Addressing Safety-Critical Applications with COTS Modules
Context
What are the avionic market needs today?
- Increasing number of Safety-Critical applications
- Different functional needs
  - Flight control
  - Display
  - Actuation
- Cost / Time pressure
- Risk averse
- SWaP constraints
- Life cycle (long term investment)
- Increasing development of UAS
There is a need for a fast, reliable and cost-effective path to develop safety-critical solutions.
How?

How do we address this need?
By Bringing Safety Into the COTS World

**Availability off-the-shelf**

_saves time, saves cost, decreases risk_

- Safety-Certifiable COTS SRU modules
- DAL-C as a baseline
- Reuse certification artifacts
By Adopting a Top Down Approach

**Integrated building blocks**
saves time, saves cost, decreases risk

- Designed to work together up to the system-level (LRU)
- One set of boards, multiple applications
By Relying on Proven Track Record

Building on service history

*saves time, saves cost, decreases risk*

- Reuse proof of certifiability from previous experience
By Planning a Path for Technology Insertion

**Take into account life cycle**

* saves time, saves cost, decreases risk

- Design for safety technology insertion
- Reduce amount of work to re-certify at next step
Recipe for success
What are the key ingredients to succeed in this exercise?
Only one

Safety by Design

“Safety must be built in from the start”
Safety must be built in from the start

For example

- Deterministic behavior
- Careful component selection
- Fault tree analysis
- Fault detection
- Detection of hazardous misleading information
- Etc.
Data Requirement List (DRLs)

**Safety must be built in from the start**

- Requirements capture (know-how)
- Requirements traceability
- Build evidences along with hardware and software
- Qualified tools (tools must be certified as well)
- Company quality management system
What’s next?
On going developments
What’s Next

- Path to COTS DAL B foreseen

- Multicore processor and safety-certification (follow conference MCFA, CTIC, industry leaders,...)

- Endorse and support open architecture such as FACE consortium
A successful recipe to save time, save cost and reduce risk in safety critical avionics projects involves:

- **SRU** : A set of off-the-shelf available HW/SW Safety-Certifiable COTS SRU module
- **LRU** : A system-level solutions leveraging the Safety-Certifiable SRUs
- **Safety by design** : A design where all aspects of safety has been considered right from the beginning
Thank You

More info: www.CES-SWaP.com/safety-certifiable

Brought to you by

Creative Electronic Systems
Martin Weymann
CTO
+41 22 884 51 22
Martin.weymann@CES-SWaP.com