Safety Analysis of the Destruction System of a Sounding Rocket*

Rogério de Lemos, Computing Laboratory – University of Kent at Canterbury, UK

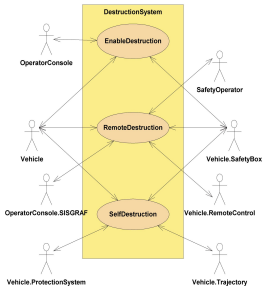
(*) Collaboration between the University of Kent at Canterbury and the Institute of Aeronautics and Space, in Brazil. Sponsored by British Council and CAPES/Brazil.

Sounding Rocket VS-40X

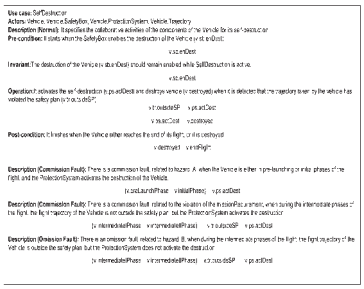
- The VS-40X is a two stages sounding rocket used for performing scientific experiments, and testing new equipment for the Brazilian Satellite Launcher (VLS).
- The self-destruction system automatically destroys the rocket when its trajectory violates a pre-defined flight envelope.

Sounding Rocket VS-40X

Use case DestructionSystem

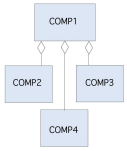


Use case SelfDestruction

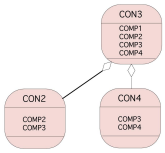


Co-operative Architectural Style

- Captures the collaborative behaviour between architectural components:
  - Components perform local computation (classes);
    - class diagrams describe the relationships between components.
  - Connectors encapsulate collaborative activity between the several components (CO actions);
    - CO action diagrams describe the relationships between connectors.

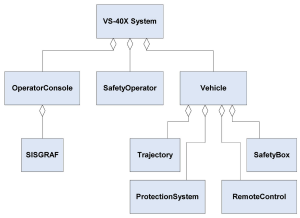


(i) Class diagram

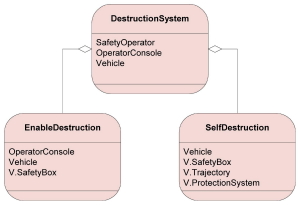


(ii) CO action diagram

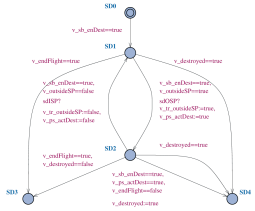
Class Diagram for the Destruction System



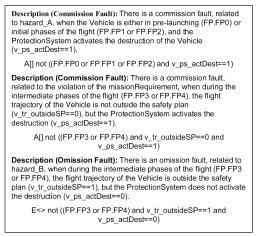
CO Action Diagram for the SelfDestruction



Validation of the Architectural Representation of SelfDestruction Using Model Checking



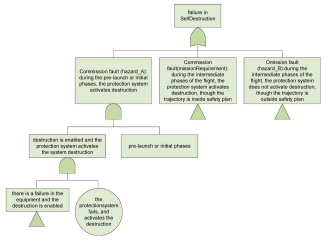
Operational model



Property model

Diversity in the Safety Arguments

- Fault trees analysis is employed for identifying component faults that could lead to the violation of either the safety or mission properties:
  - component failures in fault tree analysis are captured in the extended timed automata representation.



Fault Tree Analysis of SelfDestruction

For further information

Contact Rogério de Lemos (r.delemos@ukc.ac.uk), or visit website http://www.cs.ukc.ac.uk/people/staff/rdl/