HOW TO USE AN OPTIMIZATION BASED METHOD CAPABLE OF BALANCING SAFETY, RELIABILITY AND WEIGHT IN AN AIRCRAFT DESIGN PROCESS

Cristina Johansson[1,2], Micael Derelöv[2], Johan Ölvander[2]

[1] *SAAB Aeronautics, Linköping, Sweden: Bröderna Ugglas gata, 582 54 Linköping, Sweden, cristina.johansson@saabgroup.com*
[2] *Linköping University, IEI, Department of Machine Design: 581 83 Linköping, Sweden, cristina.johansson@liu.se; micael.derelöv@liu.se; johan.ölvander@liu.se*

ABSTRACT: Aircraft design is a complex process that involves many different disciplines to obtain a holistic approach. In order to help the decision-maker in early design phase to improve, more cost-efficiently, the system safety and reliability base line of the design concept, a method (MOSART) that is able to handle trade-offs such as system safety, system reliability and other characteristics, for instance weight and cost, is used. MOSART - Multi-Objective Optimization for Safety and Reliability Trade-off - has been developed and implemented at SAAB Aeronautics. The aim of this paper is to demonstrate how the implemented method might work to aid the selection of optimal design alternatives. The method is a three-step method: step 1 is modelling of each considered target, step 2 is optimization, and step 3 is visualization and selection of results (results processing). The method is implemented by using, for each objective function, the existing available tools at the company and creating a user-friendly interface to guide the potential user. This paper uses the method to find the optimal choice of equipment vendors (the solutions balancing safety, reliability, weight and cost) of a fuel system concept (selection of design alternative). Due to the nature of the optimization problem, the optimization technique used is based on a Genetic Algorithm. The safety and reliability objectives were modelled using existing models within the Reliability Workbench program. In this paper, the analysis is performed within Architecture Design and Preliminary Design steps, according to the company's Product Development Process. The existent failure data and the associated cost and weight of every part included in the system are used to find the optimal design solutions. In order to investigate what can be gained and what can be learned from this demonstration, the problem is formulated in three different ways. Case a is to find the solutions balancing the safety, reliability, weight and cost of a fuel system concept and propose a selection of vendors for equipment. This case uses one main system safety and one system reliability objective as well as cost and weight objectives. Case b has been extended for three slightly different architectures of the system. The same objectives and weighting of objectives against each other are performed for all three architectures (slightly different concepts). Three configurations of the fuel system are compared and one of the architectures might be chosen. Case c has also the same scope as in case a, extended by using multiple safety or reliability objectives. The lessons learned regarding use of the implemented trade-off method in the three cases are presented. The results are a handful of solutions, a basis to aid the selection of a design alternative. While the implementation of the trade-off method is performed for a company, there is nothing to prevent adapting it to be used in other industrial applications with minimal modifications.

I. INTRODUCTION AND BACKGROUND

The Product Development Process (PDP) comprises numerous steps or phases, described somewhat differently by different authors (Ref. 13). Various authors present different models of the design process, such as for example Refs. 12, 2 and 9. Companies also have their own view of how to proceed in the process, although they have great similarities (Ref. 4). Staged processes were popular for decades because of their controlled design structures (Ref. 13). These processes methodically follow a series of steps, are characterized by few iterations and rigid reviews, and tend to freeze design specifications early. The generic development process should be divided into the following six phases according to Ref. 12. In this paper, the term *early design phases* means the time span from late in concept development to midway through system level design, as presented in Fig. 1.

Aircraft design is a complex process that involves many different disciplines to obtain a holistic approach. In order to reach an optimal solution, there are many aspects that need to be balanced against each other, e.g. safety requirements, reliability goals and performance specifications. System safety and reliability are, among other factors, two driving forces in

an aircraft design. However, while system safety and reliability analyses might begin early in the design (Ref. 10), with the aim of increasing confidence in the chosen design and avoiding taking decisions regarding design changes at a later stage (which means higher costs), it is in a later phase of the design that most of the system safety and reliability work is done. In practice, the designer is typically faced with the challenge of simultaneously achieving several targets (e.g. low costs, high revenues, high reliability, low accident risk). Typically, the targets related to economic performance and those related to safety performance may very well be in conflict so that the final choice is necessarily a compromise solution (Ref. 3). Trade-offs between these targets in early design phases might improve the reliability and system safety *base line* and avoid late changes due to safety or reliability issues. In this paper, the term *base line* means the preliminary results of system safety and reliability objectives, based on allocated values.

A method (MOSART - Multi-Objective Optimization for Safety and Reliability Trade-off*)* that is able to handle trade-offs such as system safety, system reliability, weight and cost has been developed by the author in Ref. 4 and implemented at SAAB Aeronautics.

The aim of this paper is to demonstrate how the implemented trade-off method (MOSART) might work in practice to aid the selection of design alternative.

Aspects considered in this paper concern what can be learned from analysing system architectures and what can be gained by applying the method. Three cases are considered to highlight those aspects. One case is when the implemented method is tested on a fuel system concept in order to find a balanced combination of vendors for the system's elements. Another case is when several architectures are compared from a system safety, reliability, cost and weight standpoint. The last case is to investigate the possibility to find an optimal solution for the design vector when balancing several safety objectives against the cost and weight objectives, when an additional system safety objective has been introduced.

II. METHOD REVIEW

The core of designing is reasoning from function to form. One of the most important tasks of design methodology is to indicate how design processes should be arranged so that they nevertheless lead to reliable, effective conclusions and are efficient as well, according to Ref. 9.

During Conceptual Development, numerous design concepts are generated and evaluated to determine whether a particular set of requirements (in terms of performance, cost, safety, etc.) can be met and associated with levels of technology and risk. The key issues of basic configuration layout and performance are addressed and one or two basic concepts will be taken forward to the *System-Level Design* phase.

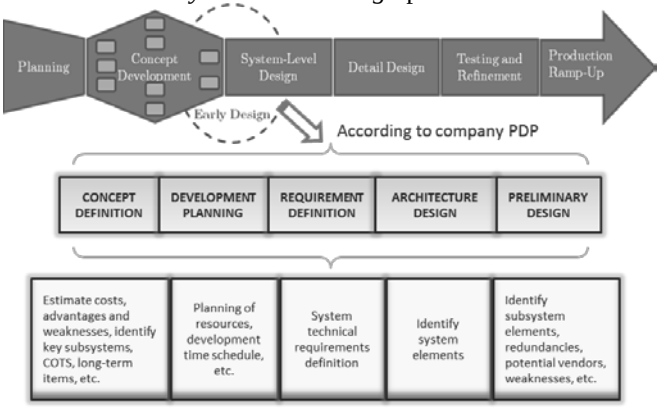


Fig. 1. Activities performed within early design phases according to the company's Product Development Process - PDP

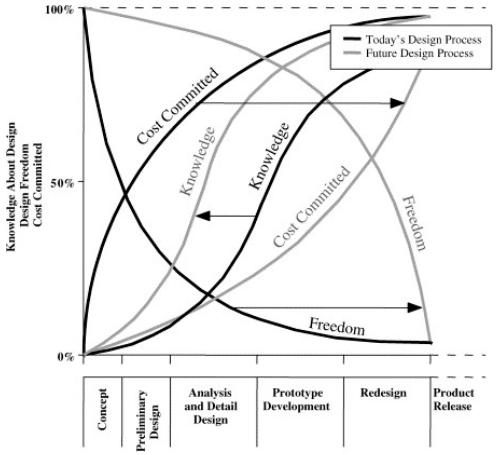


Fig. 2. Design Evolution according to Ref. 7

The selected concept(s) begin to increase in level of detail. Sub-systems begin to take shape while detailed analyses and simulations are carried out. During this phase, the product is defined and the design will be *frozen*. The final step in the design process is the *Detailed Design* phase, during which all components and parts are defined in full detail and most of the manufacturing documentation is produced. According to the company's PDP, the steps shown in Fig. 1 are performed in early design phases. Design problems are always set within certain limits or constraints. One of the most important limits is that of cost (Ref. 2). It is in the early phases of the design process that most of the cost is committed. Within the timespan of the design process, knowledge about the problem is gained but the design freedom is lost due to the design decisions made during the process. The desire to shift more knowledge forward in the design timeline is complicated by an equally

important, according to Ref. 7, caveat: tracking the incompleteness in knowledge representation that (defined as uncertainty) is always prevalent in early design stages. In the effort to make good design decisions, one is interested in how this uncertainty affects both the feasibility (which deals with constraints) and viability (which deals with objectives) of the design space of alternatives. The characteristics of design evolution with time are illustrated in Fig. 2. A generic objective, or measure of value for the design process (for instance *knowledge* and *freedom*, as well as *cost committed*), is displayed as a random variable with a time-dependent probability distribution. As the design evolves, according to Ref. 7, it is desirable to shrink the variability of this objective, as well as shift its mean to more desirable levels (a *lower the better* scenario is depicted in Fig. 2). Nowadays, in other words, it is essential within the design of new products, to increase awareness (knowledge) early in the design phases and keep the design decisions (freedom) open as long as possible, and with that also keep down the allocated costs.

A method that can make possible the change in the desired direction, by balancing contradictory objectives, to aid the decision-maker in early design phases, has been developed and implemented at SAAB Aeronautics: MOSART, Multi-Objective Optimization for SAfety and Reliability Trade-off.

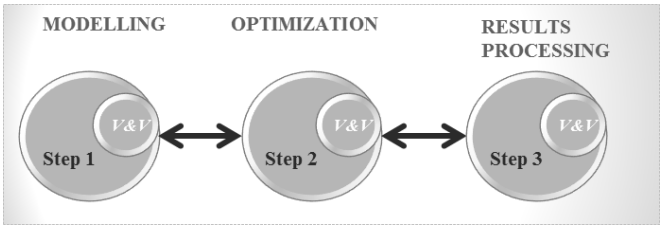


Fig. 3. The theoretical method (MOSART)

MOSART, (based on Ref. 4) is a general three-step method, shown in Fig. 3, that is able to balance several objectives of varying mathematical nature that have high impact on the design choices. The steps are *model building* for cost, weight and system reliability and safety, etc., *optimization*, and *results processing* with selection of optimal trade-off solution. However, the formulation influences the optimization technic used to solve the optimization problem. The chosen strategy is to convert the multi-objective optimization problem into a single objective problem by using an aggregating method. Weighted sum approach (Ref. 1) combines different objectives using some weights w_i, $i = 1,..., M$ (where $w_i \in [0, 1]$ is the weight of the M-th objective function and M is the number of objectives). Then using these weights the objective functions are merged into a single function. Thus, the objective function is:

$$f(x) = \sum_{i=1}^{M} w_i \times f_i(x) \tag{1}$$

Using weighted sum of the objectives can only be done after normalizing the objective values. The general form of the optimization problem now is minimize/maximize $f(x)$. Due to the nature of the optimization problem, the optimization technique used for solving is based on a Genetic Algorithm (GA) (Refs. 15, 3 to 5). The optimization is performed multiple times, for several relative estimated importance vectors w, since when using this preference-based strategy (weighted sum), the optimal solution obtained is highly subjective to the particular user.

Fault Tree Analysis (FTA) (Refs. 7, 8, 10, 11 and 14) is used to model system safety, Reliability Block Diagram (RBD) (Refs. 7, 8 and 14) for reliability characteristics.

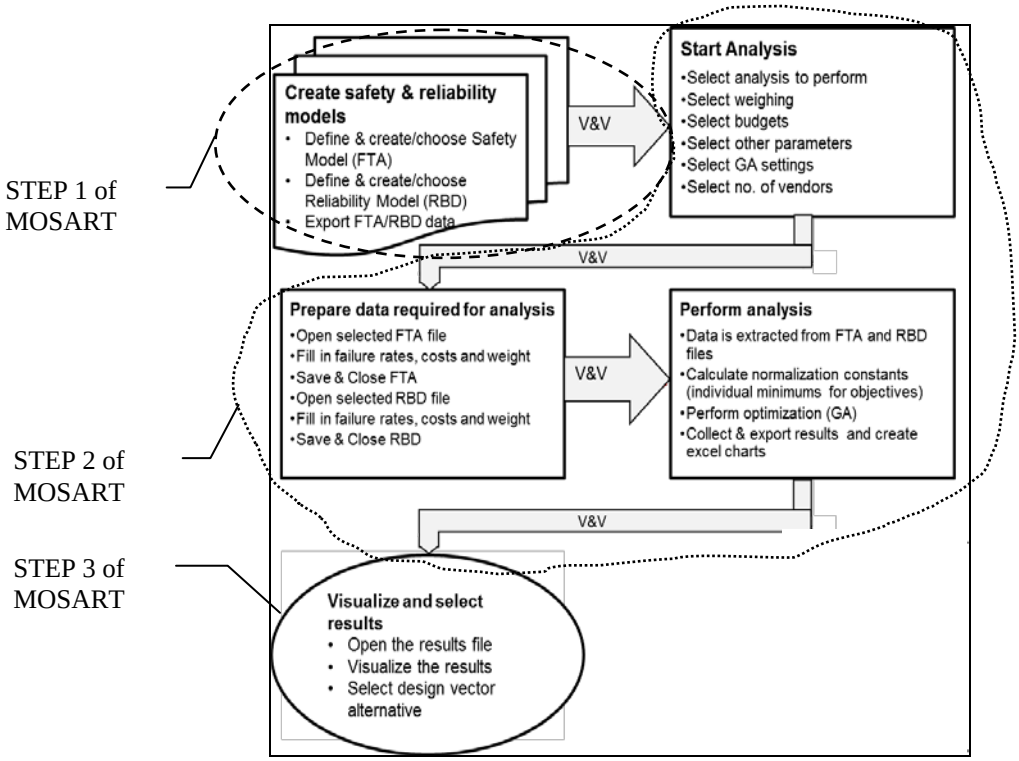


Fig. 4. Analysis steps from a user point of view (the legend refers to the method steps in Fig. 3)

The method was implemented using (for each objective function) the tools available at the company and creating a user-friendly interface to guide the potential user. The analysis workflow when working with the implementation of the MOSART method described in Fig. 3 is shown in Fig. 4. The legend connects the method from Fig. 3 with the analysis workflow of its practical implementation at SAAB. The practical use of the method is followed in a case study in section III.

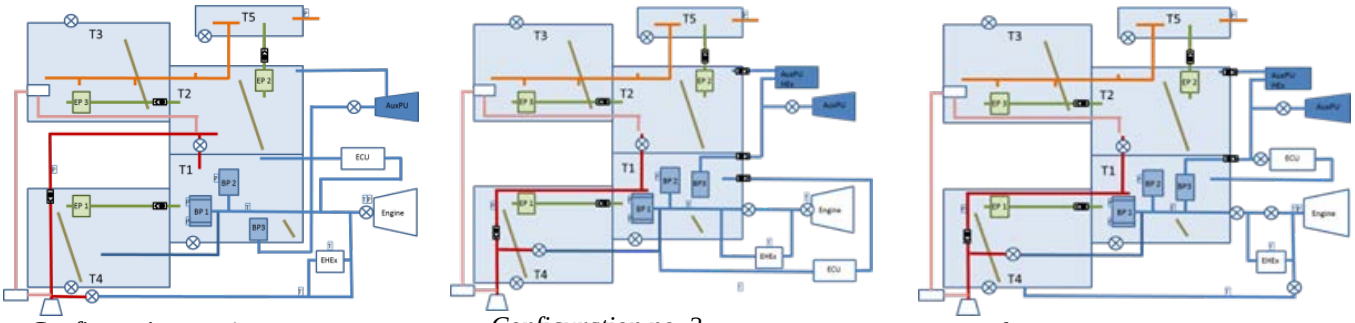
III. CASE STUDY

The case study is on an aircraft's fuel system. Several concepts are investigated. The desired solution is the one with the lowest probabilities of occurrence for the system safety objective, the highest probability of occurrence for reliability, and the lowest values of cost and weight (Fig. 3 and Fig. 4). As these objectives are naturally contradictory, there seldom exists one design that meets all these goals.

In this paper, it is assumed that the best benefit of such an analysis might be obtained when there is some input data for all chosen objectives, while still being able to change the architecture design without entailing huge costs (Fig. 2). It is difficult to decide beforehand when the best results of such an analysis will be achieved (Ref. 13). In the concept definition phase (Fig. 1) it was very difficult to collect data about all the objectives' costs, weights, potential vendors, *failure rates* or *mean time between failures* - MTBF, etc. For instance, these kinds of data were available (though incomplete) sometime in the timespan between the end of configurations no. 1 and no. 2 (Fig. 5) of the fuel system. This situation might differ from project to project and from company to company. Therefore, the analysis is performed within the *Architecture Design* and *Preliminary Design* steps, according to Fig. 1.

III.A. Fuel System Description

The general layout of the fuel system may consist of one or more boost pumps that feed the engine from a collector tank (for instance T1 in Fig. 5). The collector tank is replenished by a fuel transfer system, which pumps fuel from the source tanks (T2, T3 and T4 in Fig. 5).



Configuration no. 1 *Configuration no. 2* *Configuration no. 3*

Fig. 5. Fuel System preliminary architecture (Configurations no. 1, 2, 3)

The system may be pressurized to avoid spontaneous fuel boiling at high altitude and cavitation in pumps, or to provide the means for fuel transfer. An aircraft's fuel system may consist of several subsystems, according to the functions to be provided, such as:

- Engine Feed System
- Auxiliary Power Unit Feed System
- Fuel Transfer System
- Pressurization and Vent System
- Centre of Gravity control
- Refuelling System
- Measurement and Management System
- Fire Prevention and Explosion Suppression System
- Cooling System where the fuel serves as a heat sink to other systems.

In the *Architecture Design* step (Fig. 1) short loops are performed, providing slightly different architectures of the fuel system. Each of these architectures is analysed and reviewed from a system safety and reliability standpoint, simulations and calculations are performed for several performance parameters, and the proposed architecture is updated according to new data. Three different architectures, focusing on providing fuel feed to the engine and auxiliary power unit as well as providing a heat sink for the engine's electronic control unit (ECU) are used as examples in this paper and shown in Fig. 5.

III.B. Problem Formulation

The three steps in the method in Fig. 3 are followed according to Fig. 4. The aim is to achieve a balance between the system safety, reliability, cost and weight targets. A solution x is a vector of n decision variables: $x = (x_1, x_2, \ldots, x_n)^T$. For instance, a vector of design variables x is used (for the sake of simplicity, in this case study called *design vector*- DV), which can adopt a number of integer values where each integer represents a different alternative. These alternatives are the system elements, e.g. components/items in the system. Each alternative includes data about the selection of suppliers, costs, weights, failure rates or mean time between failures – MTBF. The cost objective includes only the purchase cost of all system elements from all potential vendors. The weight objective is the sum of all elements' weight and might differ depending on the vendor. The system safety objective might be different depending on the failure conditions analysed, for instance *loss of fuel feed to the engine*, *loss of cooling to engine control unit (ECU)*, etc. The reliability objective is considered to be full function of the respective subsystem of the fuel system (feed fuel to the engine, provide ECU cooling, etc.).

The objective function can be formulated in different ways. It might be formulated as easy to solve problems, such as finding individual solutions that minimize the cost or the weight. On the other hand, problems might be stochastic and harder to solve, e.g. find individual solutions that maximize the safety or reliability of the system. Perhaps the most interesting problems, however, are a mix of all factors. The influence of each objective in each analysis to be performed (from individual minimums to a mix of all factors) and the potential constraints are chosen arbitrarily.

Other aspects considered in this paper concern *what can be learned* from analysing one of the architectures presented in Fig. 5 and *what can be gained* by applying the method presented in section II. Three cases are considered to highlight those aspects:

- *Case a:* Analyses the safety and reliability, weight and cost objectives of one architecture.

First, the implemented method is tested on a fuel system concept in order to find a balanced combination of vendors for the system's elements. The analysis is performed on configuration no. 1, in Fig. 5. The system safety objective is *no fuel*

supply to the engine. This event causes engine disturbances and loss of aircraft and is thus one of the most important failure conditions to analyse.

- *Case b:* Analyses the safety and reliability, weight and cost objectives of three architectures.

Second, this paper investigates what can be learned when comparing several architectures from a system safety, reliability, cost and weight standpoint. The analysis is performed repeatedly on configurations no. 1, no. 2 and no. 3, as shown in Fig. 5. All the objectives are maintained as in *Case a*.

- *Case c:* Analyses multiple safety objectives and one reliability, weight and cost objectives of one architecture.

Third, an additional system safety objective has been introduced to investigate the possibility to find an optimal solution for the design vector when balancing several safety objectives against the cost and weight objectives. In everyday engineering practice, a system safety engineer has to investigate several failure conditions causing the same output (with the same criticality). The system safety objectives are *no fuel supply to APU during engine flame out* and *loss of cooling to ECU*. Both events will cause engine disturbances and loss of aircraft. The reliability objective is to *provide fuel supply to APU* and is of interest from a mission reliability standpoint.

IV. RESULTS

The results obtained are a handful of design solutions (in the form of design vectors) regarding the choice of vendor for each piece of equipment in order to balance the objectives.

A total of 11 potential vendors for fuel system equipment are taken into consideration. The company itself is one of the vendors for installation components and some of the items. For each item, weight and a general failure rate are provided. Some of the items have several potential vendors, while others have just one possible solution, with just one vendor.

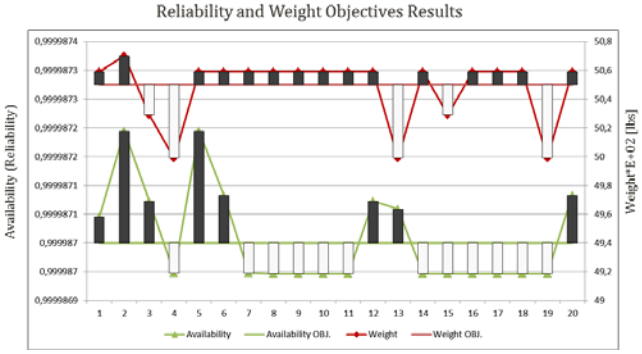
The design vectors consist of several positions (for instance, 29 positions in *case a*), each position taken by an element of the fuel system and consisting of integer values between 1 and 11, representing the identified potential vendors.

- *Case a*

In this case, the safety objective is *loss of fuel feedto the engine*, the reliability objective is *provide fuel feeding to the engine*, and the cost and weight objectives are as described in section III.B.

The results can be visualized (step 4 in the method) to highlight the gain or loss of each objective compared with the requirements or goals for the respective objective, as shown for instance in Fig. 6 a. and b. The black stamps in Fig. 6 a. indicate the results that do not meet the requirement/goal for the respective objective, while the white stamps show the gain when the results of each objective are compared with the requirement/goal. The top stamp-diagram in Fig. 6 a. represents the cost objective, while the bottom stamp-diagram represents the safety objective. In Fig. 6 b. the top stamp-diagram represents the weight objective and the bottom diagram stands for reliability objective.

a. Safety and Cost Objectives compared with the requirements / goals



b. Reliability and Weight Objectives compared with the requirements / goals

Fig. 6. Objectives compared with requirements/goals

The safety objective results for the 20th solution in the analysis can be read on the left vertical scale, while the cost objective results can be read on the right scale in Fig. 6.a. Similarly, in Fig. 6.b the reliability objective results can be read on the left vertical scale and the weight objective results on the right scale.

In Fig. 6.a it can be observed that while some of the solutions (represented on the horizontal axis) are more cost-effective, none of the solutions meets the system safety quantitative requirement (1E-07 for loss of fuel feed to the engine).

Furthermore, the differences between the results and the safety requirement are substantial (more than 10 times higher than the requirement) and might suggest a change in fuel system architecture rather than in vendors.

In the reliability objective diagram, as the black stamps stand for probability values higher than the requirement value, they represent higher reliability than the reliability goal. Fig. 6.b shows that there are only two solutions that meet both the reliability and the weight requirement/goal: solutions no. 3 and no. 13 (solutions represented on the horizontal axis in Fig. 6.b). These solutions also meet the cost requirement (Fig. 6), but not the system safety requirement.

- *Case b*

In this case, the safety objective is also *loss of fuel feed to the engine*, the reliability objective is *provide fuel feed to the engine*, and the cost and weight objectives are as described in section .

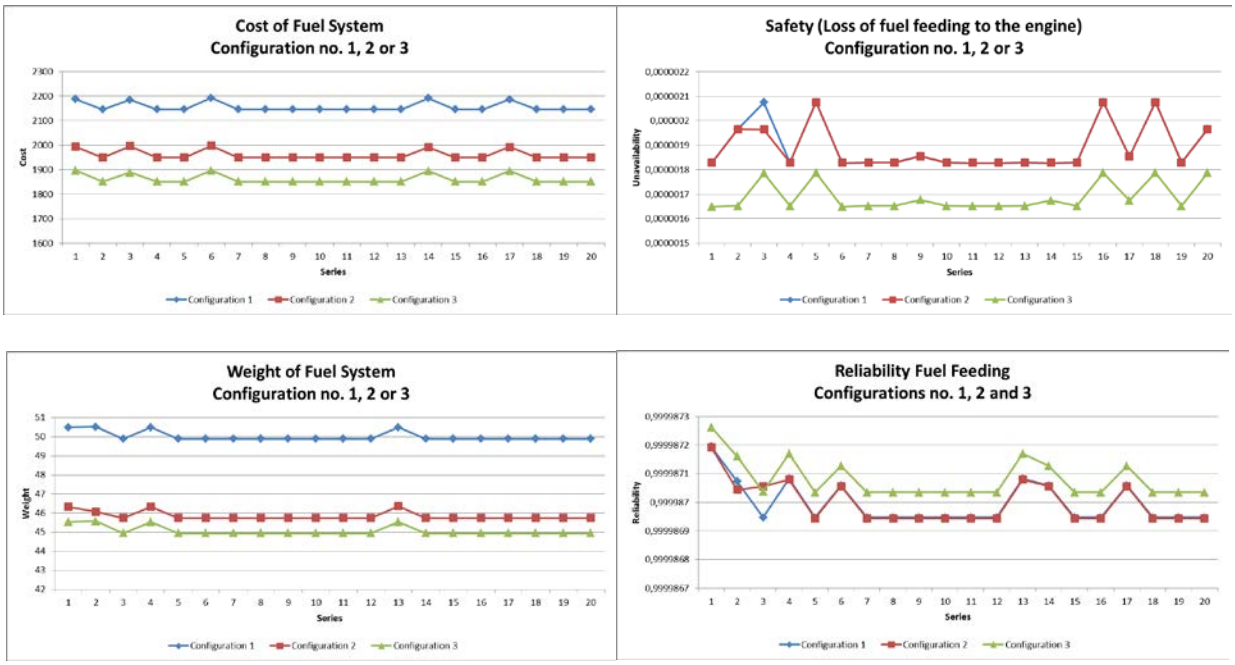


Fig. 7. Cost, Safety, Weight and Reliability objectives for all three fuel system architectures (Fig. 5)

However, the analysis is repeated for all three architectures shown in Fig. 5. The solutions of each configuration are compared for each objective (cost, safety, reliability and weight) in Fig. 7. The results in Fig. 7 suggest that configuration no. 3 (green line, triangle dots) is better than configurations no. 1 (blue line, rhomb dots) and no. 2 (red line, square dots) from all objectives' standpoints. The safety and reliability objectives have almost all the solutions identical for configurations no. 1 and no. 2, which means that from the safety and reliability standpoint there were no improvements in safety or reliability of design between these two architectures except in solution no. 3.

- *Case c*

Multiple system safety objectives, such as *no fuel supply to APU during engine flame out* and *loss of cooling to ECU*, are considered and the reliability, cost and weight objectives are as described in section III.B. These objectives concern parts of the fuel system and there are thus no requirements for cost and weight objectives. The solutions might be visualized and filtered using a parallel coordinate plot, as shown in Fig. 8.

The solution suggested (the blue line) is no. 11, where the best balance between the objectives is achieved. This is when all objectives are considered equally important. Solution no. 11 points out the suggested vendors for all elements included in the analysis in order to balance the cost, system safety, system reliability and weight objectives.

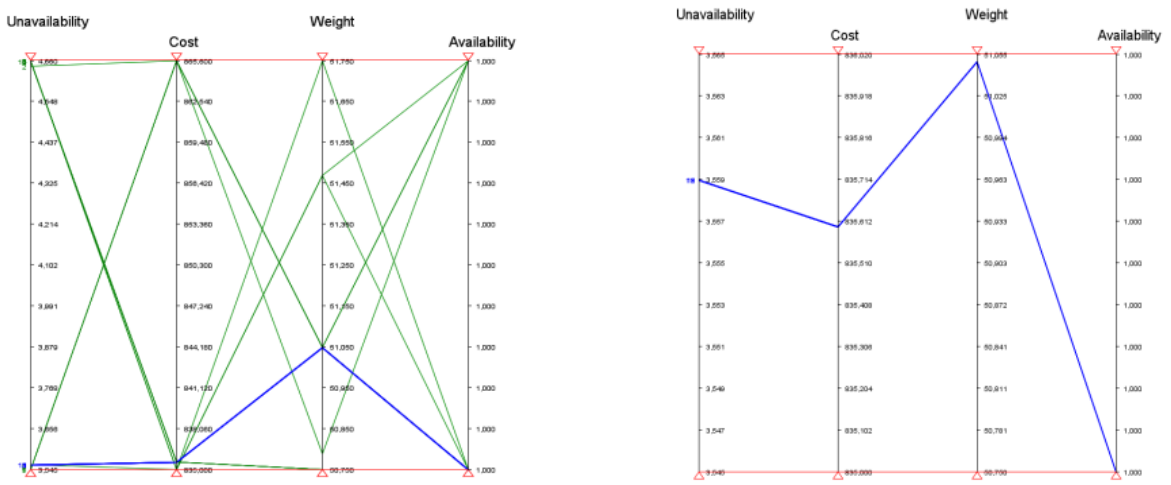


Fig. 8. Visualization and sorting of solutions in a parallel coordinate plot for multiple safety objectives

V. DISCUSSION

From the results in *Case a*, the main insight is that the design should be changed in order to be closer to the system safety requirement, since none of the solutions were even close to this requirement, while there were solutions that met all the other requirements/goals. This might be achieved by finding other vendors for the system elements, provided that it is possible from other standpoints, e.g. technological, political, financial, etc., or by changing the system architecture (more redundancy, diversity, etc.). However, the results shown in Fig. 7 suggest that this was not the case. Changes were made in the architecture of the fuel system concept (configuration no. 2), but mainly due to other characteristics. The main difference in architecture was to change the main boost pump from a hydraulic solution to an electrically driven pump. The new solution was lighter and cheaper and the results show an improvement in these objectives (Fig. 7). The failure rates, however, were similar and what is gained from a slightly better failure rate for the electrical pump is balanced out by introducing a few new elements (valves) with their potential failures. The new solutions thus do not indicate an improvement in the safety and reliability objectives for configuration no. 2.

Configuration no. 3 changes the architecture of the system by introducing a triple redundancy for feeding fuel to the engine, cooling the ECU and feeding fuel to the APU, as well as reducing, as much as possible, the number of installation components outside the fuel tanks to reduce the risk of leakage outside the fuel tanks. Although the system safety requirement is still not achieved, a clear improvement in all the solutions can be observed in the results presented in Fig. 7, as well as for the reliability objective.

Fig. 8 shows another way of visualizing and sorting the results. However, *Case c* might be the case most likely to be used in practice. The failure conditions and hazards analysed in a system safety analysis such as Functional Hazard Assessment (FHA) and Preliminary Hazard Analysis (PHA) (4 and 10) are assigned early in the design, a criticality classification and a maximum allowed probability of occurrence (safety requirements). At some point, the safety requirements might even be in contradiction. For example, introducing a heat exchanger, purchased from a certain vendor on the fuel feed line, might decrease the probability of loss of ECU cooling, but increase the probability of engine disturbances due to clogging. Using multiple safety objectives clustered by a safety requirement (for example, 1.0E-07 failures/flight hours for a catastrophic event) gives the opportunity to analyse the system at a higher level, as a whole (for example, non-combat loss rate - NCLR - might be an overall safety objective). The same reasoning goes for using multiple reliability objectives. Combining, for example, several mission reliability objectives, it is possible to trade off aircraft reliability to perform several different missions against targets like safety, cost and weight.

The analysis presented in this paper was performed not during the time line presented but afterwards in later phases of the project. This might present a challenge but also give different insights into the product development process and put MOSART in perspective.

The architectures (Fig. 5) included in this paper were developed within the time span of three months with a few weeks in-between. One challenge was to collect the information and reasoning around decision-making backwards, when the project itself was moving forward. However, the design process had an iterative development as described by Ref. 9, rather than straight forward as in Fig. 1 and Fig. 2.

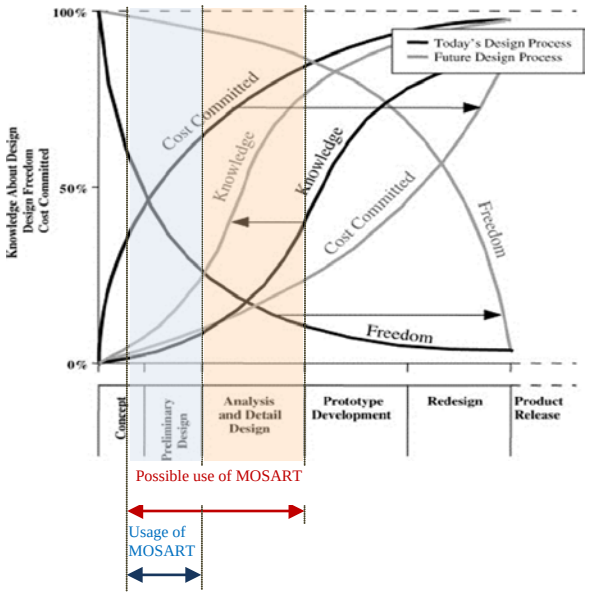


Fig. 9 Potential use of MOSART within the design process, exemplified by design evolution diagram (based on Fig. 2)

The design process during the analysed period was characterized by short loops focused on different properties of the design (three architectures within a timespan of three months). These loops comprise sequences of steps ending with a comparison between the obtained results with the desired results. The knowledge gained in one loop is fed back to the design proposal, formulation of problem and requirements. As the results also show, in one loop not all properties were considered at the same time. For example, in one loop of the case study, the designers focused on decreasing the weight of the system, disregarding the influence on system safety and reliability. System safety as a property of the system was considered in another iteration, etc. This can be explained by aspects such as specifics of the project and organisation (large project, different departments working with different systems and subjects, the physical location of the designer teams, etc.). By using MOSART, several different properties of the design (for instance safety, reliability, weight and cost) were included in one loop, covering larger parts of the solution space or, if desired, decreasing the number of iterations. The development of the design still has the iterative, somehow spiral-like character, but with another distribution of knowledge diagram as in Fig. 9. The same knowledge is gathered earlier in the design phases, when the design freedom is higher and changes are less expensive. Furthermore, the specific design phase might be somehow shortened, either by decreasing the number of loops needed to gather the same experience, or gathering more knowledge in a shorter time.

This paper assumed that the best benefit of such an analysis might be obtained when there is some input data for all chosen objectives, while still being able to change the architecture design without entailing huge costs. This was an assumption based on experience. It was possible to collect input data for all chosen objectives, according to the company's PDP in Fig. 1, first in the architecture design phase (within the concept phase in Fig. 9). While possible to use MOSART in earlier phases (such as the concept definition phase) of the PDP, when certain metrics of the design are estimated (such as key sub-systems and components, costs, etc.), the knowledge gained by applying this method in the timespan between *architecture design* and *preliminary design*, is still considered more valuable. As the design progressed, the input data has changed. For instance, for reliability and safety targets, from allocated values based mostly on engineering judgement and potential vendor predictions provided from similar items, to predictions based on analysis performed according to specific requirements and field experience for the product to be designed. Even if the design freedom decreases, MOSART might still be used within the whole *preliminary design phase* and in *detail design* (Fig. 9) to motivate trade-offs between targets (for instance safety, reliability, weight and cost). This was not included in the scope of the analysis in this paper's case study. With hindsight, this timespan might be as in Fig. 9, between the *architecture design* phase within the *concept* phase (Fig. 1), and the end of the *detail design* phase.

Analysing each proposed architecture and searching for the best balance of the objectives might also provide the company with traceability of the steps in concept and embodiment design and feedback on each decision influencing the design. Traceability is a very important property, especially within aircraft design, when it is not unusual for the time between new aircraft models to be around 20 years. The improvements in the solutions can be followed all the way through

embodiment design by comparing the architectures from different standpoints, as exemplified in Fig. 7. The design loops in new similar products might be further shortened by avoiding potential pitfalls highlighted by the usage of MOSART.

VI. CONCLUSIONS

The aim of this paper was to demonstrate how the implemented method (MOSART) might work in practice to aid the selection of a design alternative. While not without challenges, this demonstration gave an insight into the real steps and loops taken during the company during early design phases.

Using MOSART, the design is provided with a reliability and system safety base line by balancing these objectives against each other in early design. This method can facilitate the selection of system elements based on safety, reliability, cost and weight aspects and at the same time be used to shorten the process or to run more loops and with a better basis for decision-makers. Knowledge and understanding regarding how the achievement of one objective is traded off against another is gained by applying this method.

The main insights from and engineer standpoint regarding the three analysed cases are:

- *case a:* the differences between all results and the safety requirement were substantial for configuration no. 1, suggesting a change in fuel system architecture rather than in vendors.
- *case b:* configuration no. 3 is better than the other system architectures from all objectives' standpoints but the results also reflect the improvements made in each configuration.
- *case c:* the system has been analysed as a whole and one solution was pointed out when using multiple safety and reliability objectives.

With hindsight, it might be concluded that the use of a trade-off method (MOSART) as shown in this paper could

- facilitate the system architecture as well as the system element selection process and increase the probability of choosing the best concept,
- using multiple safety or reliability objectives, clustered by a safety or reliability requirement, gives the opportunity to analyse the system at a higher level, as a whole,
- increase understanding of how the achievement of one objective is traded off against another,
- shorten the loops within the design process or shorten the design process,
- can also provide good traceability of the steps in concept and embodiment design and provide feedback for decision-makers.

While the implementation of the trade-off method is performed for the company, there is nothing to prevent adapting it for use in other industrial applications with minimal modifications.

ACKNOWLEDGMENTS

The implementation and demonstration of MOSART presented in this paper is part of a research programme funded by Saab Aeronautics and the National Aviation Engineering Research Program (NFFP), jointly driven by the Swedish Armed Forces, the Swedish Defense Materiel Administration (FMV), and the Swedish Governmental Agency for Innovation Systems (VINNOVA).

REFERENCES

1. Bandyopadhyay, S., Saha, S., *Unsupervised Classification. Similarity Measures, Classical and Metaheuristic Approaches, and Applications*, Springer Berlin Heidelberg, 2013,ISBN 978-3-642-32450-5 ISBN 978-3-642-32451-2 (eBook), DOI 10.1007/978-3-642-32451-2
2. Cross, N., *Engineering Design Methods. Strategies for Product Design* (Fourth Ed.), John Wiley & Sons, 2014, England, ISBN 978-0-470-51926-4
3. Enrico Zio, Luca Podofillini, *Importance measures and genetic algorithms for designing a risk-informed optimally balanced system*, Reliability Engineering & System Safety, Volume 92, Issue 10, October 2007, Pages 1435–1447, doi:10.1016/j.ress.2006.09.011
4. Johansson, C., *On System Safety and Reliability in Early Design Phases*, Linköping Studies in Science and Technology, Thesis No. 1600, 2013, Linköping University, Division of Machine Design, Department of Management and Engineering, ISBN 978-91-7519-584-1,ISSN 0280-7971, LIU-TEK-LIC-2013:34
5. Limbourg, P and Kochs, H-D., *Multi-objective optimization of generalized reliability design problems using feature models—A concept for early design stages*, 93, Reliability Engineering and System Safety, 2008, ss. 815-828.
6. Marvin R and Arnljot H., *System Reliability Theory. Models, Statistical Methods and Applications*. Second Edition, 2004, ed. New Jersey and Canada: John Wiley&Sons, Inc. Hoboken, ISBN 0-471-47133-X
7. Mavris, D. N., DeLaurentis, D. A., A probabilistic approach for examining aircraft concept feasibility and viability , Aircraft Design, Volume 3, Issue 2, 2000, 79–101, doi:10.1016/S1369-8869(00)00008-2
8. O'Connor, Patrick D. T., *Practical Reliability Engineering* (Fourth Ed.), John Wiley & Sons, 2002, New York, ISBN 978-0-4708-4462-5.
9. Roozenburg, N.F.M. and Eekels, J., Product Design: Fundamentals and Methods, John Wiley & Sons, 1996, England, ISBN 0 471 94351 7; 0 471 95465 9
10. SAE ARP4761, *Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment*
11. Stephans, A.R, (2004), *System Safety for the 21th Century*, Wiley&Sons, ISBN 0-471-44454-5
12. Ulrich, K.T. and Eppinger, S.D., *Product design and development*. 3rd ed. New York: McGraw Hill, 2004.
13. Unger, D and Eppinger, S.D., *Improving product development process design: a method for managing information flows, risks, and iterations*, Journal of Engineering Design, 2011, 22:10, 689-699, http://dx.doi.org/10.1080/09544828.2010.524886
14. Verma, K., Srividya, A., Karanki, R.D., *Reliability and Safety Engineering*, 2010, ISBN 978-1-84996-231-5
15. Yang, C., R. Remenyte-Prescott and J. D. Andrews, *Pavement Maintenance Scheduling using Genetic Algorithms*, International Journal of Performability Engineering Vol. 11, No. 2, March, pp. 135-152, (2015).