

Safety Critical Interactive Computing Systems' Modelling

MFES Integrated Project Proposal

José Creissac Campos¹ and Miriam Alves²

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

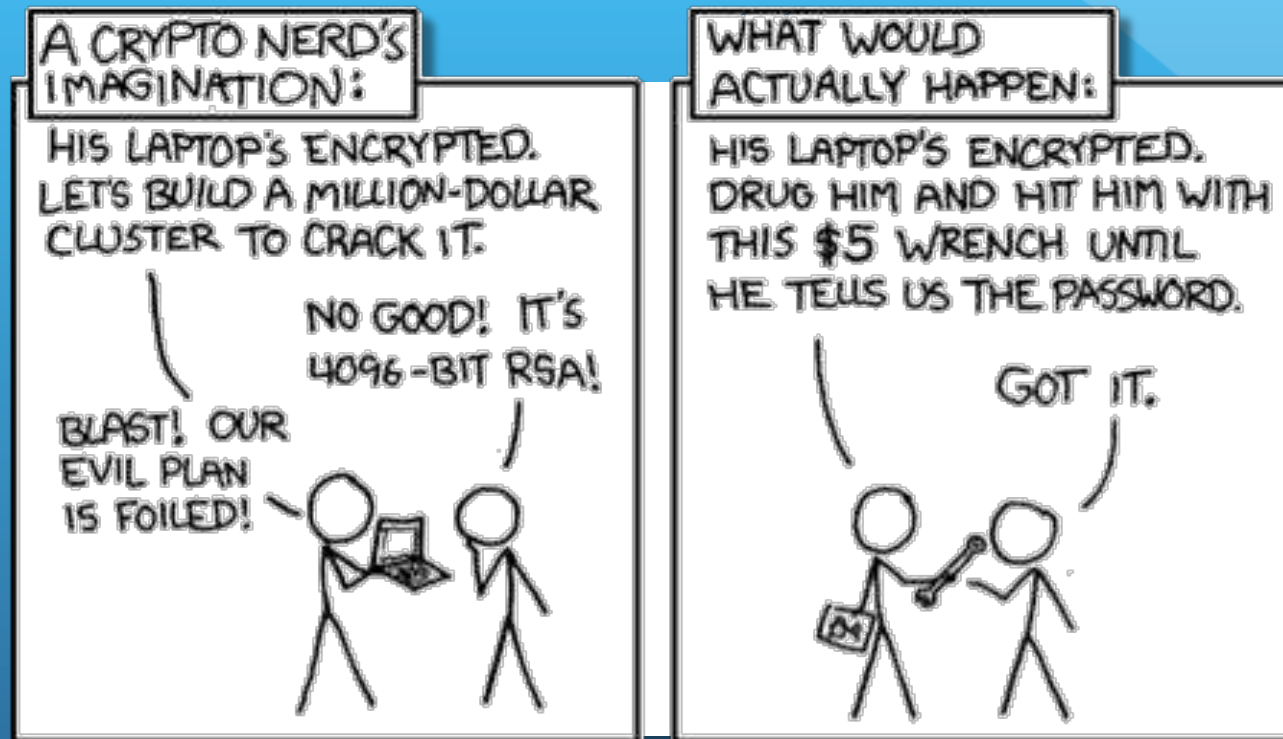
Braga, Portugal

²Instituto de Aeronáutica e Espaço

São José dos Campos, Brasil

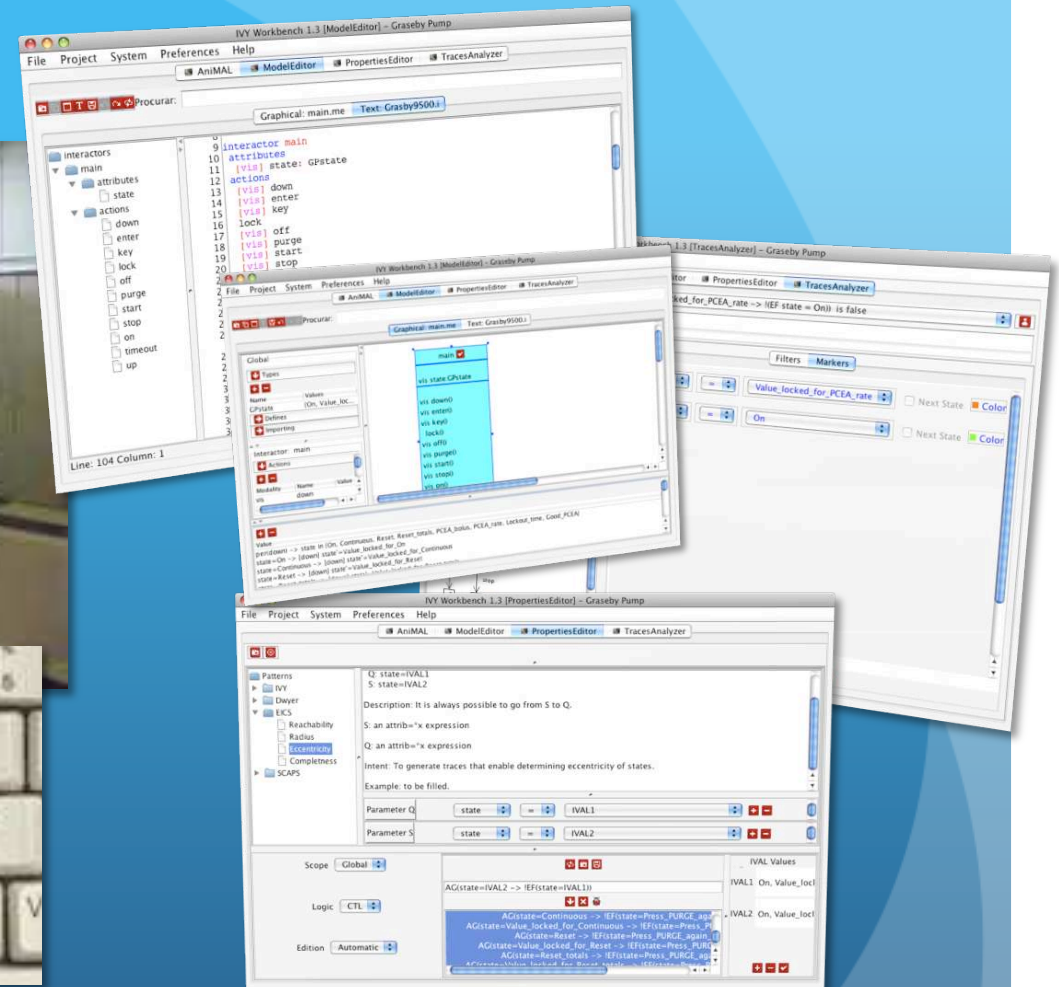
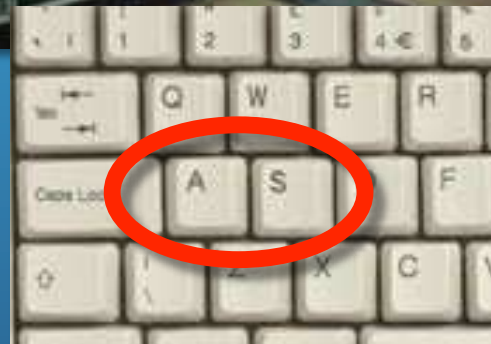


Motivation



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

Context

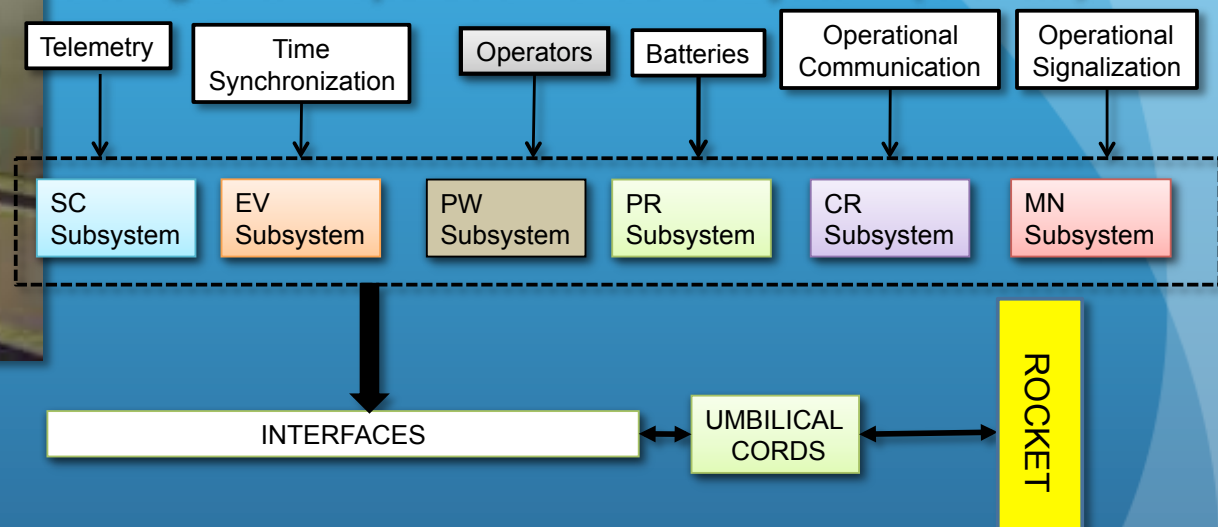


- IAE
 - Develops and operates Brazilian's satellite launchers
- HASLab
 - Model-based tools for exhaustive analysis of interactive systems

Context



Testing and Preparation Ground System (BCVLS)



- 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

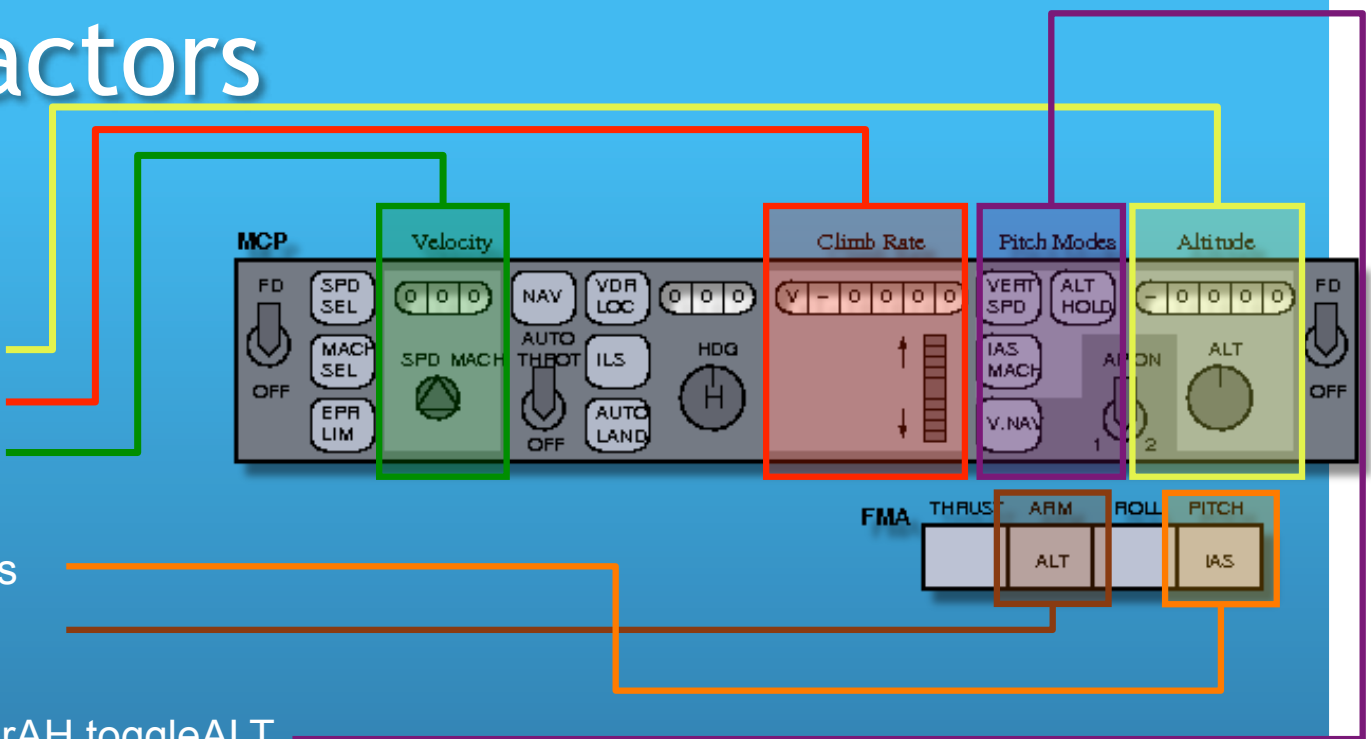
- [vis] pitchMode: PitchModes
- [vis] ALT: boolean

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

Safety Critical Interactive Computing Systems' Modelling

Integration of Theorem Proving in the IVY workbench

MFES Integrated Project Proposal

José Creissac Campos¹ Michael Harrison² & Paolo Masci²

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

Braga, Portugal

²Queen Mary, University of London

London, UK



Context



- Inquires into accidents and incidents
 - *Human error* a typical outcome



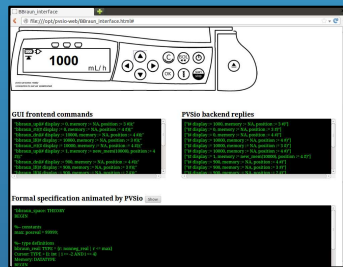
- Which human?
 - the user?
 - the designer?

(Leveson)

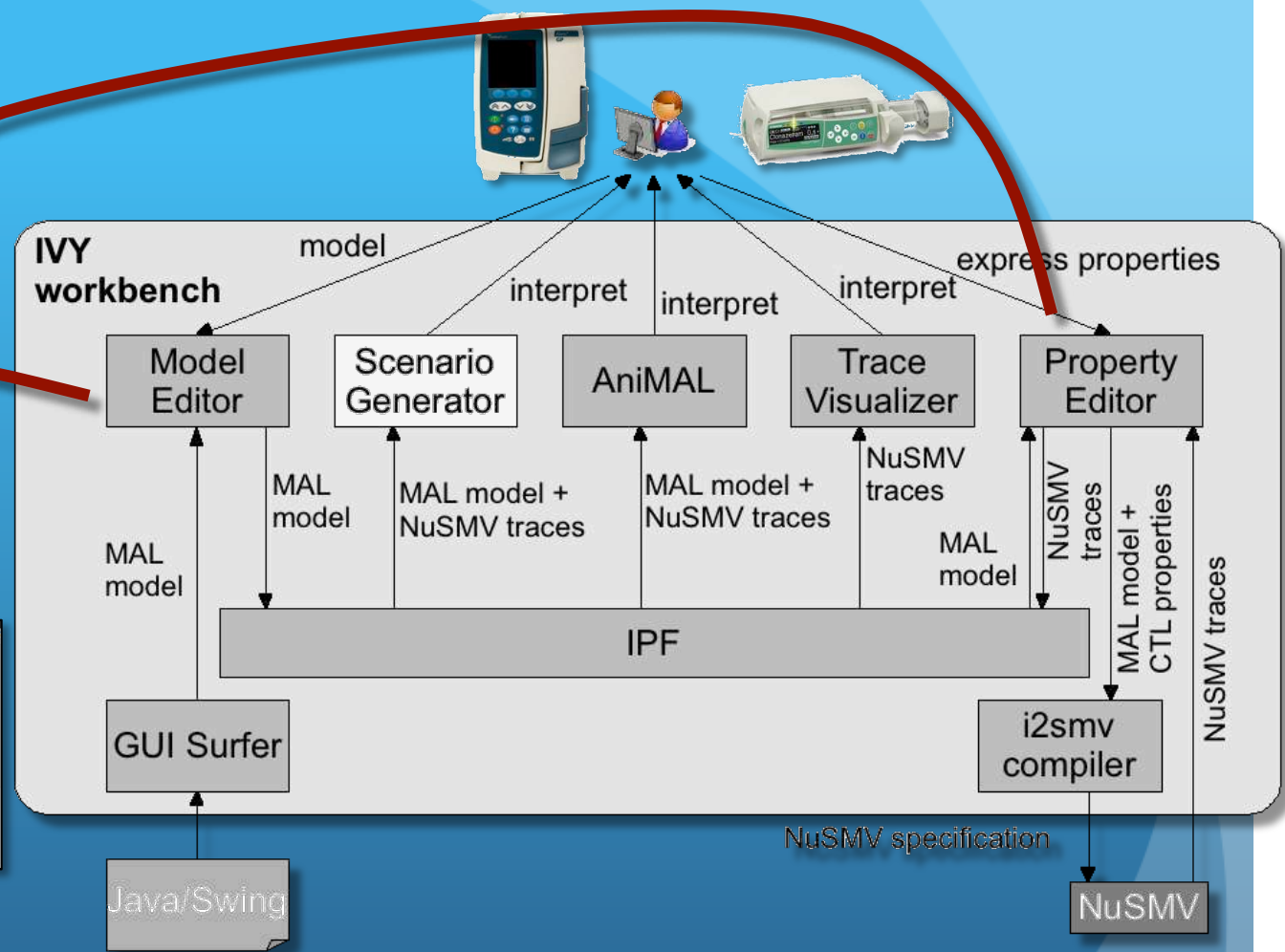
Context



Verification



Simulation



- 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

Integration of Theorem Proving in the IVY workbench

MFES Integrated Project Proposal

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

MFES Integrated Project Proposal

José Creissac Campos¹ José Machado² & Emilia Vilanni³

*¹Dept. de Informática/Universidade do Minho and HASLab/INESC TEC
Braga, Portugal*

*²Departamento de Engenharia Mecânica/Universidade do Minho and CT2M
Guimarães, Portugal*

*³Instituto Tecnológico de Aeronáutica
São José dos Campos, Brasil*



Context / Goals



Projeto pioneiro
O primeiro microsatélite construído por universitários brasileiros tem o objetivo de coletar dados ambientais e meteorológicos

Órbita
O satélite dará uma volta completa em torno da Terra a cada 90 minutos

Custo final
R\$ 5 milhões

Altitude
600km de distância da Terra

Peso: 85kg

1 A intenção é que o Itasat, desenvolvido desde 2004, seja lançado em 2012 e permaneça em órbita baixa por cerca de um ano

2 Uma vez em órbita, o equipamento funcionará como um repetidor. Cerca de 700 plataformas implantadas na Terra farão a coleta de dados como temperatura, pressão, umidade e velocidade dos ventos. Esses dados serão enviados para o satélite

3 O Itasat retransmitirá essas informações para duas estações possíveis. No caso do Brasil, em Cuiabá (MT) e outra em Alcântara (MA)

4 As estações receberão esses dados e os transmitirão para Cachoeira Paulista (SP), onde fica a sede do Inpe. Tanto o satélite quanto as plataformas possuirão antenas que possibilitarão a comunicação

5 Os dados coletados serão transmitidos constantemente aos usuários interessados, formando uma rede de comunicação

Capacitação
Inserido no plano pluri-anual voltado para o desenvolvimento e lançamento de satélites tecnológicos de pequeno porte, o projeto tem o principal objetivo de promover a capacitação brasileira de profissionais. Somente em 2009, envolveu 32 alunos de graduação, 23 de mestrado e cinco de doutorado

Alcântara (MA)
Antena de recepção Cuiabá (MT)
Sede do Inpe

Fonte: ITA
Pablo Alejandro/CB/D.A Press

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