



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.

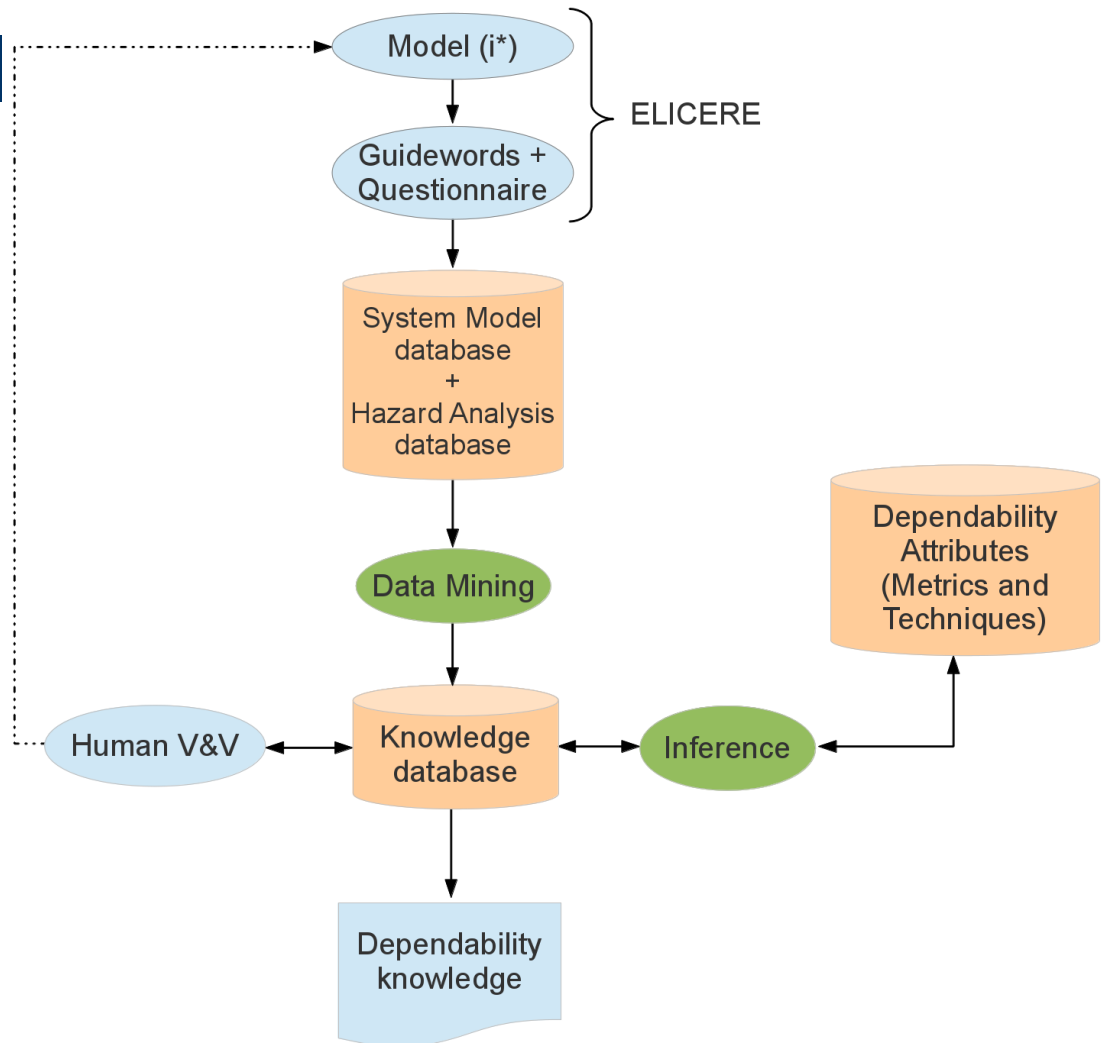


PRO-ELICERE

- 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.

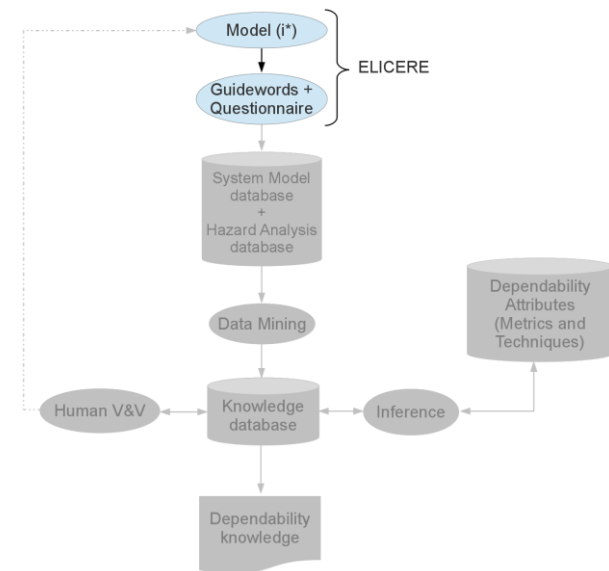
PRO-ELICERE

PRO-ELICERE overview



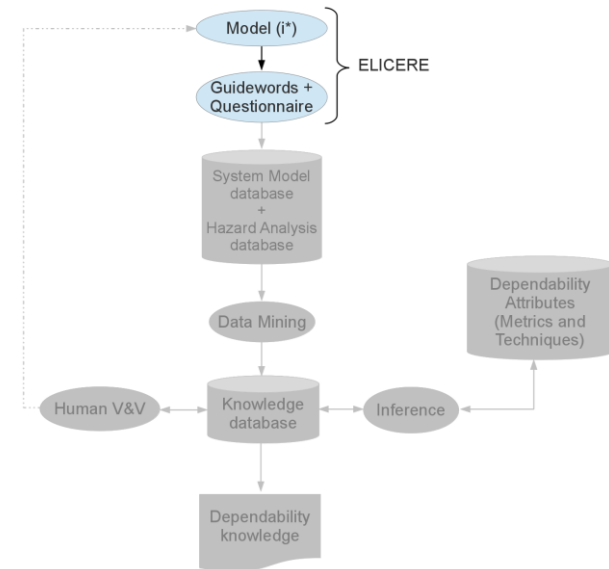
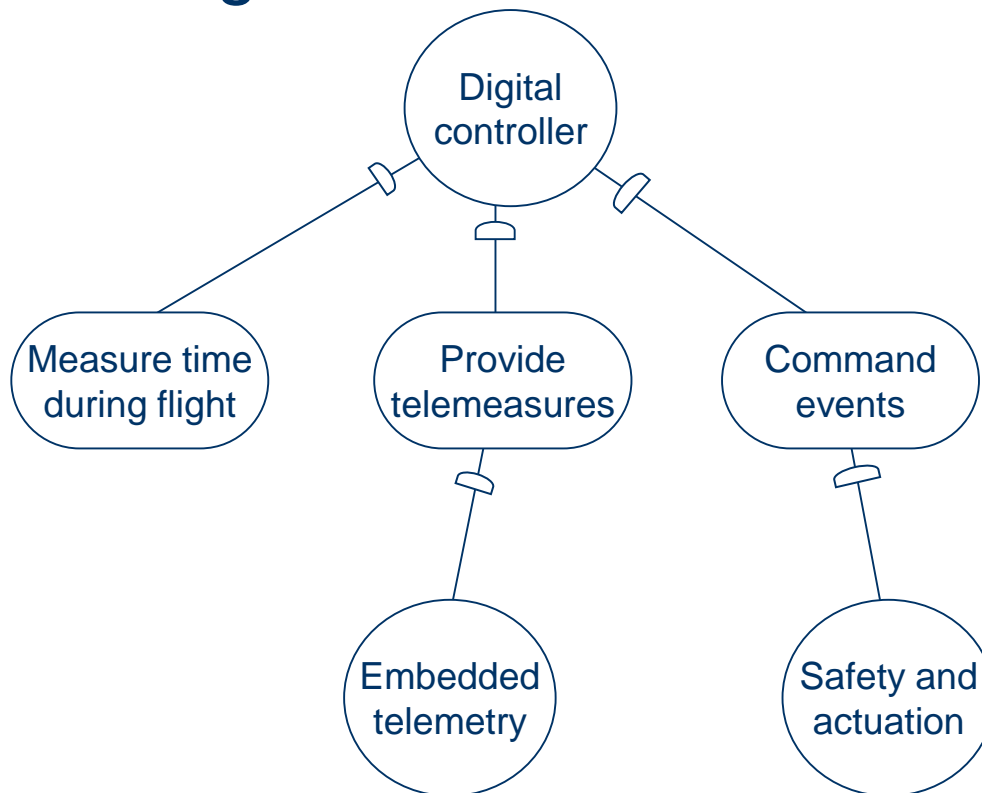
PRO-ELICERE: ELICERE

- 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.



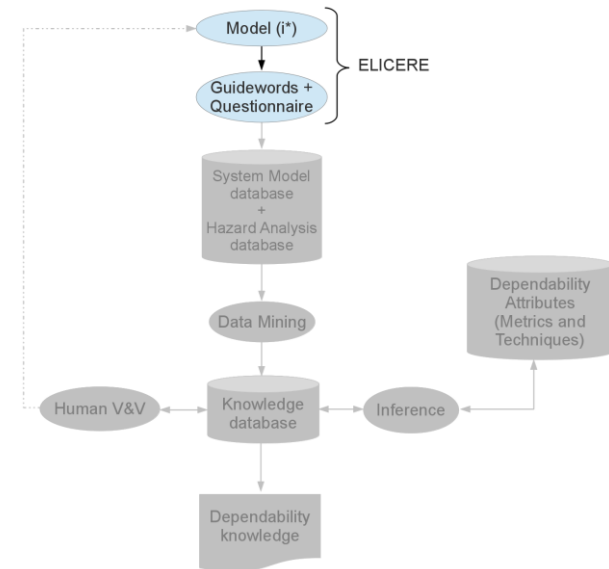
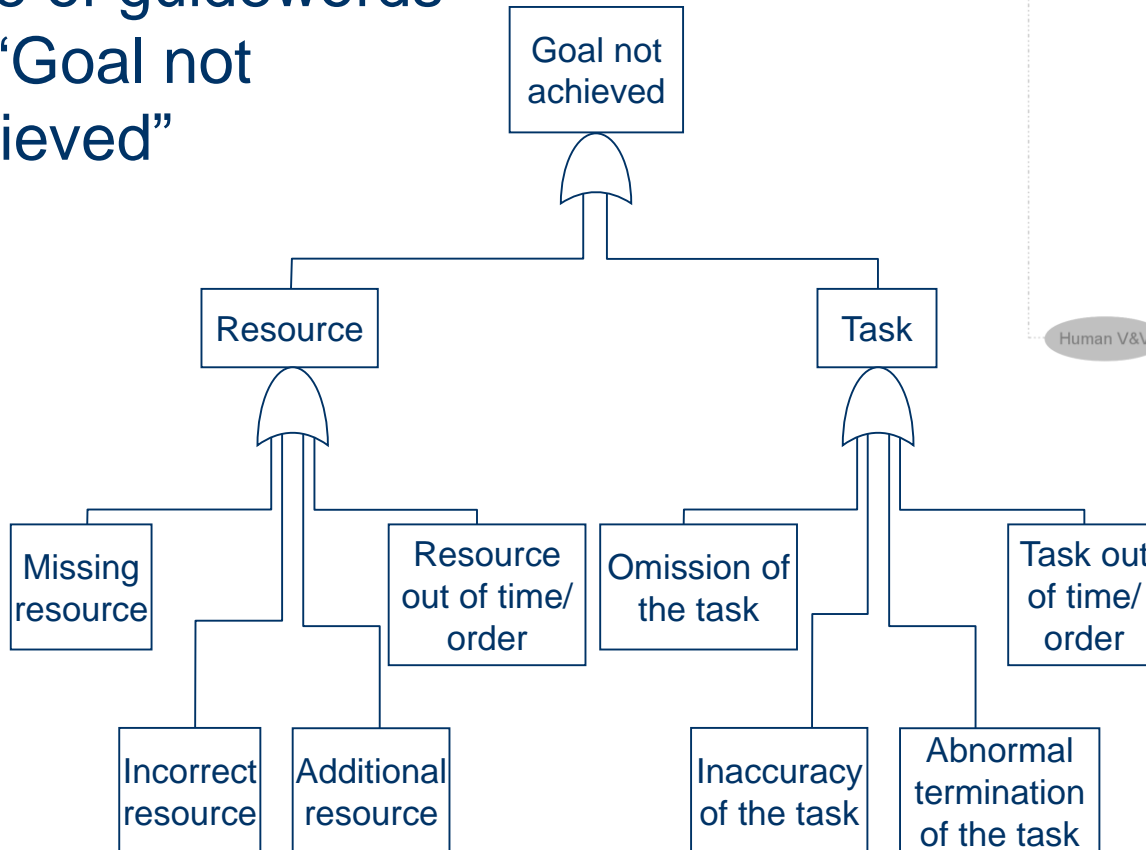
PRO-ELICERE: ELICERE

Mission goals



PRO-ELICERE: ELICERE

Tree of guidewords for “Goal not achieved”





PRO-ELICERE: Dependability Tools (RMSDB)

Microsoft Excel - RMSDB.xls

File Edit View Insert Format Tools Data Window Help Custom Adobe PDF

Type a question for help

100%

Security...

Arial 8

F34

	A	B	C	D	E	F	G	H	I	J
		Code	Architecture Element	Subsystem	Change level	Original	New	Work	Probability	Mission Success
2	OUTPUTS	B	Baseline					434	0.93993	
3		I-1	F2	Z2	mtbf x 2	r=0.98000	r=0.98990	281	0.9403	
4		I-2	F2	Z2	mtbf x 4	r=0.98990	r=0.99492	204	0.9403	
5	Basic Performance	I-3	F1	S1	mtbf x 2	r=0.99000	r=0.99497	174	0.9403	
6	Pareto	I-4	F1	S1	mtbf x 4	r=0.99497	r=0.99748	159	0.9403	
7	Work	I-5	F1	S2	mtbf x 2	r=0.99000	r=0.99497	145	0.9593	
8	Duration	I-6	F2	Z2	75% comps	c=200	c=150	133	0.9593	
9	Subsystem Sens	I-7	F2	Z2	50% comps	c=200	c=100	120	0.9593	
10	Subsystem Mods	I-8	F1	S3	mtbf x 2	r=0.99000	r=0.99497	107	0.9690	
11	Goal Seek Work	I-9	F2	Z1	mtbf x 2	r=0.99500	r=0.99749	100	0.9699	
12	Goal Seek: Duration	I-10	F1	S2	mtbf x 4	r=0.99497	r=0.99748	93	0.9797	
13	Safety Sens									
14	Components Sens									
15	Reliability Sens									
16										
17										
18	Return to Inputs									
19										
20										
21										
22										
23										
24										

Improvement Code	Work (hrs.)
I-3	174
I-4	159
I-5	145
I-6	133
I-7	120
I-8	107
I-9	100
I-10	93

Improvement Code	Mission Success
I-3	0.9403
I-4	0.9403
I-5	0.9593
I-6	0.9593
I-7	0.9593
I-8	0.9690
I-9	0.9699
I-10	0.9797

Notes:

This table lists ten changes to particular subsystems that result in the largest improvements in expected work (hours). The changes are based on iteratively selecting the top contributing subsystem, and improving it by either a reduction in:

- Basic Functional Number of Components (eg. 75% comps)
- Improvement in Avg. Component Reliability (eg. mtbf x 4)

The changes in the table are additive, thus the Work Level for the improvement in line 10 (fifth improvement) assumes changes I-4 have been also implemented, and the last case (tenth improvement) assumes all previous 9 changes have been implemented. Also note that improvements to Avg. Component Reliability increase P[Mission Success], but that a reduction in components has no effect in this parameter.

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)

Displaying project : ' adq '

Add phase

they have written. | | | | | coded with its type.

5 . Qualification testing and software delivery :

At this stage an important step has to be made - transferring the software system from the developer to the customer. The need for documentation and training is essential. They help the users understand more clearly how the system works, which are the delicate functions of the system and feel more comfortable with it.

Failure	O	S	D	RPN	Reccomendations
Training does not provide the entire necessary information and is not available at any time, only when the system is delivered.	6	4	6	144	The development team should create formal documentation, icons and hints in the working environment of the system, develop an online help tools, demonstrations for different services. This will help the users to find out easy what they have forgotten - accessing a file, use of a new class or function ...

6 . Software installation and maintenance :

Software life cycle does not end with the delivery of the product to the users. e delivery. As a

ped by : Koko ©

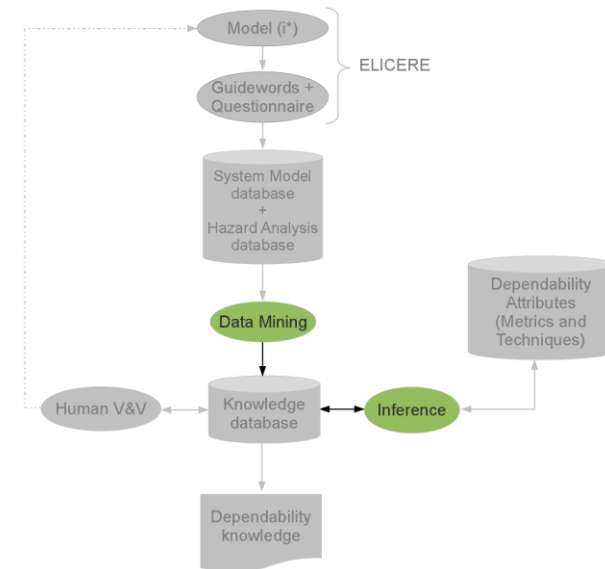
[Print](#)

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).

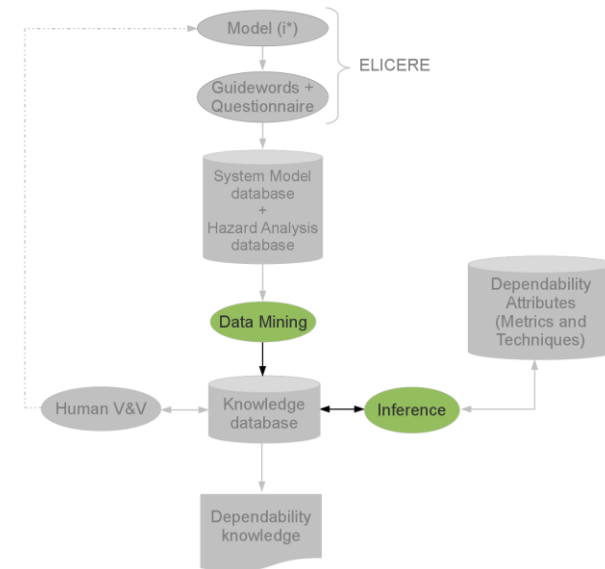
PRO-ELICERE: KD Techniques (NLP)

- 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 and relationship found, it is possible to define an ontology.





PRO-ELICERE: KD Tool (XCALIBR)

NASA > Space Science > Astronomical Search for Origins > TPF Mission Container > Ak1Mission > Structural Decomposition > Space Segment > Spacecraft

Basic Requirements Data	
Name	Spacecraft
Description	
Type	Spacecraft
DataSource	N/A

Metrics

Descriptors

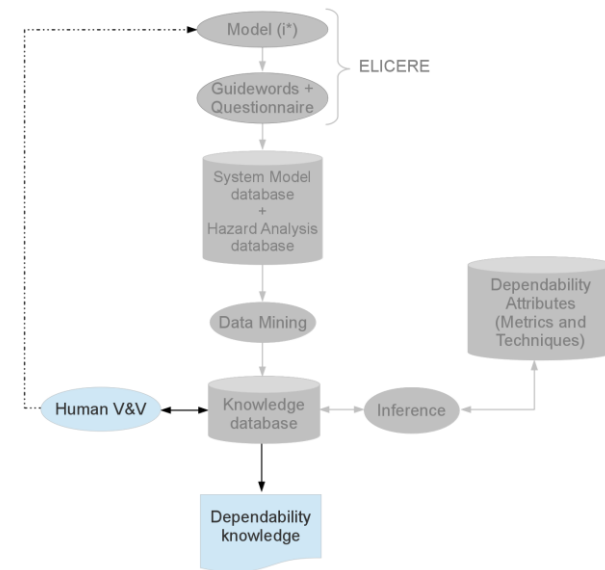
XML-based database.

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