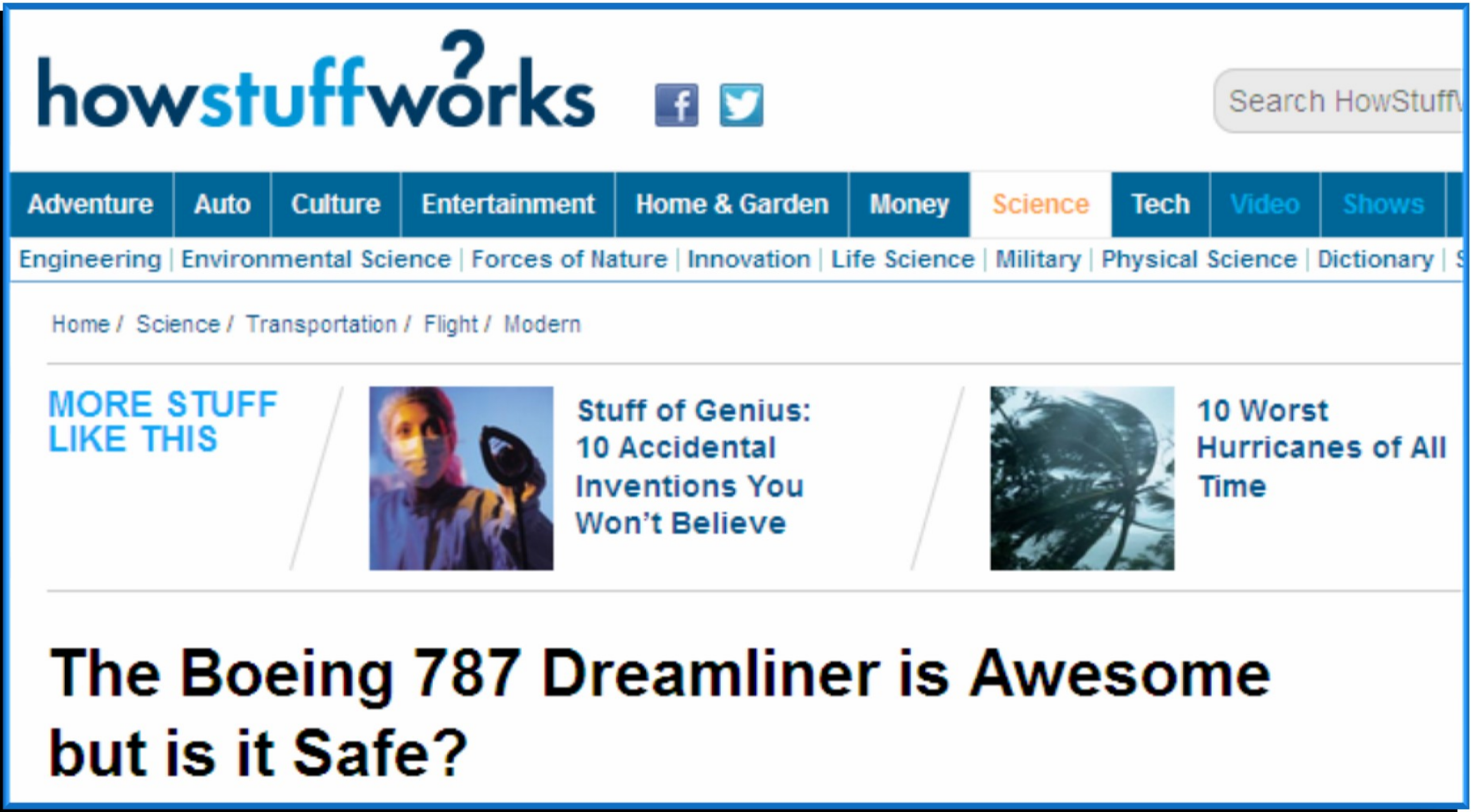
AUTOSAR & Functional Safety

John Favaro
Intecs

Jochen Olig
Elektrobit

Mixed Criticality

Unsafe Airplanes?



howstuffworks
Search HowStuffW
Adventure
Auto
Culture
Entertainment
Home & Garden
Money
Science
Tech
Video
Shows
Engineering | Environmental Science | Forces of Nature | Innovation | Life Science | Military | Physical Science | Dictionary | S
Home / Science / Transportation / Flight / Modern

MORE STUFF LIKE THIS

Stuff of Genius: 10 Accidental Inventions You Won't Believe

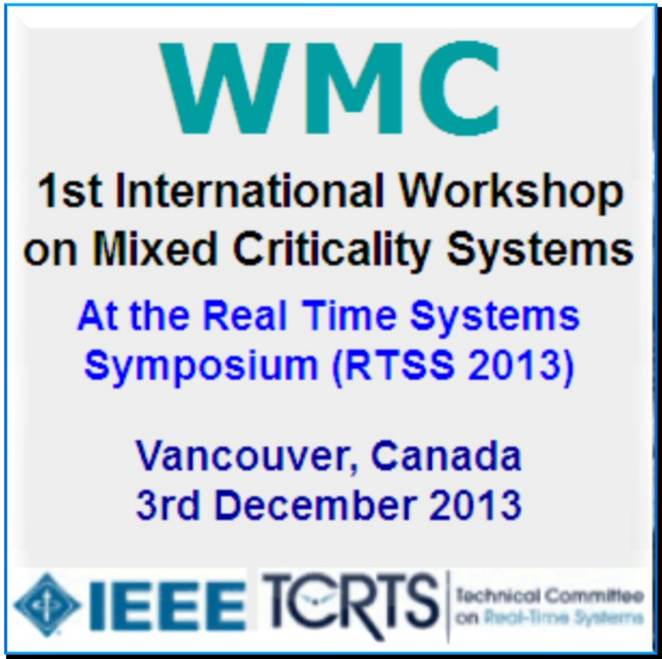
10 Worst Hurricanes of All Time

The Boeing 787 Dreamliner is Awesome but is it Safe?

Strange Bedfellows

- Are modern airplanes safe? Much controversy
- One reason: modern onboard flight systems include
  - Extremely **critical functions** (e.g. flight control)
  - Extremely **non-critical** functions (e.g. movies)
- This is **mixed criticality**

A Hot Topic Around the World



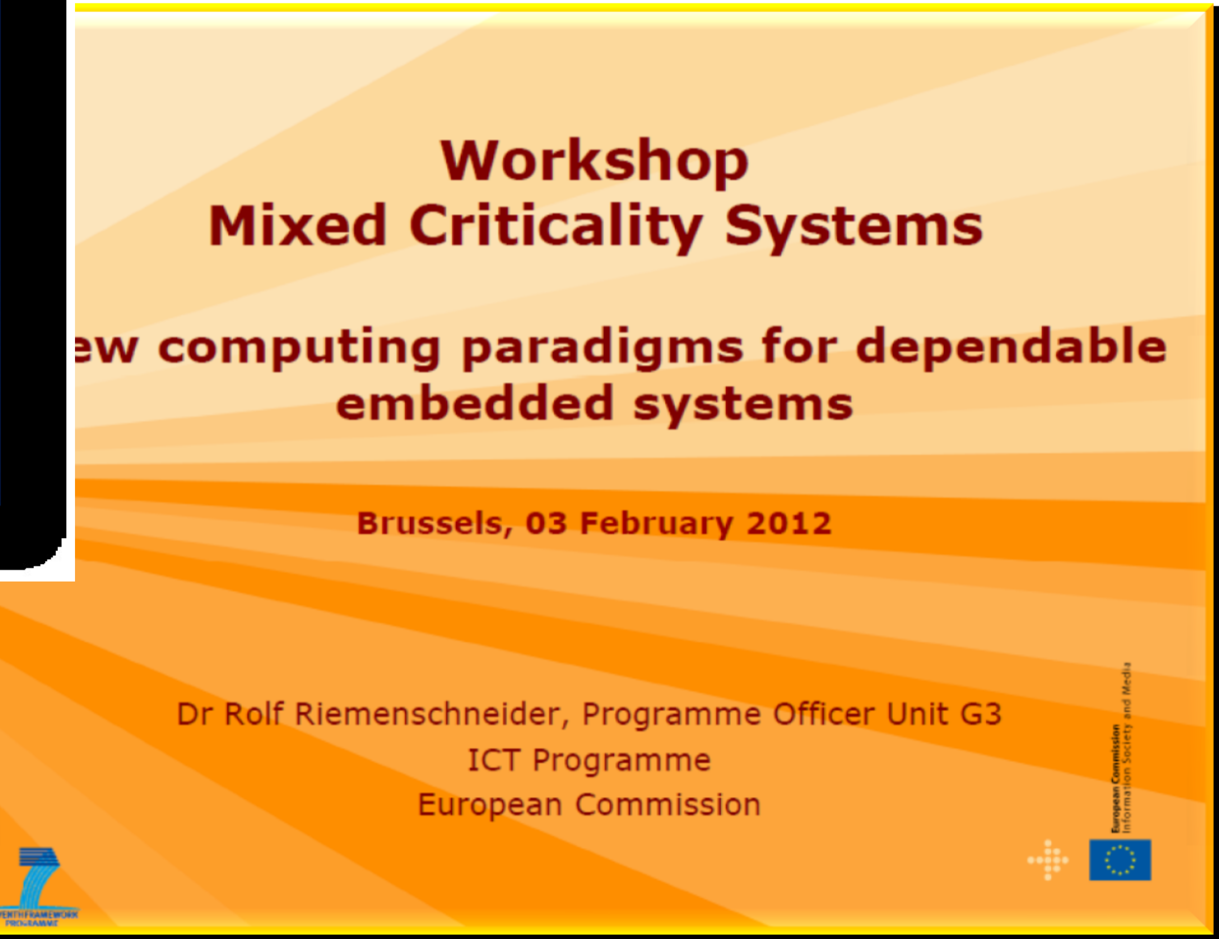
WMC

1st International Workshop on Mixed Criticality Systems

At the Real Time Systems Symposium (RTSS 2013)

Vancouver, Canada
3rd December 2013

IEEE TCRTS Technical Committee on Real-Time Systems



Workshop
Mixed Criticality Systems

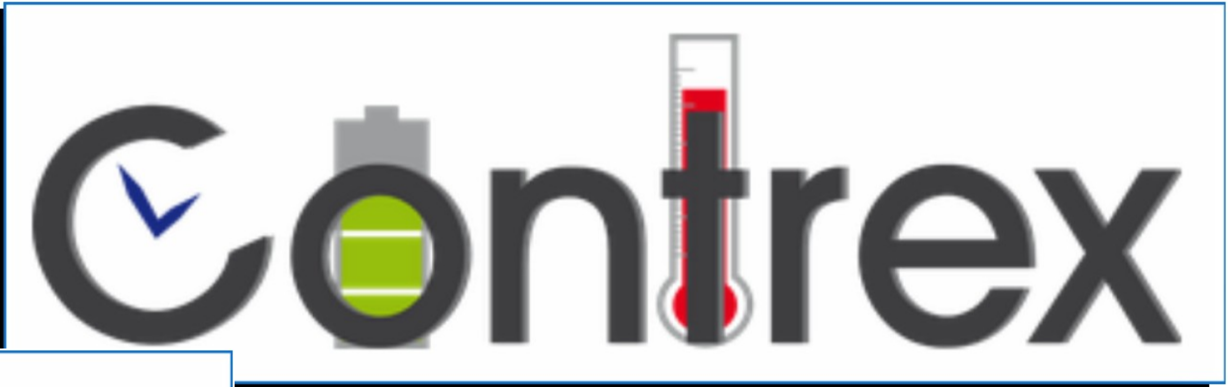
ew computing paradigms for dependable embedded systems

Brussels, 03 February 2012

Dr Rolf Riemenschneider, Programme Officer Unit G3
ICT Programme
European Commission

SEVENTH FRAMEWORK PROGRAMME
European Commission
Information Society and Media

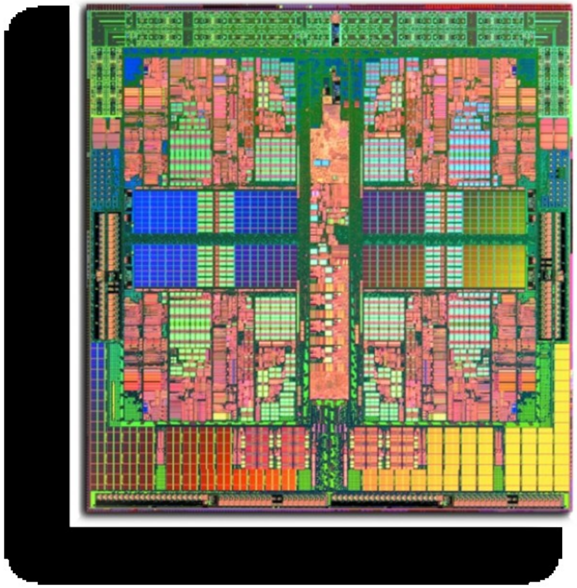
EU Mixed Criticality Projects



Why the Trend?

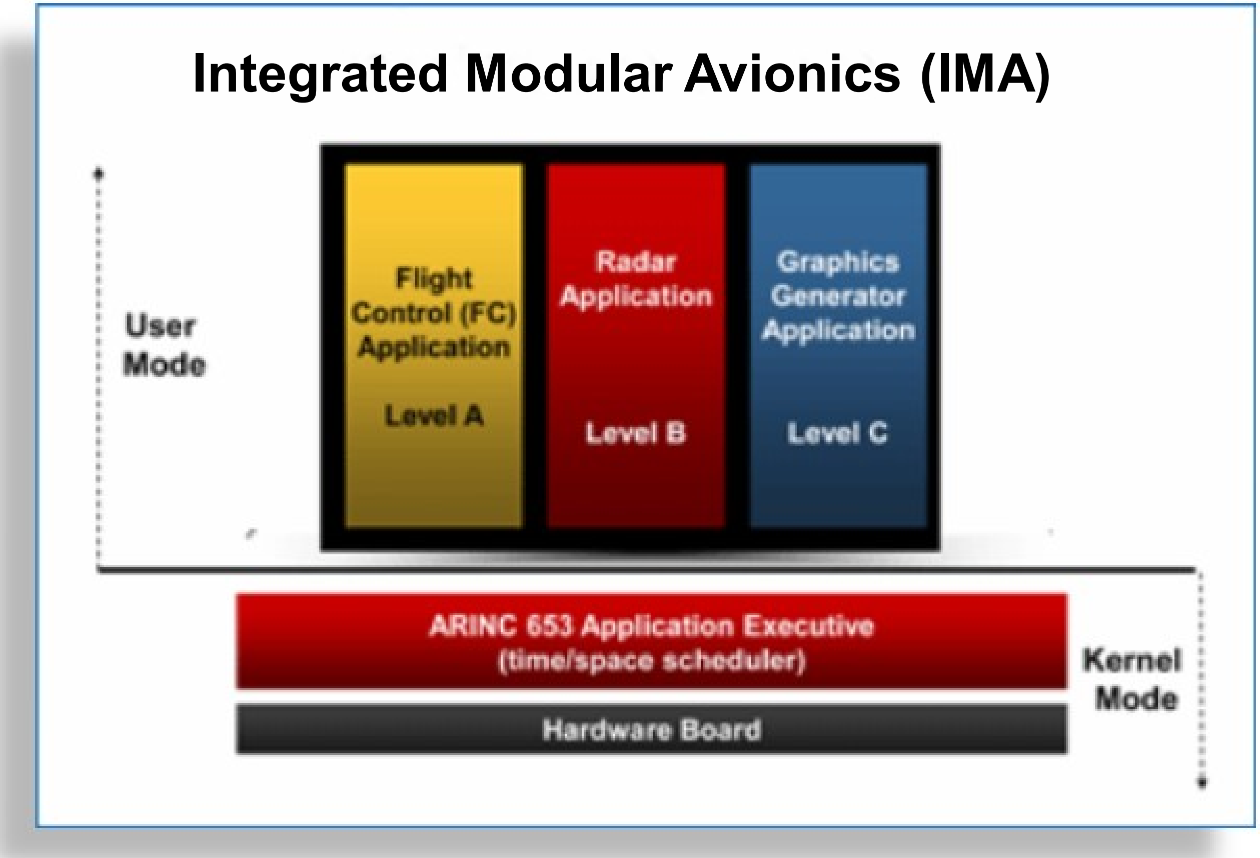
"Because we can"

Modern multicore processors have the power to support an incredible amount of functionality



Lightweight, power efficient, space saving, …

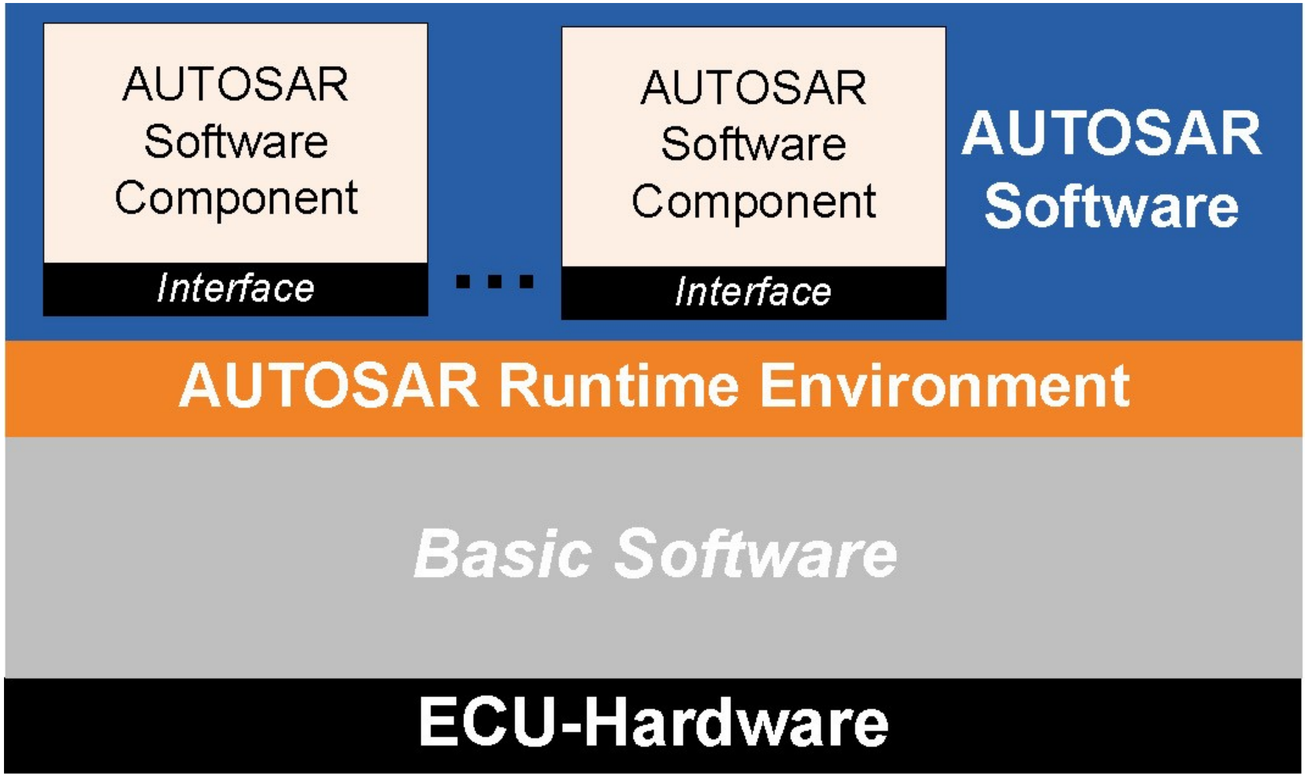
Integrated Architectures


Integrated Modular Avionics (IMA)
User Mode
Flight Control (FC) Application
Level A
Radar Application
Level B
Graphics Generator Application
Level C
ARINC 653 Application Executive (time/space scheduler)
Hardware Board
Kernel Mode

Modern integrated architectures make it possible to host all of the system functionality on a single platform

AUTOSAR

AUTOSAR enables integration of all kinds of functionality, from applications to basic software, on the same platform


AUTOSAR Software Component
Interface
...
AUTOSAR Software Component
Interface
AUTOSAR Software
AUTOSAR Runtime Environment
Basic Software
ECU-Hardware

(Uni Potsdam)

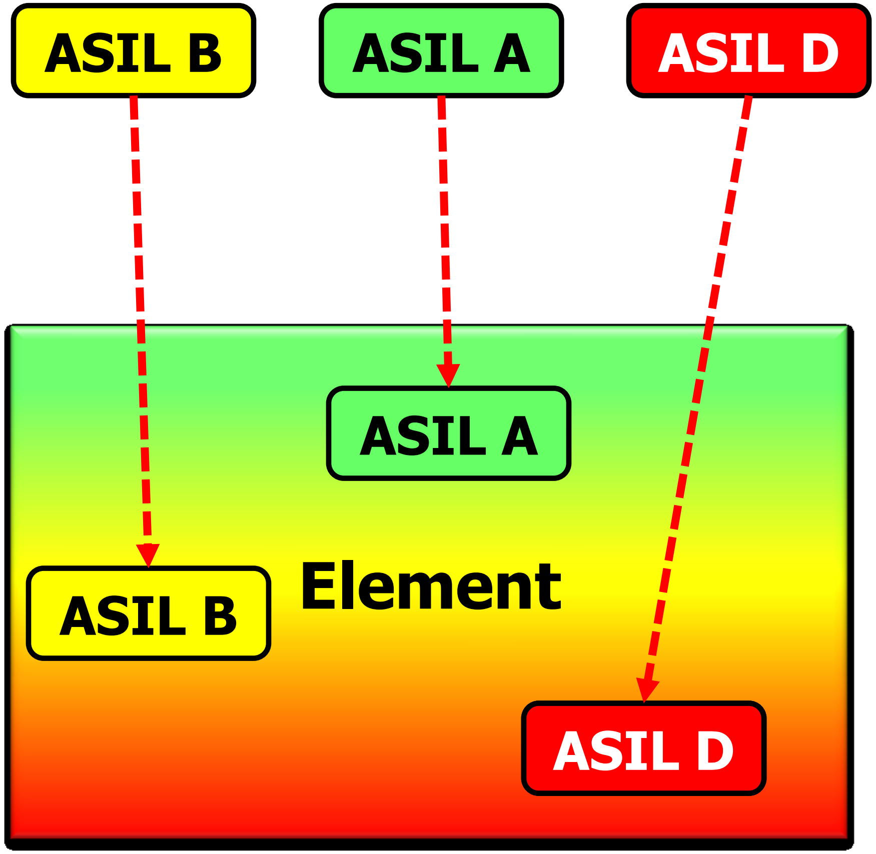
Functional Safety

and

Mixed Criticality

Functional Safety = ISO 26262

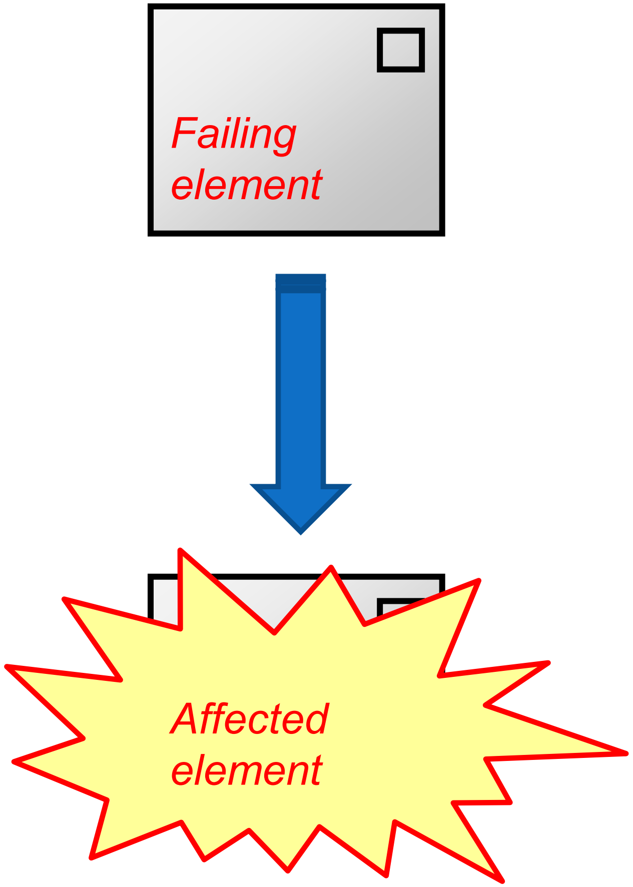
- What does ISO 26262 say about mixed criticality?
- Part 9, Clause 6 describes the **Criteria for Coexistence of Elements**



Freedom From Interference

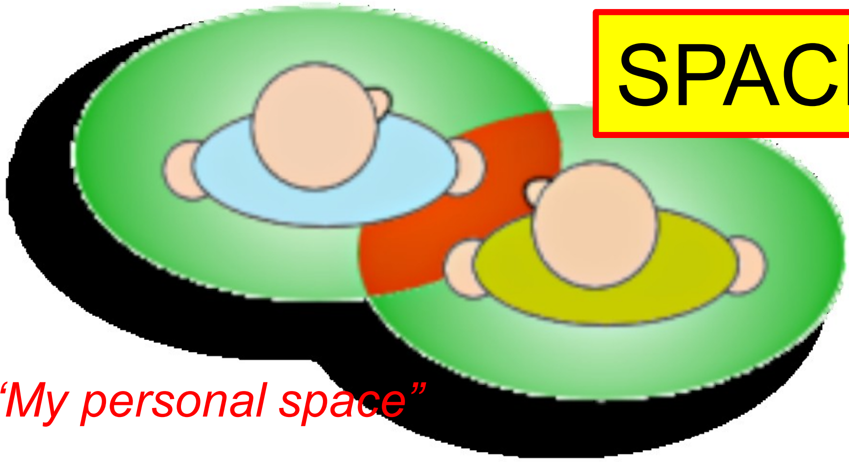
- The key to mixed criticality software in ISO 26262 is to demonstrate **freedom from interference**

- Freedom from interference means that a software element is unable to make another software element fail through erroneous behavior



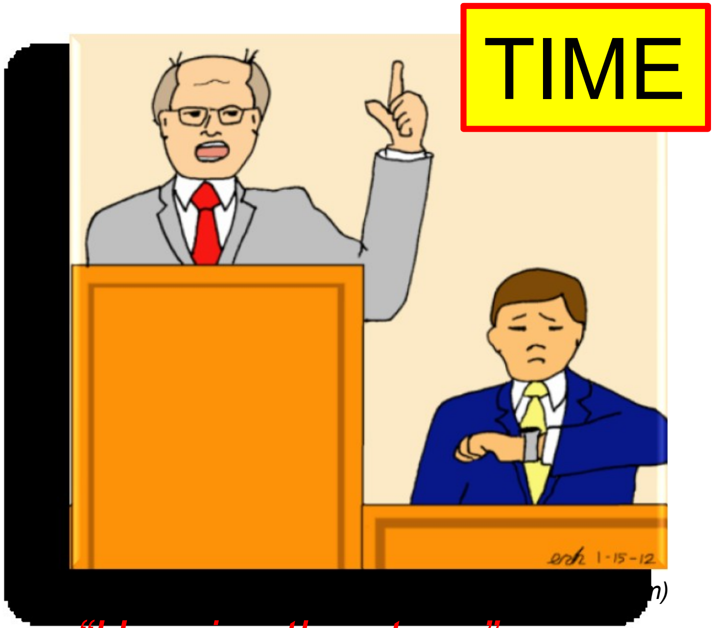
Kinds of Software Interference

SPACE



"My personal space"

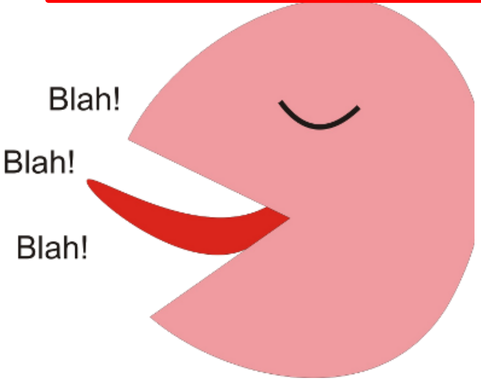
TIME



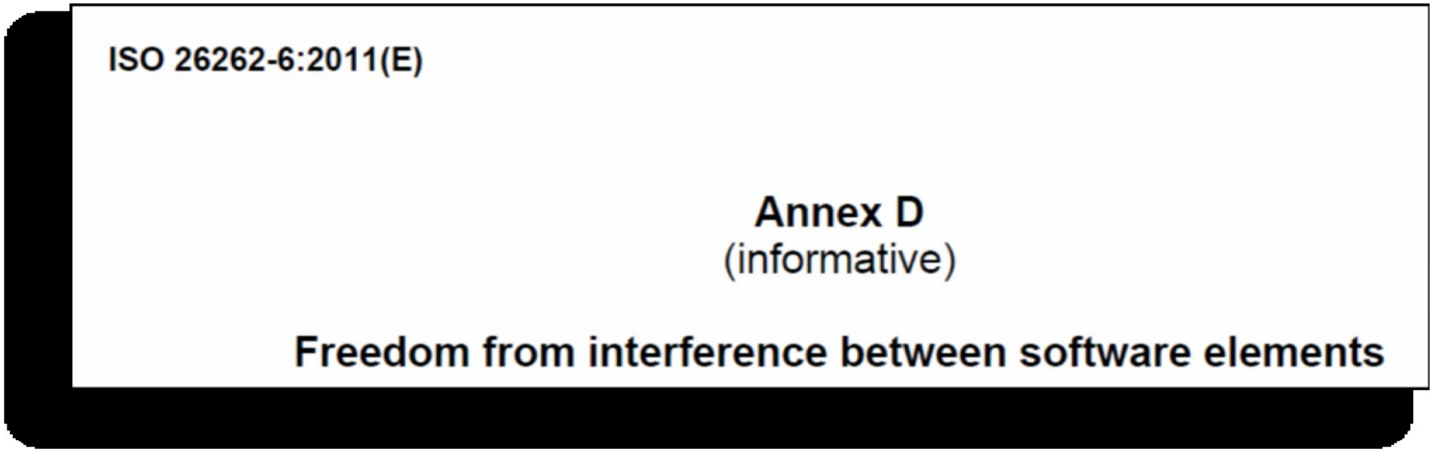
n)

"Hogging the stage"

COMMUNICATION



"Babbling idiot"



ISO 26262-6:2011(E)

Annex D
(informative)

Freedom from interference between software elements

“Do-It-Yourself”?

- Why not just “do it yours
  - Construct your applicatio
    “very carefully”
- Unrealistic! Broken softw
  cannot “heal itself”
  - Too many unknown ways
  - Too many *unk-unks*
- The only realistic path is
  platform-level support
  - ISO 26262 agrees

No “do-it-yourself”