Bridging the gap between systems engineering and safety and dependability analysis (RAMS)

The proliferation of innovative mission concepts together with the increasing concerns about sustainability of space operations brings the **safety and dependability** disciplines back to the backbone of systems engineering. Space missions providing critical services (such as communications, global positioning or monitoring for emergency response) require high availability, human flights and vehicles re-entering the atmosphere are subjected to strict safety policies, scientifical programs in outer space benefit from high reliability… and the overall increase of systems in orbit makes mandatory the adoption of mitigation and contingency measures to protect and preserve the space environment.

Considering all the above, the need to implement safety and dependability measures since early design phases becomes evident; usually these aspects will drive major aspects of the operational concepts and systems architectures of space programs. Unfortunately, from experience, these topics are often overlooked or kept aside until later phases of the development process once the major design tradeoffs have been frozen. An additional problem is that safety and dependability are sometimes kept out of the loop where the main design choices are made, reducing the scope of the discipline to a verification task where the objective is to assess that the system that has been designed complies with a set of requirements.

With the emergence of **Model Based Systems Engineering** (MBSE), our company, Anzen[1], has identified an opportunity to directly address these aspects from the mission concept and architectural models, offering new tools to systems engineers to tackle safety-related challenges all along the design and development process of complex space programs.

- Starting from the conceptual analysis of the mission, the safety framework allows to signal feared events and hazards, and identify mitigations to be implemented in the operational concept and the design of the system.
- At system architecture level, systems engineers could analyze the severity of functional hazards and determine the need for redundancies as well as setting reliability and availability objectives.
- Along the design and development phases, the framework allows to keep information up to date, and ensure consistency between design choices and results from dependability analysis. To that purpose, bridges between MBSE and domain-specific reliability and availability analysis tools are being implemented.

This work was initiated in 2022 after an initial research phase. Currently, an early demonstrator is available in Capella; and the team is just starting the analysis for the integration with the ESA SysML Solution. This framework, especially conceived to help systems engineers, RAMS and FDIR specialists; will cover topics such as Functional Hazard Analysis, reliability and availability budgets, Failure Modes and Effects Analysis (FMEA), Hardware Software Interaction Analysis (HSIA) among others.

Contact: Pablo López Negro
pablolopez@anzenengineering.com

[1] **Anzen Aerospace Engineering** is an ESA incubated company (ESA BIC Madrid Region, 2020-2022) that was born with the mission of improving system safety and dependability analysis, and to share methods, tools and good practices across different industries (aeronautics, advanced air mobility, defence, automotive …). Model Based Systems Engineering is a core discipline in Anzen; with a team committed to the development of a model-based framework, named ATICA, that allows running safety and dependability analysis directly from systems engineering models.