drone-Killing Microwave Weapon." <https://www.popularmechanics.com/military/weapons/a29198555/phaser-weapon-air-force/>, accessed 1 April 2020.
- [22] Vergun, D. "Proliferation of Drones Posing Risk for U.S. Military, Expert Says." <https://www.433aw.afrc.af.mil/News/Article-Display/Article/1612325/proliferation-of-drones-posing-risk-for-us-military-expert-says/>, accessed 27 March 2020.
- [23] Raytheon Technologies. "Phaser High-Power Microwave System." <https://www.raytheonmissilesanddefense.com/capabilities/products/phaser-high-power-microwave>, accessed 25 March 2020.
- [24] Mizokami, K. "This Is the ATV-Mounted Jammer That Took Down an Iranian Drone." <https://www.popularmechanics.com/military/weapons/a28471436/lm-dis-iranian-drone/>, accessed 1 April 2020.
- [25] Swanbeck, D. "Program Executive Officer Land Systems." <https://www.marcorssyscom.marines.mil/PEOs/-PEO-LS/PM-GBAD/>, accessed 27 March 2020.
- [26] U.S. Army Space and Missile Defense Command. "Mobile Experimental High Energy Laser (MEHEL)." https://www.smdc.army.mil/Portals/38/Documents/Publications/Fact_Sheets/MEHEL.pdf, accessed 1 April 2020.
- [27] Mizokami, K. "U.S. Marines Have Started Testing Its Drone-Killing Laser Weapon." <https://www.popularmechanics.com/military/research/a28120435/laser-weapon-claws/>, accessed 1 April 2020.
- [28] Tadjdeh, Y. "Defense Department to Stand Up New Counter-Drone Office." <https://www.nationaldefensemagazine.org/articles/2020/1/14/just-in-defense-department-to-stand-up-counter-drone-office>, accessed 1 April 2020.

BIOGRAPHIES

KYLE CARNAHAN is a research engineer with the Aerospace, Transportation, and Advanced Systems Laboratory at Georgia Tech Research Institute (GTRI), where he focuses on C-UAS test and evaluation. His research interests include C-UAS policy, UAS vulnerability and lethality analysis, and C-UAS system-of-systems design. Mr. Carnahan holds a B.S. and M.S. in aerospace engineering from Georgia Institute of Technology.

DARREL ZEH is a research engineer with the Advanced Concepts Laboratory at GTRI and a student at Georgia Tech's Sam Nunn School of International Affairs. He previously worked for the DoD assessing security issues related to UAS. Mr. Zeh holds a B.S. in aerospace engineering from the University of Florida.

(Photo Source: 123rf.com)

CHARACTERIZATION OF

COMPOSITE

SPACED ARMOR PERFORMANCE

By Sierra I. Semel, Daniel V. Camp, John T. Hailer,
and Delaney M. Jordan

SUMMARY

Composite spaced armor is an unconventional armor system capable of stopping armor-piercing (AP) projectiles at lower areal density than possible with traditional metallic and ceramic armor systems, which makes it especially attractive for weight-sensitive applications. Prior testing of this armor system at normal obliquity has shown that it has great potential to reduce weight in aircraft systems while providing improved ballistics protection. The anisotropic nature of this composite spaced armor further differentiates it from traditional metallic and ceramic systems because its directionally-dependent mechanical properties cause performance to vary with obliquity. Ballistics testing evaluated normal and oblique angle impacts to quantify performance at a range of shot lines. Results indicate that for a limited range of oblique shot lines, the tumble of the bullet is reduced, resulting in degraded

performance of the armor. However, this can be mitigated through system-level design and careful integration or eliminated with technology solutions.

INTRODUCTION

In order to stop AP rounds, traditional armor systems require a hardened strike face, often made of ceramic material, which fractures the penetrator of the round. Including this hardened strike face results in a significant weight gain, making this type of armor impractical for weight-sensitive aviation platforms. A new composite spaced armor system, consisting entirely of ultra-high molecular weight polyethylene (UHMWPE), has been developed to defeat AP rounds at a much lower areal density than traditional systems.

Composite spaced armor is an unconventional armor system that uses two armor panels separated by an air gap. The first panel imparts an asymmetrical load onto the bullet, causing it to tumble. This rotation increases the presented area of the projectile and negates the advantage of the AP penetrator, allowing it to be stopped by the second panel. Spaced armor systems consist of three typical components—a striker, an air gap, and a catcher. In the case of composite spaced armor, the striker is an armor panel constructed out of UHMWPE using a proprietary manufacturing process. The trade name for this armor

In order to stop AP rounds, traditional armor systems require a hardened strike face, which fractures the penetrator of the round.

material is “turning block,” and it is manufactured by Hardwire LLC [1].

The bullet first passes through this striker panel, and the turning block imparts an asymmetrical load onto the round, causing it to tumble (Figure 1). This round then passes through an air gap, nominally ranging from 4 to 10 inches. A larger air gap can defeat faster rounds but is limited by the space allocated to the armor system. The tumble of the round increases the presented area of the projectile and turns the hardened penetrator of the AP round away from the path of the shot line. This rotation allows the catcher, also made of UHMWPE, to attenuate the energy and stop the round.

Composite spaced armor is considered multifunctional. In addition to its primary function of protecting critical systems and occupants, the panels used have some load-bearing capabilities.

This is particularly attractive in aerospace applications, where weight is a premium resource. Theoretically, the catcher in this armor system could replace the core material in a sandwich-composite aircraft floor. The dual purpose of this system as an armor and load-bearing structure would allow the reduction of parasitic weight. Prior investigations of multifunctional spaced armor are documented by the Highly Durable Floor/Armor for Rotorcraft (HDFAR) Program that concluded in 2019 [3].

PROBLEM/APPROACH

Traditional AP armor systems are metallic and/or ceramic; they exhibit a positive relationship between obliquity and performance. The more oblique the shot line, the more material is in the path of the bullet, and more energy can be attenuated. Such armor systems are isotropic and homogeneous—the mechanical properties are consistent throughout the material and behave the same in every direction. Composite armor systems, however, are anisotropic and nonhomogeneous—they exhibit different mechanical properties in different directions, and the properties change throughout the thickness of the material. This creates the potential that the armor system will behave differently at oblique shot lines compared to traditional metallic and ceramic armor systems, and there will not be a purely positive relationship between obliquity and performance.

In previous, unpublished testing of the subject composite spaced armor system, conducted internally by the Army, such a phenomenon was observed. At certain obliquities, the projectile tumbled consistently nose-up, while at other obliquities, the projectile tumbled consistently nose-down. The authors theorized that there is an obliquity that

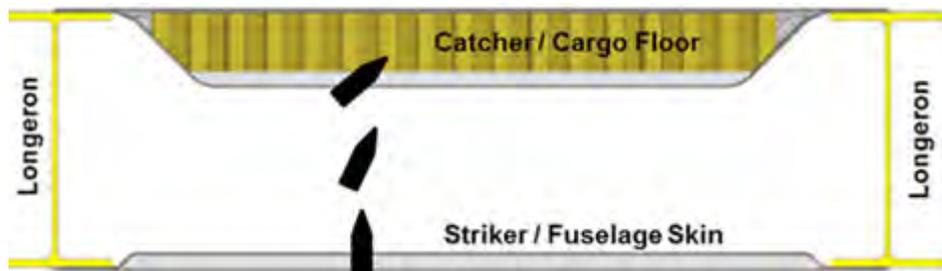


Figure 1: Turning Block Spaced Armor Integrated With Aircraft Skin and Floor Sections (Source: Robeson [2]).

acts as an inflection point in which the striker imparts no tumble to the round and the armor system experiences degraded performance.

To test this hypothesis, ballistics testing was completed and analyzed at normal and oblique shot lines. Testing was conducted at an indoor range at the U.S. Army Combat Capabilities Development Command (CCDC) Aviation & Missile Center (AvMC) Ballistic Test Range for Aircraft Component Survivability at Fort Eustis, VA. A test rig was constructed (Figure 2, left) to hold the armor system in place with repeatable boundary conditions and simulate realistic shot lines. This setup enabled control over the obliquity of the striker and catcher, as well as the distance of the air gap.

Two high-speed video cameras on the side and below the armor panels were used to record data (Figure 2, right). One camera captured video footage from the left side; this camera was used to measure the angle of the bullet's tumble and its velocity as a function of distance. The second camera was placed on the bottom of the test rig and recorded video facing up toward the shot

Traditional AP armor systems are metallic and/or ceramic; they exhibit a positive relationship between obliquity and performance.

line; this camera was used to measure the yaw of the bullet. Both cameras were used in conjunction with a velocity screen, which measured muzzle velocity of the round directly after leaving the gun, to ensure accuracy of the high-speed video velocity measurements. The video consistently measured 1.1% slower than the velocity gates; this discrepancy was considered acceptable.

Two types of tests were conducted to better understand this armor system's performance. The first test was a standard V_{50} determination, as specified by MIL-STD-662F [4]. A V_{50} describes the velocity at which an armor has a 50% chance of stopping a given

projectile (threat); thus, a higher V_{50} is desirable for a given weight. Second, turning block was shot without a catcher at varying obliquities and with constant velocity (100-m standoff velocity ± 100 ft/s). This test examined the round's angle of tumble as a function of both air gap distance and armor obliquity.

The areal density of the armor, the threat being tested, and the velocity of the round will not be disclosed in this article due to their security classifications. However, in order to portray the effects that velocity had on test results, this classified velocity (which corresponds to the 100-m standoff velocity of the unstated threat) will henceforth be referred to as the "reference velocity." Each subsequent velocity included here will be a delta (Δ), or numerical difference, from this unstated reference velocity.

RESULTS

V_{50} Testing at 0° and 45° Obliquities

First, V_{50} 's values were determined at 0° and again at 45°, each test maintaining a 6-inch air gap between striker and catcher. The results can be seen in Figures 3–6. Figures 3 and 4 demonstrate the relationship between the angle of tumble and the distance traveled from the back face of the striker, while Figures 5 and 6 illustrate the relationship between bullet velocity and angle of tumble. Additionally, color coding is used to differentiate between shots that were a partial penetration (green) vs. complete penetration (red). A partial penetration is terminology used by the armor community to specify a successful stop, but one in which the armor accrued some damage.

A few preliminary conclusions can be drawn from these initial V_{50} tests. First, the performance of the spaced armor

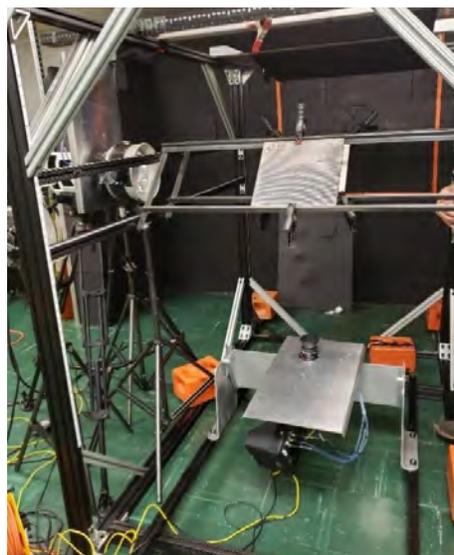


Figure 2: (Left) Test Rig at 0° Obliquity and (Right) Test Rig at 45° Obliquity With Cameras (Source: CCDC AvMC).

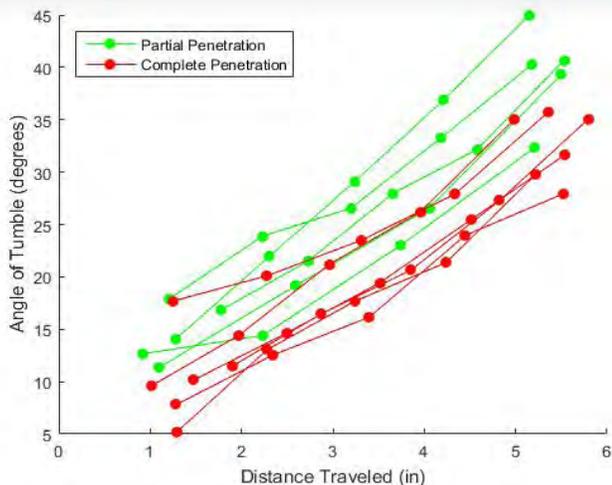


Figure 3: V_{50} at 0° : Angle of Tumble vs. Distance Traveled (Source: CCDC AvMC).

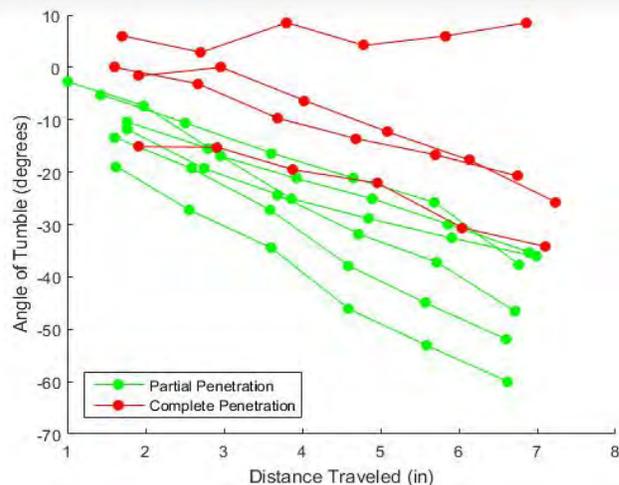


Figure 4: V_{50} at 45° : Angle of Tumble vs. Distance Traveled (Source: CCDC AvMC).

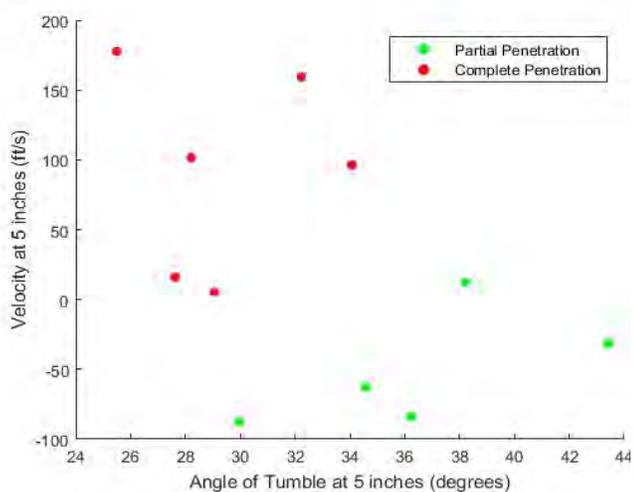


Figure 5: V_{50} at 0° : Velocity vs. Angle of Tumble at 5 Inches (Source: CCDC AvMC).

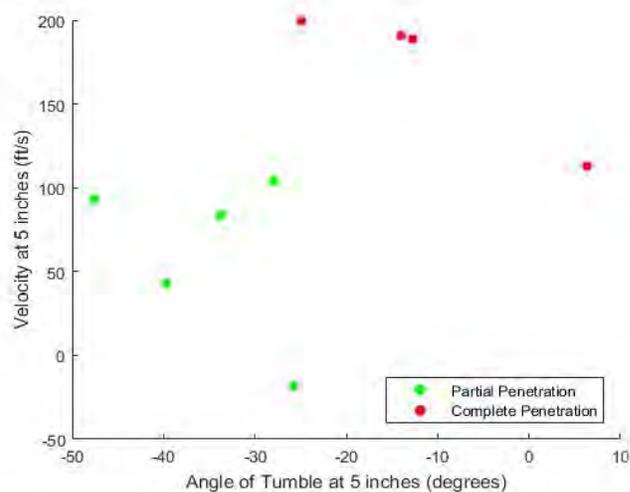


Figure 6: V_{50} at 45° : Velocity vs. Angle of Tumble at 5 Inches (Source: CCDC AvMC).

system was fairly consistent at normal obliquity. The relationship between angle of tumble and the distance traveled was mostly linear, leading to the conclusion that the turning block imparts a constant tumble rate on the round.

Bullet velocity, as well as angle of tumble, both affect whether the shot is a complete or partial penetration. As the velocity increases and/or the tumble decreases, it appears that the round becomes more difficult to stop. This conclusion follows the principles that

govern spaced armor performance. A faster round has more energy, and a less-tumbled bullet has a lower presented area, resulting in greater impact energy per unit area. Both conditions decrease the effectiveness of the catcher. It is worth noting that there are multiple causes of reduced tumble angle, including faster velocity (less time to tumble) and smaller air gap (less distance to tumble).

Normal obliquity (0°) produced a V_{50} of $\Delta 5.8$ ft/s (regarding reference velocity), and 45° resulted in $\Delta 147.3$ ft/s. The

V_{50} at 45° was higher than the V_{50} at normal obliquity; however, the predicted anomaly was observed in the course of testing. Ten shots were fired to calculate the V_{50} at 45° . One of them exhibited almost no tumble, causing it to pass straight through the armor system with little attenuation of energy. This particular shot can be clearly distinguished in Figure 4 as the line with 0° slope (the angle of tumble does not increase with distance traveled). This degraded performance condition is considered an inherent characteristic

of the spaced armor system, so the anomalous shot was classified as a valid data point (not an outlier) and is included in the V_{50} calculation.

While 0° tumbled nose-down 100% of the time (12/12), 45° tumbled nose-up $\sim 90\%$ (9/10) of the time. After seeing 1/10 shots exhibit this decrease in angle of tumble, it was clear that some degraded performance in this spaced armor system was present. The angle of the armor system was then stepped back first in 5° and then 10° increments from 45° to 15° to

determine if more pass-through events were possible.

Angle of Tumble vs. Distance Traveled at Varying Obliquities

In these tests, the gunpowder grain input was modified to shoot all of the projectiles at the reference velocity to hold this variable constant. However, due to the variable nature of ballistics, a delta of ± 100 ft/s is present in this data. Additionally, the rounds were shot at turning block only; no catcher was used to observe the angle of tumble past the

traditional air gap maximum distance of 10 inches.

Various obliquities were tested, and the results are shown in Figures 7–11. Additional 0° and 45° data were captured without catchers, and the results are included in this set. Figures 10 and 11 show the angle of tumble as negative, which corresponds to the bullet tumbling nose-down instead of nose-up.

The coordinate system is relative to the orientation of the turning block;

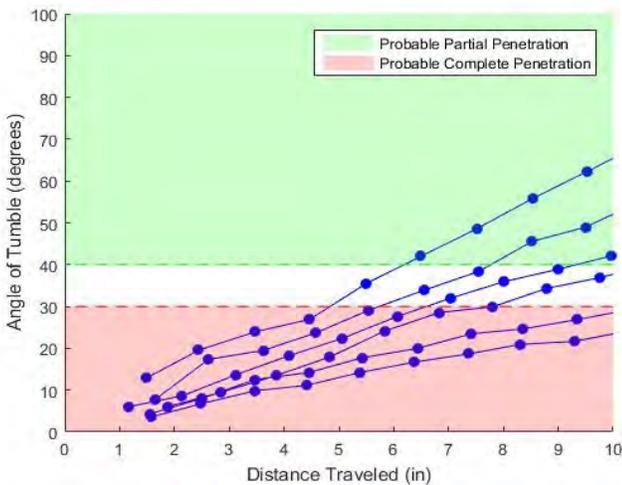


Figure 7: 0° : Angle of Tumble vs. Distance Traveled (Source: CCDC AvMC).

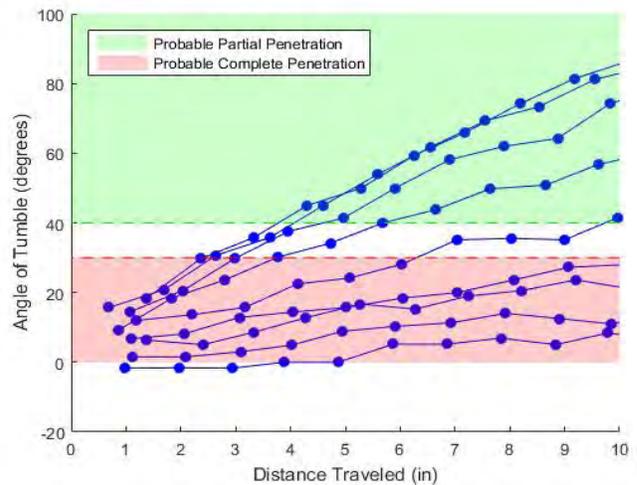


Figure 8: 30° : Angle of Tumble vs. Distance Traveled (Source: CCDC AvMC).

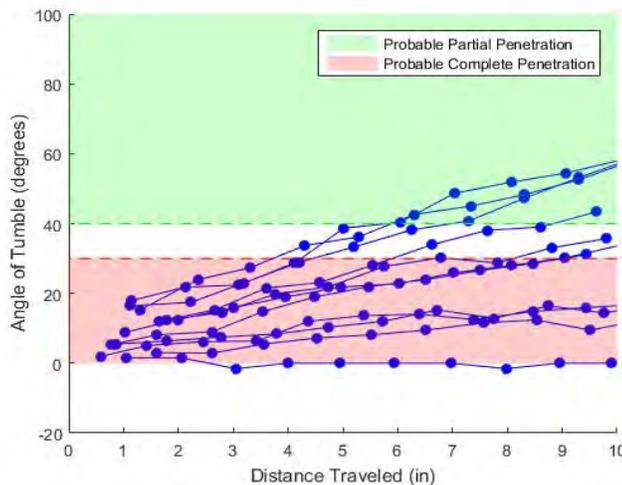


Figure 9: 35° : Angle of Tumble vs. Distance Traveled (Source: CCDC AvMC).

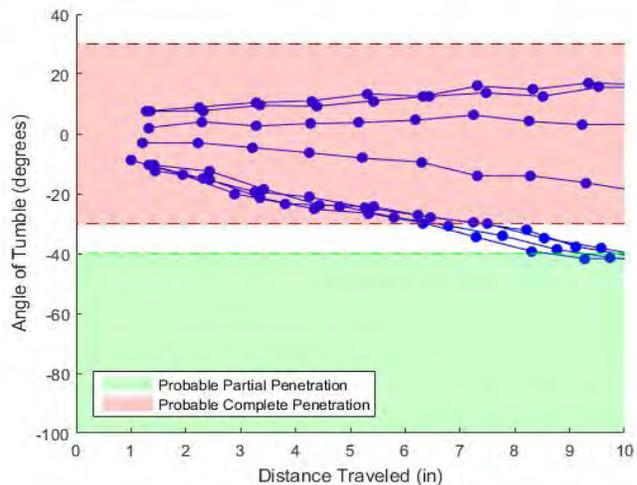


Figure 10: 40° : Angle of Tumble vs. Distance Traveled (Source: CCDC AvMC).

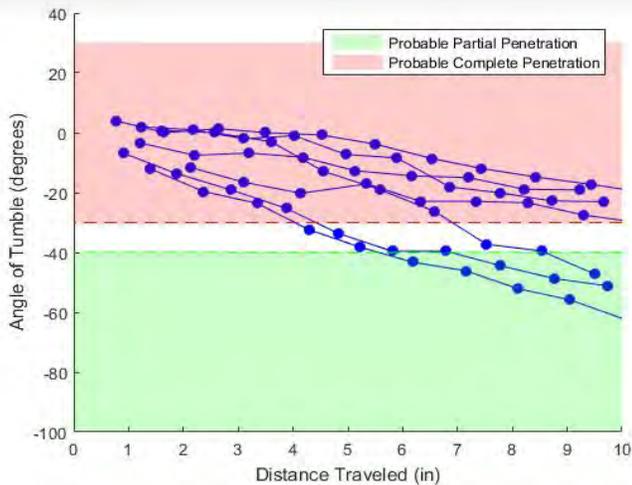


Figure 11: 45°: Angle of Tumble vs. Distance Traveled (Source: CCDC AvMC).

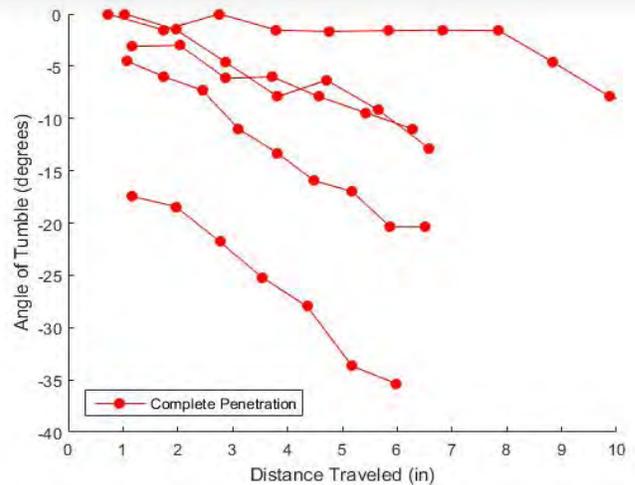


Figure 12: Attempted V_{50} at 40°: Angle of Tumble vs. Distance Traveled (Source: CCDC AvMC).

in this experiment, it was set so that every bullet tumbles nose-up at normal (0°) obliquity. Analysis of the previous V_{50} test results indicates that 100% of bullets fired were stopped when they exhibited at least $\pm 40^\circ$ of tumble. Therefore, shots that meet this criteria are assumed to result in a partial penetration (represented in green in Figures 7–11).

Alternatively, according to analysis of previous V_{50} tests, 100% of bullets fired passed through when they displayed less than $\pm 30^\circ$ of tumble. Therefore, it was assumed that shots meeting this criteria would result in a complete penetration (shown in red in Figures 7–11). The section of the plots with no color coding, between $\pm 30^\circ$ and $\pm 40^\circ$, represents an area where there is no conclusive evidence to predict how the armor will perform based on current data.

After analyzing the test results, 40° appears to be the hypothesized inflection point. As shown in Figure 10, some shots exhibit a nose-up rotation, others exhibit little-to-no tumble, and the rest exhibit a nose-down rotation. Due to the variability and lack of rotation of the projectiles at this obliquity, it would be expected that the performance of

the armor system as a whole would be reduced.

To further characterize the performance of the armor system at the 40° obliquity, V_{50} testing was conducted; the results are displayed in Figure 12. The air gap was initially set to 6 inches, but no partial penetrations occurred within four shots, even after significantly reducing the velocity to $\Delta 765$ ft/s below the reference. At this point, the air gap was increased to 10 inches; however, the armor system was still unable to stop the round. After five shots, this V_{50} test was concluded because it was clear that a worst-case obliquity was identified.

CONCLUSIONS

While more work and testing needs to be done to make statistically-stronger conclusions, preliminary trends can be drawn from this experimental data. At normal obliquity, this armor system performs, as intended, against the proposed threat at 100-m standoff velocity and is effective at stopping the projectile at much lower weights than traditional armor systems.

As hypothesized, there appears to be an inflection point, at or near 40° , where the tumble of the round is

At normal obliquity, this armor system is effective at stopping the projectile at much lower weights than traditional armor systems.

greatly reduced, resulting in degraded performance. Additionally, the obliquities near the inflection point, especially between 30° and 40° , also exhibit similar intermittent reduction in tumble and decreased performance.

At and around the 40° inflection point, there were certain shots that exhibited little-to-no tumble. These shots were especially noteworthy, as bullet rotation is the only mechanism by which this spaced armor system can defeat AP threats at a reasonable areal density. While this undesired phenomenon did not occur 100% of the time, its existence, even intermittently, threatens the performance of the armor at this specific, narrow range of obliquities.

To fully characterize this armor system, additional research and testing are needed to better understand when and why this reduced tumble occurs and the full impact of the lack of tumble. This increased understanding will enable the development of solutions to overcome this inherent vulnerability in the armor. It is worth noting that these solutions, while likely able to eliminate the inherent vulnerability, will probably increase the overall weight of the armor. However, this vulnerability can also be mitigated through system-level design and careful integration without any need to add weight to the system.

While the armor system suffers from a small range of vulnerable shot lines, it represents a new, effective, lightweight class of high-performance armor. Its multifunctional applications and low areal density make it attractive for aircraft, as well as ground vehicles and

building walls. Further development work could enable such systems to revolutionize Army rotorcraft survivability. ■

REFERENCES

- [1] Tunis, G. C., S. Kendall, and S. L. Kinnebrew. U.S. Patent 8,739,675 B2, 2014.
- [2] Robeson, M. "Structural Multifunctionality for Weight Reduction." Proceedings of the AHS 74th Annual Forum, Phoenix, AZ, May 2018.
- [3] Berry, O., D. Misciagna, G. Hickman, M. Molitor, and B. Justusson. "Highly Durable Floor/Armor for Rotorcraft (HDFAR) Program: Phase 6 of the Rotorcraft Durability and Damage Tolerance (RDDT) Program." Final Report for Agreement W911W6-11-2-0014, U.S. Army Research, Development and Engineering Command Technical Report (TR) 18-D-63, June 2019.
- [4] U.S. Department of Defense. V_{50} Ballistic Test for Armor. MIL-STD-662F, revision F, 18 December 1997.

BIOGRAPHIES

SIERRA I. SEMEL is a mechanical engineer at CCDC AvMC, where she develops and matures aircraft structures technology. Her areas of focus include aircraft vulnerability reduction; composite aircraft design, manufacturing, and repair; and additive manufacturing. Ms. Semel holds a B.S. in mechanical engineering, with a minor in math and physics, from Virginia Commonwealth University.

DANIEL V. CAMP is an aerospace engineer at CCDC AvMC, where he develops and matures aircraft structures technology. His areas of focus include aircraft vulnerability reduction and composite aircraft design, manufacturing, and repair. Mr. Camp holds a B.S. in aerospace engineering from North Carolina State University.

JOHN T. HAILER is a mechanical engineer and program manager at CCDC AvMC, where he develops heat transfer, electrical conversion, and armor technology. His current focus is on survivability of aircraft engines and improvement of electrical and thermal systems in support of enhanced rotorcraft survivability. Mr. Hailer holds a B.S. and M.S. in mechanical engineering from West Virginia University.

DELANEY M. JORDAN is an aerospace engineer at CCDC AvMC, where she develops and matures aircraft structures technology. Her areas of focus include composite aircraft design, manufacturing, and repair. She previously specialized in coating technology and novel microprocessing techniques in support of piezoelectric microelectromechanical systems at ARL in Adelphi, MD. Ms. Jordan holds a B.S. in materials science and engineering, with a focus in nanotechnology, from the University of Maryland, College Park.

(Source: 123rf.com)

INVESTIGATING SURFACE
STRUCTURES FOR

INFRARED SIGNATURE MANAGEMENT

By Qaisar Manzoor



SUMMARY

This article investigates the physics principles that govern the effects of type, smoothness, and surface structure of materials on a material's emissivity. A simple classification of materials is metals and nonmetals. Nonmetals tend to have higher emissivity above 0.8, while metals generally have low emissivity below 0.2.

Other factors that affect the emissivity of materials include smoothness or roughness of the surface, irregular surface structures, and regular surface structures. Irregular surface structures of materials produce varying emissivity, depending on the smoothness or roughness of the surface. This results in different emissivity of the same surface. Regular geometries, such as grooves, show an enhancement in the emissivity of an object [1].

This study proposes using regular geometries with varying parameters to produce desired results. The findings can help develop the framework for a possible software solution that could help in designing materials with regular geometries that produce a desired material's emissivity. Follow-on experiments will verify the software's validity. The software would provide the researcher a tool in developing materials with regular surface geometries that produce a desired increase or decrease its emissivity.

INTRODUCTION

Infrared (IR) imagery is a good tool for intelligence, reconnaissance, and surveillance of potential targets. IR signature management provides the means to develop methods, which can alter the IR signatures of objects for various purposes. Some factors affecting the signature of objects in a real environment include the wavelength of the incident radiation, the size of

Infrared imagery is a good tool for intelligence, reconnaissance, and surveillance of potential targets.

the object, polarization of light, and atmospheric phenomena [2]. Other factors that affect the signature of the object include irregular and regular surface structures [1].

This article focuses on the role of irregular and regular surface structures in IR signature management. Understanding the physics behind the interactions between irregular and regular structures on the emissivity of materials provides the ability to design structures on materials that would produce the desired IR signature responses. Understanding the principles that affect the emissivity of materials through manipulating their surface structures could also provide the framework for a software solution. This would guide the researcher in the material's surface structure design that would produce the intended IR signature response.

This article also discusses the effects of applications of paints, paint additives, and coatings on regular structures on a material surface.

IR AND SURFACE INTERACTIONS

Passive IR cameras view the emitted and reflected radiation from a material. Every object above zero K radiates energy, which depends on the material's temperature and surface conditions. IR cameras are capable of measuring the energy radiated by an object [3]. The wavelengths of the emitted radiation are in the IR region of the spectrum.

Figure 1 shows the electromagnetic spectrum, with emphasis on the IR region. Near-IR range is about $0.75 \mu\text{m}$ to about $1 \mu\text{m}$, short-wave IR (SWIR) range is from about $1 \mu\text{m}$ to about $2.5 \mu\text{m}$, mid-wave IR range is from about $3 \mu\text{m}$ to about $5 \mu\text{m}$, and longwave IR range is from about $8 \mu\text{m}$ to about $12 \mu\text{m}$ [4].

Figure 2 shows the different types of reflections. The reflections are dependent on the type surface with which the incident energy interacts. Figure 2 (left) shows specular reflection for a very smooth surface. Figure 2 (middle) shows diffuse and specular reflections for a reflecting surface, with

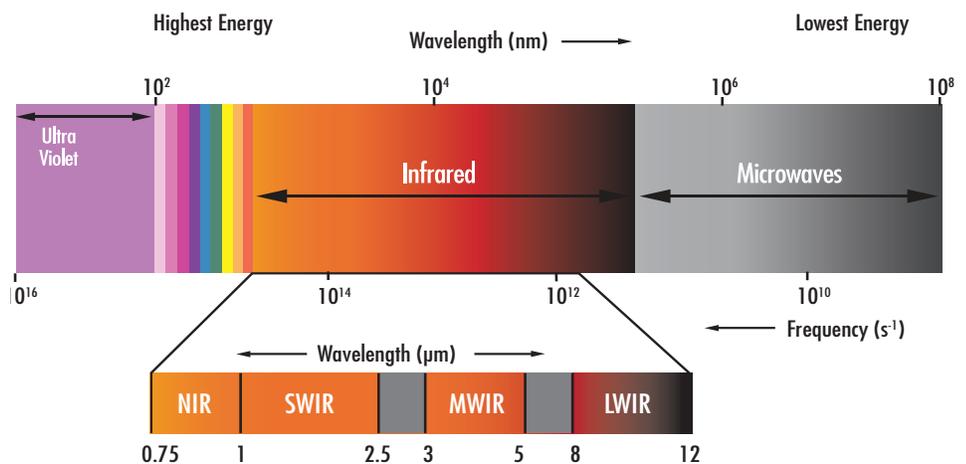


Figure 1: Electromagnetic Spectrum (Source: Edmund Optics Worldwide [4]).

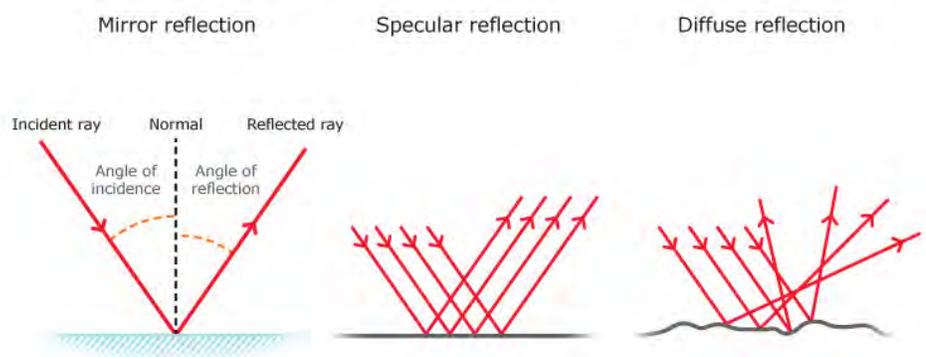


Figure 2: Effects of Surface Type on Reflection of Incident Radiation (Source: Science Learning Hub [5]).

some micro roughness. Figure 2 (right) shows only diffuse scattering for a surface, with a lot of micro roughness [1].

Irregular geometries on a surface can cause surface roughness. Diffuse or a combination of diffuse and specular reflection occurs due to the roughness of the surface. A surface acts rough or becomes smooth relative to the wavelength of the incident radiation [6]. Randomly-oriented irregular geometries that are much larger than the wavelength of the incident radiation result in diffuse reflection. Likewise, if the surface irregular geometries and variations are much smaller than the wavelength of the incident radiation, then the surface will result in specular reflection.

Diffuse reflection reflects the incident radiation in every direction, while specular reflection reflects the incident radiation at an opposite angle. The angle of reflection is equal to half of the incident angle. Snell's Law of Radiation, shown in Equation 1, illustrates the relationship between the angle of incidence, angle of refraction, and the refractive indices of each of the mediums [7].

$$n \sin \phi = n' \sin \phi' \quad (1)$$

Diffuse or a combination of diffuse and specular reflection occurs due to the roughness of the surface.

Equation 1 states that the index of refraction of first medium (n) times the sine of the incident angle (ϕ) is equal to the index of refraction of the second medium (n') times the sine of the refracted angle (ϕ').

Equation 2 shows the radiative transfer equation (RTE) that is the expression for the scene radiance. $L_{\lambda, atm}^{\uparrow}$ and $L_{\lambda, atm}^{\downarrow}$ are the upward and downward atmospheric radiance, ϵ_{λ} is the emissivity of the object, $B_{\lambda}(LST)$ is the blackbody radiance at the land surface temperature, and τ_{λ} is the transmission through the object.

$$L_{\lambda} = \epsilon_{\lambda} B_{\lambda}(LST)\tau_{\lambda} + L_{\lambda, atm}^{\uparrow}\tau_{\lambda} + (1-\epsilon_{\lambda})L_{\lambda, atm}^{\downarrow}\tau_{\lambda} \quad (2)$$

The relation in Equation 3 gives the estimated value emissivity of an object from Kirchhoff's Law.

$$\epsilon = I - R \quad (3)$$

Equation 3 defines the relationship between emissivity and reflectivity [8]. As discussed earlier, the object's reflectivity depends on the wavelength of the incident radiation, which implies that the object's emissivity also depends on the wavelength of the incident radiation. Regular geometries affect the total normal emissivity of an object by adding up the normal emissivity and the angled geometry's emissivity [1]. Accurately designing regular geometries will provide the ability to customize emissivity of materials to produce the desired results.

EFFECTS OF SURFACE STRUCTURE ON AN OBJECT'S EMISSIVITY

Metals and nonmetals are two simple classifications of materials. Nonmetals, such as paint, paper, glass, stone, and others, have high emissivity values that can range above 0.8, while metals show an emissivity below 0.2. Irregular structures on surfaces lead to varying emissivity. Some metals can reach emissivity of 0.2 or lower, but the presence of irregular surface structure can result in emissivity of 0.8 or higher. Regular geometries are well-defined structures, like the grooves shown in Figure 3.

Figure 3 shows regular grooves on a polished metal surface. For example, the emissivity of the surface is $\epsilon_{normal} = 0.04$. The apex angle of the grooves is 60° . The grooves enhance the emissivity of the material normal to the macroscopic surface shown in the figure, which illustrates the mechanisms that play an important role in enhancing the emissivity of the material.

There are two contributors to the radiation emitted from spot 1 that is normal to the macroscopic groove surface and characterized by $\epsilon(60^{\circ})$. The radiation from spot 2 is reflected from spot 1 in the normal direction.

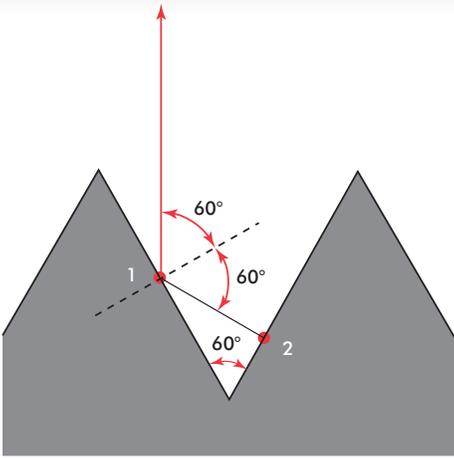


Figure 3: V-Groove Model of a Polished Metal Surface With Low Emissivity (Source: Vollmer and Möllmann [1]).

The contribution from spot 2 is characterized by $\varepsilon(60^\circ) \cdot R(60^\circ)$, which is equal to $\varepsilon(60^\circ) \cdot [1 - \varepsilon(60^\circ)]$. The third contributing factor is the radiation

Accurately designing regular geometries will provide the ability to customize emissivity of materials to produce the desired results.

emitted from spot 1 in the direction of spot 2, which reflects off spot 2 to spot 1 and is then reflected in the normal direction. The relationship $\varepsilon(60^\circ) \cdot R(0^\circ) \cdot R(60^\circ)$, which is equal to $\varepsilon(60^\circ) \cdot [1 - \varepsilon(0^\circ)] \cdot [1 - \varepsilon(60^\circ)]$, characterizes the contributions from this interaction. Adding the individual contributions results in the grooved surface's total emissivity.

The total normal emissivity for a polished surface with a normal emissivity of $\varepsilon(0^\circ)$ of 0.04 and an emissivity at $\varepsilon(60^\circ)$

of 0.05 is calculated using Equation 4. By using these formulations, the total emissivity of the grooved surface is calculated, as shown in the equation, and shows an increase in the normal emissivity of the surface by a factor of 3. The calculated enhanced emissivity of a polished surface with $\varepsilon(0^\circ) = 0.04$ and an emissivity at $\varepsilon(60^\circ) = 0.05$.

$$\varepsilon_{total,normal} = 0.04 + 0.04(1 - 0.05) + 0.05 \cdot (1 - 0.04) \cdot (1 - 0.05) = 0.124. \quad (4)$$

This also explains why rough surfaces have a higher emissivity than a polished flat surface.

Calculations for a variety of angles, such as the angles shown in Figure 3, show a strong variation in emissivity, with varying observation angles [1].

CONCLUSIONS

Literature research suggests the viability of IR signature management by managing regular surface structure geometries. IR signature management is comprised of emitted energy and reflected energy from an object. The angle at which an IR camera views the emitted and reflected energy also affects the appearance of the image in an IR camera. Numerical calculations show that the normal emissivity of a surface can be enhanced using regular geometries.

Investigation into the effects and viability of using paints, paint additives, and coatings on regular structures on a surface could help further enhance or degrade IR signatures. Further experimentation with regular structures, paints, and coatings will help in developing an understanding of the impacts of these methods on IR signature management that could be of interest for unconventional countermeasures.

Understanding the physics behind the principles could also aid in developing a

software solution, which could provide numerical assessment of the effects of various angles on a surface's emissivity with regular structures with or without applying paints, paint additives, or coatings. ■

REFERENCES

- [1] Vollmer, M., and K. Möllmann. *Infrared Thermal Imaging: Fundamentals, Research and Applications*. Second Edition, WILEY-VCH Verlag GmbH & Co., 2018.
- [2] Andersson, K. E. "A Review of Materials for Spectral Design Coatings in Signature Management Applications." SPIE, 2016.
- [3] Havens, K. S. "Absolute Zero." Retrieved from ScienceDirect, <https://www.sciencedirect.com/topics/earth-and-planetary-sciences/absolute-zero>, 2016.
- [4] Edmund Optics Worldwide. "What is SWIR?" <https://www.edmundoptics.com/knowledge-center/application-notes/imaging/what-is-swir/>, 2020.
- [5] Science Learning Hub. "Types of Reflection." <https://www.sciencelearn.org.nz/images/45-types-of-reflection>, accessed 6 May 2020.
- [6] Bakker et al. "Principles of Remote Sensing." Enschede: The International Institute for Geo-Information Science and Earth Observation, 2001.
- [7] Aldrich, R. "Laser Fundamentals." Retrieved from FAS Military Analysis Network, <https://fas.org/man/dod-101/navy/docs/laser/fundamentals.htm>, 9 April 1999.
- [8] Physical Concepts. "Product Tutorial on Land Surface Temperature (LST)." Chapter II, http://eumetrain.org/data/4/460/print_2.htm#page_2.0.0, 2017.

BIOGRAPHY

QAISAR MANZOOR is a research physicist and member of the unconventional countermeasures team at the Geotechnical and Structures Laboratory at the U.S. Army Engineer Research and Development Center. His research focuses on understanding the interactions between electromagnetic radiation and material properties on synthetic aperture radar, IR, and multispectral imaging. As a veteran of the U.S. Armed Forces, he served in the U.S. Navy, Army, and Army Reserve. Mr. Manzoor holds a B.S. in physics, with a second major in mathematics, from The University of Memphis. He is currently pursuing his master's degree in applied physics from Johns Hopkins University.



Defense Systems
Information Analysis Center

4695 Millennium Drive
Belcamp, MD 21017-1505

DSIAC ONLINE

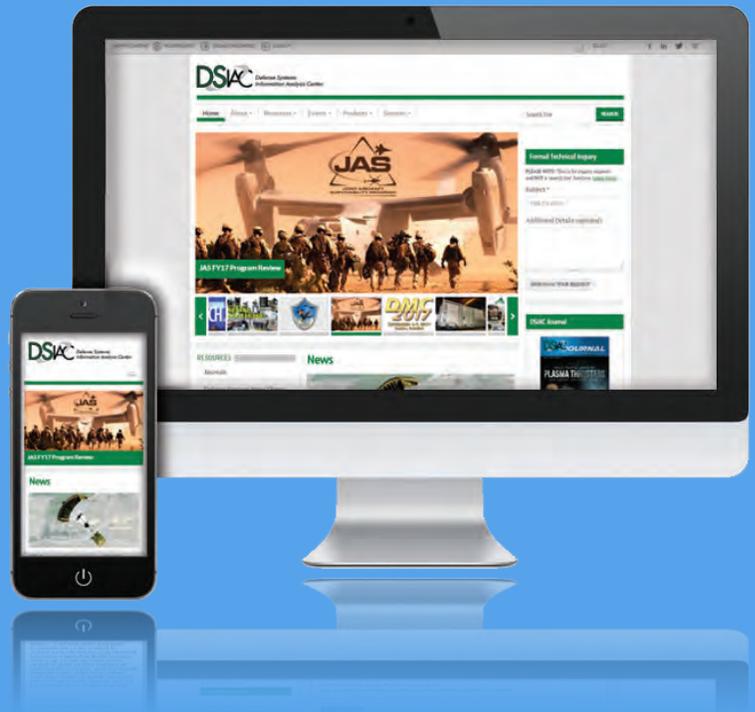
www.dsiac.org

DSIAC PRODUCTS AND SERVICES INCLUDE:

- Performing literature searches.
- Providing requested documents.
- Answering technical questions.
- Providing referrals to subject matter experts (SMEs).
- Collecting, electronically cataloging, preserving, and disseminating Defense Systems scientific and technical information (STI) to qualified users.
- Developing and deploying products, tools, and training based on the needs of the Defense Systems community.
- Fostering and supporting the DSIAC technical Communities of Practice.
- Participating in key DoD conferences and forums to engage and network with the S&T community.
- Performing customer-funded Core Analysis Tasks (CATs) under pre-competed IDIQ Delivery Orders.

DSIAC SCOPE AREAS INCLUDE:

- Advanced Materials
- Autonomous Systems
- Directed Energy
- Energetics
- Military Sensing
- Non-Lethal Weapons
- Reliability, Maintainability, Quality, Supportability, and Interoperability (RMQSI)
- Survivability and Vulnerability
- Weapon Systems



CONNECT WITH US ON SOCIAL MEDIA!