Understanding and Managing The Counterfeit Parts Problem

Yaw Obeng
NIST

This Presentation is Based in part on Information Shared at NIST PAIM Workshops and Other public Forums

What is a Counterfeit?

Many Definitions

The SAE (Society of Automotive Engineers) International Standard AS5553 Rev A (2013) defines a "Counterfeit Part" as:

"… part that has been confirmed to be a copy, imitation,

OR

substitute that has been represented, identified, or marked as genuine,

AND / OR

altered by a source <u>without legal right</u> with intent to mislead, deceive, or defraud."

Many Definitions

U.S. Department of Energy, Office of Environment, Safety and Health (Office of Corporate Performance Assessment) defines a "Counterfeit Item" as:

…. a suspect item that is a copy or substitute without legal right or authority to do so

OR

one whose material, performance, or characteristics are knowingly misrepresented by the vendor, supplier, distributor, or manufacturer.

Counterfeit or Piece of Art?

http://techcrunch.com/2011/08/30/stupid-people-are-gods-funny-little-angels/?icid=maing-grid7%7Cmain5%7Cdl17%7Csec1_lnk2%7C91628

"The Wooden iPad"

Counterfeit or Art?

Coca-Cola Bottle Casket

Counterfeit or Art?

Bottega Veneta Shoulder Bag Cake

What Brand?

The Official Egyptian Team Wear

ww.bbc.co.uk/news/world-middle-east-18995905

Free Hotmail | Windows Marketplace | Windows Media | Windows | Imported From IE | NIST Inside NIST Homepage

Home | US & Canada | Latin America | UK | Africa | Asia | Europe | Mid-East | Business | Health | Sci/Environ

26 July 2012 Last updated at 06:33 ET

428 Share

London 2012: Egypt Olympic team get 'fake' Nike kit

Members of Egypt's Olympic team have been given fake Nike gear, a synchronised swimmer has alleged.

Tomna Khallaf said her workout bags had a big Nike logo in the front but the zippers had an Adidas branding on them.

Nike said it was concerned about the allegations

The Egyptian Olympic Committee (EOC) secretary general, Motaz Sonbol, said they were shocked to find that the gear was not "directly from Nike".

Nike said it was "concerned" athletes may have received products that do not meet the company's quality standards.

A Nike spokesman said the company was recently made aware that the EOC chose a sports gear vendor who allegedly supplied counterfeit footwear and apparel bearing the Nike trademarks.

The company said it was now in discussions with the EOC to see if a solution could be reached.

But the committee's chairman, Gen Mahmoud Ahmed Ali, defended the decision to go for the "counterfeit" gear because of his country's tight finances, AP reports.

"We signed with a Chinese distributor in light of Egypt's economic situation," he said.

Ms Khallaf tweeted that she had to spend more than $300 (£195) of her own money to buy satisfactory gear.

BBC Arab Affairs Editor Shaimaa Khalil says the incident has caused a major controversy on social media, with some users describing it as a disgrace.

Egypt is being represented by 112 Olympians at London 2012.

Related Stories

- Olympics soccer fiesta continues
- Aboutrika in Egypt Olympics squad
- Medany struggles with sport & religion

Olympics coverage online

- From the BBC:
- London 2012: All Olympics news
- Sport: Reports, reaction, news
- Weather: UK five-day forecast
- Official Olympic travel links:
- Traffic and travel in London
- Travel info for other Games locations
- Traffic updates via Twitter @GAOTG

NIST Product Authen
Information Manage

“Copy Merchandize” Malls In China

Copy or Counterfeit?

Actors: Apple vs. Goophone

GizChina is reporting that GooPhone claims to have a patent on the iPhone 5's design in China.

Well, they have a patent on their design, but it's remarkably similar to the design of the iPhone 5.

	iPhone 5	Goophone i5
Screen Size	4-inch	4-inch
Resolution	1,136 x 640	1,280 x 720
Storage	16GB/32GB/64GB	16GB/32GB + Memory card slot
CPU	Dual-Core Apple A6	Quad-Core Nvidia Tegra 3 1.4Ghz
RAM	1 GB	1 GB
Operating System	iOS 6	Android 4.0 (ICS) iOS Theme
Camera	8 MP (3264 x 2448)	8 MP (3264 x 2448)
Networking	Wi-Fi, 2G, 3G, 4G LTE	Wi-Fi, 2G, 3G
Price	$649/$749/$849	$299

KUWAITIFUL.COM

Conformance vs. Counterfeits

Conformance vs. Counterfeits

Conformance testing or **type testing** is testing to determine whether a product or system conforms with the requirements of a specification, contract or regulation.

SEMKO | CE mark | British Standards | Japanese Industrial Standards | Norma Oficial Mexicana | ISI mark | Energy Star | NTA Inc

Conformance vs. Counterfeits

IAEA-TECDOC-1169

Managing sus
counterfeit ite
nuclear

INTERNATIONAL ATOMIC ENERGY AGEN

FOREWORD

Some manufacturers and suppliers use inferior materials and processes to make substandard supplies whose properties can vary significantly from established standards and specifications. Other suppliers distribute items that they know do not meet the purchase requirements or provide documentation that misrepresent actual conformance to established specifications and standards. These substandard supplies, or *s*uspect/*c*ounterfeit *i*tems (S/CIs), pose potential threats to the safety of workers, the public and the environment and may also have a detrimental effect on security and operations at nuclear facilities.

Nuclear facilities often procure and use commercial-grade items and the quality assurance policies/procedures and procurement methods are not always properly applied to avoid the entry of S/CIs into those facilities. This publication offers practical guidance on how to apply existing quality assurance programmes to effectively prevent the procurement and use of S/CIs. In particular, it provides a practical method of applying the requirements and guidance contained in the IAEA Safety Series 50-C/SG-Q: Code and Safety Guides on Quality Assurance for Safety in Nuclear Power Plants and other Nuclear Installations (1996), to the S/CIs issue.

The preparation of this publication took place between October 1999 and May 2000. Two meetings were held with experts of various Member States who contributed with their experience in nuclear facility quality policy and regulation development, quality assurance programme implementation, design, procurement and enforcement. The preliminary draft was distributed to interested organizations in several Member States, including manufacturers, suppliers, regulators and certification/accreditation bodies, for comments and inputs that were considered and included where appropriate in the final version.

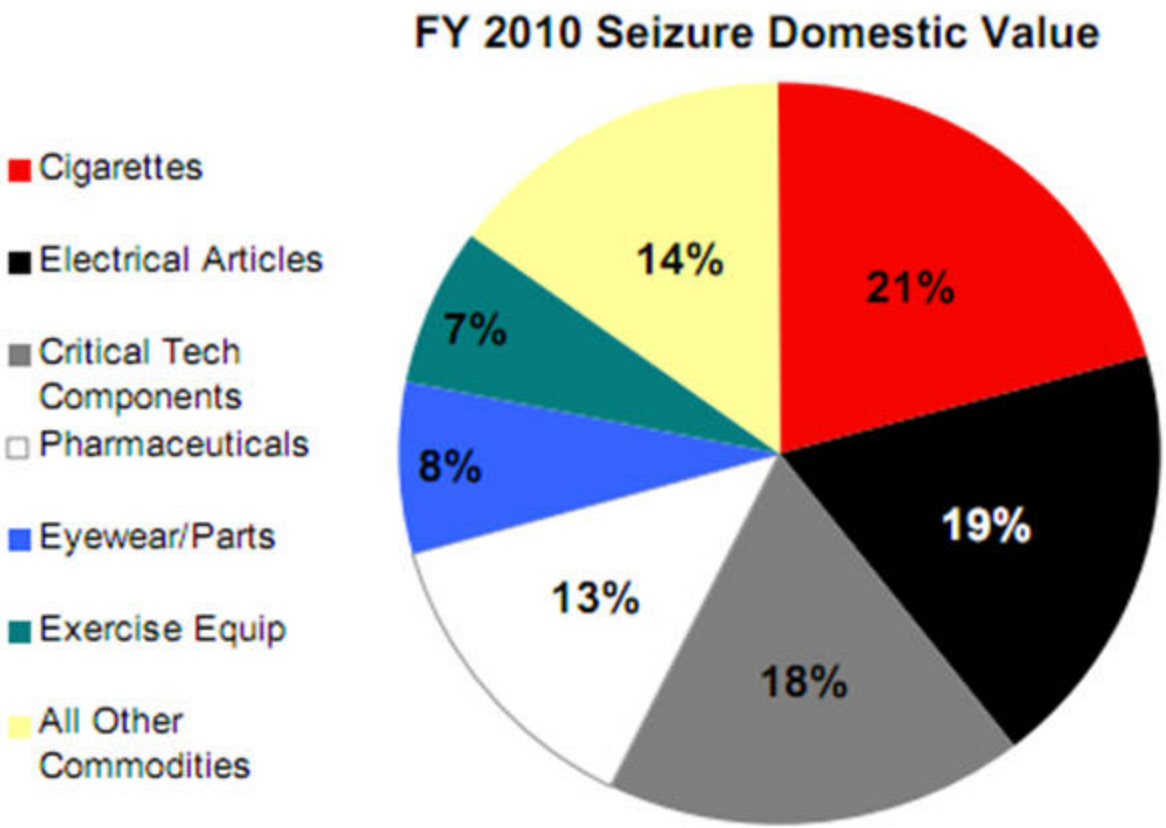
The IAEA received valuable financial support from the Department of Energy (DOE), United States of America, for the development of this publication.

The Secretariat wishes to acknowledge the efforts and assistance provided by the contributors and participants at the preparatory and review meetings, listed at the end of this publication. The IAEA is especially grateful to G. Danielson, USA, the main writer of the original manuscript, and to N. Redman, United Kingdom, who reviewed the final manuscript. The IAEA staff member responsible for this work was N. Pieroni of the Division of Nuclear Power.

Understanding the Scope of the Problem

The Economics of Counterfeits

Consumer Counterfeits in the USA



Sign In Register Print Subscription Conversations Today's Paper Going Out Guide Jobs Cars Real Estate Rentals Classifieds

POLITICS OPINIONS LOCAL SPORTS National World Business Investigations Lifestyle Entertainment Multimedia

The Washington Post with Bloomberg

BUSINESS *Where Washington and Business Intersect*

Economy Industries Local Business Markets Policy & Regulation Technology World Business Blogs & Columns Innovations On Small Business

In the News Apple wireless carrier?

Advertisement

Hazing in D.C. area schools continues

U.S. defense equipme counterfeit parts from

Text Size Print E-mail Reprints

By Tony Capaccio, Published: November 8

Nov. 8 (Bloomberg) -- Dozens of suspecte defense equipment from Raytheon Co., L- including aircraft deployed to Afghanistan

The Senate Armed Services Committee fo at least seven aircraft, including the Lockh P-8A Poseidon maritime patrol and L-3 2

4 Comments

Weigh In Corrections?

United States Government Accountability Office

GAO

Testimony

Before the Committee on Armed Services, U.S. Senate

For Release on Delivery
Expected at 9:30 a.m. EST
Tuesday, November 8, 2011

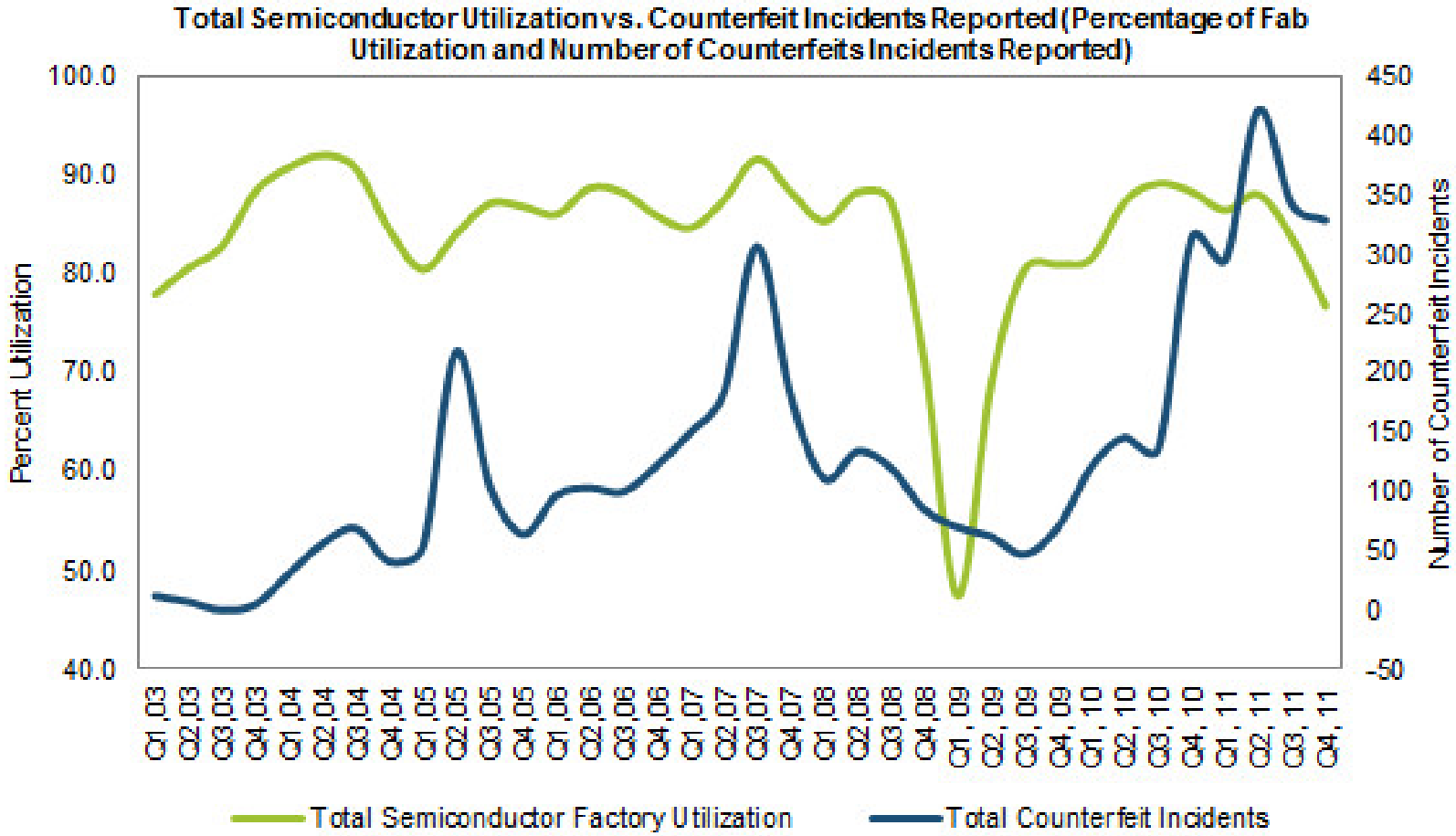
DOD SUPPLY CHAIN

Preliminary Observations Indicate That Counterfeit Electronic Parts Can Be Found on Internet Purchasing Platforms

Statement of Richard J. Hillman, Managing Director
Forensic Audits and Investigative Service

NIST Product Authentication Information Management Pro

"Counterfeiters track market conditions much in same way that legitimate producers of original parts do!"



Source: IHS iSuppli Research, November 2012, IHS Parts Management, CAPS Universe, Q3 2012

The Economics of Counterfeiting: The Case of Galaxy Gear

www.businessinsider.com/chinese-counterfeiters-samsung-galaxy-gear-2014-1

Free Hotmail | Windows Marketplace | Windows Media | Windows | Imported From IE | Inside NIST Homepa... | BBC News - Africa | Google

BUSINESS INSIDER

Tech | Finance | Politics | Strategy | Life | Entertainm

Starting at $29,900*
The all-new 2014 Mercedes-Benz CLA
Expand to E

TECH

More: Samsung Galaxy Gear Smar

Even Chinese Counterfeiters Aren't Interested In Samsung's Galaxy Gear Smart Watch

STEVE KOVACH
JAN. 16, 2014, 10:30 AM 2,040 1

Recommend 38 | Share 6 | Tweet 139 | +1 9 | EMAIL | MORE

Even Chinese counterfeiters who make a living from selling knockoff iPhones and Samsung Galaxy phones aren't too hot on Samsung's smart watch, the Galaxy Gear, according to a report from CNN.

Samsung's smart watch, the Galaxy Gear, launched last fall to so-so reviews. Critics panned the device for its limited functionality, poor battery life, and bulky body.

It seems those negative reviews have trickled down to counterfeiters in China. CNN talked to several and none of them

The Samsung Galaxy Gear.

See Also

REPORT: Samsung's New Ga

NIST Product Authentication Information Management Project

Counterfeit Backdrop

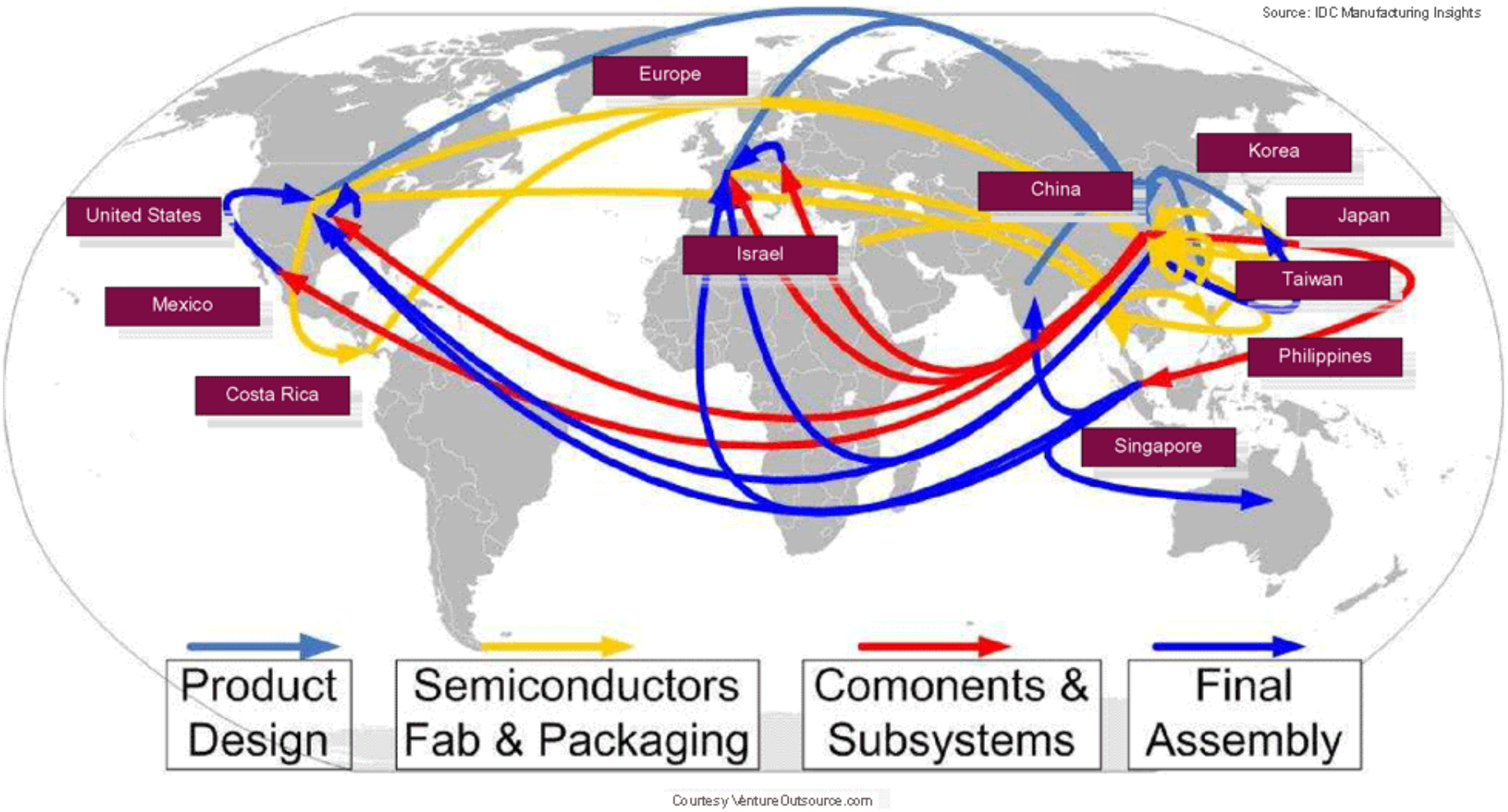
Drivers of Supply & Demand of Counterfeit Products

Macro-level drivers of supply	Macro-level drivers of demand
• The growing prevalence of digital and networked technologies • The globalization of trade, the growing importance of international brands • The presence of large integrated markets supporting free trade • Low or weak enforcement of penalties targeting violators of IPR infringements • The growing presence and involvement of organized crime in the production and distribution of counterfeited and pirated goods • Industry-specific factors.	• Social acceptance to buy products that violate intellectual property rights • Limited availability of authentic goods • The high price of authentic goods • The rising quality of counterfeit goods.

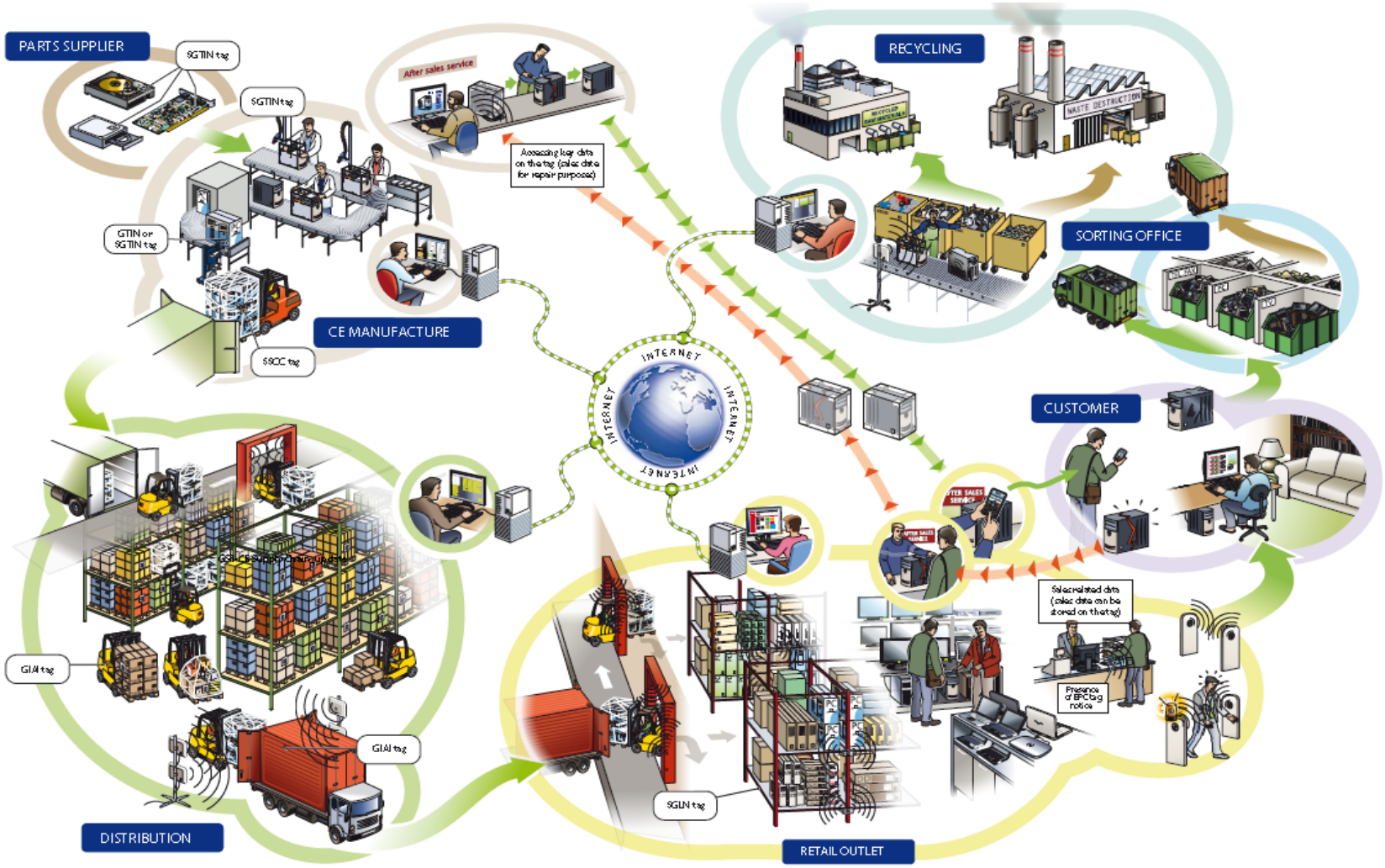
Source – Rand Corporation, 2012

Counterfeits Electronics

Semiconductor industry characterized by global transfer of goods and services:

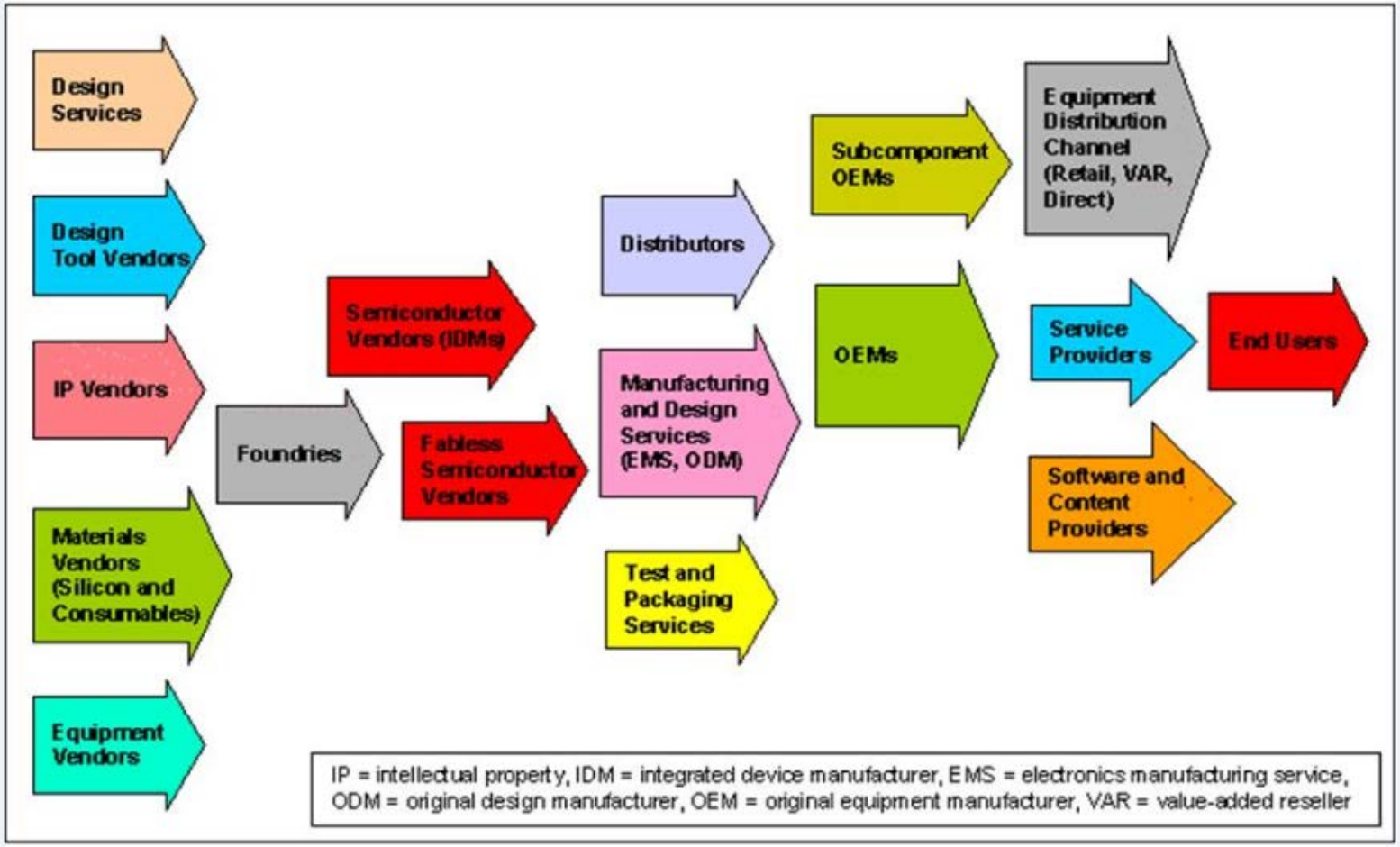


The Global Consumer Electronic Supply / Distributor Chain



Source: Global Business of Language, 2012

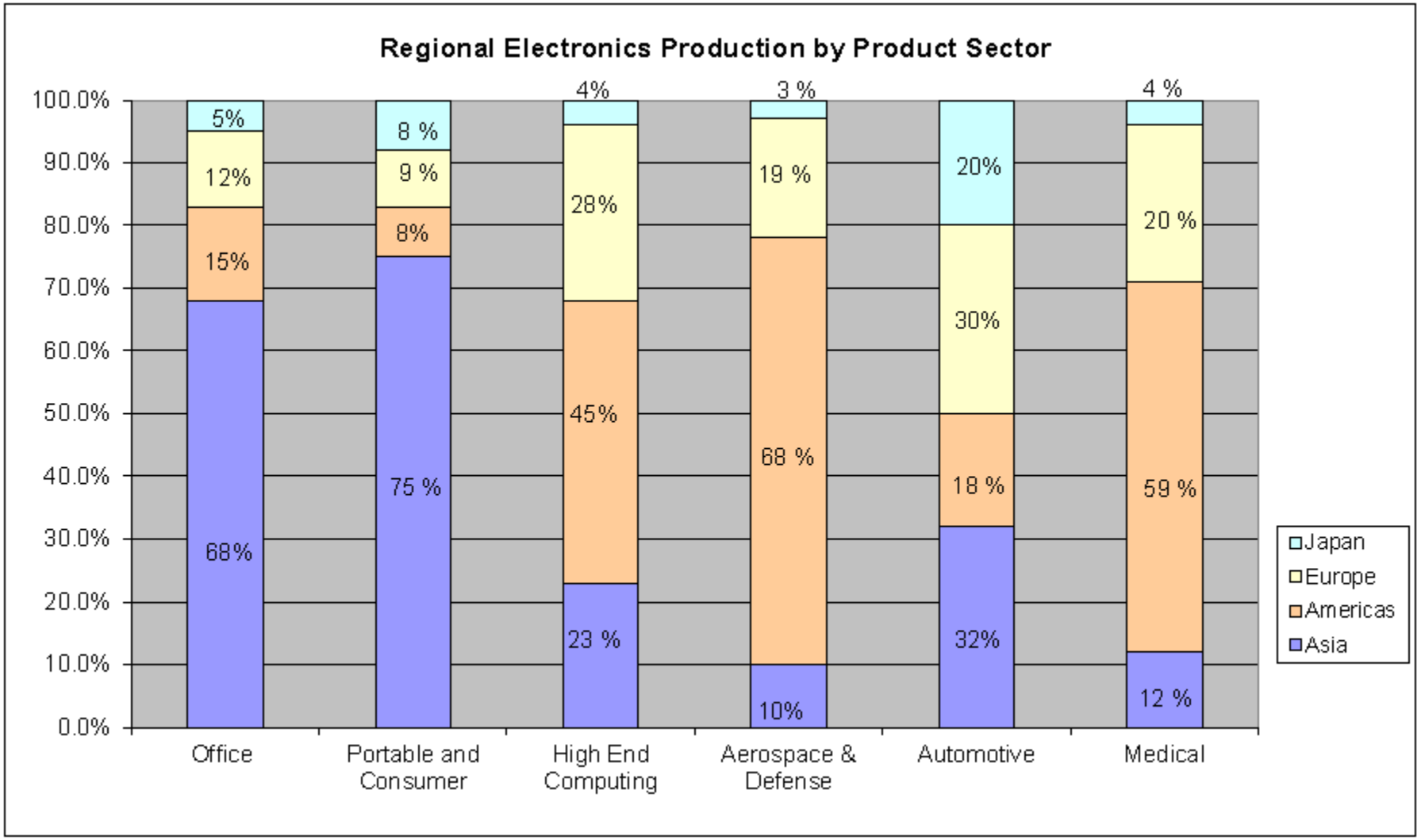
Semiconductor Industry *Value Chain*



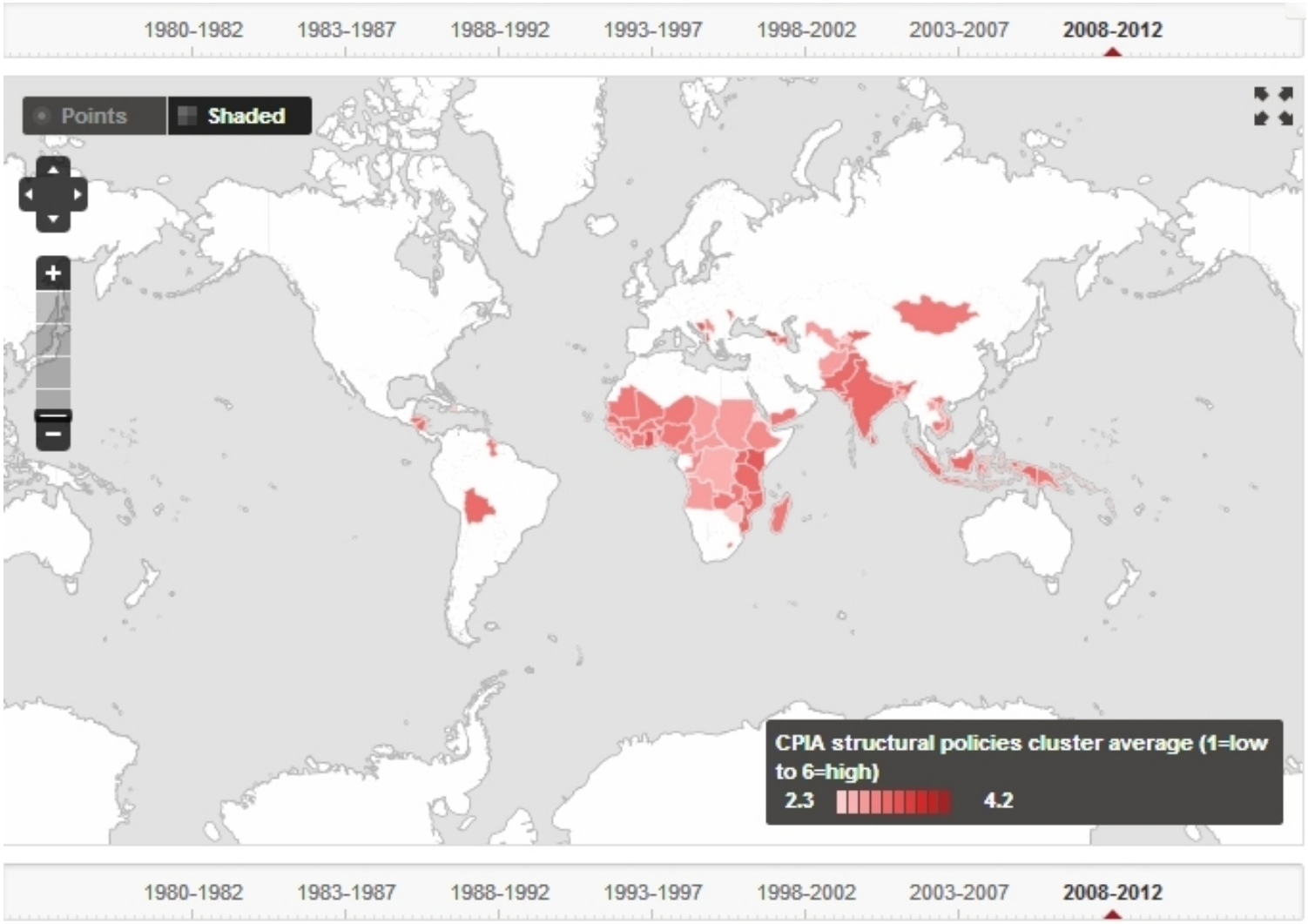
Source: Gartner (March 2005)

Where are the Electronics Being Made?

Regional Electronic Production in 2012



World Bank Corruption & Transparency Index



Culled from http://data.worldbank.org/indicator/IQ.CPA.STRC.XQ/countries/1W?display=map

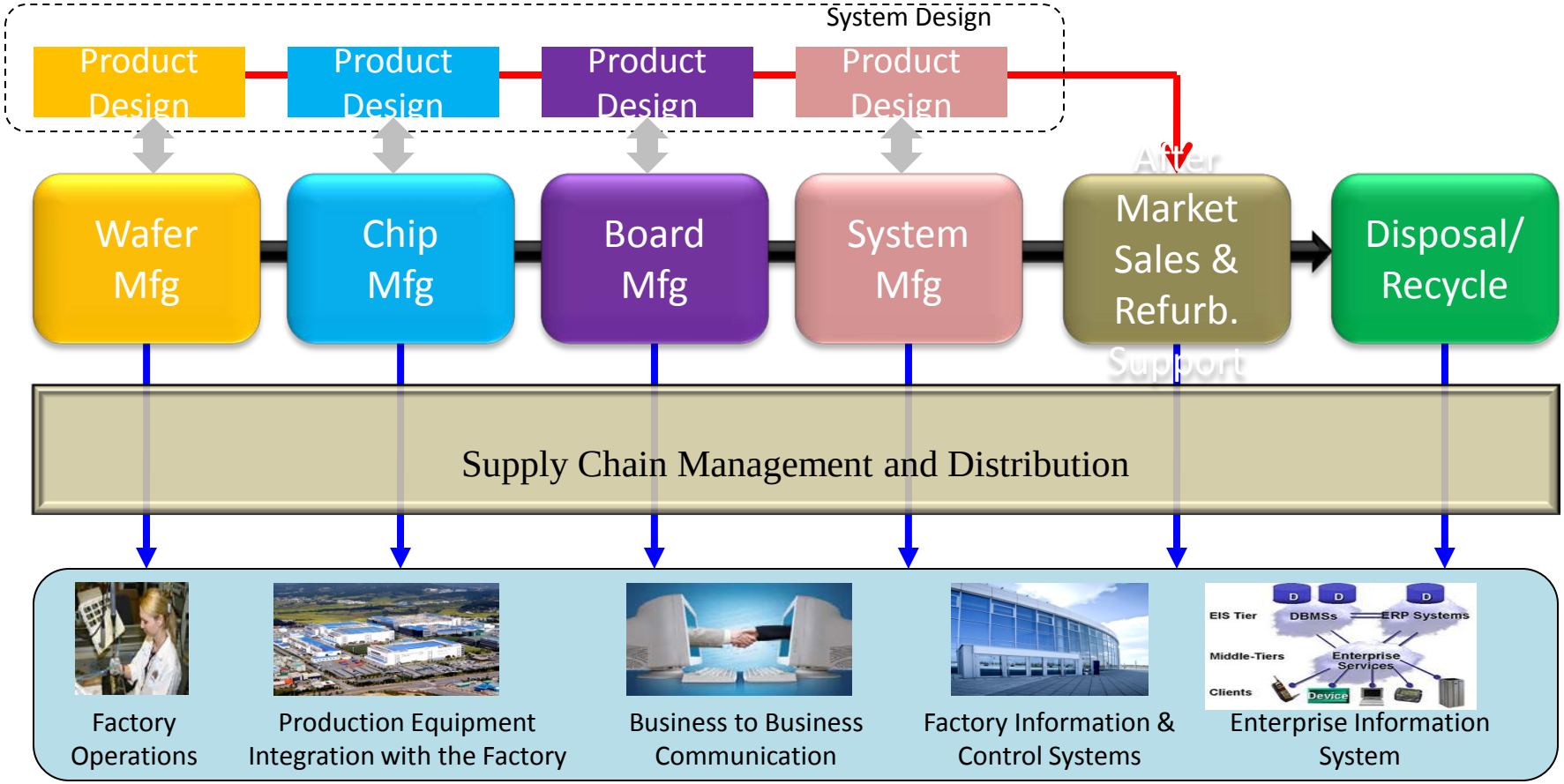
Counterfeit Attack Vectors

- Recycled or Refurbished ICs
- Substandard Parts (Defective)
- Missing Process Flow (i.e. testing, upscreening …)
- Remarked Parts
- Forged Documentation
- Cloned ICs
- Overproduction
- Tainting

Tehranipoor, M., 'Utilizing IC Parameters for Security and Trust', Univ. Connecticut March 2012
Adapted by IGG, Counterfeit Components Symposium and Workshop, November 2006
http://counterfeitparts.files.wordpress.com/2012/03/types_of_counterfeit_parts.pdf from SAE AS5553

Why is it Such a Tough Problem?

Electronic Manufacturing Workflow Diagram



Source: iNEMI, 2010 Roadmap

Solutions - Technologies

Mechanisms and partial solutions to address the counterfeiting problem within manufacturing industries

- Product and component tracking/tracing
- Sequential marking
- Embedded RFID chips
- Cryptographic tags
- Bar codes
- Holograms
- Covert product features
- Tamper resistant/evident security packaging
- Color shifting inks
- Incorporation of uniquely identifiable nano-particles in manufacturing goods
- Product history data
- Scanning systems
- Audits
- Authentication services
- Increased supply chain security

Case Study #1: Suspect Counterfeit, Microcircuit, Digital, Microprocessor

GIDEP ALERT # C5-A-13-01

Narrative:

- During a failure investigation it was noted that the processor marking on parts supplied by **XYZ, Inc.** were inconsistent.
- As part of investigation the pedigree for parts was investigated by contacting Intel to confirm part lot date code.

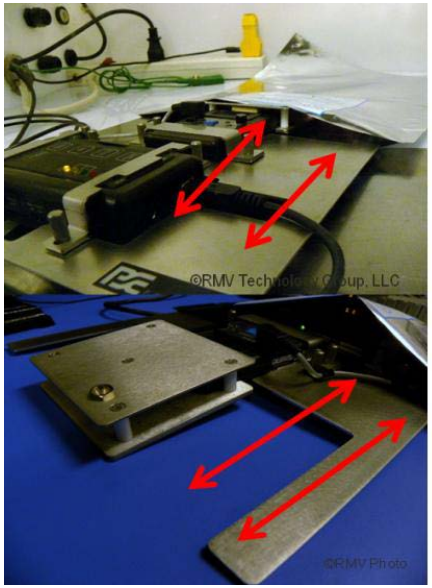
- IDM never made any MG80C186 with a batch number "M832100B" or batch ID "464724338P with a date code "832".

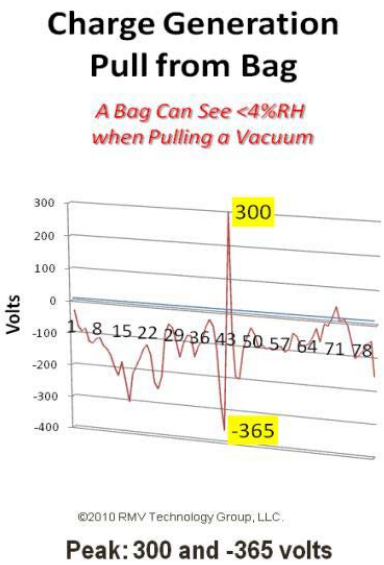
Conclusion: The part is a counterfeit 5962-8850102ZA (MG80C186-12/B).

Footnote: Batch had previously passed 5 third party validations!

Case Study #2: Is ESD Really a First Line of Defense For Suspect Component Detection ?

The Electronics component bagging required by the DOD is to provide a charge free shielding environment for ESD sensitive components





In March 2012, RMV demonstrated that despite accurate initial qualification efforts for ESD materials utilized in the DOD supply chain, <u>four of the five packaging products (pulled from new inventory</u>) yielded failing results:

1. Fast Packs (Failed)
2. Antistatic Bubble wrapping (Passed)
3. Antistatic Pink Poly Film (Failed)
4. Type 1 Aluminum ESD Moisture Barrier Film and Bags (Failed)
5. Type 3 Metalized ESD Shielding Film and Bags (Failed)

Authentication Technology Evaluation

Type	Technology	Description	What it does	What it doesn't do	System Requirements	Limitations / Killers	Examples / Commentary
Materials / Chemical	**DNA Tagging**	Adding a consigned materal to the product provided by a trusted source			Perfect Control of taggant, Detectors	Readers, Detection not real time	DLA Mandate !!
	Phosphor Tagging	Adding a consigned materal to the product provided by a trusted source					
	Micro-ceramic Particles	Adding a consigned materal to the product provided by a trusted source					
	Carbon-dating-like ingredient	Chemical decay (a designed and measurable shift in performance)					
Visual	**Proof Tag**	Serialized label affixed with a small drop of a clear polymer that has bubbles randomly dispersed within it. Entropy comes from bubble formation	Unique identification. Impossible to counterfeit	Fast visual validation	Extensive DB requirements, Access to Proof Tag DB	Pre built Custom tags, Proof Tag and Supplier DB synch	Wine
	Color Shift Ink	Unique type of pigmentation that changes color depending on the angle of the light reflecting off the ink	Visual identifier of brand	Guarantee it's genuine	Control of bulk labels	None	Common technology
	Holographic Image	Three-dimensional images change as the position and orientation of the viewing system changes	Image can be complex. Visual identifier of brand	Guarantee it's genuine	Control of bulk labels	None	Common technology
	Authenti Guard	AuthentiGuard is a security printing and document security technology.	Unique prism mark on label validated by an APP	Easy validation	DB requirements, Access to smart phone app	Expensive, Label info may deteriorate over time	Common technology
	Nano Pattern	Deliberate paterning that counterfeiters cannot afford to do					
	Un-clonable High Resolution Mark	Large two-dimentional barcodes containing 5 to 20% random errors. Entropy comes from equipment jitter	Detects clones. ID impossible to counterfeit	Prevent tampering. Cannot store custody info	High res camera. Public key access	Adds time to marking process if mark is variable	Uses existing commonly deployed equipment. Automotive, wine
	Extreme magnification	Any surface mag'd enough becomes unique.Digitizing and signing this view becomes an authentication signiture	Unique identification	Easy validation	High mag equipment	expensive, requires expertise, slow	
	Bar Code	Form of mass serialisation	Enables Track and Trace	Guarantee it's genuine. Prevent tampering	Remote transactional DB, data access policy & line of sight	Mutual Trust	Multiple ...commonplace
Electronic	**RFID**	Active and passive and can be embedded in chip	Captures & stores shipment info - non line of sight tracking, provides non volatile storage	Guarantee it's genuine. Prevent tampering	RFID Gateways, antennas on products	Close proximity, cost/piece + equipment. Error rates. Limited non volatile storage	Walmart
	PUF	There are half a dozen implementations of this. Random secret unknown to everyone incl manufacturer. Extracting the secret should destroy the part	Unique ID, impossible to counterfeit, can be hidden from everyone	No info captured, stored, inactive during shipment	Built into IC architecture - must be designed in	New Concept … not well understood by practitioners	Being evaluated by many IC mfgs.
	Thermal Profiling	University research at Howard U. (by Dr. Preston D.Frazier). Creates fuzzy thermal fingerprint - catches radical shifts in thermal profiles	Creates thermal fingerprint ref of known authentic high level assy	Manage legitimate changes to the ref assy	Thermal 2D imaging high res	Change management, accuracy limitations	Academic concept / proposal ..POC
	Prorgramable cells	fuses, Eprom, Flash, etc. - used to store private keys or other secrets	Mfg can embed unique ID & performance info into part	Inactive during shipment	Built into IC architecture - must be designed in	Trust the manufacturer	CPU ID instructions. Over 20 years experience
	Odometer circuits	U. of Conn. Research on circuits that change with time	Detects if a part is used	Guarantee it's genuine. Prevent tampering	Built into IC architecture - must be designed in	New Concept … not well understood by practitioners. Sensitive to process variations	Academic concept / proposal .
	Random Number Gen.	Used to protect programmed secrets … protecting data ,,. Not the part	Source of entropy to protect data	Guarantee it's genuine. Prevent tampering	Built into IC architecture - must be designed in	Not designed to protect parts	Feature of 4th gen core architecture
Other	**Mass Serialisation**	Remote and secure database storing attribute data	Enables Track and Trace	Guarantee it's genuine. Prevent tampering	Remote transactional DB, data access policy	Mutual Trust	Multiple …parts ~ space shuttle tiles
	As-built data records	Materials used in most BOM's change over time.	Creates data fingerprint of each high level assy	Guarantee it's genuine. May not prevent tampering	Fingerprint data storage & protection	Data Volume, Storage & Protection	Historic records by all mfgs

NIST Product Authentication Information Management Project

Who is In Charge?

Standards are a common language used to communicate expected levels of performance for products and services

Standards are Essential to Global Economy

- Ensuring interoperability among trade partners
- Facilitating increased efficiencies in the global economy
- Making the development, manufacturing, and supply of products and services more efficient, safer and cleaner
- Providing governments with a technical base for health, safety and environmental legislation
- Safeguarding consumers, and users in general, of products and services - as well as to make their lives simpler

Governments Care

- **US National Technology Transfer and Advancement Act of 1995 (NTTAA)** (Public Law [P.L] 104-113, Sec 12-d-1)

  "Federal agencies and departments shall use such technical standards as a means to carry out policy objectives... ."

- **World Trade Organization Agreement on Technical Barriers to Trade** encourages the use of international standards and conformity assessment systems because of their potential for improving the efficiency of production and facilitating international trade.

Businesses adopt standards when it is clear that they can gain competitive advantage

Countries use international standards compliance as a trade barrier and differentiator for their companies

SUMMARY STATUS OF STANDARDS EFFORT

- Anti-counterfeiting solutions must be implemented and supported throughout entire manufacturing supply chains that include:
  - Raw material providers
  - Parts suppliers
  - OEM
  - System integrators
  - Shippers
  - Border crossings
  - Seaports
  - Truck inspection & weigh stations
  - Distributors
  - Maintenance service providers
  - Retailers
  - Consumers
- Solutions must be based upon standards that can be implemented across the supply chain
  - **Some standards do exist today: SEMI-T20 Series**.

Pitfalls and Lessons Learned

Too many standards!

- Supply chain integration issues
- Interoperability
- Lack of Harmony between Science and Standards
- Awareness and understanding

Slow to evolve

- Cumbersome standardization process
- Room for growth and flexibility

Security

- Security in obscurity
- Security in diversity
- Open prototyping and testing

Opportunities

Understand Market Needs

- Develop a vision for electronic product identity management
- Develop use cases for product authentication

Develop Specifications

- Develop unique IDs
- Incorporate unique IDs into current BoMs
- Leverage user authentication schemes for product authentication
- Leverage security assessment criteria for product authentication solutions

Drive Convergence

- Manage product life cycle identity information
- Standards interoperability (*we must avoid the spaghetti effect!!)*

Innovate!

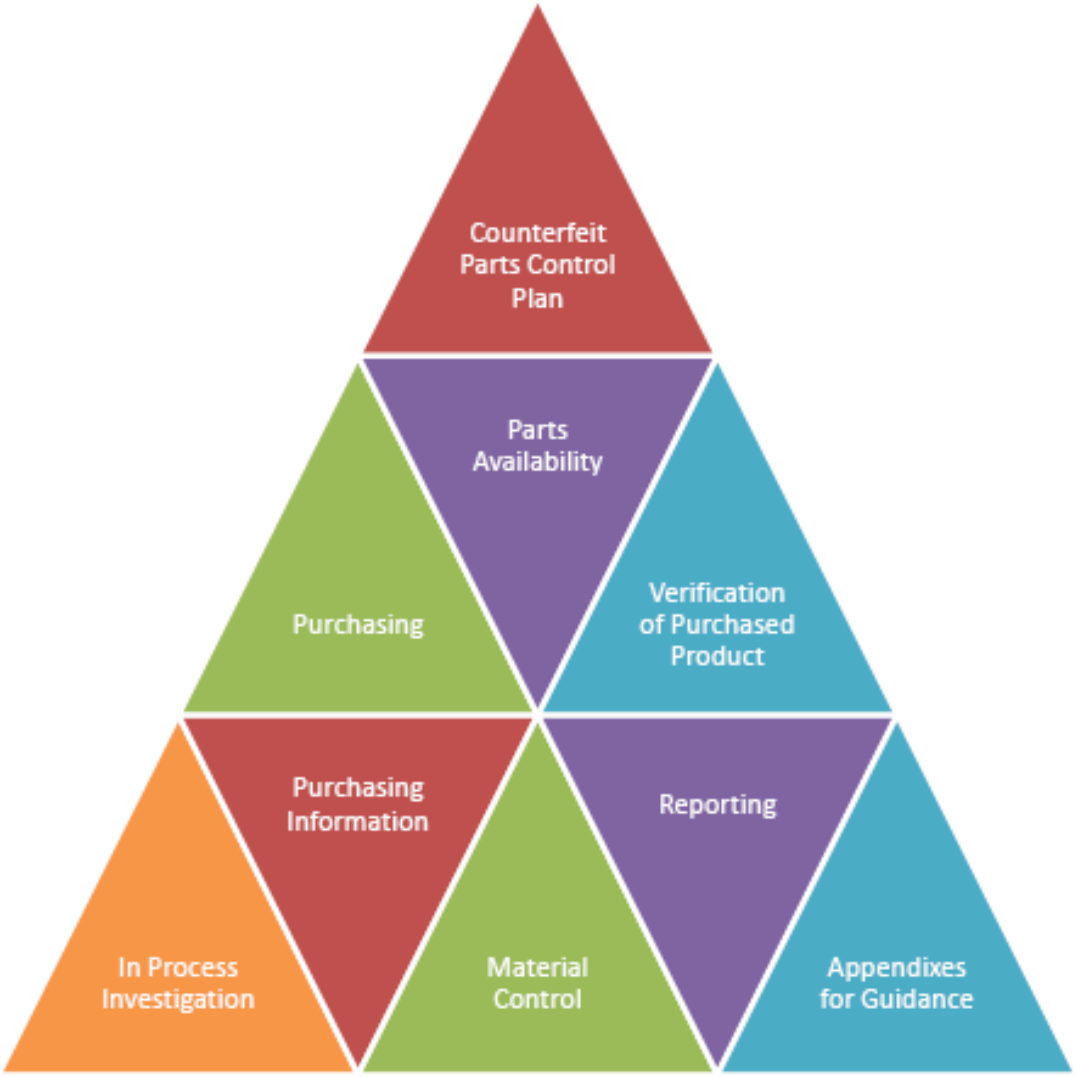
Official contribution of the National Institute of Standards and Technology; not subject to copyright in the United States.

Certain trademarks are identified in this paper to foster understanding. Such identification does not imply recommendation or endorsement by the National Institute of Standards and Technology.

Backup Slides

Current Response Profile

SAE AS5553 Requirements



Solutions - Technologies

Mechanisms and partial solutions to address the counterfeiting problem within manufacturing industries

- Product and component tracking/tracing
- Sequential marking
- Embedded RFID chips
- Cryptographic tags
- Bar codes
- Holograms
- Covert product features
- Tamper resistant/evident security packaging
- Color shifting inks
- Incorporation of uniquely identifiable nano-particles in manufacturing goods
- Product history data
- Scanning systems
- Audits
- Authentication services
- Increased supply chain security

Technical Issues - Standard Solutions

- Stopping counterfeiting is difficult because solutions must be appropriate to the product being protected, reliable, technically feasible, affordable, and scalable for widespread use.

- Mechanisms must be able to rapidly distinguish between legitimate and counterfeit products at every stage of the supply chain - only a small portion of imported goods are inspected. → **Metrology Needed!!**

- Individualized solutions for each manufacturer are not practical, especially considering that critical security checkpoints are ports of entry where government customs inspectors are responsible for checking an extremely large number of types of products from many different manufacturers.

The Current Industry View is Reactionary:

Parts may Authentic perhaps, but where have they been? …

- Many parts acquired from Independent Distributors may be authentic, but show evidence of …
  - Poor storage and handling conditions
  - Termination refurbishing or reclamation

- To ensure confidence that parts are of the same quality and reliability as when first shipped by the original component manufacturer, users should apply a suite of **test and inspection protocols** to …
  - Detect counterfeits
  - Eliminate defects associated with handling and storage → **Test**
  - Identify refurbished or reclaimed parts → **Inspection**.

- The current scope of industry activities are guided by the industry view

→ Need to Be Proactive

Proactive Response Profile

Metrology, Best Practices and Standards to Mitigate Counterfeits Electronics

- Documentary Standards :
  - Industry-led trade groups
    - SIA, iNEMI, HDPUG, JIPDEC
  - SDO's
    - ISO TC 247 WG-3, SEMI
  - Develop documentary standards for device traceability and authentication information management protocols
- Metrology
  - Enable non-destructive discrimination between authentic and bogus electronic components in real time
- Functional and Reliability Tests
  - Massively parallel testing platform to improve failure statistics

HDP Info Exchange

Supply Chain Requirements

Final

HDP USER GROUP INTERNATIONAL, INC.®

SC Step	Supply Chain Stage	Data Required at this Step	Controls that can be applied	Trust Assurances
1	**Raw Materials Supplier** (Chemicals, Metals, Pastes..)	Material Supplier ID and COC by Unique Batch ID No for all materials supplied	Unique composition	Ethical Source
2	**Wafer Manufacturer**	Materials Supplier ID and COC for all materials received by Unique Batch ID No	Unique composition	Limited Source
3	**Component Manufacturer** (IC, Caps, Resistors, Cables …)	For all materials used - Wafer Supplier ID, Unique Material Batch ID No with COC,	Laser Marking. Taggants, Doc Retention to support Product Lifecycle	Approved Mfg
4	**Board Manufacturer** (PCBs, Modules, Drives, PSUs…)	For all components & materials used - Component Supplier ID, Unique Component ID for high value / high risk items, unique Batch ID for low value / low risk items	MAC, VPD, S/N, Auth System, Taggants, GIDEP Alert	Approved Mfg
5	**System Manufacturer** (Complete System)	For all components - Board Mfg ID, Unique Component ID for high value / high risk items, unique Batch ID for low value / low risk items	Content by S/N, GIDEP Alert	Approved Mfg
6	**System Integrator** (H/W & S/W Integration)	For all components (H/W & S/W) - System Mfg ID, Unique Component ID for high value / high risk items, unique Batch ID for low value / low risk items	GIDEP Alert	??
7	**Distribution** (Authorised Channel)	For all products - System Integrator ID and Unqiue Product ID	Physical Access, Invoice S/Ns, Doc Retention, GIDEP Alert	Authorised Distributor
8	**Retail / Broker**	For all products - Dist ID and Unqiue Product ID. Procurement & Sales record for all products	Invoice S/Ns, Doc Retention, Lab Insp records for IDEA brokers, GIDEP Alert	IDEA Certified
9	**Service / Repair**	For all products used - Distributor / Broker ID and proof of autenticity.		Certified
10	**Customer**	Proof of Purchase with Supplier ID and unique Product ID listed	Archive spare parts, GIDEP Alert	

SC Optimum Protocol

SC Step	Supply Chain Stage
1	**Raw Materials Supplier** (Chemicals, Metals, Pastes..)
2	**Wafer Manufacturer**
3	**Component Manufacturer** (IC, Caps, Resistors, Cables …)
4	**Board Manufacturer** (PCBs, Modules, Drives, PSUs…)
5	**System Manufacturer** (Complete System)
6	**System Integrator** (H/W & S/W Integration)
7	**Distribution** (Authorised Channel)
8	**Retail / Broker**
9	**Service / Repair**
10	**Customer**

Optimum Data Protocol

1. Material ID (PN, SN)
2. Supplier ID
3. Date Procured
4. Customer ID
5. Date Sold

iNEMI Calculators

Risk of Counterfeit Use – Calculator #1

- This calculator quantitatively asses the relative risk of a product being counterfeit
- Can be used by
  - Component Manufacturers – identify risk for their product
  - Product Designers – identify risk of products to be used or of end product
  - Distributors – identify products at risk and those requiring extra controls
  - End Users – identify risks of selected products and provide product ranking
- It is based on 4 key attributes – product profile, supplier and supply line characteristics, counterfeit deterrents used on the product and channel characteristics
- The user selects the appropriate rating for each of the elements from the rating table and the calculator provides an overall risk assessment for that product.
- The higher the rating, the higher the risk of counterfeit for that product
- The relative ratings for a product portfolio enables the company to focus their efforts on the high risk products.

Risk of Counterfeit Use - Calculator #1

Risk of Counterfeit Use v3.0

iNEMI

Methodology to Evaluate or Assess the Risk of Counterfeit Use

CF = Counterfeit

Profile		Input					Process				Output							
Select or Enter Product Type	Demand / EOL	Supplier	Supply Line	Mitigation & Controls	Supplier History	Input Score	Ease of Counterfeit	Ease of Detection	Counterfeit Controls	Process Score	Sales Channel	Excess Inventory & Prototype	Customer	Rework	Ease of Fraudulent Reuse	Disposal	Output Score	Total Rating
Hard Drive	3	1	1	1	1	1	5	3	2	30	4	4	5	3	1	1	240	524
	0	0	0	0	0		0	0	0		0	0	0	0	1	0		

Please select the rating from the table below that best corresponds to the description for that rating.

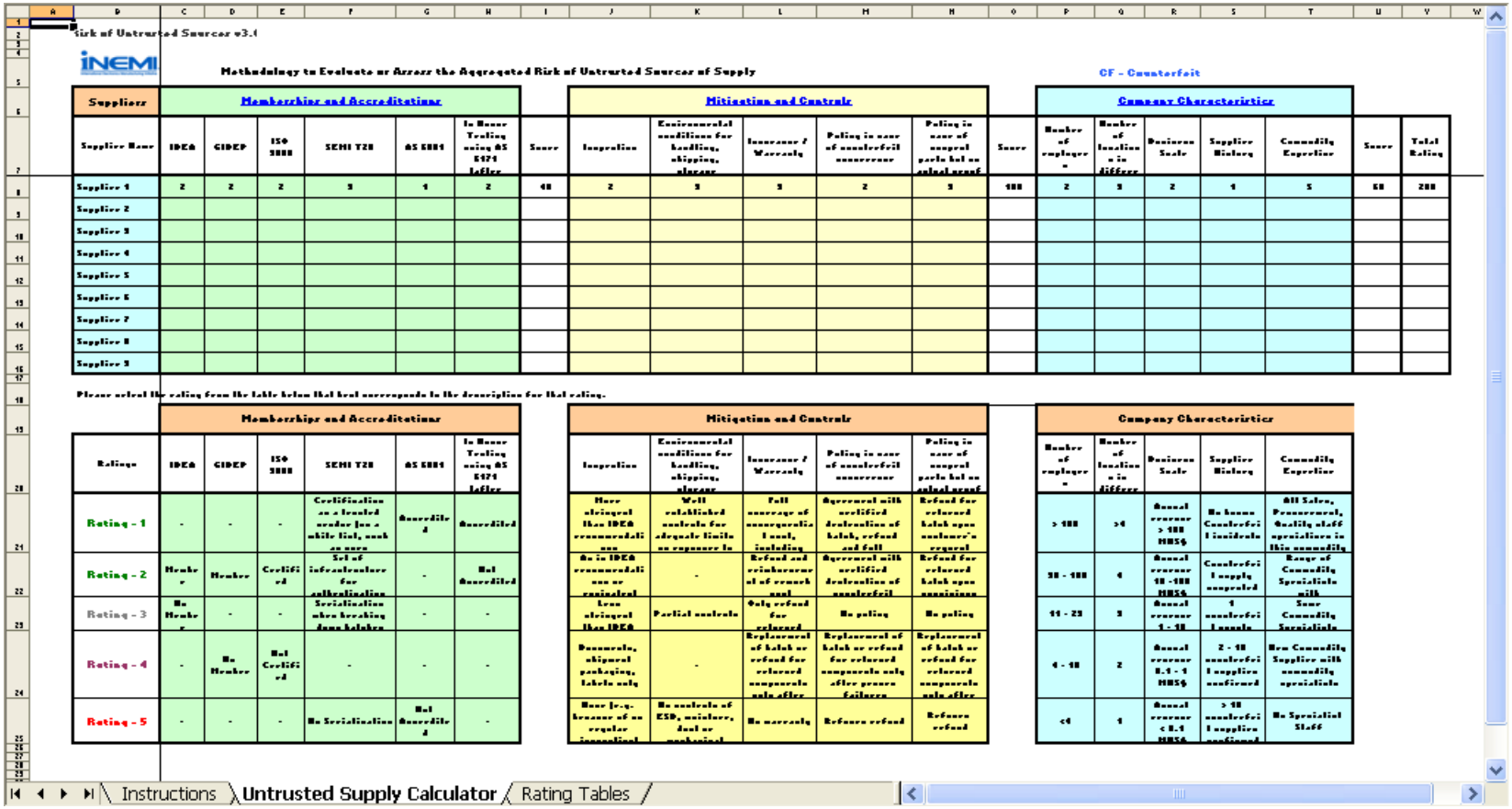
Rating = 1	Product has Low demand and/or is not EOL	OCM	Direct from OCM	Supplier has Strong Mitigation & Controls	No known Counterfeit Incidents	Very difficult to counterfeit; requires factory access or capital investment >$1M	Easy to detect, e.g. by check of packaging, documents, labels, history	Uses Unique Overt and Covert Controls & Identifiers that are easy to validate	Direct-OCMs/ Manufacturers /Suppliers	Minimal Excess inventory. Very limited prototyping/tight OCM security and traceable records that are digitally signed/encrypted and/or independently audited.	Direct to OEM	In-house only under tight controls in certain designated areas, tight security and traceable records (signed / encrypted and/or independently audited)	Exponential factor of 1 for low ease of reuse	In house only, on site physical destruction, traceable records (signed / encrypted and/or independently audited)	1	
Rating = 2	No 2 rating	No 2 rating	No 2 rating	No 2 rating	No 2 rating	Requires major equipment / facilities such as wire bonders and laser markers, >$100k	Possible by optical inspection	Unique Overt or Covert Controls / Identifiers that are easy to validate	Known channel: Franchised/ Authorized Distributors	Excess and prototype inventory under tight controls and security	Trusted Sales Rep and Franchised Distributor to OEMs	In-house + vendor, under tight controls and security	Exponential factor of 2 for high ease of reuse	In house + vendor physical destruction, traceable records, third party certification *	2	
Rating = 3	Product has Low demand and is EOL or high demand and not	Authorized Distributor	Multiple known suppliers	Some evidence of mitigation / controls	Counterfeit supply suspected	Requires moderate equipment and capital ($10k-100k)	Possible by routinely applied 2D X-ray inspection, decapsulation	Overt and Covert Controls / identifiers but validation not easy	Limited - OEMs/ CMs and some use of Brokers	Significant inventory but under tight controls and security	Trusted Sales Rep and Unfranchised distributor to CMs	Primarily offsite vendor based, with controls and security.		Offsite vendor, with controls and records for physical destruction	3	
Rating = 4	No 4 rating	No 4 rating	No 4 rating	No 4 rating	No 4 rating	Needs simple equipment such as sand blasters and ink printers	Requires advanced analytical tactics, i.e. XRD, CSAM, 3D X-	Some overt controls / identifiers but validation not easy	Very Limited - Primarily Reputable Independent Distributors /Brokers	Some controls in place. No traceable records. No security	Independent Distributors, dependent on end	Offsite some controls in place. No traceable records. No security		Offsite vendor, some controls and records. No	4	
Rating = 5	Product has High demand & is EOL	Broker or Ind. Distributor	Supply line not defined / clear	No evidence of mitigation / controls	Counterfeit supply confirmed	Easy - little / no investment required (<$1000)	Difficult to detect; nearly indistinguishable from authentic	No special controls in place	No control / Unknown- Unknown Independent Distributors/ Brokers /Unknown	Excess and prototype inventory not controlled	Customer not defined, open market.	Offsite Vendor, no controls and no traceability		Vendor or no vendor. No controls, no records	5	

NIST Product Authentication Information Management Project

The risk calculator for untrusted sources (#2)

- Based on objective information, the calculator produces relative ratings which are expected to be correlated to the risk of receiving counterfeits from untrusted sources.
- The ratings can support a decision whether to purchase from a particular source or which of several suppliers to choose.

Screenshot of Untrusted Source Risk Calculator



Risk of Untrusted Sources v3.1

Methodology to Evaluate or Assess the Aggregated Risk of Untrusted Sources of Supply

CF - Counterfeit

Suppliers	Memberships and Accreditations							Mitigation and Controls						Company Characteristics						
Supplier Name	IDEA	GIDEP	ISO 9000	SEMI T20	AS 5001	In House Testing using AS 5171 Jaffer	Score	Inspection	Environmental conditions for handling, shipping, storage	Insurance / Warranty	Policy in case of counterfeit occurrence	Policy in case of output parts but no actual proof	Score	Number of employees	Number of locations in different	Business Scale	Supplier History	Commodity Expertise	Score	Total Rating
Supplier 1	2	2	2	3	1	2	40	2	3	3	2	3	100	2	3	2	1	5	60	200
Supplier 2																				
Supplier 3																				
Supplier 4																				
Supplier 5																				
Supplier 6																				
Supplier 7																				
Supplier 8																				
Supplier 9																				

Please select the rating from the table below that best corresponds to the description for that rating.

	Memberships and Accreditations						Mitigation and Controls					Company Characteristics				
Ratings	IDEA	GIDEP	ISO 9000	SEMI T20	AS 5001	In House Testing using AS 5171 Jaffer	Inspection	Environmental conditions for handling, shipping, storage	Insurance / Warranty	Policy in case of counterfeit occurrence	Policy in case of output parts but no actual proof	Number of employees	Number of locations in different	Business Scale	Supplier History	Commodity Expertise
Rating - 1	-	-	-	Certification as a trusted vendor (on a white list, such as ours	Accredited	Accredited	More stringent than IDEA recommendations	Well established controls for adequate limits on exposure to	Full coverage of nonsequential cost, including	Agreement with certified declaration of batch, refund and full	Refund for returned batch upon customer's request	> 100	>4	Annual revenue > 100 MMS$	No known Counterfeit incidents	All Sales, Procurement, Quality staff specialists in this commodity
Rating - 2	Member	Member	Certified	Set of infrastructure for authentication	-	Not Accredited	As in IDEA recommendations or equivalent	-	Refund and reimbursement of remark cost	Agreement with certified declaration of counterfeit	Refund for returned batch upon conditions	30 - 100	4	Annual revenue 10 -100 MMS$	Counterfeit supply suspected	Range of Commodity Specialists with
Rating - 3	No Member	-	-	Serialization when breaking down batches	-	-	Less stringent than IDEA	Partial controls	Only refund for returned	No policy	No policy	11 - 29	3	Annual revenue 1 - 10	1 counterfeit supply	Some Commodity Specialists
Rating - 4	-	No Member	Not Certified	-	-	-	Documents, shipment packaging, labels only	-	Replacement of batch or refund for returned components only after	Replacement of batch or refund for returned components only after proven failures	Replacement of batch or refund for returned components only after	4 - 10	2	Annual revenue 0.1 - 1 MMS$	2 - 10 counterfeit supplies confirmed	New Commodity Supplier with commodity specialists
Rating - 5	-	-	-	No Serialization	Not Accredited	-	None (e.g. because of no regular inspection)	No controls of ESD, moisture, dust or mechanical	No warranty	Refuses refund	Refuses refund	<4	1	Annual revenue < 0.1 MMS$	> 10 counterfeit supplies confirmed	No Specialist Staff

Instructions | Untrusted Supply Calculator | Rating Tables

NIST Product Authentication
Information Management Project

Counterfeit Losses & Costs – Calculator #3

- This calculator provides an estimate of the costs and losses associated with counterfeit product
- There are 3 assessments provided
  - A) Total loss estimate by product
  - B) Loss estimate by GEO or market
  - C) Total Counterfeit Cost & Losses estimate.
- The total loss estimate is based on the output from calculator #1 … where the counterfeit risk result is classified as low, medium or high
- The loss by GEO or market is generated using the World Bank Corruption Control index
- The Total Counterfeit Cost is an estimate of all aggregated costs & losses incurred by a company where counterfeit product has entered that company's supply chain.

Total Counterfeit Loss – Calculator #3

iNEMI
International Electronics Manufacturing Initiative

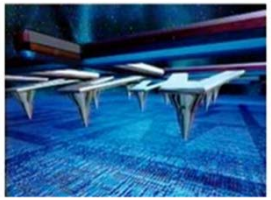
Return to Instructions

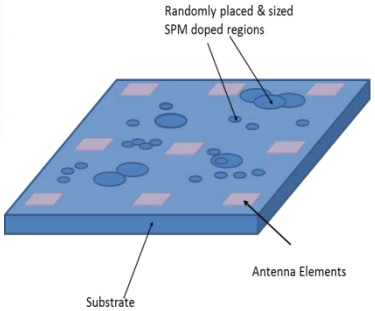
Total Counterfeit Loss Estimation

Products	T3 Risk of Counterfiet	Industry Counterfeit Estimate	W/W Product Revenue US$ (K)	Estimted Losses US$ (K)
Product 1	Medium	5%	200	6.67
Product 2	High	3%	50	1.50
Product 3	Low	3%	100	1.00
Product 4	Medium	3%	250	5.00
Product 5	Medium	3%	100	2.00
Product 6	High	3%	150	4.50
Total			**850.00**	**20.67**

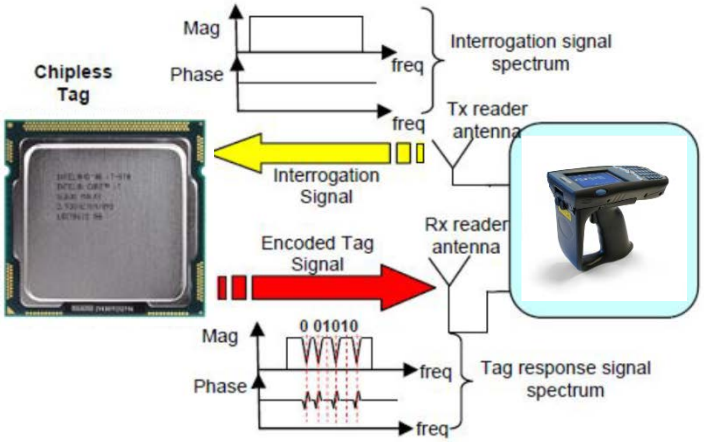
Nano-structured Certificates of Authenticity using Probe Assisted Doping

1. CREATE: Use probe arrays to create nanostructured CoAs



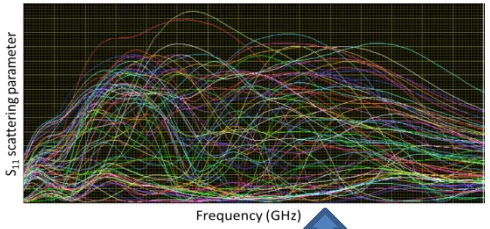


2. READ: Handheld scanners to interrogate CoAs.

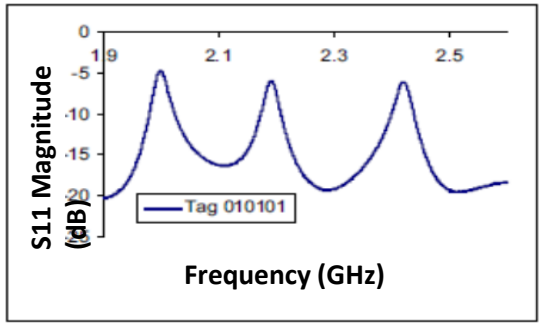


3. VERIFY: interpret and compare output

Raw data



Data transform



GOOD – NO GOOD indicator

NIST Proc Informat

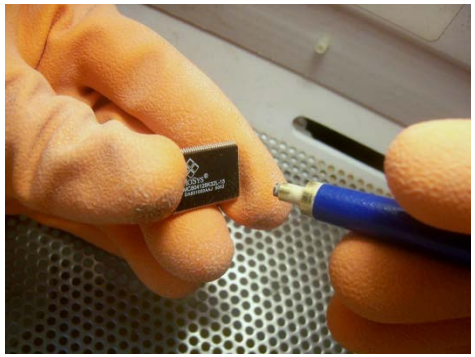
Trusted Microelectronics Stakeholder Needs

- **Government Needs:**
  - Secure components with no side channels for information leakage,
  - Functional fidelity,
  - Reliable components, and
  - Dependable supply sources

- **Industry Needs:**
  - Trustworthy and reliable components,
  - Authenticable components
  - Functional fidelity and
  - Error free mass manufacturing (with the ~10^{12} transistors per chip).

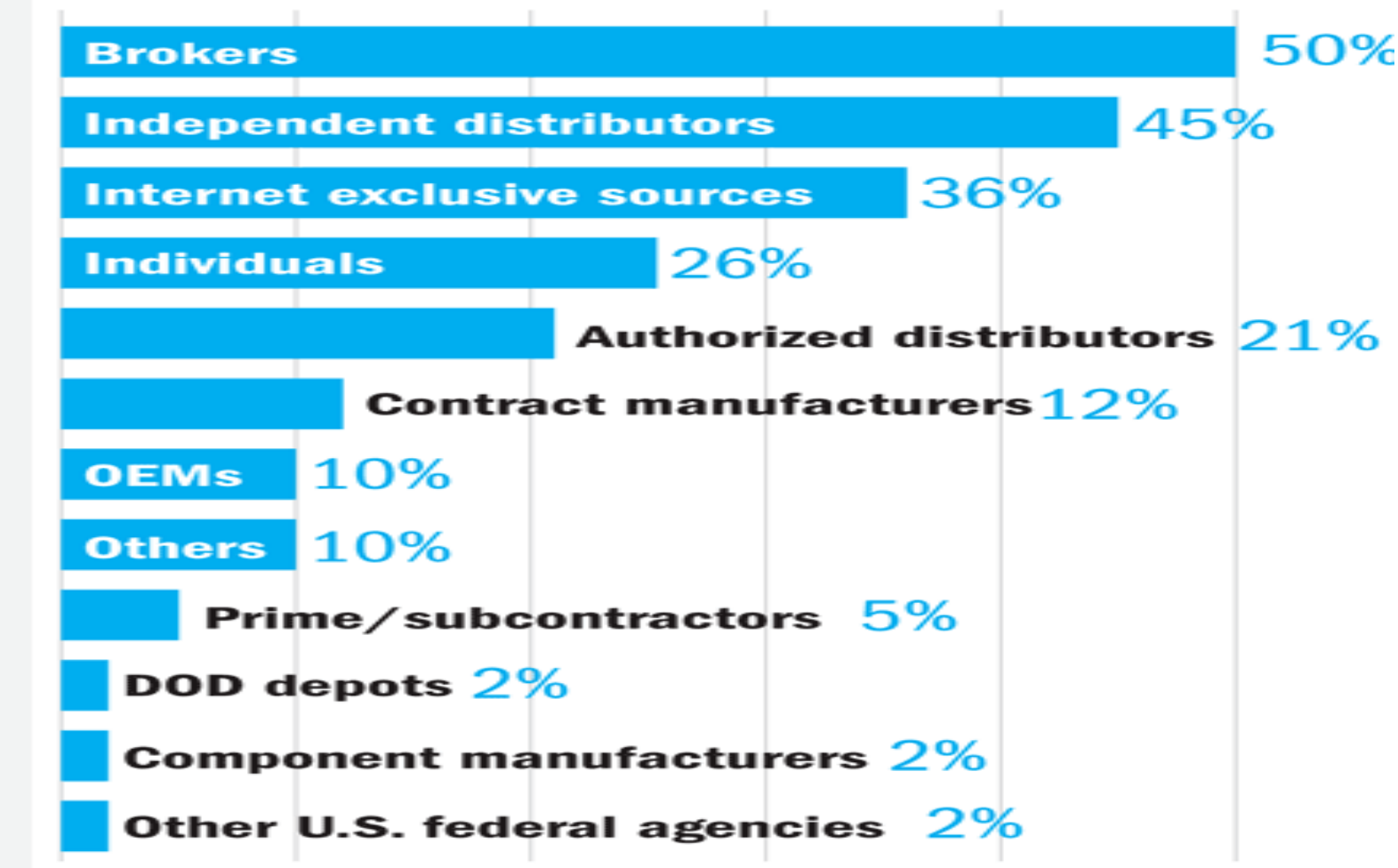
Are Electronic Component Packaging That Is Easy to Alter?

Before and After Microblasting



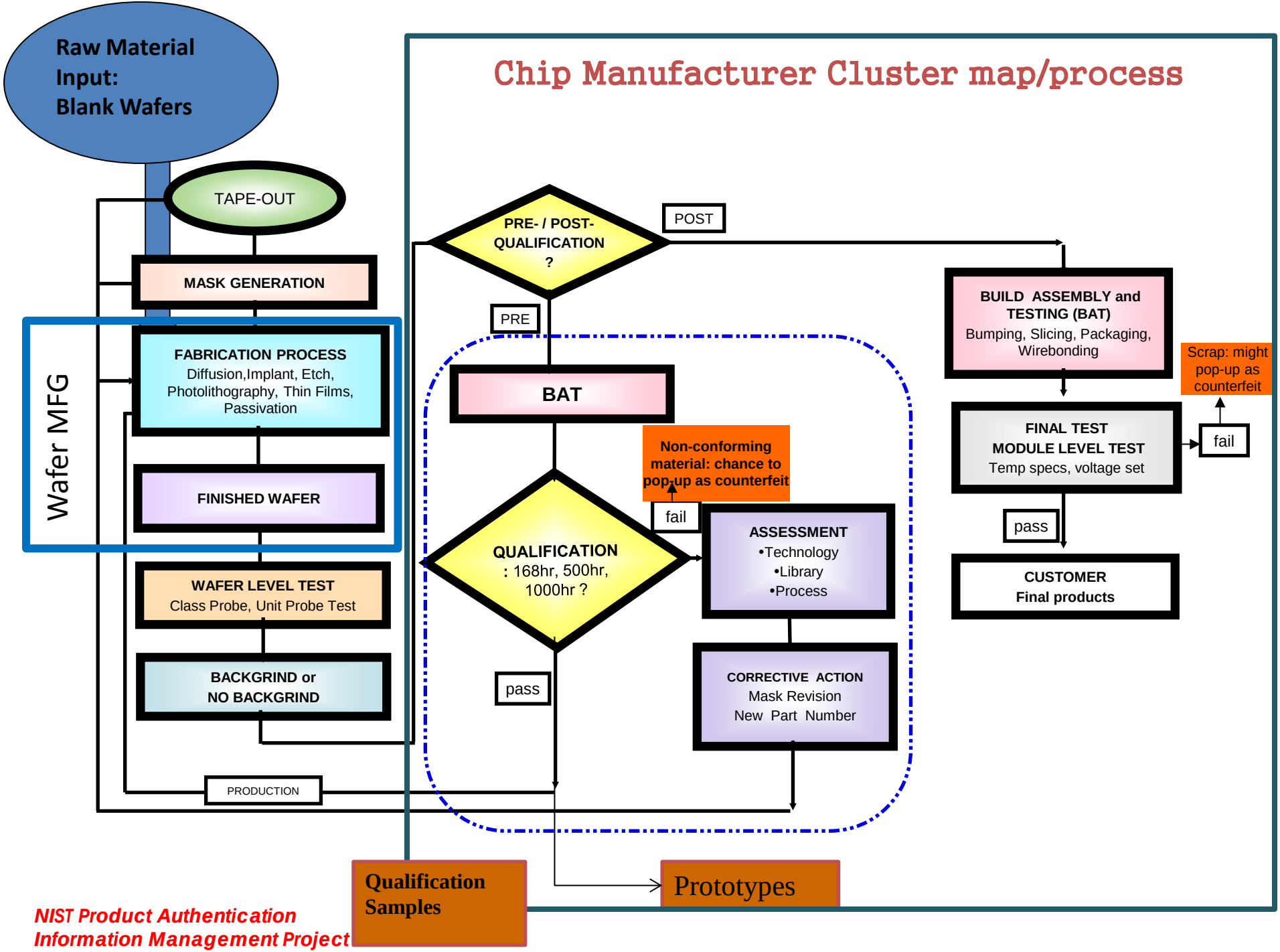
Images from RMV Technology Group, LLC

Where In the Supply Chain are Counterfeits Detected



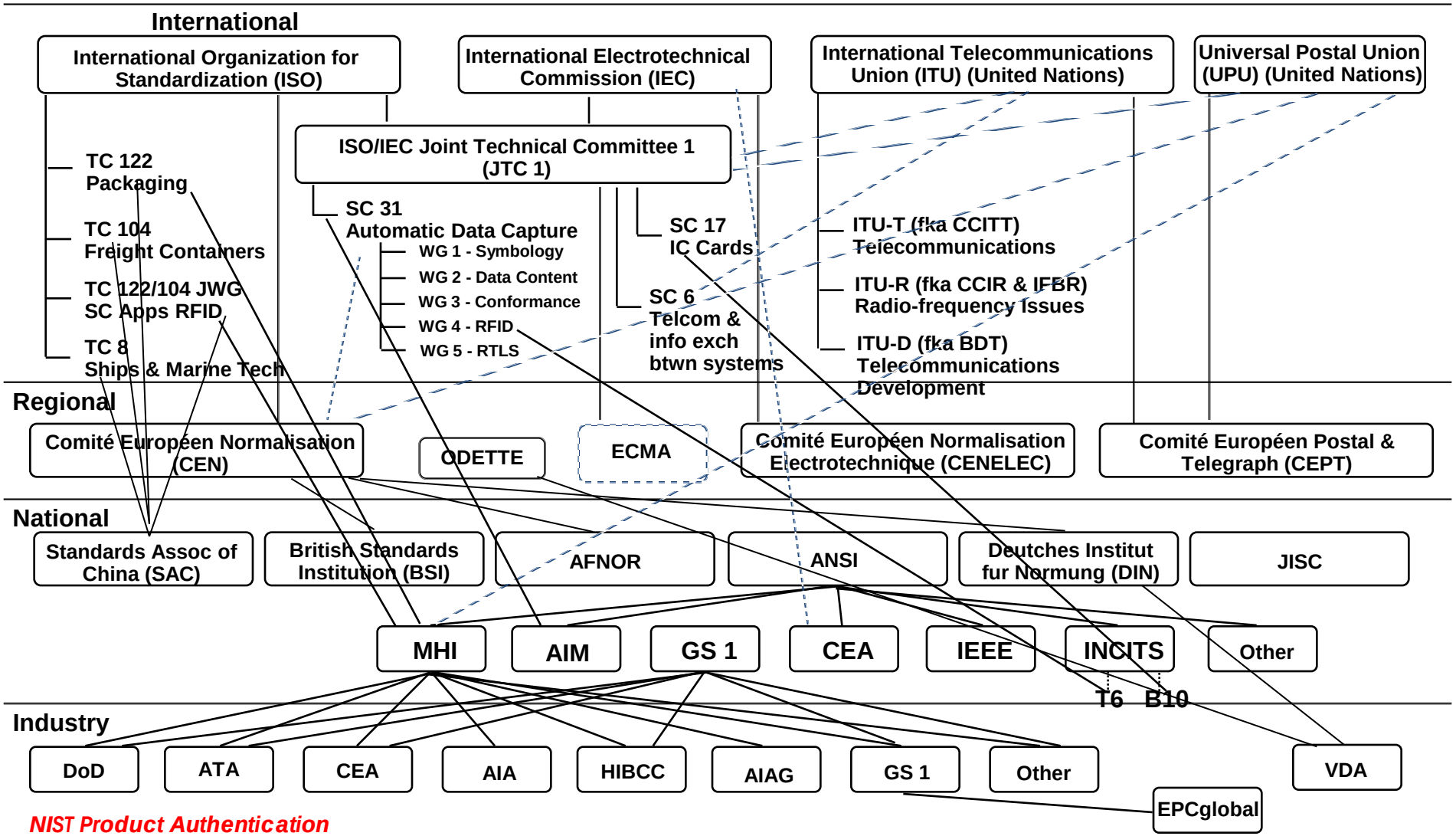
Source: OCM survey, 2009

Chip Manufacturer Cluster map/process



NIST Product Authentication Information Management Project

Standards Organizations



NIST Product Authentication Information Management Project