

Project: GPU Unified Architecture for Resilient Defense (GUARD): SE / IoT

Problem: The GPU Unified Architecture for Resilient Defense (GUARD) project seeks to provide a solution for defense in a diversity of IoT systems. The processing needs envisioned to enable the capabilities that our future warfighters need at the tactical edge far exceed what is available today. Forward-deployed tactical edge solutions demand a security posture significantly beyond what is commercially supportable. The GUARD project will develop a secure graphics processing unit prototype that is based on mature commercial GPU technology and proven protection concepts to enable forward-looking architecture for a family of secure edge GPU ecosystems for both defense and commercial applications.

Solution: A low SWaP-C (Size, Weight, Power, and Cost) secure GPU module will enable users to rapidly deploy and update emerging AI algorithms to promote an asymmetric advantage in AI and sensor processing. GUARD will advance the technologies needed to significantly reduce SWaP-C required for future edge computing assets, develop a holistic security posture to protect the control flow of the processor from external influence, ensure the integrity of the system during execution, prevent exfiltration of critical program information, and provide a means to recover from and/or respond to threats in real time. GUARD draws on commercial secure-compute approaches, including confidential compute, trusted execution environments, inline memory encryption, and secure boot, and extends them to meet the security posture and SWaP-C constraints of the defense tactical edge.

Project Performers / Role:

- **Northrop Grumman Corporation (NGC):** Project prime. Integrate their secure processing solutions to deliver edge compute designs, proof of concept demonstrations, and security testing.
- **Battelle:** Security modeling and analysis.
- **The University of Maryland (UMD):** Side channel leakage and vulnerability analysis, security architecture curriculum development.
- **NVIDIA (partner):** Technical consultation inputs for GPU secure compute architecture.

