Redundancy Concepts for Minimum Mass and Acceptable Failure Protection

Lorenzo Bitetti [(1)], Olivier Rigaud [(1)], Régis De Ferluc [(1)], Gerald Garcia [(1)]

[(1)] *Thales Alenia Space, 100Bvd du Midi, BP99, 06156 Cannes La Bocca Cedex, France,*

CONTEXT

A R&T study has been performed in 2017-2018 by Thales Alenia Space for ESA (contract n° 4000119307/17/NL/PS/md) aiming at deriving a generic approach for a spacecraft performance-centred redundancy design. It will represent an alternative to the current full duplication of units allowing to avoid passive and non-operating redundancies and thus reducing the mass and costs of future missions.

The in-orbit return over experience has shown that some units have reliabilities higher than the expected ones and that several satellites remained in orbit for a period of time well beyond their expected lifetime. They have also showed good performances and behaviour even without ever using the redundant units. As a result, their redundant counterpart is often never used, which results in unused resources carried on-board that could have been retrospectively avoided.
In addition, maintaining full functionality of the spacecraft is not always necessary for some missions. Some of them have been partially or completely successful even after the occurrence of failures.

Finally, nowadays the usual strategy of adding redundancy to increase the reliability of a satellite and its mission success is challenged by the new missions that have more and more constraints in terms of mass budget, costs and time to market.

OBJECTIVE OF THE STUDY

The main objective of this study was therefore to derive a generic approach for a spacecraft performance-centred redundancy design alternative to the current full duplication in order to avoid passive, non-operating redundancies.

This new approach will be used to identify since early design phases, some opportunities to remove full redundant systems (when graceful degradation is possible) in order to comply with restrictive requirements in terms of mass, cost, complexity, reliability, safety. Note that graceful degradation is understood here as a degradation of performance that could be acceptable in case of failure in a no longer fully redundant S/C but still guaranteeing the success of part of or ideally the totality of the mission.

This will ideally allow to improve the design of future missions, that need to comply with more and more stringent constraints, and to derive when and how a change in the design philosophy from current fault tolerance thanks to the use of redundancies for each satellite unit to a functional redundancy could be possible in the space domain.

STUDY ORGANIZATION & ACTIVITIES

In order to achieve these objectives the whole study has been organized in three main phases:

- Task 1 : Assessing functionalities and performance against mission success criteria whose main activities have been :
  - to choose a reference study case among different missions;
  - to identify and map the functionalities and performance of the reference mission against its needs, constraints and success criteria;
  - and finally to identify where some graceful degradation could be accepted and therefore the redundancy schemes optimized.
- Task 2 : Approach for a spacecraft centred redundancy design - Case study assessment whose main activities have been :
  - to identify a list of candidate solutions for the redundancies removal and/or functional redundancies on the reference study case;
  - to determine the impact on the mission and the degradation of performances in case of failure from a system, dependability, fault management and operations points of view;
  - to conclude on the applicability and interest of the evaluated candidate solutions for the reference case of this study.
- Task 3 : Approach for a spacecraft centred redundancy design - Methodology definition whose main activities have been to define:
  - a generic approach to eliminate redundant units and to identify satellite resources implementing functional redundancies;
  - a generic methodology for the definition and allocation of reliability requirements that would take into account also possible graceful degradations and system needs;
  - a generic approach to an alternative fault management strategy when redundancies are removed and/or functional redundancies are implemented.

STUDY RESULTS

A LEO constellation has been chosen in **[1]** as the reference study case. This choice has been justified by the fact that, being a constellation, redundancy removal is of high interest for system engineers and, at the same time, can be more easily accepted by dependability ones. In fact, the reliability and availability of the constellation are linked not only to the reliability/availability of each satellite but also to the whole constellation design. Therefore

some redundancies could be removed while still guaranteeing the compliance with the client needs and other requirements (e.g. those related to end of life disposal regulations).

The mission goals, the required performance, functionalities and satellite design of the reference study case have been then described in detail in **[1]**. While mapping the functionalities to the physical architecture of the satellite, some performance degradations and opportunities for redundancy removal have been identified.

The analyses have been described firstly with a classical 'document-based' approach and then with a Model Based approach. The open source Capella tool **[4]**, based on Arcadia approach **[5]**, has been used for this purpose. It has supported the system engineering activities required in the first phase of the study : from the definition of the system needs to the selection of the physical architecture, through functional analyses and mapping of functionalities against the mission success and the physical components.

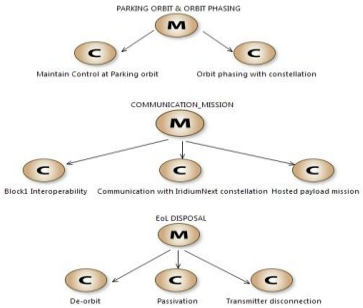

Figure 1 : Example of Mission sub-phases and System Capabilities

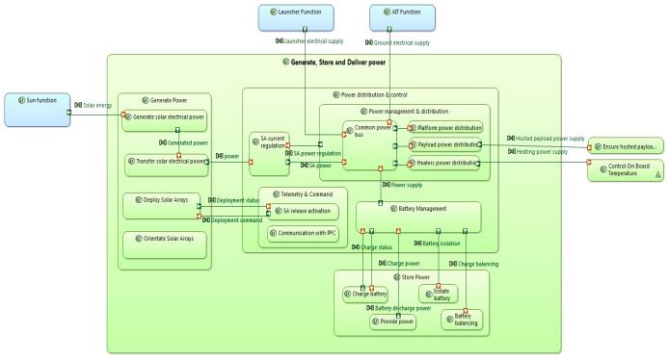

Figure 2 : Example of Functions and functional exchanges between System and Actors Functions

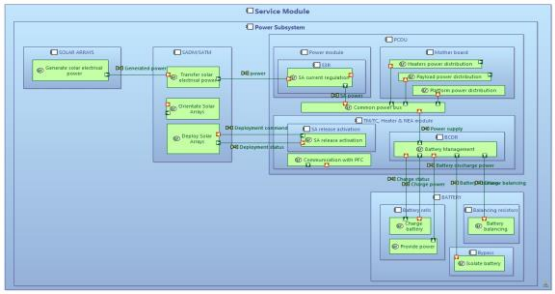

Figure 3 : Example of mapping of Logical Functions to Logical Components (Electrical Power Subsystem case)

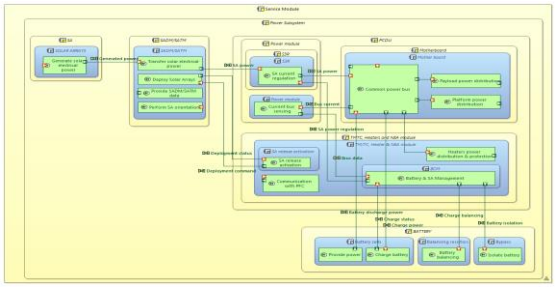

Figure 4 : Example of Physical architecture (Electrical Power Subsystem)

While using these models for the system engineering activities, it has been derived that some of the Capella features could also support and improve the current dependability process.

In this sense a new Capella viewpoint dedicated to Reliability analyses has been implemented. This preliminary version allows to compute the reliability figures of a function or of the whole system starting from the Capella model realized by system engineers (see **Figure 3**) and the reliability information filled by dependability engineers (see **Figure 5**).

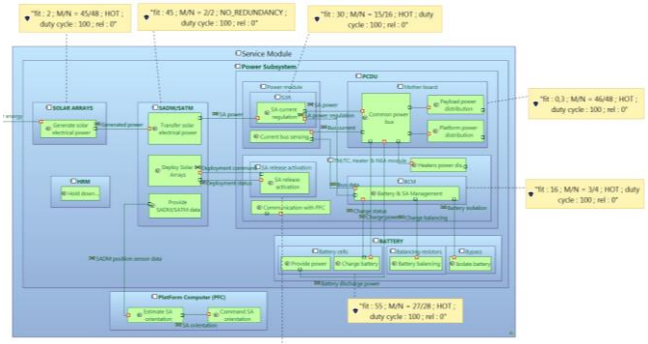

Figure 5 : Example of Capella model with the information allowing to compute the reliability (Electrical Power Subsystem case)

The Capella viewpoint provides as an output a table that gathers all the reliability parameters in a structured way and that can be then exploited by the already existing dependability tools based on Excel, as shown in **Figure 6**.

S/System	Equipment	Mission redundancy %	PIT on	PIT off	PIT ratio	N	k	type	Reliability
EPS	Solar Array	100	2	0	2	45	48	A	1,0000
	SADM / SATM	100	45	6	45	2	2	A	0,9945
	Battery cell	100	55	6	55	27	28	A	0,9959
	PCDU S3R	100	30	3	30	15	16	A	0,9996
	PCDU BCM	100	16	2	16	3	4	A	1,0000
	PCDU Battery switch	100	18	2	18	6	8	A	1,0000
	PCDU SA release	0	2111	211	211	1	2	A	1,0000
	PCDU Main bus	100	0,3	0	0	46	48	A	1,0000
	PCDU TM/TC	100	140	14	140	1	2	A	0,9999
	PCDU TM/TC I/F	100	7	1	7	1	2	A	1,0000
	PCDU Heater distr	100	626	63	626	1	2	P	0,9992
	PCDU TLM Ibat/Ibus/Isa	100	15	1	15	1	2	P	1,0000

Figure 6 : Example of reliability model in Excel derived from Capella Reliability Viewpoint (Electrical Power Subsystem case)

Thanks to this Reliability viewpoint and those already existing (Mass, Cost and Performance) Capella could be used to easily and quickly compare different architectures proposed during the early phases of the satellite development and to choose the best one from both system engineering and dependability points of view.

In **[2]** the approach for a spacecraft centred redundancy design has been derived and applied on the reference study case. System engineering, dependability and fault management trade-off criteria have been defined and then evaluated for each candidate solution. Then a weight has been assigned to each trade-off criterion depending on its importance on the multi-disciplinary trade-offs.

Finally the total weighted score has been computed for each candidate in order to conclude if the solution can be accepted, discarded or to be further evaluated for the reference study case

It has been demonstrated that the proposed approach is valid and useful. In fact, for those solutions already applied or discarded on the reference study case, this approach has led to the same conclusions and recommendations.

In addition, other solutions that could have led to even higher mass and costs reductions while being still compliant with the satellite reliability figures have been found. For some of these solutions a modification of the fault management strategy and/or ground operations would have been necessary in order to guarantee the success of the mission even in case of failure.

This approach for redundancy removal has been then generalised in **[3]** to any kind of mission. An Excel tool has been also implemented in order to support all the following steps :

- selecting the type of mission (see Figure 7) and evaluating its needs, constraints, performance and mission success criteria;
- choosing the weight for each criterion (see Figure 8);
- assigning a score to each candidate solution;
- computing the total weighted sum;
- concluding on the solution acceptability (see Figure 9) depending on the mission properties and the solution benefits and limits.

Mission design and properties	Choice
Orbit	LEO
Mission duration	between 5 and 10 years
Mission configuration	large/mega constellation
Application	telecommunication
Propulsion subsystem	electrical only
Electrical Power subsystem	SA + SADM (2 wings)

Figure 7 : Example of mission inputs selection

Mission needs / constraints	Weight
Mission success	2
Acceptable performance degradation	2
Required mass gain	2,5
Required costs gain	3
Required satellite reliability & safety	1,5
Required fault management	1,5
Operations workload & constraints	2
Availability requirement	2

Figure 8 : Example of mission needs/constraints and weights selection

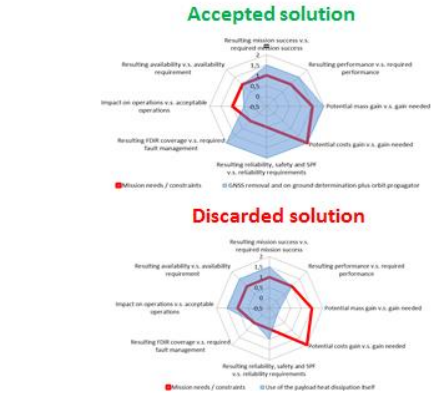

Figure 9 : Example of graphical outputs of the Excel file supporting the generic methodology

In parallel, also a generic methodology for the reliability definition and allocation has been derived in **[2]**. For the requirements definition the main conclusions and recommendations of a previous ESA R&D study **[6]**, where this topic has been addressed in details, have been used.

For the reliability allocation, an approach has been proposed taking into account both functional aspects (contribution of each functional chain to the overall success of the mission, acceptable graceful degradations) and physical ones (mass and cost objectives, previous or feasible redundancy schemes, etc.).

The main goal has been to specify the reliability requirements to each subsystem, and thus to select the corresponding redundancy schemes, so that the overall mass and costs of the satellite could be optimized while achieving the required reliability goal. A proof-of-concept of a mass-cost-reliability optimization tool supporting this methodology has been implemented and its feasibility and interest demonstrated with preliminary data. (see Figure 10).

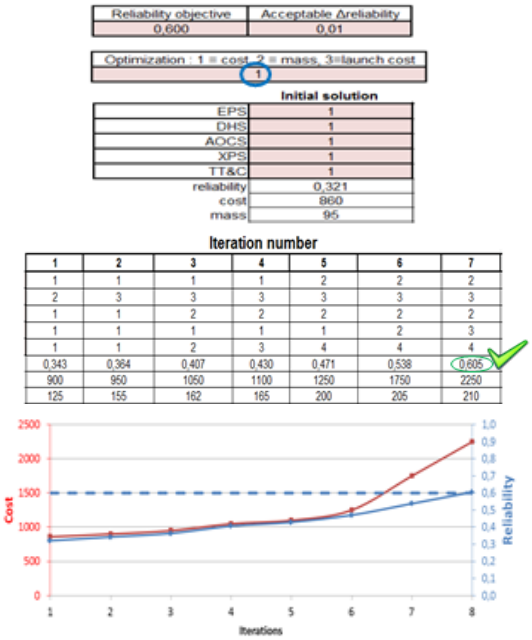

Figure 10 : Example of application of the mass-cost-reliability optimization tool

CONCLUSION AND PERSPECTIVE

All the activities of this study have been achieved with success and the main objectives have been fulfilled. A generic approach has been derived for a satellite redundancy design alternative to the current full duplication of units that has shown its limits or at least some axes of improvements for the future. The main conclusions and recommendations provided by this study are summarized hereafter. It has been derived that in order to optimize the redundancy schemes of future satellites, and thus also their mass, costs and time to market:

- it is indispensable to have a precise evaluation and specification of the different sub-missions, their contribution to the overall success of the mission and the performance degradations that can be accepted;
- both functional and physical aspects have to be considered in the reliability allocation process
- only limited mass and costs gains can be achieved at satellite level by removing some redundancies and still guaranteeing an acceptable reliability figure. Reductions higher than those linked to the removal of redundancies could be probably achieved with new technologies or by challenging the current philosophy on the design margins.

In addition, some future improvements and applications have been identified for the promising approaches identified in the frame of this study:

- The **Model Based approach** is expected to improve the current dependability tools, the co-engineering activities and the links between all the stakeholders involved in the satellite development process.

  Other RAMS activities could be supported by the open-source Capella tool in addition to the preliminary Reliability viewpoint developed in the frame of this study. This will help performing multi-disciplinary analyses and better evaluating the impact of design choices from different points of view since the early phases of the project.

- The **mass-cost-reliability optimization tool**, currently being a proof-of-concepts, could support Concurrent Design Facilities (CDF) activities. For instance to achieve a given reliability figure while optimizing (limiting) the cost and/or the mass of the satellite; and to evaluate the impact of different reliability requirements on the overall mass and costs.

  This tool could be improved in the future to take into account also the severity and availability of different architectures, and linked to the Model Based tools.

To conclude, it is recommended to follow this generic approach for a spacecraft centred redundancy design, and to further evaluate the aforementioned promising solutions and proof-of-concepts in future studies.

REFERENCE

[1] TN1 : Determination and assessment of current redundancy approaches and associated rationale. 0005-0008764381

[2] TN2 : Approach for spacecraft performance centred redundancy design – Case study assessment. 0005-0009448946

[3] TN3 : Approach for spacecraft performance centred redundancy design – Methodology definition.

[4] CAPELLA : Model Based System Engineering tool. https://www.polarsys.org/capella/ index.html

[5] ARCADIA : Model Based System Engineering (MBSE) method: https://www.polarsys.org/capella/arcadia.html

[6] Approach for Quantitative RAMS requirements definition and flow-down. TASF-RAMS-0010