INTERNATIONAL CONFERENCE ON ENGINEERING DESIGN
ICED 03 STOCKHOLM, AUGUST 19-21, 2003

SAFETY CONSIDERATIONS IN OPTIMISATION OF DESIGN SPECIFICATION CONTENT

Christian Grante and Johan Andersson

Abstract

It is becoming more and more difficult to decide which customer functions to include in new complex systems and products. This work presents a methodology supporting the designer or product planer in the evaluation of which customer functions and technical implementations to include in a product or system. It uses economical criteria in the form of profit and development cost for the evaluation and also considers that the product should be safe. Among the most promising combinations of concepts the methodology guides the designer in making the choice and to improving it so that it is safe. In a case study performed at Volvo Car Corporation on active safety systems more than 50 possible functions existed, many of them sharing technical implementers, giving more than 70 billion possible combinations in the final product. The methodology is proven effectual and much better results were achieved than with current used methods. Optimisation of profit alone can however lead to safety problems. The methodology presented therefore helps in finding weak safety areas and safe product concepts can be achieved often with a small cost increases.

Keywords: Safety, Product planning, Design optimisation, Evolutionary optimisation

1 Introduction

Companies often divide their development into three phases, represented by three organisations: research, advanced engineering (AE) and project. In research new technology is investigated, in AE systems are designed using new technology both from within the company and from other sources; these become “off the shelf” systems that are selected among and incorporated in products in the project phase. The combinations of “off the shelf” systems are becoming more and more complex and it is difficult to make the design specifications for products. A key factor is that many products are becoming mechatronical [1]. This means that they are computer controlled and have sensors as well as mechanical actuators. The mechatronic systems give new possibilities and can often incorporate many more functions than if designed with traditional mechanical and electrical systems. It is possible to achieve the same level of functionality in non mechatronic products but most often the cost will be higher and the physical packaging hard to solve.

Mechatronic systems are often designed with open architectures, which makes it easy to add and remove sub-systems during design [2]. The customer functions of the mechatronic products usually depend on several sub-systems (technical implementers). The customer functions create customer value and the technical implementers are needed to realise them but are associated with costs. However, the main economical advantage is that customer functions can share technical implementers, and thereby their cost. This makes the design specification far more complex then for more traditional mechanical systems. For large systems and products it thus becomes extremely complex to decide which functionality to include; therefore methods for concept selection are needed for the development of the product specifications [3].

There are many different selection methods within the engineering design domain. Most of them consider selection among different concept solutions, e.g. the Pugh matrix [4], but there are also those like the morphological matrix [5] that support designers in choosing which implementations to combine in a product to provided required functionality. In order to make requirements for mechatronical systems, selection methods are needed that can both help the designer to choose the technical implementations and at the same time explore which of the many possible customer functions to include. In a previous study at Volvo Car Corporation it was found that the aim (criteria) in the selection is to maximise the profit and minimise the development cost [6]. It was also found that this evaluation is not possible to do manually for an industrial size problem; it was not even possible to calculate the profit and development cost of all possible concepts. A concept is defined as a combination of different implementations; each concept supporting one or more functions. An automation of the selection process was needed in order for the selection process to be practically feasible.

This methodology is most applicable in early project design phases or if changes are made to the product specification. In the automotive industry and several other industries “off the shelf” products are used. This means that sub-systems/technical implementations are often pre-developed or possible to buy from suppliers and also that fairly detailed information exists about the systems and their costs. The product profit is defined as the amount the customer is prepared to pay for the function (customer value) minus the total cost. The customer value is somewhat difficult to estimate and depends on several parameters, but the automobile industry is familiar with such estimation. It was shown in case studies at Volvo Cars that this approach was better then with the old manual methods using the same data: However, one problem was found. Although most restrictions are already incorporated in the “off the shelf” products and it was thought that it was possible just to use economical criteria in the early project conceptual selection, safety arose as a problem. Many of the active safety systems are safety-critical and the method suggested combinations that often became unsafe when designed. It was concluded that safety, or rather the total risks, must also be a selection criterion for the early project concept selections. This work presents how risk of failure can be considered in early project concept design selections. A methodology that supports designers in the process of concept development is presented. It considers profit and development budget and assures that the safety is not jeopardised. Furthermore, the methodology has been evaluated in a new case study at Volvo Car Corporation and compered to the existing method.

The research has been conducted by the use of the Design Research Methodology presented by Blessing, Chakrabarti and Wallace [7]. The methodology consists of four steps: criteria, descriptive study I, prescriptive study and descriptive study II. Success factors are investigated in criteria; the problem is analysed in description I; in the prescriptive study a solution is proposed; and in description II the proposed solution is evaluated with respect to initial criteria.

2. The Methodology

Most design processes used today have in common that they start with a design specification, called a requirements list by Pahl and Beitz [5], functional requirements by Suh [8], and product specification by Ulrich and Eppinger [9]. To obtain the design specification there is a phase before the actual design starts; this phase is called “Planing and clarifying the task” by

Pahl and Beitz, “Mapping from customer needs to functional requirements” by Suh, and “Planning” or “Phase zero” by Ulrich and Eppinger. Suh writes, in this phase, about ranking the different customer needs with respect to their value. Pahl and Beitz and Ulrich and Eppinger also write about ranking needs, and about market analysis, life cycle analysis and finding the products ideas. Pahl and Beitz, and Ulrich and Eppinger stress the importance of describing the functionality and finally of estimating the cost target or the budget linked to the company’s goals in this “pre-design phase”. There is, however, a lack of methods to establish the design specification for complex systems in this “pre-design phase”. Such methods have to find the concepts with the highest probability of economical success and still meet other demands, such as the development budget.

2.1 Evaluating with regard to economical criteria

This work builds on and enhances the work presented at ICED’01 [3]. A new, descriptive study I, shows that safety is an important criterion that must be considered, but the economical evaluation from the prescriptive study in [3] still is valid. It first models the in-data to the design specification. The in-data consists of all customer functions that are possible to implement in a product to be designed, together with their expected customer value and the technical implementations that they need to be impended with their costs. This can be seen as a set of functions with relations formed by the use of the technical implementers. A concept is viewed as a set of technical implementations. The cost depends on which implementers are included in the concept and the value depends on which customer function that the implementers can realise. Note that customer functions can share technical implementations.

In the previous work it was found that for industrial size problems it is impossible to calculate all the data for all possible concepts. In the case study performed at Volvo Cars more then 70 billion concepts excited. Optimisation was necessary. This section considers an enhancement of the optimisation presented in [3]. Instead of using a weighted goal function, a Pareto optimisation is used [10]. This means that instead of resulting in one optimal concept the designer or product planer is presented with a trade-off curve, Pareto front, of different concept that elucidate the trade-off between obtaining high profit and simultaneously having a low development budget. Pareto optimality is defined as the set of solution for which there exists no other solutions that are better in all criteria. In this application this implies that the Pareto front contains the concepts for which the development cost could not be lowered without a decrease in the profit. Selection between these concepts can only be made by weighting the importance of high profit against the importance of low development budget. In order to implement the Pareto optimisation, the mathematical description that follows has been developed.

The customer functions are represented in the customer function vector (*CF*) and the technical implementations in the technical implementation vector (*TI*). A coupling vector CV_i expresses which technical implementations are necessary in order to realise the customer function CF_i. Each element of the coupling vector could either be one, indicating that the corresponding technical implementation/s are needed, or zero indicating not needed. The coupling vectors for all customer functions, cv_i, $i = 1..m$, make up the coupling matrix CM. Thus the problem can be described according to equation (1).

$$\mathbf{CF} = \mathbf{CM} \cdot \mathbf{TI} \quad \text{i.e.} \quad \begin{bmatrix} CF_1 \\ \cdots \\ \cdots \\ CF_m \end{bmatrix} = \begin{bmatrix} - & \mathbf{cv_1} & - \\ & \cdots & \\ & \cdots & \\ - & \mathbf{cv_m} & - \end{bmatrix} \begin{bmatrix} TI_1 \\ \cdots \\ \cdots \\ TI_n \end{bmatrix} \qquad (1)$$

where *m* is the number of potential customer functions and *n* the number of technical implementations.

Each combination of technical implementations yields one possible solution to the problem, one concept. For a problem with *n* technical implementations there exist 2^n different concepts. A particular concept, *X*, is expressed by a vector $X = [x_1,x_2,...x_n]$, where x_i can either be one, if the technical implementation TI_i is in the concept, or otherwise zero.

In order to calculate the value for a specific concept we have to find the customer functions that are possible to realise with the concept's technical implementations. The function realisation vector, *W*, represents this. *W* is calculated according to equation (2).

$$\mathbf{W}(\mathbf{X}) = \begin{bmatrix} w_1 \\ \cdots \\ \cdots \\ w_m \end{bmatrix}, \text{ where } w_i(\mathbf{X}) = \left\lfloor \frac{\mathbf{cv}_i \bullet \mathbf{X}^T}{\mathbf{1}^T \bullet \mathbf{cv}_i^{\ T}} \right\rfloor \tag{2}$$

The notation $\lfloor a \rfloor$ denotes the largest integer less than or equal to a. $\mathbf{cv}_i \bullet \mathbf{X}^T$ represents the number of technical implementations necessary for customer function *i* that are included in concept *X*. This number is divided by the sum of all functions needed in order to implement customer function *i*, i.e. $\mathbf{1}^T \bullet \mathbf{cv}_i^{\ T}$, where 1^T is a vector of ones. If *X* contains all functions needed by CF_i this quotient equals 1, otherwise it is less then one. Thus equation (2) returns 1 only for the customer functions that are implemented by *X*.

The total value, *tv*, of a concept is calculated by summing the customer value for each customer function realised by concept *X*, see equation (3).

$$tv(\mathbf{X}) = \mathbf{W}(\mathbf{X})^T \bullet \mathbf{V} \ , \tag{3}$$

where *V* is the customer value for each customer function, i.e. $\mathbf{V}^T = [v_1, v_2, ..., v_m]$.

The cost of implementing each technical implementation is represented by the implementation cost vector *IC*, $\mathbf{IC}^T = [ic_1, ic_2, ..., ic_n]$, where each implantation cost, ic_i, is made up of the development, material and production costs. The total cost, *c*, for the concept is thus simply obtained by multiplying *X* and *IC*, see equation (4).

$$c(\mathbf{X}) = \mathbf{X} \bullet \mathbf{IC} \tag{4}$$

In this simplified model, the company profit, p, is expressed as the value the customer is prepared to pay for a particular concept minus the cost of developing and producing it, see equation (5).

$$p(\mathbf{X}) = tv(\mathbf{X}) - c(\mathbf{X}) \tag{5}$$

The problem could thus be described as finding the concept *X* that maximises the profit $p(\mathbf{X})$ without exceeding the cost *c*(X), see equation (6).

$$\begin{aligned} &\max_X \ p(\mathbf{X}) \\ &\min_X \ c(\mathbf{X}) \\ &\text{s.t.} \ \ \mathbf{X} = [x_1, x_2, ..., x_n] \\ &\qquad x_i = 0 \vee 1, \forall i \{1,2,...,n\} \end{aligned} \tag{6}$$

2.2 Safety considerations

The safety problems that arise with the mechatronic systems in the automotive industry are not unique; there are many systems also in other industries that are safety-critical with large numbers of functions. Even other non-safety critical systems can have this kind of problem although a failure may result in customer indignation rather than a safety hazard. Products introduce on the market have to have reasonable risk, in other words they have to be safe [11].

Risk according to most safety standards [12] and safety litterateur e.g. [13] [14] consist of two parameters the frequency of the event and the consequences of the event and is defined as:

$$Risk = Frequency\ of\ the\ event \cdot Consequences\ of\ the\ event. \qquad (7)$$

Since several events can occur, the risk is the sum of all events. For n events, the risk is then

$$Risk \ = \sum\nolimits_i^n (frequency)_i \cdot (consequence)_i \qquad (8)$$

2.2.1 Consequence

The consequence (Hazard) of an event is what will happen if a piece of equipment or component does not perform its intended function. The definition of a hazard is "*a state or set of conditions of a system (or an object) that, together with other conditions in the environment of the system (or object), will lead inevitably to an accident (loss event)* [14]. This relates to the customer functions and not to the technical implementations, as it is always the loss of function the user/driver will experience and not which component or system that actually failed. The hazard can be identified by the use of Functional Hazard Analysis (FHA) [14]. Commonly used standards have four severity categories: Catastrophic, Critical, Marginal, and Insignificant, which describe the severity of Hazards [12]. In different standards there are different criteria for the different severity categories, one example being the MIL standard-882D [15], the specifics of which can be seen in Table 1.

Table 1. Severity categories in the MIL STD-882D standard [15].

Description	Environment, Safety, and Health Result Criteria
Catastrophic	Could result in death, permanent total disability, loss exceeding $1M, or irreversible severe environmental damage that violates law or regulation.
Critical	Could result in permanent partial disability, injuries or occupational illness that may result in hospitalisation of at least three personnel, loss exceeding $200K but less than $1M, or reversible environmental damage causing a violation of law or regulation.
Marginal	Could result in injury or occupational illness resulting in one or more lost workday(s), loss exceeding $10K but less than $200K, or mitigable environmental damage without violation of law or regulation where restoration activities can be accomplished.
Insignificant	Could result in injury or illness not resulting in lost workday, loss exceeding $2K but less than $10K, or minimal environmental damage not violating law or regulation.

There exist different approaches in order to turn the qualitative severity categories into quantitative; in this work we use the CENELENC standard [16]. The CENELENC stipulates the quantities 10^{-1} for Catastrophic, 10^{-2} for Critical, 10^{-3} for Marginal and 10^{-4} for Insignificant hazards.

2.2.2 Reliability

As stated in formula (7) the risk depends on the frequency of the event and the consequences of the event. The frequency of an event is defined as:

Frequency of an event = 1- Reliability (9)

Reliability is defined as "*the probability that a piece of equipment or component will perform its intended function satisfactorily for a prescribed time and under stipulated conditions*" [14]. The reliability relates to the technical implementations and can be obtained either from field data or from standards estimating reliability for non-tested components. In order to evaluate the complete system risk, it is necessary to obtain each function's reliability which when multiplied, according to the CENELENC, with the function failure consequence can be summed with the other functions risk to the total systems risk. The problem is that in this early project phase no architecture exists for the system. The aim of the phase is to establish which customer functions and technical implementations the design specification should contain; the next step is to develop the architecture. Without the system architecture the reliability for each function can not be obtained, this means that an architecture must be assumed. In this case strict series architectures are assumed where the system stops functioning if one component fails. This is the worst scenario possible and often gives a fair estimation of the later architecture at this level of abstraction. If redundancy is already planned at this level, the redundant components have to be modelled as single component. The frequency of the event is expressed in failure per hour.

2.2.3 Concept risk evaluation

In order to evaluate each concepts risk, two more input vectors of data are needed. The first vector **H** = [h_1, h_2, ..., h_m], contains the hazard for each customer function and the second vector **F** = [f_1, f_2, ..., f_n] containing the frequency of malfunction for the technical implementations. The reliability of each customer function is calculated by multiplying the reliability for the technical functions needed in order to realise that customer function. Consequently, the frequency of malfunction for each customer function, cff_i, can be calculated according to equation (10). **CFF** is the customer function frequency vector which contains the malfunction frequency for all customer functions. The risk for each customer function, cfr_i, is then obtained with help of the CENELENC standard by multiplying the frequency of malfunction with the hazard, see equation (11), where *diag(**H**)* represents a diagonal matrix with the elements of **H** in the diagonal. The total risk, *R*, of a concept is equal to the sum of the customer functions' risks included in the concept. Thus R is calculated by multiplying the customer function risk vector with the function realisation vector **W**(**X**), see equation (12).

$$\mathbf{CFF} = \left[cff_1, cff_2, ..., cff_m\right] \text{ where } cff_i = 1 - \prod_{j=1}^{n}\left(1 - f_j\right), \forall j \text{ where } \mathbf{CM}_{ij} = 1 \qquad (10)$$

$$cfr_i = h_\mathrm{i} \cdot cff_i \;\Rightarrow\; \mathbf{CFR} = diag\left(\mathbf{H}\right) \cdot \mathbf{CFF} \qquad (11)$$

$$\mathbf{R} = \mathbf{CFR}^T \cdot \mathbf{W}\left(\mathbf{X}\right) \qquad (12)$$

Safety of concepts is possible to evaluate using *CR.* Safety is defined as an acceptable risk; which there are different ways to evaluate [11]. In this work the safety risk classification matrix of the CENELEC safety standard is used [16], see Table 2. This standard is used since it provides quantitative measures where the definition in (7) can be applied to this problem and calculated without changes or extra procedures and thus possible to automate.

Table 2 shows that risk classification has a logarithmic behaviour where a risk of: 10 $^{-4}$ and above are Intolerable, between 10 $^{-7}$ and 10 $^{-5}$ are Undesirable, between 10 $^{-9}$ and 10 $^{-8}$ are Tolerable, and 10 $^{-10}$ and lower are Negligible. In the case study it was decided that a reasonable risk is 10 $^{-8}$, concepts with lower risks are regarded as safe concepts.

Table 2. Risk classification matrix from the CENELEC standard [15]

Hazard probability level		Risk Classification			
Quantitative	Qualitative				
y. 10 $^{-2}$	Frequent	Intolerable	Intolerable	Undesirable	Undesirable
y. 10 $^{-3}$	Probable	Intolerable	Undesirable	Undesirable	Undesirable
y. 10 $^{-4}$	Occasional	Undesirable	Undesirable	Undesirable	Tolerable
y. 10 $^{-5}$	Remote	Undesirable	Undesirable	Tolerable	Tolerable
y. 10 $^{-6}$	Improbable	Undesirable	Tolerable	Tolerable	Negligible
y. 10 $^{-7}$	Incredible	Tolerable	Tolerable	Negligible	Negligible
x, y are scaling factors {.. , 10 -1 , 1, 10, .. } depending on application		Catastrophic	Critical	Marginal	Insignificant
		x. 10 -1	x. 10 –2	x. 10 -3	x. 10 -4
		Hazard severity level			

3 Results

The results presented are mainly from a case study at Volvo Car Corporation. This case study was conducted within the same area of active safety systems as the case study mentioned in the earlier work [3] but more extensive as the extra criterion, safety, been added. Advanced engineering had 52 potential customer functions for new car project, which together required 48 technical implementations giving more the 70 billion concepts possible to implement in the car design. The application of the Pareto-front optimisation with the two goals: maximise profit and minimise development cost, gave the results seen in the upper front in Figure 1.

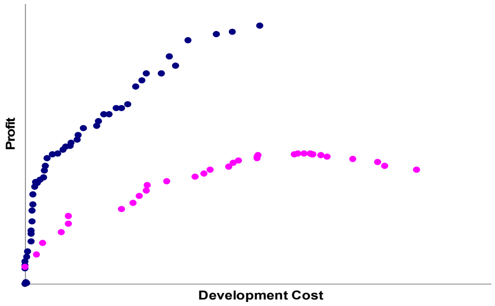

Figure 1. Pareto-front visualising the optimisation result of the Volvo Car's case study and the results from previous methods used at VCC. The upper front is the optimisation result, the lower the result from VCC's previous approach. The scales on both axes are linear with origin of coordinates zero but with different scales.

In descriptive study II the designers felt that the Pareto-front gave them a good overview of the problem; it was appreciated that there were no weights in the goal function as these were difficult to estimate, and that only one optima was the result, limiting the designers possibility to chose. The approach with the weighted goal function in [3] had given valuable information but the designers had started building Pareto-front themselves to view the problem by guessing weights. This was, however, time consuming and it was difficult to know if all potential concepts had been found. The prioritisation of customer functions to be included in the car project made “the old way” by experts relying on their “gut feeling” are also included in Figure 1. and shows great potential for optimisation.

3.1 Exploring safety of concepts

The study continued by safety analysis of the concept in the Pareto-front as the issues in this paper arose because some of the concept, when built according to previous work, was shown to be unsafe. In Figure 2 the concept's risk (CR) is seen. There is step in the risk results for different Pareto optima, which otherwise is relatively continuous in its dependency between profit and development cost of the concepts. Before this step, the concepts are regarded as safe, and after they have an undesirable high risk.

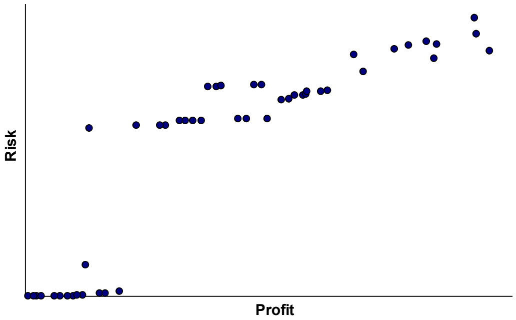

Figure 2. The Pareto concepts risk as a function of profit.

In order to analyse the risk contribution of each different function, the functions’ risks were evaluated (seen Figure 3). The results implied that there are four functions that have potentially high contribution to the safety problem. It showed that only function 1 is frequently used in the concepts and it is this function that causes the problem. The other three functions are expensive as well as having high risk, and are not used by the Pareto-optimal concepts. Function 1 depends on three technical implementations with malfunction frequencies of 10^{-7}, 10^{-6}, and 10^{-10} respectively. The problematic component is the one with the highest frequency of malfunction. This implied that the possibility to increase the reliability of this particular technical implementation should be investigated. It showed to be a fairly inexpensive sensor, which was exchanged for one with significantly better reliability but at double the cost: the result is seen in Figure 4, note that the risk scale is different from Figure 2. A new economical evaluation was made and showed that this redesign did not effect the Pareto-front. It could, however, have been a key component, which would have required a new approach to be taken where the technical implementation in question was eliminated. In the cases where several solutions with almost the same profit exist, the designer is advised to also consider the risk as a factor of selection although all concepts are safe.

5. Discussion and conclusions

In the case study a clear problem could be identified in one of the functions, but this is not always the case. It can be that almost all concepts in the Pareto are unsafe and that several factors contribute to the concepts being unsafe. In these cases it can be better to use safety as a limiting criterion in the optimisation. The advantage is that all concepts in the Pareto front will be safe; the disadvantage is that it is harder to see potential for modifications that can give even better concepts.

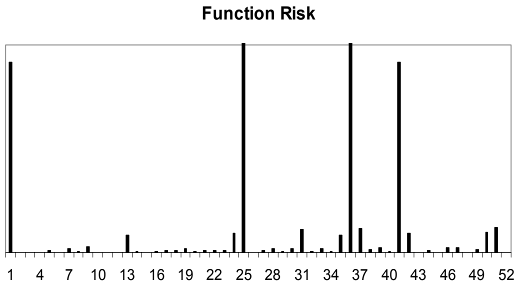

Figure 3. The CFR of the functions

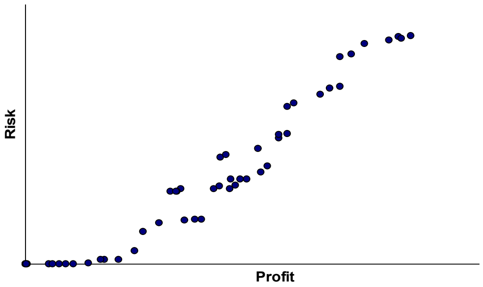

Figure 4. The Pareto concepts risk as a function of profit after change of the critical implementation

In some cases it can be difficult to decide which approach to use. An option is then to solve the case as a three-dimensional Pareto optimisation with the aims to maximise profit, and minimise development cost and risk. The result of this approach used on the problem in the case study can be seen in Figure 5. The difficulties with three-dimensional Pareto optimisation is that it is somewhat slower to solve than in two dimensions, but what is more important it is difficult for the designers to evaluate the result. It is not only the three-dimensional response that makes it difficult to understand the answer. There are many solutions that are not “clever” choices. This depends on the minimising of risk, because safe is defined as tolerable risk many concepts will be chosen with a risk much lower then is required for a safe product. These concepts will often have poor performance with regard to the other optimisation criteria giving less attractive concepts. The usefulness is therefore mainly that it can be seen if the Pareto surface indicates a stable growth of risk when profit increases and development cost decreases or, as in the case in Figure 6, there are spikes in the surface. If there are spikes the approach used in this study is to recommend since it indicates that particularly weak areas exist. If, on the other hand, the surface is smooth and shows the absence of specific weaknesses, the optimisation with safety as the limiting criteria should be used.

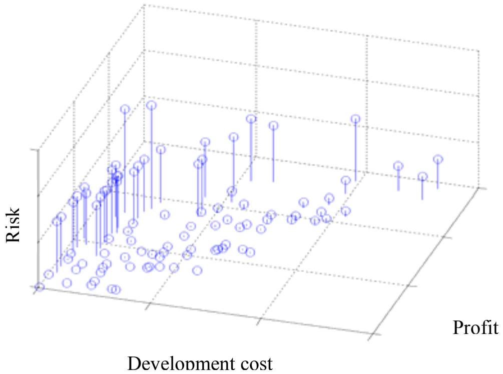

Figure 5. The resulting surface from the three dimensional Pareto optimisation. Each concept is seen as a sphere.

In the work presented it has been shown that Pareto optimisation can add great value to selection of which customer functions that should be included in systems and products with open architecture. The method presented helps the designer to identify the concepts with best potential without having to weight the different criteria in the goal function. The problem of an unsafe concept being selected has been addressed and successfully eliminated. It was shown that unsafe concepts could be found early, even before the design specification and product architecture existed, and the designers could be assisted in finding key issues to address, issues which could otherwise jeopardise the success of concepts.

References

[1] Birkhofer H., “From mechanics to Mechatronics – Towards a Demand-Oriented Education in Machine Elements”. Institute of Machine Elements and Engineering Design, Dramstadt University of Technology, 2000.

[2] Coulouris G. Dollimore J. and Kindberg T., “Distributed Systems, Concepts and Design.”, Addison-Wesley, Harlow, 2001.

[3] Grante C. Williander M. Krus P. and Palmberg JO., “An approach for Structuring of Design Specification for Complex Systems by Optimization.”, Proceedings of ICED’01, Vol. 2, Glasgow, 2001, pp. 513-520.

[4] Pugh S., “Total Design”, Addison-Wesley, Workingham, 1990.

[5] Pahl G. and Beitz W., “Engineering Design”, Springer-Verlag, London, 1996.

[6] Grante C., Williander M., Krus P. and Palmberg J, “Optimization of Design Specification for Mechatronic Automobile Systems.” Proceedings of SICFP’01, Vol.3, Linköping, 2001.

[7] Blessing L., Chakrabarti A. and Wallace K., “Designers – the Key to Successful Development”, Springer-Verlag, London, 1998.

[8] Suh N., “Axiomatic Design.” Oxford University Press, New York, 2001.

[9] Ulrich K. and Eppinger D., “Product Design and Development. Second edition”, McGraw-Hill Companies, US, 1995.

[10] Fonseca C. and Fleming P., “Multiobjective optimization and multiple constraint handling with evolutionary algorithms - Part I: a unified formulation.”, IEEE Transactions on Systems, Man, & Cybernetics Part A: Systems & Humans, vol. 28, 1998, pp. 26-37.

[11] Bahr N.J., "System safety engineering and risk assessment: A practical approach", Taylor and Francis, Wash. DC, 1997.

[12] Papadopoulos Y. and McDermid J. A., “The potential for a generic approach to certification of safety critical systems in the transportation sector”, Reliability engineering & system safety, 1999, pp. 47-66.

[13] Thomson J.R., “Engineering Safety Assessments, an introduction”, Longman Scientific & Technical, Longman Group UK Limited, 1987.

[14] Leveson N., “Safeware, System Safety and Computers”, Addison Wesley, Reading, 2000.

[15] ”MIL-STD-498, Software Development and Documentation”, USA Department of Defense, 1994.

[16] ”CENELENC (European Committee for Electrotechnical Standardisation), Railway Application: the specification and demonstration of dependability, reliability, availability, maintainability and safety. Draft prEN 50126”, 1995.

For more information please contact:

Christian Grante Volvo Cars, PVÖS36 SE-408 31 Göteborg Sweden
Tel: Int +46 31 595853 E-mail: cgrante@volvocars.com