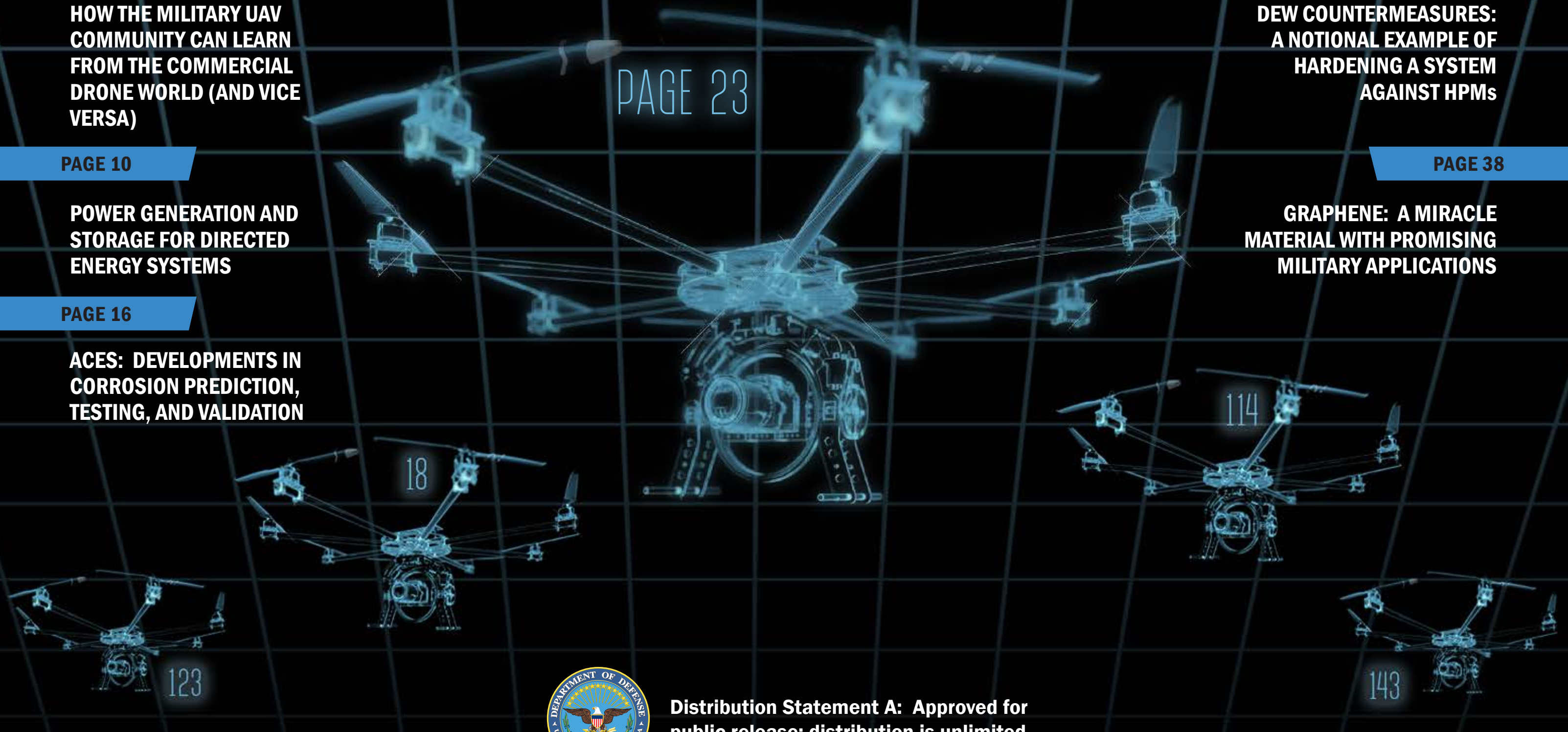
DSIAC JOURNAL

A Quarterly Publication of the Defense Systems Information Analysis Center

Volume 5 • Number 2 • Spring 2018

CYBER-PHYSICAL COMMAND-GUIDED SWARM



DSIAC JOURNAL

VOLUME 5 | NUMBER 2 | SPRING 2018

Editor-in-Chief: Brian Benesch

Copy Editor: Eric Edwards

Art Director: Melissa Gestido

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.

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

CONTENTS

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 CONTRACTING OFFICER REPRESENTATIVES

Peggy M. Wagner (COR)
704 TG/OL-AC
2700 D Street, Building 1661
Wright-Patterson AFB, OH 45433-7403
Office: 937.255.6302

Brad E. Forch (ACOR)
U.S. Army Research Laboratory
RDRL-WM
Aberdeen Proving Ground, MD 21005
Office: 410.306.0929

DSIAC PROGRAM MANAGEMENT ANALYST

Marisiah Palmer-Moore
IAC Program Management Office (DTIC-I)
8725 John J. Kingman Road
Fort Belvoir, VA 22060-6218
Office: 703.767.9109

MESSAGE FROM THE EDITOR

By Brian Benesch

In concert with ongoing continuous improvement efforts, DSIAC has recently refined our purpose, mission, and vision statements to more concisely convey the benefits of our offered services and products to the defense systems community. As a result, I am excited to share these newly unveiled statements with you.

- **Purpose:** The purpose of DSIAC is to provide information research and analysis for Department of Defense (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.

Complementing our vision statement, we established the following subtitle for DSIAC to help reinforce who we are—a "DoD Information Research Partner." With our *raison d'etre* defined, we generated some enhancements to optimize our services and products to achieve our vision.

We have also established a Notable Technical Inquiries webpage to provide a flavor of the types of efforts we conduct under our 4 free hours of research.

For example, we have recently renovated our biweekly *Defense System Digest* to better highlight DSIAC activities in addition to sharing relevant news and events. We have also established a Notable Technical Inquiries webpage to provide a flavor of the types of efforts we conduct under our 4 free hours of research. In addition, we maintain a regularly updated list of Newly Available STI that has been uploaded to the Defense Technical Information Center (DTIC).

Even the *DSIAC Journal* is being improved by the addition of Technology Spotlight articles—which has resulted, in part, from the overflow of article submissions we receive and sort through each quarter—and, most importantly, the continued emphasis on featuring articles authored by civilian, contractor, and/or academia in support of DoD laboratory efforts. This spring issue presents articles from subject-matter experts at the Naval Surface Warfare Center, Crane Division; the Air Force Research Laboratory; the University of Texas, Dallas; Purdue University; the Office of Naval Research; the Army Tank Automotive Research, Development and Engineering Center; GCAS Incorporated; Grant Drone Solutions; and DSIAC.

I hope that you enjoy this season's *DSIAC Journal*, and please stay connected to DSIAC as we work to implement additional advancements to maintain and enhance our value as the premier information research partner for defense systems. ■

HOW THE MILITARY UAV COMMUNITY CAN LEARN FROM THE COMMERCIAL DRONE WORLD (AND VICE VERSA)

By Barbara G. Grant

INTRODUCTION

The commercial unmanned aerial vehicle (UAV) marketplace is large and growing. Estimates of its worldwide size vary: a typical number is $5.6 billion in 2016 [1], while Bloomberg News projects a $127 billion value by 2020 [2]. At first glance, similarities between military and commercial drone communities appear slight, as though they are merely distant cousins connected by a common ancestor. Some military drones, particularly those used for theater intelligence, surveillance, and reconnaissance (ISR) and combat support, have no obvious relative in the commercial drone community, but smaller drones used in military applications can closely resemble their commercial cousins. While military UAVs have a mission-specific purpose from the outset, commercial drones have seen an explosion of potential applications, including some that might be created right before a specific drone takes flight. This article examines how military UAV users can benefit from the lessons learned in the development of the commercial UAV marketplace, as well as how the military's technical acumen can aid applications in commercial industry where image quality and quantitative information satisfy critical needs.

THE COMMERCIAL UAV MARKETPLACE

The commercial UAV marketplace comprises two major categories: consumer drones and enterprise drones. Consumer drones are purchased for personal use; enterprise drones are used by businesses (large and small), universities, and public agencies, including those tasked with law enforcement, search and rescue, and fire protection. For the purposes of our analysis (to compare between military and commercial UAV markets), the focus here is on enterprise drones.

The commercial UAV marketplace is highly competitive. It includes established providers of imaging equipment as well as newer companies whose cameras are geared for specific applications, such as precision agriculture. Fixed-wing and rotary-wing aircraft are both found in this market and are selected according to the needs of the enterprise.

The market is highly sensitive to disruption as new technologies and strategies emerge and as Federal Aviation Administration (FAA) regulations are changed to allow greater UAV integration into the domestic airspace. Table 1 lists some of the current FAA limits for small unmanned aerial systems (sUAS) [3].

Table 1: Key FAA Requirements (14 CFR Part 107)

• Total weight of platform and sensors(s) less than 55 lbs
• Visual line-of-sight (VLOS) operation only
• Operate only over persons participating in the mission
• No operation under a covered structure
• Operate in daylight only
• Operating altitude less than or equal to 400 ft above ground level (AGL)

THE MILITARY UAV MARKETPLACE

The military UAV marketplace develops from specific missions, such as the Raven (shown in Figure 1), whose prime contractors are selected long in advance of deployment. Unlike commercial UAVs, military aircraft platform and sensor types are mission specific from the outset.

Military UAV sensors are manufactured by firms with many years experience and do not differ significantly from sensors on manned aircrafts. In fact, Global Hawk uses the same sensors formerly integrated onto U2s.

Competition among military prime contractors can be intense, but the field is necessarily limited due to the small number of airframe manufacturers. Though the market is not particularly sensitive to disruption, the military UAV community experiences the effects of disruption through the deployment of commercial drones by nonstate actors and hostile countries.

LESSONS THE MILITARY CAN LEARN FROM THE COMMERCIAL UAV COMMUNITY

Flexibility in Platform and Sensor

The commercial UAV market is segmented by application; several of the most important are shown in Table 2 [4]. These applications are, in turn, supported by product manufacturers, including those who develop task-specific cameras and software, and by industry consultants familiar with the needs of the end user.

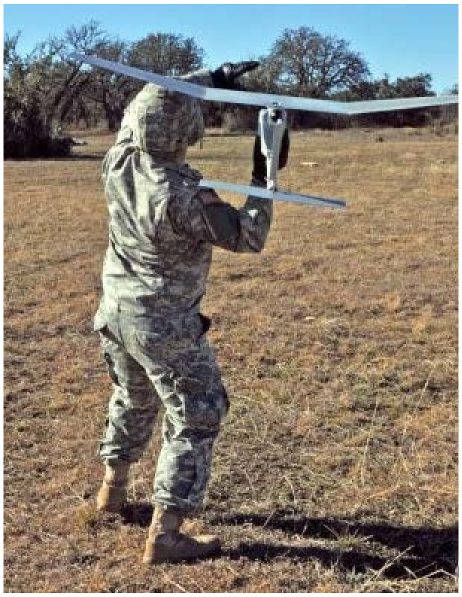


Figure 1: Army Military Police (MP) Preparing to Launch the RQ-11 Raven sUAS, Which Is Used for Short-Range Reconnaissance and Situational Awareness *(Photo Credit: Sgt. Samuel Northrup).*

Table of Contents

Table 2: Key Commercial UAV Applications

- Civil Infrastructure Inspection
- Construction Monitoring
- Emergency Response/Search and Rescue
- Insurance Investigation
- Law Enforcement and Security
- Mining and Aggregates
- Power, Process, and Utilities
- Precision Agriculture
- Surveying and Mapping

That the commercial UAV industry is segmented by application—and not platform—allows the enterprise flexibility. For instance, fixed-wing aircraft are often used in construction stockpile monitoring, but the hovering capability of multirotor aircraft is essential for close-in inspection tasks [5]. Tracking a suspect in a law enforcement setting might be performed with a fixed-wing drone over long distances, but monitoring that suspect's capture and arrest is best performed by a hovering multirotor. Flexibility in sensor choices for either platform type provides an additional degree of freedom.

In practice, commercial application managers deploy what they have; and if they have a choice between platforms, they can use each platform for maximum effectiveness while swapping out sensors if they have more than one set. If military sUAS users were given the latitude to use more than one platform type per mission as the situation changes on the ground, as well as to swap out sensors when necessary, the overall mission result could be enhanced. In the process, data on platform type, sensors, ground activities, and mission results would be gathered. That data, when analyzed, could lead to the development of quality metrics—a task that the military is extremely good at—that could be fed back into future mission-planning activities.

Disruption as Teacher

Not only is the commercial UAV culture welcoming to disruptive innovations, the predisposition to disruption is embedded in its DNA. New innovations are quickly adapted as companies compete for market share; and the market itself widens as the FAA loosens operating restrictions.

An example of the latter may be found in precision agriculture, which is defined as "a farming management concept based on observing, measuring, and responding to inter and intra-field variability in crops" [6]. This departure from traditional farming methods makes the discipline itself a disruptive innovation. Satellite imagery or imagery gathered by aircraft over large farm areas can provide significant data to improve crop yield, but such flights are expensive. Alternatively, sUAS can gather data more cheaply (although large farms may require many flights to gather data due, in part, to FAA constraints) [7].

If the FAA's VLOS restriction (listed in Table 1) is lifted [8], the application faces disruption. Data gathering will no longer be limited by line-of-sight but rather by battery power to the UAV and by data capacity. While number of flights will vary according to farm and UAV, fewer flights promote a higher-quality data set as these data are obtained under similar atmospheric and illumination conditions. Removal of one constraint—in this case, line-of-sight operation—can work to produce a more informative result. In the words of Roger Ohlund of SmartPlanes, a Sweden-based provider of UAV solutions, "One may conclude that we are probably right now at the beginning of what in time might be called an Agro-drone revolution" [7].

In addition, the need and desire to obtain more and better-quality data have a ripple effect throughout an industry. If battery power becomes the limiting factor in data gathering, companies wishing to stay ahead of the game will seek higher-quality battery/power alternatives to stay ahead of their competitors. Likewise, data analytics—proprietary software that turns imagery into quantitative information for the agricultural end user—will increase in importance to where it may become the next disruptive driver. These developments will in turn drive the need for sensors offering higher performance while also reducing cost, similar to the manner in which today's computer market has developed.

The military UAV community does not operate under FAA restrictions, but it must defend against threats from users of commercial equipment designed primarily for U.S. markets. And defeating these threats requires understanding and tracking the technology behind them. Thus, adapting military thinking to the commercial culture of disruption will facilitate a more effective approach to the threat.

Joint Ventures

The commercial world leverages expertise from smart people across disciplines to work toward a common goal; this lesson has not been lost on the military. Some military communities have already begun leveraging commercial expertise by holding “hackathons” and hacker classes, particularly in the strategically important area of command and control of a drone swarm [9] (an example of which is shown in Figure 2).

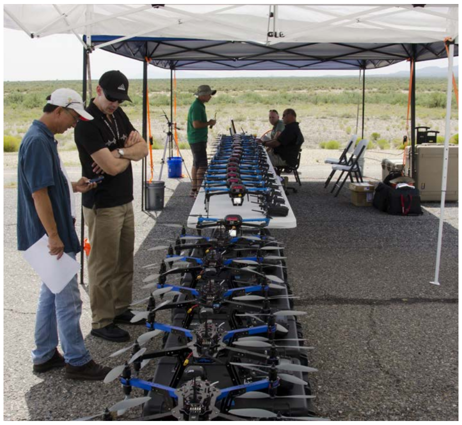


Figure 2: Small Drones Can Operate Together via a Unique Command-and-Control Structure. Hacking the Logic Behind Drone Swarms Is Key to Countering Their Threat *(Photo Credit: John Andrew Hamilton [U.S. Army Test and Evaluation Command]).*

Commercial startups are particularly good places for creativity to emerge as individuals from various backgrounds pool their expertise to develop a product or service. Recognizing this trend, stakeholders from both military and commercial communities are currently working together to identify and fund technology companies in several mission-critical areas [10]. While these developments are positive in themselves, the military’s increasing adaptation of the commercial mindset could lead to more creative use of human resources—the skills of its engineers and scientists. This author began her career supporting Department of Defense (DoD) projects and noted that the matrix management approach favored by many large military contractors worked against technologists developing technical breadth [11]. The threat, which was well-characterized in the old Cold War days, is now in flux, and strong arguments in favor of broader human resource utilization could be made.

The Dragon’s Dominance

Something happened on the way to commercial UAV market development: Chinese drone manufacturer Dà-Jiāng Innovations (DJI) became the world’s dominant manufacturer of sUAS platforms (such as the one shown in Figure 3), with some reports placing their market share at 70% [1]. This development has significantly affected many domestic manufacturers, such as 3D Robotics (3DR), which ceased manufacturing its airframes [12].

DJI has more than 1,500 employees working on research and development, according to recent market research. Moreover, electro-optical and infrared sensor manufacturers, such as U.S.-based FLIR Systems, produce cameras exclusively for use on DJI platforms [13]. Accordingly, military solution developers would be wise to consider that the next threat is likely to arrive via a DJI drone or drones from other Chinese manufacturers [1].

Figure 3: Chinese-Made DJI Drone in Use by the U.S. Air Force *(Photo Credit: Wesley Farnsworth).*

LESSONS THE COMMERCIAL UAV COMMUNITY CAN LEARN FROM THE MILITARY

High-End Hardware and Evaluation of Image Quality

Manufacturers of commercial drone cameras include those who provide cameras to a variety of markets (e.g., FLIR Systems and Sony) as well as companies who develop hardware only for drone applications. Not surprisingly, prices vary widely, as does image quality.

Not all the applications listed in Table 2 require high-quality imagery, as processed imagery from lower-quality cameras is sufficient for many tasks. Construction stockpile monitoring, for instance, will not suffer when highly processed imagery corrected for camera defects is used, and cameras costing a few hundred dollars can provide data to high-end mapping software that includes adjustment for known lens distortions [14].

In other applications, high data quality is essential. The General Image Quality Equation (GIQE) [15], which depends on the signal-to-noise ratio in unprocessed imagery, and the National Imagery Interpretability Rating Scale (NIIRS) value it predicts [16] are related to the three major discrimination tasks of detection, recognition, and identification, which are essential in military applications. Civilian applications such as agriculture, search and rescue, and infrastructure monitoring also benefit from high-quality imagery [17]. Figure 4 shows two military police performing a prelaunch checkout of a system designed to gather high-quality data.

Law enforcement is perhaps the key civilian area in which image-quality

Figure 4: Army MPs Perform Pre-Launch Checks of a Raven sUAS. The Raven's High-Quality Imaging Sensors Provide Data Used by Military Missions to Maintain Situational Awareness in Daytime and Nighttime Conditions *(Photo Credit: Sgt. Samuel Northrup).*

metrics will play a role. Imagine a trial in which a suspect is charged with a crime based on imagery gathered by a drone (such as the one shown in Figure 5) during a civil disturbance [18]. If the drone camera is of low quality with known optical distortions, a defense attorney could legitimately argue that the processing software identifying his client as the suspect led to the wrong party's arrest. Cameras must also provide imagery of a quality sufficient to identify and distinguish between phenomena that may arise during a civil disturbance, such as debris reflection and the signatures of explosive devices.

Figure 5: An sUAS Used by Police in Colorado *(Source: U.S. Department of Justice/ AeroVironment Inc.).*

The best data analytics in the world will be of dubious value when applied to imagery that is substandard in the first place. The fact that drone case law development is in the beginning stages motivates the need to understand and quantify technical performance. This is an area in which the commercial UAV marketplace, particularly in law enforcement, can learn from military development.

The Need for Accurate Radiometric Calibration

A radiometric calibration associates a physical quantity, such as the radiation received by an imaging sensor, with the sensor's output signal. The DoD, its contractors, and university partners have developed precise techniques for calibration; many of these are in the infrared portion of the spectrum and aid discrimination applications and target signature determination.

Atmospheric correction is necessary when the desired result of imaging is quantitative data on the ground, provided by the process diagrammed in Figure 6. The atmosphere is not a perfectly transmissive window, even on a so-called "clear day." To solve this problem, military components have developed and improved upon radiative transfer codes (models), which correct for atmospheric effects in the imaging sensor's output signal.

Several commercial companies manufacture cameras specifically for precision agriculture. They claim to provide calibrated imagery [19] but do not account for the transmission of the atmosphere in their literature. Without accounting for atmospheric transmission, reflectance values are not absolute. In some locations, this difference is significant, such as California's Central Valley agricultural region in which thick Tule fogs [20] lie close to the ground several months of the year.

If the commercial UAV community applies the results of military-derived atmospheric codes, they will receive more accurate data for their models and maps. When the FAA raises the commercial drone operating height limit, the need for correct atmospheric information may become another disruptive driver in precision agriculture.

The best data analytics in the world will be of dubious value when applied to imagery that is substandard in the first place.

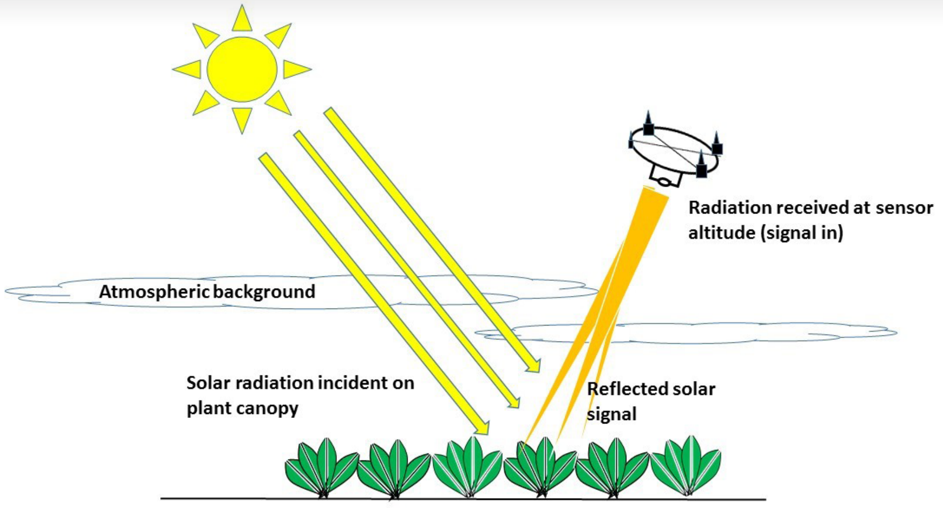

Radiation received at sensor altitude (signal in)
Atmospheric background
Solar radiation incident on plant canopy
Reflected solar signal

Figure 6: Agricultural Remote Sensing Configuration. The Solar Signal Reflected From a Plant Canopy Passes Through the Atmosphere to the UAV. A Calibration Function Infers the Input Signal's Value From the UAV Sensor's Output *(Source: Grant Drone Solutions, LLC)*.

CONCLUSION

Many commercial UAV image-gathering applications require only a "pretty picture," but for applications requiring high-quality imagery and radiometrically calibrated data, the military UAV community is far ahead of the commercial drone world. Furthermore, imaging sensor developers who produce for both military and commercial markets are ahead of the game in delivering high-quality data, but their products usually cost more than cameras manufactured for specific commercial markets.

As discussed, the military UAV community can learn from the commercial drone world in several significant areas, including the need for rapid adaptability and response to disruption. While adaptability in the commercial space is tied directly to market share, the military requires adaptation to new and changing threats. Partnering with commercial industry to develop data analytics, hackathons, and joint venture funding for promising technologies demonstrate the DoD community's willingness to adapt.

These two communities—military and commercial—seem far apart on many key issues relating to UAV deployment and data use, but that need not be the case. Each can learn from the other. And when that happens, the military will see rapid adaptability to changing threats, and the commercial world will benefit from high-quality imagers and the standards necessary to accurately interpret their data. ■

REFERENCES

[1] Joshi, D. "Commercial Unmanned Aerial Vehicle (UAV) Market Analysis—Industry Trends, Companies, and What You Should Know." *Business Insider*, http://www.businessinsider.com/commercial-uav-market-analysis-2017-8, 8 August 2017.

[2] Moskwa, W. "World Drone Market Seen Nearing $127 Billion in 2020, PwC Says." *Bloomberg Technology*, https://www.bloomberg.com/news/articles/2016-05-09/world-drone-market-seen-nearing-127-billion-in-2020-pwc-says, 9 May 2016.

[3] Federal Aviation Administration. "Summary of Small Unmanned Aircraft Rule (Part 107)." *FAA News,* https://www.faa.gov/uas/media/Part_107_Summary.pdf, 21 June 2016.

[4] Karpowicz, J. (editor). *Commercial UAV News.* https://www.expouav.com/news/, accessed 14 February 2018.

[5] Salmon, J. "Secrets to the Successful Selection of a UAV Platform." *Commercial UAV News*, https://www.expouav.com/news/latest/secrets-successful-selection-uav-platform/, 19 October 2016.

[6] Wikipedia. "Precision Agriculture." https://en.wikipedia.org/wiki/Precision_agriculture, accessed 27 December 2017.

[7] Ohlund, R. "Precision Agriculture Utilizing UAVs." SmartPlanes website, http://smartplanes.com/precision-agriculture-utilizing-uavs/, 20 April 2017.

[8] McNabb, M. "Is BVLOS Flight Getting Closer in US? Drone Industry Thinks So." *dronelife*, https://dronelife.com/2017/08/31/bvlos-flight-getting-closer-us-drone-industry-thinks/, 31 August 2017.

[9] Schuman, J., and E. Hall. "UAS Threats, Solutions, and the Collaboration Imperative." *DSIAC Journal,* vol. 4, no. 2, https://www.dsiac.org/resources/journals/dsiac/spring-2017-volume-4-number-2/uas-threats-solutions-and-collaboration, spring 2017.

[10] Defense Innovation Unit Experimental. DIUx website. https://www.diux.mil/team, accessed 16 January 2018.

[11] Wikipedia. "Matrix Management," https://en.wikipedia.org/wiki/Matrix_management, accessed 9 January 2018.

[12] Glaser, A. "DJI Is Running Away With the Drone Market." *recode*, https://www.recode.net/2017/4/14/14690576/drone-market-share-growth-charts-dji-forecast, 14 April 2017.

[13] FLIR Systems. Zenmuse XT Product Brief. https://www.flir.com/browse/industrial/aerial-kits/, accessed 28 December 2017.

[14] Peters, J. "Move from Drones to Maps: Unmanned Aerial Systems Support for ArcGIS." 2017 Esri Public Sector CIO Summit Proceedings, http://proceedings.esri.com/library/userconf/ciosummit17/papers/ps_cio_15.pdf, 30 March 2017.

[15] Griffith, D. "General Image Quality Equation (GIQE)." National Geospatial Intelligence Agency Briefing, https://calval.cr.usgs.gov/wordpress/wp-content/uploads/Griffith_Doug_JACIEGIQERev3cor2sjs6with-Caveat.pdf, 18 April 2012.

[16] Grant, B. *Getting Started with UAV Imaging Systems: A Radiometric Guide*. SPIE Press, https://spie.org/Publications/Book/2239236?SSO=1, July 2016.

[17] Federation of American Scientists. *Civil NIIRS Reference Guide*. https://fas.org/irp/imint/niirs_c/guide.htm#12, March 1996.

[18] Grant, B. "Imagery Analysis: Standards Needed for the Drone Age." *SPIE Newsroom*, http://spie.org/newsroom/5594-imagery-analysis-standards-needed-for-the-drone-age?SSO=1, 21 August 2014.

[19] Parrot Sequoia. Marketing Material. https://pix4d.com/wp-content/uploads/2016/02/Sequoia_Flyer.pdf, accessed 31 December 2017.

[20] Wikipedia. "Tule fog." https://en.wikipedia.org/wiki/Tule_fog, accessed 15 January 2018.

BIOGRAPHY

BARBARA GRANT is an electro-optical engineer and imagery analyst. She is President of Grant Drone Solutions, LLC, which provides consulting, training, and media content to military and commercial UAV communities. In addition, Ms. Grant is the author of *Getting Started with UAV Imaging Systems: A Radiometric Guide*, the first book on the market to focus on radiometry in a UAV context. She also teaches short courses in radiometry and UAV applications, is an Affiliate Instructor with Georgia Tech Professional Education Defense Technology Training, and is a Distinguished Instructor in the University of California, Irvine's Optical Engineering Certificate Program. Ms. Grant holds an M.S. in optical sciences from the University of Arizona.

(Source: U.S. Navy)

POWER

GENERATION AND STORAGE FOR DIRECTED ENERGY SYSTEMS

By Sarwat Chappell

INTRODUCTION

For many years, antiship missiles have represented an ongoing threat to U.S. military operators, as well as a challenge to U.S. defense planners and technology developers. In 1987, during the Iran-Iraq War, the frigate USS *Stark* was hit and severely damaged by two antiship Exocet missiles (as shown in Figure 1). These missiles were also the cause of the 1982 sinking of the British guided missile destroyer HMS *Sheffield*.

To address this issue, multiple kinetic missiles have traditionally been employed to defeat antiship missiles, such as in the 2016 engagement of two cruise missiles by the destroyer USS *Mason*, which used two Standard missiles and an Evolved Seasparrow Missile (ESSM). However, directed energy weapons (DEWs), such as high-energy lasers (HELs), offer the military a new and improved opportunity to defend against antiship missiles, potentially reducing the cost and timeline of an engagement and providing an increased ability to engage multiple target sets.

But DEWs come at a cost—power. These weapons require increased power, energy, and thermal management systems on platforms to address current and future threats. DEW developers must thus work to account for increased power levels and storage, which are dependent on many factors, such as the distance to the target, materials of the target, and the power generation capability of the platform engaging the target. In short, the challenge is to maximize the effectiveness of DEWs while minimizing the power impact to the host platform.

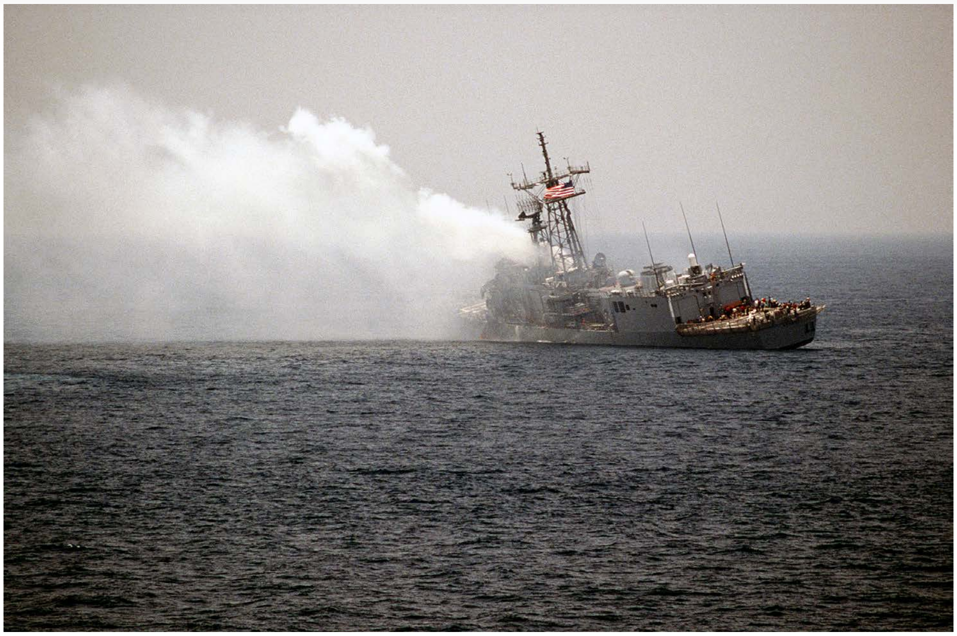


Figure 1: Damage to the USS Stark From Two Antiship Missile Hits *(Source: U.S. Navy).*

It would not be advantageous to have DEWs that require all the power of a platform, leaving little or no power for other system needs. Careful platform integration is required to ensure on-demand power for warfare system propulsion and platform services while employing DEWs. As illustrated in Figure 2, DEWs such as lasers are highly inefficient in converting energy from either electrical, chemical, or optical to energy for light amplified stimulated applications. Therefore, the platforms in which DEWs are integrated need to provide increased input power and storage. Several DEW demonstrations have been produced but were not fully integrated into platforms due to power-related challenges. However, if the U.S. military is going to use energy as a weapon, it better have plenty of it.

PAST AND EXISTING DIRECTED ENERGY SYSTEMS

Historically, military lasers capable of generating the higher laser power necessary to defeat hard targets have been explored and developed. Initially, the Department of Defense (DoD) invested in chemical and gas lasers in the 1980s and '90s. This investment resulted in the development and scale-up of the largest chemical laser testbed, the Mid-Infrared Advanced Chemical Laser (MIRACL)/Sea Lite Beam Director (SLBD) testbed. The U.S. Navy gained valuable information from testing the laser against missiles and other targets. This information concerned target lethality and how to control the laser beam in the atmosphere. As a result, programs such as the Airborne Tactical Laser (ATL), Airborne Laser (ABL), Space Based Laser (SBL), and Tactical High Energy Laser (THEL) were initiated. The limitations of these lasers, however, were that they used large quantities of toxic chemicals as a power source, which limited their magazines and created huge reloading and safety and handling issues. The DoD thus began to

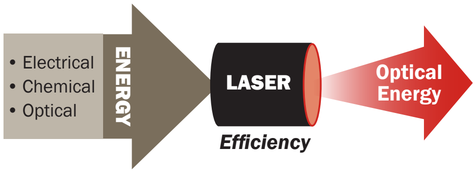


Figure 2: A Laser Simply Converting One Form of Energy Into Optical Energy *(Source: ONR).*

explore electric lasers as an alternative to chemical lasers.

One type of electric laser, the free electron laser (FEL), produces high-quality, low-energy electrons that are accelerated to almost the speed of light. These energized electrons emit light as coherent radiation at HEL powers. Figure 3 shows a simplified diagram of an FEL system with a linear accelerating cavity structure and permanent magnet wiggler for light extraction. The figure also shows optional optical cavity mirrors, which make the FEL an oscillator if installed. If the mirrors are removed, then the FEL is configured as an amplifier. FELs have no chemicals and have an unlimited magazine as long as electrical power is applied to it. Unfortunately, FELs also require a lot of source power to operate at HEL levels.

Another type of electric laser suitable for DoD applications is a solid-state laser (SSL). Currently, fiber lasers and slab lasers are the primary options of SSLs being explored for HEL systems. Both types require a gain medium, a pumping mechanism, a feedback mechanism, and output couplers. SSLs are typically at fixed wavelengths and are adaptable to ship, air, and ground platforms due to their size and weight for low-power engagements. In addition, SSLs offer near-continuous target engagement but are limited by removal of waste heat energy from the gain material.

> If the U.S. military is going to use energy as a weapon, it better have plenty of it.

Electric-gas lasers have also been explored by the DoD. One example is the airborne CO_2 laser invented by the Air Force. Other types of gas lasers include diode pump alkali lasers, which have the potential to achieve high power. They are desirable because of their optical-to-optical conversion efficiency.

So, where are we in our quest to achieve high-power lasers? Low-power fiber lasers have been tested and demonstrated by the Navy, Army, and Air Force. The Navy system uses incoherent beam combined fiber lasers and has been tested against short-range, in-port, littoral, and blue water threats. The Army is also working on SSL systems to defend bases in the field. The Ground-Based Air Defense (GBAD) system is a Marine Corps concept of a laser weapon system that consists of a vehicle-mounted HEL; command, control, and communications; and volumetric surveillance radar that would be capable of shooting down threats. GBAD will demonstrate the capability of a rugged expeditionary HEL system that can be cued by a radar capable of detecting low-radar-cross-section (RCS) threats. It will be able to perform hard kills of asymmetric threats to prevent reconnaissance surveillance and targeting and acquisition of expeditionary forces.

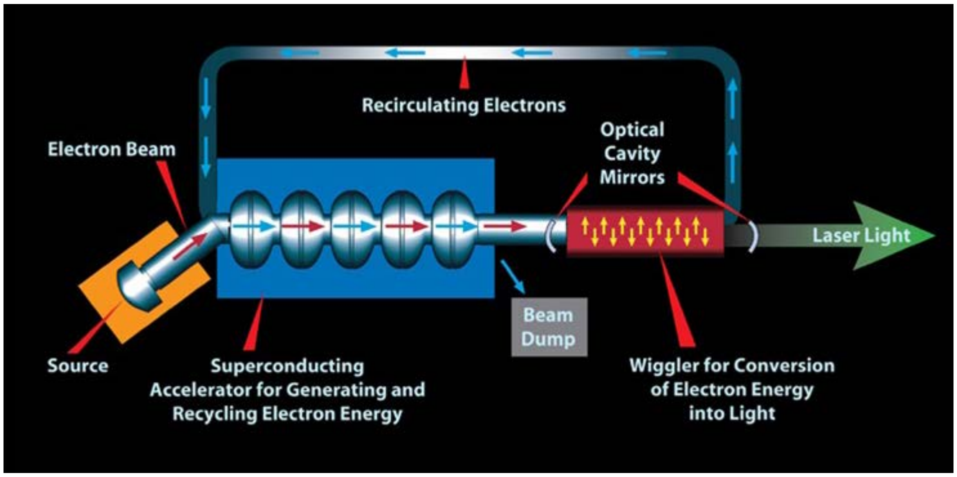

Recirculating Electrons
Electron Beam
Optical Cavity Mirrors
Laser Light
Beam Dump
Source
Superconducting Accelerator for Generating and Recycling Electron Energy
Wiggler for Conversion of Electron Energy into Light

Figure 3: A Simple Diagram Showing Accelerator Cavity and Permanent Magnet Wiggler for Extracting Light From Electrons *(Source: ONR)*.

THE POWER PROBLEM

Current prototype laser weapon systems and projected future systems require increasing levels of electrical power to generate the laser energy needed to defeat threats. Requirements for power range from low-power levels, needed for situational awareness and disrupt/defeat of short-range asymmetric threats, to high-power levels, needed for harder targets. As the power and range of laser technologies increase, so do the challenges to maintain input power, thermal management, and integration related to size and weight.

Power scale-up challenges are caused by low-efficiency, thermal management, and control issues. High input power, such as with megawatt-class lasers, requires tens of megawatts of input power to be provided by a platform in extremely short engagement timeframes. To accommodate the power demands of other platform subsystems, high-energy-density power storage solutions need to be explored. The increased power will cause thermal management issues in the laser diodes, optics, and couplers, as well as controls and switches. The power controllers and switches needed depend on the kill chain timeline, which determines duty-cycle requirements, transients, turn-on times, and load levelling. Current sea platforms have the ability to produce electrical power using different types of generators. Air and ground platforms rely on power pods and auxiliary generators while shore-based systems rely on grid or base power systems. Table 1 shows the power sources, current, and potential power for DEWs based on their application. For air, sea, and ground systems, power generation, platform integration, and thermal management are key issues.

Power for DEWs is also required for laser diode cooling and power conditioning, as well as illuminating, pointing, and tracking systems. The challenge is providing the power without impacting platform performance during HEL engagements.

The Navy has conducted studies through the Naval Postgraduate School [1–3] on energy storage options to address a notional ship firing multiple HEL shots without taxing the ship's electrical system. Several laser power levels were investigated on existing naval vessels. Energy storage options considered were batteries, capacitors, and flywheels. The study compared how quickly the stored energy can be used, the amount of energy stored for a given size and weight (energy density), size, weight, discharge, and recharge rate. The study concluded that a hybrid system comprising a generator, flywheel, and batteries was the preferred choice. Although current capacitors have extremely fast discharge and recharge rates, they were not selected because they do not have sufficient energy densities and are too large and heavy. There are numerous other storage solutions also being investigated for platforms, with some of these solutions having better energy storage capacities and being more compact.

A comparison of platform-type power requirements shows that power and thermal integration risks increase with increasing power and reduced platform size. Projecting heat off of the laser, through the platform, and into the environment at the requisite distribution and rejection rates is a challenge. Thermal acquisition challenges are constrained by proprietary capabilities and compounded by a lack of common interfaces for thermal subsystems. SSLs using laser diode pumps require specialized cooling technologies, which are currently limited to lower-power handling capability. The design of thermal management and transport systems needs to accommodate growth in system requirements for megawatt-class weapon and sensor systems such as distribution voltage increases.

Table 1: DEW Power Based on Application *(Source: ONR)*

Application		Power Source	Current → Potential Power
Sea		GTGs/Steam TGs Aux Generators Energy Magazine	kW → 10's MW
Combat Air		Power Pods Auxiliary Generators	kW →100's kW Class
Mobile Ground		Main/Aux Generators Energy Magazine	kW →100's kW Class
Shore		Grid Power On-base Power System	MW →10's MW

CURRENT AND FUTURE RESEARCH AREAS

The Office of Naval Research is conducting basic and advanced research to address many of the power-related challenges that DEWs face. The following list briefly states the various areas in which research is ongoing. Figure 4 depicts the research areas for various types of platforms in power generation, energy storage, and distribution and control.

- Development of compact power conversion technologies with wide band gap devices for higher voltage shipboard power distribution systems.
- Development of a power dense and efficient electrical backbone with dynamic reaction times.
- Investigation of dielectric materials for bidirectional power control modules and development of power converters and power management controllers.
- Development of components and methods to quickly detect and clear electrical faults and replace slow-acting circuit breakers and protective relays (thus enabling safer operation, reducing arc faults, and increasing the power density of the electrical system and overall power for mission loads).
- Development of high-power solid-state circuit breakers for shipboard power.
- Development of advanced power generation and energy storage technologies for lithium-ion batteries, fuel cells, and ultracapacitors.

- Development of multifunction and reconfigurable energy storage solutions for buffering pulse loads.
- Development of compact, large-format, module-level, high-density tactical energy storage technologies.
- Improvement of current fuel cell technology using novel membrane materials.
- Development of hybrid polymer/ceramic dielectric materials and devices, supercapacitors, and electrochemical capacitors for auxiliary power applications.
- Development of phase change heat transfer and materials with increased thermal conductivity for thermal management.

Future and emergent research areas include:

- Development and fabrication of boron carbide, boron nitride, and graphene for power electronics to enable higher voltages, frequencies, and temperatures.
- Identification/development of new materials with higher thermal conductivity and a lower cost than standard wide band gap semiconductor materials.
- Identification/development of manufacturing techniques that process materials to modify their surface structure to enable tailored heat transfer properties.
- Identification/development of new phase change substances that absorb heat by changing the phase of the material.
- Development of artificial intelligent controls using deep learning neural networks for load-leveling and high-power switches and controls.
- The use of photonic crystals and plasmonic sensors for diagnostic systems for high-temperature systems.
- Integrated modeling and simulation of the power and thermal management and controls systems as part of the platform.

CONCLUSION

DEWs will provide future platforms with the capability to protect themselves against current and future advanced, maneuvering, high-speed threats. Development of DEWs that will defend future forces against attacks by current and future high-speed maneuvering missiles, unmanned aerial vehicles, and small boats is underway. However, significant research

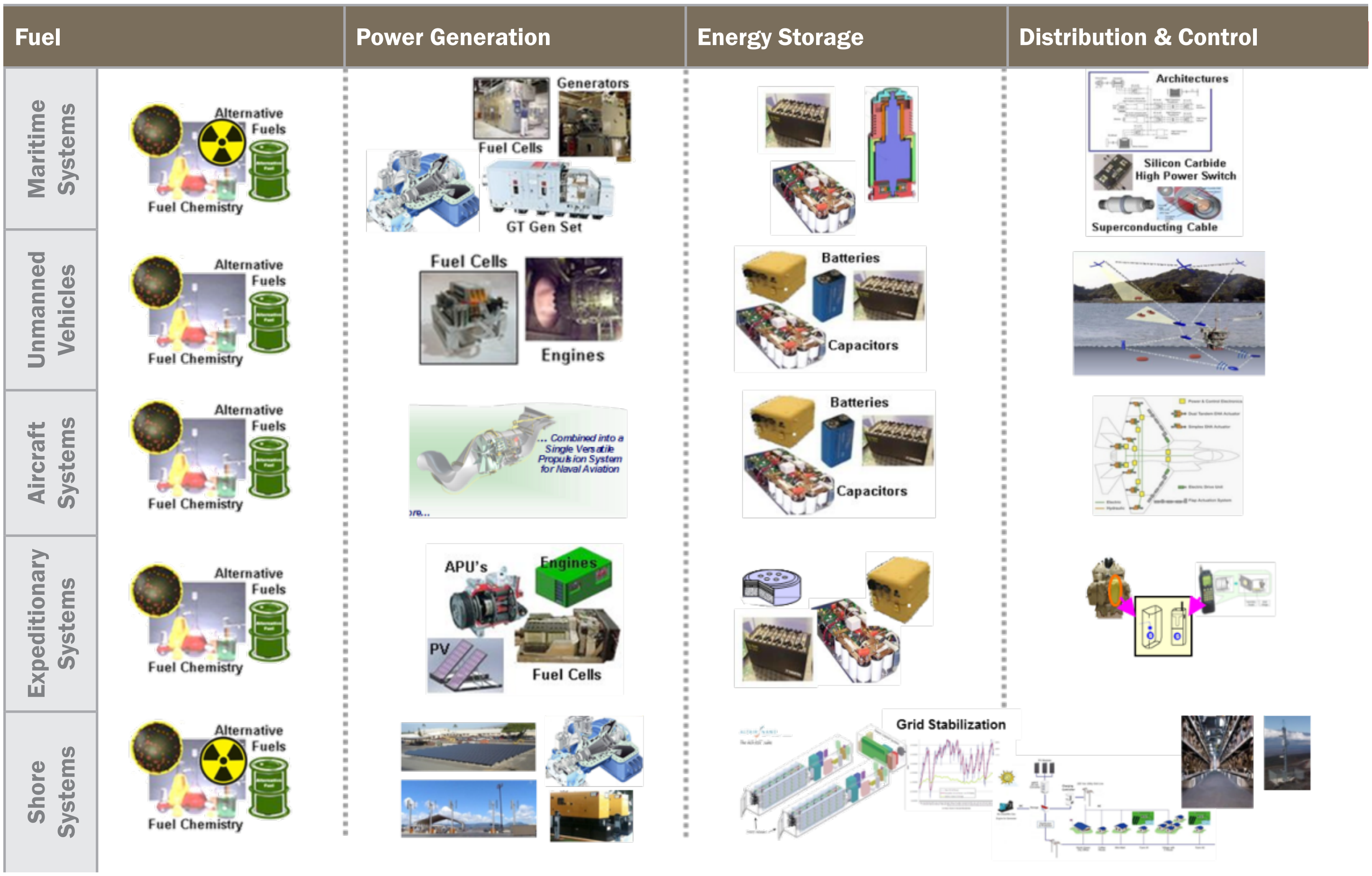


Figure 4: Power and Energy Technology Development Areas *(Source: ONR)*.

and development are still needed to ensure adequate power, energy, and thermal management is available for future DEWs. Namely, power control systems must be developed to handle the relatively high powers necessary for DEWs without affecting platform operations during a directed energy engagement. In addition, more research is needed on how to successfully integrate power, energy, and thermal management technologies into new and existing platforms, thus enabling the full capability of DEWs for the nation's defense. ■

ACKNOWLEDGMENTS

The author thanks Mr. Quentin Saulter from the Office of Naval Research (ONR) for his insights on the subject matter and for his review of and comments on this article.

REFERENCES

[1] Gattozzi, A. L., J. D. Herbst, R. E. Hebner, J. A. Blau, K. R. Cohn, W. B. Colson, J. E. Sylvester, and M. A. Woehrman. "Power System and Energy Storage Models for Laser Integration on Naval Platforms." Electric Ship Technologies Symposium, June 2015.

[2] Woehrman, Lt. Cmdr. Michael A. "Power Systems Analysis of a Directed Energy Weapon System for Naval Platforms." Master's Thesis, Naval Postgraduate School, Monterey, CA, 2013.

[3] Sylvester, Jeremy E. "Power Systems and Energy Storage Modeling for Directed Energy Weapons." Master's Thesis, Naval Postgraduate School, Monterey, CA, 2014.

BIOGRAPHY

SARWAT CHAPPELL is Program Officer for Weapons, Power and Energy at ONR's Sea Warfare and Weapons Department, leading the basic research of novel technologies for surface and undersea weapons, vehicles, power, energy, and thermal management. She has held numerous ONR positions in the areas of lasers and directed energy, including leading the Office of Secretary Defense (OSD) Atmospheric Propagation Sciences for High Energy Lasers (APSHEL) U.S.-India collaborative program and the OSD HEL-JTO Advanced Concepts Technology Area Working Group (AC TAWG). Ms. Chappell has also served as the ONR Program Officer for Directed Energy, as the Deputy Program Manager and the Lead Program Manager for the Free Electron Laser Innovative Naval Prototype (INP) program, and as the manager of the Applied Electromagnetics (APPEL) and initial Hyper Velocity Projectile (HVP) programs. Prior to joining ONR, Ms. Chappell was Chief Scientist for Naval Gunnery at Program Executive Office Integrated Warfare Systems (PEO IWS) and the PEO IWS Advanced Technology Director for all Surface Ship Weapons, and she also worked as an engineer at the Naval Surface Warfare Center Dahlgren Division. Ms. Chappell holds a bachelor's and master's degree in electrical engineering from Tennessee Technological University.

DEFENSE ACQUISITION UNIVERSITY (DAU)

Defense Acquisition University (DAU) is the Department of Defense's training arm for all things acquisition. Everything we do at DAU— including formal courses, on-line training, job aids, and consulting—is designed to help the acquisition professional develop and manage the acquisition programs, projects, and systems that make our nation's Warfighters the best-equipped armed forces in the world.

DAU CAN HELP YOU...

- ***Find Solutions -*** Some of the most sought-after resources we provide exclusively to the acquisition workforce are found in our Knowledge Center (www.dau.mil/library). Here, you will find curated information on defense programs, acquisition policy, and job support tools. Additionally, our Online Knowledge Repository (KR) for government acquisition workforce members will allow you to search periodicals or reach out to us using the Ask-a-Librarian services if you need further assistance.
- ***Understand Policy Updates -*** Policy changes can be robust and complex—it takes time to sort through updates and assess how they impact your situation. When new policies and guidance are released, organizations can request rapid deployment training for analysis and insight.
- ***Stay Current -*** Keeping up with acquisition policy and best practices is important. DAU can help. We constantly update curriculum and develop new courses and tools to give you access to the latest acquisition news, guidebooks, and communities anytime you want.
- ***Engage Senior Leaders -*** DAU is connected with defense, government, and industry acquisition leaders. Hot Topic Forums, Acquisition Training Symposiums, and other events provide numerous opportunities for acquisition workforce members to engage thought leaders while earning Continuous Learning Points (CLPs).

Visit DAU.mil for more information and dates for upcoming acquisition training events.

TARGETED RESEARCH SUPPORT

(https://identity.dau.mil/EmpowerIDWebIdPForms/Login/Krsite)

ASK A PROFESSOR

https://www.dau.mil/aap/Pages/default.aspx

ASK A KR LIBRARIAN

library@dau.mil

ACES:

DEVELOPMENTS IN CORROSION PREDICTION, TESTING, AND VALIDATION

By Derek M. Sabiston and
C. Thomas Savell

INTRODUCTION

Because military assets of the past, present, and future remain in use for decades after their initial production, corrosion will continue to be an important and costly issue for the Army and Department of Defense (DoD). According to an LMI study [1], the estimated annual corrosion cost in the Army alone is more than $3 billion, which is more than 12% of the Army's total annual maintenance cost. Corrosion is also attributed to an estimated annual 719,441 nonavailable days for Army ground vehicle, missile, and aviation assets. Furthermore, within the entire Department of Defense (DoD), the estimated annual corrosion cost is $20.6 billion and more than 1.1 million nonavailable days. This estimation is nearly 20% of the DoD's annual maintenance costs and more than 8% of the nonavailable days. Thus, effective corrosion prediction and prevention methods and tools can add immense value in helping to reduce life-cycle costs and prevent catastrophic failures to Army and other DoD systems.

CURRENT CORROSION TESTING AND VALIDATION

Currently, retrofits and new designs for Army vehicles are validated for corrosion performance by the Accelerated Corrosion Deterioration Road Test (ACDRT). Unfortunately, the ACDRT occurs relatively late in the design cycle, as it is performed on a fully operational vehicle after initial production has already begun. The ideal time to determine corrosion performance is during the initial design phases of the vehicle, as any design changes to improve corrosion performance can be made cheaply and quickly at this point in the process. On other hand, changes made at the time of the ACDRT are often costly and time consuming. The test itself is also expensive and relatively long, which can be made even worse if several tests need to be conducted due to design changes. The ACDRT has also been found not to mimic corrosion performance in the field for certain materials. However, the bottom line is that the ACDRT is the only corrosion test in existence for Army vehicles, and there is currently no full-scale vehicle modeling and simulation (M&S) tool for corrosion in use by the Army or other Services.

FUTURE CORROSION TESTING AND VALIDATION

Based on the current need for a relatively quick, easy, and cheap method for corrosion evaluation, the Accelerated

Corrosion Expert Simulator (ACES) system was developed. The first full-scale vehicle corrosion M&S tool for use by the Army or other Services, ACES is designed to predict the initiation and growth of corrosion on any asset over time. The system is able to simulate the coating and corrosion performance in a multitude of scenarios and can display any deterioration that occurs at defined time intervals. It can also be used to quickly and cheaply perform trade-off studies of possible design changes—such as alternative geometries, materials, or coatings—to determine how they affect the asset's corrosion performance.

The U.S. Army Tank Automotive Research, Development and Engineering Center (TARDEC) intends to use the ACES tool for new programs and any redesigns when possible. Other entities outside of the Army are also interested in using, or have already used, the tool. Currently, running an ACES simulation on Army programs is not mandatory, and full vehicle field corrosion testing (ACDRT) continues to be the basis for certification of new procurements. As the ACES tool continues to be improved, however, it is hoped that the use of such computer simulation will replace some, if not all, of the required physical testing.

At this stage in its development, ACES is simply used as an up-front, early-stage screening for corrosion issues. This limited usage is because there have been a number of corrosion issues where ACES was not able to successfully predict, or has mispredicted, the corrosion observed in the ACDRT or in the field. Once the simulator has matured to the point of achieving a 95% prediction success rate for the majority of the time, ACES will become the primary validation test for new designs and retrofits.

Once the simulator has matured to the point of achieving a 95% prediction success rate for the majority of the time, ACES will become the primary validation test for new designs and retrofits.

How ACES Works

ACES analysis begins with importing a full three-dimensional (3-D) computer-aided design (CAD) model of the vehicle, aircraft, ship, etc., together with the materials, coatings, and any ancillary information associated with every part. The user can then select preloaded scenarios in four different categories that relate to the vehicle, its operation, and its application. These categories are as follows:

- **Environment -** which includes temperature, humidity, salt, mud, ultraviolet (UV) exposure, vibration, chipping, etc.
- **Maintenance Activities -** which include washing, drying, lubrication, joint exercise, etc.
- **Operating Profile -** which includes ground time, storage, gravel roads, fording, loitering, takeoffs/landings, etc.
- **Accidental Contamination -** which includes animals, chemical spills, mercury, lavatory spillage, fire residue, etc.

Initially, ACES divides the vehicle into separate zones, each having its own specific environmental scenario, or microenvironment. This division is necessary because, for instance, a part in the engine compartment of a vehicle experiences a much different environment than a part on the roof. All of this information is used by ACES to determine the likelihood of corrosion occurring over time.

To date, ACES has gone through validations in the automotive and aviation fields, but the tool has the potential to be used in other applications as well (as illustrated in Figure 1 [2]).

To perform the corrosion analysis, the ACES tool uses a combination of procedural physics-based (electrochemical) and artificial intelligence statistical-based techniques. Figure 2 shows a schematic of the procedures and processing that occur within ACES.

Beginning on the right side of the figure, the 3-D CAD models are imported into the tool as a STEP AP214 file [3]. All of the materials, coatings, and ancillary data must be either imported with the STEP file, as separate Excel spreadsheets, or input by the user. The integrity of the geometry is then validated, ensuring there are no duplicate parts, parts without a defined geometry, or invalid geometry description. The geometry of the model is then analyzed to define part interactions. This geometry includes parts that are in physical contact as well as those within a certain distance (or "area of influence") of the selected part. Nearby parts can affect the corrosion performance of a selected part without being in direct contact; therefore, all of these interactions must be defined. All the information is stored in the working

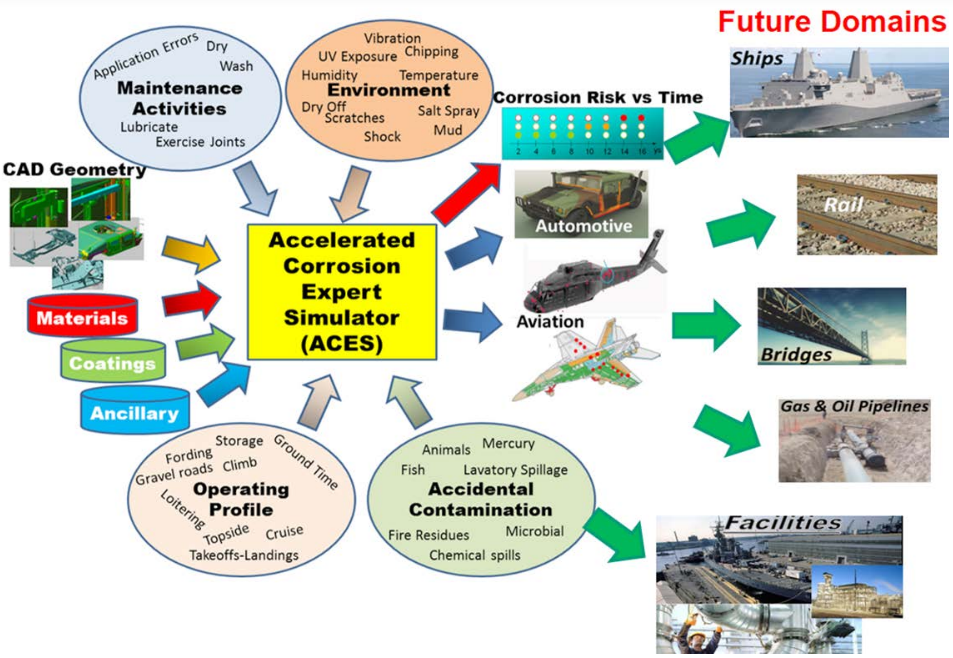


Figure 1: ACES Architecture [2].

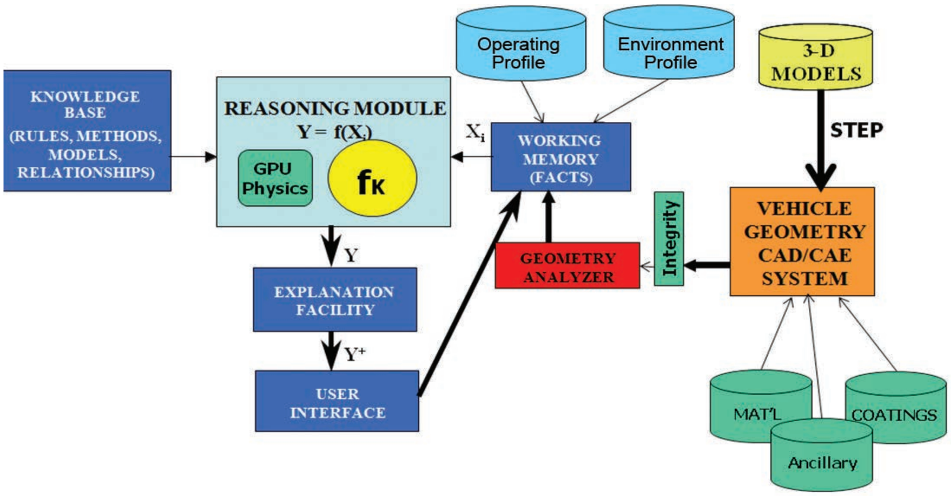


Figure 2: ACES Structure/Process Map [2].

memory, along with the user-defined scenarios (operating, environmental, etc., profiles).

The left side of Figure 2 represents the knowledge base of the tool, which includes the preprogrammed rules, methods, models, and relationships that are based on corrosion principles and that are used to perform the analysis on the information in the working memory.

The ACES tool's reasoning module uses the input information and its knowledge base to output the likelihood of corrosion occurring.

Benefits

The ACES tool has many possible benefits in its current configuration. First and foremost, it offers a fast and inexpensive review of corrosion vulnerabilities in new designs, as well as updates to old product designs. In this way, ACES can shorten the development phase of a product's life cycle by finding corrosion issues much earlier than waiting for the results from the ACDRT. Therefore, any changes to the product can be made earlier in the development, which is much easier, cheaper, and quicker to implement than waiting to make changes after the ACDRT is completed.

ACES can also assist with selecting geometric shapes and materials for optimal corrosion performance. A part's material and geometry can be changed and a new corrosion simulation quickly performed to demonstrate how that change will affect the corrosion performance of that part or area. ACES should also be able to help predict when corrosion-based maintenance needs to be performed and give an estimate as to the life expectancy of a part due to corrosion.

Overall, the use of ACES should lead to a more corrosion-resistant product that uses maintenance personnel more efficiently, thereby reducing the cost of maintenance and repair (and subsequently the "cost of corrosion"), with an improved system reliability and fleet readiness. Furthermore, additional benefits are expected as ACES continues to be upgraded and improved in the future.

The ACES simulator has undergone two phases of acceptance testing:

- Calibration testing by GCAS Incorporated, the company that developed the simulator.
- Third-party validation testing by Oshkosh Defense, a manufacturer of many Army and Marine Corps vehicles.

Calibration of the ACES Algorithms

The algorithms used in the ACES tool were first calibrated using ACDRT data from the Army's Family of Medium Tactical Vehicles (FMTV). In general, ACES correctly predicted the corrosion performance of most parts over time. There were two highly notable and impressive predictions.

The first was the successful prediction of severe corrosion of the T-handle door assembly, which initially suffered heavy corrosion on the T-handle itself and the carbon steel dish behind the handle (as shown in the top photo in Figure 3).

The middle drawing in Figure 3 is a cross section of the assembly with the material and coating information noted. The original design of the assembly was a die-cast zinc T-handle with electrophoretic paint (E-coat) and chemical agent resistant coating (CARC). The assembly also included a carbon steel pin, shaft, and washer; a zinc-plated carbon steel dish with an E-coat and CARC; and a carbon steel panel with no coating whatsoever. The interactions of the zinc-plated dish and die-cast zinc handle with the rest of the carbon steel parts, including some with no coating, caused galvanic and crevice corrosion of the handle and dish.

The ACES Version 0.9 correctly predicted these corrosion failures (as seen at the bottom of Figure 3 in the colorized likelihood of corrosion levels). Red-colored parts signify a severe level of corrosion, blue represents no corrosion, green represents an acceptable level of corrosion, and yellow (not pictured) represents a critical level of corrosion. The ACES predictions matched the experienced failures seen in the photo.

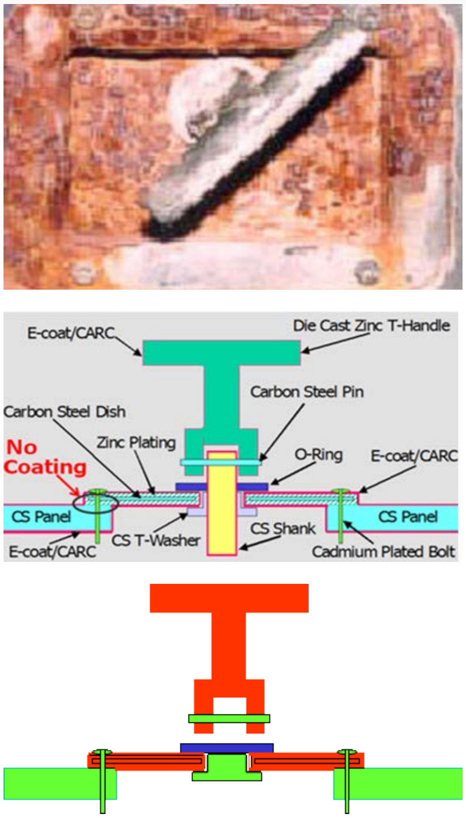


Figure 3: T-Handle Door Assembly Corrosion, Material/Coating Information, and ACES Prediction [2].

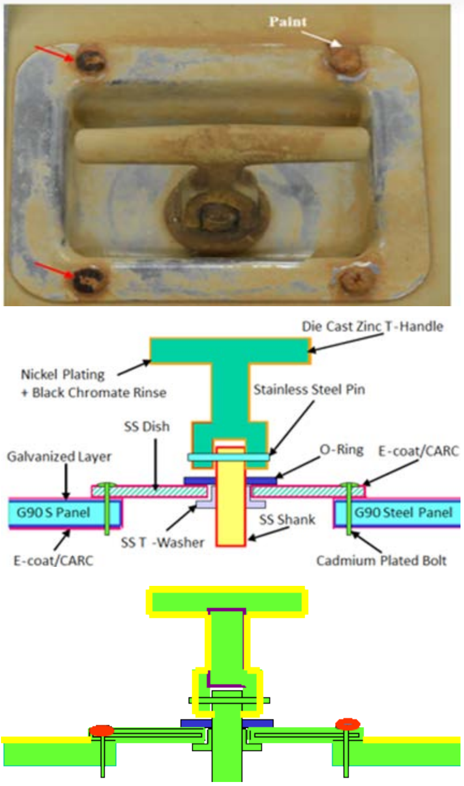


Figure 4: Redesigned T-Handle Assembly With Minimal Corrosion, New Material/Coating Information, and ACES Version 0.9 Correct Prediction [2].

Due to the corrosion failure of the initial design discussed previously, the T-handle assembly was redesigned (as shown in the middle drawing of Figure 4) to have a nickel-plated zinc handle and stainless steel dish, pin, shank, and washer. The steel door panel was galvanized, and an E-coat/CARC was added. The result of the redesign was significantly better corrosion performance. Both the ACDRT of the redesign (as shown in the top photo in Figure 4) and the ACES Version 0.9 prediction (as shown in the bottom of Figure 4) indicated that the only severe corrosion occurred on the bolts holding the dish.

Over time, new enhancements have been incorporated into the ACES algorithms with the expectation of improving the accuracy of the predictions. However, in the case of the T-handle door assembly, unexpected behavior occurred. Although the current version of ACES, Version 1.3, continued to correctly predict the corrosion of the original design (Figure 3), it now incorrectly predicts corrosion performance of the redesigned assembly. Figure 5 shows the current version incorrectly predicts unacceptable severe corrosion of the nickel-plated handle and the galvanized door panel. It also does not predict any corrosion of the bolts holding the dish, which were the only parts that did experience corrosion during the ACDRT retesting.

A second example of a highly successful prediction was the FMTV engine break. This assembly suffered a safety-critical failure due to its butterfly shaft seizing inside the part (as shown in Figure 6). This failure occurred due to galvanic corrosion from the stainless-steel butterfly shaft passing through the iron pillow block.

ACES Version 1.3 correctly predicted this failure as seen by the severe corrosion of the pillow block in Figure 7. This successful prediction highlights one of ACES benefits. If this issue could have been detected during the initial design phase of the product using ACES, significant time and money would have been saved by not waiting to discover the issue during the ACDRT.

One notable calibration case study where ACES was not successful in predicting the experienced corrosion during calibration was the FMTV aluminum transmission cooling shroud assembly (shown in Figure 8). The shroud suffered severe corrosion in two distinct areas:

- At the fastener interface, which failed due to galvanic corrosion from using steel fasteners on the aluminum shroud and from crevice corrosion under the fastener heads (left in Figure 8).
- In an area that created a water trap, allowing water to pool and act as an electrolyte in that area, thus causing the corrosion (right in Figure 8).

The ACES Version 1.3 prediction did correctly show the severe galvanic corrosion of the shroud and critical galvanic corrosion of the fasteners but did not predict the severe crevice corrosion that occurred under the fastener heads (as seen in the left photo in Figure 9). The crevice corrosion on the shroud was intensified by the electrolyte entrapment, which occurred due the geometry of the assembly.

These calibrations on the FMTV showed that the current version of ACES can

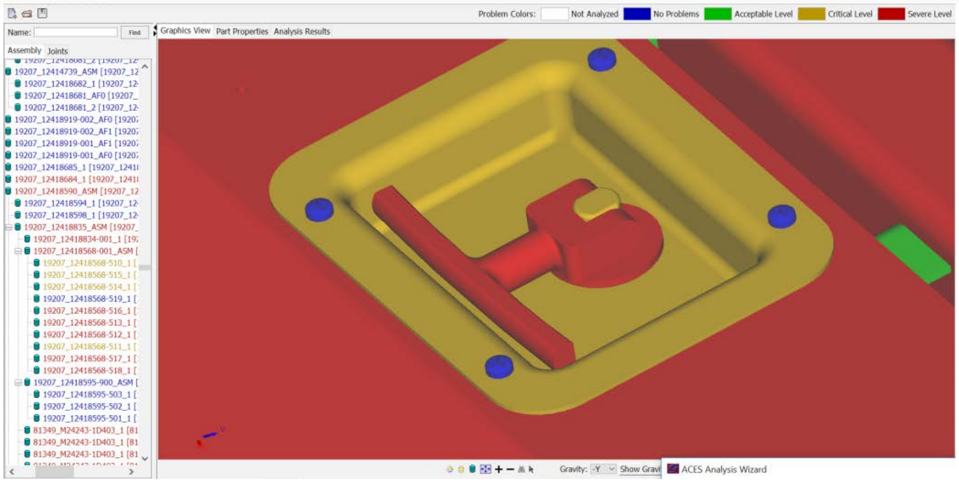


Figure 5: ACES Version 1.3 Incorrect Severe Corrosion Prediction of T-Handle and Door Panel [2].

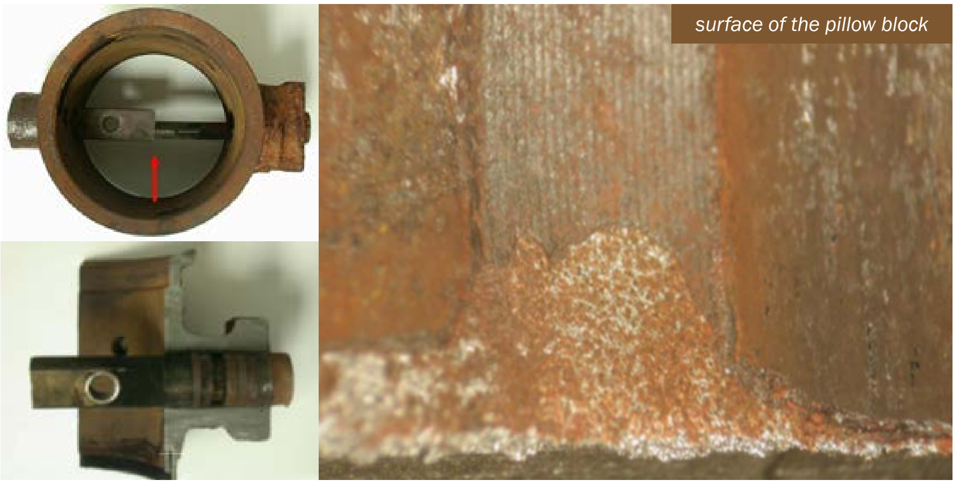


Figure 6: Engine Break Butterfly Shaft Seized Inside Iron Pillow Block [2].

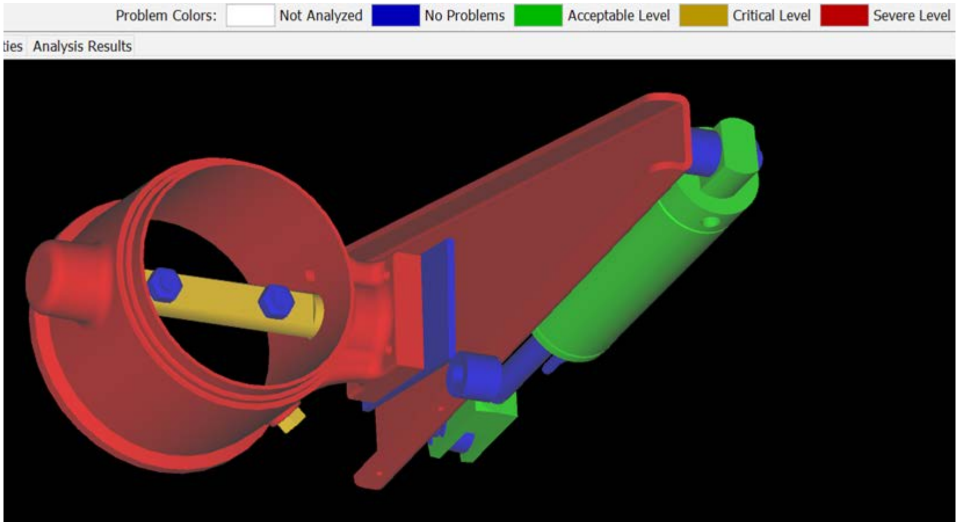


Figure 7: ACES Prediction of Pillow Block Corrosion (Severe) and Butterfly Shaft Corrosion (Critical) [2].

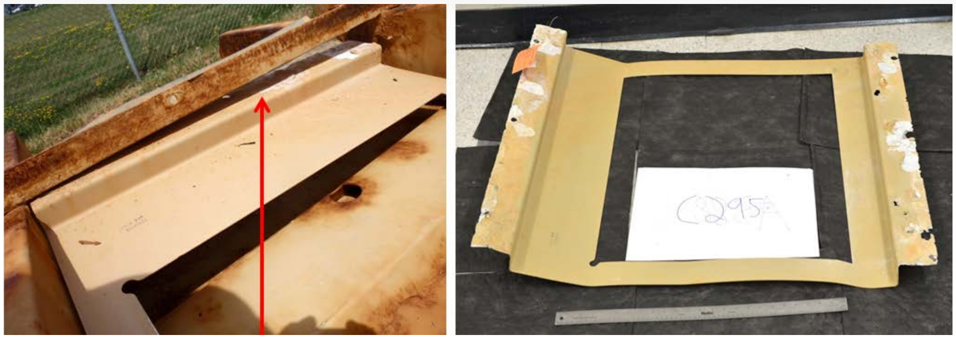
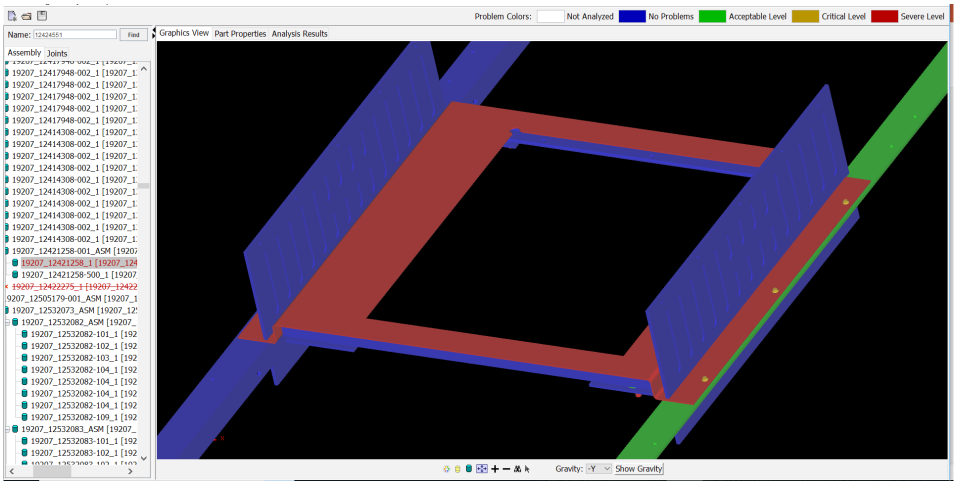


Figure 8: Transmission Cooling Shroud Crevice and Galvanic Corrosion at Bolted Joints and Water Entrapment Area [2].


Problem Colors: Not Analyzed No Problems Acceptable Level Critical Level Severe Level
Graphics View
Part Properties
Analysis Results
Assembly
Joints
Find
Gravity:
Show Gravity

Name: 12424551

19207_12417948-002_1 [19207_1
19207_12417948-002_1 [19207_1
19207_12417948-002_1 [19207_1
19207_12417948-002_1 [19207_1
19207_12417948-002_1 [19207_1
19207_12414308-002_1 [19207_1
19207_12414308-002_1 [19207_1
19207_12414308-002_1 [19207_1
19207_12414308-002_1 [19207_1
19207_12414308-002_1 [19207_1
19207_12414308-002_1 [19207_1
19207_12414308-002_1 [19207_1
19207_12414308-002_1 [19207_1
19207_12414308-002_1 [19207_1
19207_12414308-002_1 [19207_1
19207_12421258-001_ASM [19207
19207_12421258_1 [19207_124
19207_12421258-500_1 [19207
~~19207_12422275_1 [19207_12422~~
9207_12505179-001_ASM [19207_1
19207_12532073_ASM [19207_12
19207_12532082_ASM [19207_
19207_12532082-101_1 [192
19207_12532082-102_1 [192
19207_12532082-103_1 [192
19207_12532082-104_1 [192
19207_12532082-104_1 [192
19207_12532082-104_1 [192
19207_12532082-104_1 [192
19207_12532082-109_1 [192
19207_12532083_ASM [19207_
19207_12532083-101_1 [192
19207_12532083-102_1 [192

Gravity: -Y

Figure 9: ACES Prediction of Galvanic Corrosion of Cooling Shroud (Severe) and Fasteners (Critical) [2].

predict the corrosion of most parts on the vehicle, and significant success stories are noted, such as the engine break and the galvanic corrosion of the original T-handle door assembly. However, the latest version of ACES was not yet able to correctly predict galvanic corrosion of the nickel-plated T-handle, crevice corrosion of fasteners, and crevice corrosion due to water or electrolyte entrapment that occurred during the FMTV testing (which was used to calibrate its algorithms).

Validation Testing

After the calibrations of the algorithms were completed using the FMTV ACDRT, further independent "validation" testing was performed by Oshkosh Defense based on an ACDRT data of Oshkosh's Marine Corps Medium Tactical Vehicle Replacement (MTVR). Elzly Technology Corporation was employed to conduct corrosion inspections of the MTVRs and developed a list of 27 hotspots where corrosion most prevalently occurred. Oshkosh selected four different assemblies on which to perform ACES validation testing that encompassed 12 of the Elzly-defined hotspots. These four assemblies were the (1) frame, (2) air tanks, (3) cargo body, and (4) fuel tank straps. ACES validation testing on the cargo body and air tanks are still underway, but the tank fuel straps and frame validations have been completed.

The frame rail hotspot consisted of all the fasteners on the frame, which suffered from severe crevice corrosion (as shown in Figure 10). ACES Version 1.2 correctly predicted this crevice corrosion failure, but Version 1.3 did not, and the prediction algorithms for crevice corrosion of fasteners is one of the enhancements currently being worked for improvement.

The MTVR fuel tank straps suffered from uniform corrosion (as shown in Figure 11). This corrosion was correctly predicted by ACES (as seen in Figure 12, top). However, ACES incorrectly predicted the entire fuel tank to corrode due to galvanic corrosion (as indicated by Figure 12, bottom).

Based on the calibration and validation results, it was determined that several enhancements were needed to improve ACES and make it more accurate and reliable. These enhancements include adding a coating deterioration

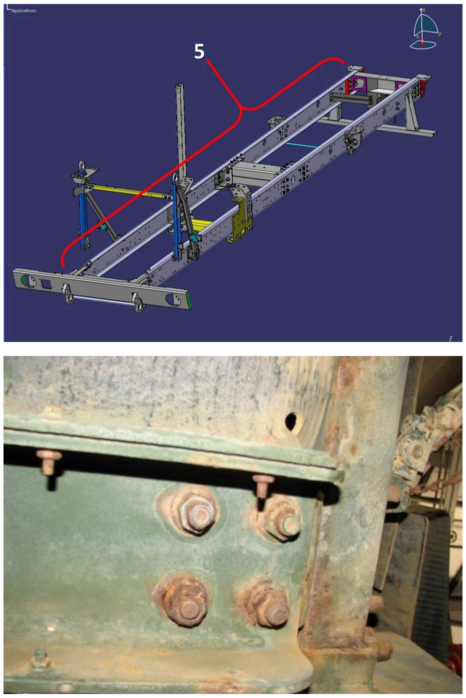


Figure 10. MTVR Frame Rail With Crevice Corrosion on Fasteners [2].

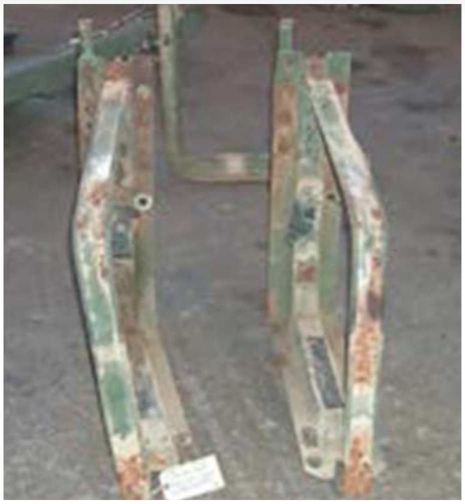


Figure 11: MTVR Corroded Fuel Tank Straps [2].

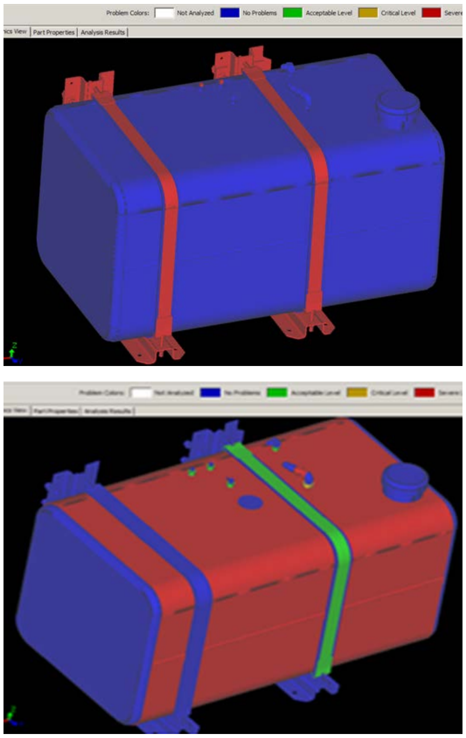


Figure 12: ACES Prediction of Severe Uniform Corrosion of MTVR Fuel Tank Straps (Top); Incorrect ACES Prediction of Severe Galvanic Corrosion of the Fuel Tank (Bottom) [2].

component, better handling of sacrificial coatings, adding crevice corrosion algorithms for fasteners (as well as other joint types), and predicting corrosion severity instead of just the likelihood of corrosion. Corrosion severity is how the Army rates corrosion in the ACDRT.

CONCLUSION

As discussed, the ACES simulator has the potential to be a highly useful tool in many fields—not only for military vehicles but also for aerospace, ships, bridges, rail, gas and oil pipelines, and facilities. And the Army believes that the tool will result in significant reduction in the future cost of corrosion and improvement in fleet readiness.

As the calibration and validation testing demonstrated, there are still areas of ACES that need to be improved, and improved prediction algorithms need to be added. Currently, the tool can acceptably predict galvanic, crevice, and uniform corrosion, but it has issues with certain areas, such as the crevice corrosion in fasteners. These issues will be addressed in the next release of ACES.

In addition, algorithms for the corrosion of joints, such as gaskets, spacers, moving joints, T-joints, sandwich joints, butt joints, and L-joints, need to be developed. Other needed enhancements include (1) the proper handling of sacrificial coatings, (2) the methods and logic for electrolyte accumulation/entrapment, (3) a video representation of corrosion progress over time, and (4) the changing of the output from the likelihood of corrosion to the Army corrosion severity levels.

A final future proposed enhancement is the addition of a knowledge acquisition facility within ACES, including learning algorithms for updating the tool's knowledge base—effectively making the tool a robust "Watson-like" prediction system. ■

REFERENCES

[1] Hertzberg, E., T. Chan, R. Stroh, and N. O'Meara. "The Estimated Effect of Corrosion on the Cost and Availability of Army Ground Vehicles." Report DAC21T2, LMI, February 2013.

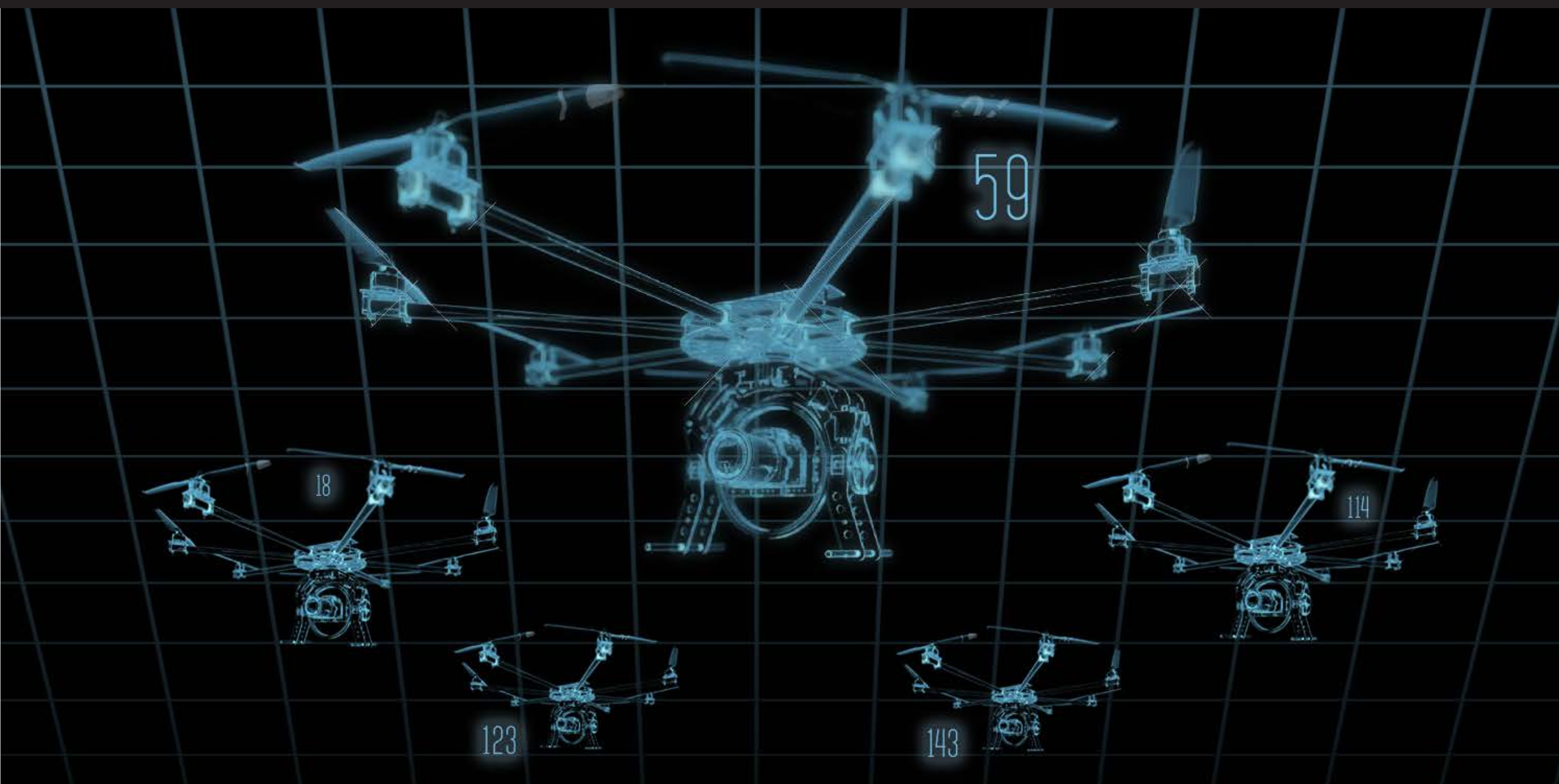
[2] Savell, C. T., S. Woodson, S. Porter, J. Repp, P. Ault, A. Thiel, and B. Hathaway. "ACES: A Simulation and Modeling Tool for Vehicle Corrosion." Paper, 2017 NDIA Ground Vehicle Systems Engineering and Technology Symposium, Novi, MI, 8–10 August 2017.

[3] Wikipedia. "ISO 10303." https://en.wikipedia.org/wiki/ISO_10303, accessed 11 January 2018.

BIOGRAPHIES

DEREK SABISTON has worked for TARDEC since 2012, including serving in the Materials Division for the past 4 years. His work in TARDEC's Metallurgy Lab includes conducting failure analyses, materials characterization, microstructural analyses, corrosion analyses, surface stress analyses, etc. In addition, he has several ongoing research projects in the areas of welding and residual stress, supporting the U.S. Army Tank-automotive and Armaments Command's PM Offices, other TARDEC teams, and industry partners. Mr. Sabiston holds a bachelor's degree in materials science and engineering from Michigan State University.

C. THOMAS SAVELL is the CEO of GCAS Incorporated and founder of its predecessor, DATA. His specialties and interest currently focus on predictive data analytics and artificial intelligence using a variety of statistical methods, such as Bayesian networks and expert systems. His experience also includes working for 13 years at General Electric (GE) Aircraft Engine Group, serving as the Group Manager of Analytical Aeroacoustics and Department Head of Dynamic Testing and Data Analysis, where he received GE's Young Engineer of the Year award. He also served as Director of Advanced Product Development at Solar Turbines International and as Technical Director for Structural Dynamics Research Corporation. Dr. Savell holds a bachelor's degree in engineering and mathematics from the University of Cincinnati, a master's degree in aerospace engineering from Georgia Tech, and a doctorate degree from the University of Cincinnati.



CYBER-PHYSICAL COMMAND-GUIDED SWARM

By Robert Cruise, Erik Blasch, Sriraam Natarajan, and Ali Raz

OVERVIEW

The Department of the Navy (DON) 30-Year Research and Development (R&D) Plan (distribution D), approved in January 2017, projects the key battlespace technological concepts. In 2025, these concepts are projected to extend from known systems, while by 2035 and 2045, the variety of these concepts are projected to be replaced by a single technological framework, including:

- Command-guided robotic-augmentation swarms.
- Swarm of swarms artificial intelligence (AI) warfare.

However, this article proposes that command-guided swarm (CGS) technology may be achievable much sooner, perhaps by the middle of the next decade, a full decade or two ahead of the DON R&D Plan. The two nations now dominating the AI field are, not surprisingly, the United States and China. If China fields single-human-operator CGS technology in 2025, a full decade before the DON intends, the U.S. position in multidomain warfare may be decisively compromised. This article also discusses an approach for R&D during the coming decade of a cyber-physical CGS.

BACKGROUND AND HISTORICAL PERSPECTIVE

A CGS is a multisensor, multiweapon, multiplatform, single-human-operator system-of-systems (SoS). The SoS is a multidomain force comprising multiple unmanned domain systems (UxS) (with x equaling space, air, ground, surface, or undersea), under the mission-oriented tactical coordination of a single human operator or *swarm tactician-supervisor*. The SoS is equipped for sensing plus kinetic/nonkinetic fires that, in concert, function as a single Warfighter's engagement capability. A single-human-operator CGS is a natural evolutionary end state of the original conception of a multisensor/multiweapon SoS discussed in the 1996 milestone paper "The Emerging U.S. System-of-Systems," by Adm. William Owens, Vice Chairman, Joint Chiefs of Staff [1].

Adm. Owens discusses a *revolution in military affairs* for intelligence, surveillance, and reconnaissance (ISR) and command, control, communications, computers, and intelligence (C4I). The concept consists of ISR (sensing and collection), advanced C4I (converting sensor awareness to battlespace understanding and mission formulation), and precision force (the resultant weapon control). Adm. Owens writes:

> *It is easy to miss the powerful synergy which exists between ISR, advanced C4I and precision force . . . . We tend to plan, program and budget for these things as if they were discrete capabilities. We are more adept at seeing the individual trees than that vast forest of a military capability which the individual systems, because of their interactions, are building for our fighting forces.*

The concept of a multisensor/multiweapon SoS was further clarified in 1998 by the late Vice Adm. Arthur Cebrowski—former president of the Naval War College and later director of the Department of Defense (DoD) Office of Force Transformation—with John Garstka in their seminal paper on network-centric warfare (NCW) [2]. To illustrate NCW, the authors discuss the Cooperative Engagement Capability (CEC), which is a multisensor data fusion system for surface ship air and missile defense that processes radar data from individual cooperating platforms and provides each cooperating platform the composite air track information. CEC also includes cooperative integrated fire control. Hence, Cebrowski and Garstka equate NCW with multisensor data fusion and with multi-weapon control data diffusion. They write:

If China fields single-human-operator CGS technology in 2025, a full decade before the DON intends, the U.S. position in multidomain warfare may be decisively compromised.

> *At the structural level, network-centric warfare requires an operational architecture with three critical elements: sensor grids and transaction (or engagement) grids hosted by a high-quality information backplane . . . . Sensor grids rapidly generate high levels of battlespace awareness and synchronize awareness with military operations. Engagement grids exploit this awareness and translate it into increased combat power.*

and

> *The cooperative engagement capability (CEC) combines a high-performance sensor grid with a high-performance engagement grid. The sensor grid rapidly generates engagement quality awareness, and the engagement grid translates this awareness into increased combat power . . . . The CEC sensor grid fuses data from multiple sensors to develop a composite track with engagement quality, creating a level of battlespace awareness that surpasses whatever can be created with stand-alone sensors. The whole clearly is greater than the sum of the parts.*

Both NCW and CEC concepts naturally culminate in a single-human-operator cyber-physical CGS tactical SoS, which leverages cutting-edge AI and advanced human partnering concepts to bring about *fusion of information* originating with the swarm's multiple sensors and *diffusion of control* out to the swarm's multiple platforms, sensors, and weapons. This article outlines a design and development approach for the AI and the advanced human-machine interface (HMI) to prototype such a swarm SoS within the next decade.

ADOPTION OF THE CYBER-PHYSICAL SoS (CPSoS) PARADIGM

In general, a CPSoS may be defined as an SoS [3],

> *where physical and software components are deeply intertwined, each operating on different spatial and temporal scales, exhibiting multiple and distinct behavioral modalities, and interacting with each other in a myriad of ways that change with context.*

The cyber-physical CGS SoS in particular is a complex network of software and digital hardware operating in cyberspace, with platforms, sensors, and weapons operating within the physical battlespace environment. (Note that the Internet of Things [IoT] is an instance of CPS that uses the Internet as its communications network. Cyber-physical CGS is an instance of CPS that does not use the Internet. Cyber-physical CGS and IoT are each an instance of a SoS [4].)

In the CGS case, the networking is wireless, adding additional complexity and interplay with the environment. The modeling and design of a CPSoS attempts to merge the discrete synchronized world of sequential programming with the continuous asynchronous world of physical laws. The differences between and within these two worlds present substantial challenges for the cyber-physical CGS design and verification. Further adding to these inherent challenges is the swarming operation of the CGS, where multiple component systems interact with each other and their human controller.

Table 1: Eight Overarching Challenges for Cyber-Physical CGS Design and Development

Coordinate Multiple Disciplines	Characterize Time
• Merge expertise in software, computer, radar, electro-optics, radio frequency (RF) communications, platform, weapon (both kinetic and electronic), human interface, and control engineering • Emphasize component dependencies via Model-Based Systems Engineering (MBSE) • Aggressive CGS SoS modeling essential for design plus test and evaluation (T&E)	• Reconcile discrete time of cyber components with continuous time of physical components • Reconcile instantaneous control assumptions with indeterminate software latencies • Reconcile time scales of target assessment and weapon control, with situation assessment and swarm force positioning, with threat assessment and mission planning
Guarantee Clock Synchronization	**Establish Real-Time Scheduling**
• Precisely synchronize control of sensors, weapons, and platforms • Determine clock drift design tolerances across entire cyber-physical CGS SoS • Maintain synchronization throughout multi-hour swarm missions	• Specify software timing constraints • Verify software synchronizations with the physical components • Formulate scheduling and coordination between sensing, information fusion processing, engagement resource planning, platform control, and weapon fires
Determine Component Interactions	**Design for Wireless Communications**
• Specify interactions among all cyber and physical components • Research asynchronous shared memory interaction design approach • Incorporate artificial intelligence agents that learn to mine data stores for appropriate input and generate suitable output for deposit in other data stores	• Design communications protocol to manage channel access, shared memory access, communication triggers, data/packet structures, routing plus network node hopping, and security • Maintain communications reliability despite RF or optical link degradation
Maximize Swarm Integrity	**Ensure Cyber Security**
• Cyber-physical CGS SoS performance maintained despite degradation, corruption, or failure of some of its cyber and physical nodes/components • Quantify component criticality and overall tolerance for degradation	• Cyber attacks threaten both cyber components and physical components (e.g., Stuxnet) • Traditional cyber security approaches cannot analyze attacks on the physical realm • Cyber security design augmented with systems theory to design effective attack countermeasures

Table 1 highlights the eight key challenges of cyber-physical CGS SoS design and development. Note that this table (which incorporates concepts and ideas presented by Rajkumar et al. [5]) excludes the many challenges of design/development of the cyber or physical components themselves and addresses only the critical overarching SoS issues.

ARCHITECTURE OF THE CYBER-PHYSICAL CGS SoS

The cyber-physical CGS SoS architecture centers on a population of semiautonomous intelligent agents operating in parallel, neither tightly coupled via a built-in command structure nor completely independent and autonomous. The CGS SoS is neither a rigidly orchestrated system nor an ensemble of statistically independent and autonomous functional entities, and therefore the SoS is an instantiation of what may be termed *organized complexity*. The regime between a highly structured SoS and an SoS populated by fully autonomous agents is the regime in which complex behavior may emerge. *Emergent complex behavior* forms the collective intelligence or *swarm intelligence* of the CGS.

The swarm intelligence of the CGS SoS arises from the distribution of information processing and engagement control across the SoS's AI agent population, from the use of active machine-learning technologies, and from the human-in-the-loop *User-Defined Operating Picture* (UDOP) interface that fully enables the human-machine partnership. The UDOP concept (illustrated in Figure 1) extends the *Common Operating Picture* (COP) such that the human operator is able to supervise the processing, exploitation, and dissemination of information for situation awareness. The UDOP allows rendering and visualization of data analytics services tailored to the operator's immediate needs for enhanced and efficient command decision-making within the context of the present mission state [6].

The *command-guided* nature of the swarm, as human-on-the-loop, means the resulting SoS is not completely autonomous but is under the real-time command of a single human swarm tactician-supervisor. The swarm tactician-supervisor functions at a high cognitive and decision-making level, establishing overall SoS mission objectives, providing mission direction, and routinely interjecting mission execution guidance/corrections, while delegating lower-level sensing and control functionalities to the constituent systems of the SoS. The constituent systems of the SoS are intelligent cyber-physical systems composed of multi-sensing and/or multi-control capabilities. Hence, rather than the human operator *interfacing* with the constituent systems via a fixed peripheral device, we say the operator is *infused* into the cyber-physical CGS SoS as the high cognitive and decision-making constituent.

A CGS method uses *AI agents*. In general, an AI agent mines data, processes information, and stores results in a distributed space. At the highest level of abstraction, the AI agents of CGS fall into one of three classes (shown in Figure 2): information fusion, control diffusion, and operator infusion.

The mining and processing of information that originates in the external environment is captured by an abstraction or class denoted `<information fusion>`. The disaggregation or decomposition or deconstruction of high-level mission objectives that originate with the human operator, coupled with the generation of plans and allocation of tasking out to specific constituent systems of the SoS, is captured by a high-level abstraction denoted `<control diffusion>`. This theoretical framework leverages control theory's representational *duality between observation and control*, which is manifested in CGS by the representational duality between the abstractions of `<information fusion>` and `<control diffusion>`. The third high-level abstraction, denoted `<operator infusion>`, within CGS places a human-on-the-loop for interpreting/assessing processed information/data, establishing mission objectives or making engagement decisions, and interacting within CGS for purposes of machine learning (ML) and fusion/diffusion augmentation/refinement.

The cyber-physical CGS SoS architecture challenge arises when multiple UxS (with x again equaling space, air, ground, surface, or undersea) comprise different classes of CGS agents and operate in a swarm to accomplish the mission objectives while infused with the UDOP. The CGS SoS architecture defines the swarm operation and its behavior by specifying the information flow and interactions between the CGS agents, between the UxS, and the single human operator. Using the three AI agent classes previously described, Figure 3 illustrates three conceptual architectures for the single human guided cyber-physical CGS SoS

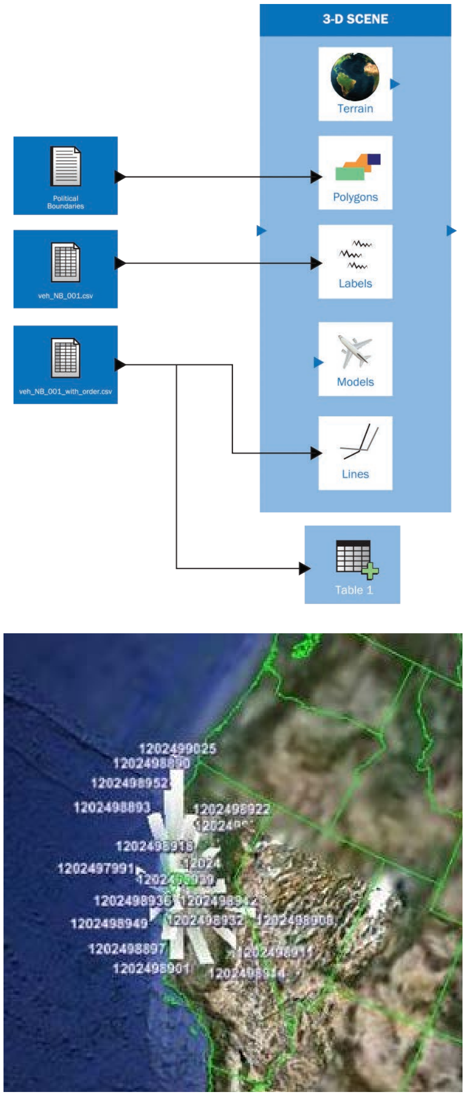


Figure 1: UDOP *(Source: NSWC)*.

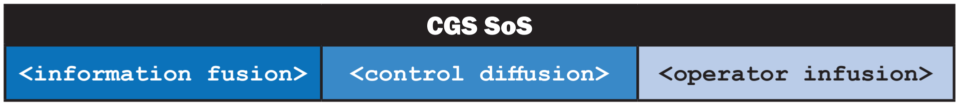


Figure 2: CGS SoS Intelligent Agent Types.

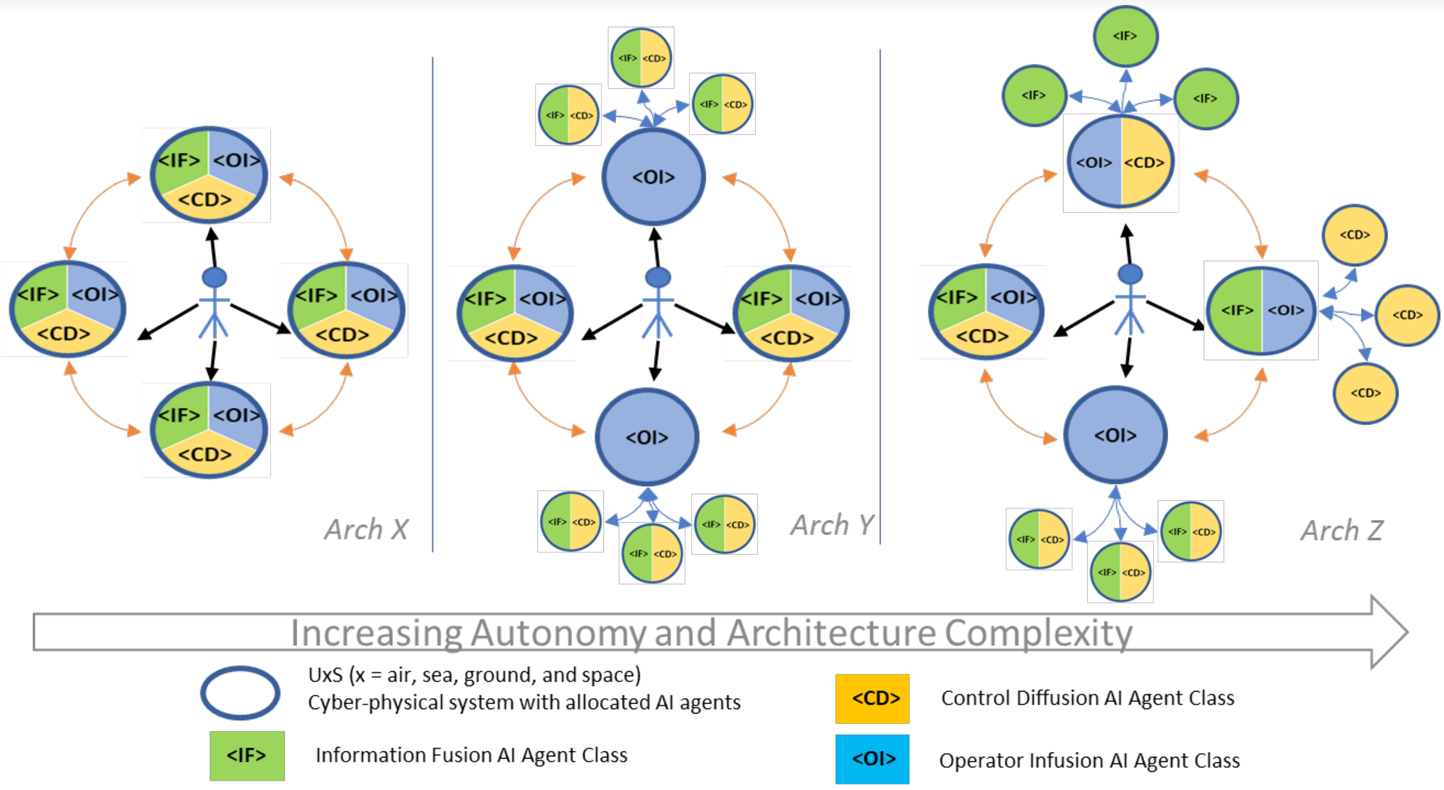

<IF>
<OI>
<CD>
Arch X
Arch Y
Arch Z
Increasing Autonomy and Architecture Complexity
UxS (x = air, sea, ground, and space)
Cyber-physical system with allocated AI agents
<IF> Information Fusion AI Agent Class
<CD> Control Diffusion AI Agent Class
<OI> Operator Infusion AI Agent Class

Figure 3. Conceptual Cyber-Physical CGS SoS Architectures *(Source: NSWC)*.

derived from the information fusion SoS architecting described in Raz et al. [7].

Each architecture in Figure 3 represents the capabilities of the individual UxS, their relationship to the human commander, and the information exchange among the UxS. The purpose of this figure is to highlight that a variety of SoS architectures can be conceived by varying the autonomy and information exchange of the cyber-physical systems within the swarm. These architectures differ in multiple dimensions in their construction, operation, and exposed opportunities that the human-commander could exploit from varying allocations of AI agents to the different UxS. Although the design and development of the AI agents that provide the CGS functionality is of significant importance, these architectures introduce a myriad of operational considerations and SoS challenges for fielding the CGS. To provide a timely tactical capability, it is imperative to develop a CGS SoS-level design and analysis capability alongside the development of the individual AI agents.

The objective of CGS SoS design and analysis is to characterize the emerging swarm behavior due to interactions of the AI agents, as well as identify architectures that maximize the CGS advantage under both normal and contested operating conditions. The SoS analysis directly addresses the key challenges for the CGS design and development discussed previously in Table 1 and describes the drivers and the root-causes of the resulting swarm behavior, which are then attributed to the design of AI agents, allocation of AI agents to UxS, and the CGS SoS architecture. Examples of the overarching questions that fall under the CGS SoS design and analysis are:

- Who should determine the critical systems, and what is the appropriate approach to studying the integrity of the swarm?
- What conditions can violate the swarm integrity, and how can those violations be mitigated by AI agent design and/ or dynamic configuration of the cyber-physical CGS SoS architecture?
- To what extent should CPSoS theory be applied to existing systems interacting with the CGS SoS?
- When and how do faults (cyber, physical, functional, malicious intent) propagate through the CGS SoS architecture?
- Why and how do the performances of different CGS SoS architectures vary (i.e., what design features and interactions of the individual AI agents lead to what emergent behavior)?
- How autonomous, robust and resilient are different CGS SoS architectures?

The tactical capabilities enabled by the cyber-physical CGS will depend upon the answers to SoS-level analysis. Nevertheless, at the core of the CGS SoS functionality are the AI agents for information fusion, control diffusion, and operator infusion. The design of these agents using ML and statistical reasoning is described next.

AI AGENTS OF THE `<information fusion>` CLASS

ML is a type of AI. Learning machines may be roughly categorized into six broad model types, shown in Table 2.

Symbolic ML, based on first-order logical models, allows for highly expressive representations of possible worlds, is excellent for implementing machine reasoning, and is able to provide the human operator with the steps in its logical reasoning. Symbolic models are the basis of what has been termed *good old-fashioned AI* (GOFAI). However, a first-order logic knowledge base is brittle in that sentences are either true or false, with no possibility of compromise. When logical systems fail, they do so blatantly or catastrophically. The problem of catastrophic failure has led to what has been termed the “AI Winter,” a period noted for its lack of progress in developing a true artificial intelligence.

> The command-guided nature of the swarm means the resulting SoS is not completely autonomous but is under the real-time command of a single human swarm tactician-supervisor.

Another important issue is that learning these models is nontrivial as the search space includes multiple levels of abstraction.

On the other hand, probabilistic ML, based on probabilistic graphical models, avoids this brittleness by softly modeling relationships as conditional probability distributions. Yet, while offering robustness not found in logical models, probabilistic models lack the rich representations and reasoning prowess of logic.

ML for the CGS agents of the `<information fusion>` class is based on a novel hybrid of symbolic and probabilistic ML. This hybrid ML approach combines Bayesian graphical models with first-order logic, which in the AI research community is referred to as statistical relational learning (SRL). Within the SRL approach, logical symbolic representations capture the underlying rich structure of the problem domain, while the probabilistic methods manage the uncertainty and error in the data. There has been immense and real success for these SRL models both from the learning perspective and from the reasoning perspective. State-of-the-art methods inspired from ML have been applied to solve real problems, including natural language understanding, image processing, and biomedical sensing problems.

Recently, the logical reasoning has been replaced with database systems to scale learning to petabytes of data. Bringing in the contextual information from big data analytics, the CGS SRL approach uses probabilistic, symbolic, and contextual information. Recently, the Defense Advanced Research Projects Agency (DARPA) has identified the future of AI in contextual adaptation to explain situations. The CGS SRL approach to information fusion falls within DARPA’s “third wave” in the historical

Table 2: Various Types of ML

MACHINE LEARNING APPROACHES		
NAMES	**DEVICES**	**APPROACHES**
Symbolic	Logical statements	Data analysis using propositional logic, first-order logic, and truth tables
Probabilistic	Probabilistic graphical models	Data analysis using Bayesian statistics, conditional probabilities, and networks of nodes
Connectionist	Artificial neural networks (ANN), multilayer ANNs (deep learning)	Data analysis using computational model inspired by neural architecture of the biological brain
Analogistic	Support vector machines (SVM), kernel methods	Analysis of data analogies and similarities via distance computations in feature hyperspace
Evolutionary	Genetic algorithms, genetic programming	Data analysis using computational model inspired by evolutionary competition and survival
Possibilistic	Fuzzy inference systems	Analysis of ambiguous data using expansion of classical logic to accommodate partial truths

development of AI, illustrated in Figure 4.

AI AGENTS OF THE <control diffusion> CLASS

Dual to the observational information processing side of AI is the planning side of AI that implements the concept of control diffusion. A tactical swarm SoS engages with its environment and by definition is equipped with multiple engagement capabilities: effectors, sensors, and platforms. The swarm SoS must dissect, deconstruct, or decompose its high-level mission objectives into specialized tasking or actions for each of its many engagement capabilities. This disaggregation and deconstruction and decomposition of high-level mission objectives, coordinated with the allocation or diffusion of tasking/actions out to specific engagement capabilities, the constituent systems of the CGS SoS, is captured by the concept of control data diffusion.

Control data diffusion is implemented by enabling an AI to undertake *planning*. Planning is an AI's effort to generate a sequence of actions based on observations. At its simplest, AI planning is implemented as a search-based agent. The agent searches the space of all possible action sequences to select the optimal sequence that reaches the goal. To make the search more efficient, a *heuristic function* that reduces the size of the search space may be computed using various techniques. In many cases, applying a good computed heuristic to the search problem will produce a reasonable estimate of the exact planning solution.

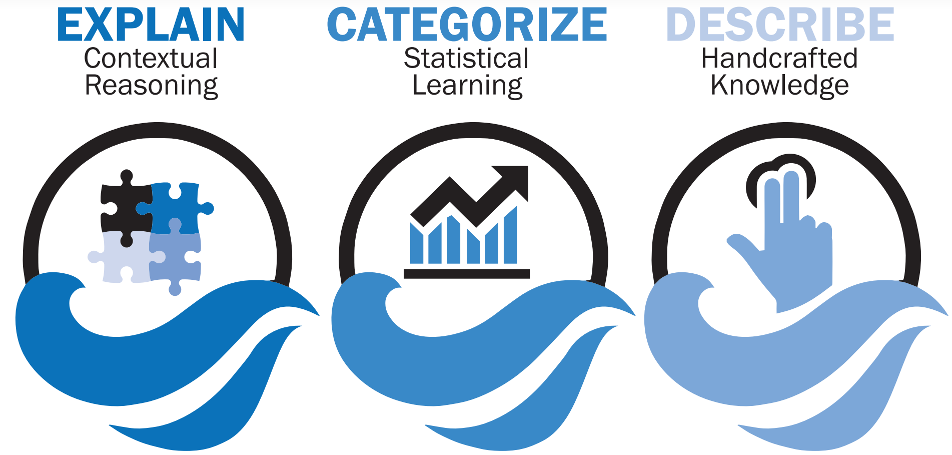


Figure 4: DARPA's Three Waves of AI *(Source: NSWC).*

Because the aforementioned planning approach seeks a single linear sequence from start to goal, it is termed *total-order planning*. A principal disadvantage of total-order planning is its inability to break or decompose the planning problem into separate subproblems. Alternatively, the approach termed *partial-order planning* does break the problem into subproblems, some of which may be solved in parallel. A partial-order planning solution forms a graph or network of actions as opposed to the linear sequence of actions of total-order planning.

The decomposition idea employed in partial-order planning may be carried further using a hierarchical approach. In *hierarchical task network* (HTN) planning, the highest-level action in the hierarchy is an overarching description of what is to be accomplished, which at the start of a CGS mission is the set of mission objectives. Via the process of *action decomposition*, each higher-level action is decomposed into a plan consisting of several lower-level actions, such as decomposition of overall mission objectives into detailed mission plans. The decomposition process continues down the hierarchy to lower levels, such as individual sensor management, and down to the lowest level of primitive actions. These *primitive actions* are the actuator/servo control signals transmitted directly to effectors, sensors, and platforms. Hence, the HTN planning process *diffuses* or fans out the high-level mission objectives to the swarm's constituent systems, terminating in these lowest-level control signals for individual effectors, sensors, and platforms.

AI AGENTS OF THE <operator infusion> CLASS

Because of the complexity of the cyber-physical CGS SoS, the interfacing for the swarm tactician-supervisor differs from the traditional COP and hand controls. The UDOP interface affords the human operator to reconfigure the interface in real time and throughout mission execution, thereby tailoring his/her information exposure not only to high-level threat summaries and projections but also to instantaneous states of affairs or situations and to individual object states/tracks, depending upon the nature of the mission and the immediate stage of mission execution. In the dual sense, the UDOP enables the human operator to focus his/her decision-making at the highest level of establishing/updating mission objective, or to expand and extend his/her decision-making involvement to include details of instantaneous coordination/integration among engagement groups within the swarm, or even to decision-making down at the level of individual sensor/weapon/platform management. This rich human operator access to, and interaction with, the entire CGS SoS suggests the human operator is *infused* into the SoS.

In conjunction with the UDOP paradigm, the operator infusion agents implement recent AI and ML innovations to accomplish true partnering of the human operator with the CGS intelligence. One typically thinks of ML as the processing of preexisting training data during system development. Yet the idea of machine learning may also be applied to accomplish the interaction and partnering between the swarm tactician-supervisor and the CGS SoS. One of the key advantages of a symbolic representation such as first-order logic is the representation of knowledge in a format that facilitates human interaction with the AI. Specifically, this human interaction may include a human *advising* the CGS SoS throughout mission execution [8].

The SRL process may be augmented to accept and exploit advice from a human domain expert; thereby infusing the operator into the swarm. This capability may be extended not only to any probabilistic logic learning model for accomplishing information fusion but also to any HTN planning model for accomplishing control diffusion.

Taking this ML approach a bit further, ML may also be accomplished via *active advice-seeking* by the machine [9], by which the CGS SoS solicits advice from its human operator throughout mission execution. The upshot is that ML by the swarm, in part, becomes a responsibility of the swarm tactician-supervisor, both in garrison and throughout the execution of missions. In other words, the Warfighter's role is an advisor and teacher to his/her cyber-physical CGS SoS, and this role is the basis of the human-swarm partnership.

CONCLUSION

The future of autonomous swarms promises to leverage numerous AI techniques that can help provide situational awareness, require fewer Warfighters, extend mission operations, and respond to ever-changing conditions. As part of this future, probabilistic, symbolic, and contextual information will be used to support a cyber-physical single-human-operator CGS SoS for multidomain operations. And whether it takes three decades or less than one to successfully field technologies such as these, it continues to be critical for the U.S. military to aggressively pursue these technological advancements and maintain its dominance in multidomain warfare. ■

REFERENCES

[1] Owens, W. A. "The Emerging U.S. System-of-Systems." National Defense University, Institute for National Strategic Studies, Strategic Forum, no. 63, February 1996.

[2] Cebrowski, A. K., and J. J. Garstka. "Network-Centric Warfare: Its Origin and Future." *Proceedings*, vol. 124, no. 1, pp. 28–35, U.S. Naval Institute, 1998.

[3] Khaitan, S. K., and J. D. McCalley. "Design Techniques and Applications of Cyberphysical Systems: A Survey," *IEEE Systems Journal*, vol. 9, no. 2, June 2015.

[4] Henshaw, M. "Systems of Systems, Cyber-Physical Systems, the Internet-of-Things . . . Whatever Next?" *Insight*, Wiley Online, vol. 19, no. 3, October 2016.

[5] Rajkumar, R., D. de Niz, and M. Klein. *Cyber-Physical Systems*. Addison-Wesley Professional - Pearson Education, Inc., 2017.

[6] Blasch, E., E. Bosse, and D. A. Lambert. *High-Level Information Fusion Management and Systems Design*. Boston: Artech House, 2012.

[7] Raz, A. K., Kenley, C. R., and DeLaurentis, D. A. "A System-of-Systems Perspective for Information Fusion System Design and Evaluation." Information Fusion 35 (2017): 148-165.

[8] Odom, P, T. Khot, and S. Natarajan. "Learning Probabilistic Logic Models with Human Advice." The Association for the Advancement of Artificial Intelligence Spring Symposium on Knowledge Representation and Reasoning, 2015.

[9] Odom, P., and S. Natarajan. "Active Advice Seeking for Inverse Reinforcement Learning." International Conference on Autonomous Agents and Multiagent Systems, 2016.

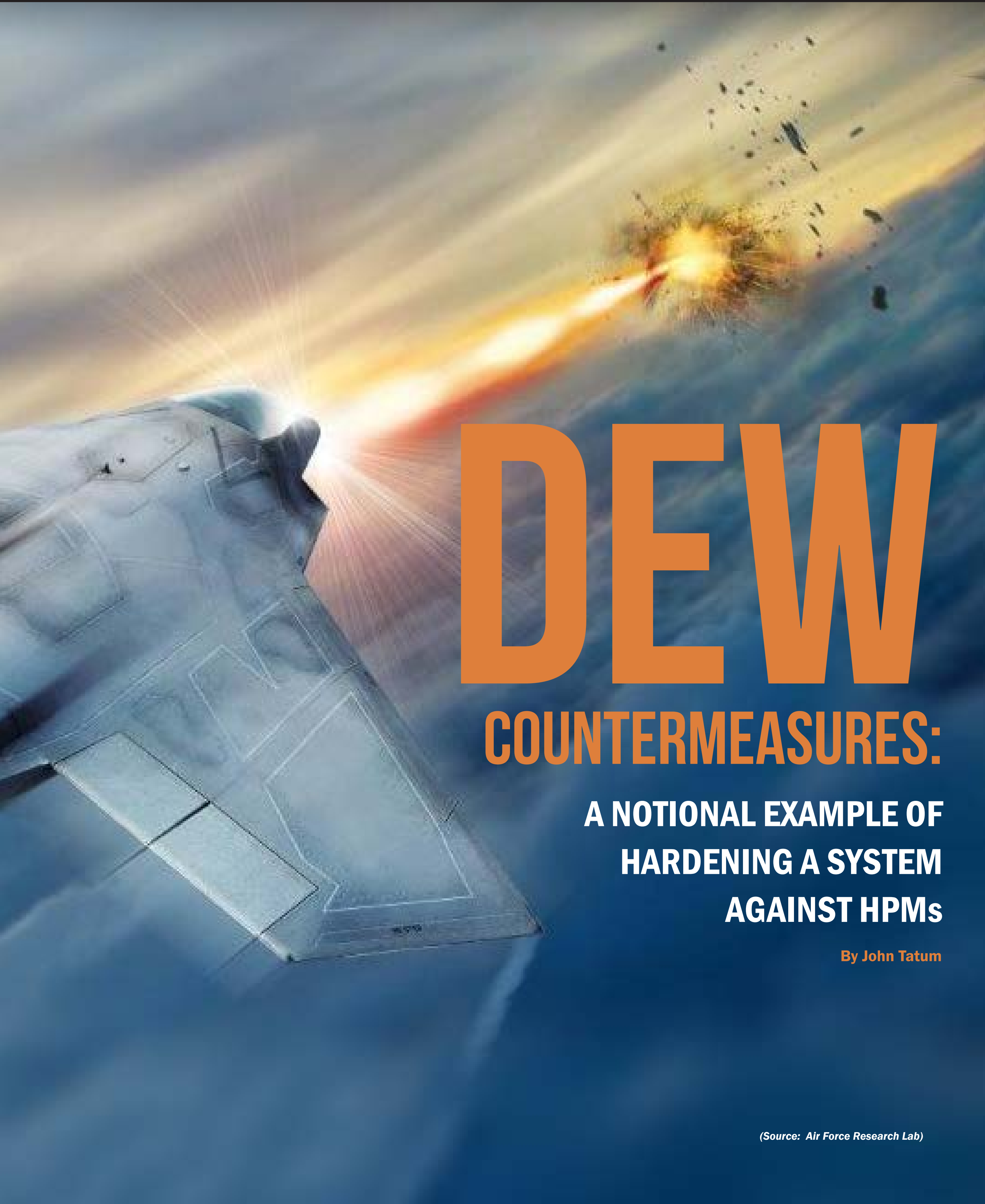
BIOGRAPHIES

ROBERT CRUISE is currently a research scientist at the Naval Surface Warfare Center (NSWC), Crane Division. His research focuses on information fusion, control diffusion, the application of machine learning and robotic control technologies to fusion/diffusion, human-in-the-loop interfacing with complex fusion/diffusion systems of systems, and test and evaluation of complex fusion/diffusion systems of systems. Previously, Dr. Cruise served as an engineer/scientist for the SIGINT Software Defined Radio Laboratory at NSWC Crane, the Ground-Based Operational Surveillance System project for the Marine Corps and Army, the Marine Corps Mortar Fire Control System project, and several Office of Naval Research fires and fire control projects. Dr. Cruise has bachelor's degrees in physics and electrical engineering from Notre Dame; an MBA from the University of Chicago; and a Ph.D. in theoretical nuclear physics from Indiana University, with Ph.D. minors in applied mathematics and computer science.

ERIK BLASCH is a program officer at the Air Force Office of Scientific Research, supporting research in dynamic data-driven applications systems. He has been with Air Force Research Laboratory as a civilian and reservist since 1996, compiling 700+ scientific papers and 19 patents. Dr. Blasch is also the author of multiple books and is a SPIE and IEEE Fellow, as well as an AIAA Associate Fellow. He earned a bachelor's degree in mechanical engineering from MIT; master's degrees in mechanical, health science, and industrial engineering (human factors) from Georgia Tech; and an MBA, master's degrees in electronics and economics, and a doctorate in electrical engineering from Wright State University. He is also a graduate of the Air War College.

SRIRAAM NATARAJAN is an Associate Professor at the Department of Computer Science at the University of Texas Dallas and is on leave as an Associate Professor of Informatics and Computer Science at Indiana University. He was previously an Assistant Professor at Indiana University and the Wake Forest School of Medicine, as well as a post-doctoral research associate at the University of Wisconsin-Madison. His research interests lie in the field of AI, with emphasis on machine learning, SRL, reinforcement learning, graphical models, and biomedical applications. Dr. Natarajan is an editorial board member of the MLJ, JAIR, and DAMI journals and is the electronics publishing editor of JAIR. He has also helped organize/lead multiple key AI, SRL, and other workshops. Dr. Natarajan holds a Ph.D. from Oregon State University

ALI RAZ is a research scientist at Purdue University's Center for Integrated Systems in Aerospace. His research interests are in complex systems, system-of-systems engineering, and information fusion. He has worked at the John Hopkins University (JHU) Applied Physics Laboratory and the DoD in the area of fusion performance evaluation. He was the recipient of Alexander Kossiakoff fellowship awarded by JHU and the International Council on Systems Engineering (INCOSE) for developing performance evaluation methods for large-scale system-of-systems in defense applications. Dr. Raz holds bachelor's and master's degrees in electrical engineering from Iowa State University and a doctorate in aeronautics and astronautics from Purdue University. He is also a certified INCOSE systems engineering professional.



DEW COUNTERMEASURES:

A NOTIONAL EXAMPLE OF HARDENING A SYSTEM AGAINST HPMs

By John Tatum

(Source: Air Force Research Lab)

INTRODUCTION

Directed energy weapons (DEW)—which include high-energy lasers (HELs), high-power radio-frequency (RF)/microwaves (HPMs) and particle beam weapons—pose a potentially high-risk threat to U.S. sensors, communications, and weapon systems. Several foreign countries are currently interested in and are developing DEW systems. The Department of Defense (DoD) is concerned that DEWs could attack friendly personnel, facilities, and/or equipment with the intent of degrading, neutralizing, or destroying their capability. Figure 1 shows some examples of DEW applications for land, air, space, and sea. The red lines depict the HEL beam, and the curved lines represent HPM energy.

HELs are high-powered light sources combined with optics that are designed to focus the beam of light on a target and create sufficient heat to burn holes in the outer skin. HELs can be chemical-based or solid state, including bulk and fiber optics. Advances in solid state and fiber-optic lasers in recent years make them a potential game changer on the battlefield. HELs have the potential to attack targets with the speed of light and typically operate at wavelengths that are outside the visible range of the human eye. HELs can be mounted on ground, air, or space vehicles to attack targets.

HPM weapons are high-power RF/microwave transmitters that are combined with antennas to direct energy at a target and produce electronic upset or permanent damage depending upon the distance between the HPM source and the target. HPM weapons can operate in any weather condition, and their beams are typically much wider than a laser beam, which increases the probability of target hit. HPM weapons produce their effects by coupling energy into a target system via intentional antennas (i.e., front doors) and unintentional antennas (i.e., back doors) and transferring the energy to sensitive semiconductor components.

RF DEWs include HPM, electromagnetic (EM)/RF weapons, non-nuclear EM pulses, and electronic bombs (E-bombs). They provide a Warfighter with the capability to attack electronic targets, with and without antennas; and they produce long-lasting effects that offer an unconventional electronic attack (UEA) that complements traditional electronic warfare (EW) jammers [1].

The typical approach to protect systems against DEW threats is a zonal approach where one tries to decrease the energy that impinges on the target and increases the robustness of the interior components. For HELs, this approach typically means two things: covering the potential victim system with materials that can reflect the laser energy and withstand the heat, and covering the sensors and optics with materials that reflect the incident energy.

If one knows the laser fluence required to cause damage to a victim system, *S*, and the exposure level of the threat laser, *E*, then one can compute the amount of attenuation or hardening, *H*, required to reduce the threat below the damage level:

$$H > S/E. \tag{1}$$

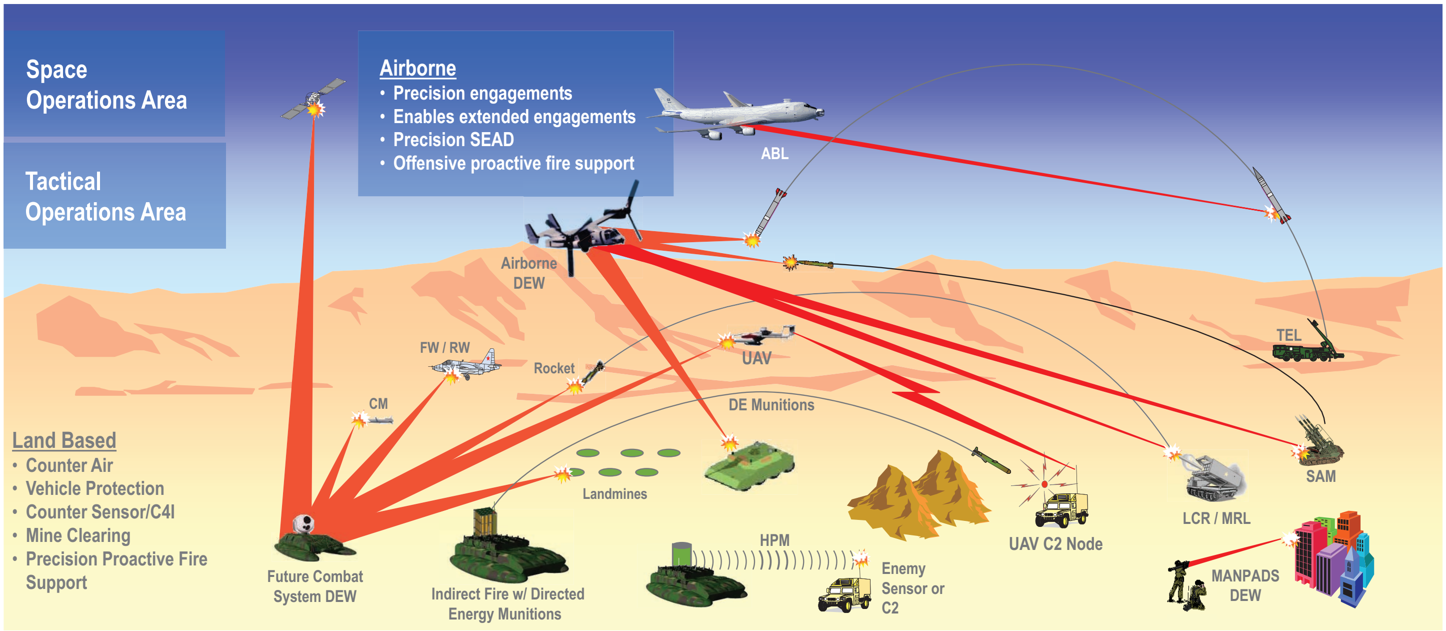


Figure 1: Possible Applications for Directed Energy Weapons *(Source: DoD HPM DEW Effects Panel)*.

Ideally, it is useful to cover a victim system with a material that has high reflectance and robust thermal properties.

For HPM threats, the effect mechanism is different than lasers and typically involves coupling the HPM energy from the skin of a victim system to the interior electronic components. Therefore, for HPM protection, this fact means reducing the energy that is transferred to the electronics and increasing the robustness of the components. Because it is difficult to harden all the components, the approach usually taken is to reduce the HPM energy that reaches the interior electronics by first providing a good electromagnetic shield, using good grounding, bonding, and shielding techniques, such as those used in electromagnetic compatibility (EMC). Next, we treat the ports of entry (i.e., penetrations) with filters to remove the out-of-band energy and limiters to reduce the in-band energy from damaging the component [2].

METHODOLOGY

Figure 2 shows a methodology for hardening systems against an HPM threat level, *E*. The “protection requirements” block in the figure shows how one can use the susceptibility level of a victim system, *S*, to compute either the hardening level, *H*, or the keep-out range, *R*, required to protect the victim system. *H* represents the amount of attenuation required between the HPM port of entry and the susceptible component or the hardening level. *R* represents the separation distance required between a victim system and an HPM threat to ensure that the threat exposure level is below the system’s susceptibility level.

Ideally, it is best to measure the HPM susceptibility level of a victim system rather than depending upon estimated levels. This measuring requires irradiating a monitored system with increasing levels of HPM power density and noting any effects on the system operation. Because the HPM susceptibility level of a system is not only a function of the incident power density but also the frequency and modulation (i.e., pulse width and repetition rate) of the waveform, it is important to cover all the threat parameters.

In 1992, the Harry Diamond Laboratories (which are now part of the U.S. Army Research Laboratory [ARL]) developed a set of HPM Hardening Design Guides (shown in Figure 3) to assist system developers in hardening their systems against HPM threats. Volumes 1–3 of the handbooks are unclassified and available through the Defense Technical Information Center (DTIC). Volume 4 is classified and contains test data on U.S. and foreign systems [2].

HPM HARDENING EXAMPLE

The following text provides a notional example of how to harden a helicopter

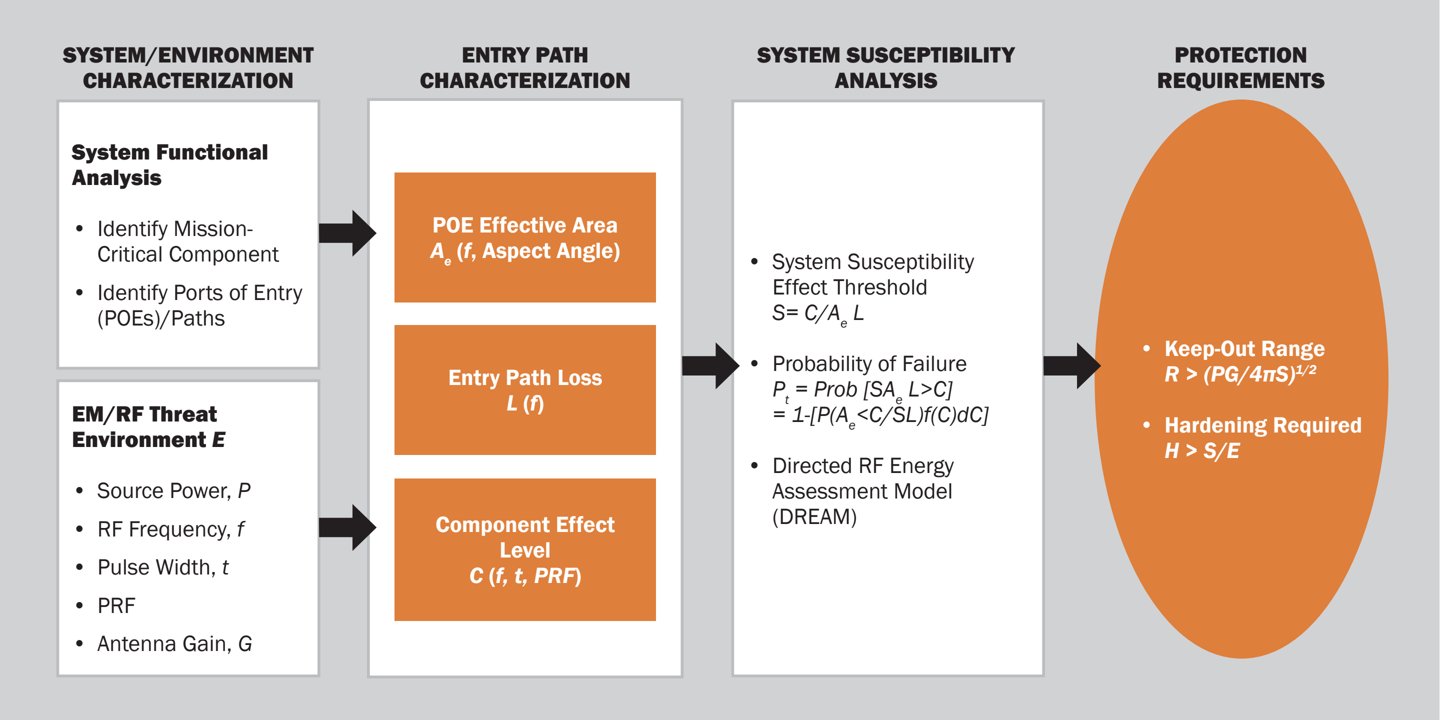

SYSTEM/ENVIRONMENT CHARACTERIZATION
System Functional Analysis
• Identify Mission-Critical Component
• Identify Ports of Entry (POEs)/Paths
EM/RF Threat Environment E
• Source Power, P
• RF Frequency, f
• Pulse Width, t
• PRF
• Antenna Gain, G
ENTRY PATH CHARACTERIZATION
POE Effective Area A_e (f, Aspect Angle)
Entry Path Loss L (f)
Component Effect Level C (f, t, PRF)
SYSTEM SUSCEPTIBILITY ANALYSIS
• System Susceptibility Effect Threshold $S= C/A_e L$
• Probability of Failure $P_t = Prob [SA_e L>C]$ $= 1\text{-}[P(A_e<C/SL)f(C)dC]$
• Directed RF Energy Assessment Model (DREAM)
PROTECTION REQUIREMENTS
• Keep-Out Range $R > (PG/4\pi S)^{1/2}$
• Hardening Required $H > S/E$

Figure 2: A Methodology for Estimated Hardening Requirements and/or Keep-Out Range for Victim Systems *(Source: SURVICE Engineering)*.

HIGH-POWER-MICROWAVE HARDENING DESIGN GUIDE FOR SYSTEMS
Volume II
Hardening Against HPM
APRIL 1992
HIGH-POWER-MICROWAVE HARDENING DESIGN GUIDE FOR SYSTEMS
Volume I
HPM and Interpreting Hardening Requirements
APRIL 1992

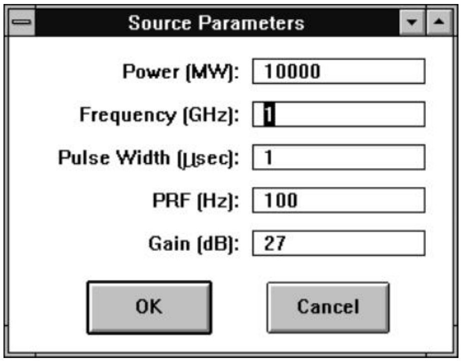
Figure 3: HPM Hardening Design Guide for Systems *(Source: AFRL)* [2].

system against an HPM DEW weapon using the aforementioned methodology. The purpose of the example is to demonstrate how to develop hardening requirements, *H*. These requirements can be thought of as the amount of attenuation that must be introduced in the entry paths to ensure the threat HPM energy reaching the helicopter, *E*, is below the helicopter's susceptibility level, *S*. Following the flowchart shown in Figure 2, the first step is to define the threat parameters and perform a functional analysis on the helicopter to identify mission-critical component and associated HPM entry paths to the components.

HPM Threat Environment

For this example, assume that the HPM threat is a high-power transmitter that can produce 1-μs, 1-GHz (L-band) pulses at a peak power of 1,000 MW with a pulse repetition frequency (PRF) of 100 Hz. Also assume that the transmitter is combined with a parabolic reflector-type antenna with a gain of 500 (27 dB). Note that these parameters are entirely fictitious and are used only to show the hardening methodology.

The Directed Radio Frequency Energy Assessment Model (DREAM), which is used for this example, is a one-on-one engagement model that simulates the interaction between a defined HPM weapon and a target system. The model computes the probability of target failure as a function of the incident RF power density on the target and the separation distance between the threat and target (range). DREAM was developed by ARL and one of its contractors, SPARTA Inc., in the 1990 time frame. It runs on a standard personal computer (PC) using Microsoft Windows [3]. The model manager for DREAM is currently the Air Force Research Laboratory (AFRL) in Kirtland AFB, NM. Figure 4 shows DREAM's input screen, which summarizes the key threat parameters.


Source Parameters

Power (MW): 10000
Frequency (GHz): 1
Pulse Width (μsec): 1
PRF (Hz): 100
Gain (dB): 27

Figure 4: Source Parameters for Notional HPM Weapon Threat.

System Functional Analysis

The next step is to identify the mission-critical subsystems on the helicopter and their associated critical electronic components. Figure 5 shows a notional helicopter and the mission-critical subsystems we have identified. Next, we try to identify the likely entry path for the HPM energy to enter a port of entry (POE) on the helicopter and travel to the component. For example, we have identified the radio as a critical subsystem since its failure could lead to a loss of communications. Within the radio, we identify the RF front-end mixer since the radio cannot demodulate the incoming signal with a damaged front end. Therefore, the entry path for the radio consists of the signal path from the ultra high frequency (UHF) antenna to the RF front end. The next critical subsystem we identified is the engine control unit. The engine control system does not have an antenna, but it does have an unintentional antenna in terms of the cable leading to the transistor control box. Continuing to follow the methodology, we see that the next critical subsystems identified are the fire control computer and the flight control computer. Each has a wire cable as a POE leading to Transistor-Transistor Logic (TTL) control circuits.

Failure Analysis Logic Tree

After identifying the critical subsystems, we develop a Failure Analysis Logic Tree (FALT) that shows the relationship of the subsystems to the operation of the overall helicopter. Figure 6 shows a FALT for the example helicopter generated by the DREAM model. The FALT shows not only the relationship between the subsystems but also the failure modes being considered and their criticalities. For this example, we are considering two major failure modes for the helicopter: Mission Abort and Forced Landing. We assume that if either mode occurs, the helicopter will fail. For Mission Abort, we assume that the radio and/or fire control computer must fail. Both are considered equally critical and, therefore, the reason for the number one in the criticality box. For Forced Landing, we assume that the engine control and/or flight control must fail. Again, they are both considered to be equally critical.

At the bottom of the FALT are the actuators that lead to the failure of the subsystems. The actuators represent the combination of the POE, entry path,

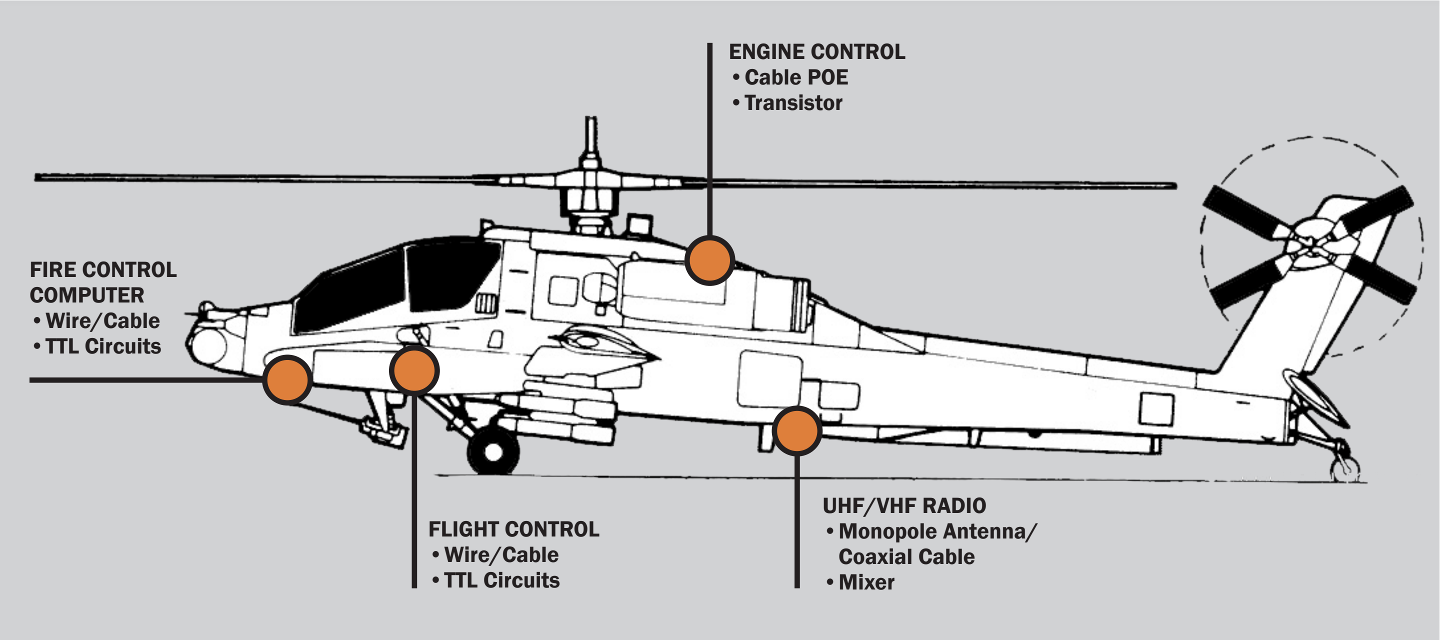


Figure 5: Functional Analysis for Notional Helicopter to Identify Mission-Critical Electronics *(Source: SURVICE Engineering)*.

and critical component. Specifically, they represent the power required to fail the critical component, P_c, the attenuation (or loss) of the entry path from the POE to the component, *L*, and the effective area of the POE, A_e.

Entry Path Characterization

We can characterize the entry paths discussed in the previous section by defining the type of POE, the path loss, and the type of mission-critical component. Table 1 shows a summary of the parameters for each of the critical subsystems being considered. The numbers shown in red are the inputs for the DREAM model; the numbers in black are computed by DREAM and are not required as inputs. Based on these inputs, DREAM computes the probability of failure for each of the actuators and then propagates the numbers up the FALT to compute the probability of failure for each of the nodes. For example, for the engine control computer, we previously defined the type of POE as a wire/cable. The gain for a wire/cable for out-of-band energy is estimated to be -3 dB [4]. Next, we estimate the attenuation of the entry path from the POE to the components. Based on experiments, we estimate a loss factor of 100 or 20 dB. Finally, we identify the type of component as a transistor. The mean damage level for a transistor for a 1-µs, 1-GHz pulse is estimated to be about 200 W [2]. Following the same procedure, we characterize the remainder of the entry paths.

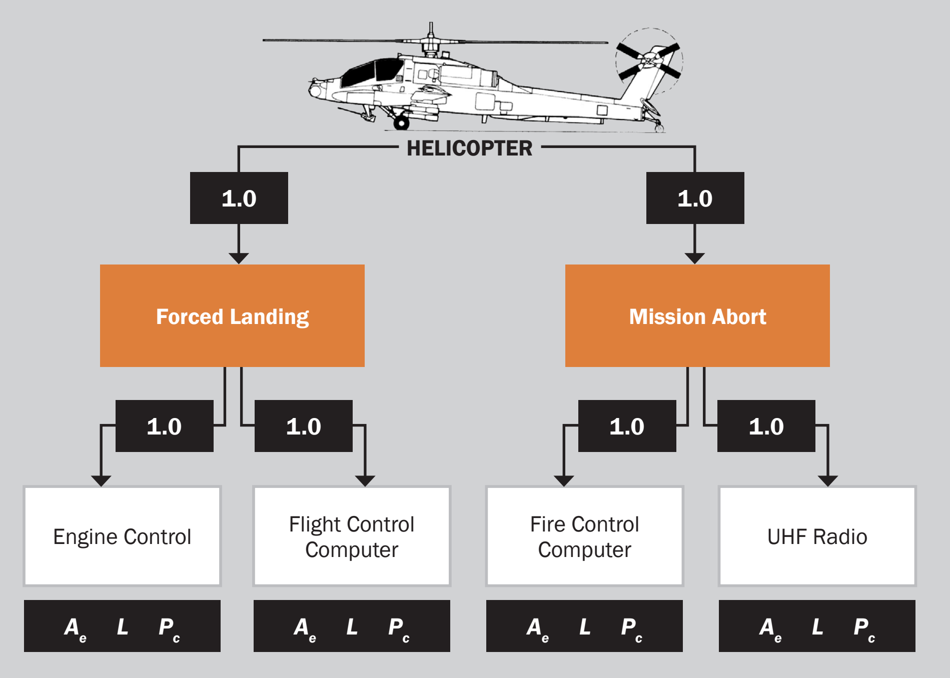


Figure 6: FALT for Helicopter Showing the Mission-Critical Subsystems and Components. (The numbers near the links represent the conditional probability that if the lower node fails, so will the upper node. The 1.0 means that the if the lower node fails, then the upper node will fail.) *(Source: SURVICE Engineering)*

Table 1: Entry Path Characterization for Example Helicopter

SUBSYSTEM	FREQ. (GHz)	RF PORT OF ENTRY			LOSS (dB)	CRITICAL COMPONENT		MEAN DAMAGE (W/cm²)
		TYPE	GAIN (dBi)	AREA (cm²)		TYPE	DAMAGE LEVEL (W)	
Engine Control	NA	Wire/cable	-3	36	20	Transistor	200	560
Flight Control	NA	Wire/cable	-3	36	20	TTL	100	300
Fire Control	NA	Wire/cable	-3	36	20	TTL	100	300
UHF Radio	.2–.4	Antenna	-3	36	10	Mixer	10	3

POE Area = ((Gain) (Wavelength)²) / 8 π

Component Damage Levels Based on R. Antinone's Component Effects Data

Probability of Failure (Damage) vs. Incident Power Density and HPM Threat Range

We compute the probability of failure of the helicopter subsystems based on the probability that the power received at the component, P_r, is greater than the component failure level, P_c. Because both P_r and P_c are essentially random variables, the probability of failure of a subsystem is equal to the difference of two random variables, which corresponds to the convolution of the Probability Distribution Function (PDF) of P_r with the PDF of P_c. DREAM computes the probability of failure of each of the mission-critical subsystems and then combines them using Boolean algebra to compute the probability of each nodes of the FALT [3].

Based on the threat parameters shown in Figure 4, the FALT shown in Figure 6, and the entry path parameters in Table 1, Figure 7 shows the probability of failure (damage) of the example helicopter that was computed by DREAM as a function of the HPM weapon's power density and range for the cases of Mission Abort and Forced Landing. The HPM weapon's power density is shown at the bottom in watts/square centimeter, and the range is shown at the top in meters. Because the probability of helicopter failure was based on either Mission Abort or Forced Landing, the curve for Forced Landing represents the overall probability of helicopter damage.

For example, we see that the weapon power density required for a 50% probability of helicopter damage is estimated to be about 10 W/cm² and occurs at a range of about 1,000 km. Because we want to ensure that the helicopter is hardened against the worst-case threat, we select a conservative value of 10% probability of damage to develop our hardening requirements. One can choose a lower probability, but this choice can lead to overhardening, which is expensive in cost and weight penalty.

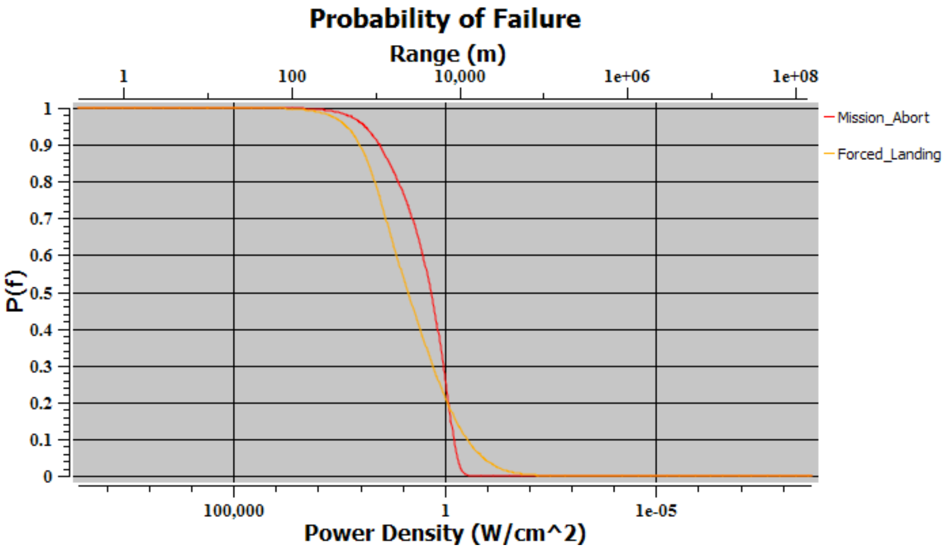


Figure 7: Probability of Failure for Example Helicopter Showing Forced Landing and Mission Abort.

Hardening Requirements

Finally, we use the susceptibility level of the helicopter to compute the hardening requirement using equation 1. Based on Figure 7, the power density associated with a 10% probability of damage is about 1 W/cm², which is the helicopter's susceptibility level for a 10% probability of damage. This can occur at a separation distance between the weapon and helicopter of about 10 km. If we want to harden to a maximum threat level of 1,000 W/cm², then the

$$\textit{Hardening Level Required} = H = S/E$$
$$= 1\ W/cm^2/100\ W/cm^2 = 0.001$$
$$(>30\ dB\ of\ attenuation).$$

The FALT shows not only the relationship between the subsystems but also the failure modes being considered and their criticalities.

Therefore, for this example, we estimate that the helicopter will need at least 30 dB of hardening added to the entry paths to ensure that the threat energy reaching the critical components is below the failure level. To achieve this level of hardening, one could use a dual-PIN diode limiter that can provide at least 40 dB of front-door protection or RF shielding materials that can provide greater than 30 dB of protection [2].

SUMMARY

Foreign-made DEWs represent an evolving threat to U.S. military systems and civilian infrastructure. This article has described a methodology that can be used to countermeasure DEWs and reduce their effects. It must be emphasized, however, that each case is different and depends upon the DEW threat parameters and the susceptibility level of the victim system. If possible, any hardening requirements should be based on the measured susceptibility level of the system. However, if this basing is not possible, the methodology described herein may be considered. In addition, interested readers are encouraged to contact the intelligence community to get the latest information on both HEL and HPM threats. ■

REFERENCES

[1] Tatum, J. "HPM DEWs and Their Effects on Electronic Targets." *DSIAC Journal*, vol. 4, no. 3, summer 2017.

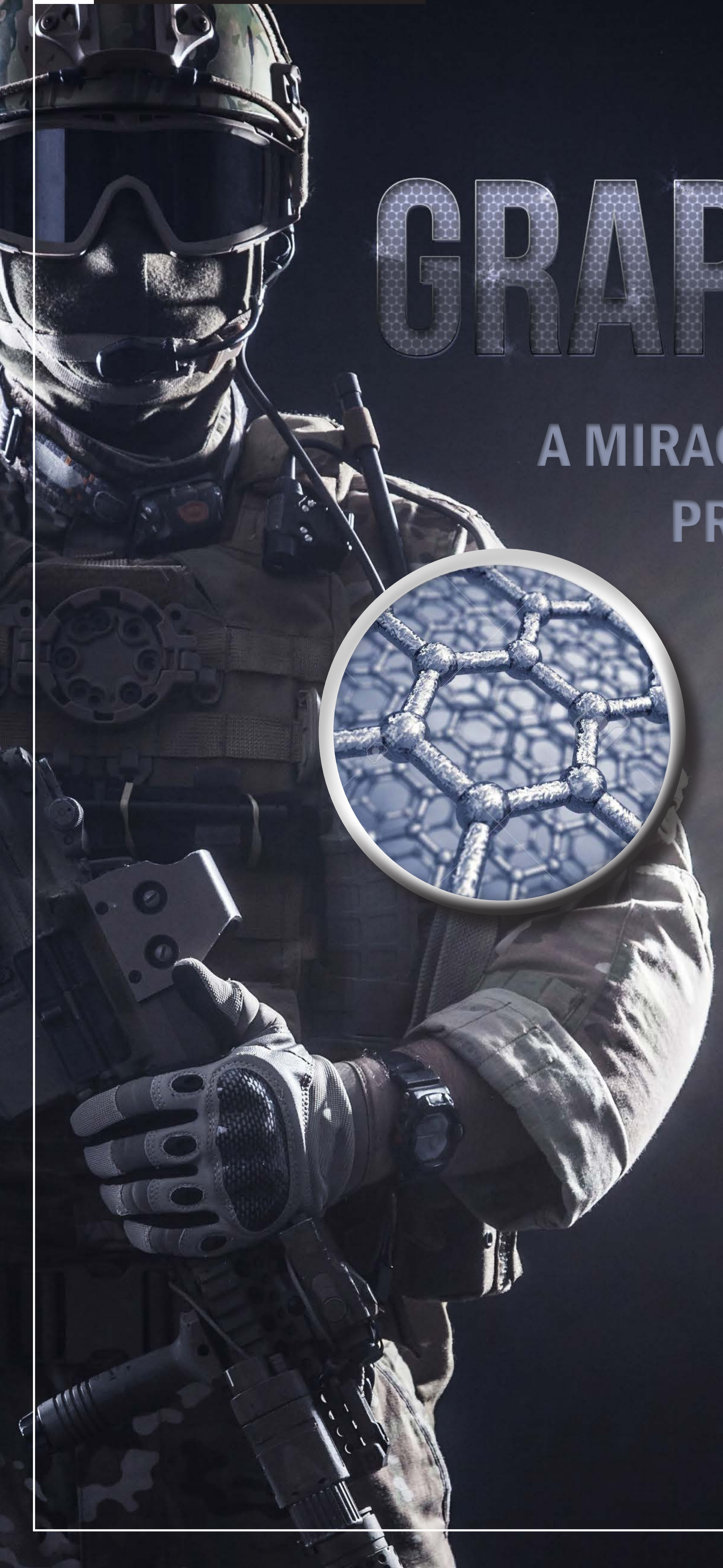
[2] Casper, J. E. (editor). "High-Power Microwave Hardening Design Guide for Systems." HDL-CR-92-709-5, U.S. Army Harry Diamond Laboratories, Adelphi, MD, April 1992.

[3] Tatum, John T., Karen R. McLaughlin, Robert E. O'Connor, and Anthony N. Valle. "Operator's Guide for DREAM: Directed Radio Frequency Energy Assessment Model." Version 0.1, ARL-TR-479, Revision 1, JTCG/AS -95-M-001, August 1996.

[4] Hayes, S. T., and R. V. Garver. "Out-of-Band Antenna Response." *Proceedings of 1987 IEEE International Symposium on Electromagnetic Compatibility*, 87CH2487-7, Atlanta, GA, August 1987.

BIOGRAPHY

JOHN TATUM is currently an electronic systems engineer with the SURVICE Engineering Company, with subject-matter expertise in EW and RF DEWs. Before joining SURVICE, he worked for more than 36 years at ARL's RF Electronics Division in radar/EW, where he directed and participated in EM/RF effects investigations on military systems and supporting infrastructure. Mr. Tatum investigated the feasibility and effectiveness of RF DEWs for various Army applications and served as the Army chairman of the RF DE JMEM Working Group. He also served as chair of the RF Effects Panel for the Office of the Secretary of Defense's Technology Panel on DEW. Mr. Tatum is also a fellow of the Directed Energy Professional Society. He holds a B.S. in electrical engineering from the University of Maryland and has completed graduate courses in communications and radar at the University of Maryland and the John Hopkins University.



GRAPHENE:

A MIRACLE MATERIAL WITH PROMISING MILITARY APPLICATIONS

By Alex Bernardo

Though the name might not be familiar to many, graphene has been heralded as a “miracle material,” the application of which includes:

- Touchscreens (for light-emitting diode [LCD] or organic light-emitting diode [OLED] displays)
- Transistors
- Computer Chips
- Batteries
- Energy Generation
- Supercapacitors
- DNA Sequencing
- Water Filters
- Antennas
- Solar Cells
- Spintronics-Related Products.

In addition, based on recent research, graphene is turning out to be an exciting advanced material, promising advantages in two particular areas for the military: (1) survivability/force protection, and (2) increased battery storage capacity. For the first area, graphene's potential as ballistic armor material has become more evident from mechanical strength investigations. For the second, research of graphene's comparatively high conductivity is leading directly to better energy density in battery storage.

WHAT IS GRAPHENE?

Graphene is a 1-atom-thick layer of tightly bonded carbon atoms arranged in a hexagonal lattice (Figure 1). It is a single atomic layer of graphite (which is used, among other things, for pencil tips). Graphene is special because of its sp^2 hybridization and extremely thin atomic thickness (0.345 nm), properties that make it remarkably strong (about 200 times stronger than steel) as well as an excellent conductor of heat and electricity. The carbon-to-carbon bonds in graphene are so small and strong that they prevent thermal fluctuations from destabilizing it. In addition, the material is extremely diverse and can be combined with other elements (including gases and metals) to produce different materials with a range of superior properties.

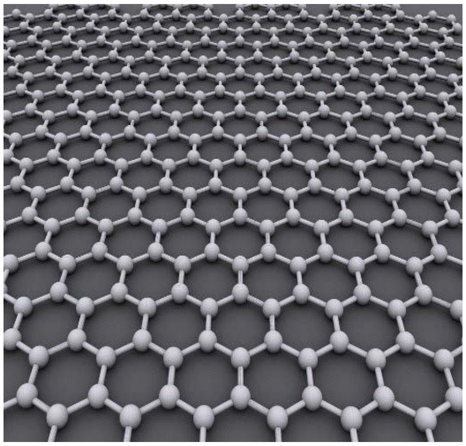


Figure 1: Graphene Is an Atomic-Scale Hexagonal Lattice Made of Carbon Atoms *(Credit: AlexanderAIUS via Wikimedia Commons).*

GRAPHENE FOR MILITARY SUVIVABILITY/FORCE PROTECTION

Mechanical Strength of Graphene

The tight lattice of graphene has extremely short (0.142-nm-long) carbon bonds, which gives it its inherent strength. With an ultimate tensile strength of 130 GPa, graphene is the strongest material ever discovered. For comparison, A36 structural steel has a 0.4-GPa and Aramid (Kevlar) has a 0.37-GPa ultimate tensile strength. Graphene is also extraordinarily light at 0.77 mg/m^2, which is roughly 1,000 times lighter than 1 m^2 of paper. It is often said that a single sheet of graphene (being only 1 atom thick) sufficient in size to cover a whole football field would weigh less than 1 g [1].

Graphene also contains elastic properties, being able to retain its initial size after strain. In 2007, atomic force microscopic (AFM) nanoindentation tests were carried out on graphene sheets that were suspended over silicone dioxide cavities. These tests showed that graphene sheets (with thicknesses of between 2 and 8 nm) had spring constants in the region of 1–5 n/m and a Young's modulus of 0.5 TPa. But more recently, graphene's in-plane Young's modulus was measured to be more than 1.0 TPa, also using AFM nanoindentation [2].

Graphene Potential for Ballistic Protection

Graphene's lightness and strength have been thought to be a potentially good fit for ballistic protection for some time. In military applications, lighter armor material provides for greater mobility and increased range for the same level of protection.

Researchers from the University of Massachusetts in Amherst studied the way graphene absorbs kinetic energy and discovered that it might be extremely efficient in preventing bullet penetration [3] (Figure 2).

The researchers constructed a miniature ballistics test using a laser pulse to superheat gold filaments until they vaporized, which simulated gunpowder firing a micrometer-sized glass bullet. The researchers tested at impact velocities of 6,000 m/s and 9,000 m/s into sheets of graphene that ranged from 30 to 300 layers.

The scientists found that graphene sheets dissipated the kinetic energy by stretching into a cone shape at the bullet's impact point, then cracking outward radially. Despite those cracks, the material still performed twice as well as Kevlar and endured 10 times the kinetic energy that steel can. In

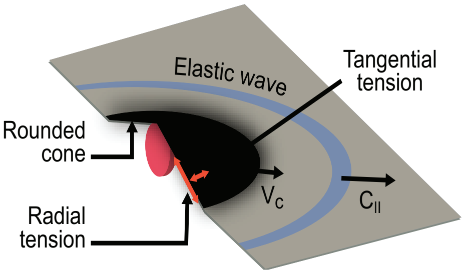


Figure 2: Graphene Mechanics as Impacted by Microprojectile [3].

microscale, the behavior of graphene to stretch into a cone before projectile penetration is eerily similar to that of fabric materials—such as Kevlar and Zylon—used in ballistic protection (as shown in Figure 3).

Ballistic tests had previously been done on fabric to measure fabric displacement (*h*), along the axis of impact and the radius (*R*) of the fabric deformation or “bulge,” as a function of time. As a result, Walker [4] was able to develop an analytical model for the dynamic response of fabrics to ballistic impact. In the model, the force, *F*, on the bullet is a function of *h* and *R*.

$$F = -\frac{8}{9} Y T^* \frac{h^3}{R^2}.$$

Y is the fabric Young’s modulus, and *T** is the fabric effective thickness. Relationships were also found between the target/projectile density ratio and normalized V_{50}. With test data, this analytical curve fit is shown in Figure 4, where

$$X = \rho' A_P / M_P,$$

and

$$V^* = \frac{c_f \varepsilon_f{}^{2/3}}{2^{1/3}},$$

where *ρ′* is the fabric areal density, A_p is the presented area of the projectile, M_p is the mass of the projectile, $c_f \sim (Y/\rho)^{1/2}$ is the bar velocity of the fabric fiber, and ε_f is the failure strain of the fiber.

Table 1 compares material properties between graphene and Kevlar, traditional ballistic fiber. For graphene, metrics normally used for fabric were calculated for comparison. We see straight off that graphene properties are impressive, in particular for E_p, the net energy required to penetrate the material.

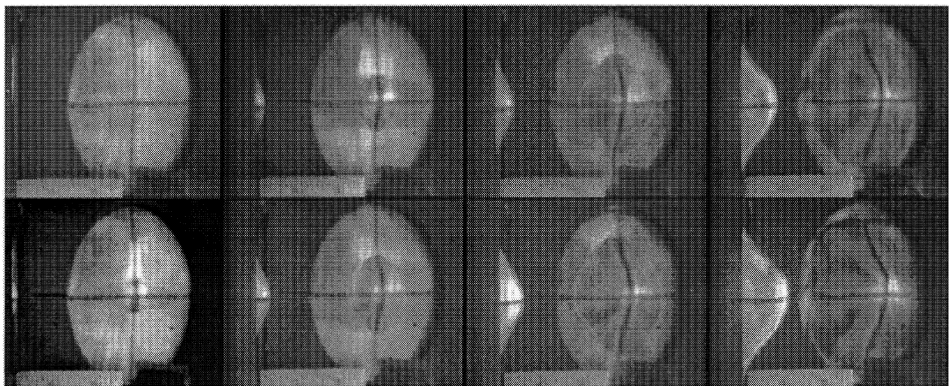


Figure 3: Images from High-Speed Video of Ballistic Fabric Deformation [4].

Because tensile mechanical stresses in a material cannot be transmitted faster than the speed of sound [$c \sim (Y/\rho)^{1/2}$], the nonequilibrium local stress arising from the inertial effect becomes important under dynamic conditions accompanying high-strain-rate, predominantly tensile loading [5]. The relatively low density (~2,200 kg/m^3) of graphene [6], along with its high modulus, leads to a superior in-plane speed of sound (*c*~21.3 km/s, compared to Kevlar at 9.5 km/s), implying that concentrated stresses applied under extreme conditions can rapidly be delocalized.

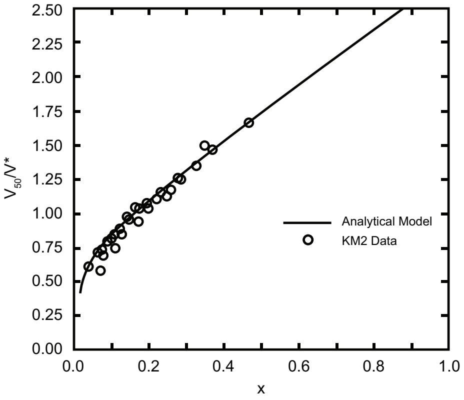


Figure 4: Kevlar KM2™ V_{50} Data and Walker Model Fabric [4].

Looking at graphene values for *V** in relation to *X*, and looking at Figure 4 for Kevlar, we can get a sense that V_{50} could be quite high for graphene compared to Kevlar. V_{50} for graphene has not been tested yet.

In separate research, at the City University of New York (CUNY), it was

Table 1: Comparison of Graphene and Kevlar Under Projectile Impact Testing [3]

PROPERTY	GRAPHENE	KEVLAR
Density, kg/m^3	2,200	1,560
Tensile Strength, GPa	130	0.37
Young’s Modulus, GPa	1,000	169
Speed of Sound, km/s	21.3	10.4
Areal Density, kg/m^2	2.28e-5 to 2.28e-4**	Varies (see Figure 4)
Projectile Mass, kg	5e-14*	
Projectile Presented Area, m^2	1.075e-11*	
Density Ratio, *X*	4.9e-3 to 4.9e-2**	
*V**, km/s	2.59**	
Specific Penetration Energy, E_p, MJ/kg	~1.15*	~0.5*

**From Lee [3] experiments.* ***Calculated from Lee experiments.*

shown that two layers of graphene exhibit a transverse stiffness and hardness comparable to diamond [7]. At room temperature, the two-layer graphene construct was resistant to perforation with a diamond indenter and showed a reversible drop in electrical conductivity through indentation and release. The researchers used atomistic computer simulations to model potential outcomes when pressurizing two layers of graphene aligned in different configurations. Subsequent validation tests agreed with the simulations. Daimene, as the construct has been dubbed, is as flexible and lightweight as foil but becomes stiff and hard enough to stop a bullet on impact. Experiments and theory both show that this graphite-diamond transition does not occur for more than two layers or for a single graphene layer. No actual ballistic impact testing was conducted on Diamene.

GRAPHENE FOR IMPROVED POWER STORAGE/BATTERIES

Electronic Properties of Graphene

Graphene is a zero-overlap semimetal with extremely high electrical conductivity. Both holes and electrons act as charge carriers. Carbon atoms have a total of six electrons; two in the inner shell and four in the outer shell. The four outer-shell electrons in an individual carbon atom are available for chemical bonding, but in graphene, each atom is connected to three other carbon atoms on the two-dimensional (2-D) plane, leaving one electron freely available in the third dimension for electronic conduction.

Tests have shown that the electronic mobility of graphene is extremely high, with previously reported results above 15,000 $\mathrm{cm^2/V{\bullet}s}$ and theoretically potential limits of 200,000 $\mathrm{cm^2/V{\bullet}s}$. It is said that graphene electrons act much like photons in their mobility due to their lack of mass. These charge carriers can travel submicrometer distances without scattering, a phenomenon known as ballistic transport. However, the quality of the graphene and the substrate that is used are limiting factors. With silicon dioxide as the substrate, for example, mobility is potentially limited to 40,000 $\mathrm{cm^2/V{\cdot}s}$ [1].

Improved Power/Battery Storage

Conventional battery electrode materials are significantly improved when enhanced with graphene. Graphene can make batteries light, durable, and suitable for high-capacity energy storage; and it can shorten their charging times. Battery life-time is negatively linked to the amount of carbon that is coated on the material or added to electrodes to achieve conductivity. Graphene adds conductivity without requiring the amounts of carbon that are used in conventional batteries.

The military continues to advance the use of electronics in missions, and these electronics are normally battery-powered. Increased longevity of stored battery power for the same weight—or, alternatively, the same storage capacity in a lighter package—enhances overall military capability. Reduced weight will either add increased range or allow increased weight in another important component, such as armor. In addition, longer battery life decreases likelihood of mission failure from loss of battery power.

Graphene can also improve such battery attributes as energy density. Lithium-ion (Li-ion) batteries can be enhanced by introducing graphene to the battery's anode and capitalizing on the material's conductivity and large surface area traits to achieve morphological optimization and performance.

It has also been discovered that creating hybrid materials can also be useful for achieving battery enhancement. A hybrid of vanadium dioxide (VO_2) and graphene, for example, can be used on Li-ion cathodes and grant quick charge and discharge as well as large-charge-cycle durability. In this case, VO_2 offers high-energy capacity but poor electrical conductivity, which can be solved by using graphene as a sort of a structural "backbone" on which to attach VO_2—creating a hybrid material that has both heightened capacity and excellent conductivity.

Another example is lithium iron phosphate (LFP) batteries, which are a type of rechargeable Li-ion battery. These batteries have a lower energy density than other Li-ion batteries but a higher power density (an indicator of the rate at which energy can be supplied by the battery). And enhancing LFP cathodes with graphene allows the batteries to be lightweight, charge much faster than Li-ion batteries, and have a greater capacity than conventional LFP batteries.

In November 2016, Huawei Technologies unveiled a new graphene-enhanced Li-ion battery that can remain functional at higher temperature (60° as opposed to the existing 50° limit) and offers a longer operation time (double of what can be achieved with previous batteries). To achieve this breakthrough, Huawei incorporated several new technologies—

including antidecomposition additives in the electrolyte and chemically stabilized single crystal cathodes—and graphene to facilitate heat dissipation. Huawei claims that the graphene reduces the battery's operating temperature by 5°.

INDUSTRIAL STATUS AND CONCLUSION

Since the isolation of graphene in 2004, numerous studies and researches have been inspired. And the material's many possible applications—such as in energy storage (batteries and supercapacitors), energy generation (photovoltaic [PV] cells), sensors, membranes, conductive material (indium tin oxide [ITO] replacement in touch displays), drug delivery, photonic applications, etc.—are expected to continue to revolutionize entire industries. Graphene may also be useful for next-generation transistors, electronic devices and spintronics devices.

There are dozens of companies that currently produce graphene (and graphene-based materials). While production volume is relatively small and prices are still high, commercial applications consistently emerge into the markets. Production volumes are predicted to increase, while prices are predicted to drop, enabling more and more products to use graphene-based materials. Mass production of large graphene sheets has not been achieved yet, but several companies are offering such materials in low volume.

Graphene shows impressive potential for the military in the areas of survivability/ force protection and battery storage. Both areas can witness increased performance for the same weight or reduced weight for the same performance. Once the economies of scale begin to take hold, increased performance can be realized for the same cost. ■

ACKNOWLEDGMENTS

The author would like to thank Mr. Ron Mertens, CEO and Editor-In-Chief of Graphene-info (http://www.graphene-info.com), for his technical guidance in writing this article.

REFERENCES

[1] de la Fuente, Jesus. "Graphene – What Is It?" www.graphenea.com/pages/graphene#.WoWFhK5KtEY, accessed 24 January 2018.

[2] Lee, C., X. Wei, J. W. Kysar, and J. Hone. "Measurement of the Elastic Properties and Intrinsic Strength of Monolayer Graphene." *Science*, vol. 321, issue 5887, pp. 385–388, 18 July 2008.

[3] Lee, Jae-Hwang, Phillip E. Loya, Jun Lou, and Edwin Thomas. "Dynamic Mechanical Behavior of Multilayer Graphene via Supersonic Projectile Penetration." *Science,* vol. 346, issue 6213, pp. 1092–1096, 28 November 2014.

[4] Walker, J. D. "Constitutive Model for Fabrics with Explicit Static Solution and Ballistic Limit." *Proceedings of the 18th International Symposium on Ballistics*, vol. 2, pp. 1231–1238, 1999.

[5] Field, J. E., S. M. Walley, W. G. Proud, H. T. Goldrein, and C. R. Siviour. "Review of Experimental Techniques for High Rate Deformation and Shock Studies." *International Journal of Impact Engineering*, vol. 30, issue 7, pp. 725–775, 2004.

[6] Anthony, J. W., R. Bideaux, K. Bladh, and M. C. Nichols (editors). *Handbook of Mineralogy, Mineralogical Society of America, Chantilly, VA, 1990.*

[7] Gao, Y., T. Cao, F. Cellini, C. Berger, W. de Heer, E. Tosatti, E. Riedo, and A. Bongiorno. "Ultrahard Carbon Film from Epitaxial Two-Layer Graphene." *Nature Nanotechnology,* vol. 13, pp. 133-138, February 2018.

BIOGRAPHY

ALEX BERNARDO is a senior engineer at the SURVICE Engineering Company's Michigan Area Operation. He has more than 20 years in research, development, test, and engineering, predominantly in the military vulnerability field. His past work has included planning, conducting, and reporting of ballistic and explosive testing. He has also performed pre- and post-test analysis using a variety of mathematical and numerical models, ranging from first-principle to empirical-based. Mr. Bernardo holds a B.S. in aerospace engineering from the University of Washington and an M.S. in mechanical engineering from California State University, Northridge.

CONFERENCES AND SYMPOSIA

DARPA Launch Challenge (DLC)
16 April 2018–31 December 2019
http://www.darpalaunchchallenge.org ▸

JUNE 2018

Gordon Research Seminar (GRS) - Energetic Materials
2–3 June 2018
Newry, ME
https://www.grc.org/energetic-materials-grs-conference/2018 ▸

Gordon Research Conference - Energetic Materials
3–8 June 2018
Newry, ME
https://www.grc.org/energetic-materials-conference/2018 ▸

2018 JASP Model Users Meeting
12–14 June 2018
Air Force Institute of Technology
WPAFB, OH
https://www.dsiac.org/events/2018-jasp-model-users-meeting ▸

2018 MSS Tri-Service Radar Symposium (TSRS)
25–29 June 2018
Monterey, CA
https://mssconferences.org/public/meetings/conferenceDetail.aspx?enc=y97SIe4oVgrjZyxuqVN%2bcg%3d%3d ▸

Robotics and Autonomous Systems Summit
25–27 June 2018
Detroit, MI
https://roboticsautonomoussystems.iqpc.com ▸

2018 NSMMS & CRASTE
25–28 June 2018
Madison, WI
https://www.usasymposium.com/space/2018/default.php ▸

For more events, visit:
dsiac.org/resourses/events ▸

JULY 2018

AIAA Propulsion Energy Forum
9–11 July 2018
Duke Energy Convention Center
Cincinnati, OH
https://propulsionenergy.aiaa.org ▸

DARPA First Annual Electronics Resurgence Initiative Summit
23–25 July 2018
San Francisco, CA
https://www.darpa.mil/news-events/2018-04-06 ▸

AUGUST 2018

Special Operations Nexus
30 July–1 August 2018
Tampa, FL
https://sofnexus.iqpc.com ▸

Army Science & Technology Symposium & Showcase
21–23 August 2018
Walter E. Washington Convention
Washington, D.C. 20001
http://www.ndia.org/events/2018/8/21/army-science

SEPTEMBER 2018

Directed Energy Systems Symposium
24–28 September 2018
Renaissance Portsmouth-Norfolk Waterfront Hotel
Portsmouth, VA
https://protected.networkshosting.com/depsor/DEPSpages/DEsysSymp18.html ▸

NOVEMBER 2018

Aircraft Survivability Symposium 2018
6–8 November 2018
Naval Postgraduate School
Monterey, CA
http://www.ndia.org/events/2018/11/6/9940-2018-aircraft ▸

2018 Workshop on Space Environment Applications, Systems, and Operations for National Security (SEASONS)
7–9 November 2018
The Johns Hopkins University Applied Physics Laboratory Kossiakoff Center
Laurel, MD
http://seasons.jhuapl.edu ▸

Army Autonomy and Artificial Intelligence Symposium and Exposition
28–29 November 2018
COBO Center
Detroit, MI
https://www.ausa.org/army-autonomy-ai-symposium ▸

DECEMBER 2018

2018 Defense Manufacturing Conference
3–6 December 2018
Nashville Music City Center
Nashville, TN
http://www.dmcmeeting.com/index.html ▸

Joint Army-Navy-NASA-Air Force (JANNAF) Meeting
10–14 December 2018
Portland, OR
https://www.jannaf.org/mtgs/2018Dec/pages/index.html ▸

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!