WHITE PAPER

Leveraging Digital RF Memory Electronic Jammers for Modern Deceptive Electronic Attack Systems

www.mrcy.com

BY TONY GIRARD
MERCURY DEFENSE SYSTEMS
MAY 2013

MERCURY SYSTEMS™

Today's advanced Electronic Attack (EA) systems are critical to holding a strategic advantage for the modern warfighter. Early EA systems focused on denying an enemy's use of electronic systems deployed to detect personnel, aircraft and warships. To gain a defensive advantage, modern EA systems have moved toward deceptive jamming to fool an enemy's system into misinterpreting the electronic environment. This paper will explore the role of Digital RF Memory (DRFM) based jammers in modern deceptive EA systems and the simulation of these EA systems to evaluate vulnerability to jamming techniques.

The Attack-Counterattack Game

In the world of electronic counter measures (ECM), there is a constant battle of one-upmanship, where each side is continually innovating to stay ahead of the other. ECM are typically developed and implemented to thwart an adversary's specific radar technology. To be effective, EA systems must be able to identify emitters in the environment and then selectively attack with specific techniques. They must also possess the ability to attack multiple emitters simultaneously with a combination of non-coherent and coherent jamming techniques.

As an example, assume a missile system is targeting an enemy aircraft. To confuse the oncoming missile, the enemy aircraft triggers an ECM. The goal of the ECM is to deny or deceive the incoming missile's targeting system so it will miss the aircraft. In order for the missile to succeed against various ECM techniques, the missile's targeting system must be "taught" to counter the countermeasure.

This attack-counterattack game has given rise to the need to develop EA systems that mirror enemy techniques in order to test U.S. and allied systems performance. These systems enable the testing and verification of weapon and defense systems against an enemy's ECM techniques. Armed with this knowledge, you can develop capabilities to counter any electronic countermeasures they employ.

Modern aircraft feature a variety of electronic counter measures for protection.

[1] Electronic attack (EA) or electronic countermeasures (ECM) involves the use of electromagnetic energy, or counter-electromagnetic radiation weapons to attack personnel, facilities, or equipment with the intention of directly affecting, degrading, neutralizing, or destroying an enemy's combat capability.

Denial Jamming

One EA technique is denial jamming. Put simply, if an enemy system emits one frequency with a particular pulse-width and pulse interval, your system detects and identifies that signal. It then blasts a massive amount of noise at that frequency, jamming the enemy and preventing that frequency from being used. The next move belongs to the enemy radar, which might simply jump to another frequency. Think of it as a countermeasure followed by a counter-countermeasure. Then the detection game starts again.

Deceptive Jamming

A step above denial jamming is deceptive jamming. Deceptive jamming requires a higher level of sophistication and this is where DRFM based jammers come into play. A DRFM based jammer receives and records the frequency, pulse-width and pulse interval of an enemy system and produces a false return signal by playing back the recorded signal. This false signal deceives the enemy system so that it sees the false return as a real target. The enemy then tracks the false target instead of the real one.

As an example, assume enemy radar has detected a fighter jet and starts tracking it. If the fighter has an EA system on-board using a DRFM based jammer, this system can detect the enemy radar, ingest the signal and create a false return to the enemy radar. This false return can take several variations including "ghosting" so that the enemy radar thinks that the target plane is in a different location. DRFM based systems are highly effective at accomplishing this based on their extremely low latency and ability to faithfully reproduce returns with all the signal characteristics of the radar source. The goal is to make the enemy radar think that the return signal is from the target rather than generated by a jammer.

In order to do this effectively, the DRFM must faithfully reproduce the characteristics of modern radar systems including frequency and phase modulations on signal pulses. An advanced DRFM based EA system also adds the necessary modulations to the return signal, such as Doppler frequency modulation to match the range rate of the false target. Lastly, an EA system using a DRFM follows any changes in signal characteristic produced by the enemy system in order to deceive the enemy system into "believing" that the false target being generated is real. This takes the focus away from the actual target and protects it.

Threat Analysis

Anticipating the capabilities of an adversary's ECM system is a key component to reducing the vulnerability of friendly radar systems to new techniques. Meanwhile, adversaries are constantly attempting to develop radar systems less susceptible to being jammed. This ongoing cat-and-mouse game is what pushes industry innovation forward.

The best way to ensure that an adversary cannot counter friendly radar and weapons systems is to test against actual enemy jammers. In the U.S., that is where the Test and Evaluation (TE) community comes into play. The TE community is composed of various agencies within the Navy, Air Force and other governmental agencies. They assess and analyze any existing or future ECM weapon systems that

Various methods, such as anechoic chambers, are used to test the effectiveness of ECMs.

present a threat to U.S. or allied systems and warfighters. It is the goal of the TE community to ensure that electronic systems are not vulnerable to jamming techniques.

The TE community collects signals intelligence data or predicts signal trends in order to identify the capabilities of enemy EA systems. Using this information, ECM techniques can be generated which mirror the behavior of enemy systems. The TE community then tests these techniques against U.S. and allied radars and weapons systems to determine their level of jamming success.

Various Testing Scenarios

Simulated RF Environments – There are multiple ways to test the effectiveness of electronic systems. In one testing scenario, an EA technique can be positioned against a radar in a laboratory or anechoic chamber. By running the EA system in this type of setting, it is possible to safely and cost-effectively determine if a jamming technique is able to the interrupt a radar's ability to acquire and track a target.

Some systems for test laboratories and anechoic chambers feature radar environment simulators (RES). State-of-the-art RES systems generate targets, weather, and other obstacles that a radar would normally encounter. Electronic countermeasures can be generated to further simulate the RF environment.

Depending on the application, an actual plane or missile seeker can be brought into a test chamber. Their radars are tested to determine if they can still track simulated targets amidst standard ECM techniques.

Flight Systems – A second testing method calls for the mounting of an EA system on an aircraft. An adversary ECM system, or an ECM system which simulates the adversary system, can be placed in a pod that is mounted on another plane's wing.

High performance EA systems such as those shown here from Mercury Defense Systems are critical for producing DRFM deceptive jamming.

The two planes are then flown against each other in an exercise which allows military analysts and/or pilots to see exactly what the aircraft's radar displays in a real combat situation.

ECM systems can also be placed in unmanned drones, which are then targeted by actual missiles. In this case, if the missiles never reach the drone, it would verify the effectiveness of the ECM system. This level of real-life testing eliminates any suppositions or estimations by engineers.

Jammer Simulation – Jammer simulation is the third EA testing method. When armed with the knowledge of specific jammer methods and techniques a jammer simulator can be programmed to mimic the capabilities of an EA system. The fidelity of the simulation can be evaluated for analysts to generate a validation report to be used by the TE community for test planning. Validated simulators can be used against a radar to verify the radars ability to operate in the presence of a particular EA system and to minimize the systems vulnerability to jamming.

Roles and Responsibilities

It is important to note that the TE community is set up to coordinate the vulnerability testing for electronic systems — and then make determinations based on its findings. It is their job to identify which systems work against which techniques, and to what degree. Additionally, the TE community — not the supplier of the EA test asset — is responsible for programming the EA system to make specific signal measurements and to generate particular jamming techniques.

For example, Mercury Defense systems will supply an EA system capable of hundreds of combinations of jamming parameters to be used for vulnerability testing. It is the TE community that selects the combinations of parameters and the test to be conducted to determine if/how an electronic system may be vulnerable.

Conclusion

DRFMs play a critical role in ECM and hence, in EA developments. By leveraging information captured from present and future enemy systems, DRFM-based test systems can be employed to test new EA systems – and verify whether or not these systems will succeed. With the growing reliance on electronic attack systems to protect warfighters and equipment, continuous testing and updating is required. And leveraging DRFM-based test systems fills this need in a modular, programmable, and cost-effective manner.

To learn more about electronic countermeasure testing capabilities, visit….mrcy.com/MDS

Innovation That Matters, Echotek, EchoCore, Ensemble and MultiCore Plus are registered trademarks, and StreamDirect, Application Ready Subsystem and ARS are trademarks of Mercury Systems, Inc. Other products mentioned may be trademarks or registered trademarks of their respective holders. Mercury Systems, Inc. believes this information is accurate as of its publication date and is not responsible for any inadvertent errors. The information contained herein is subject to change without notice.

MERCURY SYSTEMS™

Innovation That Matters™

Corporate Headquarters
201 Riverneck Road
Chelmsford, MA 01824-2820 USA
(978) 967-1401 • (866) 627-6951
Fax (978) 256-3599
www.mrcy.com

Europe **Mercury Systems, Ltd.**
Unit 1 - Easter Park, Benyon Road
Silchester, Reading
RG7 2PQ United Kingdom
+ 44 0 1189 702050 • Fax + 44 0 1189 702321
www.mrcy.com