SFTA, SFMECA AND STPA APPLIED TO BRAZILIAN SPACE SOFTWARE

Carlos H N **Lahoz**

Instituto de Aeronautica e Espaco (IAE)

Instituto Tecnologico da Aeronautica (ITA)

BRAZIL

STAMP/STAP Workshop 2014
25-27 March 2014 - MIT Campus

Agenda

Context of this work

Space Software - Case Study

Combined approach SFTA+SFMECA

STPA

Considerations

Context of this work

This work reports some results of a research project performed at IAE/Brazil using dependability techniques applied to space computer system

- SFTA and SFMECA was conducted on system software specification (SSS) in a case study of an hypothetical spacecraft software
- STPA is being applied to one scenario in order to evaluate possible additional information about how the behavioral safety constraints can be violated

Space Software - Case Study

FTC: function responsible for calculating the time in pre-flight and flight phases (Lower Time Limit -LTL and Upper Time Limit -UTL).

RED: function responsible for detecting the reference-events expected during the pre-flight and all flight phases through the information of vehicle acceleration, obtained by the inertial sensor (IS), and flight time

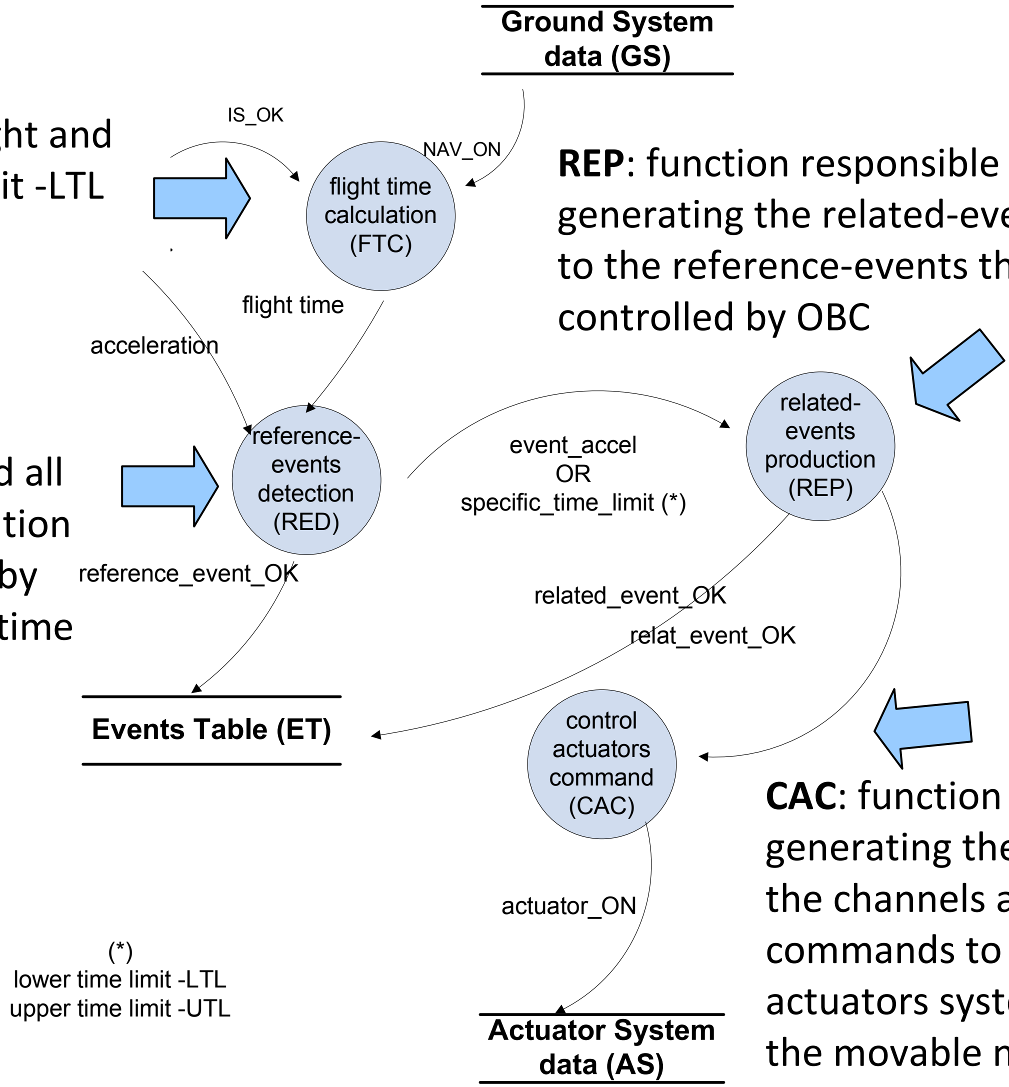
List of RED events:

RED_PRE, RED_A, RED_A6

RED_B, RED_C, RED_D

REP: function responsible for generating the related-events linked to the reference-events that must be controlled by OBC

CAC: function responsible for generating the data used by the channels activation commands to the rocket actuators system (AS), such as the movable nozzles



Sequence of Flight Events (SFE) dataflow

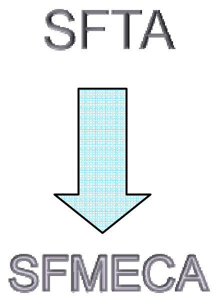
SFTA+SFMECA combined approach

Converse Combination approach:

•According to the system's function requirements and the failure definition, this technique selects one or more specific undesirable events as the top events to build the responsible SFTA

•After the qualitative analysis, some important basic events are selected

•These events are analyzed and evaluated by the FMECA procedure
•According to the result of SFMECA, further analysis and calculation of the fault tree analysis can be carried out



Converse combination approach

SFTA+SFMECA combined approach

Four steps:

Step 1- Preparation for techniques application: evaluating SFTA level (specification or code level) and SFMECA table tailoring

Step 2 - SFTA analysis: to look at the software faults related to resources (data) and tasks (functions) that could cause a hazard

Step 3 - SFMECA analysis: using ELICERE guidewords to classify failure modes from SFTA

Step 4 - Identify compensating provisions: in order to suggest new non-functional requirements

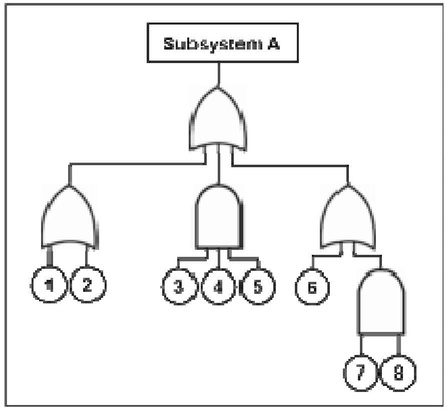
SFTA+SFMECA: step 1

ELICERE guidewords		other approaches (*)	description
Resource	Absent	Omission total No	resource not provided; hardware failure; lack or loss of messages; lack of input values of a sensor; lack of input values or output; failure to receive the required data; loss of data due to hardware failure sensor failure to send the data
	Incorrect	Comission, Omission partial More, Less Reverse Part of Other than	bad data; any resource that does not correctly describe the use of the system or its operating environment; spurious or unexpected signals in the output of a device; error values for routine firing of triggers; incomplete data structure; lack of some data in a sequence; resource was greater or less than required; only part of the resource was offered; offered opposite resource; another resource was offered; information delivered with wrong value
	Wrong Timing	Early Before Late After	device start out of time specified; device start out of order specified; obsolete data used to the control decision; spurious data; inadvertent or flawed that occur only with some entries; resource provided before the time required; resource provided after the required time; ABDC sequence occurs in a sequence of events that should be ABCD
	Duplicated	Comission repetition As well as	additional resource offered; saturated data; duplicate data; overflow; resource offered when not required; a data from an expected communication is repeated when it should not be

Classes of Failures: ELICERE resource guidewords

(*) CHAZOP (Nimmo; Nunns and Eddershaw, 1987), SHAZOP (Burns and Pitlado, 1993) SFMEA (Lutz and Woodhouse, 1996), SHARD/LISA (Pumfrey, 2000)

SFTA+SFMECA: step 2

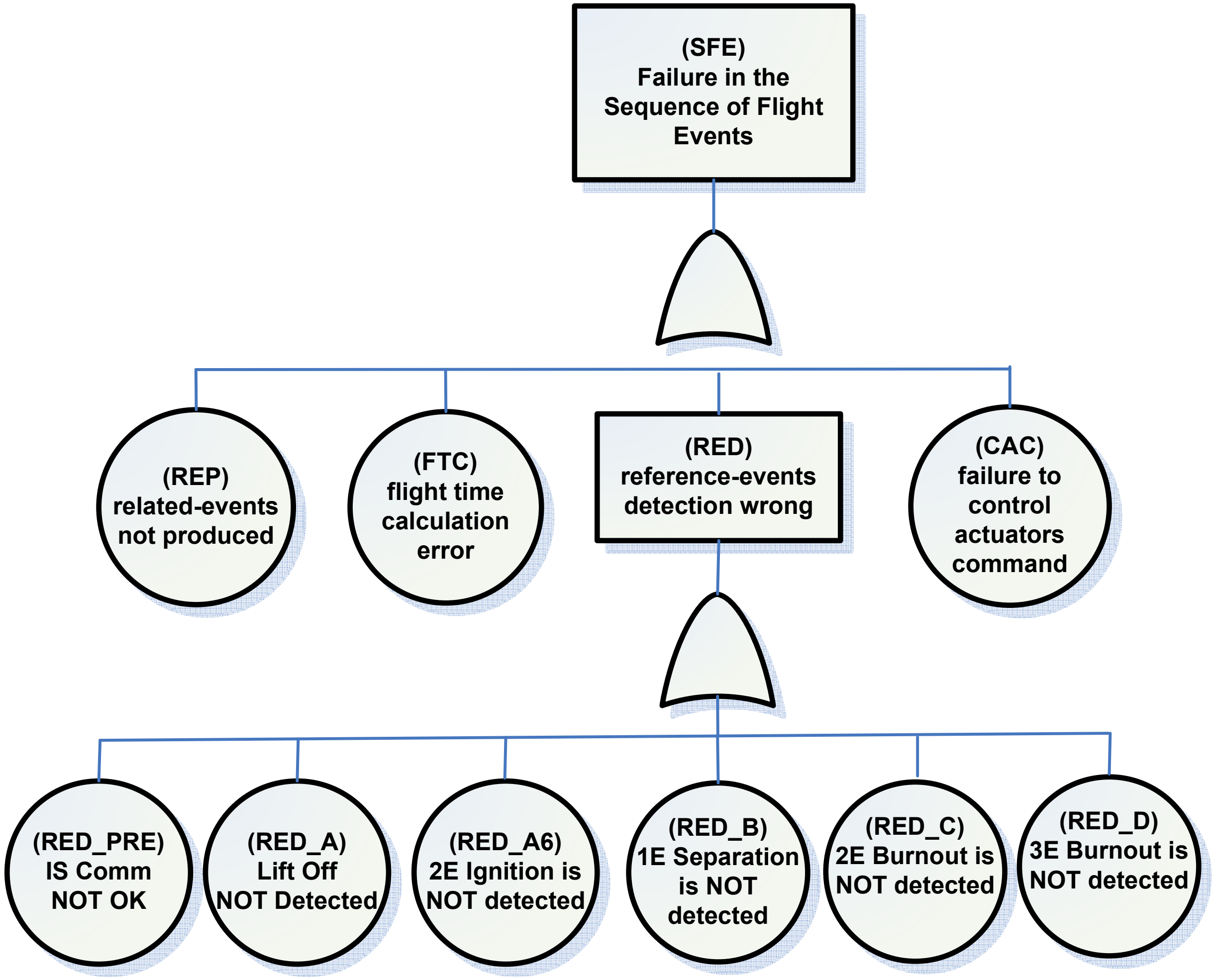


SFTA: top down (deductive) technique that focuses on how errors, or even normal functioning of the system can lead to hazards.

Top event = hazard (system software requirements not met)

Basics events = set of possible causes (software requirements not met)

SFTA+SFMECA: step 2



SFTA application for “Sequence of Flight Events”

SFTA+SFMECA: step 3

POTENTIAL
FAILURE MODE AND EFFECTS ANALYSIS
Front Door L.H.

System 1 - Automobile
Subsystem 2 - Closures
X Component 3 - Front Door L.H.
Model Year(s)/Vehicle(s) 199X/Lion 4dr/Wagon
Core Team A. Tate Body Engrg, J. Smith - OC, R. James - Production, J. Jones - Maintenance
Process Responsibility Body Engineering
Key Date 3/31/2003
FMEA Number 1450
Page 1 of 1
Prepared By J. Ford - X6521 - Assy Ops
FMEA Date (Orig.) 3/10/2003 (Rev) 3/21/2003

Item / Process Function/Requirements	Potential Failure Mode	Potential Effect(s) of Failure	Sev	Class	Potential Cause(s)/Mechanism(s) of Failure	Occur	Current Process Controls Prevention	Current Process Controls Detection	Detec	RPN	Recommended Action(s)	Responsibility & Target Completion Date	Actions Taken: Actions Taken	Actions Taken: Sev	Actions Taken: Occ	Actions Taken: Det	Actions Taken: RPN
3 - Front Door L.H.																	
Manual application of wax inside door. To cover inner door, lower surfaces at minimum wax thickness to retard corrosion.	Insufficient wax coverage over specified surface.	Deteriorated life of door leading to: - Unsatisfactory appearance due to rust through paint over time. - Impaired function of interior door hardware.	7		Manually inserted spray head not inserted far enough.	8		Visual check each hour - 1/shift for film thickness (depth meter) and coverage.	5	280	Add positive depth stop to sprayer.		Stop added, sprayer checked on line.	7	2	5	70
					Spray head clogged - Viscosity too high - Temperature too low - Pressure too low.	5		Test spray pattern at start-up and after idle periods, and preventive maintenance program to clean heads.	3	105				7	1	3	21
					Spray head deformed due to impact.	2		Preventive maintenance program to maintain heads.	2	28				7	2	2	28
					Spray time insufficient.	8		Operator instructions and lot sampling (10 doors/shift) to check for coverage of critical areas.	7	392				7	1	7	49

SFMECA: Bottom-up (indutive) method used to find potential system problems

SFMECA is applied in the SFTA basic events, identifying:

- potential failure modes (guidewords)
- consequences, severity
- criticality
- possible compensating provisions

SFTA+SFMECA: step 3

Failure Mode	Failure Class	Potential Cause	Effect	Severity	Criticality
RED_PRE IS Comm NOT OK (Inertial System communication is not been working)	**Incorrect Data**	Incorrect information that the rocket is ready to flight OR Incorrect information that indicate the IS is ready OR Incorrect information of longitudinal acceleration of the vehicle to detection of reference events OR Incorrect control flag to start the execution of each control algorithms OR Incorrect information of the time (flight time)	**Wrong data time of the reference events RED_PRE and the instant of starting communication from IS to OBC** **OR** **Incorrect time instant of starting the vehicle flight (from FTC)**	5 Mission loss	B

SFMECA application for "Inertial System Communication Not OK”

SFTA+SFMECA: step 4

Compensation Provision:

- Ensure that the event that starts the communication with the IS and OBC is correctly identified (CONSISTENCY)

STPA

Step 0: Establish the fundamentals

•Define what is "accident" for the system and what is an unacceptable loss

For the SFE: accident is the fact that the software was not able to perform the sequence of flight events causing loss of mission

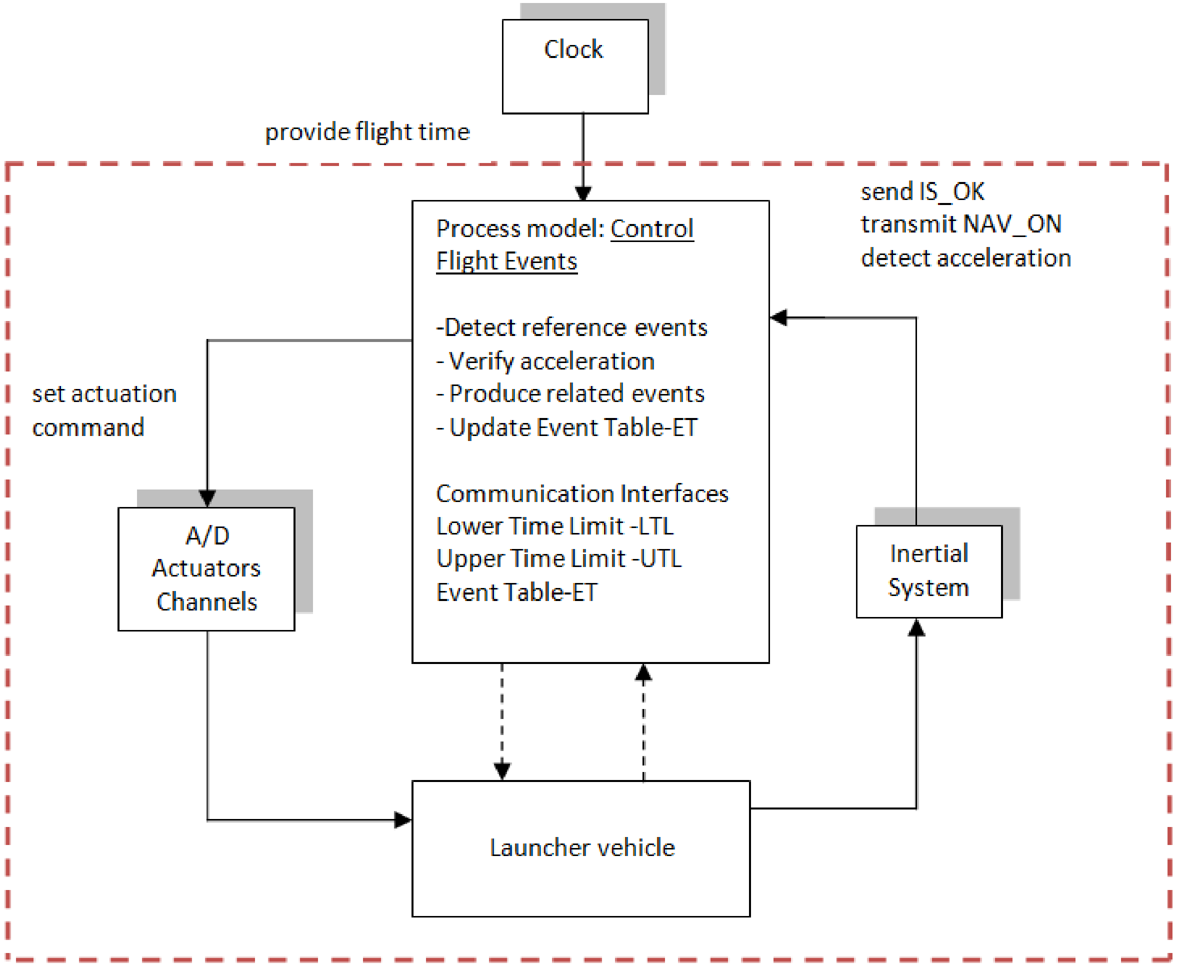
STPA

Step 0: Define what are the system hazards (H) and their safety constraints (SC)

System Hazards	Safety Constraints
H1=Failure on RED_PRE	SC1= ensure the correct communication with the IS to activate the pre-flight event
H2=Failure on RED_A	SC2= the software must receive the NAV_ON to initialize the flight time
H3=Failure on RED_A6	SC3= the ignition of the second rocket stage (2E) must be detected
H4=Failure on RED_B	SC4= the separation of the first rocket stage (1E) must be detected
H5=Failure on RED_C	SC5= the burnout of 2E must be detected
H6=Failure on RED_D	SC6= the burnout of 3E must be detected
H7=Failure on actuation command	SC7=verify if the channels are actuated

STPA

Step 0: Define a basic control structure



STPA

Step 1: Identify potentially inadequate (unsafe) control actions of the system that could lead to a hazardous state (unsafe control)
As well as ELICERE guidewords, STPA classify four unsafe controls:

Control Action	Not Providing causes hazard	Providing causes hazard	Wrong timing or order causes hazard	Stop too soon or applied too long
Send IS_OK	IS_OK not sent	Not applicable	Not applicable	Not applicable
Provide acceleration	IS do not supply the data	IS supplied the incorrect data	IS supplies the data with long delay	IS bus stops functioning
transmitt NAV_ON	GS not supplied	Not applicable	GS supplied after 1E burnout	Not applicable
Detect acceleration	RED do not acquire the data	Not applicable	RED acquires data out of the time window	RED stops to acquire data during the fly
Set actuation command	CAC do not set the A/D channel	CAC provides the wrong actuation	CAC provides the actuation in a wrong time	Not applicable

STPA

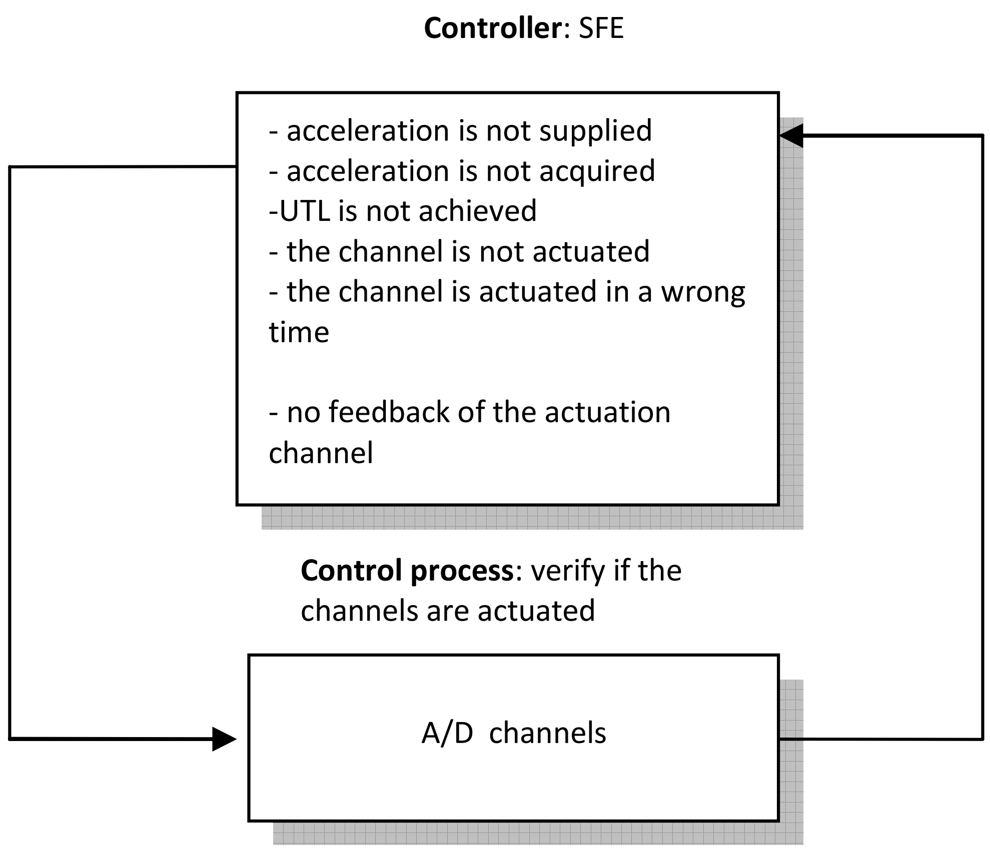
Step 2: Identify causes of unsafe control actions

Hazard control behavior identified in this case study:

•no feedback by the actuation command from I/O channels: information to the SFE if the first stage (1E) was physically separated after the activation of the respective digital channels (output)

STPA

Step 2: SFE Causes of Unsafe Control Actions from “set actuation command”



STPA

Step 2: Develop mitigations to "set actuation command"

•onboard software should read the data from 1E movable nozzle actuation channel (input), located in the 2E, to check if the value is zero. The zero value in this channel means that the 1E was physically separated

Considerations: case study

•The integrated use of SFTA (top events) and SFMECA (basic events) for software dependability analysis allowed identifying gaps in meeting requirements: SFTA: produced 62 gates and 170 basic events

•Most of SFE basic events that had been identified by SFTA were also identified in STPA hazard analysis

•The STPA unsafe control action "no feedback of the actuation channel", is not clearly identified by SFTA+SFMECA

•Although the STPA was not used extensively in the project, provides a structured process for hazards analysis, that apparently helps to reduce the analytical burden

Considerations about (S)FTA & (S)FMECA

- FMECA results are presented in a less intuitive way: tabular format (Hong, L. & Binbin, L. 2009)

- The effort to use FTA is 2x more than STPA (Yahia, H. & Fawzy, E., STPA Workshop 2013)

- If FTA or FMEA focused only on the physical architecture without consideration to control system propagation paths and feedback mechanisms, it may be possible to miss some safety requirements (Sundaram, P.& Hartfelder, D., STPA Workshop 2013)

Considerations about STPA

•Domain expertise and a level of familiarity with control engineering is needed (Malakis, S., STPA Workshop 2012)

•In multiple controllers case, it is important to understand interaction (interference) among controllers. However, it is difficult (Ujiie, R. & Ishimatsu, T., STPA Workshop 2012)

• STPA analyze not only safety aspects, but also functional goals (Thomas, J., STPA Workshop 2012)

•STPA addresses misbehaviors due to software problems and may help address regulatory concerns (Torok, R. & Geddes, B., STPA Workshop 2013)

Considerations about STPA

- Use of STPA allowed the design team to identify more casual factors for quality losses than FMEA or FTA, including component interactions, software flaws, and omissions and external noises (Goerges, S., STPA Workshop 2013)

- How to develop real-time constraints? (Yahia, H. & Fawzy, E., STPA Workshop 2013)

- Likely to require a facilitator for new users and dependent on analysis boundary (Torok, R. & Geddes, B., STPA Workshop 2013)

- The third step of STPA needs a lot of effort, time and deep knowledge for examining the controllers with process models (Abdulkhaleq, A., STPA Workshop 2013)

Thank you

Carlos H N Lahoz
lahozchnl@iae.cta.br
55-12-997131177 mobile
Instituto de Aeronautica e Espaco (IAE)
Sao Jose dos Campos - Brazil

This study is a part of the on-going research project "Verification and Validation of Space Projects - Software Systems" sponsored by National Council for Scientific and Technological Development (CNPq), Brazil (Process 559973-2010-1)

CNPq
Conselho Nacional de Desenvolvimento Científico e Tecnológico