Session 3

Dependability challenges for airborne vehicles

(Chair: Andrea Bondavalli)

"On the Security and Safety of Collaborative Intelligent Vehicles" or "An explosion of problems"

Roberto Gallo, Unicamp, Kryptus - Brazil

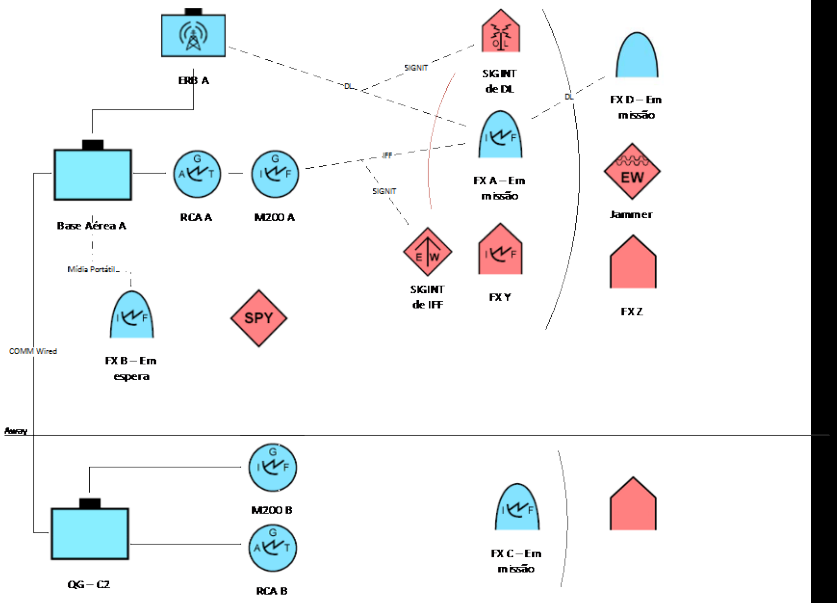
Fly me to the moon ….

Michael Hinchey, Lero - Ireland

ROBERTO GALLO

Roberto started describing a few sophisticated threats

- Eaversdroppig of Keyboard
- Fake GPS
- Change Microcircuits
- Vulnerabilities of VxWorks



And then Battlefield scenarios for drones UAVs

1. IFF (identification foe or friend)
2. Netcentric warfare system
3. Drone cyber security

FORTUNA FRAMEWORK

From observations .....some of which controversial

- **“The security of systems has a probabilistic nature (not the attacks);“**
- **(questions and discussion on the extent of probabilities in such security scenarios)**
-

And from derived Properties…….

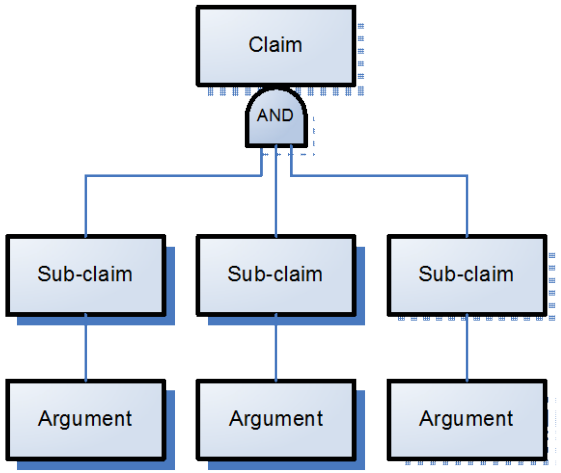
MODELS & ASSURANCE CASES

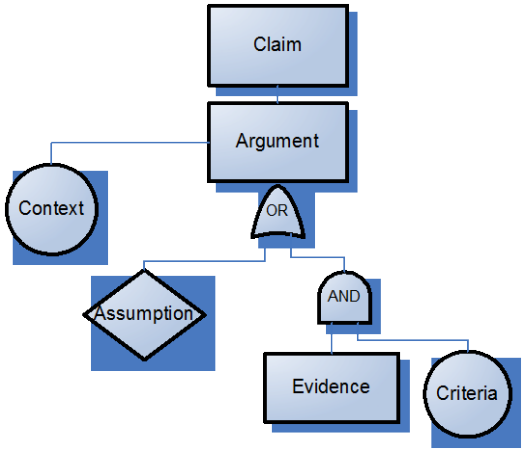
build models (three models):

- Two are graph-based:
  - Model 1: Bit leakage
  - Model 2: Adversary path
- One based on Decision Theoretic Probabilistic ProLog – DTProbLog

Resulting in policies

And Assurance cases





QUESTIONS AND DISCUSSION

Probabilistic nature of the models

Where probabilities are appropriate for capturing reality and where deterministic behaviors apply.

Mohamed, Bill, John, Andrea....

MIKE HINCHEY

Mike started from the big-bang....

..... EDSAC and the Differencial machine

To get to challenges on Sofware engineering

(besises usual increase of complexity and functionalities

Performance and reaction times... Productivity and costs

He pointed out at

regular changes and evolving systems

EVOLVING CRITICAL SYSTEMS

LERO ECS Research Agenda: to build software that

(a) is highly reliable, and

(b) retains this reliability as it evolves, *without* incurring prohibitive costs.

Key Focus Areas

- **A: Methods & Standards for High Integrity Systems**
- **B: Adaptive & Autonomous Systems**
- **C: Software Performance**
- **D: Security & Privacy**

SPACE EXPLORATION

Complex and **expensive** software applications.

High Levels of **Autonomy**.

Significant consequences for failure. → **Critical**

Swarm Technologies….

Three concept sub-missions:

Lander Amorphous Rover Antenna (LARA)
Saturn Autonomous Ring Array (SARA)
Prospecting Asteroid Mission (PAM)

ECS Contributions in:

Formal Methods

Autonomic Computing

Software Product Lines

Automatic Code Generation

Mike described several lines of contribution, including automatic code 'derivation' for evolution

QUESTIONS AND DISCUSSION

Hiro: Autonomic vs. Autonomous

Elias: Dynamic code generation

Eliane: Continuous testing on the generated code and related issues...