Research paper

Space systems resilience optimisation under epistemic uncertainty

Gianluca Filippi[a,*], Massimiliano Vasile[a], Daniel Krpelik[b], Peter Zeno Korondi[c,d], Mariapia Marchi[c], Carlo Poloni[c,d]

[a] *Aerospace Centre of Excellence, University of Strathclyde, 75 Montrose Street, G1 1XJ, Glasgow, United Kingdom*
[b] *Department of Mathematical Sciences, Durham University, Lower Mountjoy, Stockton Rd, Durham, DH1 3LE, United Kingdom*
[c] *ESTECO S.p.A, Building B, 99 Padriciano, Area Science Park, Trieste, 34149, Italy*
[d] *Department of Engineering and Architecture, University of Trieste, Piazzale Europa, 1, 34127, Trieste, Italy*

ARTICLE INFO

Keywords:
Epistemic uncertainty
Resilient satellite
Complex systems
Evidence theory

ABSTRACT

This paper introduces the concept of Resilience Engineering in the context of space systems design and a model of Global System Reliability and Robustness that accounts for epistemic uncertainty and imprecision. In particular, Dempster-Shafer Theory of evidence is used to model uncertainty in both system and environmental parameters. A resilience model is developed to account for the transition from functional to degraded states, and back, during the operational life and the dependency of these transitions on system level design choices and uncertainties. The resilience model is embedded in a network representation of a complex space system. This network representation, called Evidence Network Model (ENM), allows for a fast quantification of the global robustness and reliability of system. A computational optimisation algorithm is then proposed to derive design solutions that provide an optimal compromise between resilience and performance. The result is a set of design solutions that maximise the probability of a system to recover functionalities in the case of a complete or partial failure and at the same time maximises the belief in the desired target value of the performance index.

1. Introduction

With the increase in computing power, more and more sophisticated numerical methods have been applied to solve problems of increasing complexity. In the classical approach to engineering design, *Design by Formula*, the active work of engineers was required throughout the whole design process. In the more recent *Design by Analysis* [1] approach, the development of software analysis tools (numerical methods) shortened the design process and enabled a better understanding of the problem without the use of expensive experimental analyses. The design and associated decision-making process were still performed by engineers, but the analysis of different configurations was automatised by numerical procedures. A further advancement was introduced with *Design by Optimisation* [2,3], where numerical optimisation tools were coupled with numerical simulations to automatically identify globally, or locally, optimal design solutions. Finally, in the last two decades an increasing attention has been devoted to tackle optimisation under uncertainty. *Design for Reliability and Robustness* and more in general Multi-Disciplinary Design (MDO) under Uncertainty [4–13] is radically changing systems engineering, making designers and decision makers able to handle higher degrees of complexity.

This paper proposes a further methodological advancement with specific application to the design of space systems. Space systems are complex systems that involve multiple interconnected components and disciplines with complex couplings: payload, structure, thermal analysis, attitude, control, etc. A system level optimal solution cannot be found by optimising the single subsystems independently. Furthermore, the design and optimisation of space systems have to account for uncertainty, in particular in the early design phase, given the required robustness, reliability and resilience of these systems.

The most common and well-established approach to handle uncertainty in space systems engineering is to use safety margins and redundancies [14–16]. These traditional methods, however, lack an appropriate quantification of uncertainty. As a consequence, there can be an overestimation or an underestimation of the effect of uncertainty which can lead to either an increase in costs and development time or to the occurrence of undesirable events. As it was recognised during the Columbia Accident Investigation Board (CAIB) [17], the classic pattern that brings to failure, common to many other tragic accidents [18], is the combination of production pressure, that pushes to reduce the safety margins, and a fragmented problem solving that lacks a system level understanding. Systems engineering can address the required

[*] Corresponding author.

E-mail addresses: g.filippi@strath.ac.uk (G. Filippi), massimiliano.vasile@strath.ac.uk (M. Vasile), daniel.krpelik@durham.ac.uk (D. Krpelik), korondi@esteco.com (P.Z. Korondi), marchi@esteco.com (M. Marchi), poloni@esteco.com, poloni@units.it (C. Poloni).

Acronyms

AOCS	Attitude and Orbit Control Subsystem
bpa	basic probability assignment
DSM	Design Structure Matrix
DST	Dempster Shafer Theory
EBRO	Evidence-Based Robust Optimisation
ENM	Evidence Network Model
FE	Focal Element
IDEA	Inflationary Differential Evolution Algorithm
LEO	Low Earth Orbit
OBDH	On-board Data Handling
TTC	Telemetry, Tracking and Command

holistic view on system performance and evolution [19,20] but the proper quantification of margins requires integrating rigorous uncertainty quantification techniques in the context of systems engineering.

If one looks at the different types of uncertainty that a system can be subject to, two macro-categories can be identified: *aleatory uncertainty* and *epistemic uncertainty* [21]. Aleatory uncertainty is natural randomness which cannot be reduced. Epistemic uncertainty is due to the lack of information or incomplete data. This type of uncertainty is reducible by acquiring more knowledge on the problem. In this work we model epistemic uncertainty by means of Dempster-Shafer theory of evidence (DST) [22–24] which offers a natural way to assign degrees of belief to the expected performance of a system. Recent examples of the application of system-level optimisation principles, including uncertainty, to the design of space systems can be found in Refs. [25,26]. Note however, that the former proposes an exponentially complex computational method that cannot be used for large scale systems while the latter does not include epistemic uncertainty.

This paper takes a further step forward and proposes an approach to Resilience Engineering in the context of space systems. Our proposed concept of Resilience Engineering extends and integrates the concepts of Design for Reliability and Design for Robustness and introduces the use of DST to model epistemic uncertainty. The idea is that a resilient system should be able to endure disturbances and recover from shocks [18,27–29] while maintaining an optimal level of performance and functionalities. In other words, the system is expected to transition between different potentially degraded states but without losing the ability to maintain or recover, in full or in part, its functionalities and associated performance. In this sense, the concept of resilience, that we will develop in this paper, blends elements of robustness and reliability. In this framework, the aim of resilience engineering is to maximise performance and resilience at the same time. This can be translated into finding the design solution that maximises the level of performance and active functionalities under the effect of uncertainty that affects the transition to multiple states.

The ability to endure disturbances can be engineered by maximising robustness. In particular, one could be interested in the worst case scenario in which the effect of uncertainties is maximum. In mathematical terms, robustness can be translated into a deterministic min-max optimisation problem [6] that aims at maximum performance in the worst case scenario. This aspect is here complemented with the ability to recover after shocks. A shock can be seen as a probabilistic transition to a degraded state. A system reliability model is then introduced to quantify these transitions and relate them to the design solutions. As an example, we consider the design of a satellite (but these concepts have a broader applicability). The reliability model mixes random occurrences (aleatory) of both *disaster* and *repair* events, during the satellite lifetime, and transitions from fully functional to degraded states (and back) that depend on design solution and epistemic uncertain parameters. The satellite is modelled as a finite multi-state system and the stochastic transitions between states are described as a Homogeneous Continuous Time Markov Chain (HCTMC) [30]. Both performance and reliability are assumed to depend on a number of uncertain and design system parameters. In the preliminary design phase, this uncertainty is epistemic in nature and thus is here modelled with DST. The reliability model is then integrated into the worst-case scenario optimisation problem by formulating and solving a constrained min-max problem under epistemic uncertainty [31].

Then, an *Evidence Network Model* (ENM) is proposed to represent a complex space system with multiple, coupled subsystems and disciplines. This representation allows one to explore techniques to reduce the computational complexity of evaluating the resilience and robustness of the system. In this model, each node is a subsystem (or component) and each link shares information between pairs of subsystems (or components). Although it is customary in multi-disciplinary design optimisation to represent a system as a set of connected components that exchange information through connecting links (see Ref. [32] for an example of multi-disciplinary optimisation under uncertainty with Evidence Theory) in an ENM the specific properties of the nodes and the form in which they exchange information is such that Belief functions can be computed in polynomial time. The properties of an ENM and the difference with respect to common MDO [33,34] formulations will be explained in Sec. 6. The ENM formulation was first introduced in Ref. [35]. The method was extended in Ref. [36] to make ENM computationally more efficient. Ref. [37] finally introduced a time-dependent reliability measure in the ENM.

This work extends the ENM and the results in Ref. [37] with a resilient-measure approach. The applicability of the proposed method to space systems engineering is demonstrated through the preliminary design of a small satellite in Low Earth Orbit (LEO). The goal of the satellite is to take pictures of the Earth. The satellite is assumed to be composed of 5 subsystems, each of which is subjected to epistemic uncertainty.

The rest of the paper is organised as follows. Section 2 introduces the concept of Resilience Engineering. The proposed resilience model is presented in Section 3. Section 4 introduces the framework of DST to model uncertainties. Section 5 describes the concept of Evidence-Based Robust Optimisation (EBRO) for the design of complex systems under epistemic uncertainty. The details of the worst-case optimisation approach is described in Section 5.1. In Section 6 the ENM is introduced. The satellite design problem is detailed in Section 7. In particular Section 7.1 presents the mathematical models for the subsystems, in Section 7.2 the resilience model is applied, Section 7.3 presents the formulation of the optimisation problem and Section 7.4 applies the ENM. Finally, the results of the case study are presented and evaluated in Section 8.

2. Resilience engineering

The concept of Resilience Engineering is relatively recent and derives from two decades of research that has first tried to formalise the definition of resilience and then developed methods to model and quantify the resilience of systems [27–29,38]. Resilience Engineering takes a step forward and attempts to make systems resilient by design. In this section, we provide our definition of resilience and an overview of our approach to design space systems so that their resilience and performance are jointly optimised.

Resilience is here defined as the ability of a system to endure disturbances or regain a desirable operational state after the occurrence of a shock. The former characteristic of resilience is directly connected to the robustness of the system. Hence in the following, we will propose an approach to enhance robustness when the possible disturbances are captured by a model of epistemic uncertainty. The latter characteristic of resilience can be quantified by measuring the degree of recovery of system performance, over time, after a failure [27]. We will then propose a global system reliability model that relates the epistemic uncertainty in system and environmental parameters and the design choices to the transition between different functioning states. Thus, our concept of Resilience Engineering, combines robustness and reliability with a time component that accounts for the temporal variation of system performance and the response to disturbances and shocks.

The uncertainties in system characteristics and environment are deemed to be epistemic in nature and are modelled with DST as the underlying assumption is that they cannot be captured by a known probability distribution. This uncertainty model is applied to a graph representation of the space system, i.e. the ENM. We then quantify the values of the performance indexes of the ENM by propagating the effects of the epistemic uncertainties through the network and the global reliability model.

We then use an optimisation method to identify those design choices that maximise performance, over a given operational time, when this performance is affected by disturbances and the possible intervention of multiple disruption and recovery events.

3. Resilience model

In this section, we introduce a method for modelling possible functionality impairments and restorations for a space system. We assume a random occurrence of both *disasters* and *repairs* during the satellite mission. The satellite is modelled as a (finite) multi-state system and its performance, both instantaneous and cumulative, depends on its state and trajectory. The stochastic transitions among states are described as a Homogeneous Continuous-Time Markov Chain (HCTMC).

We denote the set of possible states of the satellite by $\mathscr{X}$ and the satellite trajectory in this state space by a stochastic process X: $\mathbb{T} \to \mathscr{X}$, where $\mathbb{T}$ is the temporal dimension. A stochastic process is uniquely determined by an initial distribution over the state space, say P_0, and a family of conditional distributions, the transition operators, $\{P(X(t)|X(s))\}$ where $\{s, t\} \in \mathbb{T}$.

In the case of HCTMC processes, the specification can be simplified [30]. HCTMC is uniquely determined by its *transition rate matrix*, $Q \in \mathbb{R}^{|\mathscr{X}|\times|\mathscr{X}|}$, which is an analogue to the derivative in the theory of ordinary differential equations. If the non-diagonal elements of a transition rate matrix are non-negative and the sum of elements in each row is zero, it induces a family of transition operators of the form:

$$P(X(t) = x|X(s) = y) = \exp(Q(t - s))(y, x), \tag{1}$$

where exp denotes a matrix exponential. The probability of obtaining state x at time t, can then be evaluated by:

$$P(X(t) = x) = \sum_{y\in\mathscr{X}} P_0(y)\exp(Qt)(y, x). \tag{2}$$

Suppose that our performance measure, which is to be optimised, is a cumulative performance, $V_T = \int_0^T V(t)dt$, over the mission time T, and that the immediate performance $V(t)$ depends on the state of the satellite at the respective time, $X(t)$. Since X is a stochastic process, $V(t)$ and the cumulative performance V_T become random variables. In order to formulate a real valued objective function for the optimisation problem, we need to take the stochastic character of V_T into account. The objective function can be replaced by a real functional on the underlying probability space. We choose it to be the expected value, thus the objective function becomes:

$$f_V(\mathbf{d}, \mathbf{u}) :=\mathbb{E}\left\{\int_0^T V(t, X(t); \mathbf{d}, \mathbf{u})dt\right\}, \tag{3}$$

where $V(t, X(t); \mathbf{d}, \mathbf{u})$ emphasises the dependency of the immediate performance on the system state, a set of design parameters (or design choices) $\mathbf{d}$, and a set of uncertain parameters $\mathbf{u}$. Due to the Fubini's theorem [39], we can switch the order of integrations to obtain:

$$f_V(\mathbf{d}, \mathbf{u}) = \int_0^T \mathbb{E}\{V(t, X(t); \mathbf{d}, \mathbf{u})\}dt. \tag{4}$$

Because the set of system states, $\mathscr{X}$, is finite, Eq. (4) attains its final form:

$$f_V\left(\mathbf{d}, \mathbf{u}\right) = \int_0^T \sum_{x\in\mathscr{X}} \left\{V\left(t, x; \mathbf{d}, \mathbf{u}\right)P\left(X(t) = x\right)\right\}dt. \tag{5}$$

Eq. (5) implies, that we can calculate the objective function in two steps. First, solve the stochastic process $X(t)$, and second, integrate the performance with pre-calculated values of $P(X(t))$. If the immediate performance function is defined to be discrete in time, the integration into the expected cumulative performance in Eq. (5) will become a summation with respect to a counting measure.

4. Evidence framework for epistemic uncertainty

A key aspect of this work is that uncertainties in system and environment parameters are deemed to be epistemic in nature and cannot be quantified by precise probability distributions. In order to capture this imprecision and lack of knowledge we propose the use Dempster-Shafer Theory of Evidence. DST has been shown to be a useful tool to model uncertainty in a number of engineering applications [22–24]. Here we take advantage of the fact that DST can associate a degree of belief in the realisation of a given event without a precise quantification of the probability of that event to occur. This quantification is particularly useful in the early design phase when decisions are affected by a fundamental lack of information on system characteristics and subjective statements. We assume that the sources of information for each system and environment parameter are independent and uncertainties are uncorrelated. This assumption is reasonable in most of the cases and one can reduce to independent sources by a proper model parameterisation.

Given an event space, the set Θ of all the mutually exclusive and collectively exhaustive elementary events (or hypotheses) $\Theta = \{\theta_1, \theta_2, \ldots, \theta_i, \ldots, \theta_{|\Theta|}\}$ is considered. The different available sources of evidence are treated independently in this paper. The collection of all non empty subsets of Θ is the Power Set $2^\Theta = (\Theta,\cup)$. One can now assign a probability mass, called basic probability assignment (*bpa*), to the elements of 2^Θ. Each element of 2^Θ with a non-zero *bpa* is called a *Focal Element* (*FE*) and is represented with the symbol γ in the following. The pair $\langle \Gamma, bpa_\Gamma \rangle$ - where $\Gamma \ni \gamma$ and $bpa_\Gamma \ni bpa_\gamma$ - is called the *Body of Evidence*.

We call the power set $U = 2^\Theta$ the *Uncertain Space*. We can now define the performance index of the system we want to analyse as:

$$f(\mathbf{d}, \mathbf{u}) \colon D \times U \subseteq \mathbb{R}^{m+n} \to \mathbb{R} \tag{6}$$

where D is the design space for the decision or design parameters $\mathbf{d}$, of dimension n, and U the event space for the uncertain parameters $\mathbf{u}$, of dimension m.

DST measures the influence of uncertainty on the quantity f, for a fixed design vector $\mathbf{d}^*$, by means of two functions, *Belief* and *Plausibility*, that generalise the concept of Probability measure given in classical probability theory. If we are interested in the amount of evidence associated to the event $f(\mathbf{d}, \mathbf{u}) \in \Phi$ we can define

$$\Omega = \{\mathbf{u} \in U | f(\mathbf{d}, \mathbf{u}) \in \Phi\} \tag{7}$$

as the corresponding set in U and then compute the cumulative Belief and Plausibility associated to that event:

$$Bel(\Omega) = \sum_{\gamma_i \subset \Omega, \gamma_i \in U} bpa(\gamma_i), \tag{8}$$

$$Pl(\Omega) = \sum_{\gamma_i \cap \Omega \neq 0, \gamma_i \in U} bpa(\gamma_i). \tag{9}$$

From Eqs. (8) and (9) we can state that the belief in the realisation of the event $f(x) \in \Phi$ is the sum of the *bpa* of all the FEs totally included in Ω, while the Plausibility is the sum of all the FEs that have a non-null intersection with Ω. More details about the DST can be found in Ref. [24].

5. Evidence-based robust and resilience optimisation

Given the performance index f in (6), Evidence-Based Robust Optimisation aims at finding the decision vector $\mathbf{d}^*$ that maximises the Belief in statement (7), given a body of evidence, and optimises the set Φ. The concept was introduced by the authors in Ref. [40] and extended in Ref. [41]. In this section, we present the basic unconstrained formulation and its extension to include constraints.

If Φ is the set $\Phi = \{f \leq \nu\}$ then one can assume, without loss of generality, that the function f in (6) has to be minimised. Then Eq. (7) translates into:

$$\Omega = \{\mathbf{u} \in U \mid f(\mathbf{d}, \mathbf{u}) \leq \nu\}. \tag{10}$$

The idea is then to find a solution to the problem:

$$\begin{aligned} &\max_{\mathbf{d} \in D} Bel(f(\mathbf{d}, \mathbf{u}) \leq \nu) \\ &\min_{\nu \in \mathbb{R}} \nu \end{aligned} \tag{11}$$

Problem (11) requires the evaluation of the Belief in statement (10) for multiple $\mathbf{d}$ vectors and ν scalars. In the general case the set Ω changes with both $\mathbf{d}$ and ν and needs to be recalculated together with the max and min values of f within each focal element in Ω. In the presence of constraints of the form $C \leq 0$ one has to consider the further statement:

$$\Omega_C = \{\mathbf{u} \in U \mid C(\mathbf{d}, \mathbf{u}) \leq \nu_C\} \tag{12}$$

with associated $Bel(C(\mathbf{d}, \mathbf{u}) \leq \nu_C)$. Problem (11) can be augmented to include a hard condition on the belief that the constraints are satisfied:

$$\begin{aligned} &\max_{\mathbf{d} \in D} Bel(f(\mathbf{d}, \mathbf{u}) \leq \nu) \\ &\min_{\nu \in \mathbb{R}} \nu \\ &Bel(C(\mathbf{d}, \mathbf{u}) \leq \nu_C) > 1 - \varepsilon \end{aligned} \tag{13}$$

Problem (13) is equivalent to general mixed robustness-reliability formulations and presents the difficulty of calculating the two Belief values associated to objective function and constraints. In the literature on Reliability Based Optimisation some authors proposed methods to efficiently solve the constraint in (13) by introducing hypotheses on the local differentiability of the constraint functions, the existence of a Most Probable Focal Element (MPFE) or by a form of probabilistic approximation of the belief functions [22,42,43] to speed up the calculation of an approximation of *Bel*. Besides focusing their attention mainly on the constraint satisfaction all these methods do not exploit the properties of the complex system and are restricted by the assumptions on the MPFE and local differentiability of the constraint functions. Among all vectors $\mathbf{d}$ that solve problem (13) the most critical one, $\mathbf{d}^*$, corresponds to the minimum values of ν and ν_C such that $Bel(f(\mathbf{d}, \mathbf{u}))$ is maximum and $Bel(C(\mathbf{d}, \mathbf{u}) \leq \nu_C))$. We call the search for $\mathbf{d}^*$, worst-case scenario optimisation in the following. Solving for the worst-case scenario renders the optimisation problem independent of the uncertainty quantification method, has a complexity that is independent of the number of focal elements and does not require any particular assumption on the constraint functions.

5.1. Worst-case scenario optimisation

The worst-case scenario optimisation introduced in the previous section can be translated into the following constrained min-max problem:

$$\begin{aligned} &\min_{\mathbf{d} \in D} \max_{\mathbf{u} \in U} f(\mathbf{d}, \mathbf{u}) \\ &s.\ t. \\ &\forall\ \mathbf{u} \in U\colon C(\mathbf{d}, \mathbf{u}) \leq 0, \end{aligned} \tag{14}$$

where f is the objective function (or performance index) and C is the constraint function. Problem (14) seeks for the decision vector $\mathbf{d}$ that minimises the maximum value of f over the uncertainty space U while guaranteeing that the constraints are always satisfied for all possible values of $\mathbf{u}$. Following the approach in Ref. [41] before tackling problem (14) the uncertainty space U is mapped to a unit hyper-cube via an affine transformation. In this way, one can easily apply a population-based global search algorithm to the solution of (14) as every sample in the unit hyper-cube is directly mapped into one focal element belonging to U.

The solution approach is summarised in Algorithm 1 and explained in the following. For more details on the convergence of the method please refer to Ref. [44].

In line 1 of Algorithm 1 the design point is initialised (randomly if there is no initial information) and the corresponding feasible worst solution is evaluated. In line 2 the archives are defined: A_u for the $\mathbf{u}$ vector of the worst-case scenarios, A_c for the $\mathbf{u}$ vector of the maximum value of the constraints and A_d for the $\mathbf{d}$ vector of the optimal design solutions. Then, outer and inner loops are alternated until the number of function evaluations is lower than the maximum allowed number N_{feval}^{max}.

In the outer loop (lines 5–7), a constrained minimisation of the objective function f over the design space is evaluated in the worst-case between the uncertainty vectors (scenarios) stored in an archive $A = A_u \cup A_c$:

$$\begin{aligned} &\min_{\mathbf{d} \in D} \max_{\mathbf{u} \in A} f(\mathbf{d}, \mathbf{u}) \\ &s.\ t. \\ &\max_{\mathbf{u} \in A} C(\mathbf{d}, \mathbf{u}) \leq 0 \end{aligned} \tag{15}$$

Line 7 updates the A_d archive with the solution $\underset{\mathbf{d} \in D}{\operatorname{argmin}} \max_{\mathbf{u} \in A} f(\mathbf{d}, \mathbf{u})$.

Algorithm 1
Constrained minmax

```
1: Initialise $\bar{\mathbf{d}}$ and run $\mathbf{u}_a = \operatorname{argmax} f(\bar{\mathbf{d}}, \mathbf{u})$ s.t. $C(\bar{\mathbf{d}}, \mathbf{u}) \leq 0$
2: $A_u = A_u \cup \{\mathbf{u}_a\}$; $A_c = \varnothing$; $A_d = \varnothing$
3: while $N_{fval} < N_{fval}^{max}$ do
4:   Outer loop:
5:   $\mathbf{d}_{min} = \underset{d \in D}{\operatorname{argmin}}\{\max_{\mathbf{u} \in A_u \cup A_c} f(\mathbf{d}, \mathbf{u})\}$s.t.
     $\max_{u \in A_u \cup A_c} C(\mathbf{d}, \mathbf{u}) \leq 0$
6:   $A_d = A_d \cup \{\mathbf{d}_{min}\}$
7:   Inner loop:
8:   $\mathbf{u}_{a,f} = \underset{\mathbf{u} \in \mathbf{U}}{\operatorname{argmax}} f(\mathbf{d}_{min}, \mathbf{u})$s.t.$C(\mathbf{d}_{min}, \mathbf{u}) \leq 0$
9:   $\mathbf{u}_{a,C} = \operatorname{argmax}_{u \in U} C(\mathbf{d}_{min}, \mathbf{u})$
10:   $A_u = A_u \cup \{\mathbf{u}_{a,f}\}$
11:   if $N_{fval} < N_{fval}^{\varepsilon} \vee \exists\ \mathbf{d} \in A_d$ t.c. $\max_{u \in U} C(\mathbf{d}, \mathbf{u}) \leq 0$ then
12:     if $C(\mathbf{d}_{min}, \mathbf{u}_{a,C}) > 0$ then
13:       $A_c = A_c \cup \{\mathbf{u}_{a,C}\}$
14:     end if
15:   else
16:     update $\varepsilon$
17:     $A_c = \{A_c \setminus \mathbf{u}_{a,C}^i\ \ s.\ t.\ \ C(A_d^i, \mathbf{u}_{a,C}^i) \leq \varepsilon\}$
18:     if $C(\mathbf{d}_{min}, \mathbf{u}_{a,C}) > \varepsilon$ then
19:       $A_c = A_c \cup \{\mathbf{u}_{a,C}\}$
20:     end if
21:   end if
22: end while
23: Cross-check between $A_d$, $A_u$ and $A_c$.
24: Return $[\mathbf{d}_{minmax}, \mathbf{u}_{minmax}]$
```

In the inner loop (lines 9–11) two optimisations are run in parallel over the uncertain parameters $\mathbf{u} \in U$ for the fixed design vector $\mathbf{d}_{min}$

found in the outer loop, a constrained maximisation of the cost function f and a maximisation of the constraint function:

$$\max_{\mathbf{u}\in U} f(\mathbf{d}_{min}, \mathbf{u}) \\ s.\ t. \\ C(\mathbf{d}_{min}, \mathbf{u}) \le 0 \tag{16}$$

$$\max_{\mathbf{u}\in U} C(\mathbf{d}_{min}, \mathbf{u}). \tag{17}$$

Lines 12–16 update the archives previously defined with the solutions of inner loop: $\mathbf{u}_{a,f} = \underset{u\in U}{\text{argmax}} f(\mathbf{d}_{min}, \mathbf{u})$ is added to the archive A_u and $\mathbf{u}_{a,C} = \underset{u\in U}{\text{argmax}}\, C(\mathbf{d}_{min}, \mathbf{u})$ is added to A_c if the constraint function is violated.

The algorithm looks for an optimal design vector that minimises the worst-case solution and is feasible over all the possible scenarios in U. However, such an optimal solution might not exist and in this case a small and increasing worst-case constraint violation ε is accepted through a relaxation procedure (line 19). In particular, a new constraint $C^* = C + \varepsilon$ is considered where ε is progressively increased by a user-defined percentage of the maximum constraint violation if a solution cannot be found. Line 24 finally performs a cross-check between the solutions stored in the archives A_c, A_u and A_d in order to mitigate the possibility to identify a local maximum that is not the global maximum during the optimisation over U.

6. Evidence Network Model

This section introduces the concept of *Evidence Network Model* (ENM) for the representation of complex engineering systems affected by epistemic uncertainty modelled with Evidence Theory. The model was presented in Refs. [35–37] and, here, is extended with the *Resilience* measure introduced in section 3.

We propose to represent a space system as a network of nodes (subsystems) connected through links (shared information). This is a common approach in multi-disciplinary design where a system is often represented with a Design Structure Matrix (see Ref. [26] for an example of application to space systems). In an ENM, however, we try to exploit the fact that information is carried by scalar quantities that lump together the effect of multiple uncertain parameters. Furthermore, we argue that the Design Structure Matrix (DSM) representation, although simple, is not ideal to describe a multi-connected system as it does not weigh the importance of each connection and does not offer an easy way to represent sub-networks or clusters. In the following, we will explain how an ENM is constructed and which properties is assumed to have.

In an ENM, the performance index defined in Eq. (6), can be written as:

$$f(\mathbf{d}, \mathbf{u}) = \sum_{i=1}^{N} g_i(\mathbf{d}, \mathbf{u}_i, \boldsymbol{\phi}_i(\mathbf{d}, \mathbf{u}_i, \mathbf{u}_{ij})), \tag{18}$$

where N is the number of nodes in the network and $\boldsymbol{\phi}_i(\mathbf{d}, \mathbf{u}_i, \mathbf{u}_{ij})$ is the vector of scalar exchange functions $\varphi_{ij}(\mathbf{d}, \mathbf{u}_i, \mathbf{u}_{ij})$ that represent the input/output of the nodes, with $j \in J_i$, and J_i the set of indexes of nodes connected to the i-th node. Eq. (18) decomposes the uncertain components in two categories: the uncoupled components $\mathbf{u}_i$ that affect only subsystem i, and the coupled variables $\mathbf{u}_{ij}$ shared among subsystem i and one or more subsystems j. We further assume that:

1. The functions g_i are positive semi-definite
2. Information is transferred from one node to another by means of the scalar functions φ_{ij}
3. The dependency of g_i on φ_{ij} is such that the $\max_{\mathbf{u}\in\gamma} g_i(\mathbf{u}) = \max_{\mathbf{u}_i\in\gamma_i}\left(\max_{\phi_{ij}} g_i\left(\mathbf{u}_i, \varphi_{ij}\right)\right)$ where during the optimisation over φ_{ij} the other uncertain parameters are anchored to the value of the worst-case scenario and γ_i is the projection of the focal element γ on the subspace of the uncertain parameters $\mathbf{u}_i$.

While the first two assumptions are easy to verify and are common to many space systems (e.g. the mass of the system), the third one is less obvious but it was verified to be true in the case investigated in this paper. We can, in fact, assume that the function φ_{ij} is also positive semi-definite in the domain of interest (e.g. the power demand or the data volume).

6.1. Decomposition

The computation of the *Bel* value over an extended network with a large number of uncertain variables can be extremely expensive as it would require to run one maximisation of the quantities of interest for each focal element. However, if the ENM satisfies the assumptions presented in the previous section, one can introduce an efficient decomposition of the network that allows for fast computation of a good approximation of *Bel*.

The decomposition aims at decoupling the subsystems over the space of uncertain variables so that optimisations can be run only over a small subset of FEs. The method was first introduced in Ref. [36] and can be summarised with the following 4 main steps:

1. Identification of an anchor point in the U space. In the following we will start with the solution of the optimal worst-case scenario problems (Eqs. (15)–(17)) as that corresponds to the most conservative solution and would generate a lower (more conservative) approximation of the full *Bel* curve. Once the partial *Bel* curves associated to the coupled variables (see step 2) are available, more anchor points can be defined by sampling the partial curves.
2. Maximisation over subsets of coupled variables and computation of m_c partial Bel_{ij} curves only considering the contribution of a given subset of coupled variables while keeping the uncoupled variables and the rest of the coupled variables at the value of the anchor point.
3. Maximisation over the uncoupled variables for different values of the coupled variables obtained from point 2 by sampling Bel_{ij}.
4. Reconstruction of the approximation $\widetilde{Bel}(\Omega)$.

In Ref. [36] it was demonstrated that, under the three assumptions introduced in the previous section, the decomposition produces an outer approximation of the *Bel* that progressively converges to the exact value as the number of samples drawn from the partial curves Bel_{ij} increases.

The decomposition procedure is summarised in Algorithm 2.

Algorithm 2
Decomposition

```
1: Initialise $\tilde{\mathbf{d}}$ s.t. $\forall\ \mathbf{u},\ C(\tilde{\mathbf{d}}, \mathbf{u}) \le 0$
2: Define $\mathbf{u}_u = [\mathbf{u}_1, \mathbf{u}_2, ..., \mathbf{u}_i, ..., \mathbf{u}_{mu}]$
3: Define $\mathbf{u}_c = [\mathbf{u}_{12}, \mathbf{u}_{13}, ..., \mathbf{u}_{ij}, ..., \mathbf{u}_{mc}]$
4: Compute $(\tilde{\mathbf{d}}, \underline{\mathbf{u}}_u, \underline{\mathbf{u}}_c) = \text{argmax} f(\tilde{\mathbf{d}}, \mathbf{u}_u, \mathbf{u}_c)$
5: for all $\mathbf{u}_{ij} \in \mathbf{u}_c$ do
6:   for all FE $\gamma_{k,ij} \subseteq \Gamma_{ij}$ do
7:     $\hat{f}_{k,ij} = \max_{\mathbf{u}_{ij}\in\gamma_{k,ij}} f(\tilde{\mathbf{d}}, \underline{\mathbf{u}}_{\mathbf{u}}, \mathbf{u}_{ij})$
8:     $\hat{\mathbf{u}}_{k,ij} = \underset{\mathbf{u}_{ij}\in\gamma_{k,ij}}{\text{argmax}} f$
9:     $m_{k,ij} = bpa(\gamma_{k,ij})$
10:   end for
11:   Evaluate partial Belief curve $Bel(F(\mathbf{u}_{ij}) \le \nu)$
12:   for all $q_{ij}$ sampled FEs $\gamma_{k,ij} \subseteq \Gamma_{ij}$ do
13:     Sort $\gamma_{ij} s.\ t.\ \hat{f}_{1,ij} < \hat{f}_{2,ij}, ... < \hat{f}_{q_{ij},ij}$;
14:     $\Delta Bel_{ij}^{q_{ij}} = Bel_{ij}(f < f_{q,ij}) - Bel_{ij}(f < f_{q-1,ij})$
15:   end for
```

(*continued on next page*)

Algorithm 2 (*continued*)

```
16: end for
17: for all the combinations $h \in \times_{ij} q_{ij}$ do
18:   for all $\mathbf{u}_i \in \mathbf{u}_u$ do
19:     for all FE $\gamma_{k,i} \subseteq \Gamma_i$ do
20:       $\hat{f}_{k,i} = \max_{\mathbf{u}_i \in \gamma_{k,i}} f(\tilde{\mathbf{d}}, \hat{\mathbf{u}}_{\mathbf{c}}^{\mathbf{h}}, \mathbf{u}_i)$
21:       $\hat{\mathbf{u}}_{k,i} = \underset{\mathbf{u}_i \in \gamma_{k,i}}{\operatorname{argmax}} f$
22:       $m_{k,i} = bpa(\gamma_{k,i})$
23:     end for
24:   end for
25:   for all the FE $\gamma_{k,\times\Gamma_i} \subseteq \times_i \Gamma_i$ do
26:     $\hat{f}_k^h = \sum_i^N \hat{f}_{k,i}$
27:     $m_k = \prod_i^N m_{k,i} \cdot \prod_{ij} \Delta Bel_{ij}^{q_{ij}}$
28:   end for
29: end for
30: Return Belief curve
```

Algorithm 2 presents only the reconstruction of the Belief curve; however, the Plausibility curve reconstruction is a symmetrical problem (minimisation instead of maximisation). In lines 1–3 of Algorithm 2 the problem is initialised for the decomposition approach. In particular, a design configuration is chosen ($\tilde{\mathbf{d}}$ in line 1), that is feasible in all the uncertain domain U.

Lines 2–3 define the uncoupled $\mathbf{u}_i$ and the coupled $\mathbf{u}_{ij}$ uncertain vectors $\forall\ i, j \in [1,2,...,N]$ with N the number of the network nodes (Eq. (18)). All the $\mathbf{u}_i$ and $\mathbf{u}_{ij}$ vectors are then collected in $\mathbf{u}_u$ and $\mathbf{u}_c$ respectively.

Line 4 evaluates the global maximum $\underline{\mathbf{u}}$ of f for the fixed $\tilde{\mathbf{d}}$ in line 1. If, for example, $\tilde{\mathbf{d}}$ is chosen to be the optimal worst case design solution $\mathbf{d}_{minmax}$, then $\underline{\mathbf{u}} = \mathbf{u}_{minmax}$.

Lines 6–10 describe the uncertainty propagation, through the network-model, of the effect of the coupled variables $\mathbf{u}_{ij}$ only, keeping all other components of the uncertain vector fixed to the anchor point $\underline{\mathbf{u}}$. More precisely, following Eqs. (8) and (10) a Belief curve Bel_{ij} is computed for each vector $\mathbf{u}_{ij} \in \mathbf{u}_c$. In order to evaluate the curve, the maximum of f ($\hat{f}_{k,ij}$ in line 7 and $\hat{\mathbf{u}}_{k,ij}$ in line 8) for each *k-FE* $\gamma_{k,ij} \in \Gamma_{ij}$ is searched and the corresponding *bpa*, $m_{k,ij}$, is saved (line 9).

In lines 12–15, each partial Bel_{ij} curve is sampled N_{ij}^c times. For each sample $q \in [1,...,N_{ij}^c]$, the values $[Bel_{ij}(f < \nu_q),\ \nu_q]^T$ are stored and a subset $\Gamma_{ij}^q \subseteq \Gamma_{ij}$ is defined by all the k-FE $\gamma_{k,ij}^q$ whose maxima are below ν_q. For each Γ_{ij}^q then, the k-FE $\gamma_{k,ij}^{q'}$ with the highest maximum $\hat{f}_{q,ij}$ is selected and the corresponding $\hat{u}_{q,ij}$ vector is saved. The maxima $\hat{f}_{q,ij}$ are then sorted (line 13) and the contribution of the q-sample ΔBel_{ij}^q to the final belief curve is computed as the difference $Bel_{ij}(f < \nu_q) - Bel_{ij}(f < \nu_p)$ where ν_p corresponds to Γ_{ij}^p which associated $\hat{f}_{p,ij}$ is the highest maximum over all the $\hat{f}_{k,ij} < \hat{f}_{q,ij}$ (line 14).

In lines 17–28, all the $\prod_{ij} N_{ij}^c$ samples (combinations of all the samples for each Bel_{ij}) are considered from the Cartesian product $\times\ \Gamma_{ij}$ of all the FEs in the space of the coupled variables $\mathbf{u}_c$. For each one of them, fixing the coupled components $\mathbf{u}_c$ from the combination of samples, the network in Eq. (18) is decomposed because the nodes are influenced only by the uncoupled components $\mathbf{u}_u$. For each node then the maxima over only the uncoupled k-FEs $\gamma_{k,i} \in \Gamma_i$ are calculated in lines 19–22 ($\hat{f}_{k,i}$ in line 20 and $\hat{\mathbf{u}}_{k,i}$ in line 21) and the corresponding *bpa*, $m_{k,i}$ are saved (line 22).

In lines 25–28, finally, the maximum of f in a generic FE $\gamma \in \Gamma_{t,1} \times ...\times\Gamma_{z,N} \times \Gamma_{k,1,2} \times ...\times\Gamma_{m,ij}$ is computed where t and z are t-th and z-th FEs in Γ_1 and Γ_N respectively and k and m are samples in the partial $Bel_{1,2}$ and Bel_{ij} curves respectively. More precisely the maximum in γ is the sum of the maxima of f evaluated in the corresponding FEs independently in the different nodes, with the coupled components $\mathbf{u}_c$ fixed from the sample h. The corresponding *bpa* of γ is the product of the *bpa* m_i of that FE due to only the uncoupled components $\mathbf{u}_u$ and all the contributions from the partial belief curves $\prod_{ij} \Delta Bel_{ij}^{q_{ij}}$ (line 27).

6.2. Computational complexity

The very important effect of the decomposition approach is the reduction in computational complexity to estimate the *Bel* function. In fact, for a problem with m uncertain variables, each defined over N_k intervals, the total number of FEs would be:

$$N_{FE} = \prod_{k=1}^{m} N_k. \tag{19}$$

The total number of focal elements N_{FE} can be rewritten in terms of coupled and uncoupled uncertain vectors:

$$N_{FE} = \left(\prod_{i=1}^{m_u} \prod_{k=1}^{p_i^u} N_{i,k}^u\right)\left(\prod_{i=1}^{m_c} \prod_{k=1}^{p_i^c} N_{i,k}^c\right), \tag{20}$$

where p_i^u and p_i^c are the number of components of the i^th^ uncoupled and coupled vector, respectively, and $N_{i,k}^u$ and $N_{i,k}^c$ are the number of intervals of the k^th^ components of the i^th^ uncoupled and coupled vector respectively. Thus one would need to run N_{FE} optimisations to calculate an exact value of *Bel*.

Instead, if one applies the decomposition approach proposed in this section, the total number of FEs, over which the decomposition algorithm has to optimise, is:

$$N_{FE}^{Dec} = N_s \sum_{i=1}^{m_u} N_{FE,i}^u + \sum_{i=1}^{m_c} N_{FE,i}^c, \tag{21}$$

considering the vector of uncertainties ordered as:

$$\mathbf{u} = [\underbrace{\mathbf{u}_1, ..., \mathbf{u}_{m_u}}_{\text{uncoupled}},\ \underbrace{\mathbf{u}_1, ..., \mathbf{u}_{m_c}}_{\text{coupled}}], \tag{22}$$

where N_s is the number of samples of the partial belief curves Bel_{ij}, $N_{FE,i}^c = \prod_{k=1}^{p_i^c} N_{i,k}^c$ and $N_{FE,i}^u = \prod_{k=1}^{p_i^u} N_{i,k}^u$. This means that the computational complexity to calculate the maxima of the function f within the FEs remains exponential for each single uncoupled or coupled vector but is polynomial with the number of subsystems.

7. System model and problem definition

The approach to Resilience Engineering described in the previous sections is here applied to the design of system and operations of a CubeSat in Low Earth Orbit (LEO). The CubeSat is divided in 5 subsystems, Attitude and Orbit Control (AOCS), Telecommunication (TTC), On Board Data Handling (OBDH), Power and Payload subsystems. The assumption is that each component has multiple functionalities and both the performance of a component and the reliability associated to each functionality are affected by epistemic uncertainty.

The satellite is translated into the ENM represented in Fig. 1. The figure shows the 5 subsystems and the interconnections with the transfer of information among subsystems. The concept of ENM was explained in Section 6 and its use will be explained in more detail in section 7.4.

The two performance indexes, or quantities of interest, are the overall mass of the satellite M_{TOT} and the total amount of data sent back to the ground station V. The former does not change in time while the latter is subject to disruptions during the operational life. These two quantities are defined as:

$$M_{TOT}(\mathbf{d}, \mathbf{u}) = M_{ttc} + M_{obdh} + M_{aocs} + M_{pl} + M_p \tag{23}$$

$$V(\mathbf{d}, \mathbf{u}, t) = V_i^c + \frac{V_{i+1}^c - V_i^c}{t_{i+1} - t_i}(t - t_i)\ \ i = 0, ..., N_o - 1 \tag{24}$$

and depend on a vector of decision parameters $\mathbf{d}$ and epistemic uncertain variables $\mathbf{u}$. Eq. (24) is a linear piece-wise interpolation of the

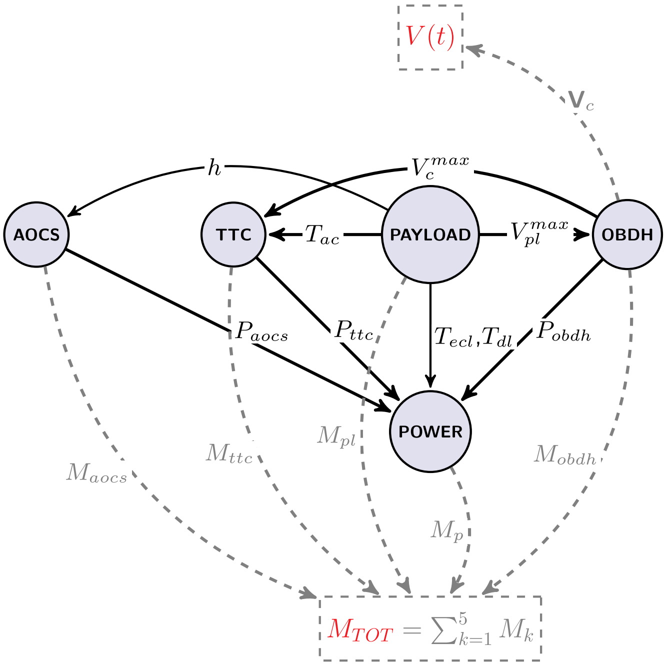

Fig. 1. Evidence Network Model of the CubeSat. The two quantities of interest are the mass of the CubeSat M_{TOT} and the total amount of data transmitted to the ground station V; M_{TOT} is the sum of the mass of the 5 subsystems and V is the quantity of data sent by the TTC after the compression in OBDH.

components of the vector $\mathbf{V}^c = [V_1^c, ..., V_{N_o}^c]^T$ of compressed data volumes sent to the ground station for each of the $\mathbf{T}_o = [T_1, ..., T_{N_o}]^T$ periods of the N_o orbits during the total mission time T, such that $T_{i+1} = t_{i+1} - t_i$ and $T = \sum_{i=1}^{N_o} T_i$.

The calculation of the subsystem masses M_{ttc}, M_{obdh}, M_{aocs}, M_{pl}, M_p and of the data volumes V_i^c will be described in more detail in the following sections.

7.1. System models

This section presents the mathematical models used to calculate the quantities of interest $M_{TOT}(\mathbf{d}, \mathbf{u})$ and $V(\mathbf{d}, \mathbf{u}, t)$ for each subsystem and $\forall\ t \in [T_0, T]$.

7.1.1. Payload

The payload is a camera that takes images of the Earth during daylight-time T_{dl} and send them to the OBDH for compression. Since there is no orbital dynamics node in this example we calculate all the orbital quantities in the payload node.

More specifically, the orbit period $T_{orb}(h) = 2\pi\sqrt{\frac{(R_E + h)^3}{\mu}}$, the eclipse time $T_{ecl}(h) = \frac{D_{EA}(h) T_{orb}(h)}{360°}$ and the daylight time $T_{dl}(h) = T_{orb} - T_{ecl}$ [45], that are used by the Payload and the Power nodes, are functions of the uncertain altitude h, where $D_{EA} = 2\arcsin\left(\frac{R_E}{h + R_E}\right)$ is the Earth Angular Diameter, $R_E = 6.3782 \cdot 10^3$ km the Earth radius and $\mu_E = 3.986 \cdot 10^{14}$ $m^3 s^{-2}$ the Earth gravity constant. The access time to the ground station T_{ac}, that is shared with the TTC node, is defined as:

$$T_{ac} = \frac{T_{orb}}{180°} \arccos\frac{\cos(\zeta_{max})}{\cos(\zeta_{min})} \tag{25}$$

where

$$\zeta_{max} = 90° - \varepsilon_{min} - \eta_{max} \tag{26}$$

$$\sin(\eta_{max}) = \sin\frac{D_{EA}}{2}\cos\varepsilon_{min} \tag{27}$$

$$\sin(\zeta_{min}) = \sin(L_{pol})\sin(L_{GS}) + \cos(L_{pol})\cos(L_{GS})\cos(\Delta L) \tag{28}$$

with ε the elevation angle, η the nadir angle, $L_{pol} = 90° - I$ with I the inclination ($I = I_0 + \delta_{inc}$ with $I_0 = 0$), L_{GS} the latitude at the ground station and ΔL the difference in longitude between orbit pole and ground station [46].

For each completed orbit the payload generates N_i^{pic} images, with $i \in [1, N_o]$. Over several orbits the numbers of images are stored in the vector $\mathbf{N}^{pic}(F_R, h) = [N_1^{pic}, N_2^{pic}, ..., N_{No}^{pic}]^T$, where the number of images per orbit is the product $N_i^{pic} = F_R T_{dl}$ between daylight time and frame rate F_R. The frame rate F_R is evaluated with a piecewise interpolation of the values $\{6.6, 26.6, 26.6, 26.6\}$ s^{-1} over the design parameter $\tau_{pl} \in \{1,2,3,4\}$. The corresponding amount of data generated by the payload system for each orbit is stored in the vector $\mathbf{V}_{PL}$:

$$\mathbf{V}_{PL} = \frac{I_{mS} B_D \mathbf{N}^{pic}}{2^{33}}, \tag{29}$$

which is passed on to the OBDH subsystem. The image size I_{mS} is piecewise interpolated using the data $\{1280 \times 1024, 640 \times 480, 2592 \times 1944, 1280 \times 1024\}$ pixel, over τ_{pl}. The bit depth B_D is a design parameter and the value at denominator is used to change units from bits to Giga bytes.

Mass and power of the payload are derived from a a look-up table of available cameras. As for the frame rate and image size, by inserting a value of the design parameter τ_{pl}, the model does a piecewise interpolation returning a mass value from the vector $M_{pl} = [1.1, 1.1, 0.256, 1.1]^T$ kg, a power value in daylight from the vector $P_{pl,dl} = [4, 4, 2.5, 4]^T$ W and a power value in eclipse from the vector $P_{pl,ecl} = [0, 0, 1.75, 9.75]^T$ W [47–49].

7.1.2. On Board Data Handling

In this system model, it is assumed that the main purpose of the OBDH is to compress and store the images coming from the payload. According to Ref. [50], the total compression rate for JPEG compression is $C = 0.0434$. Thus, the volume of data after the compression, that is used in Eq. (24) for the second quantity of interest, is:

$$\mathbf{V}_c = \mathbf{V}_{PL} C. \tag{30}$$

The design parameter τ_{obdh} does a piecewise interpolation of the type of OBDH within a list of four available systems. The model takes the value of τ_{obdh} and linearly interpolates the specific mass and power for the single OBDH module from the vectors: $m_{obdh}^d = [2.3, 2, 1.5, 3]^T$ kg and $p_{obdh}^d = [15, 20, 22, 30]^T$ W. The maximum data storage is $v_{obdh}^d = 4$ Gbytes [51]. The total mass M_{obdh} and the power P_{obdh} of the OBDH are then functions of the compressed data volume $V_c^{max} = \max(\mathbf{V}_c)$, and the uncertain parameters δP_{obdh} and δM_{obdh}:

$$M_{obdh} = m_{obdh}^d \frac{V_c^{max}}{v_{obdh}^d}(1 + \delta M_{obdh}) \tag{31}$$

$$P_{obdh} = p_{obdh}^d \frac{V_c^{max}}{v_{obdh}^d}(1 + \delta P_{obdh}) \tag{32}$$

7.1.3. Telecommunication system

The TTC is composed of an antenna, an amplified transponder and a radio frequency distribution network (RFDN). *TTC* connects the transmitter antenna on the CubeSat with the receiving antenna on the ground station. A patch antenna is considered. The mass M_{ant} of the antenna depends on the diameter D:

$$D = \frac{\lambda_{ant}}{\pi}\sqrt{\frac{G_t}{\eta_{ant}}} \tag{33}$$

with η_{ant} the uncertain antenna efficiency and λ_{ant} the wave length.

$$M_{ant} = \pi\frac{D^2}{4}(0.0005\rho_c + 0.0015\rho_d) \tag{34}$$

with $\rho_c = 8940\ kg/m^2$ and $\rho_d = 2000\ kg/m^2$ respectively the density of copper and the density of dielectric material. Eq. (34) can be found in Ref. [52]. The RFDN mass M_{rfdn} is an uncertain variable while the amplified transponder mass M_{amp} and the power requirement P_{amp} are derived from available data as described in Ref. [53], as a function of the transmitter power P_t (power in output from the antenna)

$$P_t = \frac{E_b}{N_0} - G_t - L_t - L_s - L_p - \frac{G_r}{T_{n,s}} + 10\log_{10}R - 228.6 \tag{35}$$

and of the amplifier type τ_{amp} (design parameter in Table 1). The relations can be found in Ref. [53] and are defined from data derived from actual flight hardware. The ratio of received energy-per-bit to noise density, $\frac{E_b}{N_0}$, is a function of frequency f_{ttc}, modulation τ_{mod} and required bit error rate $BER = 10^{-5}$ as in Ref. [54] where f_{ttc} and τ_{mod} are design parameters. For each modulation type from the list {PSK, BPSK, CFSK, BFSK, FSK, DPSK, QPSK, NRZ} a different formula to evaluate $\frac{E_b}{N_0}$ [54] is given. A linear pairwise interpolation is done of the $\frac{E_b}{N_0}$ values over the τ_{mod} parameter. The quantity L_t is the uncertain on-board loss, while $L_s = 92.44 + 20\log_{10}d_A + 20\log_{10}f_{ttc}$ is the free space path loss with d_A the distance between the transmitter and receiving antennas [54]. The distance d_A is here assumed to be equal to the altitude h for sake of simplicity. The term L_p is the propagation loss and it collects atmospheric attenuation, rain attenuation, pointing loss and other losses that are taken into account in the uncertain parameter L_{other}. $G_r = 60dB$ is the receiver antenna gain. The temperature $T_{n,s}$ is the system noise temperature. $R = \frac{V_c^{max}}{T_{ac}}$ is the data rate, where V_c^{max}, in bits, is the maximum transmitted data volume across all orbits and T_{ac} is the access time to the ground station.

Finally, the mass of the TTC system is the sum of its components:

$$M_{ttc} = M_{ant} + M_{amp} + M_{rfdn}. \tag{36}$$

The power of the TTC is a function of the transponder only. In particular, the value in decibel of P_{ttc} is linearly interpolated using the vector $[0.0792, 0.5441]^T$ over the range $[0.1461, 1.9031]^T$ [53]. P_{ttc} is then used as input for the Power subsystem.

7.1.4. Attitude and Orbit Control system

The AOCS is in charge of controlling the orientation of the CubeSat with a three axis stabilisation system. The actuators are reaction wheels and magneto-torquers.

During the mission, the CubeSat is assumed to be affected by a number of disturbances and it is expected to perform some slew manoeuvres. In particular, the solar radiation pressure T_s, the magnetic torque T_m, the torque due to aerodynamic drag T_a and the gravity gradient torque T_g. The torque due to solar radiation pressure is defined as:

$$T_s = l\frac{I_s}{c}A_{sc}(1 + r_f) \tag{37}$$

with $I_s = 1420\ \mathrm{W/m^2}$ the incident solar radiation, c the speed of light, A_{sc} the uncertain area of the surface normal to the sunlight, l the offset between the centre of gravity and centre of pressure of the satellite (a design parameter in Table 1) and r_f the uncertain reflectance factor. The torque due to the magnetic field is:

$$T_m = m_{dip}B \tag{38}$$

with m_{dip} the uncertain spacecraft residual dipole and B the planet magnetic field strength:

$$B = \frac{B_0 R_E^3}{(R_E + h)^3}\sqrt{3\sin^2(l_M) + 1} \tag{39}$$

where l_M is the magnetic latitude. The torque due to drag is defined as:

$$T_a = p_{dyn}C_d A_{sc} l. \tag{40}$$

In Eq. (40) $p_{dyn} = \frac{1}{2}\rho v^2$ is the dynamic pressure, where $\rho = \rho_0 e^{-h/H_{sh}}$ is the atmospheric density, with $\rho_0 = 1.2250\ \mathrm{kg/m^3}$ and $H_{sh} = 8.6$ km, and v the velocity on a circular orbit at altitude h. C_d is the uncertain drag coefficient of the spacecraft. A_{sc} is the uncertain area of the surface normal to the velocity vector considered equal to the surface area in Eq. (37) (please refers to Table 2 for the value of this uncertain parameter). Note that we assume that both the area of the surface normal to the sunlight and the one normal to the velocity are the same. The torque due to the gravity gradient is:

$$T_g = \frac{3\mu_E}{2(R_E + h)^3}|I_z - \min(I_x, I_y)|\sin 2\psi \tag{41}$$

where $I_z = 0.1417(1 + \delta I)\ \mathrm{kg\ m^2}$, $I_y = 0.1083\ \mathrm{kg{\cdot}m^2}$ and $I_x = 0.0417\ \mathrm{kg{\cdot}m^2}$ are the principal moments of inertia of the satellite and $\psi = 8.7266{\cdot}10^{-2}$ radiant is the angle between the spacecraft z-axis and the nadir vector [35]. The total disturbance is the sum:

$$T_d = T_s + T_m + T_a + T_g \tag{42}$$

The momentum due to T_d that is stored in the reaction wheels, H_d, and the momentum required for the slew manoeuvres, H_{sl}, are defined as:

$$H_d = \frac{T_d T_{orb}}{4e} \tag{43}$$

$$H_{sl} = \frac{4\phi_{sl}I_z}{t_{sl}} \tag{44}$$

with $e = 8.7266{\cdot}10^{-2}$ radiant the pointing accuracy, ϕ_{sl} the slew angle and t_{sl} the time allowed for the manoeuvre (design parameters in Table 1). The mass, M_{rw}, and power, P_{rw}, of the reaction wheels are computed by interpolation from available real data [53], as functions of the maximum between H_d and H_{sl}:

$$M_{rw} \propto \max(H_d, H_{sl}) \tag{45}$$

$$P_{rw} \propto \max(H_d, H_{sl}) \tag{46}$$

In particular, for momentums of $[0.0016, 400]^T$ Nms, the masses are respectively $[0.072, 20]^T$ kg and the power consumptions are $[0.465, 110]^T$ W. It is assumed that the momentum stored in the reaction wheels is unloaded with magneto-torquers. The mass and power of the magneto-torquers are interpolated as functions of the required magnetic dipole D_{mag} as in Ref. [53]:

$$M_{mt} \propto D_{mag} \tag{47}$$

$$P_{mt} \propto D_{mag} \tag{48}$$

where

$$D_{mag} = \frac{T_d}{B} \tag{49}$$

with B given in Eq. (39). In particular, for dipoles D_{mag} of $[0.06, 4000]^T$ $\mathrm{Am^2}$, the masses are respectively $[0.0835, 50]^T$ kg and the power consumptions are $[0.155, 16]^T$ W. Finally, the outputs of the AOCS

Table 1
Design parameters.

SYSTEMS	d	LB	UB	$\underline{R}_d$	$\bar{R}_d$
AOCS	t_{sl} (s)	30	90	1	1
	ϕ_{sl} (deg)	10	60	0.899	1.097
TTC	f_{ttc} (GHz)	7	10	0.85	1.2
	τ_{mod}	0	1	0.95	1.05
	τ_{amp}	0 (TWTA)	1 (SSA)	0.95	1.05
Power	V_{bus} (V)	3	5	0.9	1.1
	V_{dr} (%)	1	5	1	1
	τ_{conf}	0 (DET)	1 (MPPT)	1	1
	τ_p	0	1	1	1
Payload	B_D	1	5	0.9	1.2
	τ_{pl}	1	4	0.9	1.1
OBDH	τ_{obdh}	1	6	0.8	1.2

Table 2
Uncertain parameters.

Systems	u	interval 1 (*bpa*)	interval 2 (*bpa*)	$\underline{R}_u$	$\bar{R}_u$
Payload	h (km)	[600 800] (0.4)	[800 1000] (0.6)	0.9	0.967
	ε (deg)	[0 5] (0.4)	[5 10] (0.6)	1	1
	δ_{inc} (deg)	[0 5] (0.3)	[5 10] (0.7)	1	1
OBDH	δP_{obdh}	[0 0.1] (0.5)	[0.1 0.2] (0.5)	1	1
	δM_{obdh}	[0 0.1] (0.8)	[0.1 0.2] (0.2)	1	1
AOCS	l (m)	[0.005 0.01] (0.5)	[0.01 0.02] (0.5)	0.94	1.2
	A_{sc} (m^2)	[0.034 0.0885] (0.5)	[0.0885 0.15] (0.5)	1	1
	r_f	[0.5 0.6] (0.5)	[0.6 0.7] (0.5)	1	1
	m_{dip} (mA $\cdot m^2$)	[0.5 1] (0.5)	[1 1.5] (0.5)	0.85	0.98
	C_D	[2 2.2] (0.4)	[2.2 2.5] (0.6)	0.9	1.1
	δI	[-0.1 0.05] (0.5)	[0.05 0.1] (0.5)	0.85	1
TTC	η_{ant}	[0.6 0.8] (0.3)	[0.8 0.9] (0.7)	1	1
	G_t (dB)	[13] (0.3)	3 5 (0.7)	1	1.15
	L_t (dB)	[0.1 0.5] (0.3)	[0.5 1] (0.7)	1	1.05
	L_{other} (dB)	[0.5 1.5] (0.4)	[1.5 2.0] (0.6)	0.85	1
	M_{rfdn} (kg)	[0.1 0.3] (0.4)	[0.2 0.5] (0.6)	1	1
Power	δD_c	[0.025 0.0275] (0.4)	[0.3 0.0375] (0.6)	1	1
	η_a	[0.8 0.85] (0.4)	[0.85 0.9] (0.6)	0.8	1
	$\delta\rho_{sa}$ (kg/m^2)	[3.5 3.6] (0.3)	[3.6 4] (0.7)	1	1
	δP_p	[0 0.1] (0.5)	[0.1 0.2] (0.5)	0.95	1.05

node are:

$$M_{aocs} = M_{rw} + M_{mt} \tag{50}$$

$$P_{aocs} = P_{rw} + P_{mt} \tag{51}$$

7.1.5. Power system

The electrical power system (EPS) is composed of a solar array, a battery pack, and a power conditioning and distribution unit (PCDU). The mass of the power system is the sum of the individual masses of its components

$$M_p = M_{sa} + M_{bp} + M_{pcdu} \tag{52}$$

The power produced by the system in daylight is the one generated by the solar array P_{sa}. The design of the solar array is a function of the power requirements during light-time P_{lt} and eclipse P_{ecl} that are calculated from the power requirements of the other subsystems:

$$P_{lt} = 16 + P_{aocs} + P_{ttc} + P_{obdh} + P_{pl,lt}. \tag{53}$$

$$P_{ecl} = 16 + P_{aocs} + P_{ttc} + P_{obdh} + P_{pl,ecl}. \tag{54}$$

where the number 16 is the base power that accounts for the maintainince of the basic functionalities of the satellite. Given P_{ecl} as well as the duration T_{ecl} of the night, the energy capacity requirement of the battery system is

$$E_{req} = \frac{P_{ecl}T_{ecl}}{\eta_{b-l}DOD} \tag{55}$$

where η_{b-l} is the transfer efficiency between battery and loads and it is the product of the efficiencies of the battery discharge regulator η_{bdr}, the distribution unit η_{du}, and the harness η_{har}:

$$\eta_{b-l} = \eta_{bdr}\eta_{du}\eta_{har} \tag{56}$$

The efficiency η_{bdr} of the battery discharge regulator is a function of the bus voltage V_{bus} and is calculated using a linear interpolation of available data [54]. In particular we linearly interpolate the efficiencies [0.90, 0.97] over the voltage range [20, 100] V. The harness efficiency η_{har} is

$$\eta_{har} = 1 - \frac{V_{dr}}{100} \tag{57}$$

and is, therefore, dependent on the allowable voltage drop V_{dr} given as a percentage of the bus voltage. The depth of discharge DOD is a function of the number $C_L = \frac{T_{tot}}{T_{orb}}$ of charge/discharge cycles, that is dependent on the fixed mission time and on the uncertain altitude h. Their relationship is defined as in Ref. [54]:

$$DOD = -36.76 \log \frac{C_L}{207800} \tag{58}$$

Given the energy requirement for the battery, the mass of the battery pack is

$$M_{batt} = \frac{E_{req}}{E_c} \tag{59}$$

where the energy density E_c (in Wh/kg) is selected from a list of available battery types depending on the capacity $C_B = \frac{E_{req}}{V_{bus}}$. The capacities C_B is used to select the energy density E_c from a look-up table. The model enters with the value C_B to the vector $[1.5,\ 5.8,\ 10,16,28,39,50]^T$ Ah and finds the closest approximation. The corresponding value of the energy density is read from the vector $[115,133,139,155,118,126,165]^T$ Wh/kg [54].

The power P_{sa} required from the solar array is computed considering the duration of the daylight T_{dl}:

$$P_{sa} = \frac{P_{ecl}T_{ecl}}{\eta_{a-b}\eta_{b-l}T_{dl}} + \frac{P_{lt}}{\eta_{a-l}} \tag{60}$$

where η_{a-b} is the transfer efficiency between solar array and battery pack, η_{a-l} is the transfer efficiency between solar array and loads. Although the uncertainty on the power requirements comes from all the loads it is assumed that a further epistemic uncertainty exists on the total demand. Therefore an uncertainty factor δP_p is applied to P_{lt} and P_{ecl}: $P_{lt} = P_{lt}(1 + \delta P_p)$ and $P_{ecl} = P_{ecl}(1 + \delta P_p)$. The transfer efficiencies can be expressed as the product of the efficiencies of the components:

$$\eta_{a-b} = \eta_{sar}\eta_{bcr}\eta_{batt} \tag{61}$$

$$\eta_{a-l} = \eta_{sar}\eta_{dist}\eta_{har} \tag{62}$$

In Eqs. (61) and (62) η_{bcr} is the efficiency of the battery charge regulator and, as for the discharge regulator, it is a function of the bus voltage V_{bus}. Also in this case we interpolate the efficiency [0.90, 0.97] over the voltage range [20, 100] V. The parameter η_{sar} is the efficiency of the solar array regulator, and it is a linear interpolation between 0.94 at 20 V and 0.99 at 100 V when the design parameter τ_{conf} selects the direct energy transfer (DET) configuration, or between 0.93 at 20 V and 0.97 at 100 V when τ_{conf} selects maximum power peak tracking (MPPT) configuration. The efficiency of the distribution unit is $\eta_{dist} = 0.99$. The charging efficiency of the battery is $\eta_{batt} = 0.96$. The array pointing loss factor is

$$\eta_p = \cos\alpha \tag{63}$$

where α is the solar incidence angle. The distance r_S (in AU) from the Sun involves a loss, or gain, that is

$$\eta_r = \frac{1}{r_S^2} \tag{64}$$

Furthermore, cells degrade with time mainly due to radiation fluence, and such degradation can be estimated as [8]:

$$\eta_{life} = (1 - D_c)^T \tag{65}$$

where D_c is the cell degradation per year and T is the cell life time (the mission time). A further important factor affecting the efficiency of the solar array is the uncertain assembly efficiency η_a. The efficiency of the array is lower than the efficiency of the single cells because of a loss due to assembly. The total cell efficiency is, therefore, $\eta_{tot} = \eta_a\eta_p\eta_r\eta_{life}$. The specific power (in Wh m^{-2}) of the array is

$$P_{cell} = 1370\eta_c\eta_{tot} \tag{66}$$

where η_c is the efficiency of the single solar cell. From this, the required area of the array is computed:

$$A_{sa} = \frac{P_{sa}}{P_{cell}} \tag{67}$$

and finally the mass of the solar array

$$M_{sa} = A_{sa}\rho_{sa}. \tag{68}$$

The values of D_c, η_c and ρ_{sa} are chosen by the design parameter τ_p. More precisely they are evaluated by a piecewise interpolation of the following data over the design parameter $\tau_p \in [0,\ 0.5,\ 1]^T$, $\rho_{sa} \in [32{\cdot}10^{-2},\ 116{\cdot}10^{-2},\ 86{\cdot}10^{-2}]$ kg/m2, $D_c \in [0.0375, 0.0275, 0.0275]^T$ and $\eta_c \in [0.1555, 0.2744, 0.2862]^T$. The uncertainty factors δD_c and $\delta\rho_{sa}$ are applied: $D_c = D_c(1+\delta D_c)$ and $\rho_{sa} = \rho_{sa}(1+\delta\rho_{sa})$.

The PCDU is a modular unit composed of modules such as battery charge and discharge regulators, solar array regulators, maximum power point tracker, shunt regulator, distribution unit (latching current limiters), telemetry interface. The number of modules, and thus the mass of the unit, depends on τ_{conf}. Indeed, if τ_{conf} is DET, there is no maximum power point tracker, and the PCDU is lighter. On the other hand, an MPPT configuration extracts maximum power from the solar array, therefore the array size decreases, but the presence of the MPPT module decreases the transfer efficiency and increases the PCDU mass. The configuration parameter τ_{conf} is used to trade-off between different components and, thus, is a design parameter. The mass M_{pcdu} can be estimated as the sum

$$M_{pcdu} = \mu_{pcdu}(2P_{sa} + P_{lt} + P_{ecl} + cP_{sa}) \tag{69}$$

where $\mu_{pcdu} = 0.001$ kg/W and $c = 0$ for DET and $c = 1$ for MPPT. The factor 2 multiplying the first term in brackets accounts for a telemetry and a distribution unit.

7.2. CubeSat resilience model

We assume that the CubeSat system can be in 3 distinct operational states. State 0: total system failure x_0; state 1: partially functional system x_1; state 2: fully functional system x_2. Each state is associated with a different value of the performance function $V(t, x; \mathbf{d}, \mathbf{u})$.

The assumption underneath the modelling of the resilience of the CubeSat is that a fully, or partially, functional system can deteriorate and a partially functional system can recover but once a total failure of the system occurs the system is not able to recover anymore and the satellite is lost. When the satellite is lost the data volume is zero. At the start of the mission the CubeSat is assumed to be fully functional, which corresponds to a probability of being in state x_2, $P(X(0) = x_2) = 1$. The further assumption is that the occurrence of a complete failure is independent of the occurrences of the partial failures and their recoveries and does not depend on decision and uncertain variables. This is a simplification that will be removed in future developments and does not impair the validity of our results. Thus, following [55], we model the probability of a complete failure of the whole satellite at time t with the Weibull distribution $p_0(t) = \prod_s p_{0,s}(t)$, where $p_{0,s}$ is the Weibull distribution defining the probability of a failure of subsystem s. The individual Weibull density function and associated parameters were taken from Ref. [55].

Until a complete failure occurs, the homogeneous continuous time Markov Chain as introduced in Sec. 3 is used to model the transition between states x_1 and x_2 and back. The stochastic dynamics of this process is given by the transition operator given in Eq. (1) with a transition rate matrix

$$Q(\mathbf{d}, \mathbf{u}) = \begin{pmatrix} -\mu & \mu \\ \lambda(\mathbf{d}, \mathbf{u}) & -\lambda(\mathbf{d}, \mathbf{u}) \end{pmatrix}, \tag{70}$$

where the first line and column refer to state x_1 and the second ones to state x_2, μ is constant and λ is a function of both design and uncertain parameters. The state of the CubeSat changes from x_2 to x_1 with rate λ and with rate μ in the opposite way. A general solution for the distribution of the system states at any time, conditional upon that the fatal failure has not yet occurred, is given by Eq. (2). The simple Markov Chain model we have chosen is well-known within reliability theory as the alternating system with constant rates [56]. Considering our initial conditions ($P(X(0) = x_2) = 1$), conditional on that the fatal failure has not occurred by time t, the probability that the system is in state x_2 at time t can be expressed explicitly as

$$p_2(t) := \Pr(X(t) = x_2 | T_{fail} > t, X(0) = x_2) = \frac{\mu}{\mu+\lambda} + \frac{\lambda}{\mu+\lambda}\exp(-t(\mu+\lambda)). \tag{71}$$

The probability that the system is in state x_1 at time t, conditional upon that the fatal failure has not occurred by time t, will be denoted $p_1(t) = 1 - p_2(t)$. It is the complement of p_2 because of the law of total probability.

The expected value of the instantaneous data increment, which is needed to evaluate the expected total volume of transmitted data (Eq. (4)), is

$$\mathbb{E}\{V(t, X(T); \mathbf{d}, \mathbf{u})\} = [V_2(t; \mathbf{d}, \mathbf{u})p_2(t) + V_1(t; \mathbf{d}, \mathbf{u})p_1(t)](1 - p_0(t)) + V_0(t; \mathbf{d}, \mathbf{u})p_0(t), \tag{72}$$

where V_0, V_1 and V_2 represent the instantaneous data increment respectively for states x_0, x_1 and x_2. $V_2(t) = V(t)$ is the data volume for a completely functional satellite. $V_1(t)$ is the data volume of a satellite in the degraded state x_1, and is here computed as:

$$V_1(t) = \frac{V_2(t)}{2} \tag{73}$$

When the satellite is in state x_0, total failure, the corresponding data volume is $V_0(t) = 0$.

The parameters μ in Eq. (70) is set to the value $1/365$ while parameter λ has a base value $\lambda_0 = 1/365$ and is related to the design and uncertain parameters through the expression

$$\lambda(\mathbf{d}, \mathbf{u}) := \lambda_0 \prod_i [r_{u,i}(u_i)] \prod_j [r_{d,j}(d_j)], \tag{74}$$

where the two functions $r_{u,i}$ and $r_{d,j}$ represent the relative influence of each of the uncertain or design parameters. This form was chosen because it corresponds to Cox's proportional hazard model [57] with covariates $\mathbf{d}$ and $\mathbf{u}$. If some observations of the process were available, the relative influences could be inferred by statistical methods. In the absence of data, we have chosen an expert estimates for the relations based on linear interpolations between the estimated influences at the lower and upper boundaries of the respective parameter spaces. For $\underline{u}_i$, $\bar{u}_i$, denoting the lower and upper bound for an uncertain parameter u_i, the respective relative influences at the boundary are denoted $\underline{R}_{u,i}$, $\bar{R}_{u,i}$ and the relative influence of u_i on the failure transition rate is

$$r_{u,i}(u_i) := \underline{R}_{u,i} + \frac{\bar{R}_{u,i} - \underline{R}_{u,i}}{\bar{u}_i - \underline{u}_i}(u_i - \underline{u}_i). \tag{75}$$

An analogous expression is used to relate $r_{d,i}$ to each d_i. For the sake of the simple exercise presented in this paper, these linear relationships and expression (74) were purposely constructed to allow the design process to change the rate of transition from x_2 to x_1 in one direction and to allow the uncertain variables to change in the opposite direction. This choice provides a verifiable result. In a more general context, appropriate relationships will need to be defined for each subsystem and component.

We chose the values of $\underline{R}_{u,i}$ and $\bar{R}_{u,i}$ in such a way that each design and uncertain parameter has a different influence on the system degradation and recovery rates. All the values of $\underline{R}_{u,i}$ and $\bar{R}_{u,i}$ are reported in Tables 1 and 2 The level of influence of each parameter is proportional to $\bar{R}_i - \underline{R}_i$. When this difference is zero, the corresponding parameter is expected to have no effect on the degradation and recovery rates. During the development of the method presented in this paper, different combinations of parameters and intervals were tested. The particular values reported in Tables 1 and 2 are only an illustrative example of the many we tested and do not represent any particular system or space mission.

7.3. Optimisation problem definition

The goal is to minimise the system mass and maximise the expected total data transmitted volume f_V with expected immediate performance given by Eq. (72). The uncertainty affects the probability of transitioning to a failure mode (reducing data volume) and the possibility to have a system mass bigger than expected. We formulate this problem by treating the expected Data Volume as a constraint and solving the following constrained min-max problem:

$$\begin{aligned} &\min_{\mathbf{d}\in D}\max_{\mathbf{u}\in U} M_{TOT}(\mathbf{d}, \mathbf{u}) \\ &s.\ t. \\ &\nu - \min_{\mathbf{u}\in U} f_V(\mathbf{d}, \mathbf{u}) \leq 0. \end{aligned} \tag{76}$$

where the worst-case scenario for the mass is such that the minimum Data Volume, over U, sent to the ground station is higher than a threshold ν. To be noted that the recovery from a partial failure is driven by the value of the design vector $\mathbf{d}$ which, in turns, affects the value of the system mass. The uncertainty domain U is defined by the Cartesian product of the intervals in Table 2. In order to facilitate the search for an optimal solution we apply an affine transformation that maps the uncertainty space into a unit hyper-cube where all the uncertainty intervals, along each dimension, are ordered and adjacent [35]. The decision domain D, instead, is defined by the Cartesian product of the intervals in Table 1. Where a continuous parameter is used in discrete or binary form, to select a particular component, its value is automatically rounded to the closest integer within the subsystem model.

7.4. Evidence Network Model and belief function estimation

The ENM describing the overall system is graphically represented in Fig. 1. The two performance indices in Eqs. (23) and (24) depend on 12 design parameters (listed in Table 1) and 20 uncertain parameters (listed in Table 2). Table 2 reports the intervals of uncertainty for each parameter with associated *bpa* in brackets. Some of the *bpa*'s were taken from Ref. [35] where the authors elicited the opinion of some ESA specialists. Other basic probability assignments were chosen to well illustrate the difference between deterministic and resilient solutions. Note that although the shape of the Belief curves depends on the particular distribution of focal elements and associated *bpa*'s, the method proposed in this paper does not depend on the particular body of evidence or uncertainty space U.

The ENM is built to model the influence of the uncertain parameters only. Hence all solid links in Fig. 1 represent the propagation of the effect of the most influential uncertain parameters. This influence is transmitted via a scalar positive quantity. In the same figure dashed lines indicate the contributions of all the subsystems to the total system mass and the total data volume. Note that after a preliminary sensitivity analysis, the dependency between Payload and TTC through δ_{inc} and ε was found to be poorly influential. Given the ENM in Fig. 1, the uncertain vector $\mathbf{u}$ can be partitioned into the uncoupled vector:

$$\mathbf{u}_u = [\delta M_{obdh}, r_f, m_{dip}, \eta_{ant}, M_{rfdn}, \delta D_c, \eta_a, \delta\rho_{sa}, \delta P_p]^T \tag{77}$$

and the coupled vector:

$$\mathbf{u}_c = [l, A_{sc}, C_D, \delta I, G_t, L_t, L_{other}, \delta P_{obdh}, h, \varepsilon, \delta_{inc}]^T. \tag{78}$$

Once the uncertain parameters are partitioned into coupled and uncoupled, one can write the total mass as an explicit function of the two groups of parameters and of the scalar exchange functions φ_{ij} (namely scalar quantities V_c^{max}, T_{ac}, V_{pl}^{max}, P_{aocs}, P_{ttc}, P_{obdh}, T_{ecl}, T_{dl} and h as represented in Fig. 1):

$$\begin{aligned} &M_{TOT} = M_{aocs}(h, r_f, m_{dip}, l, A_{sc}, C_D, \delta I)+ \\ &M_{ttc}(V_c^{max}(h), T_{ac}(h), \eta_{ant}, M_{rfdn}, G_t, L_t, L_{other})+ \\ &M_{pl} + M_{obdh}(V_{pl}^{max}(h), \delta M_{obdh})+ \\ &M_p(P_{aocs}(h, l, A_{sc}, C_D, \delta I), P_{ttc}(V_c^{max}(h), \\ &T_{ac}(h), G_t, L_t, L_{other}), P_{obdh}(V_c^{\max}(h), \delta P_{obdh}), \\ &T_{ecl}(h), T_{dl}(h), \delta D_c, \eta_a, \delta\rho_{sa}, \delta P_p) \end{aligned} \tag{79}$$

where only the dependencies on the uncertain parameters are made explicit. Note that M_{pl} does not depend on any uncertain parameter and that the values of δ_{inc} and ε in the calculation of the access time were fixed to the value coming from the worst case analysis, due to their low influence on the calculation of mass and power. Furthermore, five exchange functions, T_{ac}, T_{ecl}, T_{dl}, V_{pl}^{max} and V_c^{max}, all depend on the same uncertain parameter h, hence in the following all these links will be treated as one and a partial belief curve will be computed for the overall influence of h on the calculation of the system mass.

With this ENM and related partitioning of the uncertain vector, one can apply the decomposition proposed in Algorithm 2 and generate a lower estimation of the *Bel* with a total cost of $28 + 26N_s$ optimisations, where the parameter N_s is the number of FEs samples from the partial curves (see Eq. (21)). In comparison an exact calculation of the *Bel* would require a total of $N_{FE}^{full} = 2^{20} = 1048576$ optimisations.

To be noted that the ENM is only used to reconstruct the Belief curves and surfaces. When problem (76) is addressed, all the couplings among subsystems are considered both in the uncertainty and design spaces. Furthermore, the number of influential links that we propose for the construction of the specific ENM in Fig. 1 only serves the scope to develop an exercise that proves the effectiveness of the methodology we described in previous sections. More complex and realistic interactions among subsystems are clearly possible but do not imply a modification of the method. They would simply scale the computational complexity as in Eq. (21).

8. Results

For the case analysed in this paper, the memetic algorithm IDEA [58] was used to find both the global maxima over U and the global minimum over D in the constrained min-max problem (Algorithm 1) and in the decomposition procedure. A few preliminary runs of the min-max algorithm were used to identify a good value of IDEA's parameters. The settings used to produce the results in this section are as follows: the number of agents for the minimisation over D (Outer pop size) was set equal to the size of $\mathbf{d}$ while the number of agents for the maximisation over U (Inner pop size) was set equal to the size of $\mathbf{u}$, the maximum number of local restart is $iun = 10$, the crossover probability, $CR = 0.75$; differential weight, $F = 0.8$, the size of the convergence box $\rho_{sc} = 0.2$, the distance from the cluster centres for the global restart $\delta_{global} = 0.1$ and the dimension of the bubble for the local restart $\delta_{local} = 0.1$. Table 3 contains a summary of the values used to

Table 3
Settings of IDEA.

Parameter	Value
Inner pop size	$dim_{\mathbf{d}}$
Outer pop size	$dim_{\mathbf{u}}$
max local restarts	$iun = 10$
CR	0.75
F	0.8
ρ_{sc}	0.2
δ_{global}	0.1
δ_{local}	0.1

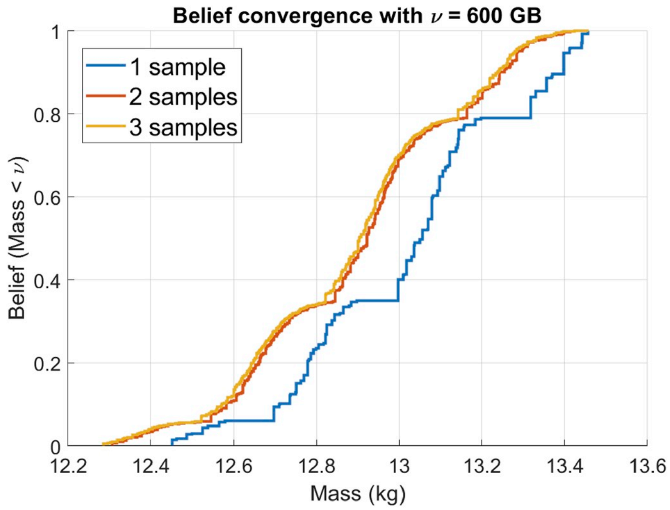

Fig. 2. Convergence of the belief curves calculated with the decomposition approach.

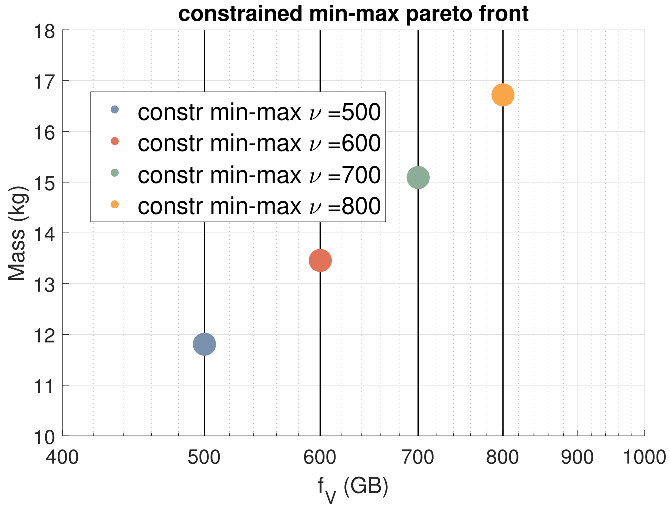

Fig. 3. Results for the constrained min-max optimisation: each point represents the minimum worst-case value in the uncertain space for both objective and constraint functions.

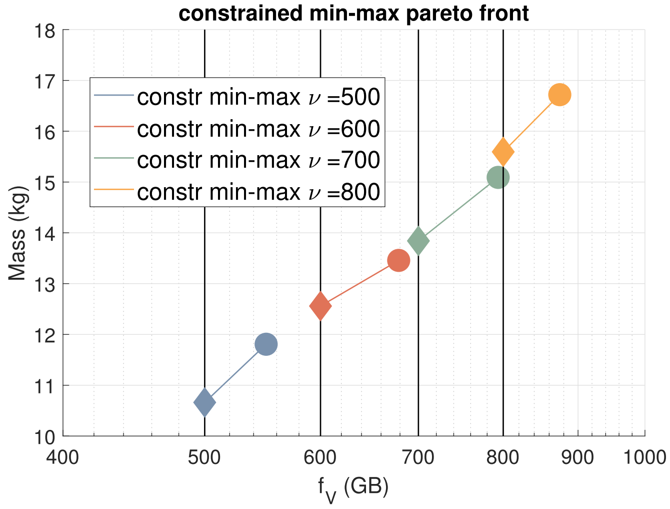

Fig. 4. Results for the constrained min-max optimisation: both the worst-cases for the mass and the constraint violation are represented.

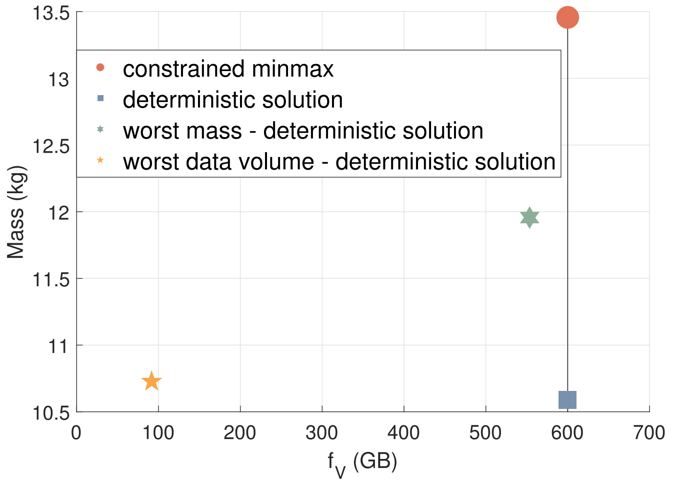

Fig. 5. Comparison, with ν = 600, of constrained and unconstrained min-max and deterministic approach.

Table 4
Design vectors of Figs. 8 and 9.

parameter	design 1	design 2	design 3	design 4	d_{minmax}	d_{opt}
t_{sl} (s)	41.730	10.000	10.081	10.000	10.000	10.000
ϕ_{sl} (deg)	41.954	50.685	78.239	52.453	53.631	75.157
f_{ttc} (GHz)	8.413	10.000	9.946	10.000	10.000	10.000
τ_{mod}	0.602	1.000	0.331	1.000	0.333	0.333
τ_{amp}	0.049	0.500	0.500	0.500	0.499	0.500
V_{bus} (V)	0.400	0.000	0.000	0.000	0.000	0.000
V_{dr} (%)	3.026	5.000	4.307	5.000	5.000	5.000
τ_{conf}	0.374	0.413	0.146	0.486	0.201	0.278
τ_p	2.380	1.000	1.069	1.000	1.000	1.000
B_D	3.837	1.000	1.075	1.000	1.000	1.000
τ_{pl}	0.852	0.343	0.045	0.259	0.061	0.022
τ_{obdh}	0.815	0.750	0.750	0.750	0.749	0.750

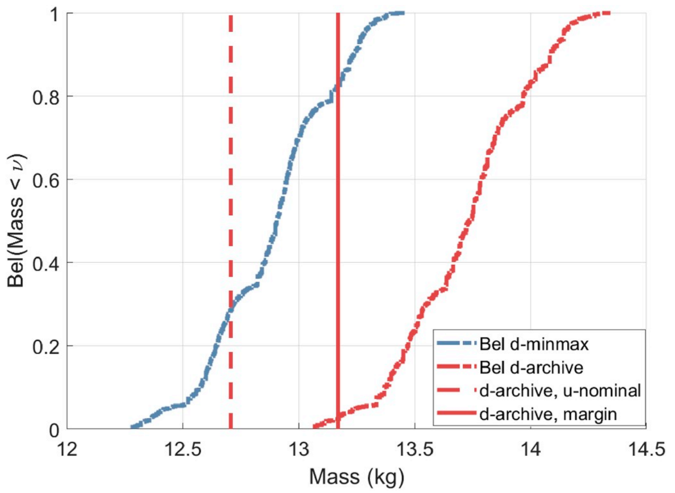

Fig. 6. Comparison between Margin approach and *ENM*.

produce the results in this section.

The total number of function evaluations for the min-max problem was set to be $2{\cdot}10^6$ while the maximum number of function calls from the optimiser for the single inner and outer loops was set to 20000. As defined in Eq. (15), in the outer loop, every time a **d** vector is evaluated, each of the **u** vectors in the archive A_u is paired with **d** and for each pair f is called. Accordingly, at each function call from the optimiser in the outer loop, f is evaluated $20000N_{Au}$ times. The algorithm calls the inner

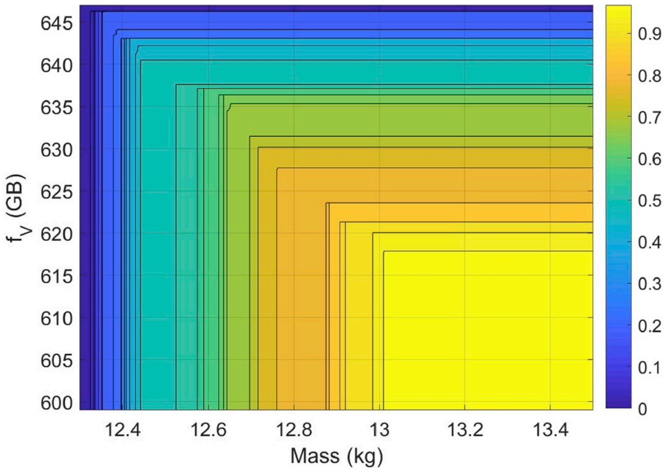

Fig. 7. Belief surface for the constrained problem formulation with the design vector $\mathbf{d}_{minmax}$. Both mass M_{TOT} and expected data volume f_V are considered.

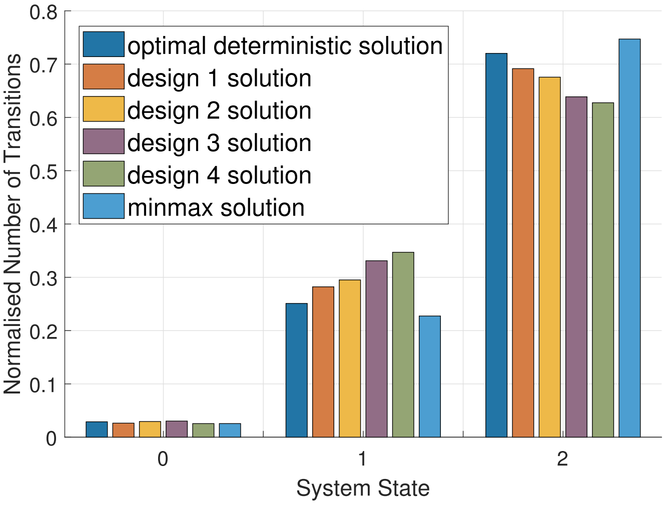

Fig. 8. Comparison of five deterministic design solutions and the resilient solution (minmax) over the number of transitions between the three system's states (0,1,2).

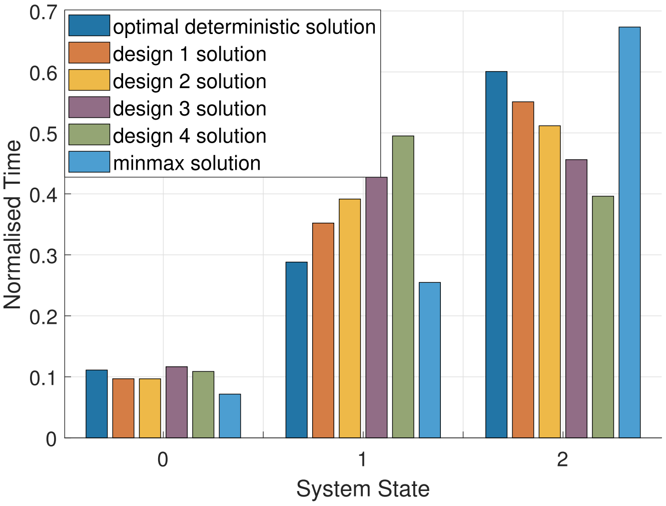

Fig. 9. Comparison of five deterministic design solutions and the resilient solution (minmax) over the time spent in each system's state (0,1,2).

loop 13 times and the outer loop 12 times. The overall number of function evaluations for the constrained maximisation in Eq. (16) is 280000, for the constraint maximisation in Eq. (17) is 280000 and for the constrained minimisation in Eq. (15) is 1440000. Considering an average time-cost of $5.5\,10^{-3}$s for the evaluation of both the function f and the constraint C, the maximum total time required for the computation of the worst case scenario would be 3 h, where more than the 63% of the computational time is used in the calculation of the expected data volume. On the other hand, over the 20 test runs we used to asses the stability of the results of the min-max (due to the stochastic nature of the optimiser), the algorithm converged to the final value in less than 200000 function calls to both constraints and objective function. This part can be greatly accelerated by improving the cost of the piece-wise interpolation of the data volume and the expectation integral.

The number of function evaluations for each maximisation in the decomposition procedure was fixed to 1000. The estimation of the final *Bel* was computed with 1, 2 and 3 samples drawn from each partial *Bel* curve, in order to show that the decomposition quickly converges to a stable solution. Fig. 2 shows the sequence of *Bel* curves computed with one, two and three samples from each partial curve, for a resilient solution computed with the constrained min-max approach. The figure shows that the curves converge as expected from below (the curve generated with one sample is more conservative than the one generated with two samples) confirming that the system models have the expected properties on an ENM. From this simple convergence analysis one can see that two samples from each partial curve are enough to produce a variation below 5% across the whole approximated *Bel* curve, i.e. using three samples would produce an approximated *Bel* that is everywhere less than 5% different from the approximation computed with two samples. Two samples from each partial *Bel* curve correspond to a total of $N_s = 2^4 = 16$ samples and $N_{FE}^{Dec} = 450$ optimisations. With a maximum time-cost of 10^{-3}s for each function evaluation (because each subsystem function is called individually), each full belief curve requires 7 min.

It is worth reminding at this point that the decomposition is used to reconstruct the belief curves and that starts from the solution of the min-max problem. The solution of the min-max problem is assumed to have $Bel = 1$. The reconstruction of the curves confirms the correctness of the min-max as no worse solution in the U space is found. Note also that a full exact reconstruction of the belief curves would require 2^{20} optimisations against the 450 required with the decomposition.

The computer used for the simulations is a Microsoft Windows 10 Pro, x64-based, Intel(R) Core(TM) i7-6700 CPU, 3.40 GHz, 3408 MHz, 4 cores, 8 Logical Processors, 8 GB (RAM) and the software is implemented in MATLAB R2018b. The solutions of the min-max problem (76) are represented in Fig. 3, for 4 different values of the threshold ν (represented by a vertical line): 500, 600, 700 and 800. For each ν the figure shows the optimal mass that corresponds to the robust design vector $\mathbf{d}_{minmax}$, which satisfies the reliability constraint in Eq. (76) for all values in the uncertain domain U.

In Fig. 4, instead, each optimal solution is represented by two points and a line that connects them. The two points correspond to the same design solution d_{minmax} but to two different uncertain vectors $\mathbf{u}$. The circle corresponds to the maximum value of the mass M_{TOT}, the diamond to:

$$\mathbf{u}_{maxC} = \underset{u \in U}{\arg\max}(\nu - f_V(\mathbf{d}, \mathbf{u})). \tag{80}$$

In all four cases the maximum constraint violation is equal to zero, thus all decision vectors $\mathbf{d}$ are always feasible. This figure also shows that the mass is maximised for a $\mathbf{u}$ vector that is inside the feasible domain.

Fig. 5 compares a particular solution from Fig. 3 (the one with $\nu = E(V) = 600$) with the solution of the following deterministic optimisation problem, where the uncertain vector $\mathbf{u}$ was set to the value $\mathbf{u}_{nom}$ (the mean value of the intervals defined in Table 2):

$$\begin{gathered}\min_{\mathbf{d}\in D} M_{TOT}(\mathbf{d},\mathbf{u}_{nom})\\ s.\ t.\\ \nu - f_V(\mathbf{d},\mathbf{u}_{nom}) \leq 0.\end{gathered} \tag{81}$$

The red point is the optimal resilient solution ($\mathbf{d}_{minmax}$, $\mathbf{u}_{minmax}$) calculated with the EBRO approach proposed in this paper, where $\mathbf{d}_{minmax}$ is in Table 4 and $\mathbf{u}_{minmax} = [2.0000{\cdot}10^{-2}$, $1.5000{\cdot}10^{-1}$, $7.0000{\cdot}10^{-1}$, $1.5000{\cdot}10^{-3}$, 2.3447, 2.6608, $6.0000{\cdot}10^{-1}$, 1.0000, 1.0000, 2.0000, $5.0000{\cdot}10^{-1}$, $8.0000{\cdot}10^{-1}$ $2.0000{\cdot}10^{1}$, $3.0000{\cdot}10^{1}$, $1.0000{\cdot}10^{2}$, $1.0000{\cdot}10^{3}$, $1.0000{\cdot}10^{1}$, $1.0000{\cdot}10^{1}$, $2.0000{\cdot}10^{1}$, $2.0000{\cdot}10^{1}]^T$. The blue square is the solution of problem (80); the green hexagram is the worst possible mass due to uncertainty, given the solution of problem (81), $\mathbf{d}^{opt}_{nom}$; the yellow pentagram is the minimum value of f_V due to uncertainty, given the design vector $\mathbf{d}^{opt}_{nom}$. From this figure one can see that by not accounting for the full variability of the uncertain parameters, problem (81) returns a solution that has a lower mass than the resilient one but violates the constraint on the data volume for some values of the uncertain parameters (yellow pentagram) and produces a worst case mass increase that also violates the constraint on the data volume (green hexagram).

In Fig. 6 we compare the resilient solution $\mathbf{d}_{minmax}$ corresponding to $f_V = 600$ from Fig. 3 with a non-resilient solution $\mathbf{d}_{archive} = [1.0007{\cdot}10^{1}$, $4.8123{\cdot}10^{1}$, 9.7875, $1.4981{\cdot}10^{-4}$, $4.0505{\cdot}10^{-1}$, $9.9803{\cdot}10^{-1}$, 4.7210, $2.4052{\cdot}10^{-1}$, 1.1660, 1.0057, $2.5439{\cdot}10^{-1}$, $7.3898{\cdot}10^{-1}]^T$ that is feasible in all the uncertain space U. The resilient solution corresponds to the dotted Bel curve in blue, while the non-resilient solution, with $\mathbf{u} = \mathbf{u}_{nom}$, corresponds to the dashed vertical line. Following the normal practice [15] and considering the satellite as an item to be developed, a 20 % margin was added to each subsystem mass of the non-resilient solution. Also a 20 % margin was added to the power requirements of the TTC, $OBDH$, $AOCS$ and $payload$ subsystems. The non-resilient solution plus margins is the solid vertical line.

One can then build the Bel curve also for the non-resilient solution (dotted line in Fig. 6). From this simple comparison one can see that the non-resilient solution without margins has $Bel = 0$ to be realised. The one with margins does not achieve $Bel = 1$ but only $Bel = 0.05$ to be realised and is oversized compared to the resilient solution. Although the non-resilient solution in this example is arbitrary, the result demonstrates that an improper quantification of uncertainty can lead to an undesirable design solution even if the recommended subsystem and system level margins are used.

Fig. 7 shows the Belief surface that corresponds to the condition:

$$Bel(M_{TOT} < \nu_M \ \wedge \ f_V > \nu_V) \tag{82}$$

where the two thresholds ν_M and ν_V are assumed to be independent from each other. While the cumulative belief distribution in Fig. 6, blue dotted line, represents the effect of uncertainty on the system mass M_{TOT} for $f_V = 600$, one could be interested in the belief that both (M_{TOT} and f_V) satisfy condition (82) at the same time. The resulting Belief-surface in Fig. 7 extends the Belief-curve in Fig. 6 by adding the evidence in support of the achievement of the values of f_V. By sectioning the surface with cuts parallel to the axes one can find, for any fixed value of f_V or M_{TOT}, the corresponding Belief-curve ($Bel(f_V > \nu_V)$ or $Bel(M_{TOT} < \nu_M)$. Fig. 7 shows that, in order to have a joint $Bel > 0.8$ that both expected data volume and mass are correct, one needs to assume a mass larger than 12.9 kg and a data volume lower than 620GBit. However, it has to be noted that the Belief values on the expected data volume were computed still using the ENM in Fig. 1. Thus one has to interpret the result in Fig. 7 as the evidence in support to the expected data volumes associated to the values of the mass that can be computed with the ENM.

In Figs. 8 and 9, finally, only the constraint function f_V is considered. Five deterministic solutions, including the optimal-deterministic solution with $\mathbf{u}_{nom}$, and the resilient solution [$\mathbf{d}_{minmax}$, $\mathbf{u}_{minmax}$] with the constraint $f_V > 600$ are compared. Table 4 lists the design vectors. The histograms show the normalised results for 10000 simulations where the time span covered by each mission is 365 days. In particular, Fig. 8 compares the total number of transitions from one state (0, 1 and 2) to another while Fig. 9 shows the cumulative time spent in each spacecraft state divided by 365 times the number of simulations.

The comparison proves that the resilient design solution increases the probability of the whole system of being in the fully functional state x_2 and decreases the number of transitions from state x_2 to the partial functioning state x_1. It also shows that the resilient solution is always the best in terms of time spent in state x_2. On the contrary, a random design solution may lead to a much longer time spent in the partially functioning state x_1. Note that all bars in the histogram correspond to the worst uncertainty vector for the expected data volume.

The optimal deterministic solution was computed using 50000 function evaluations, compared to the 200000 used to compute the resilient solution. However, the higher computational cost of the min-max solution is repaid by a lower failure rate as shown in Figs. 8 and 9. More importantly, Fig. 5 has shown that the effect of uncertainty leads to a considerable increase in mass with respect to the min-max solution and a substantial violation of the reliability constraint.

9. Conclusions

The paper introduced a method for resilience optimisation of space systems under epistemic uncertainty. It was demonstrated that this method can accommodate models for robustness and global system reliability in the same framework and produce optimised worst case solutions with problems of moderate dimension and complexity. It was also theoretically proven that the method is scalable and can handle larger dimensional systems provided that the resulting ENM has some specific properties.

The results show that the method allows for a rigorous optimisation of the complex system also when it is affected by epistemic uncertainty. A design configuration can be found that is feasible and resilient for all the possible realisations of the uncertain variables; this design configuration, furthermore, minimises the worst value of the objective function over the uncertain variables. Compared to a solution that uses standard safety margins, the resilient solution was proven to be better both in terms of resilience and performance. Furthermore, compared to an optimised solution that does not account for uncertainty, the resilient solution was shown to improve the number of transitions to a fully functional state.

It was also shown that the computational cost is affordable provided that subsystem performance and reliability metrics can be evaluated in a short time on a standard desktop. In this respect, although we argue that the properties of the ENM that allow for an efficient decomposition are common to general space systems, an approach will be proposed in future works to relax some of these properties so that more generic complex systems can be handled. Likewise, once the computational cost of individual subsystems become important compared to the overall evaluation of system performance and reliability, an approach based on hierarchical surrogate models can be used, as demonstrated in Ref. [59]. Finally the model of resilience presented in this paper is not dynamically affecting the structure of the ENM. This aspect will be investigated in future works.

Acknowledgement

The work in this paper was supported by the H2020-MSCA-ITN-2016 UTOPIAE, grant agreement 722734.

References

[1] P. Pedersen, C.L. Laursen, Design for minimum stress concentration by finite elements and linear programming, J. Struct. Mech. 10 (4) (1982) 375–391, https://doi.org/10.1080/03601218208907419 http://www.tandfonline.com/doi/abs/10.1080/03601218208907419.

[2] F.L. Silva, Otimização estrutural acoplada à interação fluido-estrutura de uma asa de aeronave tipo uav, (2011).

[3] M. Nicolich, G. Cassio, System models simulation process manangement and collaborative multidisciplinary optimization, INCOSE Italian Chapter Conference on Systems Engineering (CIISE2014), Rome, Italy, 2014 www.esteco.com.

[4] G.-J. Park, T.-H. Lee, K.H. Lee, K.-H. Hwang, Robust design: an overview, AIAA J. 44 (1) (2006) 181–191, https://doi.org/10.2514/1.13639 http://arc.aiaa.org/doi/10.2514/1.13639.

[5] M. Kalsi, K. Hacker, K. Lewis, A Comprehensive Robust Design Approach for Decision Trade-Offs in Complex Systems Design vol. 123, The American Society of Mechanical Engineers, 2001, https://doi.org/10.1115/1.1334596 https://mechanicaldesign.asmedigitalcollection.asme.org.

[6] H.-g. Beyer, B. Sendhoff, Robust optimisation: a comprehensive survey, Comput. Methods Appl. Mech. Eng. 196 (2007) 3190–3218, https://doi.org/10.1016/j.cma.2007.03.003.

[7] X. Du, W. Chen, Towards a better understanding of modelling feasibility robustness in engineering design, Tech. rep. (2000) citeseerx.ist.psu.edu/viewdoc/download?doi = 10.1.1.26.1858{&}rep = rep1{&}type = pdf.

[8] X. Zhuang, R. Pan, L. Wang, Robustness and reliability consideration in product design optimization under uncertainty, 2011 IEEE International Conference on Industrial Engineering and Engineering Management, IEEE, 2011, pp. 1325–1329, , https://doi.org/10.1109/IEEM.2011.6118131 http://ieeexplore.ieee.org/document/6118131/.

[9] E. Zio, Reliability engineering: old problems and new challenges, Reliab. Eng. Syst. Saf. 94 (2) (2009) 125–141, https://doi.org/10.1016/j.ress.2008.06.002.

[10] L. Padovan, V. Pediroda, C. Poloni, Multi Objective Robust Design Optimization of Airfoils in Transonic Field, Springer, Berlin, Heidelberg, 2005, pp. 283–295, https://doi.org/10.1007/3-540-27167-8_9.

[11] A. Clarich, C. Poloni, V. Pediroda, A competitive game approach for multi objective robust design optimization, AIAA 1st Intelligent Systems Technical Conference, American Institute of Aeronautics and Astronautics, Reston, Virigina, 2004, , https://doi.org/10.2514/6.2004-6511 http://arc.aiaa.org/doi/10.2514/6.2004-6511.

[12] V. Pediroda, C. Poloni, A. Clarich, A Fast and Robust Adaptive Methodology for Design under Uncertainties Based on Dace Response Surface and Game Theory, (2005), pp. 29–36 https://arts.units.it/handle/11368/2555015?mode = full.1219#.XNsh_9MzbyI.

[13] N. Croisard, M. Vasile, S. Kemble, G. Radice, Preliminary space mission design under uncertainty, Acta Astronaut. 66 (5–6) (2010) 654–664, https://doi.org/10.1016/J.ACTAASTRO.2009.08.004 https://www.sciencedirect.com/science/article/pii/S0094576509004019.

[14] Nasa mass growth analysis spacecraft & subsystems the nasa subsystem mass growth analysis was formulated with contributions and guidance by the following employees, Tech. rep. URL https://www.nasa.gov/sites/default/files/files/12_Larouche_NASA_Cost_Symposium_2014_MassGrowth_Final_TAGGED.pdf.

[15] S. Division, Space Engineering: Engineering Design Model Data Exchange (CDF), (2010) Tech. Rep. ECSS-TM-E-10-25A 20 October 2010 First.

[16] Tech. rep, ANSI/AIAA S-120A-201X Draft for Public Review American National Standard Mass Properties Control for Space Systems, (2015) https://www.aiaa.org/uploadedFiles/Publications/Standards/S-120A_SEC_Public_Review_andCo_ballot_Draft.pdf.

[17] D.D. Woods, D. Woods, Creating foresight: how resilience engineering can transform NASA's approach to risky decision making, Tech. rep. (2003) https://www.researchgate.net/publication/237353911.

[18] A. Madni, S. Jackson, Towards a conceptual framework for resilience engineering, IEEE Syst. J. 3 (2) (2009) 181–191, https://doi.org/10.1109/JSYST.2009.2017397 http://ieeexplore.ieee.org/document/4895241/.

[19] A.W. Wymore, Model-Based Systems Engineering, C. Press, 1993.

[20] S.A. Sheard, Twelve systems engineering roles, INCOSE Int. Symp. 6 (1) (2014) 478–485, https://doi.org/10.1002/j.2334-5837.1996.tb02042.x.

[21] J.C. Helton, J.D. Johnson, W.L. Oberkampf, C.J. Sallaberry, Representation of analysis results involving aleatory and epistemic uncertainty, Int. J. Gen. Syst. 39 (6) (2010) 605–646, https://doi.org/10.1080/03081079.2010.486664.

[22] J. Helton, Uncertainty and sensitivity analysis in the presence of stochastic and subjective uncertainty, J. Stat. Comput. Simul. 57 (1997) 3–76.

[23] W. Oberkampf, J. Helton, Investigation of evidence theory for engineering applications, AIAA 2002-1569, Denver Colorado, 4th Non-deterministic Approaches Forum, 2002.

[24] G. Shafer, A Mathematical Theory of Evidence, Princeton University Press, 1976.

[25] W. Yao, X. Chen, Y. Huang, Z. Gurdal, M. Van Tooren, Sequential optimization and mixed uncertainty analysis method for reliability-based optimization, http://arc.aiaa.org, (2013).

[26] X. Hu, X. Chen, V. Lattarulo, G.T. Parks, Multidisciplinary optimization under high-dimensional uncertainty for small satellite system design, AIAA J. 54 (5) (2016)

[27] G.P. Cimellaro, A.M. Reinhorn, M. Bruneau, Framework for analytical quantification of disaster resilience, Eng. Struct. 32 (2010) 3639–3649.

[28] D.D. Woods, E. Hollnagel, Essential Characterstics of Resilience, (2006), https://doi.org/10.1136/qshc.2006.018390.

[29] M. Ruth, S. Goessling-Reisemann, D.D. Woods, Essentials of Resilience, Revisited, Handbook on Resilience of Socio-Technical Systems (January), (2019), pp. 52–65, https://doi.org/10.4337/9781786439376.00009.

[30] J.R. Norris, Markov Chains, Cambridge University Press, New York, 2009.

[31] M. Vasile, On the solution of min-max problems in robust optimization, The EVOLVE International Conference, Jian-Guo Hotel, China, July 2014, pp. 1–4.

[32] H. Agarwal, J.E. Renaud, E.L. Preston, D. Padmanabhan, Uncertainty quantification using evidence theory in multidisciplinary design optimization, Reliab. Eng. Syst. Saf. 85 (1) (2004) 281–294 alternative Representations of Epistemic Uncertainty https://doi.org/10.1016/j.ress.2004.03.017 http://www.sciencedirect.com/science/article/pii/S0951832004000663.

[33] W. Yao, X. Chen, W. Luo, M. van Tooren, J. Guo, Review of uncertainty-based multidisciplinary design optimization methods for aerospace vehicles, Prog. Aerosp. Sci. 47 (6) (2011) 450–479, https://doi.org/10.1016/J.PAEROSCI.2011.05.001 https://www.sciencedirect.com/science/article/pii/S0376042111000340.

[34] A. Gaiddon, J.-N. Greard, D. Pagan, Automated optimization of supersonic missile performances taking into account design uncertainties, 33rd AIAA Fluid Dynamics Conference and Exhibit, American Institute of Aeronautics and Astronautics, Reston, Virigina, 2003, , https://doi.org/10.2514/6.2003-3879 http://arc.aiaa.org/doi/10.2514/6.2003-3879.

[35] S. Alicino, M. Vasile, Evidence-based preliminary design of spacecraft, in: 6thInternational Conference on Systems &Concurrent Engineering for Space Applications, Vaihingen Campus, University of Stuttgart, Germany, 08-10 October 2014.

[36] M. Vasile, G. Filippi, C. Ortega, A. Riccardi, Fast belief estimation in evidence network models, in: EUROGEN, Madrid, 13-15 September 2017.

[37] G. Filippi, M. Marchi, M. Vasile, P. Vercesi, Evidence-based robust optimisation of space systems with evidence network models, 2018 IEEE Congress on Evolutionary Computation (CEC), Rio de Janeiro, IEEE, 2018, pp. 1–8, , https://doi.org/10.1109/CEC.2018.8477917 https://ieeexplore.ieee.org/document/8477917/.

[38] S. Hosseini, K. Barker, J.E. Ramirez-Marquez, A review of definitions and measures of system resilience, Reliab. Eng. Syst. Saf. 145 (2016) 47–61 https://doi.org/10.1016/j.ress.2015.08.006 http://www.sciencedirect.com/science/article/pii/S0951832015002483.

[39] G. Fubini, Sugli integrali multipli, Rend. Acc. Naz. Lincei, 1907, pp. 608–614.

[40] M. Vasile, Robust mission design through evidence theory and multiagent collaborative search, Ann. N. Y. Acad. Sci. 1065 (2005) 152–173, https://doi.org/10.1196/annals.1370.024.

[41] S. Alicino, M. Vasile, An evolutionary approach to the solution of multi-objective min-max problems in evidence-based robust optimization, Proceedings of the 2014 IEEE Congress on Evolutionary Computation, CEC 2014, 2014, https://doi.org/10.1109/CEC.2014.6900286.

[42] Z.L. Huang, C. Jiang, Z. Zhang, T. Fang, X. Han, A decoupling approach for evidence-theory-based reliability design optimization, Struct. Multidiscip. Optim. 56 (3) (2017) 647–661, https://doi.org/10.1007/s00158-017-1680-x http://link.springer.com/10.1007/s00158-017-1680-x.

[43] Z.P. Mourelatos, J. Zhou, A design optimization method using evidence theory, https://mechanicaldesign.asmedigitalcollection.asme.org, (2006).

[44] G. Filippi, M. Vasile, A Memetic Approach to the Solution of Constrained Min-Max Problems, IEEE congress on evolutionary computation, Wellington, New Zealand, 10-13 June 2019.

[45] [link]. URL http://propagation.ece.gatech.edu/ECE6390/project/Sum2015/team3/Imaging.html.

[46] G. Gordon, W. Morgan, Principles of Communication Satellites, John Wiley and sons, Inc., 1993.

[47] Features Heritage:-3 units for world's fastest communication satellite "KIZUNA" (WINDS)-8 units for greenhouse gas observation technology satellite "IBUKI" (GOSAT)-3 units for Quasi-Zenith Satellite "MICHIBIKI" (QZSS)-6 units for Global Change Observation Mission 1st-Water SHIZUKU" (GCOM-W1), Tech. rep. URL www.meisei.co.jp/english.

[48] Features Heritage:-3 units for world's fastest communication satellite "KIZUNA" (WINDS)-8 units for greenhouse gas observation technology satellite "IBUKI" (GOSAT)-3 units for Quasi-Zenith Satellite "MICHIBIKI" (QZSS)-6 units for Global Change Observation Mission 1st-Water SHIZUKU" (GCOM-W1), Tech. rep. URL www.meisei.co.jp/english.

[49] ECAM-DVR4 Digital Video Recorder, 4-Port Features ECAM-DVR4 Application ECAM-DVR4 Malin Space Science Systems Exploration Through Imaging Space Cameras and Systems, Tech. rep. URL www.msss.com.

[50] C. M. Evan Clinton, Andris Jaunzemis, F. Wang, Satellite downlink. URL http://propagation.ece.gatech.edu/ECE6390/project/Sum2015/team5/satellite-downlink.html.

[51] Payload Data Handling System VPDHS-VECTRONIC Aerospace. URL https://www.vectronic-aerospace.com/space-applications/payload-data-handling-system-vpdhs/.

[52] C. Brown, Elements of Spacecraft Design, AIAA Education Series, 2002.

[53] J. Wertz, W. Larson, Space Mission Analysis and Design, third ed., Microcosm Press,

1999.

[54] W. Ley, K. Wittmann, W. Hallmann, Handbook of Space Technology, John Wiley and Sons, Inc, 2009.

[55] J. Castet, J. Saleh, Satellite and satellite subsystems reliability: statistical data analysis and modeling, Reliab. Eng. Syst. Saf. 94 (11) (2009) 1718–1728.

[56] E.E. Lewis, Introduction to Reliability Engineering, John Wiley and Sons, Inc, 1994.

[57] D.R. Cox, Regression models and life-tables, J. R. Stat. Soc. Ser. B 34 (2) (1972) 187–220 http://www.jstor.org/stable/2985181.

[58] M. Vasile, E. Minisci, M. Locatelli, An inflationary differential evolution algorithm for space trajectory optimisation, IEEE Trans. Evol. Comput. 15 (2).

[59] M. Di Carlo, M. Vasile, C. Greco, R. Epenoy, Aas 19-285 robust optimisation of low-thrust interplanetary transfers using evidence theory, AAS (Agents Actions Suppl.) (2019) 1–20.