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

EXPLORING DESIGN PROCESSES FOR SAFETY-CRITICAL SYSTEMS DESIGNED AS COMBINATIONS OF 'OFF-THE-SHELF' SOLUTIONS

Belinda López-Mesa and Christian Grante

Abstract

There is an increased incorporation of mechatronic systems in the automotive industry. Some of these systems are safety-critical. This work addresses issues of how to design this type of system, making use of knowledge from both the engineering design research domain and the safety field. The aim is to understand the factors that make a design process suitable for development of complex safety-critical products that are new combinations of 'off-the-shelf' solutions. The factors can be used by academia to evaluate new and existing processes and by industry to find weak areas in their design processes. Four design processes from different areas are analysed to evaluate their advantages, concerns and uniqueness.

Keywords: engineering process, safety, product structuring, introduction of processes in industry.

1 Introduction

Many systems are becoming more and more complex to design. In the automative industry, for instance, there is an increased incorporation of mechatronic systems. Many of these systems, such as the braking system, are safety-critical, and in the near future the steering system will also become mechatronic. The reason for this trend is that mechatronic systems can provide functionality that is hard to achieve, expensive to produce and difficult to package with traditional mechanical solutions [1]. The greater simplicity with which mechatronic solutions can incorporate functionality allows for more frequent innovations. Those innovations are new combinations of known sub-solutions in which the reliability of the complete mechatronic system is hard to test and the level of experience is low. Thus, to develop mechatronic systems the use of methods is essential [1]. The need to solve the trade-off between innovative combinations and reliability of the whole system is addressed in this paper. The research is concerned with design processes suitable for the development of such systems. The results can be applied to other applications where the trade-off between new combinations and reliability is also essential.

Today, there are various methods developed within the area of safety [2] to support development of safety-critical systems and products. These methods focus on safety aspects. However, it is also essential in developing complex safety critical systems to produce solutions with respect to diverse criteria. General design methods and design processes have been developed for this purpose within the engineering design field. Unfortunately the majority of them have not been successfully transferred into industry [3]. Most of the engineering design methods and almost all of the safety-related methods are developed and used as stand-alones. The results from methods used in earlier design phases are frequently forgotten and not used as inputs in later phases. Engineering practice is also characterised by the use of numerous methods in some design phases, but few, if any, in others [4].

The step-wise engineering design processes, e.g. [5], have failed to be implemented in industry because they are difficult to adapt to the industrial ways of working and to the different kinds of projects dealt with (i.e., different size, different level of novelty, different timing, different resources). Large companies, for instance, often divide their development into three phases: research, advanced engineering (AE) and product projects. The research organisation deals with new technology development. In AE new solutions for systems are developed up to the point that they become 'off-the-shelf' solutions, i.e., solutions that become part of a stock with known performance, that can be incorporated in complete product projects. In product projects a combination of 'off-the-shelf' solutions for the different systems of the product is selected to meet customer demands and detail adjustments are made to optimise the complete product performance. Since traditional engineering design processes do not fit into this way of working, companies tend to assign the task of defining their own processes to employees and consultants. However, companies demand verification of effectiveness of their processes. Many companies do not feel secure today if their processes are the most efficient for their organisation and if they can use them to ensure safety in design of safety-critical systems.

In this paper our aim is not to produce an ideal process, because it would not fit into every organisation. Instead, the aim is to understand the factors that make a design process suitable for development of safety-critical systems that are new combinations of 'off-the-shelf' solutions. The factors can be used by academia to evaluate new and existing processes and by industry to find weak areas in their design processes.

2 Method

The research method used in this work [6] is in four steps:

- 'Criteria'. Here the success criteria for the factors to be useful for evaluation of design processes are explored.
- 'Descriptive Study I'. In this step the advantages and limitations of four design processes are analysed.
- 'Prescriptive Study'. The factors that prohibit and that make a design process suitable for development of complex safety critical products are proposed.
- 'Descriptive Study II'. The proposed factors are evaluated with respect to initial criteria.

The research presented has been conducted by two academics located at Volvo Car Corporation (VCC). This situation has allowed the authors to gain insight into actual engineering practice, into the process of formal and informal decision-making [7], and into the engineers' working environment. Long-term co-operation between academic institutions and industry is essential in order to conduct the research presented. Without this approach the understanding of how design is practiced would not be reached [8]. Only with a clear understanding of today's engineering practice can we as researchers contribute to its improvement. As stated by Blessing, Chakrabarti and Wallace "*The aim of engineering design research is to support industry by developing knowledge, methods and tools which can improve the chances of producing a successful product*." [6]. The authors of this paper are involved in a long-term project with Volvo Car Corporation and have for the last three years been physically located in the chassis department for strategy and concept development.

3 Success criteria of evaluation factors

The following success criteria for the factors to be useful for the evaluation of design methods were obtained through brainstorming, in co-operation with the business strategy department at Volvo Cars :

- The factors should not prescribe specific solutions but should give insight into problems and advantages of characteristics of design processes.
- The factors should be understandable and measurable.
- The factors should consider industrial needs.

4 Descriptive study I: analysis of four design processes

In order to analyse the design processes that have been defined by academia and those that are used in industry, design methods are allocated to their different stages and the technique called Advantages-Limitations-Uniqueness-Opportunities for change (ALUO) is used. The objective is to study their usability as tools for design of safety-critical systems that are conceived as combinations of 'off-the-shelf' solutions.

Table 1. Methods allocated in the design processes

GENERAL METHODS		SAFETY-RELATED METHODS
DIVERGENT	CONVERGENT	
D1 Invitational stems	C1 Highlighting	S1 System Failure Mode Effect Analysis (FMEA)
D2 Ladder of abstraction	C2 Affinity diagram	S2 Component FMEA
D3 Reverse brainstorming	C3 Multi-fact picking up	S3 Assembly FMEA
D4 Concept fan	C4 Interrelationship digraph	S4 Simplified FMEA
D5 Personal analogy	C5 Card sort	S5 Failure Mode Effect and Criticality Analysis (FMECA)
D6 Word dance	C6 Interaction net	S6 Interfaced Focused FMEA
D7 Brainstorming	C7 Compatibility matrix	S7 Environmental FMEA
D8 Forced analogy	C8 Pugh method	S8 Failure Mode and Maintainability Analysis (FMMA)
D9 Morphological matrix	C9 Prioritisation matrix	S9 Functional Hazard Assessment (FHA)
D10 Visual connections	C10 Weighted objectives tree	S10 Functional failure Analysis (FFA)
D11 Gallery	C11 Product-market matrix	S11 Hazard and Operability (HAZOP)
D12 Direct analogy	C12 Screening method	S12 Event Tree Analysis (ETA)
D13 Attribute listing	C13 Interaction matrix	S13 Fault Tree Analysis (FTA)
D14 Classification schemas	C14 Quality Function Deployment	S14 Reliability Block Diagrams
D15 Objectives tree	C15 Axiomatic analysis	S15 Hierarchically Performed Hazard Origin and Propagation Studies, HIP-HOPS
D16 Function structure	C16 Quality Benchmarking Deployment	S16 Markov models
D17 Factorisation	C17 Assumption smashing	S17 Formal methods
D18 Particles method algorithm	C18 Analysis graph of ellipses	S18 Hybrid methods (HM)
D19 Brainwriting	C19 Cost-benefit analysis	S19 Checklist
D20 Design catalogues	C20 Rating & Weighting method	
D21 Forward steps	C21 Strength diagram	
D22 Lotus Blossom Technique	C22 Sensitivity analysis	
D23 Manipulative verbs list	C23 Value engineering	
D24 Fishbone chart	C24 Desirability function optimisation	
D25 PPCO	C25 Parameter profile matrix	
D26 Systematic doubting		
D27 Value engineering		
D28 Closed-world algorithm		

4.1 Design methods allocated in the different phases of the design processes

In order for the design processes to provide support in engineering practice, it is useful to specify the possible design methods that can be used in the different phases. It is also helpful for academia and industry as a way to detect possible gaps in design methodology, and to gain understanding about the information flow that can exist between methods. In this paper design methods are allocated in the different phases of the four design processes. The methods have been classified in two sub-groups: general methods and safety-related methods. In this way, the phases academia has concentrated on to solve the problem of developing safety-critical systems can be observed. The general methods are also sub-classified according to their divergent/convergent purpose. The safety methods are mainly of an analytical character. Their results can be used with either a divergent or a convergent purpose.

The methods used in this study are listed in Table 1. It is not feasible to include all existing methods in this paper due to the large number that exist; a representative spectrum of the most widely known has thus been used. A code has been assigned to each method. These codes can be found in the different phases of the four analysed design processes in Figures 1, 2, 3, and 4. The allocation of methods in the processes results in a "map" of design phases with methods that can be analysed to explore characteristics of the four processes.

4.2 Design processes selected for analysis

The design processes selected are briefly described in the following paragraphs. The Pahl and Beitz design process [5] is used as representative of the design processes generated within the field of engineering design (see Figure 1). It shows the importance of early identification of the specifications that a product should meet, and the need for considering diverse solutions at conceptual level before detail design is undertaken. It specifies both deliverables and tasks that have to be undertaken to achieve them. The version of Pahl and Beitz in Figure 1 is a simplified version of the one published in [5].

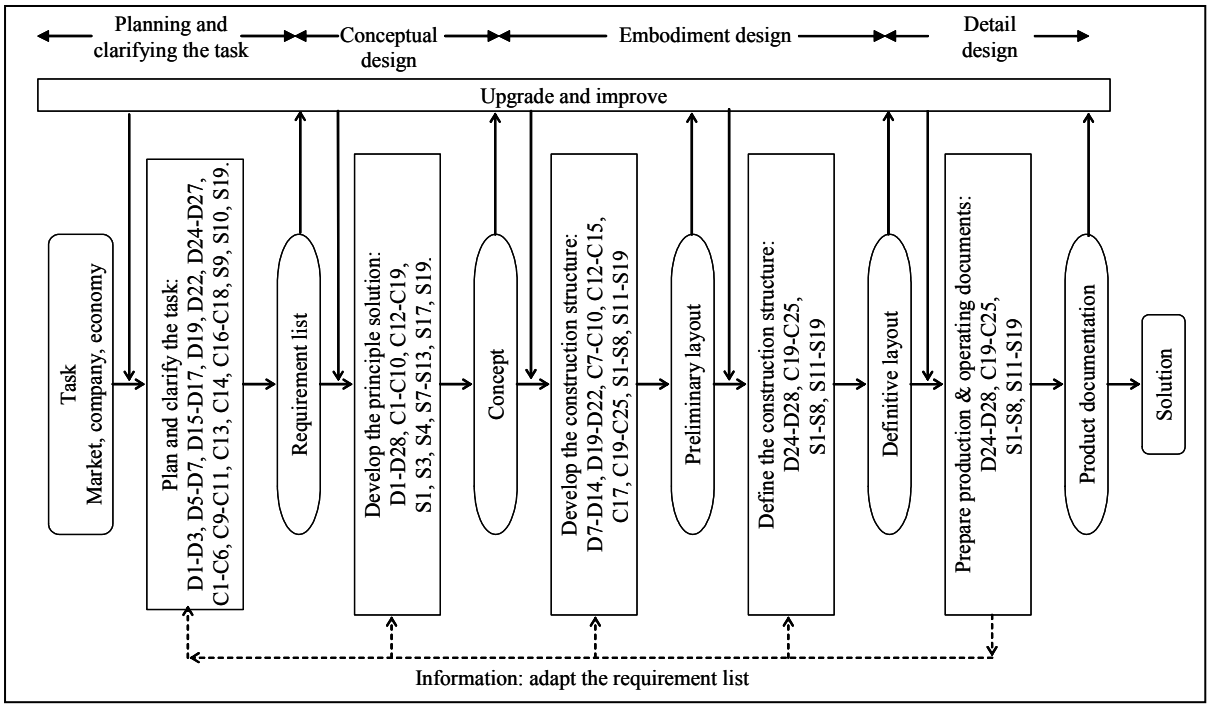

Figure 1. The engineering design process suggested in Pahl & Beitz

The Creative Problem Solving (CPS) process [9] has been developed within the field of creativity (see Figure 2). It is a helpful model that provides individuals from any discipline a flexible set of easy-to-use tools including divergent and convergent. It is flexible and adaptable because it does not aim to substitute any existing process, but to support the different activities that have to be undertaken to solve problems with methods.

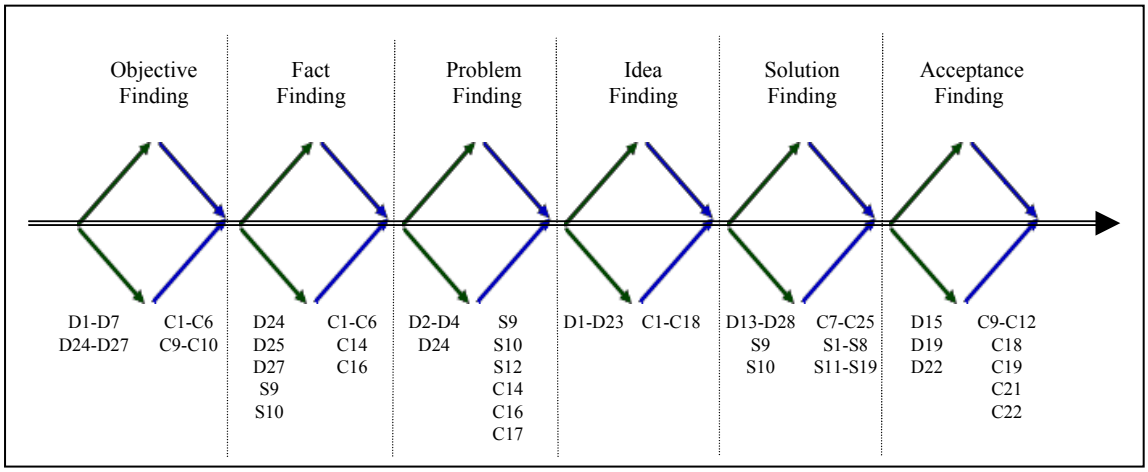

Figure 2. Osborne-Parnes Creative Problem Solving (CPS) process

The safety standard EUROCAE/SAE's design process [10] represents a design process that has been applied within the aerospace industry (see Figure 3). It emphasises safety analysis with the goal of achieving safety certification for the developed system or product. The five boxes to the right in Figure 3 represent the holistic design process, the other blocks are dedicated to and show the safety process. The process describes design tasks to be accomplished and does not specify exact methods.

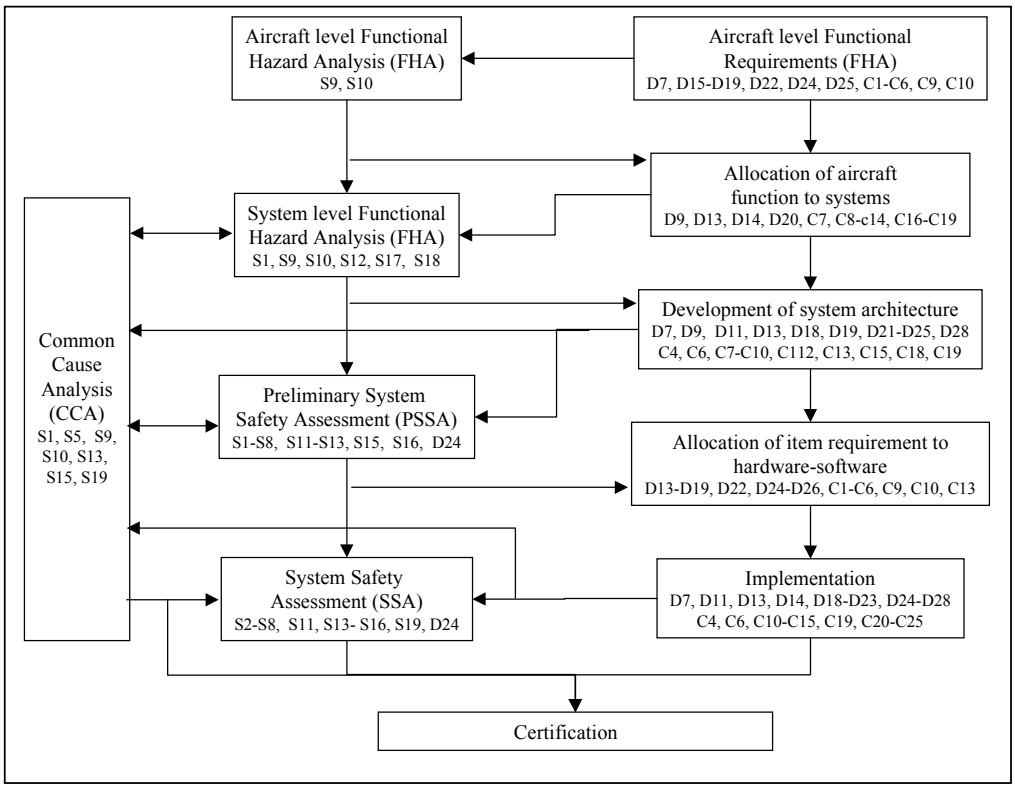

Figure 3. The design process suggested in the safety standard EUROCAE/SAE

The fourth model explored is a model in implementation at VCC for the development of active safety systems (see Figure 4). In contrast to the EUROCAE/SAE process, the VCC process is intended for development of products manufactured in high volumes, and is based on the V-model [11]. VCC divides its development into the three phases mentioned in the introduction: research, advanced engineering (AE) and product projects. The research phase is not included in the design process in Figure 4. The AE process plus the product project process are included in VCC's so called W-model. It specifies deliverables rather than tasks.

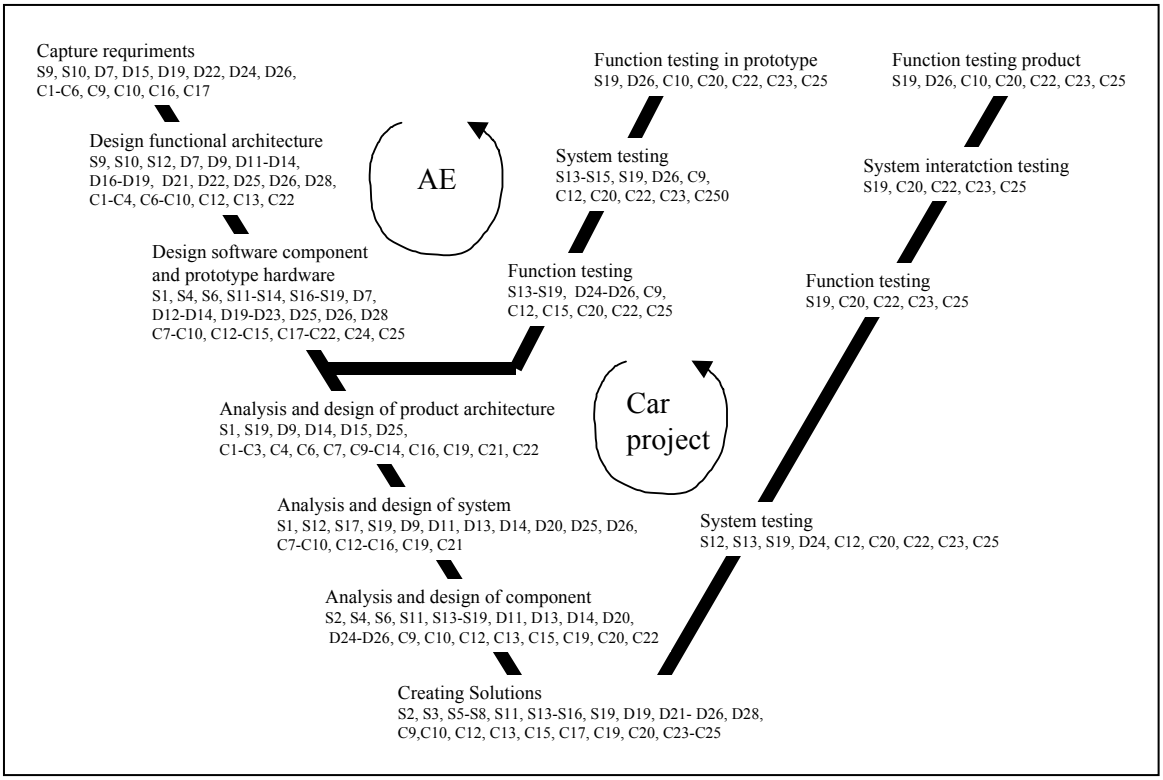

Figure 4. Design process for active safety systems at VCC

4.3 ALUO analysis of the design processes

An ALUO analysis of the different design processes is used to investigate the design's advantages, limitations and uniqueness. The ALUO analysis has not covered the 'Opportunities for change' because the aim is not to improve the processes explored but to identify factors of existing methods that make them suitable for safety-critical products. The result of the ALUO study is shown in Table 2.

W model	EUROCAE	CPS process	Pahl & Beitz	
See (A1), (A2) and (A6) A7 The distinction between AE and product project makes it suitable for both adaptive and innovative design.	See (A1) and (A2) A6 Its capacity to divide a complex project into smaller sub-projects makes it suitable for industrial application.	A4 Non prescriptive process that is adaptable to any situation. A5 Useful for searching for new solutions to problems.	A1 Clear and logical goals and tasks make it easy to understand. A2 Documentation milestones that constitute the outputs of a phase and the inputs of the next one allow for ensuring information flow and for tracing-back decision criteria. A3 Continuous upgrade & improvement is suggested.	ADVANTAGES
U6 The separation of AE and product project and the strong emphasis on verification makes it suitable for industrial application. U7 It is clear about when the verifications of the assumptions made during design can be made.	U5 Strong emphasis on safety	U3 It highlights the importance of undertaking separately the divergent and convergent activities. U4 Good support for the thinking process of problem resolution.	U1 It is very detailed with hints that can help beginners to know the elementary steps that product development should have. U2 Well accepted within academia.	UNIQUENESS
C9 Good for small innovations but not for completely new concepts. C10 A successful use of this process depends too much on the iteration process, which can be very costly. C11 The demands on compatibility between different AE are handled in the project phase, which can either make the product project too long or can restrict the innovation opportunity in the AE.	C7 The innovation phase is ignored. C8 It does not allow for iterations.	C4 Not suitable to handle a complete industrial project because it is too generic and not industrial-specific. C5 Hard to understand by engineers because it is abstract. C6 It depends too much on a small group undertaking the whole activity. This makes it unsuitable for industrial application.	C1 Unsuitable for re-design or adaptive design. This makes it unsuitable for industrial applications. C2 Very linear process that does not explain what activities can be done simultaneously. It does not facilitate task and time planning. C3 Inflexible about how things should be done because it specifies, precisely, the steps that must be followed to achieve the goals. Alternative, shorter ways are often required in industry.	CONCERNS

Table 2. ALUO analysis of four design processes

5 Prescriptive Study I: What makes a process suitable for developing combinations of off-the-shelf solutions that are safety-critical?

'Prescriptive Study I' aims to find the factors that help or hinder the effectiveness of a design process (process success – process cost) and ensure that the resulting product, a combination of 'off-the-shelf' solutions, performs well with respect to diverse criteria including safety. This is achieved with two different research activities:

- Discussion of the issue with engineers of the VCC Business Strategy department. Brainstorming and Highlighting were used in three sessions. The problem was stated as: "What are the factors that an ideal design process should meet to maximise the process profit (process success - process cost) and to ensure that the resulting product performs well with respect to diverse criteria including safety?" After a satisfactory number of factors was obtained, efforts were made to translate them into measurable factors.
- Factors were also obtained by querying why the four processes explored with the allocated method present the advantages, unique characteristics and limitations of Table 2.

Once the factors were obtained they were evaluated with respect to the initial criteria. This lead to improvement and re-statement of some of them. The factors to look for in the evaluation of new or existing design processes are:

- GOALS AND DOCUMENTATION TRANSPARENCY. Goals and documentation milestones should be expressed clearly and in a way easy for engineers to understand. This enhances proper flow of information and the possibility to trace back decision criteria. The goals should also be arranged in an order that has been proven to be valuable and that is able to provide a holistic view of the development process at the same time that it can inform about the reason for a task to be placed in relationship to other tasks.
- SUGGESTION OF ALTERNATIVE PROCEDURES AND METHODS. The methods and required steps to achieve the goals should not be presented in a prescriptive way. The reason for this is that engineers should have the possibility to adjust the amount of work to the type of project. However, alternative ways and methods (divergent and convergent) to achieve the goals should be suggested.
- REQUIREMENTS FOLLOW-UP. The process should include milestones to ensure that all relevant requirements (including safety) are considered at every stage, and that the project lead-time, risk and product cost are under control.
- REFLECTION OF COMPANY STRUCTURE. The design process should reflect the way the company is organised. For instance, if research, advanced engineering and product project are handled separately, the process should reflect the three sub-processes and their relation-ships. In industrial processes, the research process is commonly forgotten.
- REFLECTION OF PRODUCT ARCHITECTURE. Milestones for defining and verifying project architecture should be included in the design process. They should also have a logical order with respect to development and verification of individual systems. Product architecture milestones allow for project division into more manageable sub-projects and help in identifying the way iterations in design should take place. Iterations are necessary because changes in requirements always occur in an industrial environment. It has been observed that industrial processes always incorporate milestones for defining project architecture, whereas it is difficult to find this in academic processes.

- LEVEL OF NEWNESS OF A DESIGN PROCESS IN A COMPANY. Modification and improvement of design processes in industry should be made gradually. It is impossible to introduce totally new design processes because they imply an initial increase of workload and low efficiency, which industry cannot afford.

These criteria can be used to evaluate design processes with respect to their suitability for the development of safety-critical systems that are unique combinations of 'off-the-shelf' solutions.

6 Conclusions

Researchers developing methodology and processes within engineering design should direct their research towards improving existing industry processes rather than creating radical new ways. They should first gain insight into industrial processes and then study possible improvements. Completely new approaches are often impossible to introduce into industry and will lack features that current practices have gathered through long experience and development. It is, however, crucial to improve the current practice in order to reach more efficient development and to be able to introduce new technologies such as safety-critical mechatronic systems.

Cooperation between university and industry constitutes a promising framework to deal with industrial practice improvements and research results transfer. The cooperation framework used in this case consists of joint definition of research projects by university and industry representatives, developed by an academic seated in an actual industrial environment. Such cooperation can benefit industry as the common, impositional style of consultancy is substituted by a careful investigation of the required change and adaptation of the change to fit the specific needs of a company. It is also advantageous for academia because it provides the opportunity to do research in an awareness of industrial reality, that is tested in real settings, and that is easier to transfer into industry.

Ideal processes that fit into every organisation are difficult, if possible, to generate. In this paper, factors to consider during the creation or improvement of design processes have been suggested. The factors are intended specifically to fit design processes for safety-critical products that are developed by combining 'off-the-shelf' solutions. However, some of them can be applied for any type of product development.

Design processes should constitute tools to help company engineers understand the goals of projects without prescribing specific ways to achieve them. Instead of prescriptions, suggestions of alternative ways to reach the goals should be provided that allow engineers to adapt the solving strategy to the specific demands of the project.

The specification of milestones is critical, and provides potential to ensure that no information is "lost" in the design process. A process to design critical safety systems with an 'off-the-shelf' strategy should include clear holistic and safety milestones, and should reflect the way AE projects and product projects are managed.

Acknowledgements

We acknowledge the assistance of the Chassis and Business Strategy departments of Volvo Car Corporation. Gratefully acknowledged financial support has been provided by Volvo Car

Corporation, the Polhem laboratory at Luleå University of Technology, and the Foundation of Strategic Research through the ENDREA program.

References

[1] Grante C., "Design methods for complex automotive systems. An approach for balancing profit and safety", Licentiate thesis, University of Linköping, Sweden, 2002.

[2] Leveson N., "Safeware, System Safety and Computers", Addison Wesley, Reading, 2000.

[3] López-Mesa B., "Selection of Engineering Design Methods using Creative Problem Solving Principles", Licentiate thesis, Luleå University of Technology, Sweden, 2003.

[4] Bylund N., Grante C. and López-Mesa B., "Usability in industry of methods from design research" Abstract accepted for the Proceedings of ICED'03. Stockholm, 2003.

[5] Pahl G. and Beitz W., "Engineering Design. A systematic approach", Springer-Verlag, London, 1996.

[6] Blessing L., Chakrabarti A. and Wallace K., "Designers - the Key to Successful Development", Springer-Verlag, London, 1998.

[7] Bender B., Reinicke T., Wunsche T. and Blessing L., "Application of methods from social sciences in design engineering." Proceedings of DESIGN 2002, Vol. 1, Dubrovnik, 2002, pp.7-16.

[8] Cyert R.M. and Goodman P.S., "Creating Effective University-Industrial Alliances: An Organizational Learning Perspective", Organizational Dynamics, Spring 1997.

[9] Parnes S.J. editor, "Source book for creative problem-solving. A fifty digest of proven innovation processes", The Creative Education Foundation Press: Buffalo, NY, 1992.

[10] EUROCAE (European Organisation for Civil Aviation Equipment) ED-79/ARP-4754, "Certification considerations for highly-integrated or complex aircrafts", Safety Standard EUROCAE, Paris, 1996.

[11] MIL-STD-498, "Software Development and Documentation", Department of Defense, United States of America, 5 December 1994.

For further information, contact:

Belinda López-Mesa
Luleå University of Technology, Sweden
Address: Volvo Car Corporation PVÖS36, SE-40531 Göteborg, Sweden
Tel: +46 31 593183
E-mail: blopezme@volvocars.com
URL: http://www.cad.luth.se/people.asp?ID=44

Christian Grante
University of Linköping, Sweden
Address: Volvo Car Corporation PVÖS36, SE-40531 Göteborg, Sweden
Tel: +46 31 594853
E-mail: cgrante@volvocars.com