Trusted Supplier Steering Group

Managing Risk with Trusted ASICs: Introducing a Guidebook to Using Trusted Suppliers

NDIA Systems Engineering Conference
Oct. 26, 2017

Guidebook Abstract

This document seeks to guide those who would like to know how to specify and procure Trusted components within DoD or security-sensitive electronics. It details the scope of what types of products and services can be obtained under the current program of accreditation as well as options within the current program. Finally, it guides interested parties to other sources of information relevant to lowering risk and increasing security within electronic systems.

Entire systems can be brought down with a single unauthorized change of the smallest integrated circuit transistor or the loss of a key semiconductor supplier.

Presentation Preview

- Intro to Intrinsix
- Disaggregation Creates Supply Chain Risk
- DoD Responds with Trusted ASICs
- Risks, Rules, Realities
- Summary and Reasons for Guidebook
- Feedback/Questions

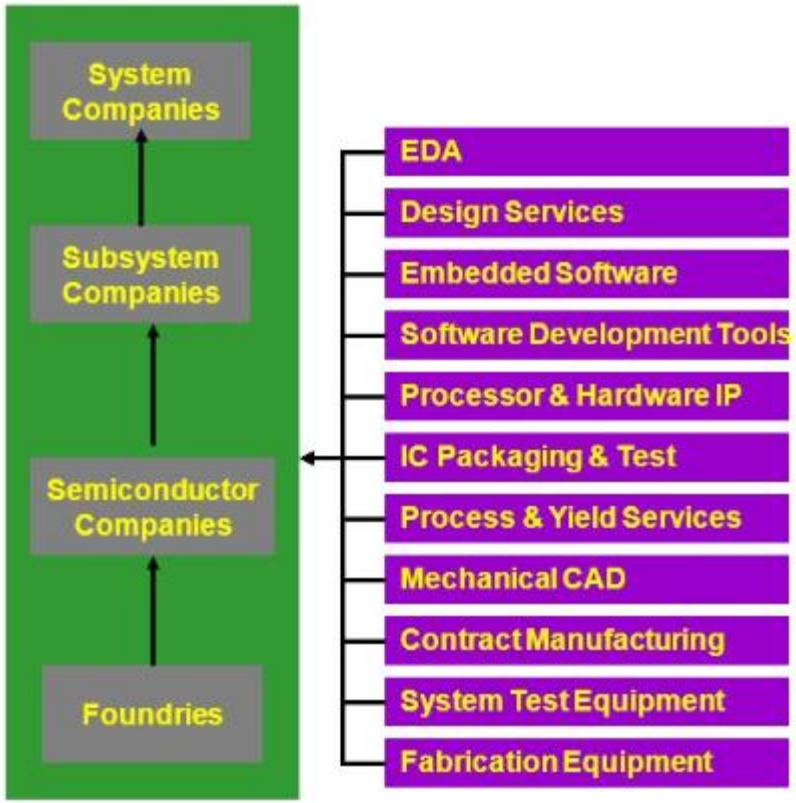
Introduction to Intrinsix

- Mixed-Signal SoC Design Services
- Team of ~60: Predominantly staffed with 15-20 year IC realization experts
- Trusted Design and Broker, Accredited since 2007, TSSG Member
- Supplier to advanced DoD and commercial semiconductor industry since 1986

Intrinsix Corporate Headquarters
Marlborough, MA

Economics Drive Disaggregation

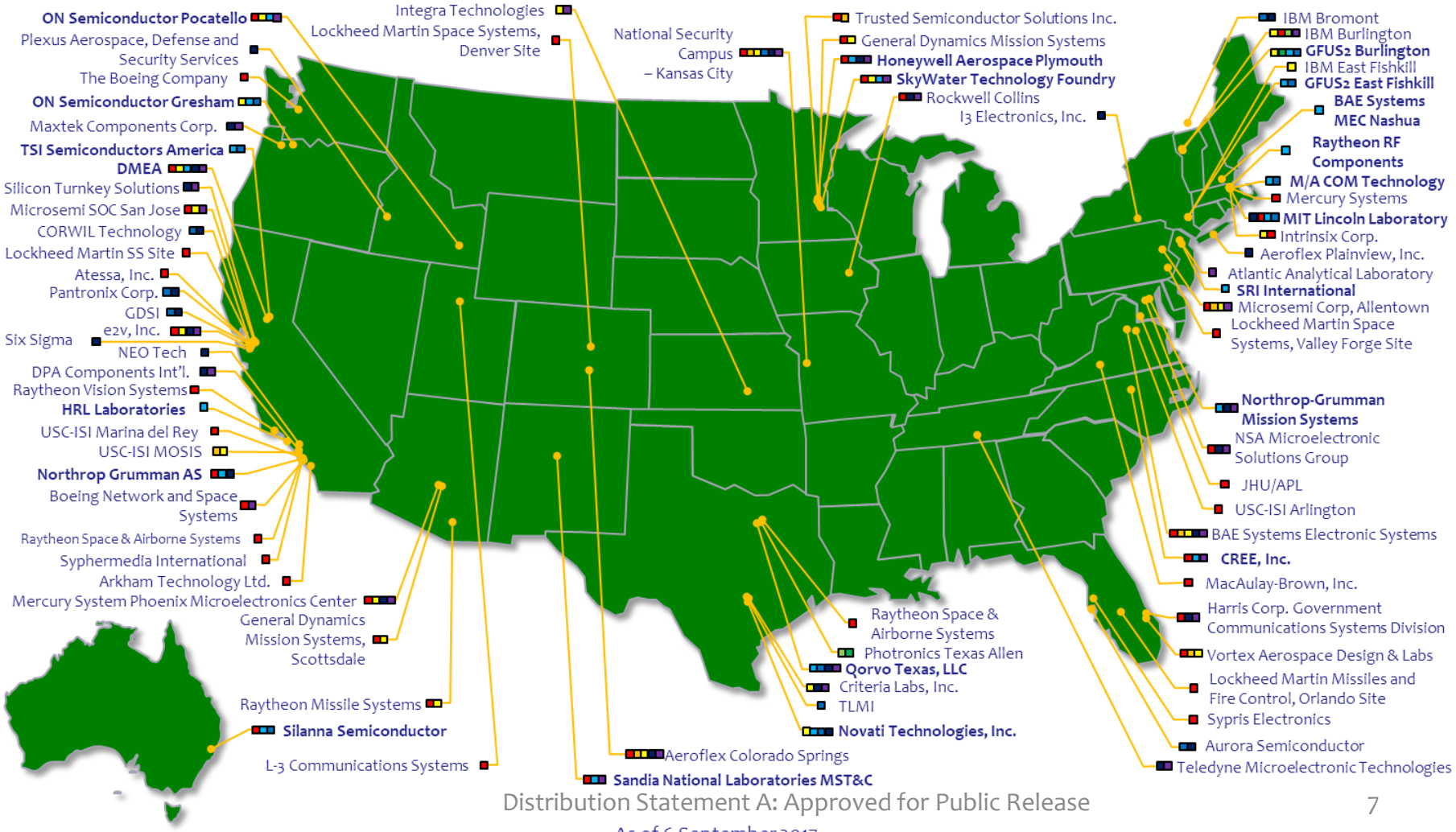
- Disaggregation multiplies risk as supply chain creates new links
- Systems companies' "in-house" or "captive" solutions lose competiveness over time
- ASIC Flows highly disaggregated and therefore inherently riskier



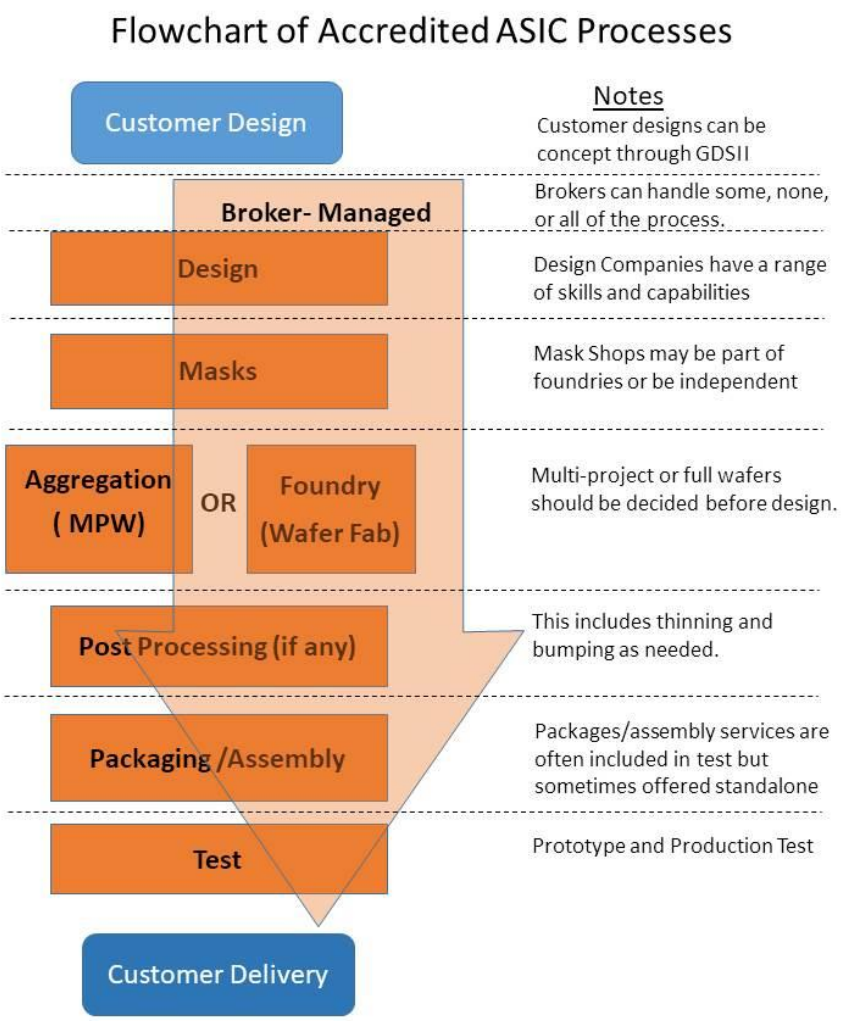
History of Trusted Accreditation

- **2003:** The Trusted Foundry Program Established
  - Administered and managed by the DoD Defense Microelectronics Activity (DMEA).
- **2005:** Defense Science Board Report highlights risk of "Trojan Horses", Recommends Expansion of Trusted Program
- **2007:** Program broadened to entire microelectronics supply chain for ASICs
  - Accreditation process launched
  - CRADA creates need for DD254
  - DSS provides location and personnel review
- **2010:** Trusted Supplier Steering Group is Formed
- **2017:** Multiple efforts to expand Trust to non-ASICs such as FPGAs, PCBs, Standard Products, etc.

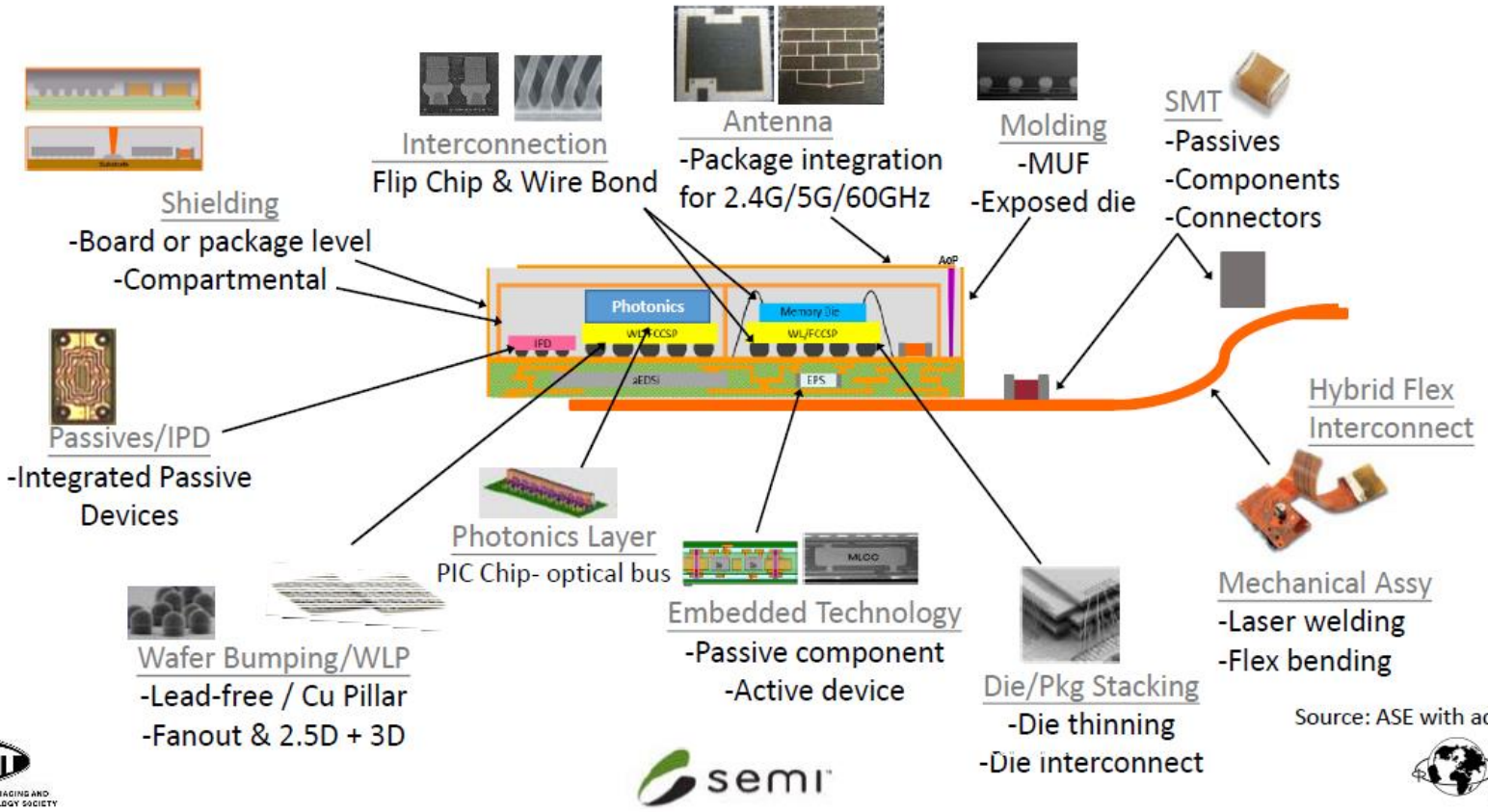
78 Trusted Suppliers



Accreditation Types - Trusted Companies



Future Supply Chains



Heterogeneous Integration is the integration of separately manufactured components into a higher assembly (SiP) that, in the aggregate, provides enhanced functionality and improves operating characteristics

Bill, Chen, " Heterogeneous Integration Roadmap," IEEE CPMC Symposium Japan, Nov 8, 2016

Spectrum of Supply Chain Risks

Quality Escape

Product defect/ inadequacy introduced either through mistake or negligence during design, production, and post-production handling resulting in the introduction of deficiencies, vulnerabilities, and degraded life-cycle performance.

Reliability Failure

Mission failure in the field due to environmental factors unique to military and aerospace environment factors such as particle strikes, device aging, hot-spots, electro-magnetic pulse, etc.

Fraudulent Product

Counterfeit and other than genuine and new devices from the legally authorized source including relabeled, recycled, cloned, defective, out-of-spec, etc.

Malicious Insertion

The intentional insertion of malicious hard/soft coding, or defect to enable physical attacks or cause mission failure; includes logic bombs, Trojan 'kill switches' and backdoors for unauthorized control and access to logic and data.

Reverse Engineering

Unauthorized extraction of sensitive intellectual property using reverse engineering, side channel scanning, runtime security analysis, embedded system security weakness, etc.

Information Losses

Stolen data provides potential adversaries extraordinary insight into US defense and industrial capabilities and allows them to save time and expense in developing similar capabilities.

DoD Program Protection focuses on risks posed by malicious actors

The Growing Risk in Electronics

Global Supply Chains and Increased Cyber Insecurity

Each New Product:

- Many Parts from a Vast Network of Suppliers
- Deep Layers of Hardware and Software
- Dozens of Countries Providing Labor/Parts

Dramatic Rise in Cyber Insecurity

- Criminal Tools Rising at Internet Speed
- More User Features = More Openings
- Economic Pressures Drive Insecurity

Types of Threats

Economic/Criminal Drivers:

- Counterfeits
- Selling of Bad Parts
- Theft of Device or Data or Money

Malicious Nation-States

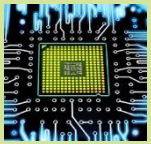
- Terror
- Mission Defeat
- Theft of National Secrets and Industrial Intellectual Property

What to PROTECT in Electronics?

Choose the Intersection of Vulnerability and Criticality

Vulnerability

- What is easy to alter?
- What alteration can be hidden?



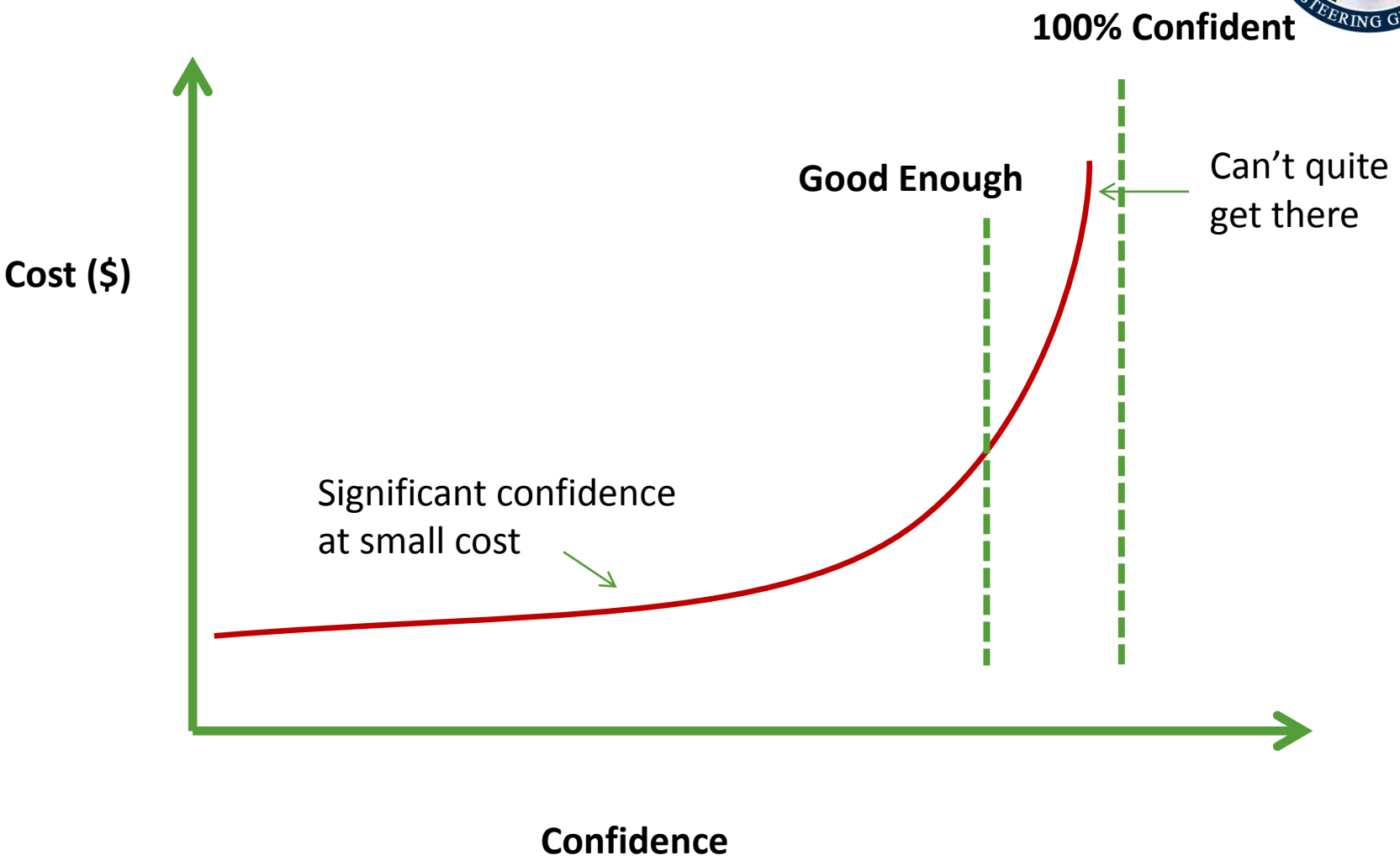
Criticality

- What is Important to Protect?
- Where is the secret sauce?

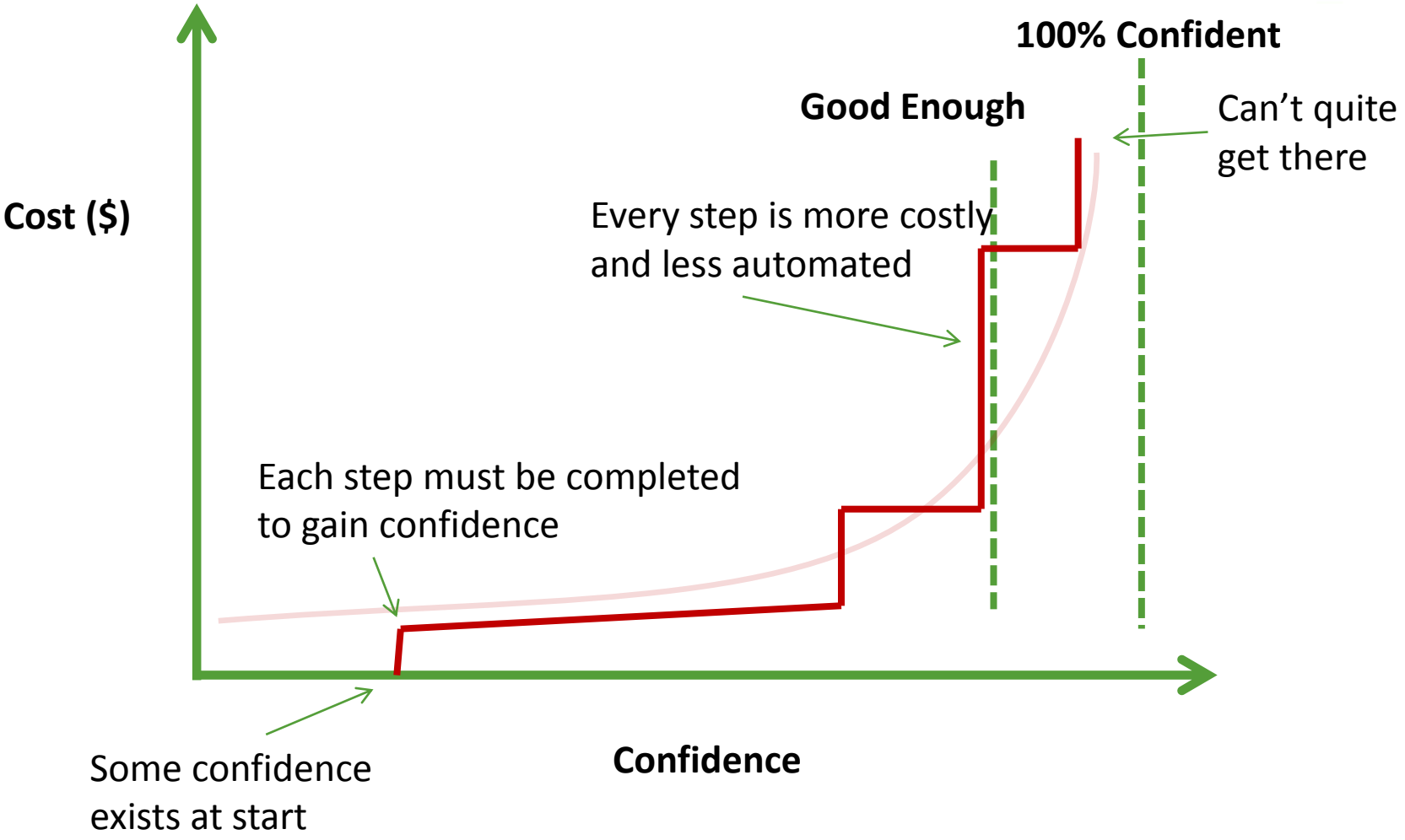
Conclusion: Protect the Intellect!

- Custom Chips: The "Intellect" of all Systems
- Compromised Chips can not be detected easily, if at all
- Offshore Design or Manufacture opens the door to alteration (as well as poor cyber-security within US firms)

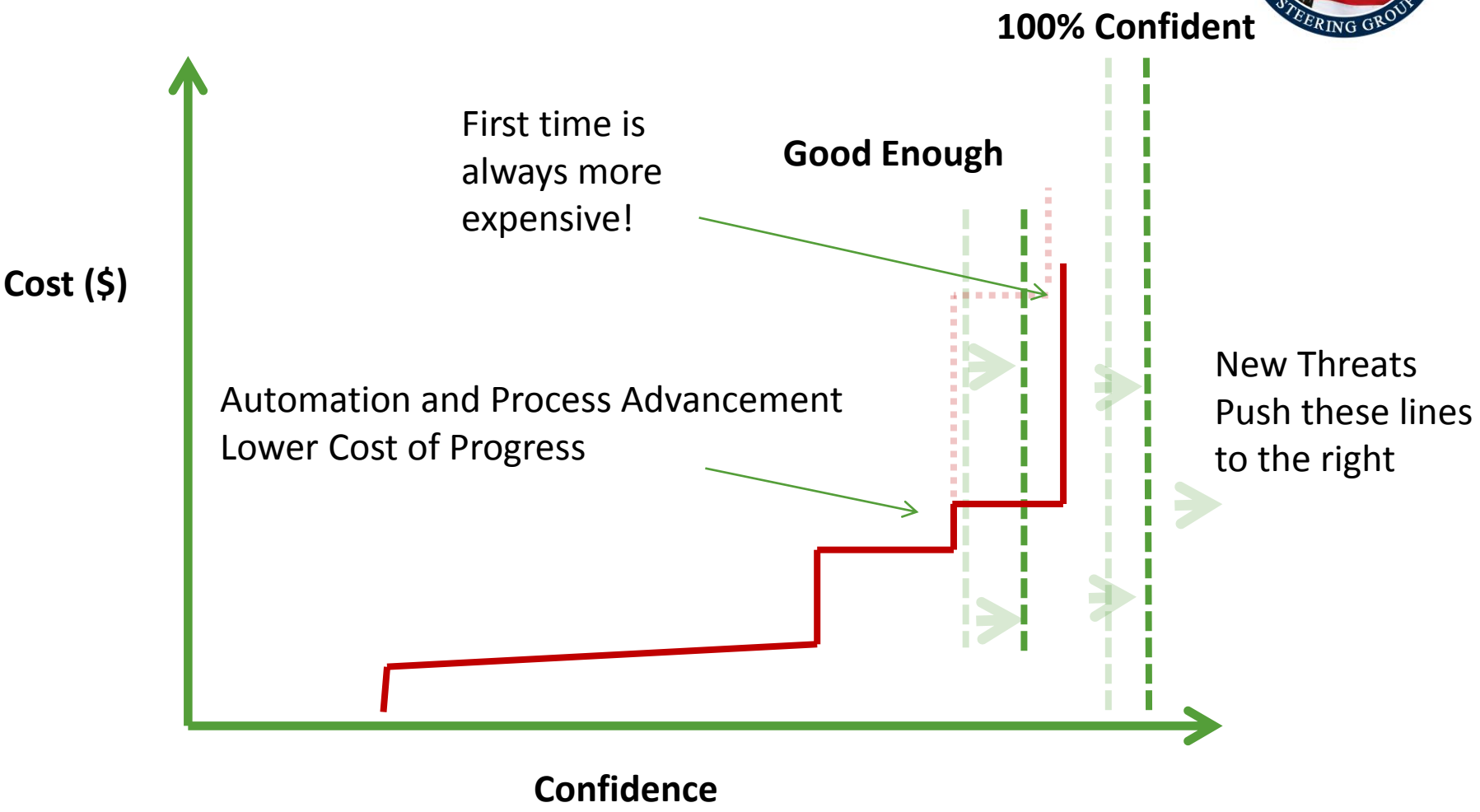
The Cost of Confidence:
An Abstract View



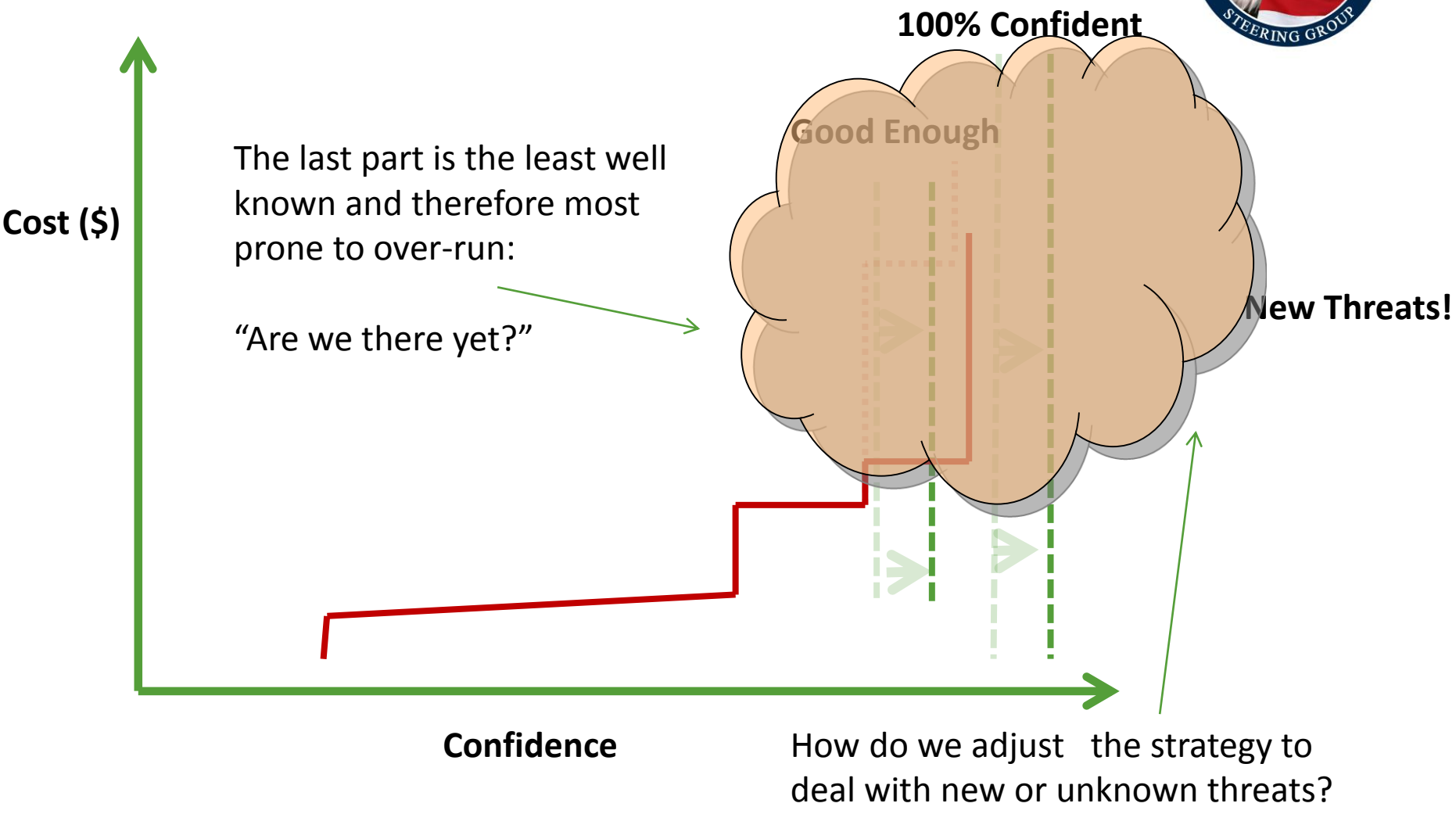
The Cost of Confidence:
Less Abstract View



The Cost of Confidence
Effects of Time

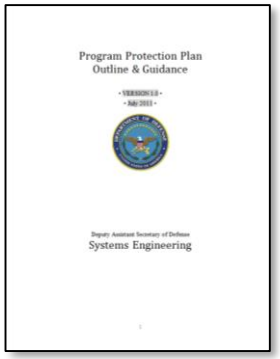


The Cost of Confidence
Clouds of Doubt



Rules and Regulations

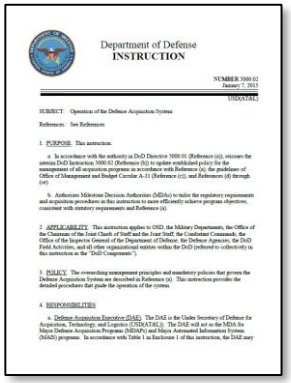
- DoDI 5000.02: **Create Program Protection Plan** (PPP)



- DoDI 5200.39: **Identify Critical Program Information**
  - CPI Includes mission critical functions, PPP covers information security threats and vulnerabilities, supply chain risk management, HW and SW Assurance, Cybersecurity, Anti-Tamper

- DoDI 5200.44: **Protection of Mission Critical Functions to Achieve Trusted Systems and Networks**

  "In applicable systems, integrated circuit-related products and services shall be procured from a trusted supplier accredited by the Defense Microelectronics Activity (DMEA) when they are custom-designed, custom-manufactured, or tailored for a specific DoD military end use (generally referred to as application-specific integrated circuits (ASICs))."

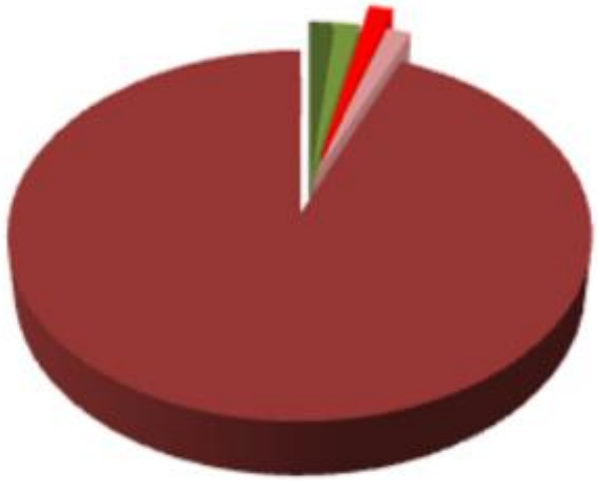


Realities of Using Trusted Flows

- Reality #1: Not All desirable ASICs are Available as Trusted
  - Developers must look closely at options
- Reality #2: Trusted is not always Classified but its often Close!
  - DSS insures ***capability*** of Secret, Developers/Suppliers choose specifics
  - Each Supplier has specific guidance and approach unique to their business
  - Classified Processing using all NISPOM standards is more expensive than commercial
- Reality #3: The MOST important thing is to lower RISK
  - Trusted Suppliers have security infrastructure, process, mindset
  - Developers should identify compliance with NIST 800-171
- Reality #4: SSE Knowledge of Risks outstrips Regulations
  - Technology and Risks change faster than any Government Process
  - Enforcement of Regulations? Systems that are Secure is the Goal!

Most Electronics: Unprotected by DMEA Trust

- Many ASICs and Most SOTA Processes
- FPGAs
- Standard Products
- Most Intellectual Property as ASIC Inputs
- PCBs and Interconnect Technology



Summary and Reasons for Guidebook

- Trusted Suppliers have distinct advantages but only for a subset of the solution space in a large dynamic risk space
- Regulation-based enforcement must trail common sense trade-offs of money vs. risk mitigation
- Standards and Rules are written by lawyers and enacted by lawmakers: **Plain language Advice and Guidance is Critical**
- DoD Stakeholders (Gov't offices, primes, subsystem manufacturers) have been looking for guidance in this form
- Guidebooks can be amended and updated at market speeds

Feedback from SSE Users will be the Lifeblood of This Effort

Trusted Supplier Steering Group

Speaker Contact Info:

Jim Gobes – CEO
Intrinsix Corp.
(508) 658-7658
jgobes@intrinsix.com

NDIA Systems Engineering Conference
Oct. 26, 2017