Sixth IAASS Conference
Safety is Not an Option
Montreal - Canada
21-23 May 2013

PRO-ELICERE: A Study for Create a New Process for Dependability Analysis of Space Computer Systems

Glauco da Silva
Carlos Henrique Netto Lahoz
ITA – Institute Technological of Aeronautics
IAE – Institute of Aeronautics and Space

Outline

- Introduction
- Goals
- PRO-ELICERE
- Conclusions

Introduction

- Traditional techniques (FMEA, HAZOP) are still in use for software applied to space system.
- These techniques generate a huge amount of data to be analyzed and treated.
- Intelligent methods can assist the safety analysis helping the identification and classification the potential hazards.

Goals

- Present the PRO-ELICERE, a new approach to the computer system dependability analysis.
- Identify some dependability tools and knowledge discovery techniques that could be used in the PRO-ELICERE process.

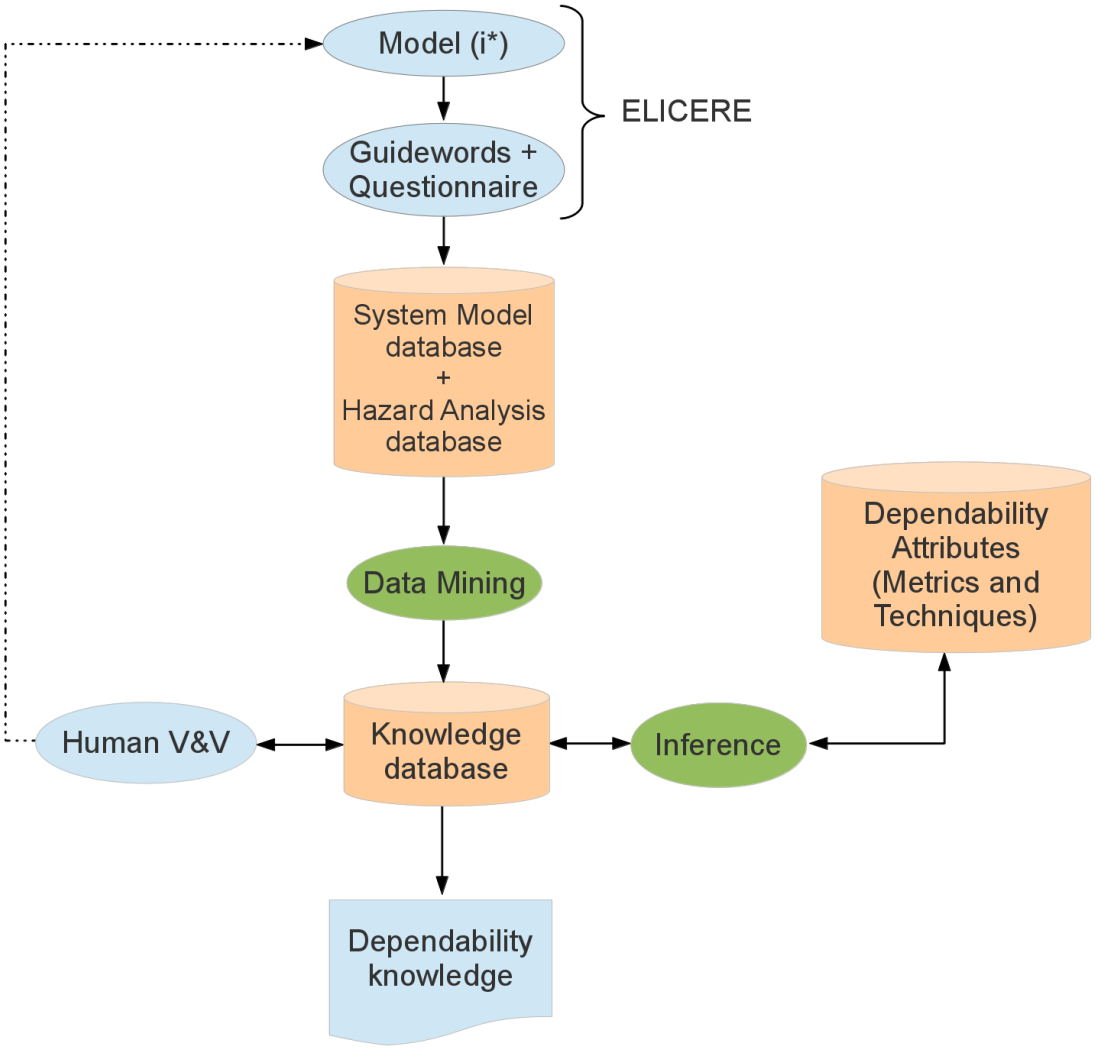
PRO-ELICERE

- Aims to gathering the dependability analysis and its requirements for critical computer system from system modeling perspective.

- It has an intelligent layer, which allows that the analysis may be performed, as much as possible, automatically.

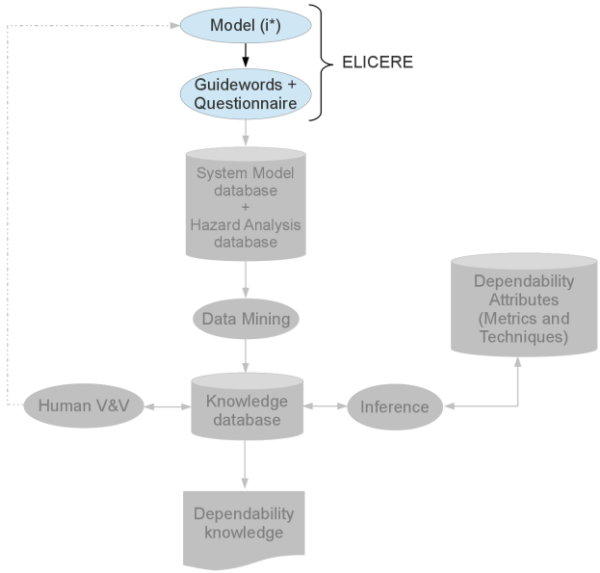
PRO-ELICERE

PRO-ELICERE overview



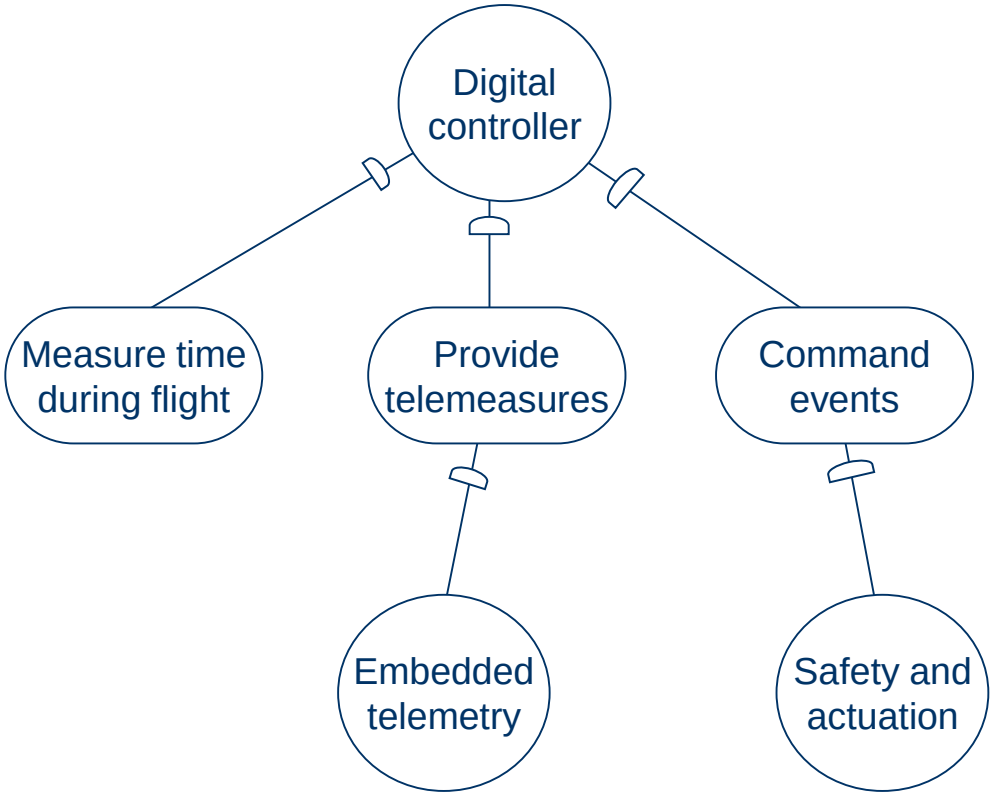
PRO-ELICERE: ELICERE

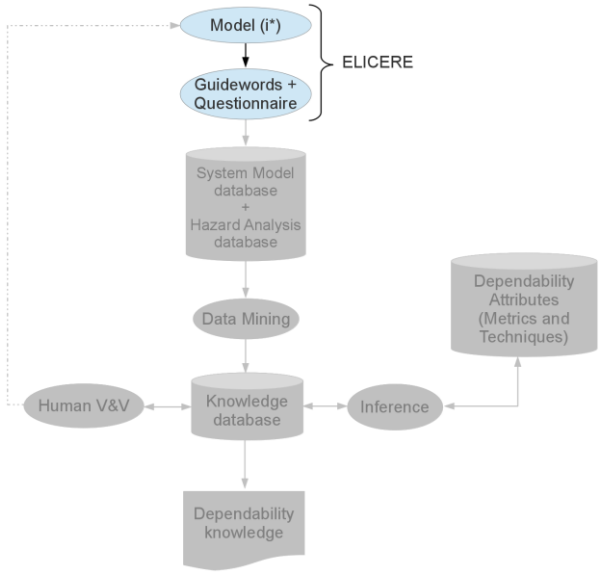
- Uses the i* framework for modeling the system behavior (modeling actors, resources, tasks and softgoals).
- Based on HAZOP and FMEA guidewords to extract softgoals.
- Propose to help the requirements engineer to define what the system cannot do.



PRO-ELICERE: ELICERE

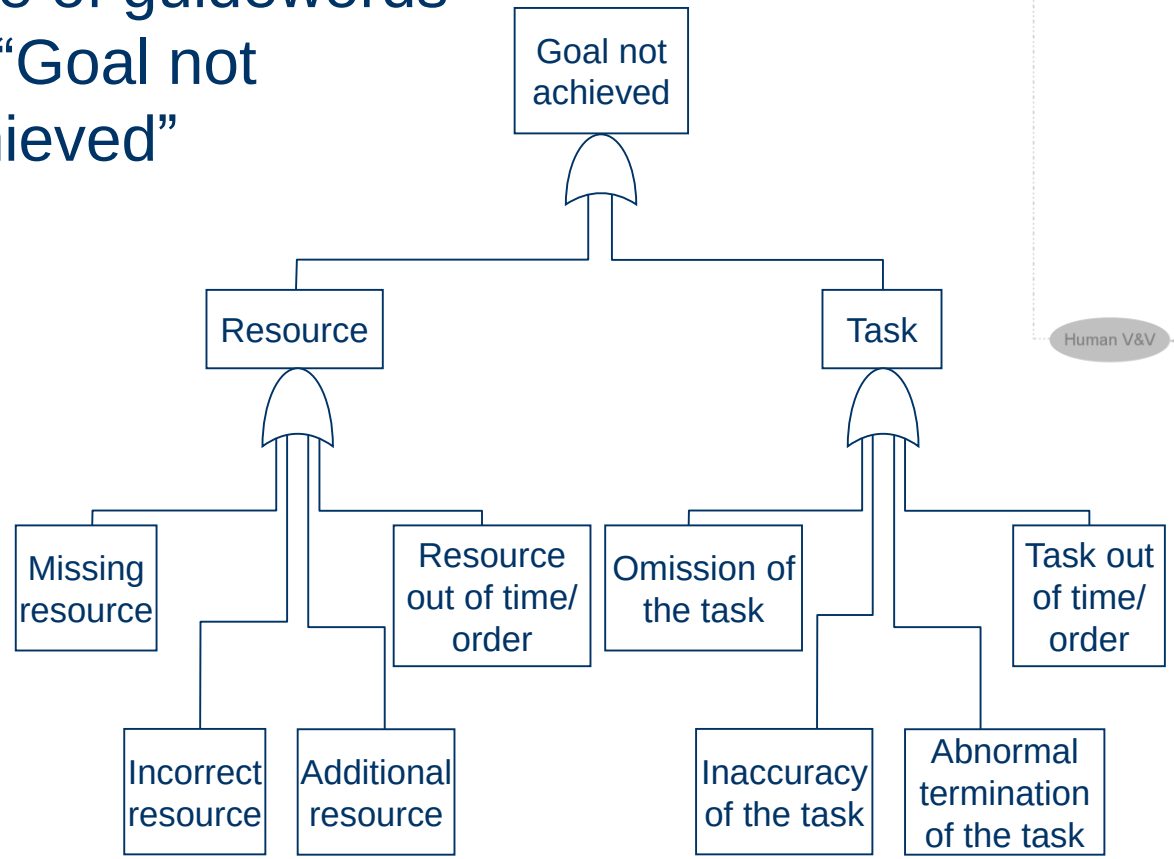
Mission goals

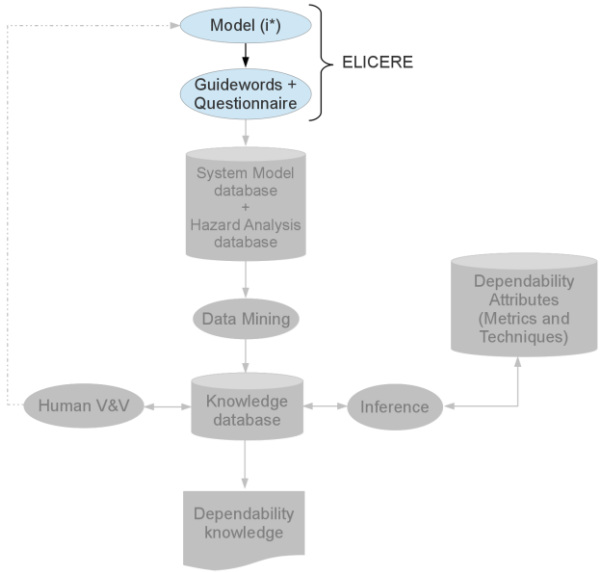




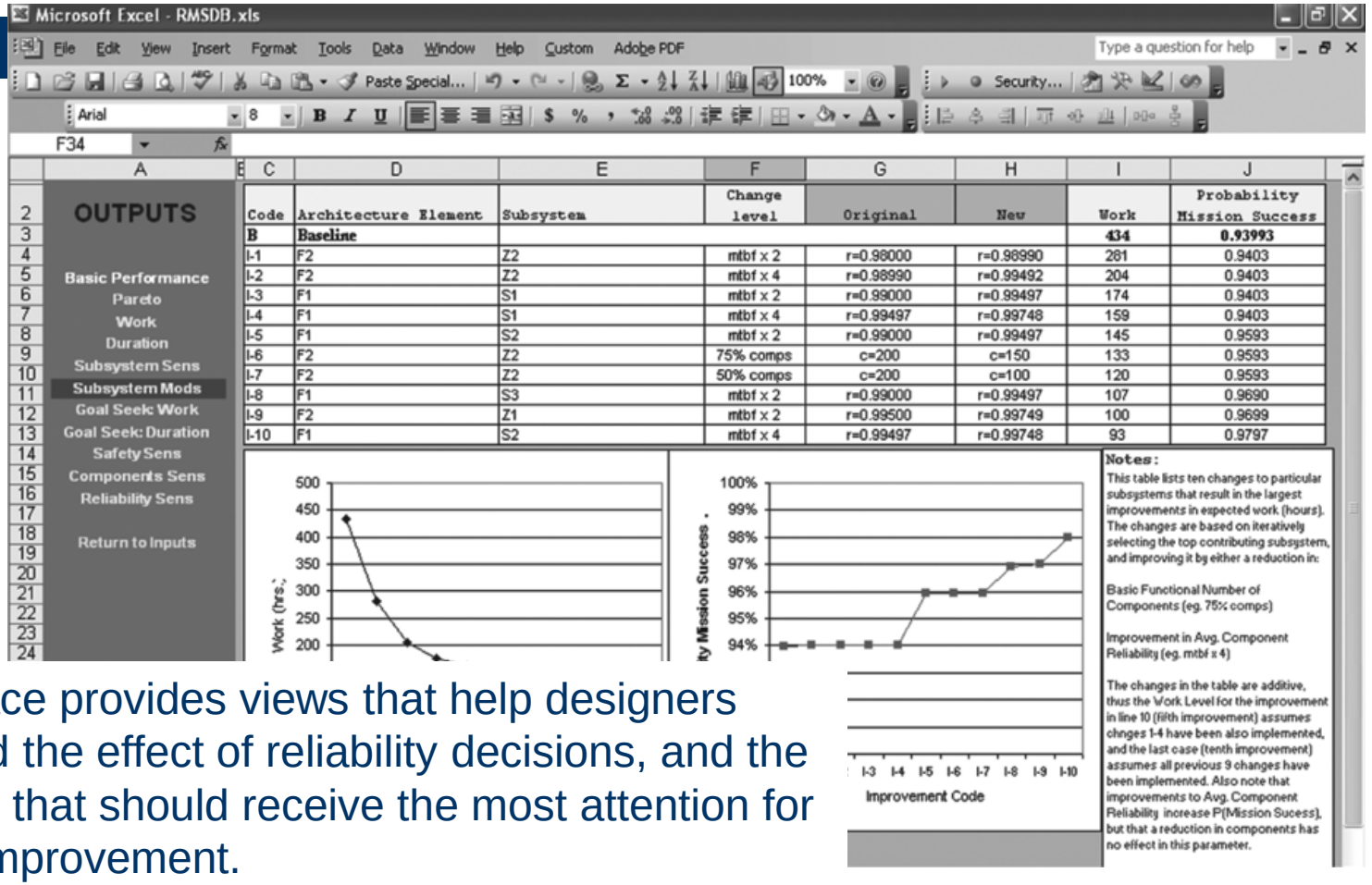
PRO-ELICERE: ELICERE

Tree of guidewords for “Goal not achieved”





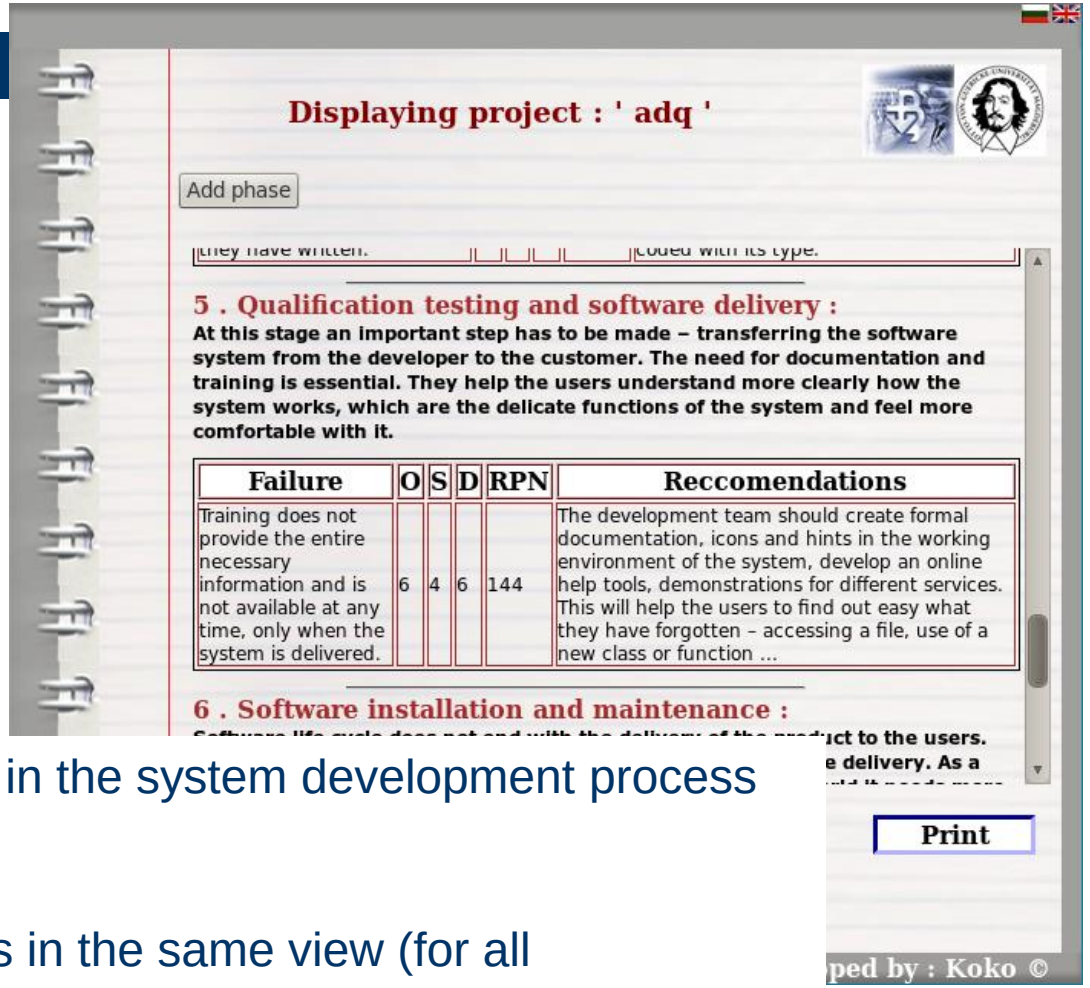
PRO-ELICERE: Dependability Tools (RMSDB)



Code	Architecture Element	Subsystem	Change level	Original	New	Work	Probability Mission Success
B	Baseline					434	0.93993
I-1	F2	Z2	mtbf x 2	r=0.98000	r=0.98990	281	0.9403
I-2	F2	Z2	mtbf x 4	r=0.98990	r=0.99492	204	0.9403
I-3	F1	S1	mtbf x 2	r=0.99000	r=0.99497	174	0.9403
I-4	F1	S1	mtbf x 4	r=0.99497	r=0.99748	159	0.9403
I-5	F1	S2	mtbf x 2	r=0.99000	r=0.99497	145	0.9593
I-6	F2	Z2	75% comps	c=200	c=150	133	0.9593
I-7	F2	Z2	50% comps	c=200	c=100	120	0.9593
I-8	F1	S3	mtbf x 2	r=0.99000	r=0.99497	107	0.9690
I-9	F2	Z1	mtbf x 2	r=0.99500	r=0.99749	100	0.9699
I-10	F1	S2	mtbf x 4	r=0.99497	r=0.99748	93	0.9797

The interface provides views that help designers understand the effect of reliability decisions, and the subsystem that should receive the most attention for reliability improvement.

PRO-ELICERE: Dependability Tools (Web-based SFMEA)

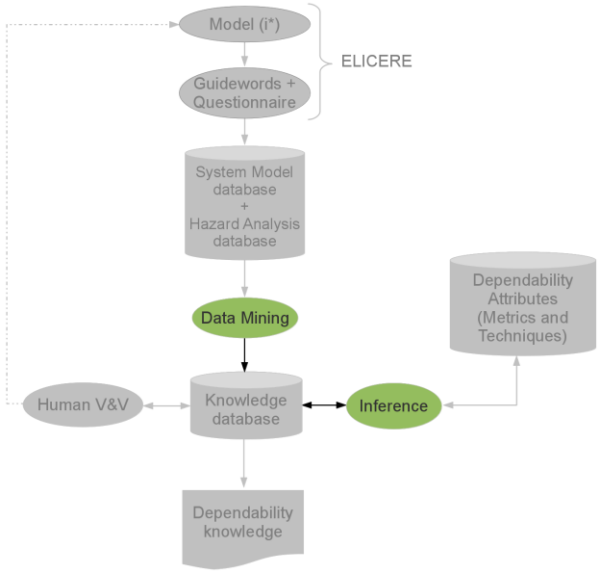


Helps the recognizing failures in the system development process and the final product.

Permit see the analysis results in the same view (for all development phases or product functionalities).

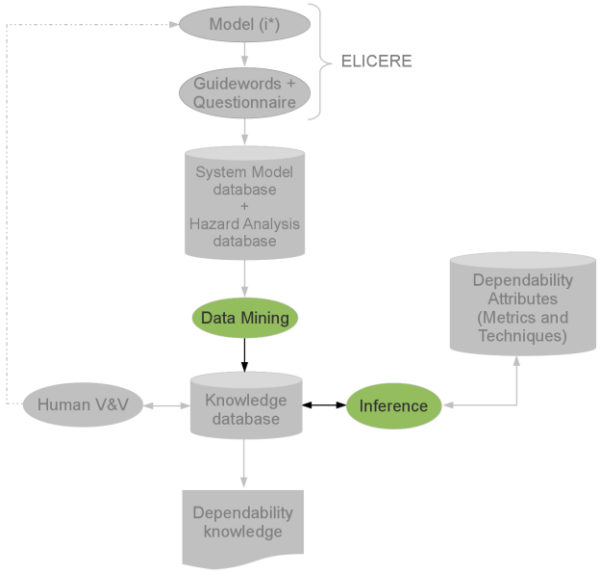
PRO-ELICERE: KD Techniques (NLP)

- NLP is used to permit the interaction between machine language and human language.
- Works with information retrieval and clustering to group contents retrieved.
- The extraction of terms and relationships can be obtained from design documents.

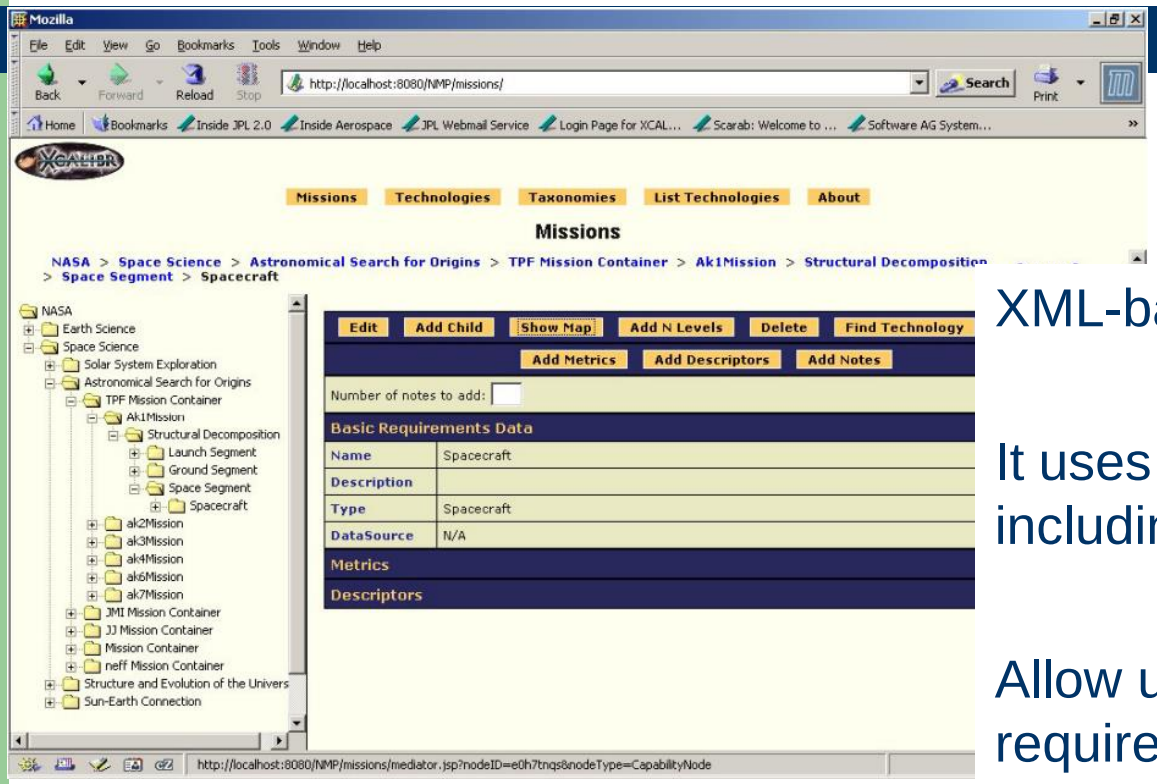


PRO-ELICERE: KD Techniques (NLP)

- The terms and relationship must be validated manually by a group of experts.
- From the terms an relationship found, is possible define an ontology.



PRO-ELICERE: KD Tool (XCALIBR)



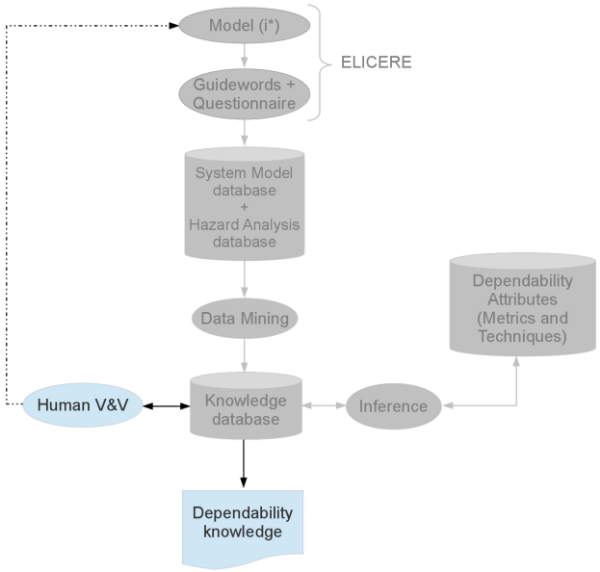
XML-based database.

It uses a detailed taxonomy, including a data dictionary.

Allow users to specify mission requirements.

PRO-ELICERE: Dependability Knowledge

- To the knowledge database should be applied a human assessment.
- The knowledge about the system is stored in the database.
- The analyst can remodel the system.



Conclusions

- PRO-ELICERE will be developed applying some of the techniques seen.
- The goal of PRO-ELICERE is gather the set of dependability requirements of the computer system as a whole.
- Next steps
  - extraction of data from the model and their storage
  - perform a data mining process on the information collected

Acknowledgments

- Space Sc. & Tech. Post Graduation Program - PG/CTE-E
- CAPES/PROAP: to travel expenses

Glauco da Silva

glaucogs@iae.cta.br