Safety Critical Interactive Computing Systems' Modelling

MFES Integrated Project Proposal

José Creissac Campos[1] and Miriam Alves[2]

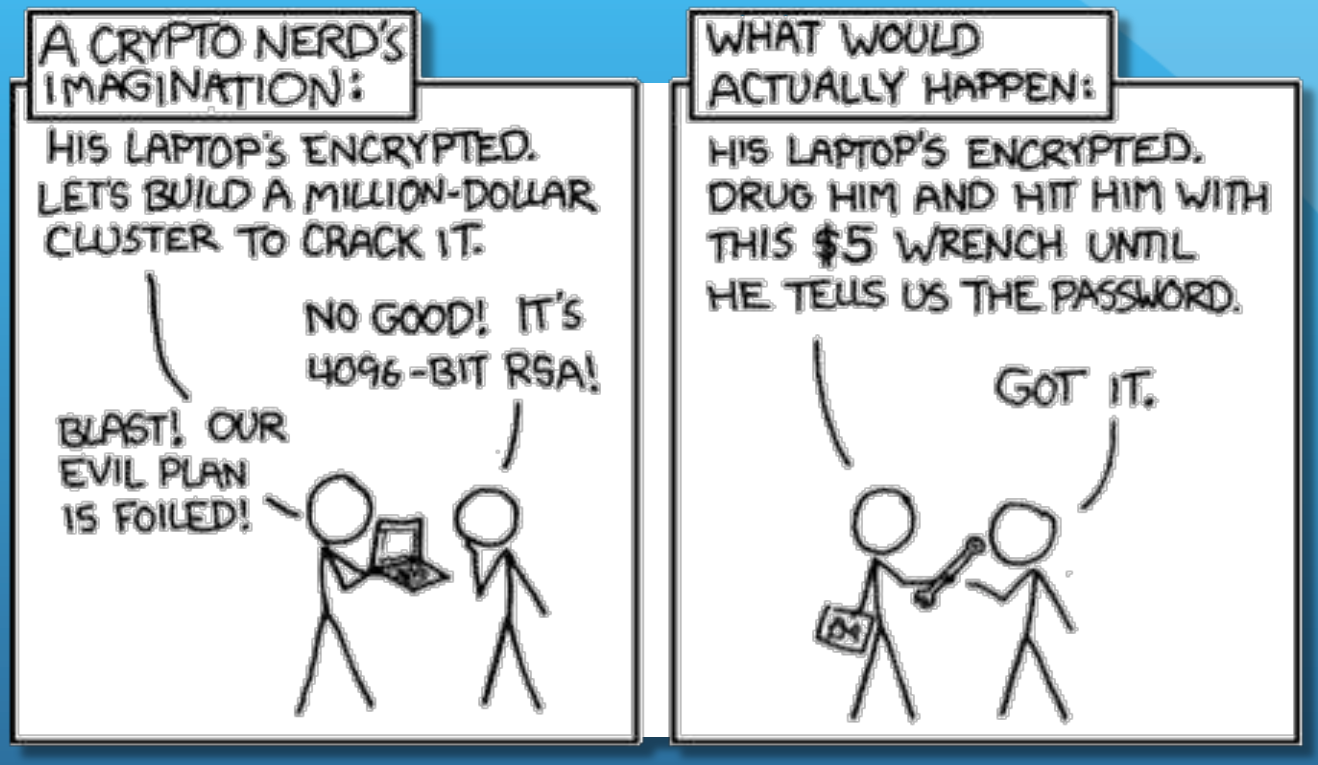
[1]*Dept. de Informática/Universidade do Minho and HASLab/INESC TEC*

Braga, Portugal

[2]*Instituto de Aeronáutica e Espaço*

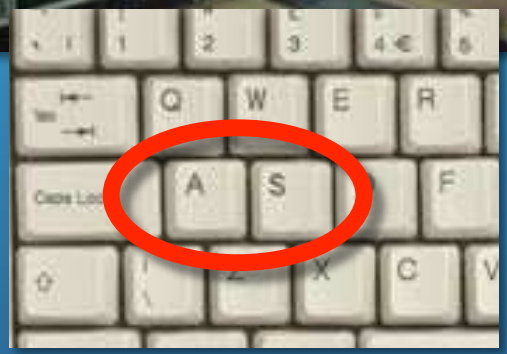
São José dos Campos, Brasil

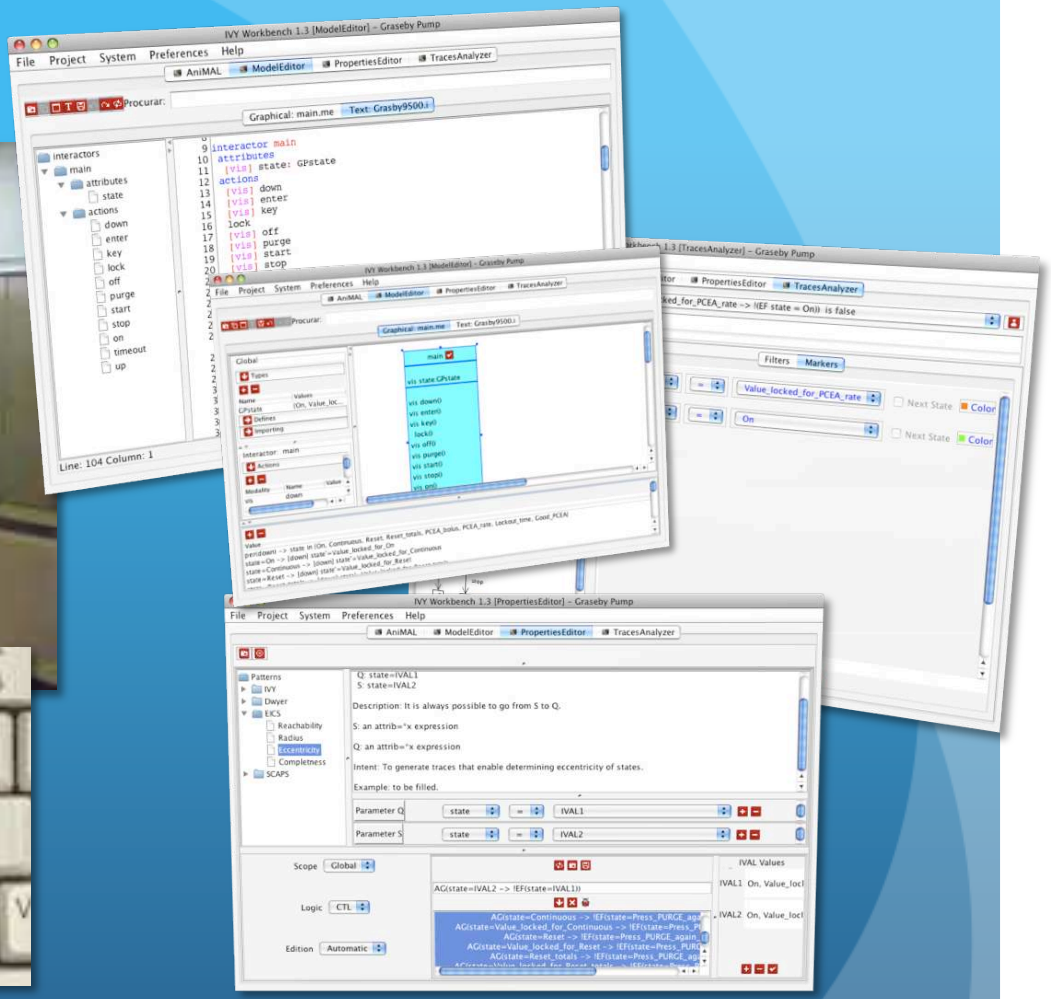
Motivation



- Impact of technology
  - hard to predict
- *Humans* a decisive factor
- Traditional UCD techniques
  - no safety guarantees
- Need for systematic and exhaustive analysis

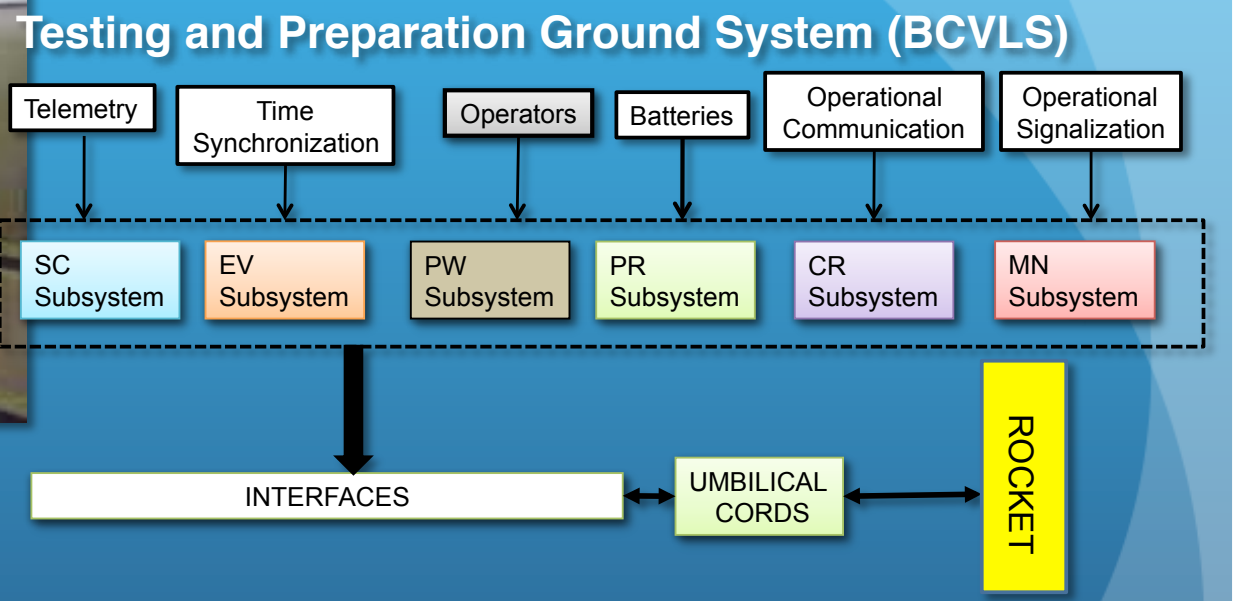
Context





- IAE
  - Develops and operates Brazilian's satellite launchers
- HASLab
  - Model-based tools for exhaustive analysis of interactive systems

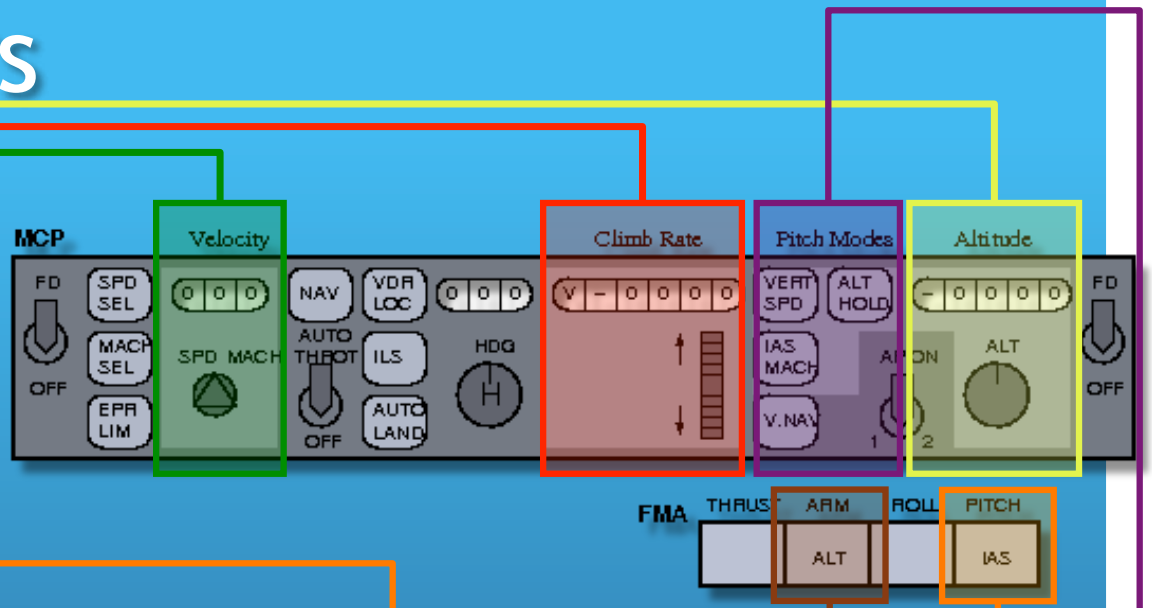
Context



- IAE
  - Subcontracting new version of BCVLS
- Can IVY support acceptance testing?

- HASLab
  - Partial models of two subsystems developed (MSc)
  - Model checking: problems with scalability

MAL interactors




```
interactor MCP
    aggregates
     dial(Altitude) via ALTDial
     dial(ClimbRate) via crDial
     dial(Velocity) via asDial
    attributes
     [vis] pitchMode: PitchModes
     [vis] ALT: boolean
   actions
     [vis] enterVS enterIAS enterAH toggleALT
     enterAC
   axioms
     [asDial.set(t)] effect(enterIAS)
     [crDial.set(t)] effect(enterVS)
     [ALTDial.set(t)] ensure_ALT_is_set
     [enterVS] pitchMode'=VERT_SPD & ALT'=ALT
     [enterIAS] pitchMode'=IAS & ALT'=ALT
     [enterAH] pitchMode'=ALT_HLD & ALT'=ALT
     [toggleALT] pitchMode'=pitchMode & ALT'=!ALT
     [enterAC] pitchMode'=ALT_CAP & !ALT'
```

Behaviour (MAL)

Goals

- Study the scalability of the models
  - How detailed can the models be?
  - Which abstractions to use?
- How best to configure NuSMV?
- Include timing considerations in the model
  - Explicit time vs. *logical* time
- 24GB quad core PC (Intel i7 960) available

Questions?

- jose.campos@di.uminho.pt

Integration of Theorem Proving in the IVY workbench

MFES Integrated Project Proposal

José Creissac Campos[1] Michael Harrison[2] & Paolo Masci[2]

[1]*Dept. de Informática/Universidade do Minho and HASLab/INESC TEC*

Braga, Portugal

[2]*Queen Mary, University of London*

London, UK

HASLab INESCTEC

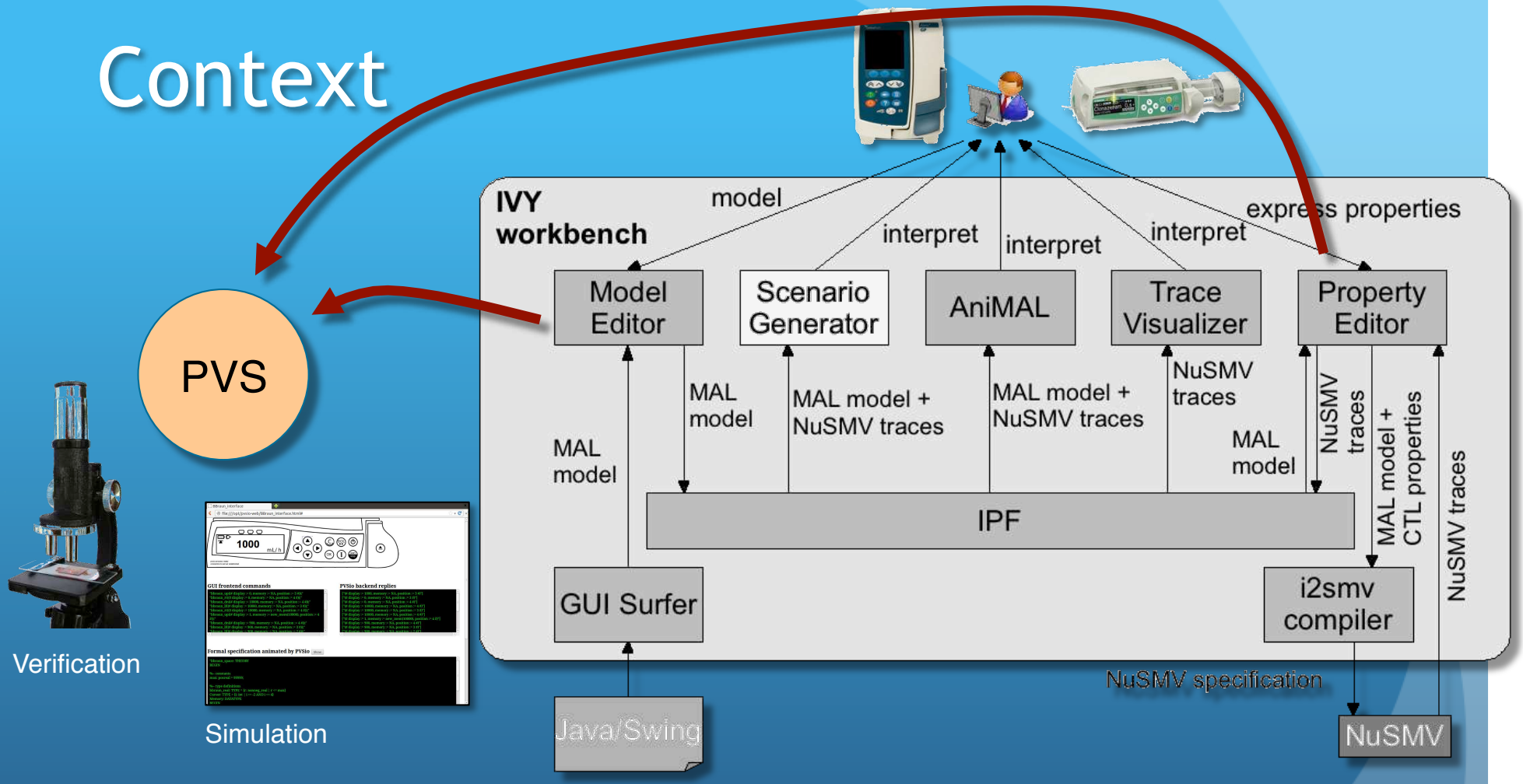
chi+med
making medical devices safer

Context

- Inquires into accidents and incidents
  - *Human error* a typical outcome
- Which human?
  - the user?
  - the designer?

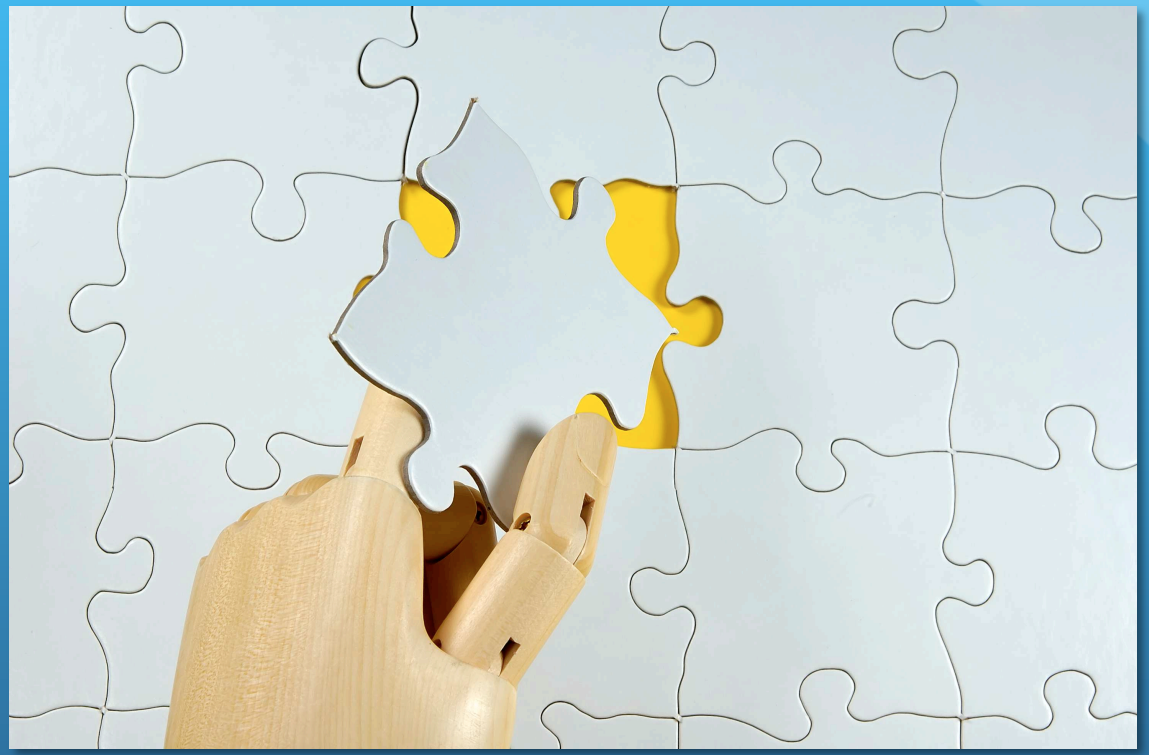
(Leveson)

Context



- There are limits to what can be done with model checking
  - e.g. number entry
- In some cases theorem proving can be more appropriate
  - being explored at QMUL

Goals



- Develop a PVS plugin for IVY
  - Preliminary work done at QMUL
  - Translate the models
  - Translate the properties
  - Identify relevant strategies
- Develop a PVS plugin for IVY
  - Integrate tool?
- In cooperation with
  - QMUL
  - second year MSc student

Questions?

- jose.campos@di.uminho.pt

Formalization of the ECSS-E-70-41A standard

MFES Integrated Project Proposal

José Creissac Campos[1] José Machado[2] & Emilia Vilanni[3]

[1]*Dept. de Informática/Universidade do Minho and HASLab/INESC TEC*

Braga, Portugal

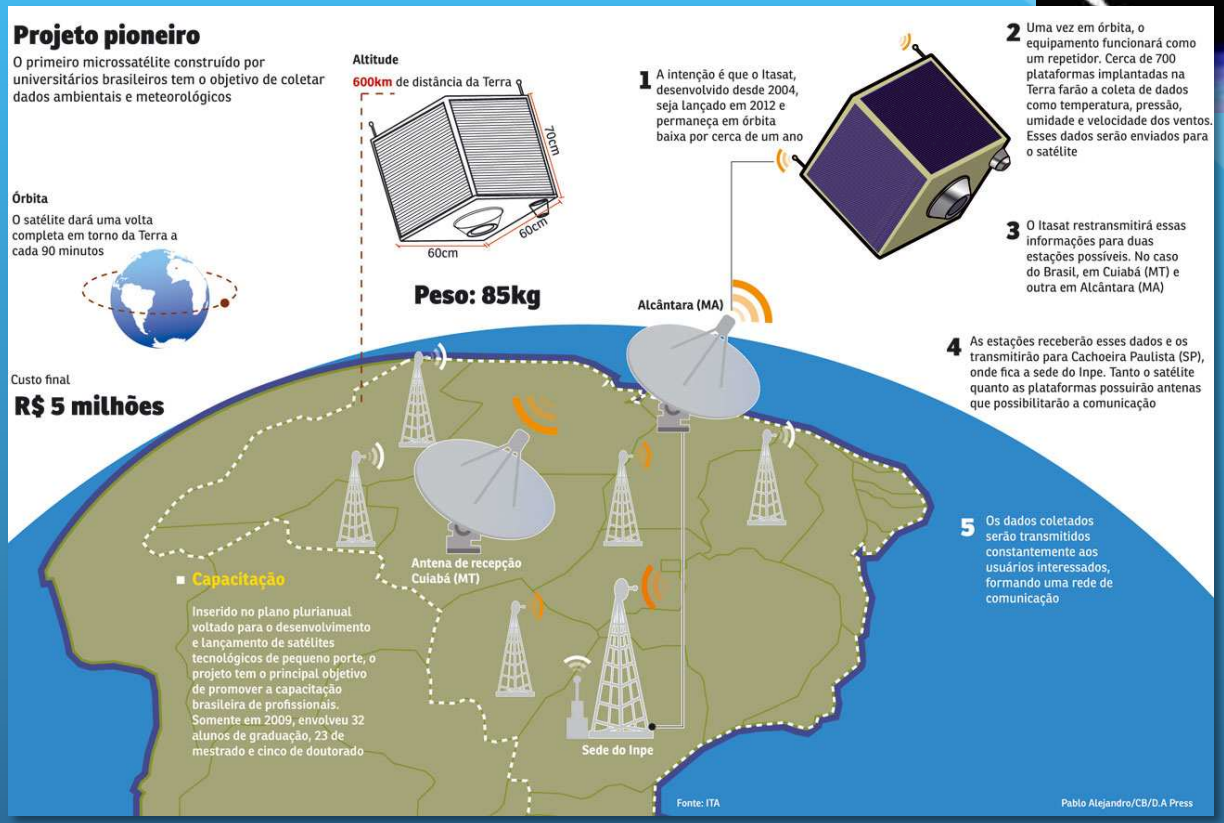
[2]*Departamento de Engenharia Mecânica/Universidade do Minho and CT2M*

Guimarães, Portugal

[3]*Instituto Tecnológico de Aeronáutica*

São José dos Campos, Brasil

Context / Goals



- Model de ECSS-E-70-41A standard in Uppall
  - Compare with ITA model