70th International Astronautical Congress (IAC), Washington, D.C., US, 21-26 October 2019.

IAC–18–D1.4B.11x46693

Evidence-Based Resilience Engineering of Dynamic Space Systems

Gianluca Filippi[a]*, Massimiliano Vasile[a]

[a]*Department of Mechanical & Aerospace Engineering,University of Strathclyde, James Weir Building, 75 Montrose Street, Glasgow, United Kingdom G11XJ*, g.filippi@strath.ac.uk, m.vasile@strath.ac.uk
*Corresponding Author

Abstract

This paper will present a method for the design for resilience of complex systems under epistemic uncertainty when the characteristics of the subsystems are time-varying. In this approach, the complex system is modelled as a network of interconnected nodes, each of which is characterised by one or more quantities of interest. The quantities of interest of each subsystem are dependent on a number of decision and uncertain variables that are strictly related only to that subsystem. A set of scalar quantities, called coupling functions, exchange information between pairs of subsystems. Each pairing function is dependent on a set of coupling uncertain parameters.
The uncertainty associated to all uncertain variables is modelled using Dempster-Shafer theory of evidence. Thus the network is called Evidence Network Model (ENM). This work in particular will consider the case in which the quantity of interest of each subsystem has a state that depends on the uncertainty and can change with time. In this way we can simulate continuous transitions between fully functioning and degraded states and the effect of disruptions and shocks that can perturbed the system. One of the quantities of interest is the mass of the subsystem that we will use as generic performance indicator of the overall system. Hence, the value of the ENM is the sum of the individual masses of each subsystem. The problem is, therefore, to minimise the system mass under uncertainty while all the other quantities of interest are concurrently optimised.

Keywords: Epistemic uncertainty, Resilient satellite, Complex systems, Evidence Theory

Nomenclature

$\mathbf{d}$	Deterministic design variables
$\mathbf{u}_i$	Uncoupled uncertain epistemic variables
$\mathbf{u}_{ij}$	Coupled uncertain epistemic variables
$\mathbf{x}$	system state
ρ	reliability function
f	performance function
g	functionality function
t	Continous time variable

Acronyms

DST Dempster Shafer Theory

ENM Evidence Network Model

IP Imprecise Probability

ODE Ordinary Differential Equation (ODE)

QoI Quantity of Interest

1. Introduction

As the complexity of a system grows - being it a natural, an engineering or an organisational system - the associated risk of bad performances, failures and even disasters will increase as well. The system survives if, dealing with hazardous events, it is able to absorb disturbances and shocks and then to adapt itself to the new environment.

A good example of a bad system in this sense is given by the Columbia space mission. The Admiral Gehman and the Columbia Accident Investigation Board (CAIB) certified that the accident of 2003 was caused by the hole in the wing produced by debris. However and more important, they found the prime cause of the disaster to be addressed to the holes in organisational decision making process.

The main factors that brought the Columbia Shuttle to be

in a risky situation and then, finally, to lose totally its functionality have been found to be a common pattern also for other accidents. The first point is that, during the design process, there is production pressure that erodes safety margins and expose the system to risky scenarios. Both efficiency and thoroughness are required, where however it is impossible to have them all. Furthermore we should recognise the paradox that safety investments are most important when least affordable, that is when there is production pressure. As a second point, organisations uses to take past successes as a reason for confidence for future designs. This comes from a misinterpretation of the meaning of "past success" where the absence of failures is taken as an indication of the absence of risk. Also, and this is a third point, there is a fragmented problem solving that make confusion at the system level perspective and clouds the big picture. Finally, fourth point, there are usually problems of communication and cooperation within the organisation [1].

In the attempt to solve these problems, in the last years, concepts like "risk reduction", "vulnerability", "recovery", "resilience", ... have started to appear in the analysis and design of complex systems.

In particular, the importance of "resilience" has been officially recognised in the Hyogo Framework for Action 2005-2015 (also known as "The Hyogo Declaration") by the United Nations International Strategy for Disaster Risk Reduction (UNISDR) during the World Conference on Disaster Reduction (WCDR) on 22 January 2005.

A resilience approach in engineering is not just an improvement of the known engineering techniques, but it is a global change in the vision. It can be seen as a totally new paradigm in contrast wit the classic "development-by-accumulation" as stated by Thomas Kuhn in the book "The Structure of Scientific Revolutions".

It is not clear where "resilience" started to be investigated. Somebody says it first appeared in ecology and in its interaction with social (economical) sciences [2]. Other says physics was the cradle of this concept [3]. Other more, the most of the literature, argue that the original fields were the disciplines of psychology and psychiatry and that the first authors were Norman Garmezy, Emmy Werner and Ruth Smith [4]. These works, in particular, were focused in analysing the interaction and correlation between risks and adverse life events on children.

The definition of resilience, also, is still controversial. The original Latin word "resilio" means "to jump back". Indeed, in the review of the most important definitions of resilience in the last years (until 2006) [5] it is suggested to look at resilience" as the "intrinsic capacity of a system, community or society predisposed to a shock or stress to adapt and survive by changing its non-essential attributes and rebuilding itself". We adopt here this broad definition.

Following [5, 6], we should also make more clarity about some terms which meaning describes concepts close to resilience. We consider *fragility* to be the probability on the realisation of some undesired events. The *vulnerability* function evaluates the *loss* that is the quantification of the damage caused by the event. *Safety* is a system property, that encompasses the behaviour of and interactions among subsystems, software, organisations, and humans. The *reliability* is the ability of a components (or the whole system) to perform required functions under stated conditions for a specified period of time.

As there is not an universal definition of resilience, there is not a unique and commonly accepted quantification of it. For some important examples of the attempt to propose a common and unified framework, please refer to [7, 8, 9, 10, 11, 12, 6]. A new approach to quantify resilience is proposed in this paper.

The aim of this paper, finally, is to propose a new *resilience engineering* approach in the design of complex systems. We want the system to be optimal, thus competitive in the market, with regards to some Quantities of Interest (QoIs) while facing all the possible challenges coming from the uncertainty of the world. And we want such a solution by design.

We propose a method that can help in solving the problems listed in [1]. We adopt Imprecise Probability (IP) and in particular Dempster Shafer Theory of Evidence (DST) [13] to capture the epistemic uncertainty affecting the design of complex systems, particularly in the early design phases. We use then a graph representation to model the system and the interaction of the subsystems and components under epistemic uncertainty. For a comprehensive description of the approach please refer to the work [14] published by the authors. This framework is useful for a proper quantification and propagation of uncertainty in the design process, even under the production pressure. Also, it assures a global vision of the problem under design, reducing the risk of fragmentation.

The novelty of this paper with regards to [14] is in the proposed resilience approach.

Indeed, we suggest here a measure of *resilience* that combines the concepts of *fragility*, *reliability*, *risk* and *vulnerability*. We model the evolution of the system's state with the use of Bifurcation Theory. It allows, indeed, to capture the continuous transitions between fully functioning and degraded states as well as the occurrence of disruptions and shocks that perturb the system. Such a model can also easily model qualitative (or topological) changes in the evolu-

tion of the system state due to the uncertainty. The *reliability* of the system is considered to be the normalisation of the instantaneous state of the system. The *fragility* of the system can bring to more or less drastic *losses* in the reliability. The *resilience*, finally, is the capability of the system to recover after the shock and bring the functionality to an acceptable level. Maximising the resilience of the system minimise also the *risk* of occurrence of catastrophes while leaving the possibility, during the mission time, to have partial failures.

2. Resilience Optimisation

Two quantities of interest are considered: the performance function f

$$f: \mathcal{R}^{n+m+1} \rightarrow \mathcal{R} \tag{1}$$

$$[\mathbf{d}, \mathbf{u}, t]^T \mapsto f(\mathbf{d}, \mathbf{u}, t), \tag{2}$$

and the functionality g

$$g: \mathcal{R}^{n+m+1} \rightarrow \mathcal{R} \tag{3}$$

$$[\mathbf{d}, \mathbf{u}, t]^T \mapsto g(\mathbf{d}, \mathbf{u}, t). \tag{4}$$

Both the performance f and the functionality g depend on the time $t \in T \subset \mathcal{R}$, the design vector $\mathbf{d} \in D \subset \mathcal{R}^n$ and the uncertain vector $\mathbf{u} \in U \subset \mathcal{R}^m$.

The constrained worst-case optimisation

$$\begin{cases} \min_{\mathbf{d} \in D} \max_{\mathbf{u} \in U} f(\mathbf{d}, \mathbf{u}) \\ \forall \mathbf{u} \in U, \ \ \forall t \in T \ \ g(\mathbf{d}, \mathbf{u}, t) \leq 0 \end{cases} \tag{5}$$

is proposed to find the *resilient* design for the complex system. The *robustness* is guaranteed by the min-max optimisation of the performance f under epistemic uncertainty. The problem is then constrained with the satisfaction, in the worst scenario, of the functionality g and a reliability model is incorporated in the constraint. The combination of *robustness* and *reliability*, finally, guarantees the *resilience* of the solution.

3. Reliability Model

We model the state of the complex system with a first-order system of Ordinary Differential Equations (ODEs) that depends on the set of parameters $\boldsymbol{\mu}$:

$$\dot{\mathbf{x}} = h_{\boldsymbol{\mu}}(\mathbf{x}). \tag{6}$$

with $\boldsymbol{\mu} \in R^m$ and $\mathbf{x}_0 = x(0)$ the initial state. This type of problems are studied in the *Bifurcation Theory* [15, 16], that here we suggest because it allows to capture the continuous transition between fully functioning and degraded states as well as the occurrence of disruptions and shocks that perturb the system.

Both the initial state $x(0) = x_0$ and the parameter $\boldsymbol{\mu}$ in Eq. (6) depend on the design vector $\mathbf{d}$, the uncertain vector $\mathbf{u}$ and the time t:

$$x, x_0, \mu: \mathcal{R}^{n+m+1} \rightarrow \mathcal{R} \tag{7}$$

$$[\mathbf{d}, \mathbf{u}, t]^T \mapsto x(\mathbf{d}, \mathbf{u}, t) \tag{8}$$

$$[\mathbf{d}, \mathbf{u}, t]^T \mapsto x_0(\mathbf{d}, \mathbf{u}, t) \tag{9}$$

$$[\mathbf{d}, \mathbf{u}, t]^T \mapsto \mu(\mathbf{d}, \mathbf{u}, t), \tag{10}$$

The reliability function ρ is then evaluated as a normalisation of the solution $\mathbf{x}$ of Eq. (6). It is assumed to belong in the interval $[0,\ 1]$:

$$\rho: \mathcal{R}^{n+m+1} \rightarrow [0, 1]^T \tag{11}$$

$$[\mathbf{d}, \mathbf{u}, t]^T \mapsto \rho(\mathbf{d}, \mathbf{u}, t), \tag{12}$$

where $\rho = 1$ indicates a system fully functioning and $\rho = 0$ a system with a non recoverable failure.

Finally, ρ is incorporated in the function g which is treated as a constraint in Eq. (5).

More precisely, the functionality g combines the information, over the time, on a selected QoI with the information of the reliability ρ:

$$g(\mathbf{d}, \mathbf{u}, t) = \int_{T_0}^{T_M} QoI(\mathbf{d}, \mathbf{u}, t) \rho(\mathbf{d}, \mathbf{u}, t). \tag{13}$$

4. Autonomous Bifurcation

We introduce here some equations, in their normal form, that are commonly used to model bifurcations' phenomena. The behaviour of real dynamical systems, usually more complex, can be captured by a combination or variation of these elementary building blocks.

In this section we consider one-dimentional ODE. We consider also μ to be a scalar and time-independent parameter: $\boldsymbol{\mu} = \mu(\mathbf{d}, \mathbf{u})$,.

4.1 Tangential bifurcation

A tangential bifurcation happens when one stable and one unstable equilibria points collide and annihilate. Consider the equation:

$$\dot{x} = \mu - x^2 \tag{14}$$

This equation present the critical point μ_c = 0. For $\mu > 0$ it has two equilibria: $x = \pm\sqrt{\mu}$. The positive one is stable while the negative one is unstable. For $\mu < 0$ instead

there are no stable equilibria. $x^* = 0$ is a non-hyperbolic equilibrium. Looking at the bifurcation diagram in Fig. (1) we can however say that it is a saddle point and then it is unstable.

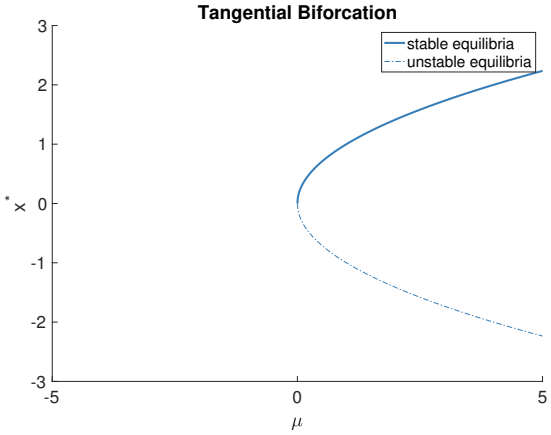


Fig. 1: Tangential Bifurcation: bifurcation graph

4.2 Trans-critical bifurcation

With a trans-critical bifurcation, the equilibria of the system exchange stability as the parameter μ crosses the critical value $\mu_c = 0$. Consider the equation:

$$\dot{x} = \mu x - x^2 \tag{15}$$

It has two equilibria points: $x^* = 0$ and $x^* = \mu$. The former is stable if $\mu < 0$ and unstable if $\mu > 0$. The latter is stable if $\mu > 0$ and unstable if $\mu < 0$. $\mu = 0$ is a critical saddle unstable point.

As for the tangential bifurcation, also for the trans-critical one it holds $f_{\mu_c}(x^*) = 0$ with $f'_{\mu_c}(x^*) = 0$. However it is also: $\frac{\partial f_\mu}{\partial \mu}(x_c) = 0$. The bifurcation plot is in Fig. (2).

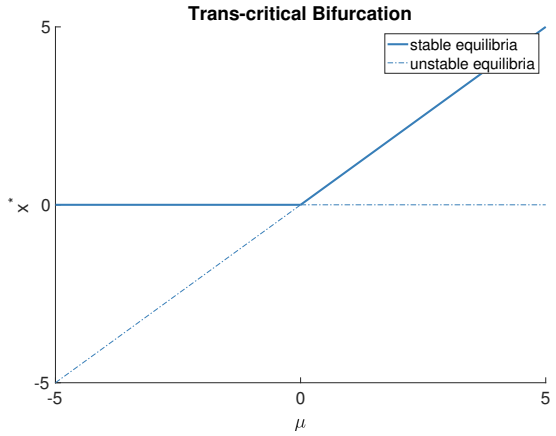


Fig. 2: Trans-critical Bifurcation: bifurcation graph

4.3 Pitchfork bifurcation

There are two types of pitchfork bifurcations. In the super-critical one,

$$\dot{x} = \mu x - x^3. \tag{16}$$

a stable equilibrium, passing through the critical point $\mu_c = 0$, becomes unstable generating other two stable equilibrium points as shown in Fig. (3).

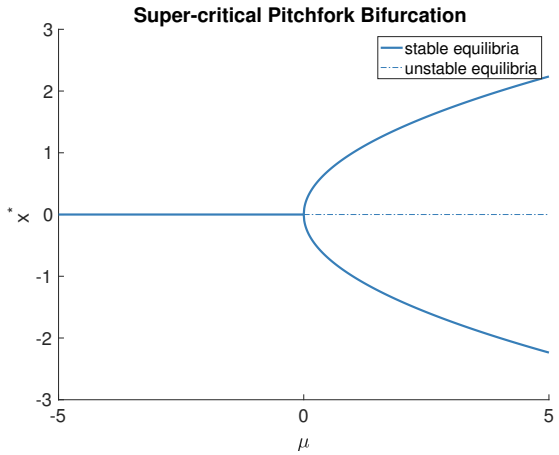


Fig. 3: Bifurcation graph: Super-critical Pitchfork bifurcation

Instead, in the sub-critical Pitchfork bifurcation,

$$\dot{x} = \mu x + x^3 \tag{17}$$

when $\mu < 0$ the dynamical system presents one stable and two unstable equilibria that, passing through the critical

point $\mu_c = 0$, collaps generating an unstable equilibrium as shown in Fig. (4).

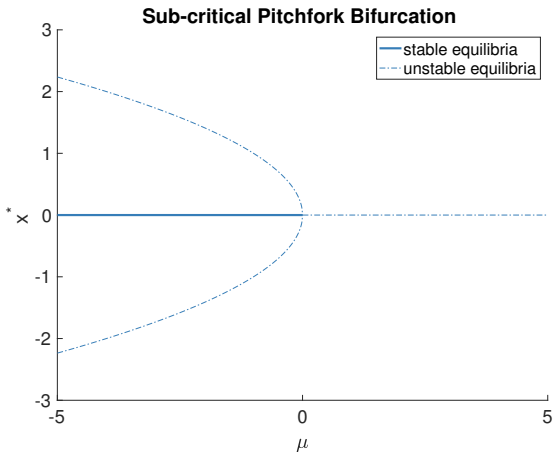


Fig. 4: Bifurcation graph: Sub-critical Pitchfork bifurcation

4.4 Bifurcation with Hysteresis

An interesting phenomenon in Bifurcation theory, is the hysteresis. It happens when, for a fixed parameter μ there exist more than one attractors. Consider, for example, the family of differential equations

$$\dot{x} = \mu + x - \frac{1}{3}x^3. \tag{18}$$

It presents two stable equilibrium sets for $-5 \leq \mu \leq \frac{2}{3}$ and for $\frac{2}{3} \leq \mu \leq 5$ and one unstable equilibria set for $-\frac{2}{3} \leq \mu \leq \frac{2}{3}$. As Fig. (5) shows, there is an overlapping between the three sets. In particular, for a fixed μ $s.t.$ $-\frac{2}{3} \leq \mu \leq \frac{2}{3}$, the system converges to different stable solution depending on the initial state x_0.

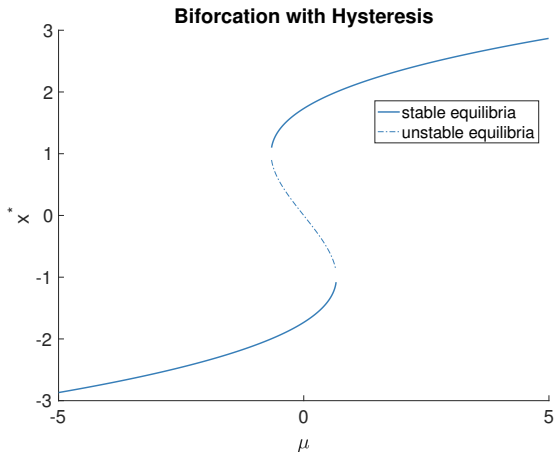


Fig. 5: Bifurcation graph: Bifurcation with Hysteresis

4.5 Hopf bifurcation

A Hopf Bifurcation occurs when a periodic solution or limit cycle, surrounding an equilibrium point, arises or goes away as a parameter μ varies.

When a stable limit cycle surrounds an unstable equilibrium point we have a *super-critical* Hopf bifurcation. When, instead, an unstable limit cycle surounds a stable equilibrium point we have a *sub-critical* Hopf bifurcation.

With a change of coordinates from Cartesian to polar, the super-critical and the sub-critical Hopf bifurcations are still represented by Figs. (3, **??**) respectively. Fig. (6) is instead a 3D phase plot of the super-critical Hopf bifurcation given by the Lienard equation:

$$\ddot{x} - (\mu - x^2)\dot{x} + x = 0. \tag{19}$$

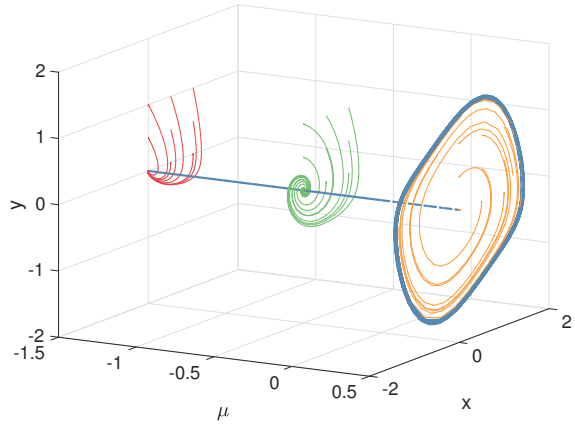


Fig. 6: super-critical Hopf Bifurcation: phase plot

Table 1: normalisation parameters

parameter	description	examples
x_{inf}	fully functional state	-5.5
x_{sup}	total failure state	5.5
$K_{-\infty}$	form factor	-1e2
K_{∞}	form factor	1e2
ϵ_ρ	minimum survival state	1e-2

5. Normalisation

In this section, we describe the normalisation procedure that is here used to reconstruct the reliability function $\rho(t)$ from the solution $x(t)$ of the sistem of ODEs.

We first have to define which value x_{inf} corresponds to the total failure $\rho = 0$ and which value x_{sup} corresponds to a total functional state $\rho = 1$. For the former we define

$$x_{inf} = \min_{\mathbf{d}\in D, \mathbf{u}\in U} x_0(\mathbf{d}, \mathbf{u}) + K_{inf} \tag{20}$$

and for the latter

$$x_{sup} = \max_{\mathbf{d}\in D, \mathbf{u}\in U} x_0(\mathbf{d}, \mathbf{u}) + K_{sup}. \tag{21}$$

with K_{inf} and K_{sup} form factors that allow to adapt the reliability function $\rho(t)$ shifting and stretching it.

We define also for which values ($K_{-\infty}$ and K_{∞}) the solution is considered to diverge. In particular:

$$x(t) \begin{cases} \text{is divergent} & \text{if } x(t) < K_{-\infty} \wedge x(t) > K_{\infty} \\ \text{is not divergent} & \text{if } K_{-\infty} \leq x(t) \leq K_{\infty} \end{cases} \tag{22}$$

The following equation is finally used to evaluate the function ρ:

$$\rho(t) = \min\left(\frac{\max(x(t)k(t) - x_{inf}, 0)}{x_{sup} - x_{inf}}, 1\right) b(t) \tag{23}$$

where $k(t)$ is a correction factor that modifies the solution when the state x diverges to $+\infty$:

$$k(t) = \begin{cases} 1 & \text{if } x(t) < K_{\infty} \\ \text{-1} & \text{if } x(t) \geq K_{\infty} \end{cases} \tag{24}$$

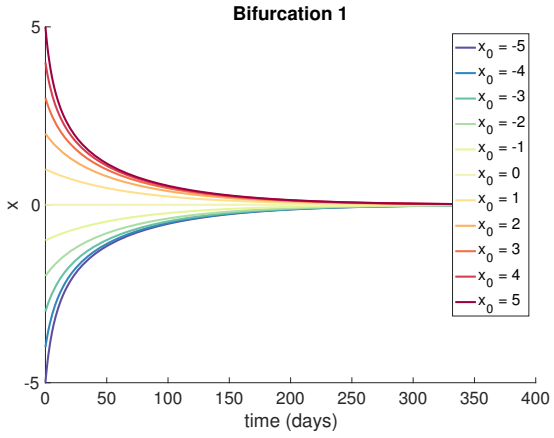
and $b(t)$ take into account the minimum accepted level for ρ:

$$b(t) = \begin{cases} 1 & \text{if } \rho(t) > \epsilon_\rho \\ 0 & \text{if } 0 \leq x(t) \leq \epsilon_\rho \end{cases} \tag{25}$$

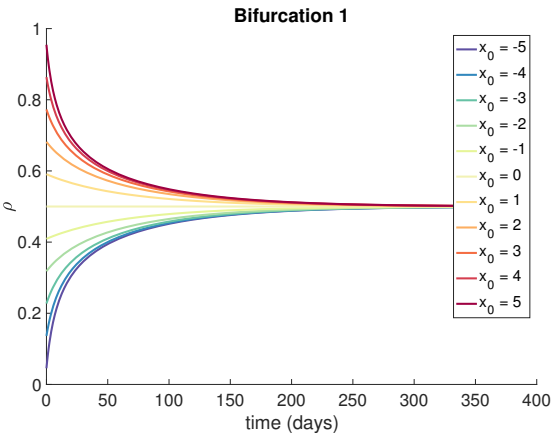
Table (1) lists the parameters used for the normalisation with the corresponding values for the examples in Figs. (7, 8, 9, 10, 11, 12, 13, 14, 15).

In particular Figs. (7, 8) refer to the super-critical pitchfork bifurcation in Eq. (16) and.Figs. (9,10) to sub-critical pitchfork bifurcation in Eq. (17). Figs. (7a,10a) plot the solution $x(\mathbf{d}, \mathbf{u}, t)$ of the system of ODEs while Figs. (7b, 9a) are the scalarised solution $\rho(\mathbf{d}, \mathbf{u}, t)$.

The results have been calculated for $x_0 \in [-5,\ 5]^T$ and for the two extrema values of the parameter $\mu = [-5,\ 5]^T$. From the figures, we see that the scalarisation preserves the qualitative behaviour of the curve. The reliability function assumes values $0 \leq \rho \leq 1$. When the solution x diverges for both positive or negative values, ρ becomes zero. If the system reduces ρ below the minimum accepted ϵ_ρ, then there is not possibility to recover.

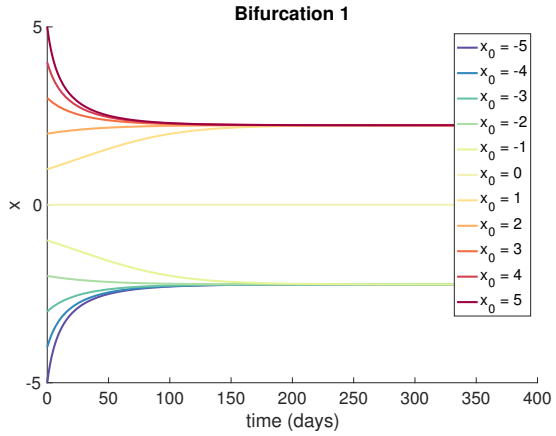


(a) state equation $x(t)$

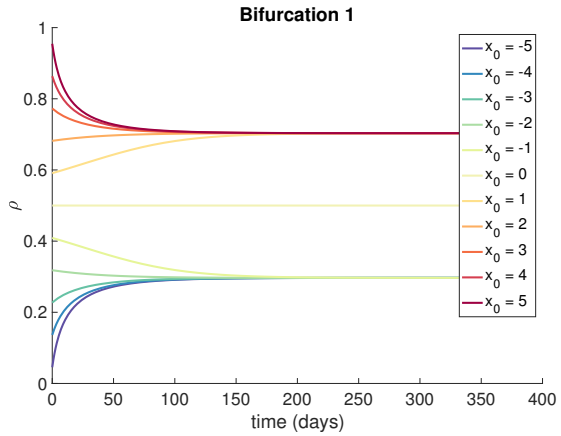


(b) reliability $\rho(t)$

Fig. 7: Evolution in time of the normalised state with μ=5 and different initial points x_0.



(a) state equation $x(t)$



(b) reliability $\rho(t)$

Fig. 8: Evolution in time of the state with μ=5 and different initial points x_0.

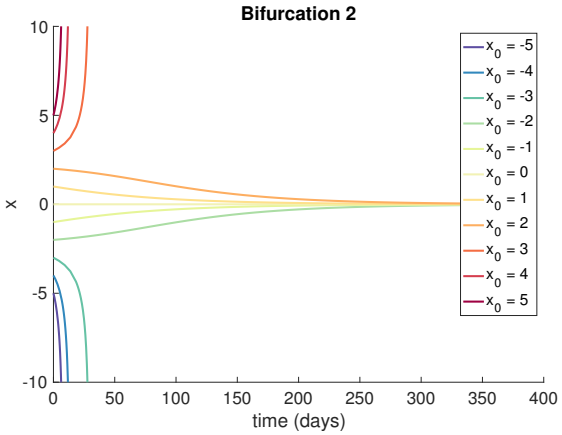
6. Non Autonomous Bifurcation ($\mu(t)$)

This section shows some possible combinations or variations of the previously listed bifurcation equations in order to describe the qualitative evolution in time of the reliability of the system.

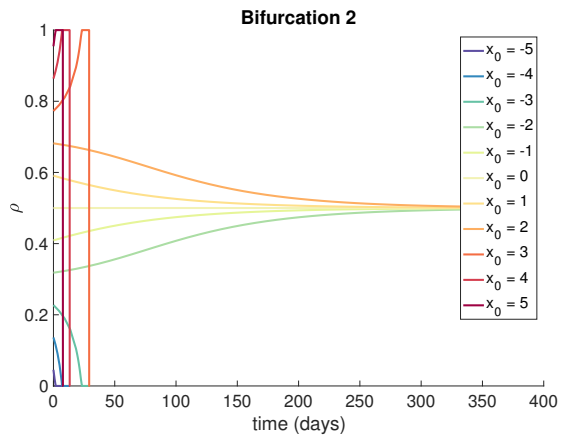
We are particularly interested in modelling:

- smooth degradation and/or recovery (subsection 6.1);
- shock (subsection 6.2): a discontinuity in ρ for both loss or recovery;
- shock followed by recovery (subsection 8.4).

All these behaviours can be described with a non-autonomous bifurcation model where the parameter

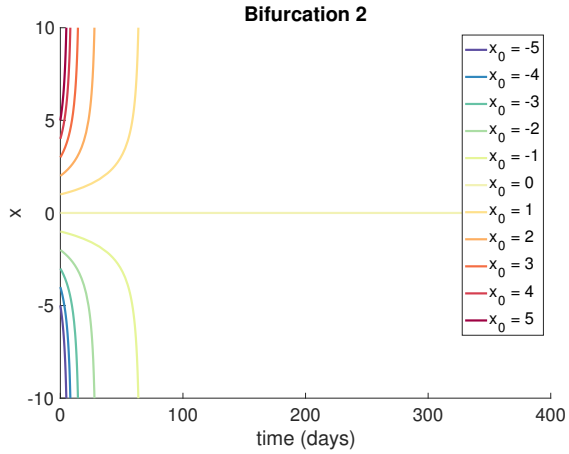


(a) state equation $x(t)$

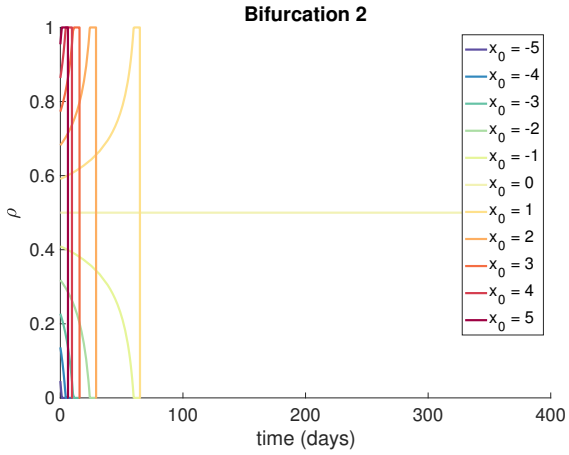


(b) reliability $\rho(t)$

Fig. 9: Evolution in time of the state with μ=-5 and different initial points x_0.



(a) state equation $x(t)$



(b) reliability $\rho(t)$

Fig. 10: Evolution in time of the normalised state with μ=5 and different initial points x_0.

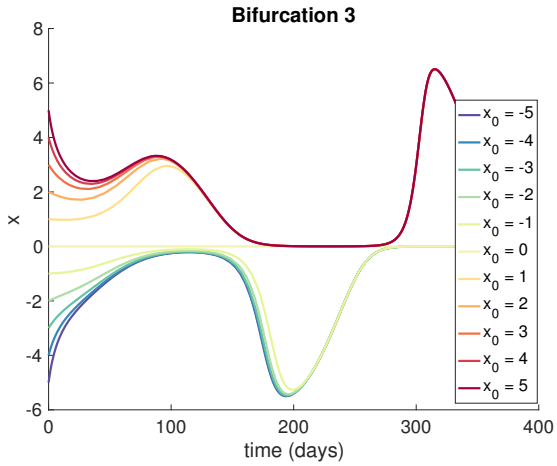
$\mu(\mathbf{d}, \mathbf{u}, t)$ is time dependent.

6.1 Smooth Degradation and Recovery

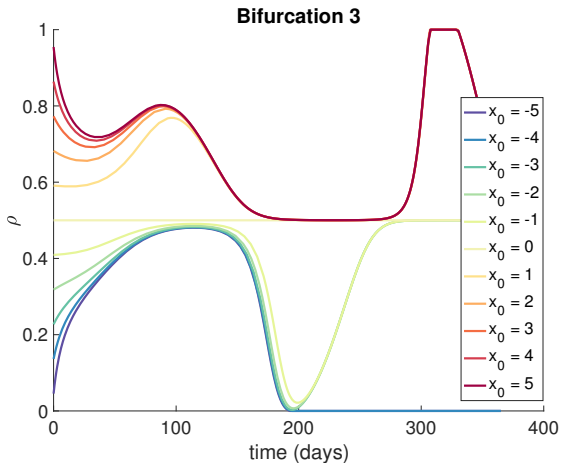
We show here how to model a smooth degradation and/or recovery. The reliability ρ is modelled with the supercritical pitchfork bifurcation in Eq. (16), where the parameter μ is:

$$\mu(t) = 13.8\mu_0 t \sin(10t)\,\mathrm{sign}(x_0). \tag{26}$$

where $\mu_0 = \mu(0)$ the initial value of the parameter μ. As μ assumes a new value, the stable and unstable equilibria change according to Fig. (3). Figs. (11) show the effect of Eq. (26) on the dynamical system.



(a) state equation $x(t)$



(b) normalised state equation $\rho(t)$

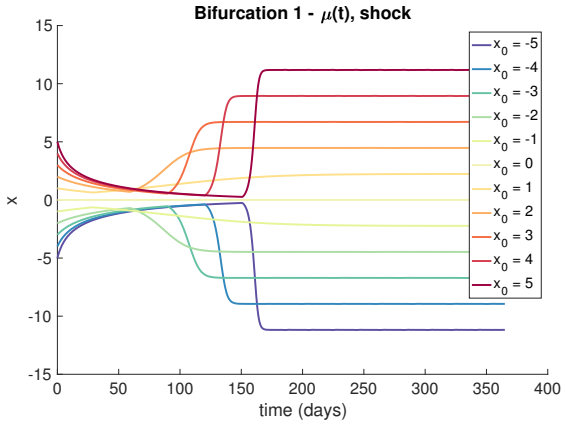
Fig. 11: Evolution in time of the state with μ_0=5 and different initial points x_0.

6.2 Shock or Recovery

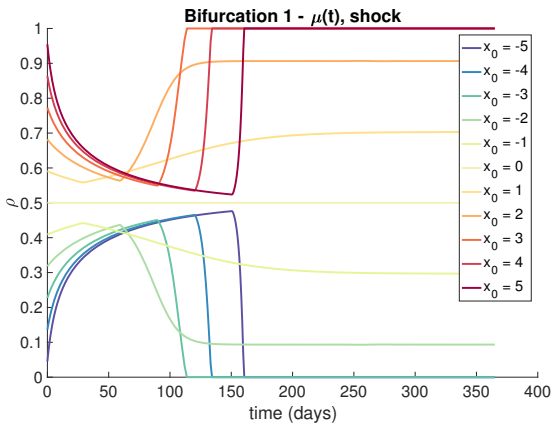
The effect of a shock on the system can be simulated with an abrupt variation of the value of μ over time. In the example plotted in Figs. (12, 13), Eq. (16) is still used. The parameter μ is however determined as:

$$\mu(t) = \begin{cases} \mu_0 & \text{if } t < \max(10, 30|x_0|) \\ -x_0^2\mu_0 & \text{if } t \geq \max(10, 30|x_0|). \end{cases} \tag{27}$$

Looking at Figs. (12, 13), we can see that the parameter $\mu(t)$ allows to a switch between the different equilibrium points of Fig. (3). This switch can be slow or fast depending on the magnitude of the discontinuity introduced by $\mu(t)$. The variation of the state can go in both the direction of degradation or recovery.

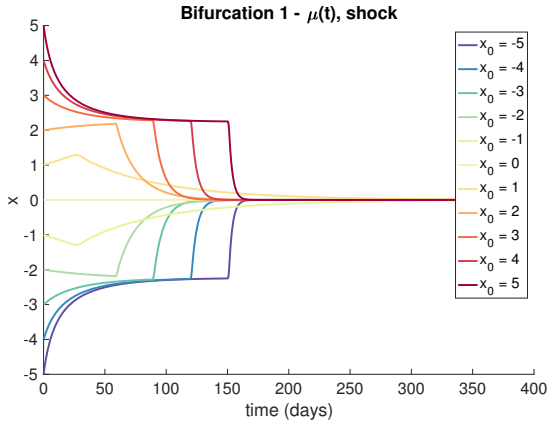


(a) state equation $x(t)$

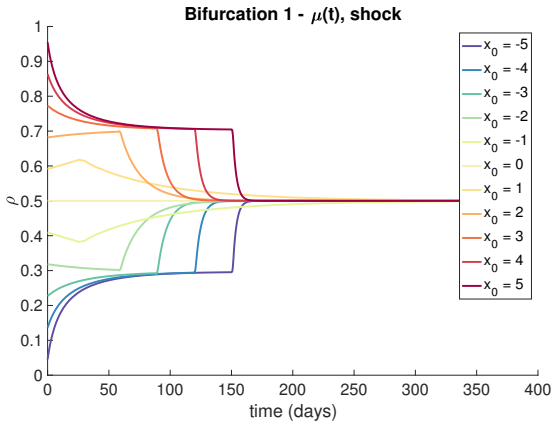


(b) normalised state equation $\rho(t)$

Fig. 12: shock.



(a) state equation $x(t)$



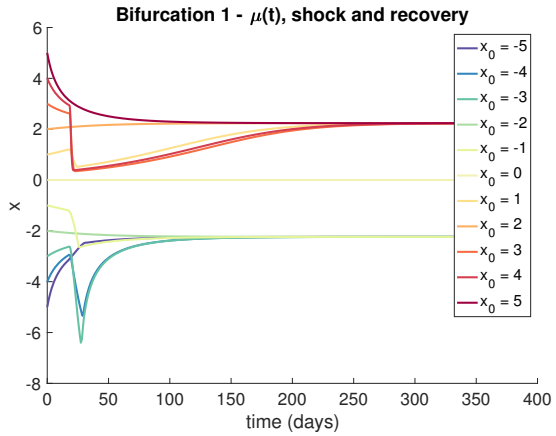
(b) normalised state equation $\rho(t)$

Fig. 13: Shok.

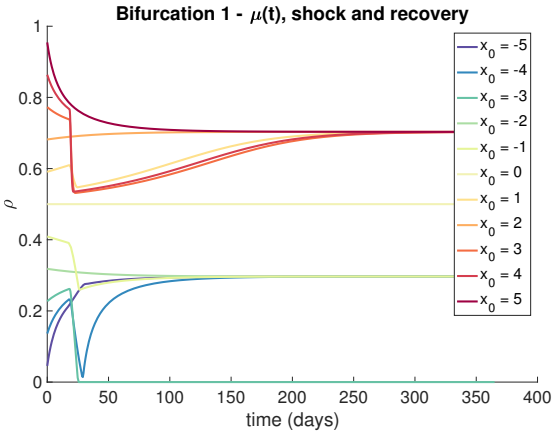
6.3 Shock and Recovery

We model here a shock followed by a recovery where the recovery is still possible iff the shock does not bring to a total failure ($\rho > \epsilon_\rho$ after the shock). Considering again the Eq. (16), the parameter μ is here modelled as

$$\mu(t) = \begin{cases} \mu_0 & \text{if } t < 20 \vee t > 20 + |x_0 - 5| \\ -2x_0|5 + x_0||\mu_0| & \text{if } 20 \leq t \leq 20 + |x_0 - 5| \end{cases} \tag{28}$$



(a) state equation $x(t)$



(b) normalised state equation $\rho(t)$

Fig. 14: Shock.

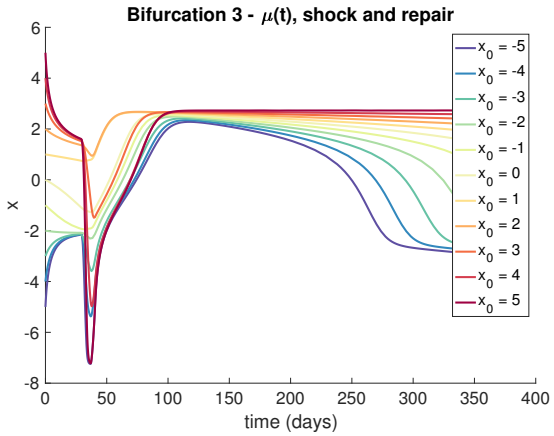
6.4 use of the unstable equilibria

The use of Eq. (**??**) to model the effect of degradation, failures and catastrophes, however, brings to a limitation. It is indeed only possible to change the state of the system while staying in the same area between the three possible that are determined by the curve in Fig. (**??**): a system with an initial state $0.5 \leq \rho \leq 1$ will always remain in that interval while a total failure can happen only if the initial state is $0 \leq \rho < 0.5$. This feature persists with Eq. (**??**) and it can be neglected by the use of a bifurcation with hysteresis.

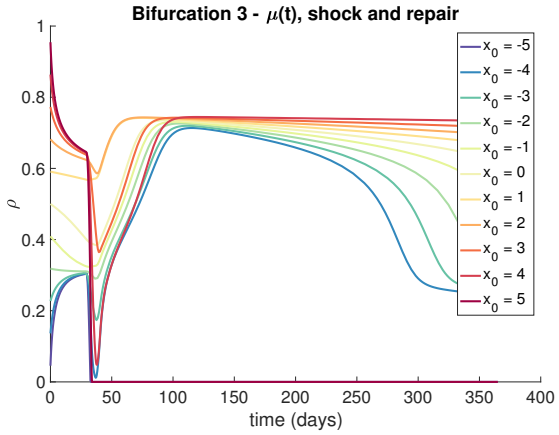
Consider, for example, the Eq. (4.4). If we model μ as

$$\mu(t) = \begin{cases} \mu_0 & \text{if} \\ -2x_0|5 + x_0||\mu_0| & \text{if} \end{cases} \tag{29}$$

we get the Figs. (15).



(a) state equation $x(t)$



(b) normalised state equation $\rho(t)$

Fig. 15: Shock, recovery and degradation with *Bifurcation3*

7. Test Case

The method is here applied to the design for resilience of a spacecraft. The space system is modelled as a network:

Table 2: Spacecraft model - design parameters

design parameter	N	sub-system
width for square detector	d_1	Payload
quality factor for imaging	d_2	Payload
operating wavelength	d_3	Payload
obdh type	d_4	OBDH
compression factor	d_5	OBDH
slew angle	d_6	AOCS
time for slew manuvers	d_7	AOCS
frequency	d_8	TTC
modulation	d_9	TTC
amplifier type	d_{10}	TTC
cell type	d_{11}	Power
bus voltage	d_{12}	Power
allowed bus drop	d_{13}	Power

Table 3: Spacecraft model - uncertain parameters

uncertain parameter	N	sub-system
altitude	u_1	Orbit
elevation angle	u_2	Orbit
inclination	u_3	Orbit
maximum incidence angle	u_4	Payload
max ground sampling distance	u_5	Payload
Δ mass	u_6	OBDH
Δ power	u_7	OBDH
antenna efficincy	u_8	TTC
antenna gain	u_9	TTC
mass distribution network	u_{10}	TTC
cell packing efficiency	u_{11}	Power
harness mass factor	u_{12}	Power
worst case angle of incidence	u_{13}	Power

each subsystem corresponds to a node and each dependency to a link, as Fig. (16) shows.

The design $\mathbf{d}$ and uncertain $\mathbf{u}$ parameters are listed in Tabs. (2,3) together with the corresponding sub-systems.

The mass of the whole system is chosen to be the QoI modelled by the performance function in Eq. (1). The mass is time-independent and it is the sum of the masses of all the subsystems:

$$f \coloneqq mass(\mathbf{d},\mathbf{u}) = \sum_{i=1}^{6} mass_i(\mathbf{d}_i,\mathbf{u}_i,h_i(\mathbf{d}_{ij},\mathbf{u}_{ij})) \quad (30)$$

where h_i is the set of coupling function between node i and all the nodes that are linked to it. The total volume of compressed data generated during the mission, instead, is the functionality in Eq. (3). This quantity is calculated integrating over time the product of the compressed data volume DV^c and system state function ρ:

$$g \coloneqq DV^c_{tot}(\mathbf{d},\mathbf{u},t) = \int_{T_0}^{T_M} DV^c(\mathbf{d},\mathbf{u},t)\rho(\mathbf{d},\mathbf{u},t)dt. \quad (31)$$

The optimisation for resilience in Eq. (5) can be then reformulated as:

$$\begin{cases} \min_{d\in D} \max_{u\in U} Mass(\mathbf{d},\mathbf{u}) \\ s.t. \;\; \forall \mathbf{u}\in U, \;\; DV^c_{tot}(\mathbf{d},\mathbf{u},t) \geq \nu \end{cases} \quad (32)$$

We want to optimise the satellite considering the worst case in the uncertainty for both performance and functionality. In other terms, we want to minimise the satellite mass while ensuring a minimum amount of compressed data volume for any possible scenario in the uncertainty space. With regard to the constraint function, the goal is to maximise the area subtended by the curve g. This could bring to a penalisation of the QoI if it means a significant increase for the reliability ρ, or vice versa. Also, a design configuration that could bring to shocks in the resilience function ρ, can be an optimal solution if it guarantees a recovery and a good functionality state after the shock.

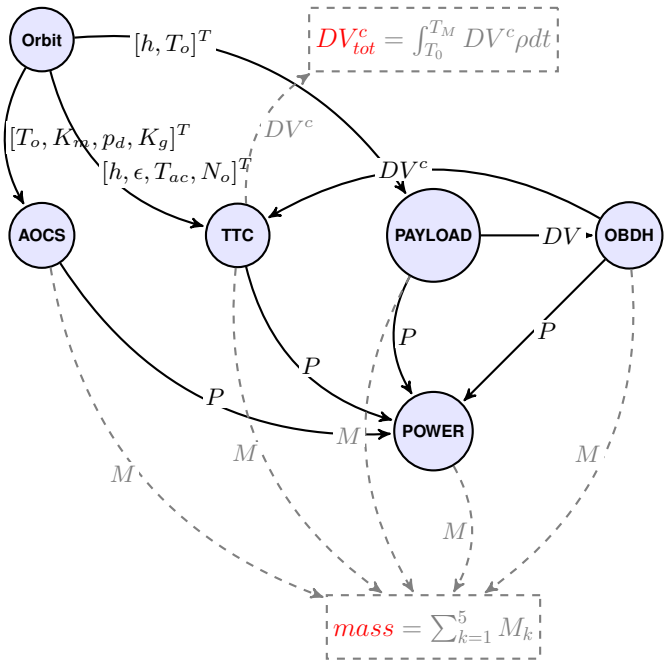


Fig. 16: Representation of the spacecraft as a complex system. The two quantities of interest are the mass of the $mass$ and the total amount of data compressed by the OBDH sub-system DV^c.

8. Results

Solving the single-objective constrained problem in Eq. (32) for different thresholds ν is an approach to reconstruct the trade-off between performance $f = mass$ and functionality $g = DV^c_{tot}$.

For the sake of simplicity and clarity, we apply the reliability model only to the node $OBDH$ and we focus only on one design parameter, d_5, and one uncertain parmeter, u_6. The unconstrained min-max problem

$$\min_{d\in D} \max_{u\in U} Mass(\mathbf{d}, \mathbf{u}) \tag{33}$$

is first solved. Problem (33) gives $d_5 = 0.2$ with $d_5 \in [0.2, 0.6]$ and $u_6 = 20$ with $u_6 \in [0, 20]$. The parameter $\mu(\mathbf{d}) \propto d_5$ in subsection 8.1 and the initial value $x_0(\mathbf{d}) \propto d_5$ in subsection 8.2 has been finally set in order to have a trade-off between f and g.

Subsections 8.1 and 8.2 show the pareto fronts when the reliability function ρ is modelled with the super-critical pitchfork bifurcation in Eq. (16). Subsection 8.3 presents the results of the sub-critical Pitchfork bifurcation. Subsection 8.4 is about the shock and recovery problem in Eq. (29).

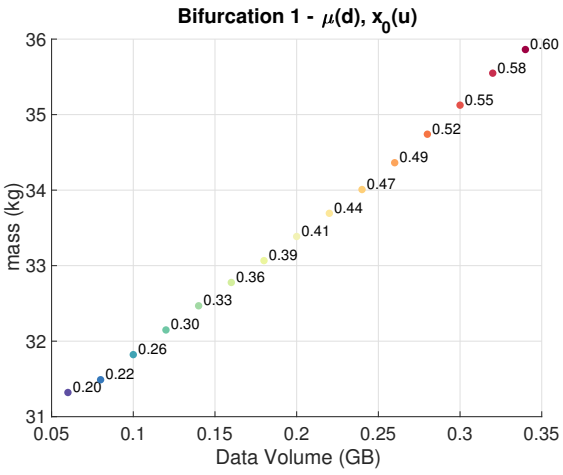
8.1 Super-critical Pitchfork Bifurcation with $\mu(d)$, $x_0(u)$

We use here the Eq. (16) and we consider the parameter $\mu \propto d_5$ to be a design variable and the initial point $x_0 \propto u_6$ to be uncertain. The results of Eq. (32) with different values for the threshold ν are then plotted in Fig. (17).

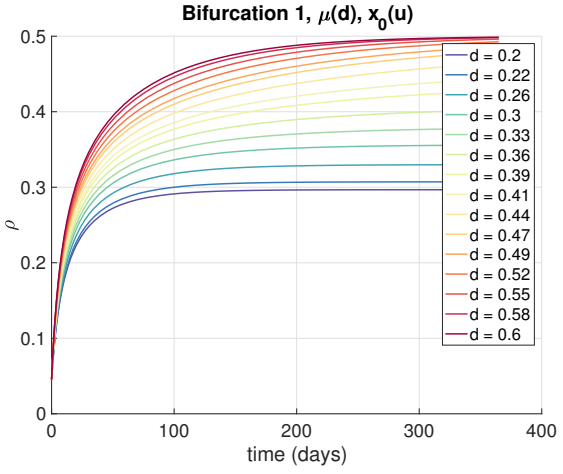
Figs. (7a,8a) show that for both negative and positive values of μ the minimum reliability (the area below the curve) is always given by $x_0 = -5$. The pictures show the particular cases $\mu = -5$ and $\mu = 5$ but the curves change linearly as show in Fig. (3). The maximum area in the worst scenario, then, corresponds to $\mu = -5$.

The parameter μ interpolates the values $\{5, -5\}$ over the design parameter $d_5 \in [0.2,\ 0.6]^T$. In this way, the model has been set such that $\mu = d_5 = 0.2$, that is optimal for the mass is also the worst for the reliability function. Progressing to $\mu = d_5 = 0.6$, then, it becomes optimal for ρ but the worst for the mass.

Due to the tension between performance and functionality, constraining the satellite to have an increasing g with different thresholds ν in Eq. (32), forces the solution to progressively move d_5 from $d_5 = 0.2$ to $d_5 = 0.6$. In this way the constraint can be satisfied but on the other hand the mass increases. This trade off is well represented in Fig. (17a).



(a) Pareto front.

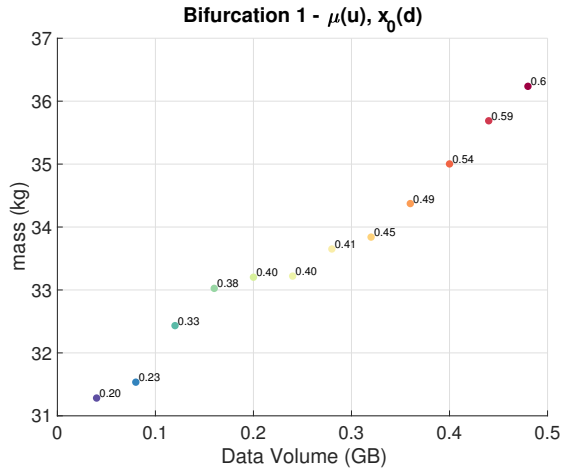


(b) Reliability curve ρ.

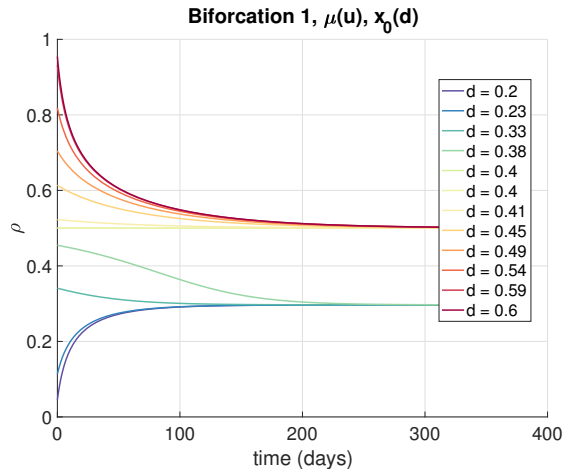
Fig. 17: Optimal resilient solution with different threshold for the compressed data volume DV^c_{tot}

8.2 Super-critical Pitchfork Bifurcation, $\mu(u)$, $x_0(d)$

The problem of the previous subsection 8.1 is here inverted: the parameter μ and the initial point x_0 are treated as uncertain and decision variable respectively. With a symmetrical interpolation with respect to subsection 8.1, a trade-off between f and g is due to the parameter $x_0 = d_1$. The pareto front with the corresponding values of d_1 and the reliability curves ρ are presented in Figs. (18).



(a) Bifurcation 1

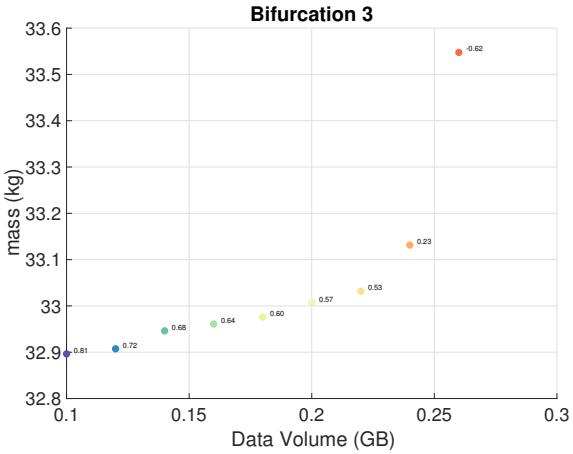


(b) Bifurcation 2

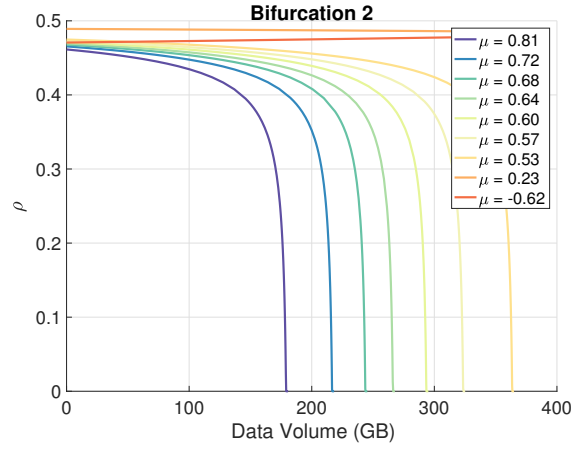
Fig. 18: Stable and unstable equilibria for the equations

8.3 Sub-critical Pitchfork Bifurcation

The parameter μ interpolates the values $\{5, -5\}$ over the parameter $d_5 \in [.2 \ \ .6]^T$, while the initial state x_0 interpolates the values $\{0, -|\mu|\}$ over the parameter $u_6 \in [0 \ \ 20]^T$. As d_5 leave the optimal value for the unconstrained problem $d_5 = 0.2$ and moves to $d_5 = 0.6$ worsening the mass, the reliability ρ increases linearly shifting the plot from Fig. (10b) to Fig. (9b). However, as $|d_5|$ increases, also the uncertainty on the initial point grows. The results are plotted in Figs. (19). Up to a certain threshold $\nu < 0.25$, the optimal solution is found for values of d_5 that are close to the optimal unconstrained solution $d_5 = 0.2$ and that generate a positive μ. For bigger thresholds, instead, the optimiser is forced to choose values of d_5 far from the optimal unconstrained solution that also increases the uncertainty on the initial point x_0 with a further increase in the mass.



(a) Bifurcation 1



(b) Bifurcation 2

Fig. 19: Stable and unstable equilibria for the equations

8.4 Shock and Recovery on the Hysteresis Bifurcation, $\mu(d,t)$, $x_0(u)$

Here we make a comparison between the optimal solution calculated with nominal values for the uncertain variables (*optimal-nominal*), and the resilient solutions we propose. The *optimal-nominal* design

$$\begin{cases} d^* = \text{argmin}_{\mathbf{d}\in D}\, Mass(\mathbf{d}, \mathbf{u}_{nom}) \\ s.t.\;\; DV^c_{tot}(\mathbf{d}, \mathbf{u}_{nom}, t) \geq 0.2 \end{cases} \tag{34}$$

is calculated considering the nominal values $\mathbf{u}_{nom}$ for the uncertain parameters equal to the mean between their lower and upper bounds. It is plotted in blue in Figs. (20).

We can however explore the uncertain space to understand better the worst possible scenarios in the uncertain space. Fixing d^* we then calculate the worst condition in terms of performance f:

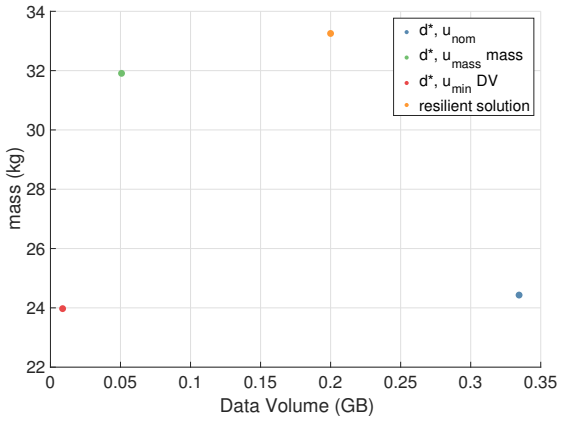
$$\max_{\mathbf{u}\in U} mass(\mathbf{d}^*, \mathbf{u}) \tag{35}$$

and the worst condition in terms of functionality g:

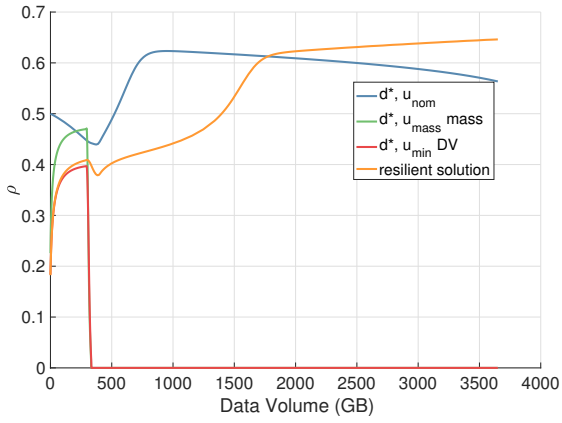
$$\min_{\mathbf{u}\in U} DV^c_{tot}(\mathbf{d}^*, \mathbf{u}). \tag{36}$$

These two solutions are plotted respectively in green and red in Figs. (20). We see that the *optimal-nominal* solution has an associated risk to not satisfy the requirements in the data volume and also to cause an increase of the mass of the final satellite during the design process.

We propose, finally, in orange in Figs. (20), the resilient solution from Eq. (32). It gives the minimum mass of the satellite in the worst condition while satisfying the constraint over all the possible uncertain scenario. Looking at Figs. (20), the orange mass is considerably bigger than the blue one and even bigger than the green. However the orange design assures to satisfy always the constraint, while the blue solution can lead to a drastic reduction of the data volume produced by the satellite. Furthermore, looking at Fig. (20b), the resilient solution is able to absorb the shock in the worst scenario and recover after that, while the blue design brings to the red curve in the worst condition and it represent a total failure without possibilities to recover after the disruption.



(a) state equation $x(t)$



(b) normalised state equation $\rho(t)$

Fig. 20: Shock, recovery and degradation with *Bifurcation3*

9. Conclusions

In this paper we presented an approach for the design of complex systems with an application to space engineering. In particular we focused here in the quantification of *Resilience* and it's integration in an optimisation process. This

approach has been applied to the ENM presented by the authors in previous publications where the complex system is described as a network, or graph. However what has been presented about the design for resilience is general and can be used in different contests.

We suggested that the dynamical behaviour of the resilience of the system (and its components) can be described by systems of ODEs. More precisely, we showed that the bifurcation theory is particularly suitable. Indeed, it gives to some parameters the power to change qualitatively the evolution in time of the functional state of the system. These parameters are here function of design and uncertain variables and this allows to better quantifies all the possible scenario given by uncertainty in the design of a real complex (aerospace) system.

We presented in the paper how the resilience model influences the search of the optimal solution. The resilient solution, through the smallest possible penalisation of the performance, assures, for a given threshold, the minimisation of the risk. Furthermore, resilience is not a rigid constraint but it leaves to the optimiser (complex system) the possibility to explore a variety of configurations and strategically accept a failure (or a penalisation) if it will bring to an advantage in the optic of the entire mission. The trade-off between performance and resilience has also been used to reconstruct the Pareto front for a multi-objective analysis.

The work will be extended in a variety of directions. First, an analogy will be studied to reflect in the resilience model the physical behaviour of the engineering system. A more realistic integration of the resilience model in the graph representation within ENM will be explored to study the interaction between the bifurcations of the subsystems for the optimisation of the performance and the functionalities of the whole complex system. Finally, more complicated and interesting phenomena will be analysed with the help of chaos theory.

Acknowledgement

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

References

[1] David D Woods and David Woods. *Creating Foresight: How Resilience Engineering Can Transform NASA's Approach to Risky Decision Making*. Tech. rep. 2003. URL: https://www.researchgate.net/publication/237353911.

[2] Charles Perrings. "Introduction: Resilience and sustainability". In: *Environment and Development Economics* 3.2 (1998), pp. 221–262. ISSN: 14694395. DOI: 10.1017/S1355770X98210126.

[3] S.E. Van der Leeuw and C.A. Leygonie. *A long term perspective on resilience in socio-natural systems*. 22–26 May 2000.

[4] J.L. Johnson and S.A. Wielchelt. "Introduction to the special issue on resilience". In: *Substance Use and Misuse* 39.5 (2004), pp. 657–670.

[5] Van Der Leeuw. "The concept of resilience revisited". In: *Disasters* 30.4 (2006), pp. 433–450.

[6] Gian Paolo Cimellaro, Andrei M. Reinhorn, and Michel Bruneau. "Framework for analytical quantification of disaster resilience". In: *Engineering Structures* 32.11 (2010), pp. 3639–3649. ISSN: 01410296. DOI: 10.1016/j.engstruct.2010.08.008. arXiv: arXiv:1011.1669v3. URL: http://dx.doi.org/10.1016/j.engstruct.2010.08.008.

[7] Michel Bruneau et al. "A Framework to Quantitatively Assess and Enhance the Seismic Resilience of Communities". In: *Earthquake Spectra* 19.4 (2003), pp. 733–752. ISSN: 87552930. DOI: 10.1193/1.1623497.

[8] Michel Bruneau and Andrei Reinhorn. "Exploring the concept of seismic resilience for acute care facilities". In: *Earthquake Spectra* 23.1 (2007), pp. 41–62. ISSN: 87552930. DOI: 10.1193/1.2431396.

[9] Scott B. Miles and Stephanie E. Chang. "Modeling community recovery from earthquakes". In: *Earthquake Spectra* 22.2 (2006), pp. 439–458. ISSN: 87552930. DOI: 10.1193/1.2192847.

[10] "A selection of papers". In: (2004).

[11] Stephanie E. Chang and Masanobu Shinozuka. "Measuring improvements in the disaster resilience of communities". In: *Earthquake Spectra* 20.3 (2004), pp. 739–755. ISSN: 87552930. DOI: 10.1193/1.1775796.

[12] Gian Paolo Cimellaro, Andrei Reinhorn, and Michel Bruneau. "Quantification of Seismic Resilience of Health care facilities". In: (2008).

[13] G. Shafer. *A mathematical theory of evidence*. Princeton University Press, 1976.

[14] Gianluca Filippi et al. "Space systems resilience optimisation under epistemic uncertainty". In: *Acta Astronautica* (2019), pp. 1–58. ISSN: 00945765. DOI: 10.1016/j.actaastro.2019.08.024.

[15] Giancarlo Benettin. "Una passeggiata tra i Sistemi Dinamici". In: (2012).

[16] R Seydel. "Basic Bifurcation Phenomena". In: *Computer* 49.June (1999).