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
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

<table>
<thead>
<tr>
<th>ELICERE guidewords</th>
<th>other approaches (*)</th>
<th>description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Absent</td>
<td>Omission total No</td>
<td>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</td>
</tr>
<tr>
<td>Incorrect</td>
<td>Comission, Omission partial More, Less Reverse Part of Other than</td>
<td>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</td>
</tr>
<tr>
<td>Wrong Timing</td>
<td>Early Before Late After</td>
<td>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</td>
</tr>
<tr>
<td>Duplicated</td>
<td>Comission repetition As well as</td>
<td>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</td>
</tr>
</tbody>
</table>

### 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

(SFE) Failure in the Sequence of Flight Events

(RED) reference-events detection wrong

(RED_A) 1E Separation NOT detected
(RED_B) 2E Burnout is NOT detected
(RED_C) 3E Burnout is NOT detected

(REP) related-events not produced

(FTC) flight time calculation error

(CAC) failure to control actuators command

SFTA application for “Sequence of Flight Events”
SFTA+SFMECA: step 3

SFMECA: Bottom-up (inductive) 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

<table>
<thead>
<tr>
<th>Failure Mode</th>
<th>Failure Class</th>
<th>Potential Cause</th>
<th>Effect</th>
<th>Severity</th>
<th>Criticality</th>
</tr>
</thead>
<tbody>
<tr>
<td>RED_PRE IS Comm NOT OK (Inertial System communication is not been working)</td>
<td>Incorrect Data</td>
<td>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)</td>
<td>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)</td>
<td>5</td>
<td>B</td>
</tr>
</tbody>
</table>

**SFMECA application for "Inertial System Communication Not OK"**

*copyright Carlos Lahoz - 2014*
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)

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

<table>
<thead>
<tr>
<th>Control Action</th>
<th>Not Providing causes hazard</th>
<th>Providing causes hazard</th>
<th>Wrong timing or order causes hazard</th>
<th>Stop too soon or applied too long</th>
</tr>
</thead>
<tbody>
<tr>
<td>Send IS_OK</td>
<td>IS_OK not sent</td>
<td>Not applicable</td>
<td>Not applicable</td>
<td>Not applicable</td>
</tr>
<tr>
<td>Provide acceleration</td>
<td>IS do not supply the data</td>
<td>IS supplied the incorrect data</td>
<td>IS supplies the data with long delay</td>
<td>IS bus stops functioning</td>
</tr>
<tr>
<td>transmitt NAV_ON</td>
<td>GS not supplied</td>
<td>Not applicable</td>
<td>GS supplied after 1E burnout</td>
<td>Not applicable</td>
</tr>
<tr>
<td>Detect acceleration</td>
<td>RED do not acquire the data</td>
<td>Not applicable</td>
<td>RED acquires data out of the time window</td>
<td>RED stops to acquire data during the fly</td>
</tr>
<tr>
<td>Set actuation command</td>
<td>CAC do not set the A/D channel</td>
<td>CAC provides the wrong actuation</td>
<td>CAC provides the actuation in a wrong time</td>
<td>Not applicable</td>
</tr>
</tbody>
</table>
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)
Step 2: SFE Causes of Unsafe Control Actions from “set actuation command”

Controller: SFE

- acceleration is not supplied
- acceleration is not acquired
- UTL is not achieved
- the channel is not actuated
- the channel is actuated in a wrong time
- no feedback of the actuation channel

Control process: verify if the channels are actuated

A/D channels
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)