A DARPA Approach to Trusted Microelectronics

A Technology-Enabled Trust Approach

Given changing threats, continued evolution in the globalized and commercially-driven semiconductor industry, and other emerging challenges, new efforts are required to ensure microelectronics security. DoD is therefore considering a technology-enabled approach to securing its microelectronics supply chain. This approach aims to provide tailored device protection while allowing greater leveraging of the advanced commercial capabilities required for high-performance military systems. Under this proposal, DoD will maintain a portfolio of technologies designed to meet the DoDI 5200.44 requirement for tailored protection of critical components. Selective application of these solutions, based on the risks faced, would help DoD to prevent, detect, and respond to threats throughout the acquisition process.

DARPA—along with DoD Service Labs, the Intelligence Advanced Research Projects Agency (IARPA), and other research and development institutions—is advancing the technologies required for a new security approach. These efforts should enable DoD to obscure the purpose of sensitive devices, verify device origin and function, protect against IP exploitation, and expand its microelectronics supplier base. This "trust through technology" framework emphasizes verifying the integrity of electronics, protecting sensitive IP in the supply chain, and better leveraging leading-edge, commercial semiconductor capabilities, many of which are available from global multinational firms operating in the United States.

DARPA is implementing various technology solutions, grouped into multiple classes—verification and validation, obscuration and marking, functional disaggregation, fine disaggregation, transience, and government-proprietary solutions—based on the protections provided and the expected level of interference into supplier best practices [Figure 5]. Protections that minimize interference into standard business practices tend to emphasize the leading-edge commercial manufacturing required for many high-performance military systems. Conversely, protections that require greater levels of government involvement in the ASIC lifecycle tend to emphasize the use of limited, strategic foundry partnerships in order to protect critical IP. Other protections may allow for blended partnerships that involve both commercial and strategic foundry partners.

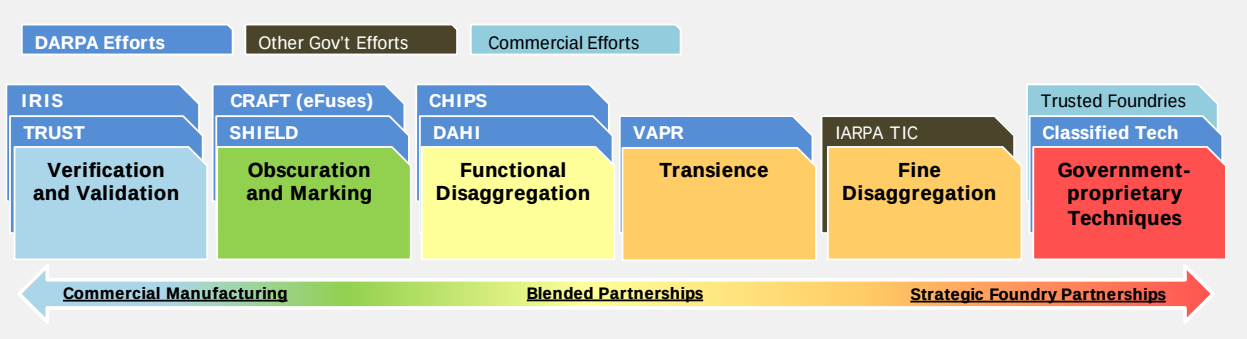

Figure 1. DARPA proposes multiple countermeasure groups, such as verification and validation. Individual tabs represent a non-comprehensive list of DARPA and other government programs as well as commercial protection efforts.

These technology-enabled protections should allow DoD to complement and improve upon the security currently provided under DoD's trusted supplier system. In providing a portfolio of security solutions, DARPA, other Federal agencies, and industry partners can enable acquisition personnel to selectively apply technological countermeasures based on a component's criticality, the risks faced, and the need to use leading-

edge technologies [Figure 6]. This developed suite of technologies should also allow DoD to securely access a broader set of commercial vendors [Figure 7].

	Protection	Program	Microelectronics Security Threats: CPI Theft	Fraudulent products	Loss of access	Malicious insertion	Quality & reliability
Strategic Foundry Partnerships	Government-proprietary	Other	●				
	Fine Disaggregation	**TIC** (IARPA): Disaggregate ASICs into non-functional parts	●	●	○	○	
	Transience	**VAPR**: Shatter lost, misplaced, or end-of-life ASICs on command	●				
Blended Partnerships	Functional Disaggregation	**SPADE**: Use secure parts to monitor commercial components packaged together into a single ASIC	●			●	●
		DAHI: Disaggregate ASICs into functional subcomponents	●		○	●	
		CHIPS: Establish a library of pre-verified, modular ASIC design IP	○		○	●	●
Commercial Manufacturing	Obscuration and Marking	**CRAFT**: Apply modularity to reduce ASIC design effort and allow portability across foundries			●		●
		eFuses: Obscure ASIC functionality until after manufacture	●			●	
		SHIELD: Authenticate ASICs at any point in the supply chain	○	●			
	Verification and Validation	**IRIS**: Derive an ASICs functionality and reliability		●		●	●
		TRUST: Reverse engineer ASICs and compare to design		○		●	

● Primary Impact ○ Secondary Impact

Figure 2. Trust through technology can help complement, improve, or replace the traditional trusted vendor security approach, providing protection against a range of microelectronics security threats.

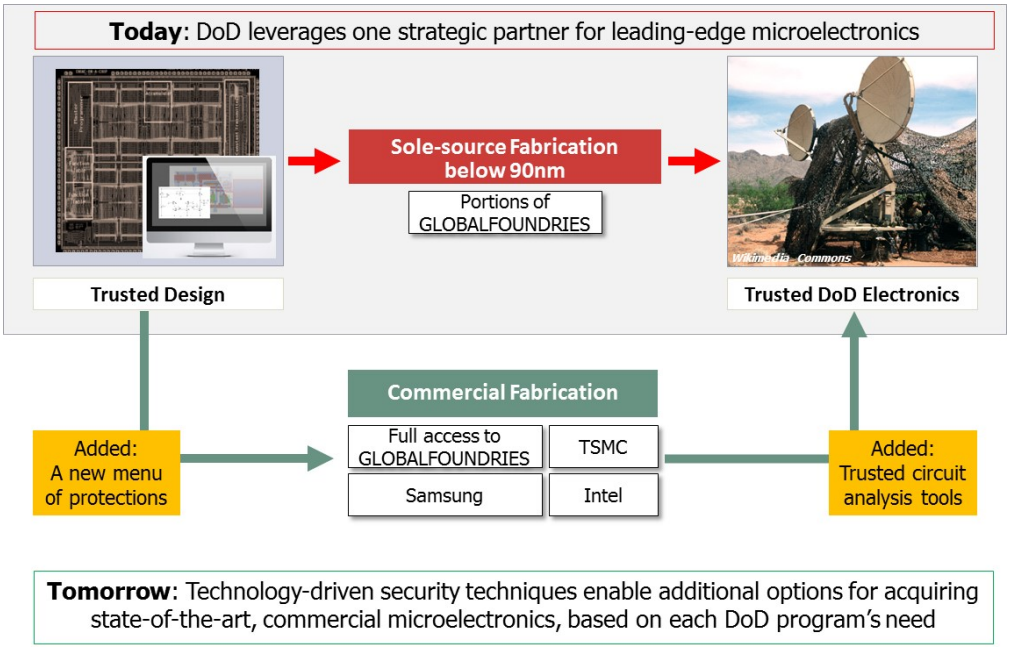

Figure 3. DARPA technologies should allow DoD to securely access a broader set of commercial microelectronics fabrication options, particularly for leading-edge devices.

A “trust through technology” example

To ensure the security of its critical microelectronics, DoD’s technology-enabled trust approach will enable acquisition personnel to selectively apply various technological countermeasures based on the component’s criticality, the risks faced, and the need to leverage leading-edge commercial processes. The following use case presents a potential concept-of-operations for protecting a representative device [Figure 8].

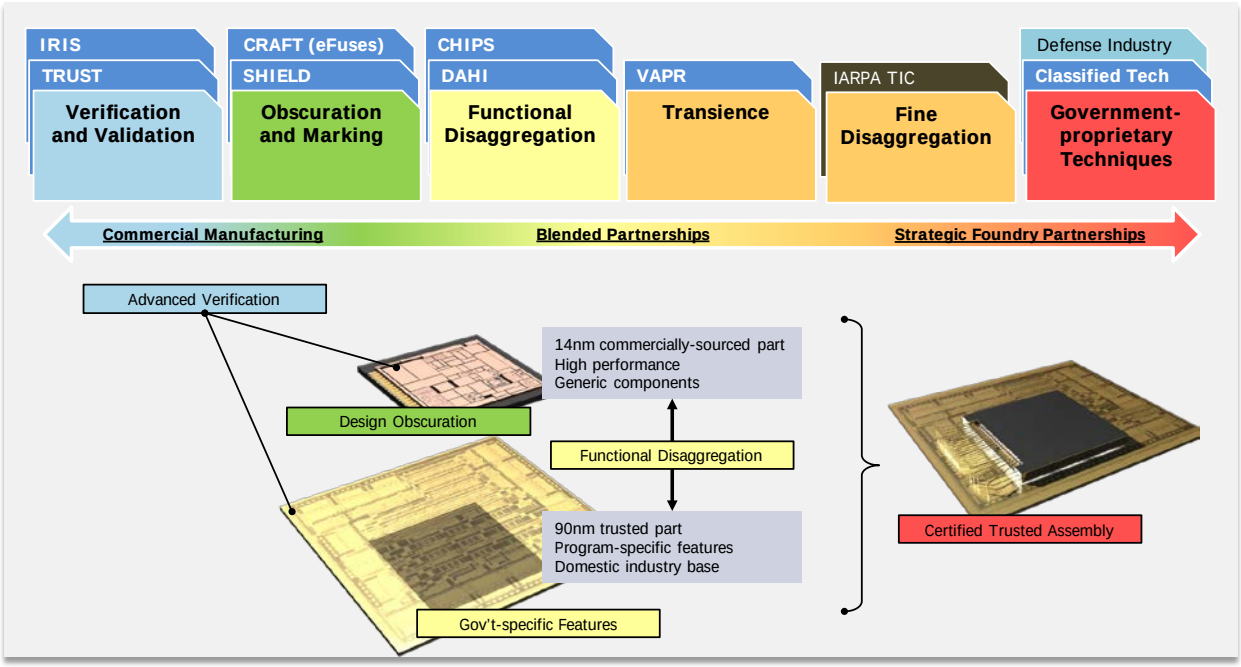

Figure 4: Selective application of countermeasures can demonstrate "trust through technology" for a representative device.

Microelectronics acquisition

During the acquisition process, DoD and its contractors determine the requirements for the device. Stringent size, weight, power, and performance requirements require the use of leading-edge commercial processes currently unavailable through the trusted supplier model. In addition, protecting against malicious insertion and loss-of-information threats suggest the need for high levels of protection.

Functional/Fine disaggregation

Applying functional disaggregation countermeasures enabled by DARPA’s SPADE program would allow DoD to leverage the performance of leading-edge technologies while restricting sensitive information to accredited vendors at less-advanced nodes. Fine disaggregation techniques under development at DARPA and IARPA could provide alternative protection measures.

Obscuration and marking

Using CRAFT’s object-oriented-design process, DoD could help ensure supply chain stability by creating designs that are portable across different foundries, manufacturing processes, and technology nodes. DARPA is exploring a component design that would enable construction at two different foundries. A component constructed using the CRAFT process could be available by FY2017.

Applying obscuration and marking countermeasures would provide for the protection of sensitive CPI, above and beyond the use of trusted vendors. Electronically activated fuses would prevent malicious actors from identifying the intent and function of the final device until after personalization at a DoD facility.

Transience

Transience countermeasures could be applied to later protect the IP in DoD microelectronics by enabling the on-command destruction of lost, misplaced, or end-of-life ASICs.

Verification and validation

Once DoD receives the disaggregated manufactured parts, applying verification and validation techniques enabled by DARPA's TRUST and IRIS programs would allow DoD to ensure that components behave only as expected.

Government-proprietary solutions

Finally, the assembly and personalization of manufactured components into a final device could leverage vendors approved through a more traditional, policy-based trust approach.

Conclusion and Summary

As demonstrated in the above example, DARPA's "trust-through-technology" techniques are designed to meet two purposes. First, they should allow for a tailored response to the range of microelectronics threats, including maliciously altered parts, counterfeit products, hardware and IP theft, quality and reliability failure, and loss of access to sole-source suppliers. Second, they should increase DoD's ability to leverage the leading-edge capabilities being developed by the commercially driven, highly diversified, and quickly adapting semiconductor industry. DARPA pilot projects and demonstration programs aim to further vet the menu of security options, help transition successful technologies to the Services, and provide the confidence required to fully pursue a technology-enable trust approach.