Models of margin: from the mathematical formulation to an operational implementation

Adrien Touboul, Romain Barbedienne, Jean-Michel Edaliti

Models of margin: from the mathematical formulation to an operational implementation

*

1st Adrien Touboul *CERMICS*
Champs-sur-Marne, France
IRT-SystemX
Palaiseau, France
adrien.touboul@irt-systemx.fr

2nd Romain Barbedienne *IRT-SystemX*
Palaiseau, France
romain.barbedienne@irt-systemx.fr

3rd Jean-Michel EDALITI *Sherpa Engineerging*
Nanterre, France
jm.edaliti@sherpa-eng.com

Abstract

This paper develops a mathematical formulation of a margin problem in an automotive battery sizing use case. This formulation is done thanks to theoretical models of margin. This enables to use an approach with explicit margins, which is compared to a worst-case analysis and a probabilistic modeling. The models of margin are then adapted to a numerical implementation through the definition of patterns and presets adapted to the case study.

Keywords— Model of margin, Design under uncertainty, Industrial practice, Reliability.

1 Introduction

Uncertainties are generated all along the life cycle of large industrial systems, in their design, manufacturing, operation and even their end-of-life. Some quantitative methods, designated under the name of Uncertainty Quantification (UQ), have been developed to provide meaningful indicators for decision. A probabilistic modeling of these uncertainties is often used [1]. However it appears that, in some industrial collaborative contexts, UQ methods are not widely shared across the variety of engineering stakeholders who must interact together, thus limiting the opportunity to go beyond purely deterministic simulations. In these contexts, engineers keep using margins to ensure the reliability of the models, the simulations and the system in general. However, the margins are often implicit or *hidden*, as they are not monitored [2]. Thus, they cannot be used as indicators to characterize the system.

To address this problem, some recent works, such as [2], focused on laying the theoretical foundation of the concept of margin in design science. In order to rigorously formulate problems on margins, independently from the engineering field or modeling practice, we proposed a formal mathematical framework to define margins in [3]. More precisely, the concept of *model of margin* was proposed, describing the sufficient information to uniquely define a margin. This approach is pursued in this paper, based on a use case. A practical link between the model of margin and the risks prevented is presented hereafter. Section 2 gives a review of the literature on the formalization of margins. In Section 3, the industrial use case is introduced. Section 4 recalls the theory of the model of margin. Its application on the use case in Section 5 shows how models of margin can be used in an industrial context to formalize and generalize the margin practices. Section 6 presents a design pattern used to guide the numerical implementation of the margin presets for the use case.

2 State of the art

2.1 Scope of the work

The word *margin* has multiple meanings in engineering. The concept that we investigate can generally be described as *an amount of something included so as to be sure of success or safety* (Oxford Dictionary). It includes the notion of safety margin, that is defined for instance in [4] as *something that is over and above what is strictly necessary and that is designed to provide for emergencies [...].* In other contexts, it can

*This research work has been carried out under the leadership of the Technological Research Institute SystemX, and therefore granted with public funds within the scope of the French Program "Investissements d'Avenir".

be called *performance margin*, *margin to damage*, *flexibility margin*, and so on.

The margin of error in Statistics, which is the length of the confidence interval, does not exactly satisfy our definition, although some links could be established with it in some specific cases (*e.g* taking a safety margin because of a margin of error). The profit margin, which is the gain made by a given operation, is not studied in this paper.

2.2 Classic margin indicators

Some indicators from the literature of various disciplines can be identified as margins. The safety coefficients $(\gamma_1, \ldots, \gamma_n)$, the reliability index β_{HL} [6], the capability process C_p [5] and the monetary risk measure $\rho(X)$ [7] are examples of indicators that are used to measure an extra amount of something preventing a risk. Thus, they can be described with a model of margin, which is presented in [3, Sec 4.].

2.3 Existing margin frameworks

Some works have been conducted to manage the margins in more systematic ways. The task group on safety margins (SMAP) was motivated by the need for a unified definition to assess margins in power plants, in the context of the regulatory evaluation of design changes. One of their conclusions is that a change in safety margins must be measured with a change in probabilities of exceedance [8].

The quantification of margins and uncertainties (QMU) approach is interested in the computation of margins so as to assess safety goals in the storage of nuclear stockpiles [9]. This framework focuses more on distinguishing the sources of uncertainties in order to have a relevant interpretation of margins than on exploiting the particular structure of margins.

In the field of complex system design, the topic of margin allocation has been the source of some recent works [10, 11]. The idea is to estimate the extra quantity to allocate to each design variable in early design phases. In [11], the margin on a design variable is defined as the difference between the chosen value and a requirement (either an upper or lower requirement). However, their margin definitions do not encompass the classic indicators such as the monetary risk measure ρ and the capability process C_p, as they cannot be taken on random variables.

The need for a margin definition which is general enough to encompass the majority of practices and precise enough to provide a good formulation of actual margin problems led us to propose our own model of margin in [3]. While covering the classic indicators of Section 2.2, it did not contain a practical example of use of models of margin. Providing such an example is one of the aim of the remainder of this paper.

3 Industrial case: an automotive battery sizing

3.1 Initial problem

The use case presented in this section is typically part of a pre-design sizing study. To this end, simple models are used in order to get a first idea of the characteristics of the system. The numerical values used in this paper are provided for the purpose of the demonstration only and are not actual values used by our industrial partners.

The system of interest for this use case is a battery used to power the starting engine of an automotive combustion engine. The battery also supplies the vehicle components with power when the engine is not running. When the engine is running, the alternator provides enough power to charge the battery and to operate the car devices.

We concentrate hereafter on satisfying the requirement: *the battery should store and supply enough energy to crank the engine running in tough conditions.* It is refined as follows:

- The battery must handle at least 6 months of storage in warm, temperate and cold countries;
- To ensure that the engine actually start, there must be enough power to perform three cranking.

3.2 Modeled phenomena

The variables used in this section are classified and explained in Table 1 and Table 2. Due to the specific needs of our analysis, we chose to only model the following phenomena:

Self-discharge Because of their internal electric conductivity, batteries cannot keep their state of charge, even when unused. The conductivity is temperature-dependent and thus affects the self-discharge rate. We assume furthermore that the discharge rate is independent from the battery state of charge at a given time. The energy consumed during a period of inactivity of t_{in} is approximated by:

$$E_{\text{discharge}} = C_{\text{batt}}\, V_{\text{batt}}\, t_{\text{in}}\, k_0 (\theta_{\text{dis}} - \theta_{\text{ref}_1})^{\alpha} \tag{1}$$

Post-cooling After the engine stops, some additional energy is required to cool the engine and avoid hot spots. The post-cooling energy is expressed as:

$$E_{\text{cool}} = \begin{cases} 0, & \text{if } \theta < \theta_s \\ P_{\text{cool}}(t_m + (t_c - t_m)\, \frac{\theta_{\text{cool}} - \theta_s}{\theta_c - \theta_s}), & \text{if } \theta \in [\theta_s; \theta_c] \\ P_{\text{cool}} t_c, & \text{if } \theta > \theta_c. \end{cases} \tag{2}$$

Electronic Control Unit standby mode Most of the car embedded electronics components (ECU) - like the battery management system - keep operating periodically after the engine is stopped. This is modeled as a linear cost with respect to the parking duration:

Variable	Description	Unit
Design parameters		
C_{req}	Minimum battery capacity needed	A h
Environment constraints		
θ^{+}_{cool}	Maximum cooling temperature required	K
$\theta^{-}_{\text{start}}$	Minimum starting temperature required	K
θ^{+}_{dis}	Maximum mean temperature required	K
Non-controllable variables		
C_{batt}	Capacity consumed	A h
E_{start}	Energy required to start the vehicle	J
$E_{\text{discharge}}$	Battery self-discharge energy	J
E_{cool}	Energy used to cooling engine	J
E_{standby}	Energy consumed by standby equipments	J
θ_{dis}	Mean battery temperature	K
θ_{cool}	Engine temperature (cooling)	K
θ_{start}	Engine temperature (start)	K

Table 1: Description of model variables

$$E_{\text{standby}} = E_0 + P_{\text{standby}} t_{\text{in}}. \tag{3}$$

Starting energy The energy required to start the engine is dependent on the temperature. This has an impact on the duration of the starting phase, which is modeled by a dependency of the time on the temperature:

$$E_{\text{start}} = P_{\text{start}} \left(t_{\text{start}} + K_1 (\theta_{\text{start}} - \theta_{\text{ref}_2})^{\beta}_{+} \right) \tag{4}$$

Total energy consumed The starting energy is counted three times to match the requirements. The expression of the total energy consumed is:

$$E_{\text{batt}} = E_{\text{discharge}} + E_{\text{cool}} + E_{\text{standby}} + 3\, E_{\text{start}} \tag{5}$$

from which we deduce the expression of the total consumed capacity:

$$C_{\text{batt}} = \frac{E_{\text{batt}}}{V_{\text{batt}}}. \tag{6}$$

3.3 Aim of the analysis

The goal of the analysis is to determine the minimum battery capacity C_{req} that fulfills the requirements stated in Section 3.1. The designer must choose the design parameter C_{req} such that for all $\theta_{\text{cool}} \leq \theta^{+}_{\text{cool}}$, $\theta_{\text{dis}} \leq \theta^{+}_{\text{dis}}$ and $\theta_{\text{start}} \geq \theta^{-}_{\text{start}}$ the inequation:

$$C_{\text{req}} \geq C_{\text{batt}}(\theta_{\text{cool}}, \theta_{\text{start}}, \theta_{\text{dis}}). \tag{7}$$

Variable	Description	Unit
Constants		
t_{in}	Vehicle parking duration	s
θ_s	Engine temperature that requires cooling	K
K_0	self-discharge coefficient	$\text{K}^{-\alpha}/\text{s}$
θ_{ref_1}	Temperature with zero self-discharge	K
α	Exponent of the temperature dependency	No unit
θ_c	Critical engine temperature that requires a long time cooling	K
t_c	Critical cooling time	s
t_m	Minimal cooling time	s
P_{cool}	Power of the engine cooling system	W
P_{standby}	Power consumed by standby equipments	W
P_{start}	Power of the starter	W
t_{start}	Time required to start engine at the temperature θ_{ref2}	s
K_1	Additional cooling time coefficient	s/K^{β}
θ_{ref_2}	Reference temperature	K
β	Exponent of the temperature and time dependency	No unit
V_{batt}	Battery nominal voltage	V

Table 2: Description of model constants.

is true. The temperature constraints $\theta^{+}_{\text{cool}}, \theta^{+}_{\text{dis}}, \theta^{-}_{\text{start}}$ represent the range of temperature for which the requirements must hold. The other limits, $\theta^{-}_{\text{cool}}, \theta^{-}_{\text{dis}}$ and $\theta^{+}_{\text{start}}$ are not considered here, as they have no influence on our modeling.

4 Model of margin

A model of margin contains the information required from the analysis of a phenomenon to uniquely define a (effective) margin. This concept has been extensively developed in [3] and the reader is invited to refer to it for a comprehensive introduction to the concept. In this section, we recall from [3, Sec 2.1] the notation used in the model of margin.

4.1 Model of margin

We call U the variable of interest, for which one is interested in computing a margin. U is a random variable on a probability space $(\Omega, \mathscr{F}, \mathbf{P})$ and it takes its values in E.

Definition 4.1 (Problem description)**.** The *problem description* is defined by the triple $(\text{E}, \mathscr{C}, \mathscr{A})$. E is the *state space*. The set of *problem constraints* $\mathscr{C}$ and the *acceptance*

set $\mathscr{A}$ are two subsets of the random variables on E, denoted by $\mathbb{L}^0(\Omega, \mathrm{E})$.

$\mathscr{C}$ characterizes the values that can be taken by the variables describing the phenomenon U due to constraints given by the model - such as physical or logical constraints.

$\mathscr{A}$ discriminates the values of U that are acceptable and then included in this set, and those that are not.

Definition 4.2 (Probing set)**.** Let $(\mathrm{E}, \mathscr{C}, \mathscr{A})$ be a problem description. The family of *probing sets* is a family of subsets of E indexed by $U \in \mathscr{C}$, and is denoted by $(\mathscr{G}_U)_{U \in \mathscr{C}}$. The intersection between a probing set and the problem constraints is $\mathscr{G}_{U|\mathscr{C}} = \mathscr{G}_U \cap \mathscr{C}$.

$\mathscr{G}_U$ gives the extent of the point evolution that one wants to consider when computing a margin at the point U.

Definition 4.3 (Coordinates of interest)**.** Let $(\mathrm{E}, \mathscr{C}, \mathscr{A})$ be a problem description and $(\mathscr{G}_U)_{U \in \mathscr{C}}$ a family of probing sets. A set of *coordinates of interest* is a metric space $(\mathbf{S}, d_{\mathbf{S}})$, provided with a family of functions $\phi_U : \mathscr{G}_U \to \mathbf{S}$ indexed by $U \in \mathscr{C}$. The family $(\phi_U)_{U \in \mathscr{C}}$ is called the family of *coordinate functions*.

The set of coordinates of interest $\mathbf{S}$ represents the quantities on which one wants to express a margin, which will be measured by the distance $d_{\mathbf{S}}$. ϕ_U is the coordinate function which associates each element of $\mathscr{G}_U$ with its coordinates in $\mathbf{S}$.

Definition 4.4 (Model of margin)**.** A model of margin is the combination of a problem description, a family of probing sets and a set of coordinates of interest with the corresponding coordinate functions. It is denoted by:

$$\mathsf{M} = (\mathrm{E}, \mathscr{C}, \mathscr{A}, (\mathscr{G}_U)_{U \in \mathscr{C}}, \mathbf{S}, d_{\mathbf{S}}, (\phi_U)_{U \in \mathscr{C}}) \tag{8}$$

4.2 Margin

Definition 4.5 (Margin)**.**
Let $\mathsf{M} = (\mathrm{E}, \mathscr{C}, \mathscr{A}, (\mathscr{G}_U)_{U \in \mathscr{C}}, \mathbf{S}, d_{\mathbf{S}}, (\phi_U)_{U \in \mathscr{C}})$ be a given margin model and $U \in \mathscr{C}$ a variable of interest. The *margin* at the point U for the model M is defined as:

$$\mathsf{m}(U; \mathsf{M}) = \begin{cases} d_{\mathbf{S}}\left(\phi_U(U), \phi_U(\mathscr{A}^c \cap \mathscr{G}_{U|\mathscr{C}})\right) \text{ if } U \in \mathscr{A}, \\ -d_{\mathbf{S}}\left(\phi_U(U), \phi_U(\mathscr{A}^c \cap \mathscr{G}_{U|\mathscr{C}})^c \cap \phi_U(\mathscr{G}_{U|\mathscr{C}})\right) \\ \text{if } U \notin \mathscr{A}. \end{cases} \tag{9}$$

Intuitively, the margin for a given point U is the distance from this point to the acceptance set, for some chosen evolution and focusing only on some coordinates describing the variable of interest. U can be a random variable, but the margin is ultimately expressed as a distance $d_{\mathbf{S}}$ in a deterministic metric space $\mathbf{S}$.

4.3 Directional margin

A model of *directional margin* is a special case of model of margin that consists in probing - *i.e* exploring - the points in one specific direction from the reference point and measuring the distance from this point to the unacceptable points in this specific direction.

The state space E is a vector space and we denote by $w \in \mathrm{E}$ the specific direction of the directional model of margin M. The margin at the point $U \in \mathscr{A}$ has the following expression:

$$\mathsf{m}(U; \mathsf{M}) = \inf\{\lambda \geq 0 \,|U + \lambda w \in \mathscr{A}^c \cap \mathscr{C}\}.$$

4.4 Taking a margin

4.4.1 Taking a margin on a set of points

when one speaks of *taking a margin* m, most of the times they implicitly think of defining a model of margin M and imposing a minimum margin $m > 0$ for this model of margin. In that case, the requirement value m is called the *demanded margin*, by opposition to an *effective margin*, which is the margin actually measured for a point U. In this paper, instead of writing that the acceptance set $\mathscr{A}$ of the model of margin M is reduced by the condition $\mathsf{m}(U; \mathsf{M}) > m$, we write that *$m$ margin is taken in* M.

4.4.2 Taking a margin on a point

Sometimes, it is easy to choose the "best" point U^* as a unique solution of:

$$U^* = \underset{U \in \mathscr{A}}{\arg\min}\, c(U). \tag{10}$$

c is a cost function, and it can possibly be trivial to compute. It can be the value of one coordinate of U for instance. It might be easy as well to choose the best point V^* from the "marged" acceptance set $\{V \in \mathscr{A} | \mathsf{m}(V; \mathsf{M}) \geq m\}$ for the same cost function. It seems common that, in that case, one says that "V^* is the point U^* with m margin".

5 Application to the industrial case

In this section, we compare two classic design methods to choose the battery capacity to an approach enabled by the model of margin, namely the *design with explicit margins*. Each of the three method have in common a formulation of an optimization problem under constraints:

$$C^*_{\mathrm{req}} = \underset{C_{\mathrm{req}} \in \mathscr{D}}{\arg\min}\, C_{\mathrm{req}}. \tag{11}$$

The difference lies in the construction of the optimization space $\mathscr{D}$.

5.1 Three design approaches

5.1.1 Worst-case design

The worst-case approach consists in taking each environment variable at its worst value for all the considered environments. Looking at the given reference values in Table 3, and considering the monotony of the capacity with respect to the environment variables, the worst case happens when $\theta^+_{\text{cool}} = 80\,^\circ\text{C}$, $\theta^+_{\text{dis}} = 35\,^\circ\text{C}$ and $\theta^-_{\text{start}} = -18\,^\circ\text{C}$. The optimization space $\mathscr{D}$ is then constructed by applying the condition of Equation (7) with the aforementioned values. Thanks to the monotonicity of the model, we compute the optimal design as $C_{\text{batt}}(80, -18, 35)$, which leads to a numerical value of:

$$C^*_{\text{req}} = 92\,\text{A h}.$$

This approach is interpreted as a sequential margin accumulation in Section 5.2.

Environment	θ^+_{cool}	θ^+_{dis}	θ^-_{start}	probability
Temperate	65 °C	20 °C	0 °C	p_{temp}
Cold	65 °C	20 °C	−18 °C	p_{cold}
Warm	80 °C	35 °C	0 °C	p_{warm}

Table 3: Reference environment constraints depending on the environment.

5.1.2 Probabilistic design

in the probabilistic approach, each environment of Table 3 is assigned to an event. The universe is then composed of three exclusive events $\Omega = \{\omega_{\text{temp}}, \omega_{\text{cold}}, \omega_{\text{warm}}\}$, modeling the event "being in a temperate (resp. cold and warm) country". A probability measure is constructed from data on the consumer profiles and assigns the probabilities p_{temp},p_{cold} and p_{warm} to each event. θ^+_{cool},θ^+_{dis} and θ^-_{start} are now random variables whose laws are given by the values associated to the probability of each scenario (see Table 3).

C_{batt} is then also a random variable. The criteria is reformulated in "satisfying Equation (7) with a probability of $\gamma \in [0, 1]$". The optimization space $\mathscr{D}$ is then given by the values C_{req} for which:

$$\mathbf{P}\left(C_{\text{batt}}(\theta^+_{\text{cool}}, \theta^+_{\text{start}}, \theta^-_{\text{dis}}) \leq C_{\text{req}}\right) \geq \gamma. \tag{12}$$

As illustrated in Figure 1, different choices of C^*_{req} are possible (43 A h, 63 A h or 69 A h), depending on the γ chosen.

One can remark that even for $\gamma = 1$, *i.e* when Equation (7) is always satisfied, the optimal value C_{req} is 69 A h, which is smaller than the worst-case value 92 A h. This characteristic is captured in margin framework, by performing a mutual accumulation on the margins instead of a sequential one, as explained in Section 5.2.

5.1.3 Design with explicit margins

the global motivation of the proposed approach is to ensure that all the margins considered in the analysis are relevant.

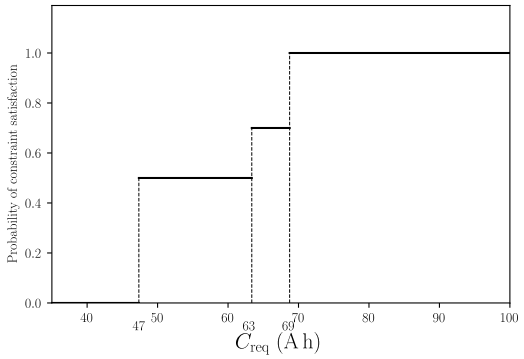


Figure 1: Probability γ to satisfy the constraint with respect to the value of C_{req}. This is also the cumulative distribution function of C_{batt}.

Margins can be explicitly identified and described thanks to their models of margin.

In Table 3, one can see that a margin of $-18\,^\circ\text{C}$ has been taken for θ^-_{start} in the cold environment, with respect to the temperate one. A margin of 15 °C for θ^+_{cool} and θ^+_{dis} has been taken in the warm environment.

As a car cannot be in a cold country and in a warm country at the same time, a simple rule is to consider that these margins must not be taken "at the same time", but instead separately. By applying this rule, one computes C^*_{req} as the maximum of $C_{\text{batt}}(65, 20, -18)$ and $C_{\text{batt}}(80, 35, 0)$. The numerical value is the same as the probabilistic modeling with $\gamma = 1$:

$$C^*_{\text{req}} = 69\,\text{A h}.$$

The rigorous interpretation of this use case in terms of models of margin is presented in Section 5.2. The rule is generalized in Section 5.3. Section 6 gives some insights to implement it globally as a numerical tool.

5.2 Detail of the design with explicit margins

We reformulate the industrial case within our margin framework. To do so, we first construct a deterministic problem description of the models of margin. The state space E is chosen to be the set of the design variables and the environment constraints given in Table 1. The set of the problem constraints $\mathscr{C}$ is given by the equations of Section 3.2. The acceptance set $\mathscr{A}$ is composed of the states satisfying the criterion of Equation (7). U represents a battery designed for temperate countries. We want to prevent two risks that are not modeled in the problem description:

- (R_1): being parked in a cold country and running out of battery;
- (R_2): being parked in a hot country and running out of battery.

We define M_1, a directional model of margin in the direction of a decrease in θ^-_{start}. To prevent (R_1), we take a

margin of 18 °C in M_1, *i.e* we impose a smaller minimum starting temperature.

We define M_2, a directional model of margin in the direction of an increase in $\theta^+_{\text{cool}}, \theta^+_{\text{dis}}$. To prevent (R_2), we take a margin of 15 °C in M_2, *i.e* we impose a greater maximum cooling and mean temperature.

These two margins lead to the conditions of Table 3 for warm and cold countries. In order to choose our best design, we use an informal design rule:

> When two risks are mutually exclusive, there is no need to add up the margins taken for each event. Instead, one could consider the possible designs with margins for each event separately and choose the best among their intersections.

This rule actually describes an implicit consideration modeled in the probabilistic design. As a car cannot be parked in a cold country and in a warm country at the same time, the values of the constraints $\theta^+_{\text{dis}} = 35\,°\text{C}$ and $\theta_{\text{start}} = -18\,°\text{C}$ should not be imposed at the same time. The optimization space $\mathscr{D}$ is then the intersection of the designs with a margin of 18 °C in M_1 and of the designs with a margin of 15 °C in M_2:

$$\begin{aligned}\mathscr{D} = &\left\{U \in \mathbb{L}^0(\Omega, \mathrm{E}) \,|\mathsf{m}(U; \mathsf{M}_1) \geq 18\,°\text{C}\right\} \\ \cap &\left\{U \in \mathbb{L}^0(\Omega, \mathrm{E}) \,|\mathsf{m}(U; \mathsf{M}_2) \geq 15\,°\text{C}\right\}\end{aligned} \tag{13}$$

The impact of different strategies of margin accumulation is illustrated in Figure 2.

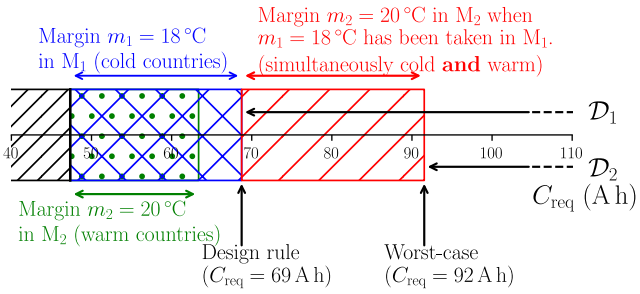


Figure 2: Reduction of the optimization space depending on the accumulation strategy. $\mathscr{D}_1$ is the optimization space in the design with explicit margins and $\mathscr{D}_2$ is the optimization space in the worst case.

With this method, our optimal value is:

$$C^*_{\text{req}} = 69\,\text{A h}. \tag{14}$$

This result is the same as the probabilistic design with $\gamma = 1$.

5.3 Generalization of the industrial case

The example given in the previous section will help generalizing it. During the design process, multiple margins are taken to cover various risks. This process can be described as:

1. Starting with some failure criteria that define a set of acceptable designs $\mathscr{A}$.

   In the previous case, $\mathscr{A}$ is given by Equation (7).

2. Considering a first risk R_1, that is not prevented by the failure criteria.

   In the previous case R_1 is "being parked in a cold country and running out of battery"'.

3. Taking some margins on some quantities to cover the risk R_1.

   $m_1 = 18\,°\text{C}$ margin in M_1 has been taken in the previous case.

4. For each other risk R_i repeating Step 3.

   Only R_2 "being parked in a warm country and running out of battery" has been considered previously.

5. Getting a "marged" acceptance set $\mathscr{A}_{\text{marg}}$ covering all the risks considered.

   This set was denoted by $\mathscr{D}$ in the previous case.

6. Choosing an optimal design among $\mathscr{A}_{\text{marg}}$.

   The optimal design was $C_{\text{req}} = 69\,\text{A h}$ in the previous case.

5.3.1 Margin accumulation strategies

An interesting remark that can be made from the previous case is that there are (at least) two different ways to take two margins simultaneously. Let us denote by $\mathsf{M}(\mathscr{A})$ the model of margin M in which its original acceptance set is replaced with $\mathscr{A}$. The two ways are:

Sequential accumulation considering a margin m_1 has been taken in M_1, take an additional margin m_2 in M_2.

$$\begin{aligned}\mathscr{A}_1 &= \{U \in \mathscr{A} \,|\mathsf{m}(U; \mathsf{M}_1(\mathscr{A})) \geq m_1\} \\ \mathscr{A}_{\text{marg}} &= \{U \in \mathscr{A} \,|\mathsf{m}(U; \mathsf{M}_2(\mathscr{A}_1)) \geq m_2\}.\end{aligned} \tag{15}$$

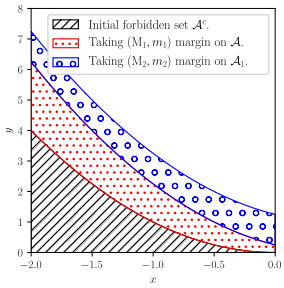
An illustration of sequential margins accumulation is shown in Figure 3a. This leads to the worst-case design in the industrial case.

Mutual accumulation the points U are required to have m_1 margin in M_1 and m_2 margin in M_2:

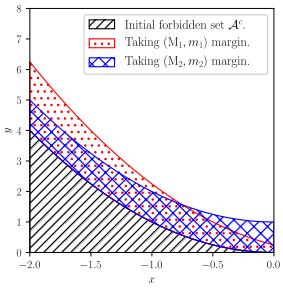
$$\begin{aligned}\mathscr{A}_{\text{marg}} = &\{U \in \mathscr{A} \,|\mathsf{m}(U; \mathsf{M}_1(\mathscr{A})) \geq m_1\} \\ \cap &\{U \in \mathscr{A} \,|\mathsf{m}(U; \mathsf{M}_2(\mathscr{A})) \geq m_2\}.\end{aligned} \tag{16}$$

An illustration of mutual margins accumulation is shown in Figure 3b. This leads to the design with explicit margins in the industrial case.

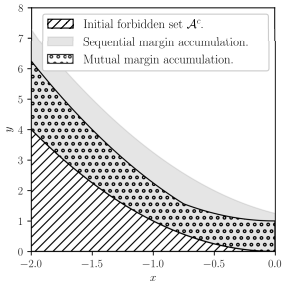
It is possible to prove that the "marged" acceptance set $\mathscr{A}_{\text{marg}}$ resulting from the sequential accumulation is always smaller than or equal to the one from the mutual accumulation. The argument is that, as $\mathscr{A}_1 \subset \mathscr{A}$, the sequential marged acceptance set is included in $\{U \in \mathscr{A} \,|\mathsf{m}(U; \mathsf{M}_2(\mathscr{A})) \geq m_2\}$ and also in $\mathscr{A}_1$. This is illustrated in the comparison of Figure 3c.



(a) Sequential margins accumulation of a margin of 1 taken in M_1 then of margin of 0.5 taken in M_2.



(b) Mutual margin accumulation of 1 margin taken in M_1 and 0.5 margin taken in M_2.



(c) Comparison of both strategies (sequential is in plain grey and mutual is dotted).

Figure 3: Two strategies of margins accumulation for the acceptance set $\mathscr{A} = \left\{(x, y) | y \geq x^2\right\}$. M_1 is a directional model of margin on a decrease in x and M_2 is a directional model of margin on a decrease in y. A margin of 1 is taken in M_1 and a margin of 0.5 is taken in M_2.

Nonetheless, the sequential accumulation should not be forbidden. In fact, both strategies are relevant depending on the purpose of the accumulation.

The purpose of the sequential accumulation is first to prevent the risk R_1 by taking a margin of m_1 in M_1. Then, assuming this risk occurs, one prevents a second risk R_2 (potentially the same) by taking a margin of m_2 in M_2.

The mutual accumulation can be seen as preventing a risk R_1 by taking a margin of m_1 in M_1 and a second risk R_2 by taking a margin of m_2 in M_2. The case in which R_1 and R_2 happen at the same time is not considered, though.

It is now possible to rewrite the informal design rule as follows:

> Assuming that R_1 and R_2 are two risks that cannot happen at the same time and a margin of m_1 (resp. m_2) has been taken in M_1 (resp. M_2) to cover R_1 (resp. R_2), the final acceptance set covering R_1 and R_2 can be constructed by the mutual accumulation of m_1 taken in M_1 and m_2 taken in M_2.

It is assumed that the models of margin M_1 and M_2 share the same problem description and, in particular, the same acceptance set.

5.3.2 On the construction of the acceptance set $\mathscr{A}$

in an optimization context of the type:

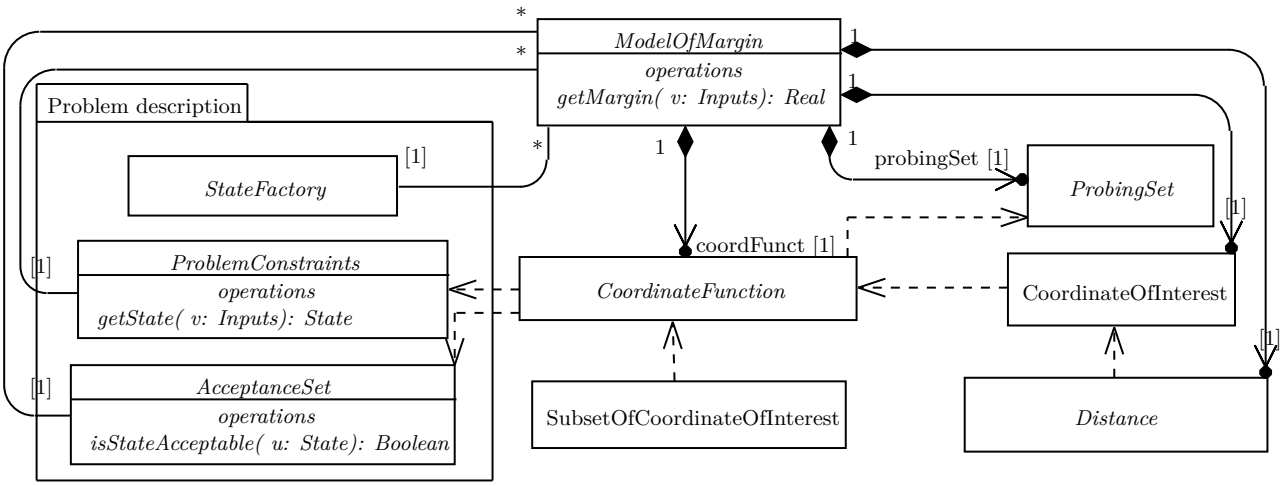
$$U^* = \underset{U \in \{V \in \mathscr{A} | \mathsf{m}(V;\mathsf{M}) \geq m\}}{\arg\min} c(U) \tag{17}$$

it seems to be a good practice to take margins on the intensity of the environment constraints - θ^+_{cool} for instance - rather than on some actual values of the environment variables - θ_{cool} for instance.

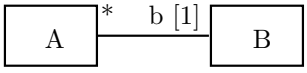
Taking a margin on a constraint only imposes a stronger constraint, *e.g* a greater θ^+_{cool}. Now, let us assume that θ_{cool} is included in the point U instead of θ^+_{cool}. In that case, a temperate constraint $\theta_{\text{cool}} > 65\,^\circ\text{C}$ would likely be included in the acceptance set, to make sure that the design would fulfill the temperate country requirements. A margin for the warm countries in an increase θ_{cool} would forbid any θ_{cool} value between 65 °C and 80 °C. Then, even a *mutual accumulation* would impose $\theta_{\text{cool}} \geq 80\,^\circ\text{C}$. With a similar reasoning on the two other environment variables, the optimal design would be the worst-case, instead of the one with explicit margins.

Method	C_{req}
Worst-case	92 A h
+ The simplest.	
− Very conservative.	
Explicit margins	69 A h
+ No more additional phenomena modeling than in the worst-case, performs better, interpretation in terms of margins.	
− Needs a modeling of the margins and of the risks.	
Probabilistic model	Depends on γ, ≤ 69 A h
+ Takes into account the correlations.	
− Requires a probabilistic framework.	

Table 4: Comparison of the three design methods

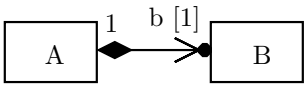


Association



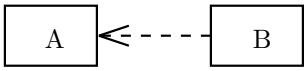
A class A has an association with another class B if an object of class A needs to maintain a reference to an object of class B. [12]

Composition



A composition is an unidirectional association, It means that A is composed of B.

Dependency



A Dependency is a Relationship that signifies that a single model Element or a set of model Elements requires other model Elements for their specification or implementation. [13]

Figure 4: Description of Margin metamodel using UML Class Diagram

5.4 Conclusion of the section

The margin that were taken during the design are now rigorously defined, thanks to the models of margin. This rigorous formulation helped us expressing a particular design margin rule for general cases. This illustrates the aim and the potential of the model of margin: to formulate problems on margins and their solutions in a rigorous, general way.

6 Structure of an implementation of a model of margin

The previous formulation of the model of margin allows an exhaustiveness to manage each model of margin. However, it may not be simple enough to be used by a specialist simulation designer. In this section, a software design pattern for the model of margin is built. This pattern enables the definition of presets that could be plugged to each concept of model of margin. A focus on the preset for the use case is presented. The pattern will be described thanks to a metamodel, that defines the concepts and the relationships between these concepts.

6.1 Metamodel definition

The *metamodel* of the model of margin describes its components, for the purpose of their software implementations. The Unified Modeling Language (UML) is used to describe the metamodel, although one does not need to be familiar with it to understand the patterns we expose. When some UML concepts are used in a figure, their meaning is given in a table below the figure.

A UML class, represented as a box, has the same meaning as classes described in programming language as C++, Java, or Modelica. It is a collection of properties and operations. Classes can be seen as a mold, where instances can be seen as items generated from a class.

Each mathematical object is modeled with an abstract class, which is a class that cannot be instantiated as is. The classes that are actually instantiated all *inherit* from the abstract classes. The process of inheritance consists in imposing the feature (attributes and methods/operations) interfaces of the parent abstract class to the classes that inherit

from it. To differentiate abstract classes from other classes, the name of abstract classes is written in *italic*. For instance, in Figure 4, each model of margin must have a class inheriting from *ProblemConstraints*. Each of these classes must have an operation getState, which represents the computation of the state (inputs and outputs) with respect to the inputs. However, the operation getState can be different for two models of margin, as they can refer to different phenomena.

6.1.1 Problem description

the abstract class *ModelOfMargin* is associated with the *ProblemConstraints*, *StateFactory* and *AcceptanceSet* abstract classes. The three latter classes come from a prior modeling, without any margin consideration *a priori*. They can then exist without the model of margin, and consequently, an association link is used.

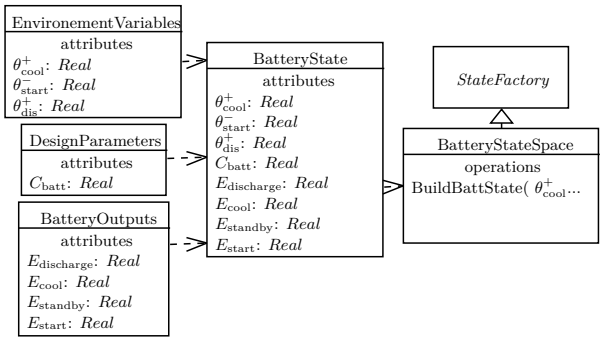
State space The role of the state space E in the mathematical model of margin is to declare what are the variables that would be of interest in the model. The variables can either be input, intermediary or output variables. The numerical counterpart is the *StateFactory*, which defines how to instantiate the state.

The BatteryState of the use case (Figure 5) is implemented to be used in an optimization context. The distinction between the design parameters, the battery outputs and the environment variables allows to identify the variables on which an optimization algorithm can operate. These variables are taken from Tables 1 and 2. The BatteryStateSpace has a method BuildBatteryState(...) to construct a state instance.

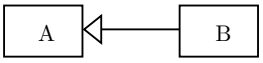
Problem constraints as written in the introduction, an implementation of the *ProblemConstraints* must have a method getState. This method is given by the models simulating the phenomenon.

Acceptance set For the numerical representation of $\mathscr{A}$, we only impose that any representation inheriting from *AcceptanceSet* has an "oracle function" *isStateAcceptable*. This function returns "True" if the state given in argument is in acceptance set and "False" otherwise. The construction of this acceptance criterion may come from various sources. For instance it can be some requirements specifications documents, the simulation itself, or a demanded margin condition.

The initial acceptance set of the use case has come from the criterion of Equation (7) and was deduced from the high level requirements. The quantity $\rho = C_{\text{batt}} - C_{\text{req}}$ can be identified as a measure of the risk, that must be smaller than the threshold $\rho_{\text{req}} = 0$. It can thus be modeled with a RiskMeasureAcceptanceSet, as shown in Figure 6. In this specialization of *AcceptanceSet*, isStateAcceptable is True if and only if $\rho(State) \leq \rho_{\text{req}}$.



Generalization



B class inherits from A class means that all characteristics of A class are included in B class

Figure 5: State of case study

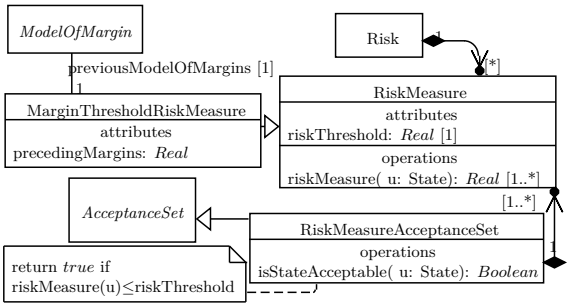


Figure 6: *AcceptanceSet* implementation for the case study .

It has been stated that taking a margin consists in reducing the acceptance set by imposing $\mathsf{m}(U;\mathsf{M}) \geq m$ (see Section 4.4.1). The implementation of this operation is illustrated in Figure 6 in the MarginThresholdRiskMeasure class. The condition can be expressed with risk measure, by defining $\rho(U) = -\mathsf{m}(U;\mathsf{M})$ and $\rho_{req} = -m$.

6.1.2 Specific objects of the model of margin

The problem description comes from the modeling of the phenomenon. The other objects, such as the probing set or the coordinate functions are specific to the model of margin.

Each model of margin specific object is defined as an abstract class. Theses classes could not exist without a model of margin and thus, they have a composition link with the *ModelOfMargin* abstract class.

Probing set for each state U, the classes inheriting from *ProbingSet* must describe the value of the states that would be explored in the computation of the margin. In a directional model of margin, it is implemented as a vector. This direction vector represents the semi-line starting at the state U and going in the direction of the vector.

In the use case, the two models of margin defined in Section 5.2 are directional margins. The probing direction of M_1 is $-e_{\theta^-_{\text{start}}}$, the unit vector in θ^-_{start} and the probing direction of M_2 is $e_{\theta^+_{\text{cool}}} + e_{\theta^+_{\text{dis}}}$, the sum of the two unit vectors in θ^+_{cool} and in θ^+_{dis}.

Coordinates functions and coordinates of interest the specialization of *CoordinateFunctions* must carry the information to project any state in the *ProbingSet* to an element of *CoordinatesOfInterest*.

In a directional model of margin, the coordinate of interest is formed by the abscissa of points on the semi-line. It can thus be deduced from the direction vector. In this case, the information of the CoordinateFunctions and CoordinateOfInterest can be factorized with the information used to construct the probing set.

Distance the implementation of *Distance* must describe how to compute a distance between two elements of *CoordinatesOfInterest*.

By convention, in a directional model of margin, the direction vector defining the *ProbingSet* (Section 6.1.2) is also the "unit vector" defining the *Distance*. However, the (mathematical) probing set and the distance remain two different conceptual objects.

7 Conclusion and future work

The application of the theoretical model of margin presented in Section 4 to the automotive case of Section 3 helped:

- Formulating a margin problem and formulating its solution in a rigorous way, in Section 5.2.
- Generalizing the solution so it can be applied in a approach of design with explicit margin, in Section 5.3. This approach consist in identifying the relevant margins.
- Deducing some software design patterns for a numerical use of the model of margin, in Section 6.

This is an encouraging sign for the ability of the model of margin to formalize practical margin approaches to handle risk.

Some different axes can be identified for some future developments:

- Other margin practices and rules can be identified in industrial cases with different contexts. Their rigorous formulation with the model of margin could help to standardize these practices for interacting stakeholders.
- Taking a margin is closely linked to a risk to prevent. This risk is not formalized in the model of margin. Is it possible to construct an operating *model of risk* that keeps some of the genericity of the model of margin?
- On a more theoretical aspect, the model of margin is itself a mathematical object. Studying it can help providing some general classes of solutions for problems such as computing a margin or optimizing a design under a demanded margin constraint.

8 Acknowledgment

The authors acknowledge Julien Reygner and Mouadh Yagoubi for their support during the redaction of the article. Exchanges with the members of the AMC team at IRT SystemX were also of great importance to shape up the margin concept.

References

[1] De Rocquigny, E., Devictor, N., & Tarantola, S. (Eds.). Uncertainty in industrial practice: a guide to quantitative uncertainty management. John Wiley & Sons. 2008.

[2] Eckert, C., Isaksson, O., & Earl, C. Design margins: a hidden issue in industry. Design Science, 5. 2019

[3] Adrien Touboul, Julien Reygner, Fabien Mangeant, Pierre Benjamin."A formal framework to define margins in industrial processes." Preprint (hal-02156493, version 1). 2019.

[4] Youngblood, RW, Risk-Informed Safety Margin Characterization (RISMC): Integrated Treatment of Aleatory and Epistemic Uncertainty in Safety Analysis Idaho National Laboratory (INL) 2010

[5] Montgomery, Douglas C, Introduction to statistical quality control, John Wiley & Sons, 2007

[6] Lemaire, Maurice, Structural reliability, John Wiley & Sons, 2013

[7] Artzner, Philippe and Delbaen, Freddy and Eber, Jean-Marc and Heath, David, Coherent measures of risk, Mathematical finance, 1999

[8] Hrehor, Miroslav and Gavrilas, Mirela and Belac, Josef and Sairanen, Risto and Bruna, Giovanni and Reocreux, Michel and Touboul, Francoise and Krzykacz-Hausmann, B and Park, Jong Seuk and Prosek, Andrej and others, Task Group on Safety Margins Action Plan (SMAP). Safety Margins Action Plan-Final Report, Organisation for Economic Co-Operation and Development, 2007

[9] Jon C. Helton, Quantification of margins and uncertainties: Conceptual and computational basis, Reliability Engineering & System Safety, 2011

[10] Thunnissen, Daniel Pierre, Propagating and mitigating uncertainty in the design of complex multidisciplinary systems, California Institute of Technology, 2005

[11] Guenov, Marin D. and Chen, Xin and Molina-Cristóbal, Arturo and Riaz, Atif and van Heerden, Albert S. J. and Padulo, Mattia, Margin Allocation and Tradeoff in Complex Systems Design and Optimization, AIAA Journal, 2019

[12] Cranefield, S.. UML and the Semantic Web (Information Science Discussion Papers Series No. 2001/04). University of Otago. Retrieved from http://hdl.handle.net/10523/1005, 2001

[13] Object management Group "OMG Unified Modeling Language (OMG UML)" consulted on https://www.omg.org/spec/UML/2.5.1/PDF December 2017.