MANNARINO®

SYSTEMS & SOFTWARE INC.

TCCA Delegates Conference

Acceptable Means of Compliance for COTS and COTS IP

November 2018

MANNARINO Systems & Software

- **Private Canadian engineering services company founded in 1999 by John Mannarino**

- **MANNARINO growth**
  - Initial years focused on essentially one customer (a FADEC/ECU OEM)
    - Projects focused on systems engineering & Level A software
  - Subsequent focus was on customer and product application diversification within the airborne & safety-critical markets
    - Level A (FADEC) experience well received by new avionics customers
    - Non-airborne product customers appreciate professionalism & rigor associated with developing flight-critical software
  - MANNARINO subsequently grew core systems & software engineering services to include:
    - Airborne Electronic Hardware (AEH)
    - Design Assurance Services

Acronyms

ECU	Engine Control Unit
FADEC	Full Authority Digital Engine Control
OEM	Original Equipment Manufacturer

MANNARINO Systems & Software

- **Engineering process definition for safety-critical industries (systems, software and programmable hardware engineering)**
  - Commercial aerospace
  - Rail industry
  - Customer experience ranging from start-ups to established OEMs

- **Aerospace certification services for software (RTCA/DO-178) & hardware (RTCA/DO-254)**
  - Authorized from Transport Canada to approve airborne software and hardware
  - Provide Design Assurance function to ensure compliance of software/hardware to certification guidelines

- **Safety-critical systems, software & electronic hardware engineering services to the aerospace, defense, space, simulation, rail and power generation industries with particular expertise in:**
  - Airborne Software (RTCA/DO-178B/C)
  - Airborne Electronic Hardware (RTCA/DO-254)
  - Real-Time Software
  - Systems Engineering (SAE ARP4754A/4761)
  - Aircraft Systems Simulation
  - Training (SAE ARP 4754A, RTCA/DO-178C, RTCA/DO-254)
  - Industrial Gas Turbine Controls Software & Simulation

Acronyms

ARP	Aerospace Recommended Practices
SAE	Society of Automotive Engineers

MANNARINO Obtains Transport Canada DAO for Airborne Software & Electronic Hardware – A first for a Canadian Service Company

MONTREAL, QUEBEC – Monday, 05 September 2016 – Mannarino Systems & Software Inc. (MANNARINO) is very proud to announce that it has been authorized as a Design Approval Organization (DAO) for Airborne Software (RTCA/DO-178) and Airborne Electronic Hardware (AEH) (RTCA/DO-254) by the National Aircraft Certification Branch of Transport Canada Civil Aviation (TCCA).

This authorization will allow MANNARINO to exercise its delegated functions in the approval process of Airborne Software and AEH products developed either by MANNARINO or any other organization. As such, the MANNARINO DAO can provide service to any aerospace OEM in support of obtaining TCCA approval for airborne software and AEH products. MANNARINO is the first service company to obtain DAO authorization for these products in Canada.

Objective

Commercial Off-The-Shelf (COTS) and COTS Intellectual Property (COTS IP) are widely used in the aerospace industry for the development of custom Airborne Electronic Hardware (AEH) programmable hardware components. The certification authorities have recently been working on a harmonized Advisory Circular (AC) 20-152A to provide a generally acceptable means of compliance for AEH development and verification, including the use of COTS IP, satisfying the industry standard RTCA/DO-254 Design Assurance Guidance for Airborne Electronic Hardware.

This presentation provides an overview of the AC content as well as a proposal of how COTS IP could be approved for a development assurance level (DAL) A program.

Digital Electronics Technology Evolution

- 1950-1960
  - The transistor and the first integrated circuits were invented
  - Inital densities of 1 to 50 transistors
- 1980 - 1990
  - PLDs and ASICs were invented
  - Massive increase in density of transistor to 100K to 500K
- 2000 – now
  - Complexity and integration increased even more
  - 20Million to 1Billion transitor density

It does not stop there

- ✓ Highly complex designs
- ✓ Complexity at every level of the Hardware Design
- ✓ Multi layered Circuit Boards
- ✓ Extensive use of COTS components

Acronyms

ASIC Application-Specific Integrated Circuit
PLD Programmable Logic Device

Definitions

Commercial Off-The-Shelf (COTS) device - device, integrated circuit or multi-chip module developed by a supplier for a wide range of customers, whose design and configuration is controlled by the supplier or an industry specification. These devices have widespread commercial use and are developed according to the semi-conductor manufacturer's proprietary development processes.

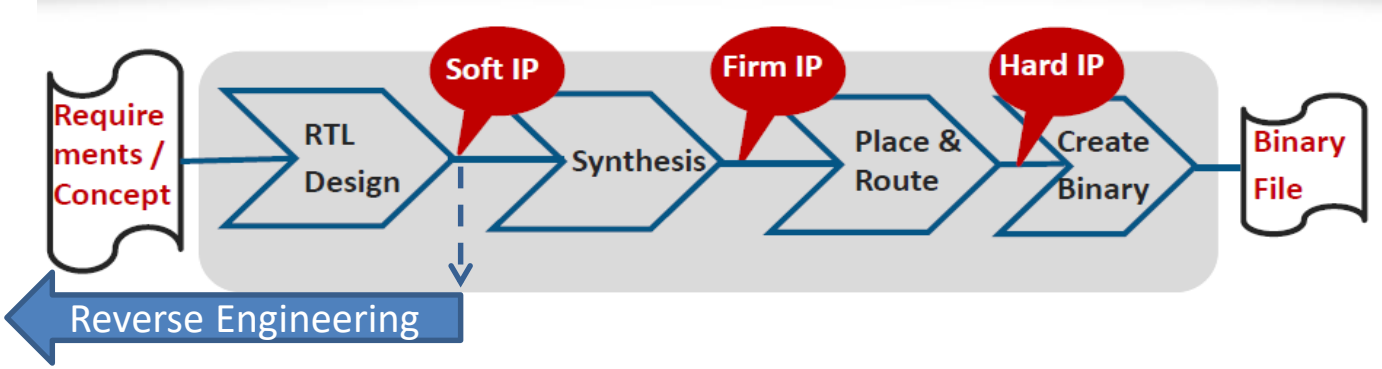
Commercial-off-the-shelf intellectual property (COTS IP) – Intellectual Property (IP) refers to design functions (design modules or functional blocks – including IP libraries) used to design and implement a part of or a complete custom device such as a PLD, FPGA, or ASIC. Intellectual Property is considered to be 'COTS IP' when it is a commercially available function, used by a number of different users, in a variety of applications and installations. COTS IP is available in various source formats:

- Soft IP
- Firm IP
- Hard IP

Acronyms

ASIC	Application-Specific Integrated Circuit
FPGA	Field Programmable Gate Array
PLD	Programmable Logic Device

Definitions (cont.)



COTS Soft IP- IP delivered at RTL level (e.g. Verilog or VHDL), provides full visibility of the detailed design allowing reverse engineering and optimization of the design.

COTS Firm IP – IP delivered after synthesis (e.g. gate level netlist – pre-layout), critical IP detailed design is a "black box", optimization can be done during place &route

COTS Hard IP – IP delivered in a layout format (post place & route), no access to detailed design, no optimization or internal analysis possible. The COTS Hard IP are integrated in the FPGA/ASIC, therefore it is treated as a COTS component within a device.

Acronyms

RTL Register Transfer Level

VHDL VHSIC (Very High Speed Integrated Circuit) Hardware Description Language

Airborne Electronic Hardware (AEH) Means of Compliance Evolution

- RTCA/DO254- was published in April 2000, providing guidance for the design assurance of:
  - Line Replaceable Units (LRU)
  - Circuit Board Assemblies (CBA)
  - Custom Micro-Coded Components (CMCC), such as ASICs, FPGAs, PLDs
  - Very limited aspects of Commercial-Off-The-Shelf (COTS) components (section 11.2)

- DO-254 was formally recognized by the FAA in June 2005 (AC 20-152), limiting the scope to programmable devices of DAL A, B &C with very little clarifications

- In 2011 EASA and TCCA imposed DO-254 DAL D for CBA & programmable devices through generic and/or program specific Certification Review Items (CRI) and TCCA Certification Memos (CM). The FAA did not impose this certification requirements...

- At the same time, additional clarifications were provided on the Acceptable Means of Complaince for COTS and COTS IP through CRI and CM, but still program specific

Acronyms
CRI Certification Review Item

Airborne Electronic Hardware (AEH) Means of Compliance Evolution (cont.)

- In 2014, seeking harmonization the Certification Authorities got together and published a Position Paper CAST-33 *"Compliance to RTCA DO-254/ EUROCAE ED-80, "Design Assurance Guidance for Airborne Electronic Hardware", for COTS Intellectual Property Used in Programmable Logic Devices and Application Specific Integrated Circuits"*

- In 2018 EASA, the FAA and TCCA jointly proposed a Notice of Proposed Amendment (NPA) by creating the new DRAFT AC 20-152A and with the aim of:
  - Increasing harmonization between Certification Authorities
  - Providing clarification for the means of compliance for AEH in general and COTS IP

- EASA, FAA and TCCA jointly proposed a Notice of Proposed Amendment (NPA) by creating the new draft of the AC 20-152A:
  - Replace program specific CM/IP with AC
  - Planned to be published by Q2 2019

Acronyms

CAST	Certification Authorities Software Team

AC 20-152A General Aspects

AC is objective driven and it covers applicability, complexity, validation, verification, COTS IP and COTS

- Applicable to devices of **DAL A, B or C**
- **Excludes certification requirements for Circuit Board Assemblies** (previously covered by EASA Certification Memorandum, imposing DO254 DAL D at board level)
- Clearly defines criteria to be used to determine device classification as **Simple or Complex**
- Same as before, **DO254 process is not mandatory for Simple devices**
- **More clarity on the verification aspects of the devices**
  - Verification coverage analysis and verification of the implementation, including simple devices
  - Post-layout netlist verification may be necessary to complement the implementation verification

AC 20-152A General Aspects (cont.)

- **For DAL A, B and C all Custom Device Requirements should be validated**, not only the derived requirements as per DO254
  - DAL A and B requires independence
- **AC imposes Detailed Design Review for DAL A and DAL B**, not clearly required per DO254
- Provides clarification on the timing performance verification of the design by guiding to **Static Timing Analysis**
- **Clearly defines the need for robustness aspects of the design**
  - DAL A and B requirements should define abnormal and boundary conditions and associated expected behavior of the design

AC 20-152A General Aspects (cont.)

- **Code Coverage**
  - For DAL A and B code **coverage is used to perform Elemental Analysis**
  - Criteria ensures coverage of the HDL code elements used in the design (e.g. Branches, Conditions, etc)

- **Tool Assessment and Qualification**
  - More details about qualification and assessment criteria
  - Independence required during the tool assessment process
  - Still allows claiming credits for relevant history of the tool – data evidence should be provided

- **Clarifications on Previously Developed Hardware**
  - Pretty well known concepts about Previously Developed Components, now clearly applicable to custom devices

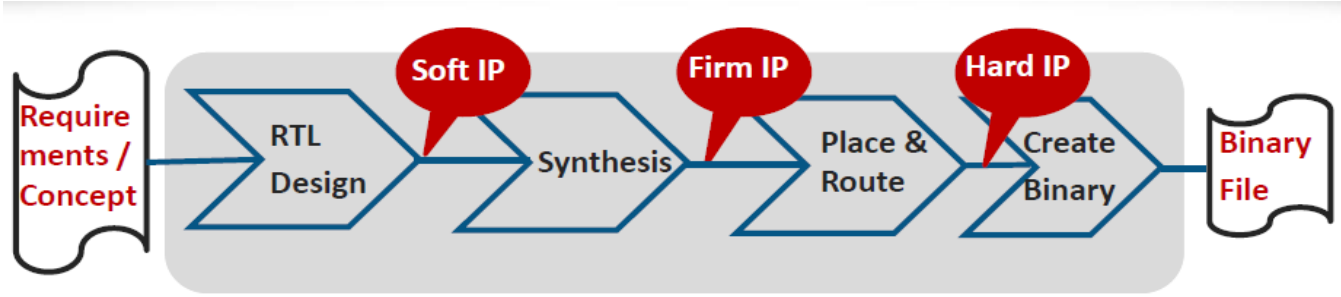
AC 20-152A COTS Aspects

- **Risks of using COTS IP**
  - Unknown behavior of the COTS IP
  - Insufficient data and verification performed by the COTS IP provider
  - Deficient quality of the COTS IP design
  - Design errors
  - Incorrect integration of the COTS IP into the custom device

- **Risks Increases even more when**
  - COTS IP provider does not have experience
  - COTS IP user does not have experience on developing and integrating those devices

- **Initial Risk Mitigation Aspects**
  - Proper selection of COTS IP and provider
  - Define proper certification strategy for the COTS components, following AC 20-152A closely is recommended
  - Coordinate Certification Authorities expectations re COTS

AC 20-152A COTS Aspects (cont.)



- **Specific Objectives for COTS IP**
  - Different types of COTS IP (Soft, Firm, Hard) will be treated differently from design assurance perspective
  - Having access to the design and code will ensure any single objective of DO254 can be achieved
  - As the design and code become inaccessible, other means shall be established to ensure functional and safety aspects of those devices

- **Hard IP**
  - Can be seen as a “black box” portion of the device component
  - Treated as COTS by the AC 20-152A

Hard COTS IP – or just "COTS" Objectives

- **COTS-1: COTS Complexity – they are Complex COTS if**
  - Multiple functional elements interacting to each other
  - Functions can be configurable
  - Other cases that will always be considered complex: Multicores, graphics processing, complex bus switching

- **COTS-2: Development Assurance**
  - Access/availability of the COTS component data: User Manual, Datasheet, Errata, Installation Manual, any other info from the component manufacturer
  - Aspects of maturity and "Component Family Lineage" can play a role

- **COTS-3: Using a COTS Outside the Range of Values**
  - Applicant will have to determine reliability and the technical suitability of the component in case the use of the component will be outside the manufacturer's specification

Hard COTS IP – or just "COTS" Objectives (cont.)

- **COTS-4: Embedded Microcode**
  - If Microcode is modified by the COTS user it shall have verification strategy defined for the proposed changes
- **COTS-5 & COTS-6: Device Malfunction**
  - Access errata for relevant service experience and know issues
  - Define mitigation means for issues that may cause COTS limitations, incompatibility or errors
  - Identify the failure modes associated the functions being used (i.e.: System Safety Assessment Process should cover the COTS components failure modes)
- **COTS-7: COTS Device Usage**
  - Device usage should be defined and verified, including HW-SW interfaces tests
  - Evidence that unused COTS device functions won't affect the overall device functionality

Microcode: Hardware-level set of instructions – defines sequences of circuit-level operations example: a BIOS that initializes a microprocessor I/O operations

Hard COTS IP – or just “COTS” Objectives (cont.)

- **COTS-8: COTS Device Usage**
  - For DAL A and B COTS, user should develop and verify means to mitigate inadvertent alteration of the “Critical configuration Settings” of the device

Critical configuration settings – Those configuration settings that the applicant has determined to be necessary for the proper usage of the hardware, which, if inadvertently altered, could change the behavior of the COTS device, causing it to no longer fulfill its intended critical function

Conclusions

- Advisory Circular AC 20-152A reflects the harmonized position amongst Certification Authorities
- There is no indication that RTCA/DO254 will be revised any time soon
- Establishing agreement on the certification aspects to COTS devices and components is crucial
- Definition of Means of Compliance for new applications containing COTS may be addressed through Coordination Memorandum with TCCA

CONTACT US

Mannarino Systems & Software Inc.

100 Alexis-Nihon Boulevard
Suite 650
Saint-Laurent, Quebec
Canada, H4M 2P2

Tel: (514) 381-1360
Fax: (514) 381-7511
www.mss.ca

Amanda Melles

Chief of Airworthiness

SW/AEH Delegate

Tel: (514) 679-3644

amanda.melles@mss.ca