CENTRE NATIONAL D'ÉTUDES SPATIALES

Counterfeit avoidance
CNES lessons learned and Policy

Philippe LAY

14th March 2013

ESCCON 2013
ESA/ESTEC

Counterfeit Parts

Facts, Detection & Prevention

- **What to know**
  - Facts
  - Evolution (EU, MIL)
  - Why counterfeiting market grows ?
  - Risks for Space Missions
  - Which type of non Original Manufacturer product ?

- **How to detect ‘counterfeit’ parts ?**
  - Indicators (‘Suspect’ Parts)
  - Techniques
  - Three case studies

- **How to prevent counterfeit risks ?**
  - Distributor/vendor Selection
  - Independent vendors

- **CNES lessons learnt on Risk Mitigation**

Facts

- **Using the Term "Counterfeit“**
  - “Quality independent distributors **do not typically use the term *"counterfeit"*** unless the manufacturer of the product states that the product is counterfeit in writing.
  - Instead independent distributors typically use the word ***"suspect“.***

“Counterfeits production is on an industrialized scale”

- **Counterfeiting**
  - Is an **industry global problem**.
  - Is increasing with emerging trends and technology.
  - Has **economic consequences**

- Organized crime is involved in the distribution network and make massive profits
- High quality of counterfeit parts often makes identification impossible without technical expertise.
- Quality is now so good that counterfeit parts may have additional security holograms, better packing, etc., than the originals !

Counterfeits = ~8% of world trade → Lost sales of as much as $600B (2008)

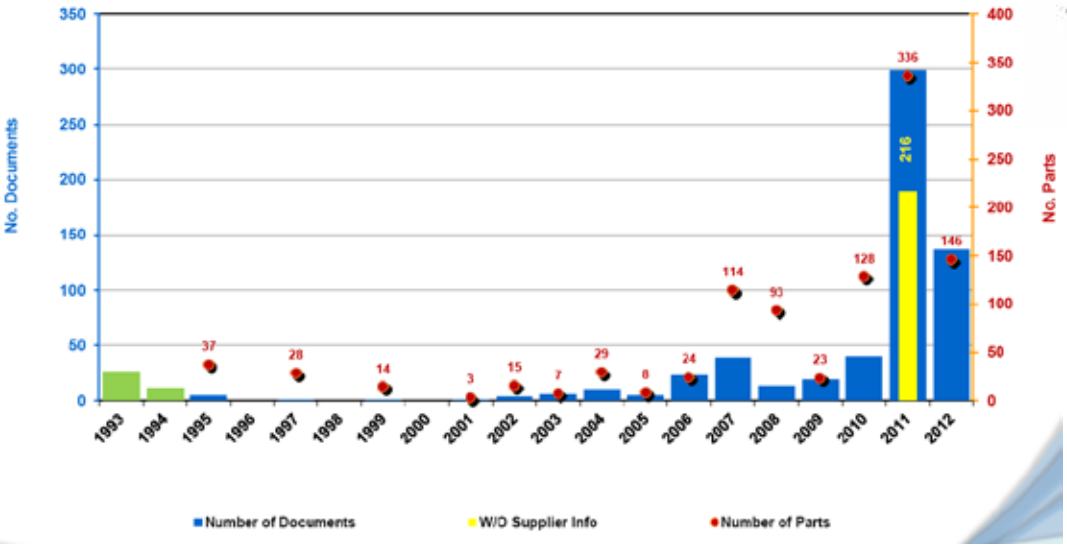
- In **2008**, EU customs have seized more than 178 million fake goods, a **126% increase from 2007**: **no indications of a decrease** in the problem, production is on an industrialized scale.

Evolution

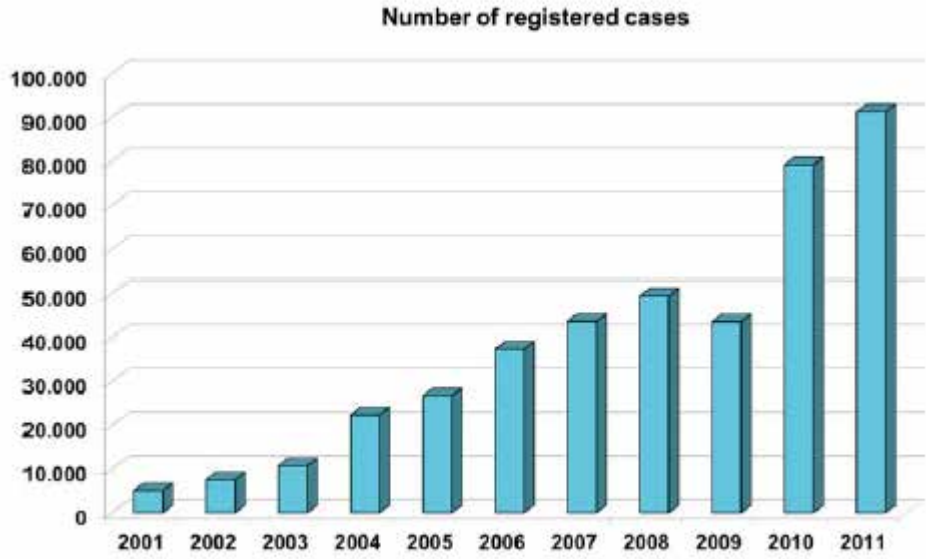
■European Commission statistics relating to counterfeit and piracy : 2010 to 2011 = +15%,

■Electronics: second counterfeited market after the pharmaceutics one

No global statistics on electronic parts



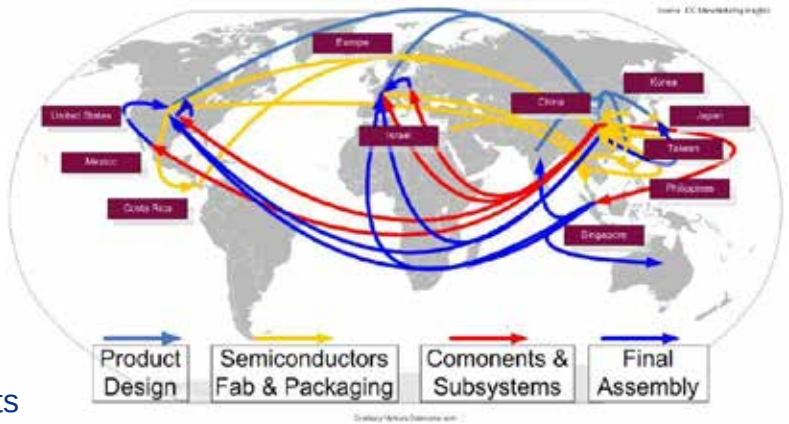
(*source: GIDEP Operation center GIDEP update October 2012*)



(*source: Report on EU customs enforcement of intellectual property rights*)

Why counterfeiting market grows ?

- **Profit**
  - Explosion of counterfeiting is essentially link to the high profits generated regarding low risks involved…
- **Supply Chain**
  - Smaller users cannot access to the original manufacturers, they are forced to procure through a supply chain with several intermediate suppliers,
  - Opportunity for the emergence of independent vendors (selling surplus products as well).
  - The supply chain from the OM design centre to the final end user (wafer fabrication site, assembly line, distributors…) is so word wide that it has become easier for the counterfeiter to penetrate the market.



- **Off-Shoring/expatriation/relocation of Manufacturing**
  - Transfer to Asia / India
    - Wafer fabrication sites
    - Assembly of PEDs and a very large proportion of hermetic products
  - Consequently Increasing of the offshore capacity providing the fake industry with a massive opportunity…
  - Difficulties in controlling industries (less control)
    - Production can move rapidly
    - New laws with limited impact
    - Unscrupulous employees produced counterfeit semiconductors at genuine semiconductor plant

Why counterfeiting market grows ?

- **Detection : Costly and Difficult**
  - Parts more complex : electrical tests more difficult
  - Counterfeiters are getting better
- **Internet**
  - part sourcing history is often impossible.
  - Responsibilities : replacement and refunding is a nightmare
- **Rapid Obsolescence**
  - Programs Time cycle >> parts time cycle
- **Planning**
  - Planning not adequate with parts delivery time
- **Price**
  - To search for unrealistic prices
- **RoHS**
  - Original manufacturers converted their processes, some parts are not more available in SnPb version.

ð **Graal quest :**

- Trend to search for parts everywhere, quicly, at low cost: loss of common sens vs attractiveness

Our Perimeter :

- Low risk for past projects (<2002)

- **Sensitive EEE Parts**
  - Usually **commercial parts**
  - But also **MIL Hi-Rel parts** (see GIDEP Alerts on QML products)
  - No/reduced risk on ESCC qualified parts ? Not (yet) impacted : direct procurement or very short procurement chain with dedicated/specialised distributors.

- **Sensitive Projects**
  - Projects with medium to high integration of commercial parts (or MIL HiRel)
  - Recurrent programs
    - Parts stocks to be renewed
    - Obsolescence…
  - Equipments from suppliers without procurement skills, know-how or capabilities

Which type of non-OM product ?

Stolen Product

- A finished product with OM markings and complete processing and testing
  - **Can be indistinguishable** from genuine product (even marking may be listed on manufacturer's website !)
  - **Can be a partially-processed one** stolen during transportation between two separate manufacturer's facilities.

- **Used techniques can be**:
  - Process from stolen masks
  - Stolen designs: deprocessing parts shoot photos, generate masks.
  - Made by authorized OM offshore site… but run off after hours… (tests skipped,…)
  - **From OM rejects… genuine marked, but failed product :not only on functional/data sheet parameter but also on Production criteria , SPC, leakage current, ...**

Fake Product

- An existing "good" / genuine part remarked as something else (higher grade : variant, quality, max frequency, temperature range, date-code).

- **Used techniques can be**:
  - To change the marking on the part
  - To change data package: fake screening or Certificate of Conformity (CoC)
  - To select a device roughly matching the specification
  - To substitute a "High Rel" part by a "commercial grade" part

Which type of no-OM product ?

Refurbished Product

- A product with an external appearance looking “new”:
  - Package cleaned-up externally (*polishing, solvent washing, boiling in DI water, tumbling with walnut shells*)
  - Leads raked and straightened, re-tinned...
- Some origins of refurbished products:
  - Parts removed from old, scrap or failing boards (called **scrapped parts**).
  - Obsolete product : parts are pulled from stock of old boards, sold at the highest price (*based on scarcity*).
  - Chip manufacturer’s production parts with gross manufacturing errors: no die inside, no wires inside.
  - Reel marked as Lead Free but actually is SnPb
  - Unmarked surface-mount component that no one can visually identified

- **Used techniques can be**:
  - To **remove parts from scrapped populated PC boards and others equipment**.
  - To **segregate parts** : style, pin count and other features
  - To **straight leads**: by hand or with dedicated equipment
  - To **erase top surface**: with sandpaper or blacktopped with epoxy, etc…
  - To **remark** them: (*discrete components smaller than 0603 may have no marking at all…*):
  - To **put parts in tubes, trays or reels,**
  - **Ready to be sold on the open market**

Indicators… *(‘Suspect’ Parts’)*

There is no methods fully efficient to detect counterfeit parts

Comparison with known authentic examples

Assistance from the original manufacturer

- Part **supplied from a non-authorized distributor** (i.e.: independent distributor, broker, authorized distributor from another original manufacturer…)
- **No information of part origins** (i.e.: no traceability of the distributor)
- **Price** of the part is unusually **low**
- **Difference appearances of parts** in the same shipment.
- Inconsistency between **vendor name on the part and on the packing**.
- Parts **packing** with **marks or scratches** (external visual inspection)
- **Labels** or parts packing are **altered, photocopied, at unusual location, incomplete / missing data** …
- Part **packaging** with **marks or scratches** (external visual inspection)
- Part packaging is **not consistent with supplier’s normal packaging** (or documentation requirements)
- **Unusual disclaimers** or denials of responsibility for the **accuracy of test results**
- Part **matches** the description of **one listed on suspect item list**
- **Suspected documentation**
- **No clear / justified /traceable procurement chain intermediaries**

Techniques

Too late…

- **Visual Inspection (External & Internal)**
  - Be careful regarding visual inspection !
  - Cases have been reported where parts samples have been offered by a broker prior to the whole shipment in order to verify parts authenticity, but if parts samples were authenticated, others parts of the shipment were counterfeits… (GIDEP Alerts PD-A- 06-01 and PD-A-06-02, "*parts marked as Analog Devices "mil temperature range" product, but contained Linear Tech die*")

- **Original Manufacturer Help**
  - Some OM provide support to users who believe they may have received counterfeit parts
  - Nevertheless, obtaining support from an OM can be a significant challenge:
    - They have no obligation to provide support for parts not acquired through an authorized source.
    - OM generally discourage users from purchasing their products from independent distributors
  - It shall be notice than during the last ***Anti-counterfeiting workshop of customs experts on semiconductors in Korea on 21-22 September 2009,*** All participants underlined the importance of having access to information from the semiconductor industry on products and processes to facilitate customs' identification of suspected counterfeit products

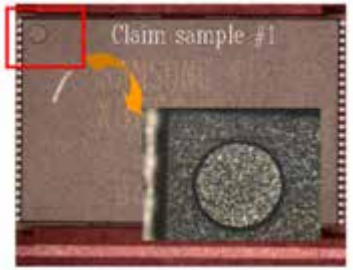
- **Electrical Tests / Burn In / Life Test …**

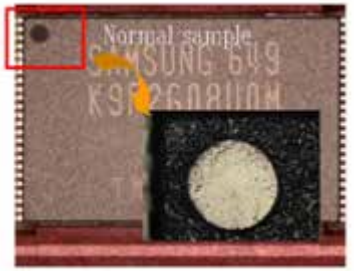
External Visual Inspection (not destructive)

- **External Physical Aspect (device surface)**
  - Used part appearance
  - Inadequate part packaging
  - Part packaging wear marks or scratches
  - No marking on parts
  - Inadequate typography
  - Device surface is erased (sanding).
  - Look at the shape of the index holes.
  - Look at the corners: reclaimed devices are desoldered from a board, then the leads are bent back into shape, then retinned. They see a lot of handling, check the package corners it often shows the damage.

claim sample

normal sample



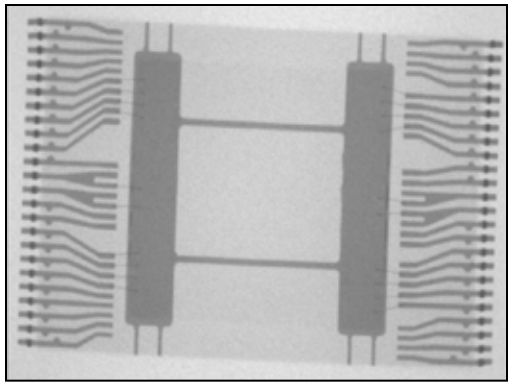


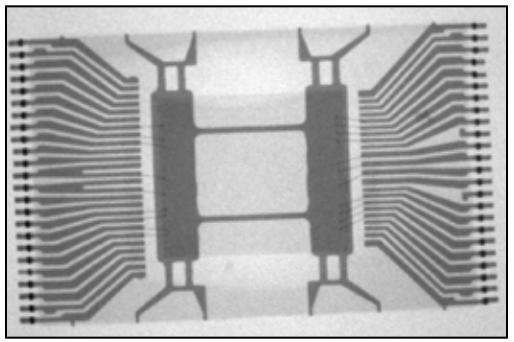
- **Physical dimension errors**
  - With a dedicated tool, sanded part can often be discovered.

- **Leads**
  - To look at the leads to verify if they are:
    - Straight,
    - Properly aligned,
    - Free from solder,
    - Free from scratches & cracks
    - Not corroded or oxidized

External Visual Inspection (not destructive)

- **Marking**
  - Lot / Date Code Verification
  - **Original Laser Marking**: As packages are very thin, counterfeiters sand just enough to re-laser mark on the device surface. In some case, counterfeiters left some of the original laser marking.
  - **Marking Permanency**: identity (and traceability) of the part on the package. As counterfeiters often use bad ones, a marking permanency test can be proceeded:
    - Don't use a too aggressive solvent (*)



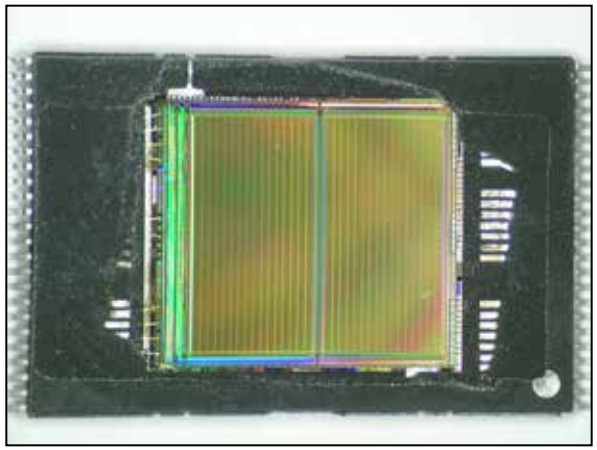


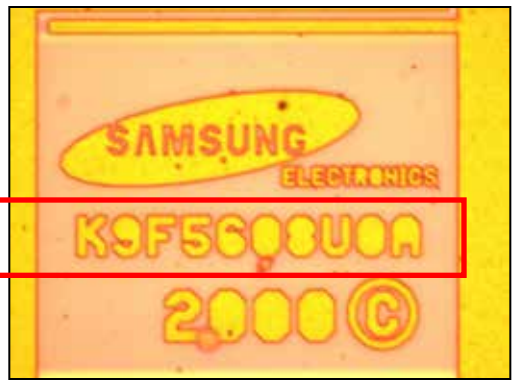
- **Die location – Frames**
  - Using X-ray to inspect die location and frames positions

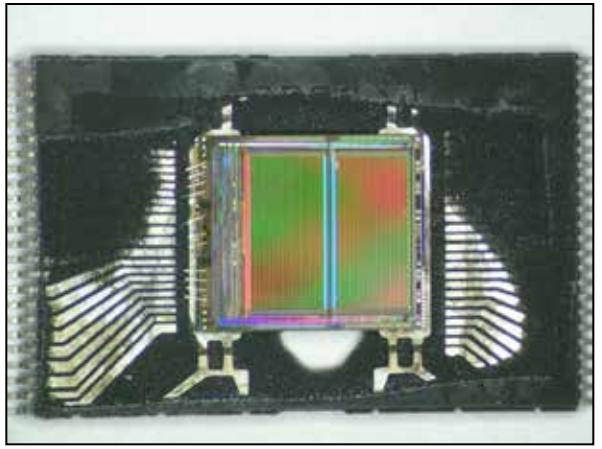
(*) As specified in ESCC Basic Specification No. 24800, "*Resistance to solvents of marking, material and finishes*", markings are resistant to Ethyl alcohol (99.5% or 95% pure by volume), Isopropyl alcohol (99% pure).

Internal Visual Inspection (destructive)

- **Destructive Physical Analysis (DPA)**
  - To detect wrong die dimensions (medium)
  - To detect wrong markings (easy)
  - To detect lack of die (easy)
  - To detect refurbished die (difficult)







There is no method fully efficient to detect counterfeit parts

Three Case Reports (CNES)

July 2006

- Failure on an electronic board (ground equipment)
- Few failed parts
  - Electrical analysis allowed to identify the wrong part
- No relation with known defaults with this type of parts
- External Visual Inspection:
  - On a batch, **lack of marking** on the bottom face à Unusual
- Non-OM Confirmation

Inexperimented Supplier

Purchasing through independent distributor

No Original Manufacturer CoC

CNES not informed of the purchasement source

Defect on a electronic board

April 2007

- CNES informed by a supplier of 'suspect' parts after DPA
  - Glassivation non-integrity
  - 2 different lead frames (RX) / different die dimensions (RX) / different bondings (RX)
  - 2 different die markings (DPA)
- Non-OM Confirmation

CPPA

Obsolete Parts

Purchasing through independent distributor

Parts at incoming revealed bad markings… but with CPPA CoC

DPA performed by the supplier

Parts already mounted on electronic boards (and obsolete parts…)

October 2007

- CNES informed by a distributor of 'suspect' parts after electrical tests + DPA
- OM Confirmation

Obsolete Parts

Purchassing through independent distributor

Electrical Tests + DPA

No Impact: Strategic Purchasement

Distributor Selection

- The most efficient approach to avoid counterfeiting is to purchase product:
  - **Directly from the Original Manufacturer** (OM), or
  - **From a distributor who is franchised or authorized by the original manufacturer**
    - An authorized distributor receive products directly from the manufacturer and may be audited by the manufacturer from time to time to verify the integrity of the supply chain.
- These two supply ways are the only ones from which the original manufacturer warrant their products.
  - Consult part manufacturer's websites for their authorized distributors, sales office contacts, resellers or aftermarket suppliers
- Advantages:
  - Original Manufacturer **warrantee**.
  - **Product integrity** via proper handling, storage and shipping procedures
  - **Failure analysis** and **corrective action support** (if needed)
  - **Traceability** via certificates of conformance and acquisition traceability

Sometimes unauthorized distributors or brokers use manufacturer trademarks or logos to communicate as an "authorized" distributor. **You shall verify if the company is listed as a true authorized distributor**. If not, to inform the OM is a good practice.

Independent Vendors

- Why to purchase parts from a broker when an authorized distributor or the OM can supply parts ?
- Nevertheless, a substantial number of products are no longer available through authorized distributors and directly from the original manufacturer: obsolete parts…
  - **Independent distributors fill this gap.**

- **Potential risks:**
  - Poor capabilities, education, training **to spot counterfeits.**
  - **Limited inspection and test capabilities** (and use unsuitable labs for inspection and testing).
  - Poor history/traceability of the whole supply chain (including storage conditions : ESD, Humidity chain break)

Be careful regarding procurement specialists !
They are generally NOT authorized distributors à To check Intermediate Vendors

Independent vendors

- ***A few rules before Purchasing…***
  - **To know** the selected independent vendor
  - **To specify** clearly and completely product to purchase (detailed specification, package, screening, date code…)
  - **To negotiate** a specific contract with him:
    - To define verification techniques on parts at incoming (visual Inspection, Verification and Testing…)
    - To define verification evidences to be submitted to the purchaser (with shipment and before payment)
    - To define traceability requirements (CoC of the original manufacturer and previous distributors…):
    - To define cost/payment plan
    - To define contract terms and conditions: "*With evidence of counterfeit parts, parts shall be destroyed and returned without payment*"

- ***A few rules After Purchasing***
  - Unless performed jointly, **to perform verification** on parts at purchaser incoming
  - **To confirm parts authenticity** from the original manufacturer (be careful: parts could be refurbished parts from scrapped boards but 'genuine' products !)
  - **To store a few items** from each shipment if further investigation is required

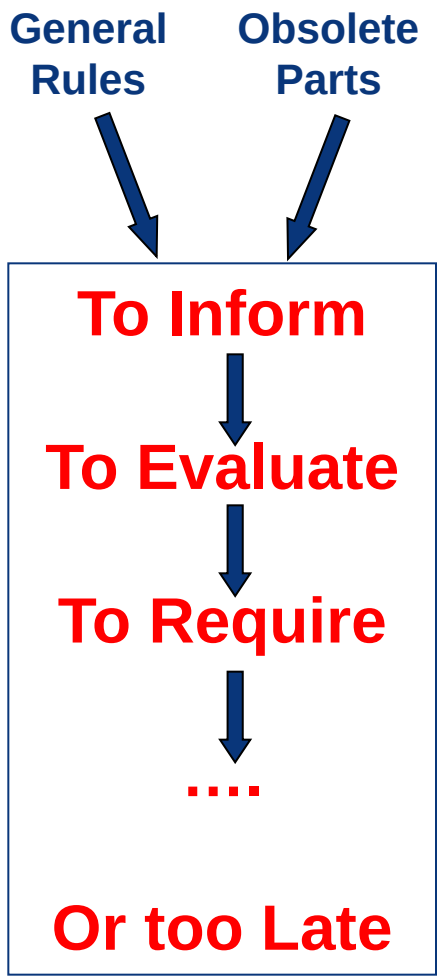
  - Inability of an independent vendor or to provide original manufacturer certificate of conformance or acquisition traceability does not imply that parts are counterfeits !

Risk Mitigation

- **Risk Evaluation on CNES current and future projects**
  - To clearly identify the whole Industrial organization: suppliers, laboratories…
  - To verify each part supply chain: CPPA, independent distributors ?
  - For each 'suspect' part: data, CoC, verification techniques, DPA… ?

- **Risk Information/education to CNES teams / Suppliers**
  - Alert CNES Sheet n ° 1081 (2007)
  - Workshop CCT Contrefaçon 2007
  - CNES Focal Point: D. STANDAROVSKI (denis.standarovski@cnes.fr)
  - Questionnaire to laboratories / suppliers about their purchasement strategy
  - Meetings with laboratories / suppliers to inform about counterfeit risks and improve their purchasement strategy

- **CNES AP requirements**
  - Questionnaire to laboratories about Requirements (ECSS-Q-60) knowledge
  - Requirement to purchase directly through authorized distributor à warrantee
  - Requirement to purchase an unique batch of parts
  - Requirement to inform CNES about the supply chain for each parts
  - Requirement to deliver Original Manufacturer CoC (if possible…)



Conclusions (1/2)

- More and more of counterfeits, including Mil system and Mil space grades (class S, QML V, MIL ER R ou S),
- The ESCC system is safe (for the moment)
- Some companies sell data bases listing counterfeit components
- There is a link between obsolescence and counterfeiting : look for the rare part whatever the conditions are
- Certificate of Conformance is not a 100% guarantee
- The procurement needs ressources, skills & know-how
- CNES published a general alert n ° 1081 (2007)
- Don’t forget the common sens (if you don’t know where/what you buy …)
- ECSS-Q-ST-60 C rev1 & 2,
- ECSS-Q-ST-60-13 (COTS) includes adequate requirements

Conclusions (2/2)

- We consider there is no 100% technic/test/sorting to detect fakes despite the incoming inspection has a certain efficiency,
- The solution is to know & guarantee the whole procurement chain : robustness, credibility, transparency, traceability.
- But to check 100% of the whole supply chain is not reasonnably feasible
- Education is also a key