Objective: Use reconfigurable logic hardware to create general purpose, secure circuitry with zeroize functionality for military systems abandonment in theater. This ensures that the enemy cannot reverse engineer US military systems, while also reducing microelectronics development costs.

Description: Current Army ground vehicle systems operate using Application Specific Integrated Circuits (ASIC), due to Size, Weight, AP-C requirements. One could move to implement designs on a reprogrammable logic board such as a Field Programmable Gate Array, with a System on a Chip (SOC) acting as the design synthesis (programming) tool host on the printed circuit board. The FPGA fabric can be used to implement the functionality that would normally be hosted using an ASIC. FPGAs, by nature (unless using an anti-fuse FPGA design), are reprogrammable. Recent advancements by the major FPGA manufacturers, Altera (Intel) & Xilinx, have brought FPGA systems much closer to the SWAP-C that ASICs operate at. These recent advancements have also brought FPGA encryption and hardening to the level that was required with ASIC designs, making it a valid platform for military systems.

Currently, efforts are only made to harden those electronics that are deemed Critical Program Information (CPI) so that they are either time-impossible, or extremely high effort to reverse engineer. However, non-CPI electronics do not receive the same hardware resiliency, and thus are still at risk of exploitation if captured. If the warfighter must abandon a vehicle in theater, valuable electronics may be attached to that ground vehicle that should be destroyed. Current standard, operating destruction procedures in require the use of pyrotechnics (thermite grenades), which can fail to completely destroy the ASIC hardware. That leaves the enemy with hardware that could be reverse engineered off the intact portion.

By hosting the design on a reprogrammable device, one can achieve the same or near-same level of SWAP-C as would be hosted by an ASIC, but have a reprogrammable design fabric to work with. Using the SOC on the device, hosting a light embedded OS with scripts to execute zero-ization at the touch of a button, one could use the design to create a kill-switch. By rewriting the fabric with a blank design, one would effectively delete the existing logic, thus making it nearly impossible to exploit the hardware. This means that the design would be tamper resistant.

A key example of where this proposed technology would have been extremely useful in was in the year 2001, where China had ‘captured’ a damaged EP-3E spy plane that had to make an emergency landing on Hainan Island Chinese military base. China had ample time to reverse engineer any of the electronics systems onboard that airplane, before returning it back to the USA, partially dismantled.

As such, any hardware ASIC design that can be ported to reprogrammable logic would be the target for this proposal, making upcoming platforms such as the NGCV far more cyber-resilient. And if shown to work, could be something applicable to all DOD agencies and OGAs. The US Army is seeking proposed designs and guidance on how such a re-synthesizable design might be implemented.

Phase I: Offeror shall conduct a feasibility study through research on whether current general purpose FPGA boards and design logic can be adapted to this design. This study shall include viability and potential applications, not covered by this topic, for military, medical, and commercial implementations.

Phase II: Depending on the results of the Phase I feasibility study, the Offeror shall implement the logic design of a system from a military ground vehicle on an FPGA platform (i.e. Altera or Xilinx) to show a proof of concept prototype. Offeror will propose the system architecture that is to be used (hardware, software, etc.). Offeror will create design logic for an FPGA using respective FPGA environments. This logic will implement a systems design that meets military data encryption standards. Offeror shall also create software that can synthesize the FPGA logic with a zeroized design if given a command to do so. This software shall be able to interface with a user interfacing system (hardware). At the end of Phase II, Offeror shall have a working prototype of this system with a Technology Readiness Level of at minimum, TRL6. Offeror shall also have a business model ready for marketing the proposed system to commercial vendors.
PHASE III DUAL-USE APPLICATIONS: Offeror will develop systems that can be retrofit with current military ground vehicles. This will provide the US military with capabilities of protecting government and our contractor’s intellectual property during wartime. It will also prevent enemies from reverse engineering our hardware and using our own designs to harm our warfighters.

Additionally, this design can see commercial viability by allowing for companies to protect their trade secrets and intellectual property, either from competitors, foreign nations, or malicious actors.

REFERENCES:


KEYWORDS: Reconfigurable, Logic, Zeroize, Organic, Circuit, FPGA, System on a Chip, SOC, tamper, Electronics, Microelectronics, Zeroization