

CORRECT BY CONSTRUCTION FOR LSCOA

A new take on an old technique is neutralizing cyber threats before they materialize.

*by Col. Trent Mills, Maj. Nikesh Kapadia and
Robert Price, Lt. Col., USA (Ret.)*

Are we willing to accept the risk of adversaries adapting cyberattack tactics, techniques and procedures (TTPs) faster than we can push new software updates? Are we willing to expose the warfighter in comms-sensitive environments to the risk of unverified software updates that may break their system?

In today's dynamic digital environment, these questions demand foolproof solutions. Yet the DOD has been conditioned to accept vulnerable software. We have resigned ourselves to a learned helplessness that defaults to applying patches after discovering software vulnerabilities. In protracted, large-scale combat operations (LSCO), this resignation will translate into catastrophe on the battlefield. However, solutions exist now to secure Army systems. It's just a matter of knowing what they are and how to apply them.

URGENT NEED FOR SOFTWARE FORTIFICATION

The continued success of our Human-Machine Integrated Formation efforts, highlighted at the Project Convergence Capstone 5 demonstration in March 2025, will paradoxically invite our adversaries to strike where we are weakest: Our networked computers on wheels and ubiquitous uncrewed systems. Our creativity and willingness to integrate robots and advanced software into our formations will provide additional attack surfaces for our adversaries to exploit.

In July 2024, the former Army Secretary, Hon. Christine Wormuth, flew on a fully autonomous UH-60A called Aircrew Labor In-Cockpit Automation System (ALIAS),

a program run by the Defense Advanced Research Projects Agency (DARPA) and transitioned to the Program Executive Office for Aviation in December 2024. When the flight ended, she approached the Army's own autonomous UH-60L test vehicle (MX) outfitted with the latest launched effects capabilities. Her first question was how to protect the autonomous systems from being hacked and used against us. The DARPA director at that time, Stefanie Tompkins, told Wormuth about a DARPA program called High-Assurance Cyber Military Systems (HACMS). HACMS proved unequivocally that a Boeing unmanned little bird (H-6U) and a commercial off-the-shelf (COTS) quadcopter circa 2017 could be protected from attacks even when the hackers had full access to the system for months using formal mathematical methods, also called formal methods. Last year, the Army applied formal methods to secure a Polaris MRZR in another DARPA test under the program, Assured Micropatching. These examples of collaboration join several others over the past decade, but their successes are disparate, small-scale and largely unharnessed by the services.

WHY FORMAL METHODS, AND WHY NOW?

For years, industry has used formal methods to verify software, but these capabilities are rarely scaled to DOD challenges. However, early DARPA-Army partnerships have pioneered how formal methods can secure cyber-physical systems: Think military systems that are a complex integration of analog, software and hardware components working together to deliver a warfighting capability. Formal methods are mathematically rigorous techniques that ensure code is free from errors and, thus, cyber vulnerabilities. For those who don't speak in terms of parsers and kernels, formal methods are the checklist and mathematical proofs (i.e., guarantees) that ensure a system does what it is specified and verified to do.

When building a bridge, instead of hoping it will not collapse, the engineer uses strict mathematical calculations to prove it will not. Before DARPA's advancements, such tools for existing software development pipelines were out of reach. Today, they're within reach and when applied to an Army system like the MRZR, formal methods demonstrated that even if a red team hacked the system, the hacker could not make the MRZR do something the blue operator did not approve.

Recent advances in formal methods tools, practices, training and ecosystems, combined with dramatically increasing computing capabilities, make applying formal methods at larger scales more affordable than ever. Today, various U.S. government agencies and industry leaders invest in formal methods due to the growing

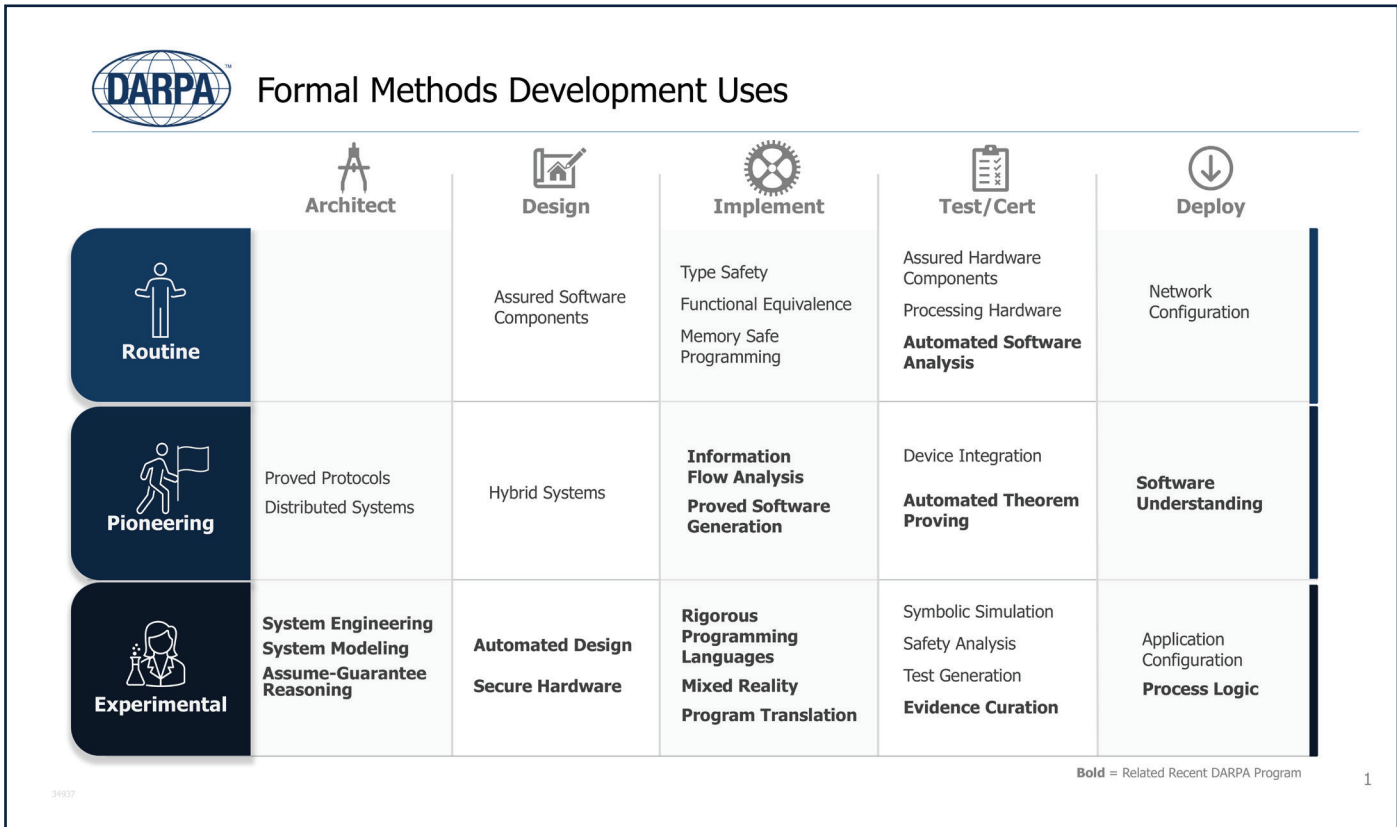
reliance on software and hardware in critical systems, such as space and aircraft flight control, critical infrastructure, communication security and medical devices.

The Army can leverage investments made by DARPA's Resilient Software Systems portfolio to secure systems:

- **Assured Micropatching (AMP)** tools sustain binary-only embedded software and firmware for which source code is no longer available.
- **Automated Rapid Certification of Software (ARCOS)** automates the evaluation of software assurance evidence to enable certifiers to determine the risk of software deployment is acceptable.
- **Cyber Assured Systems Engineering (CASE)** tools provide necessary design, analysis and verification tools to allow system engineers to design in cyber resiliency.
- **SafeDocs** tools verify data coming in and out of systems and their components.
- **Verified Security and Performance Enhancement of Large Legacy Software (V-SPILLS)** tools enable modernization of large legacy software systems.

The Army can help guide the operational direction of DARPA's new assurance programs:

- **Assured Neuro Symbolic Learning and Reasoning (ANSR)** develops novel algorithms that integrate contextual understanding to build safety and trustworthy military systems.
- **Pipelined Reasoning of Verifiers Enabling Robust Systems (PROVERS)** makes formal methods accessible to the engineers and integrates tools into the design process.
- **Safe and Assured Foundation Robots for Open Environments (SAFRON)** seeks new approaches to ensure Foundation Model-controlled robots perform as directed by warfighters.
- **Securing Artificial Intelligence for Battlefield Effective Robustness (SABER)** seeks to operationalize adversarial-AI techniques and red teams to assess emerging military systems.



PROCESS FOR SUCCESS

DARPA’s Resilient Systems Portfolio consists of programs with a shared vision to increase the survivability of our military systems. This chart highlights examples of formal methods techniques based on maturity level (vertical axis) and ways to implement them (horizontal axis). (Graphic courtesy of Matthew Wilding, DARPA)

THE ARMY PREPARES FOR THE NEXT FIGHT

In 2016, the HACMS “edge” case included a malign actor using a USB stick to hijack an Army system. At the beginning of the program, the HACMS red team could hack into the H-6U onboard flight-control computer and take control of the entire system. Then, the HACMS blue team modified the H-6U using formal methods and gave the same red team six weeks of unfettered access to the H-6U. They couldn’t hack it. The red team was then given access to a non-essential partition of the helicopter as a way in, but the red team could not expand access or disrupt operations. In other words, the front door of the bank was open, but they did not have the combination to the vault. Perhaps more importantly, the safety pilots of the H-6U did not know the system was hacked as it maintained full functionality. To demonstrate durability of the solution, DARPA offered the same HACMS 2016 quadcopter to hackers at the premier defense hacking conference, DEF CON, for another go. They also failed.

Formal methods can secure DOD systems now. If inclined, the Army could proactively apply formal methods to the Autonomous Resupply Vessel before it rolls off the production line, or the Navy could reinforce the 240-ton DARPA autonomous vessel called USX-1 Defiant (conducting sea trials in 2025). But the scope doesn’t have to be limited to just future systems; rather, formal methods can be applied to legacy systems warfighters rely on today.

Formal methods can minimize software updates for network-connected capabilities. Doing so would increase survivability by extending the time Army systems can operate in no-comms environments.

“Formal methods are the best route to shift security from a reactive practice to a proactive guarantee that we can build upon to

gain advantages in the DOD,” said Mark A. “AI” Mollenkopf, science advisor to the U.S. Army Cyber Commanding General.

The Army can make protracted LSCO possible—think secure and survivable weapons systems, transport platforms, critical infrastructure and lines of communication that are ready for the next fight.

Rapid action to implement formal methods tools in current and future systems can dramatically reduce the DOD’s software vulnerabilities. In fact, DARPA estimates that broad application can eliminate 80 to 90% of our military’s cyber vulnerabilities.

“Formal methods application should start at the outset of the formal requirements process to secure our weapons systems and other platforms,” said Maj. Gen. Jake S. Kwon, director of Strategic Operations, Headquarters, Department of the Army G-3/5/7. “We can ill afford to retrofit our weapons systems after they’re fielded. As formations continue to experiment with COTS solutions and coding at the edge, formal methods provide a clear advantage in securing our innovation efforts.”

ASSURANCES IN THE FUTURE OPERATING ENVIRONMENT

Although formal methods offer many benefits, they are not a silver bullet. The adversary has a vote and is already enhancing their cyberattack TTPs.

Future Army systems increasingly rely on artificial intelligence (AI)-based technologies to propel the capabilities of robotics and decision support tools towards the complex military scenarios in the future. However, large neural network architectures and foundational models create new opportunities for adversaries to corrupt data feeds and exploit underlying algorithms. DARPA is exploring how we can secure these emerging AI technologies. Moreover, the Army can help them understand the future operational concepts and lean forward on new requirements to build assurances for our future military systems. These assurances will ensure that military AI-based systems perform as expected in complex and dynamic battlefields.

CONCLUSION

The Army and DARPA are collaborating on a capstone application of formal methods. Instead of a single platform, the Army is considering an entire acquisition line. The Air Force and Navy are also participating. In the aggregate, these capstone efforts will signal that the DOD Enterprise understands the software vulnerabilities underpinning the Interim National Defense Strategy and

supporting warfighting concepts, and serves as a leap forward in creating learned resilience across the joint force.

For more information, go to <https://www.darpa.mil/research/research-topic-spotlights/formal-methods>.

COL. TRENT MILLS is the Army advisor to the DARPA director. He is an Army strategist with a Ph.D. in rhetoric from Georgia State University, and holds an M.A. in national security and strategy from the Naval War College, an M.A. in English from Washington State University and a B.A. in English from Gonzaga University. He has a deep background in modernization efforts for the land domain (U.K. and U.S.). His previous assignment was with the Director of the Army staff.

MAJ. NIKESH KAPADIA is a DARPA innovation fellow leading fundamental science research towards Army operational challenges. He is an Army FA-49 (Operations Research and Systems Analysis) officer with an M.S. in systems engineering from the University of Virginia and a B.S. in mechanical engineering from the U.S. Military Academy.

ROBERT PRICE, LT. COL., USA (Ret.), is completing his 15th year as a systems engineering and technical advisor supporting the DARPA Director’s Office. He holds an M.S. in information technology management from Colorado Technical University; an M.S. in international relations from Troy State University; an M.S. in data analytics and policy from Johns Hopkins University; and a B.A. in psychology from the University of Virginia. Before retiring, he served two tours on the Army staff, contributing to critical digitization efforts in the G-3/5/7 and Program Objective Memorandum development in the G-8.