

COTS IN DEFENCE

P.Langlois

Project Officer CapTech Technologies for Components & Modules



CONTENT



- What are we talking about
- Why COTS
- COTS Market
 - Trends
 - Risks associated
 - Mitigation options
- COTS in Defence : needs & requirements
 - For what purpose
 - Military specificities
 - What types of COTS
- Conclusion
 - Recommendations
 - Roadmap

WHAT ARE WE TALKING ABOUT

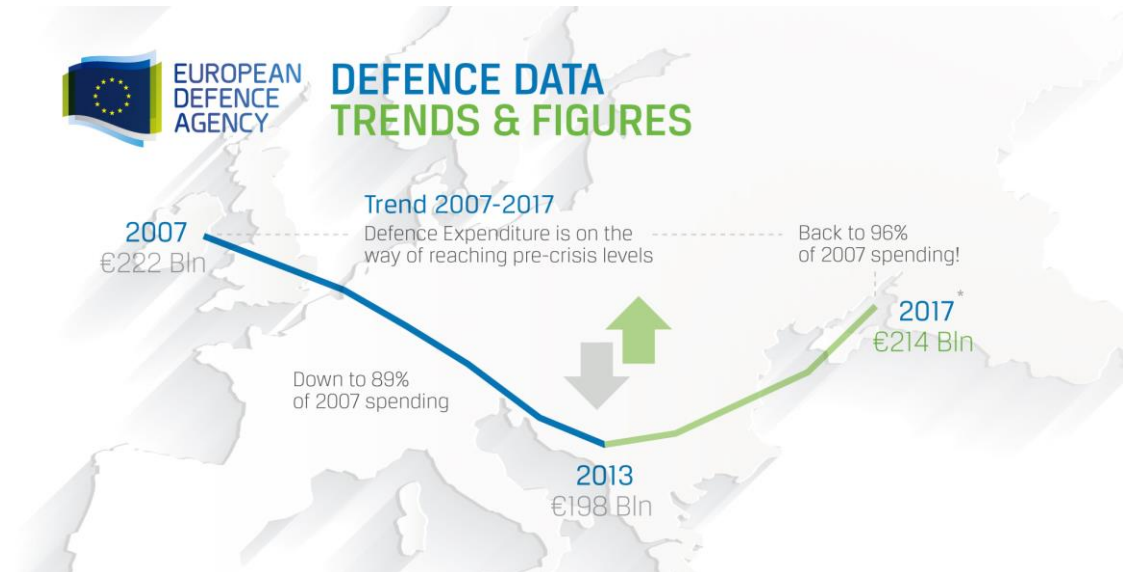
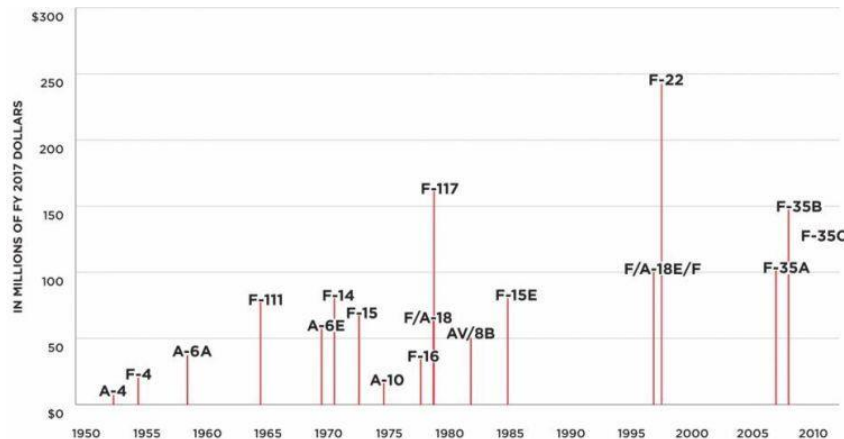


Some definitions of COTS

- **COTS:** An assembly or part designed for commercial applications for which the item manufacturer or vendor solely establishes and controls the specifications for performance, configuration, and reliability (including design, materials, processes, and testing) without additional requirements imposed by users and external organizations.
- **COTS Plus:** A COTS part supported by test data available to end users establishing random failure rate assumptions, performance consistent with the manufacturers data sheet and methods to exclude infant mortal parts, parts with latent defects, weak parts, or counterfeit parts.
 - For example, automotive electronics council-certified (AEC) or compliant automotive parts are one type of COTS Plus.
- **MOTS (military off-the-shelf)** refers to an off-the-shelf product that is developed or customized by a commercial vendor to respond to specific military requirements.
- U.S. government, the **Federal Acquisition Regulation (FAR)** has defined "**COTS**" as a formal term for commercial items, including services, available in the commercial marketplace that can be bought and used under government contract

WHY COTS

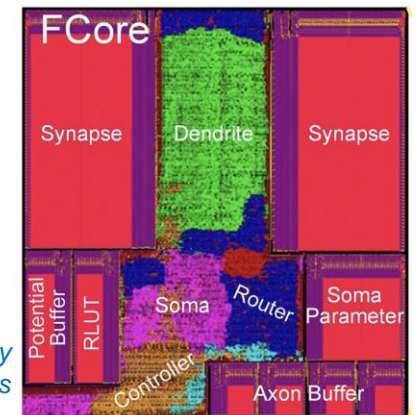
- Defence used to be a major driver of semiconductor technologies back in the 1960s and 1970s, and its purchases were significant.
- Now, Defence purchases are less than 1% of the semiconductor market,
 - Meaning that most of the time Defence Equipment manufacturers can only purchase semiconductors that are manufactured for the broad market.
 - Integrated circuits are a mass-production technology, and with 300mm wafers and \$7B fabs
- In Europe, Defence budget issue:
 - Global defence expenditure recovering after reduction
 - Advanced weapons are more and more costly
 - Quantities per system are reducing (in western countries)



COTS MARKET

Trends & Challenges

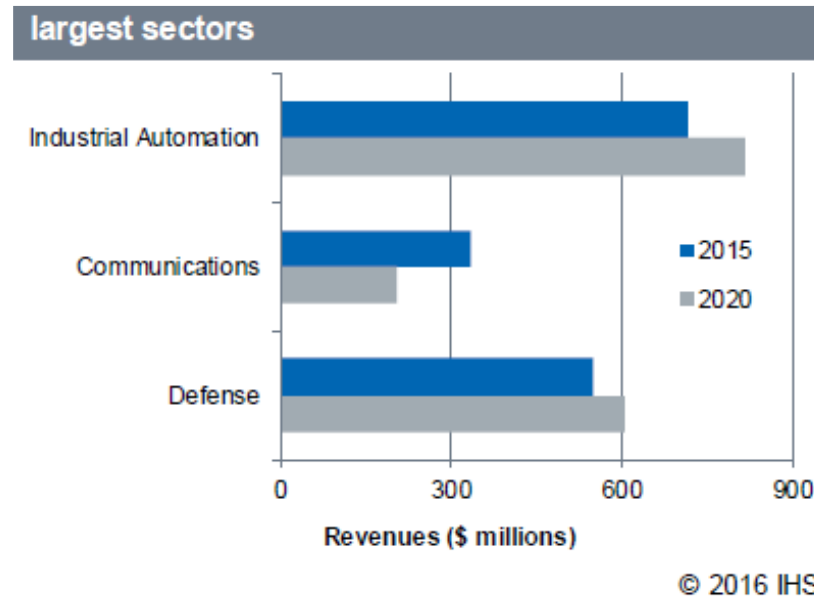
- Semiconductor companies are focusing in vertical markets,
 - Such as analog processing, automotive, power electronics, smart phones, servers ...
- The general-purpose IC companies:
 - Either disappear or are acquired by more specialized companies focused on a few application markets;
- Packaging such SiP and chiplet gain ground as costs of advanced node designs increase,
 - but DSM chips continues to play a role for smart phones, data servers, neural networks and FPGA;
- Traditional devices such DSP, FPGA and GPP used in military applications are disappearing;
 - Their functions are integrated as ASSP solutions designed for one specific application domain.
 - It will become more difficult for the military OEM to get access to these ASSP developed for high volumes and requiring important engineering support efforts.
 - As well GPU devices are not accessible for custom designs for low volume applications;
- New paradigms in application such Artificial Intelligence, Internet of Things (IoT) and automatic driving will bring new digital processing solutions.



The layout of an "FCore" computing core in the Tianjic chip by China's Tsinghua University scholars

Trends & Challenges

- The world market for Embedded Computing, boards, modules and systems is forecasted to represent more than US\$ 3 Billion by 2020

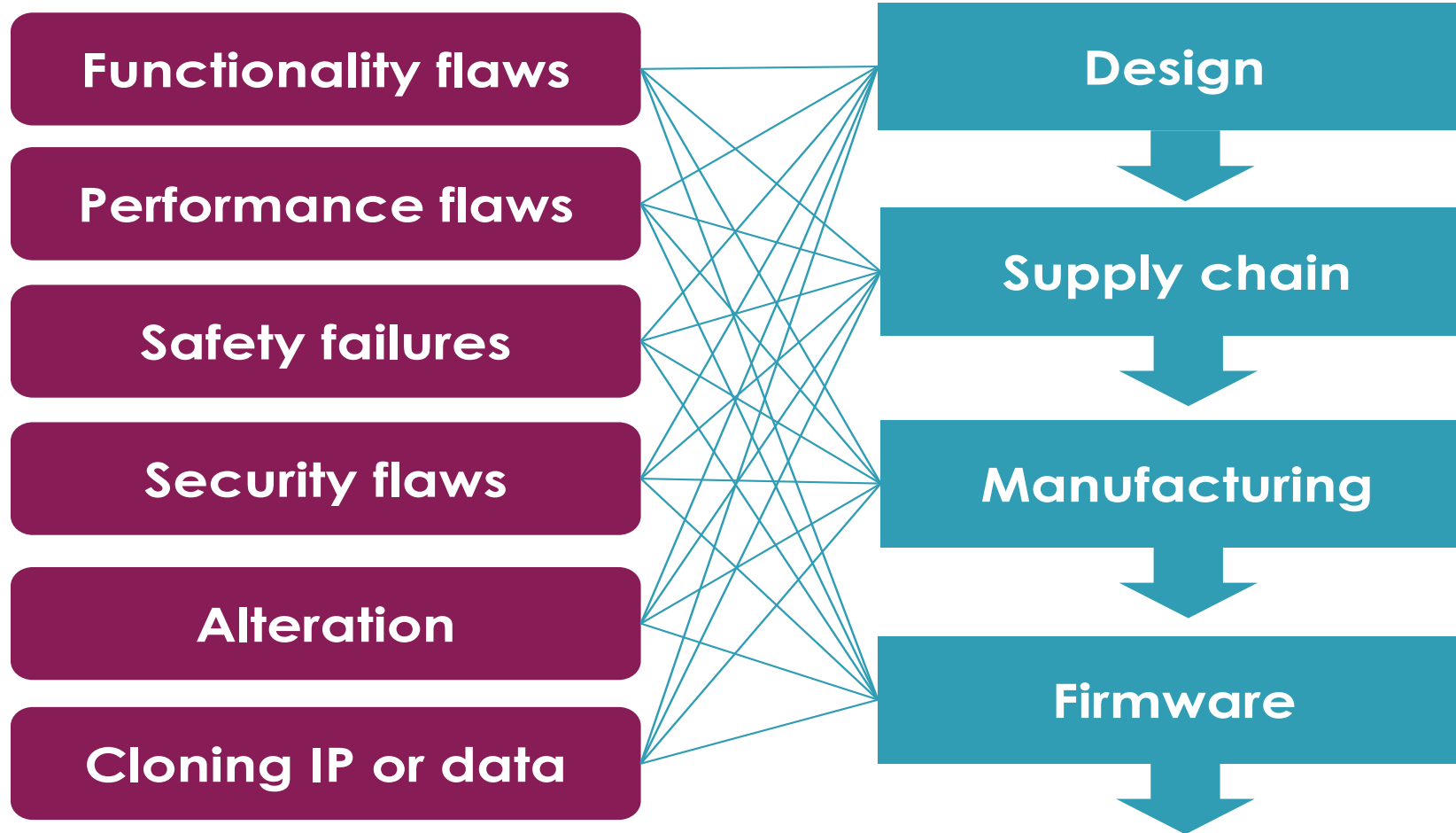


- The three largest sectors are Industrial automation, **Defence** and Communications.

- On Defence Market, VITA forms (VME & VP standards) represent a big part of the used solutions for data processing, and around US\$ 250M in revenue.
 - Military systems represented over 78% of sales by revenue for VITA products in 2015 and National defence expenditure (particularly US) represents the major growth driver for sales of VITA boards and systems.
 - For complex boards solutions, VME continues to be used, however VPX solutions are more and more used for new designs.

Trends & challenges

- Multicore processor technology is fuelling growth in the defence embedded systems market over the next five years
 - Emergence of modern electronic warfare (EW) and network centric warfare systems
 - And the increased use of wireless and cloud computing technologies
- Legacy architecture X86 is mostly used in Digital COTS boards products
 - Vulnerabilities have been declared in X86 (Meltdown...) and related COTS boards
- dedicated architectures
 - GPU:
 - Only usage is with COTS processing boards
- Most COTS electronics used in defence systems are manufactured overseas
 - so at risk from tamper



Trusted design, manufacturing and programming of Digital processing platforms COTS

COTS IN DEFENCE: NEEDS & REQUIREMENTS

COTS IN DEFENCE : NEEDS & REQUIREMENTS



For what purpose ?

- The CDP has defined priorities actions on
 - Land and Ground combat capabilities,
 - Naval manoeuvrability,
 - Underwater control contributing to resilience at sea,
 - Air superiority,
 - Air mobility,
 - Integration
- New military Systems are demanding more digital processing performances.
 - Most demanding ones: Digitalization of the battlefield, Collaborative combat, Cybersecurity, payloads for miniaturized drones
- Moreover advanced processes and technologies are required for cryptographic components
 - Cybersecure solutions require also anti-tamper technologies, secure and trusted processors and FPGA

Military specificities

- More generally Embedded processing platforms are questioned today by 3 main challenges
 - New technologies ie connectors to improve the bandwidth and backplane high precision clocks.
 - Embedded security features and trusted solutions
 - Open architectures to ease usage in military and to reduce the cost of Defense stakeholder's total ownership where these architectures are applicable
- As an example:
 - Three main US DoD funded programs (e.g. ERI) are developing the related Open Architectures and are targeting:
 - Easy upgrade, shared development and platforms between different programs using COTS, **facilitated in-service support (ISS)**
 - **Common solutions** to Naval, Air and Army military applications
 - **Common cabinets and Electronic processing Boards for several payloads and different equipment** (Air, Land, Naval)
 - India & China are also implementing such initiatives (open source HW)
 - In Europe, several national initiatives on reliability of COTS for defence,
 - e.g. the PISTIS project launched by the French procurement agency DGA focus on the advanced technologies (DSM, FPGA, RF GaN...)

COTS IN DEFENCE: NEEDS & REQUIREMENTS



What types of COTS

- Components (actives, passives):
 - Optoelectronics: COTS are relevant for Electro Optical detectors (visible, IR...)
 - RF and Microwaves domain is not very suitable to COTS components in most cases
 - Signal & data processing (processors, memory, converters...): most of the applications use COTS
 - Development around RISC V to avoid ITAR risks with ARM
 - Power supply and energy management: COTS or dual use solutions for PSEM functions on military platforms is relevant but challenging
 - Sensors and Smart Actuating devices: Main related COTS are MEMS devices
- Boards
 - Mainly VME & VPX standards boards,
 - Board processing units used in cabinet in warship for combat management consoles
- Display Flat panel:
 - Military used COTS DFP and adapt them for the military environment
- Connectors
- ...

COTS IN DEFENCE: NEEDS & REQUIREMENTS



What types of COTS

- Specificities:
 - Environmental conditions (Temperature range, humidity, salt, HAST...),
 - Certification and standardization, interoperability, obsolescence:
 - Different approaches: Automotive, defence (MIL Std), space (ESCC...), avionic (DO) standards
 - Reliability models evolution:
 - mainly in defence and automotive with mission profile (FIDES,...), screening & burning
- Critical technology & suppliers:
 - Technology: how to be confident (long term access, reliability assessment...)
 - How to get and to assess reliability data on technologies from foreign and large volume suppliers
 - Suppliers:
 - What is a trusted supplier (what needs to be done to get this status, see US trusted foundry approach), qualification (per product, per supplier ?)
 - what about the Merging & acquisition risk of for commercial companies...),
 - what are the best practice in Europe
- Impact on our R&D activity
 - New studies to be launched ?
 - Supply chain development via R&D programs (see RF GaN and SoC approach)

CONCLUSION

What types of COTS / defence approach

- Key questions are:
 - **Which type of Which components** : Parts (like active & passive components) / sensors / boards subassemblies?
 - **For what sector (automotive, avionics, industrial, consumer, military)?**
 - **What driven applications and which OEM in Europe are concerned?**
 - The list of COTS used in military may be quite sensitive in many system capabilities and the information is to be preserved
- Defence approach of the COTS: example of France
 1. Selection of suppliers and preferred manufacturers list (with synergies in other long-term markets).
 2. Check maturity and technology risks on advanced products
 3. Reliability predictions of Electronic System: « FIDES Methodology ».
 4. Qualification at system or equipment level.
- COTS based ASSP developed for AI may not be accessible and less suitable for military needs
 - less big data driven but mainly mission profile driven for AI in military, cybersecure devices.
 - Defence actors will need to design custom military ASSP for artificial intelligence and so access at advanced deep submicron below 28 and 22nm;

RECOMMENDATIONS

What next

- Gain in maturity level (TRL & MRL)
- To develop a « matrix of COTS certification equivalences » between
 - Avionic (civil)
 - Transport (automotive)
 - Space
 - Defence
- To reinforce cooperation between EU players & EU institutions
 - Common objectives / Joint funding
 - Best practice in procurement of EEE COTS
 - REACH & RoHS (e.g. Pb-free) common issues
- Benefits:
 - Cost reduction for introducing more COTS
 - Better reliability for introduction of new technologies

RECOMMENDATIONS



What next

- Prepare and made available “Open architecture” COTS processing solutions, state of the art and covering European needs.
- Define a Protection Profile for COTS boards targeted for military applications.
- Define and develop a prototype of a secured COTS board compliant to the Protection Profile.
- Get a FLSC (First Level Security Certification) evaluation of the first prototypes of European secured COTS Boards.
 - Of course stay in line with VITA standard
- We should not forget skills & competences requested !!



THANKS YOU

TIME FOR QUESTIONS