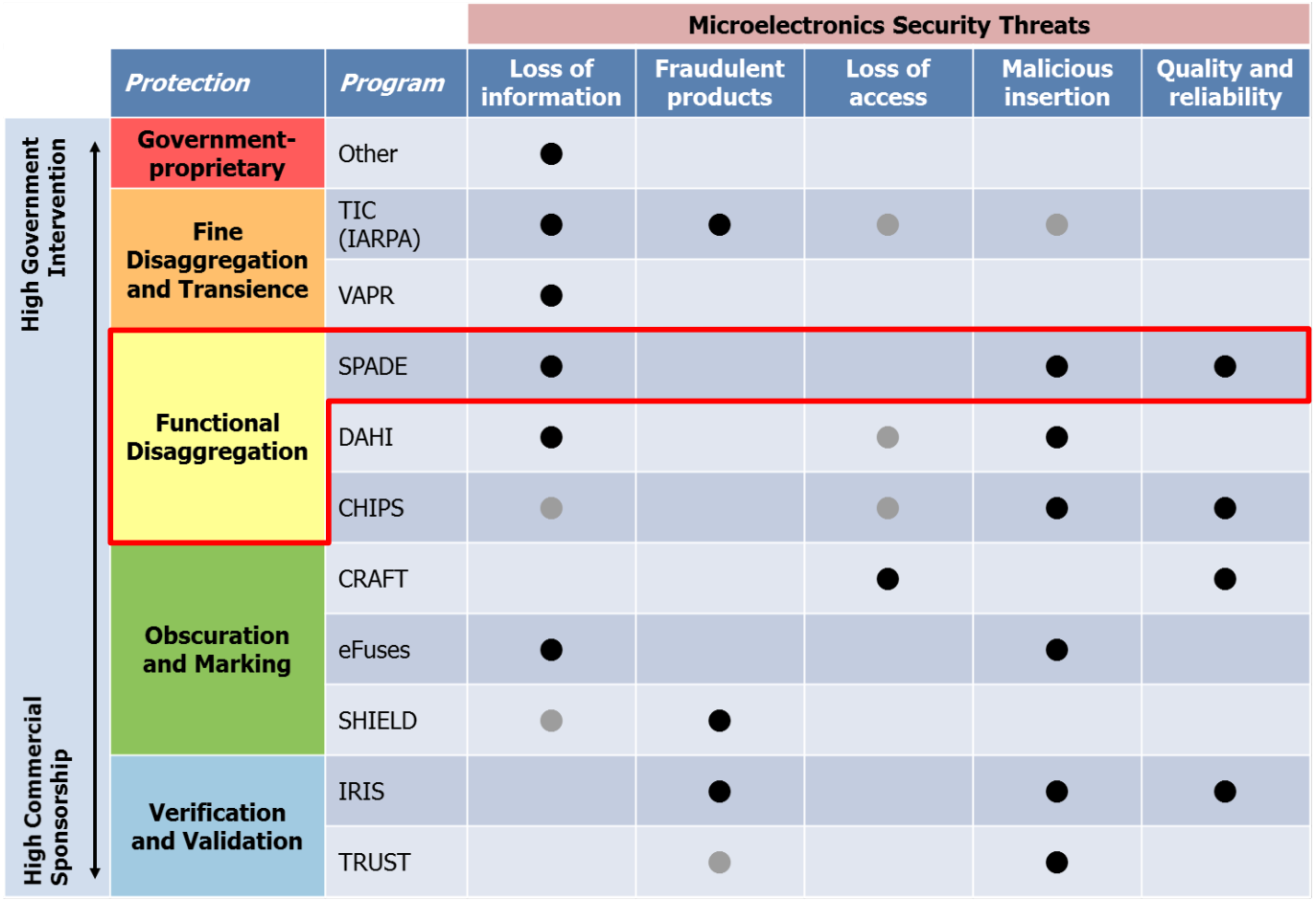
TRUST THROUGH FUNCTIONAL DISAGGREGATION

Ken Plaks, DARPA/MTO Program Manager

NDIA Trusted Microelectronics Workshop

August 17, 2016

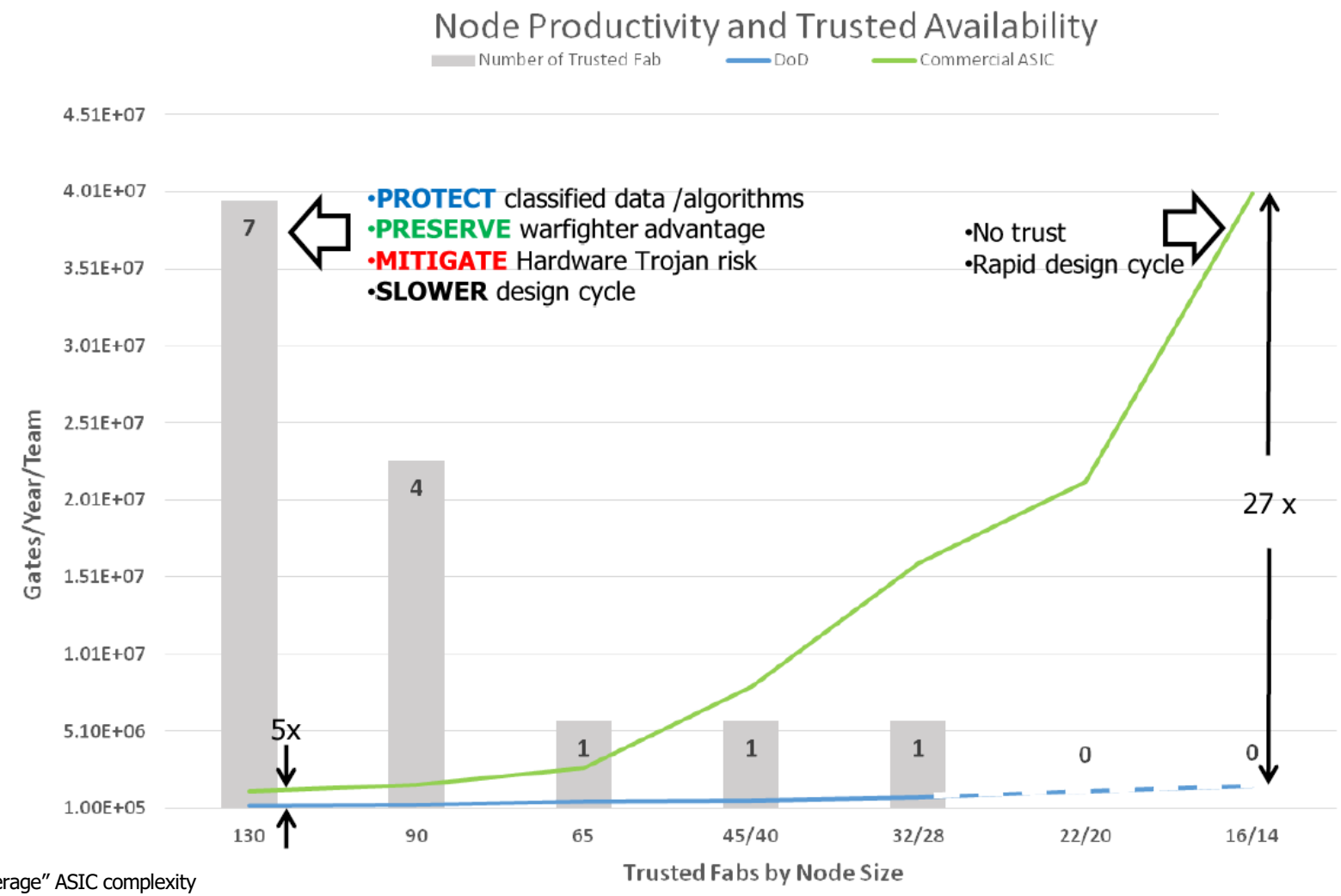
The DARPA solution is to provide a menu of hardware security options that can be selectively applied based on need



		Microelectronics Security Threats				
Protection	*Program*	Loss of information	Fraudulent products	Loss of access	Malicious insertion	Quality and reliability
Government-proprietary	Other	●				
Fine Disaggregation and Transience	TIC (IARPA)	●	●	○	○	
	VAPR	●				
Functional Disaggregation	SPADE	●			●	●
	DAHI	●		○	●	
	CHIPS	○		○	●	●
Obscuration and Marking	CRAFT			●		●
	eFuses	●			●	
	SHIELD	○	●			
Verification and Validation	IRIS		●		●	●
	TRUST		○		●	

SPADE will help to prevent and respond to threats such as the malicious insertion of hardware trojans and reliability failures.

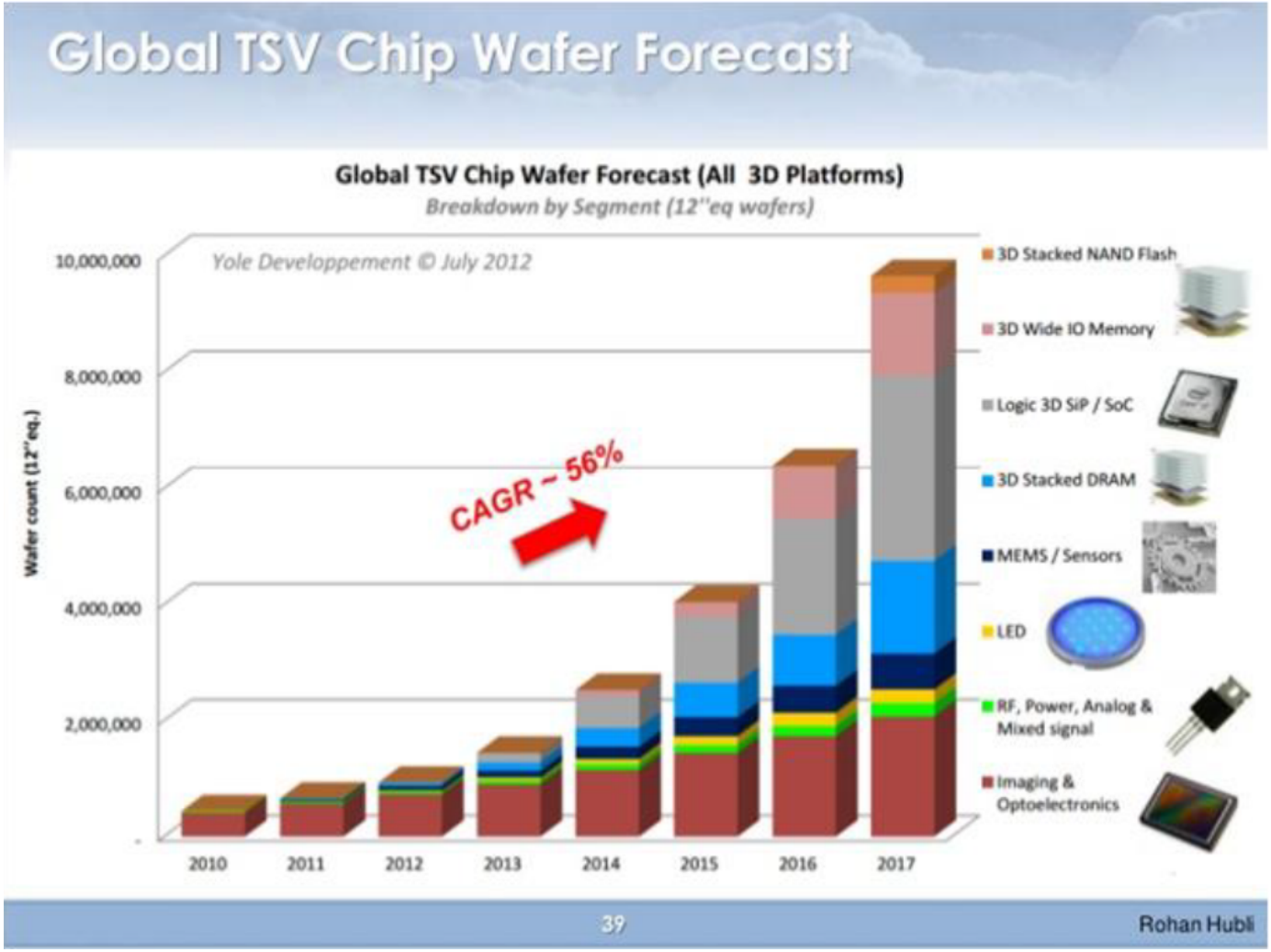
The ASIC Dilemma



Source: ITRS "average" ASIC complexity

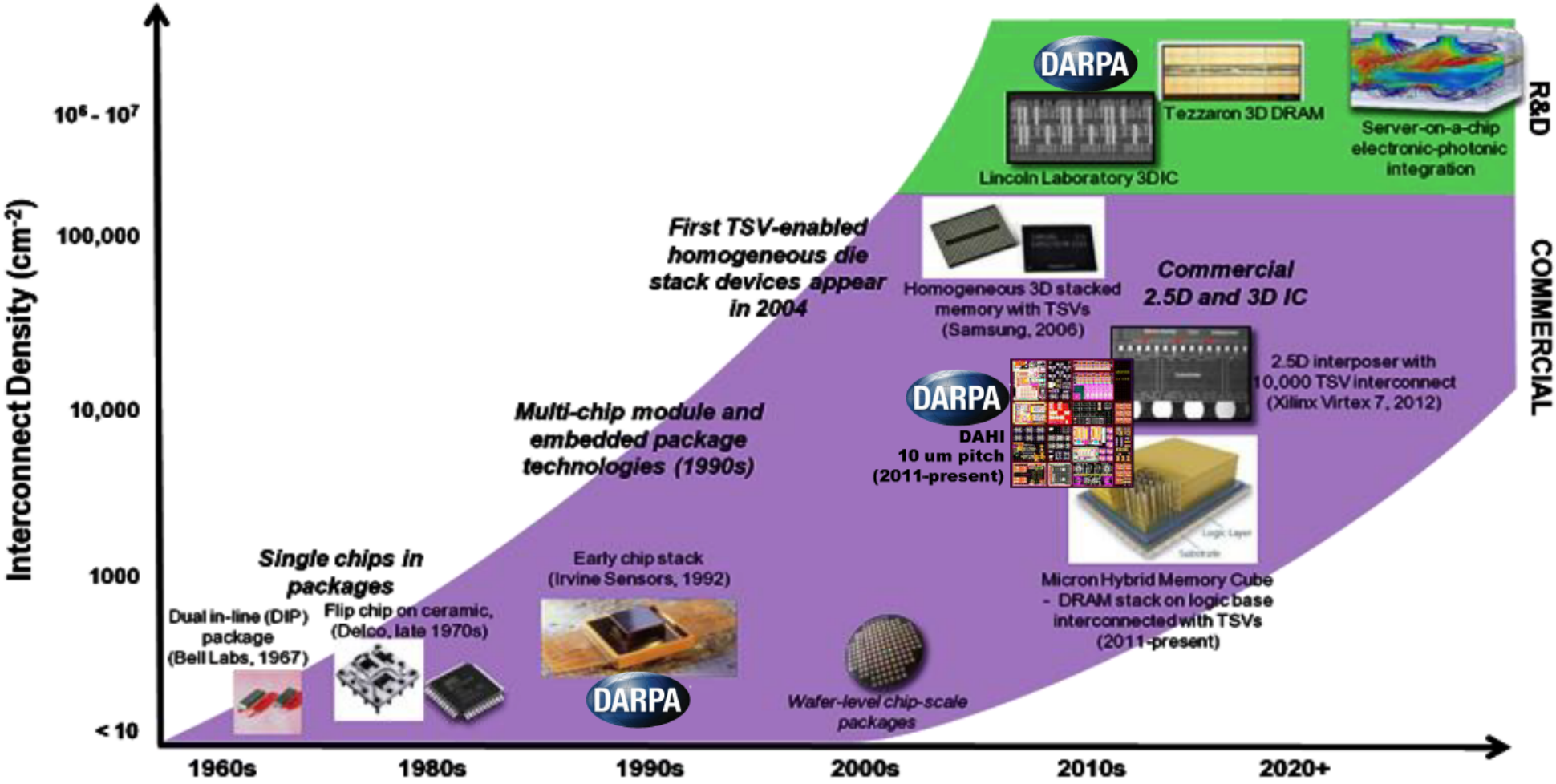
How do we ensure that the warfighter has access to state-of-the-art electronics?

Advanced packaging



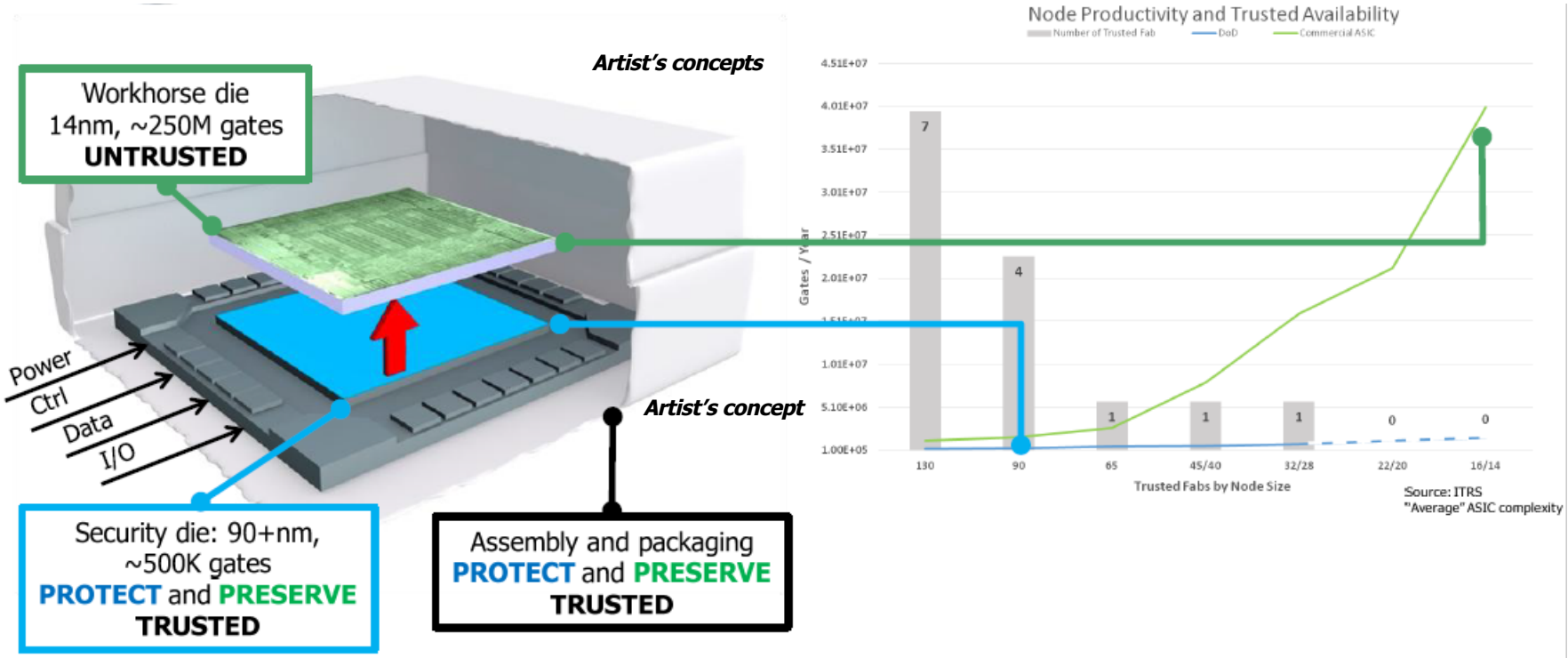
- Manage complexity
- Improve yield
- Allow specialization

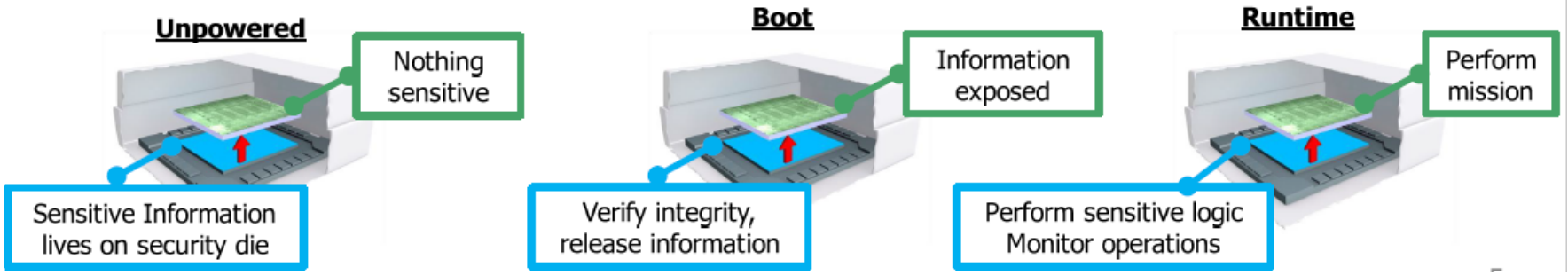
Key technical enabler … interconnects



Source: MIT Lincoln Labs

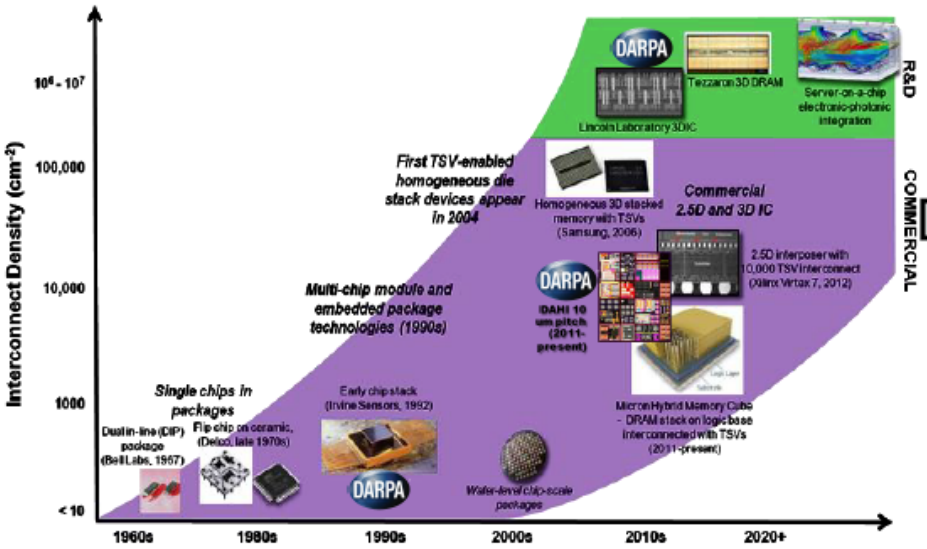
ASIC trust solution

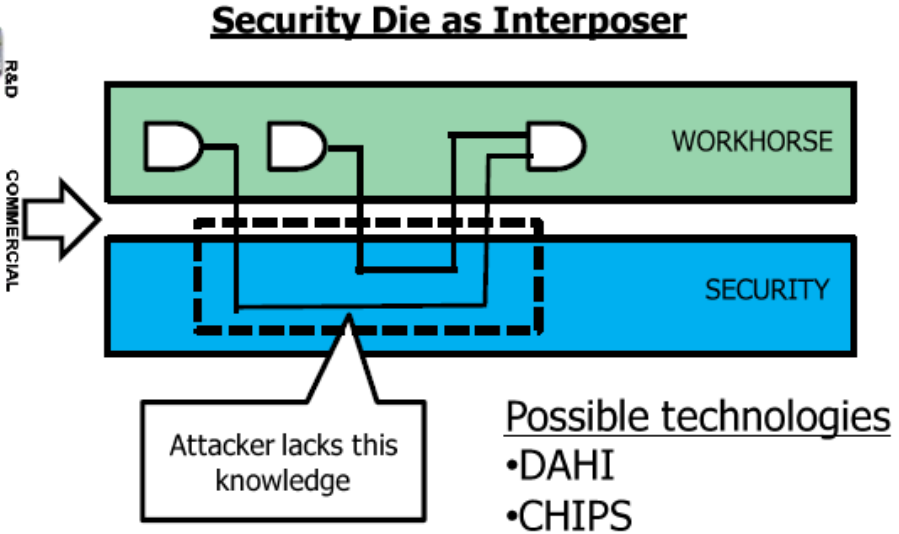




Malicious logic: passive techniques

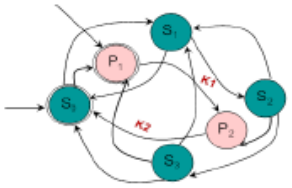
- Goal: make it harder to insert hardware trojan/malicious logic
  - **MITIGATE** risk through obfuscation
  - Interconnect density allows much more thorough obfuscation





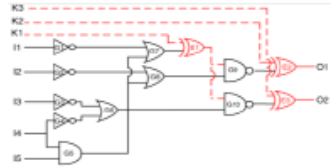
Source: MIT Lincoln Labs

- Plus: full suite of commercial obfuscation techniques…



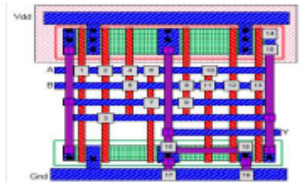
[1] Chakraborty & Bhunia, ICCAD 2008

State-Space Obfuscation



[2] Rajendran et. al., IEEE Tcomp, 2015

Logic Encryption

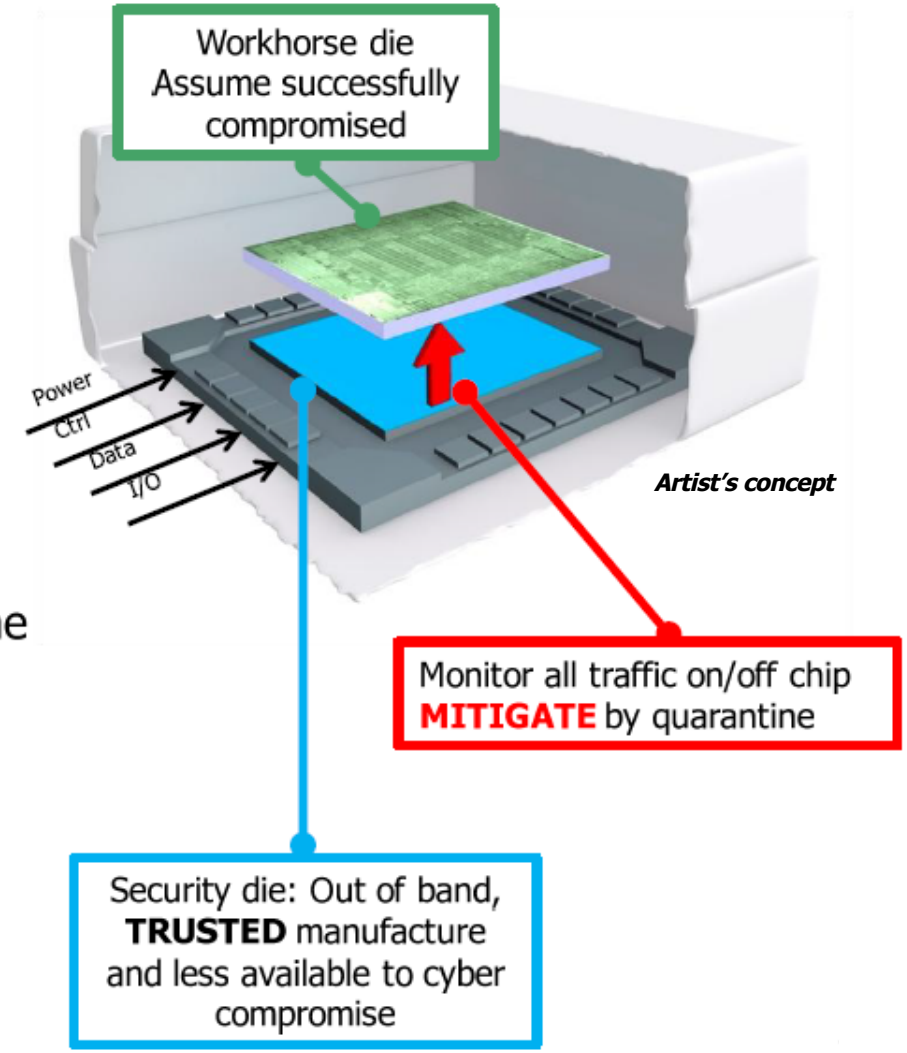


[3] J. P. Baukus et al., U.S. Patent 8111089, 2012

Camouflaging

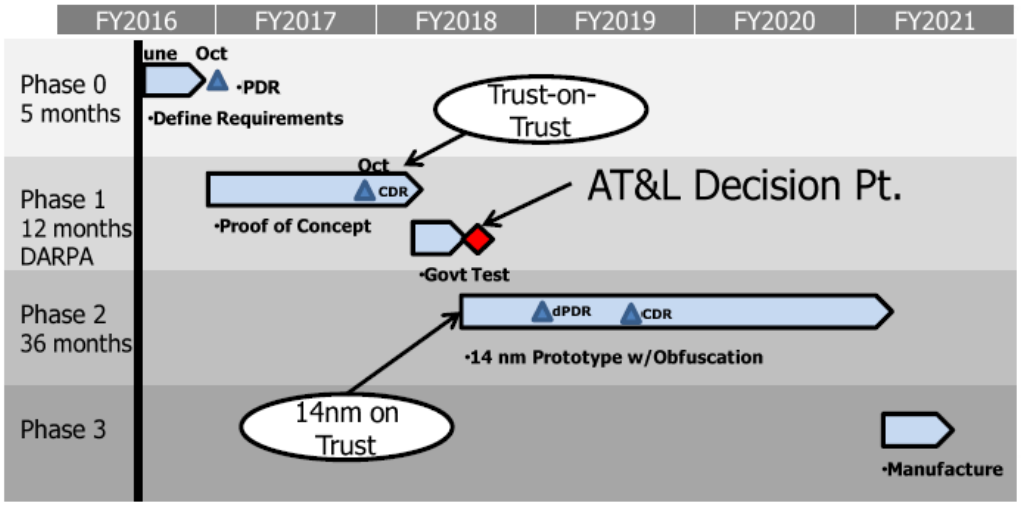
Malicious logic: active techniques

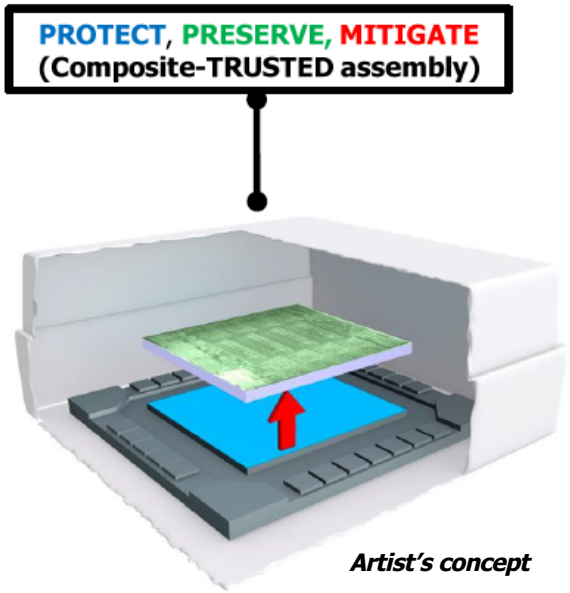
- Assume: attacker has successfully compromised untrusted portion
- Goal: **MITIGATE** impact and contain contamination
- Key research questions:
  - How do you detect?
  - How do you mitigate impact?
  - Is it scalable? Performance impact?
- Security die moderates all signals:
  - Enables active monitoring
    - IO
    - Control
    - State (privilege, etc)
  - Out of band with mission circuits
  - Prevent spread of contagion by quarantine



SPADE trust demo for ASICS

- Phase 1 DARPA SPADE demo
  - Trust-on-Trust: Surrogate 45/90 nm workhorse
  - Proof of concept, functional demo, security demo
  - Delivers data for phase 2 decision
- Phase 2 SPADE prototype
  - 14nm workhorse
  - Full obfuscation



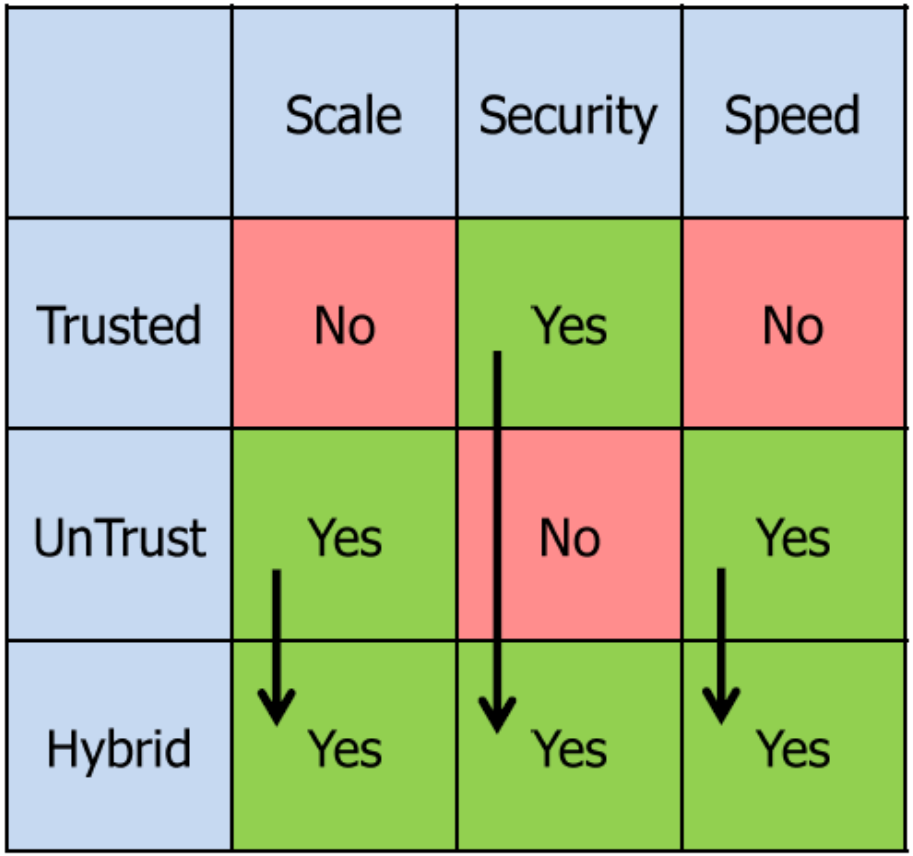


Artist's concept

Achieve the spirit and intent of trust while meeting warfighter need

Conclusion

- DoD is good at protecting critical data,
  - has trouble with large designs
- Industry is good at massive integration,
  - has trouble protecting critical data
- Technology allows a marriage
  - Massive interconnect density
  - Vertical stacking
- Success will allow DoD to
  - **PROTECT** classified data /algorithms
  - **PRESERVE** warfighter advantage
  - **MITIGATE** Hardware Trojan risk
  - **FASTER** design cycles than the status quo



Bring the state-of-the-art back to military electronics

www.darpa.mil