

F2008-SC-041

CONSIDERATION OF DESIGN METHODS APPLIED FOR REDUNDANT SAFETY-CRITICAL ELECTRONIC VEHICLE SYSTEMS

Fülep, Tímea

Department of Automobiles

Budapest University of Technology and Economics, Hungary

KEYWORDS – x-by-wire, redundancy, reliability analysis, failure mode, effect

ABSTRACT - The development of safety critical systems is mainly driven by that social demand, that the societies wants to see safer, more reliable vehicles on the roads, which can also handle more complex situations than the human driver can. Redundant electronic systems confront us with new challenges in reliability analysis like handling and defining their back-up levels using qualitative and quantitative approaches. Are these reliability analyses appropriate for redundant electronic systems, mostly for electronic brake systems in terms of determining their reliability? Results show that even handling only one failure at a time is legally prescribed, hidden failures or failure combinations can cause unintended effects in systems operation despite of redundancy. That is why qualitative reliability analysis and its structural appearance can be systematic input for the further needed quantitative reliability analysis.

INTRODUCTION

The importance of safety is increasing also in the automotive industries. This includes making driving and the components, their architecture safer. This latter, system safety, depends strongly on the failure probability of individual components and how the handles different faults, errors and failures (4). In wide interpretation, under the notion of dependability, system safety expresses operation without catastrophic events harming users and the environment (5), while reliability and availability presents the continuity in system readiness. Regarding reliability is more précised concerning its time dependence from which availability can be derived.

In today's automotive industry, companies are organized into simultaneous engineering teams to develop their new products. The new way of doing business enables some companies to develop their new products quicker, cheaper with higher quality and reliability. In the past few years there has been the tendency to increase the safety of vehicles by introducing intelligent assistance systems (e.g. ABS, Brake Assistant (BA), ESP, etc.) that help the driver to cope with critical driving situations. These functions are characterized by the active control of the driving dynamics by distributed assistance systems, which therefore need a reliable communication network.

The faults in the electronic components, which control these functions, are safety-critical. However, the assistance functions deliver only an add-on service in accordance with a fail-safe strategy for the electronic components. If there is any doubt about the correct behaviour of the assistance system, it will be switched off. For by-wire systems without a mechanical back-up a new dimension of safety requirements for automotive electronics is reached. After a fault the system has to be fail-operational until a safe state is reached (3).

AUTOMOTIVE ENGINEERING DEPENDABILITY

Currently, only limited statistics are available regarding accidents involving trucks and even less is known about the cause of these accidents. To fill in this lack of knowledge, the European Commission (EC) and the International Road Transport Union (IRU) launched a unique scientific study, the European Truck Accident Causation (ETAC) study (7). Knowing that there are many factors which contribute to an accident and knowing that those factors are interlinked, the aim of the study is to identify the main causes of accidents involving trucks. From a research point of view, the main cause is the cause which has made the greatest contribution to the fact that the accident happened (Figure 1).

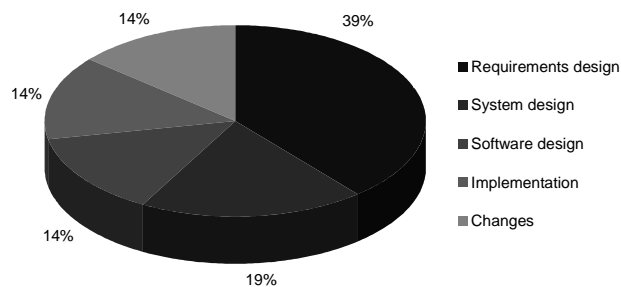


Figure 1. Main accident cause for all road users

In the architectures of currently designed vehicle systems will be included a significant percentage of electronics, communications and software in safety-critical systems, thus making these systems very complex (4, 6). Today 30% of the cost of a car is in electronics and 4 % of the production costs are Software. Until 2010 this will increase to 13% and 90% of all the new innovations will be based on electronic systems. Currently, the average number of micro-controllers per automobile vehicle is about 25 (4) and this number is expected to increase in the following decade. It has been estimated that the number of in-vehicle networks currently is about 5 and will reach 15 in the year 2015. System complexity raises also safety questions concerning their impact of the vehicle and its occupants. Safety-critical systems need to be carefully and properly designed (Figure 2) and certified by appropriate certification body.

For automotive, the certification standards most likely to be used will be similar to e.g. IEC 61508, which is a European generic safety standard for industrial systems. A UK consortium of automotive companies published the MISRA guidelines specifically for vehicle-based systems. MISRA is a consortium of UK motor manufacturers and electronics suppliers, which was responsible for the production, in 1994, of the 'Development guidelines for vehicle based software' (also known as the 'MISRA Guidelines').

These have received widespread use throughout the international automotive electronics industry. The MISRA Guidelines provide important advice to the automotive industry for the creation and application of safe, reliable software within vehicles. The Guidelines are intended to use by all those involved in the creation, procurement and support of vehicle based software. Users may be within vehicle design and manufacturing companies, component suppliers, development tool suppliers and diagnostic equipment suppliers. The Guidelines encapsulate many principles and concepts, such as:

- Safety, like justice and democracy, must be seen to be present.

- Software robustness, reliability and safety, like quality should be built rather than added on the requirements for human safety and security of property can be in conflict. Safety must take precedence.
- System design should consider both random and systematic faults.
- It is necessary to demonstrate robustness, not rely on the absence of failures.
- Safety considerations should apply across the design, manufacture, operation, servicing and disposal of products.

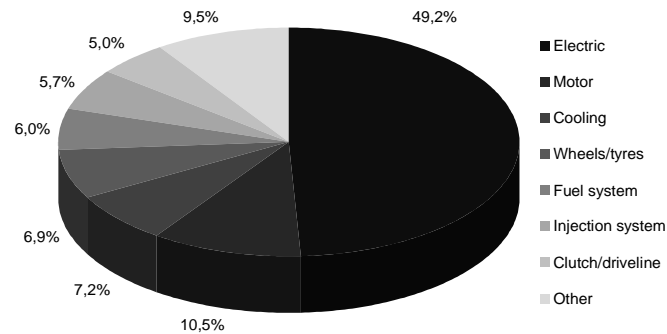


Figure 2. Main problems occurring in cars

To increase system reliability, the system designer may consider component redundancy because under certain conditions, it may be the quickest or the easiest solution or the solution with the least cost or the only solution. On the other hand, redundancy has the following disadvantages: it might be too expensive or it may exceed limitations on size, weight or power or it may require sensing and switching devices so complex as to offset the advantages. Component replication is often essential to achieve required levels of safety or reliability (8). However, the options for replication in a non-trivial design are typically too many to consider in detail, so designers often rely on experience and evaluation of a few different design options to arrive at decisions about the location and level of component redundancies.

Reliability design in the concept design phase is primarily oriented towards defining of reliability specification and selecting of the most acceptable solution from the point of view of reliability meeting requirements, which means that reliability of systems and their elements is analyzed. The process of system designing is started by translating the users' requirements and needs into the specification for designing, i.e. into the design assignment within creating of the pre-design. The concept design phase also defines the design goals from the point of view of meeting of the standards and regulations.

Conducting the analysis of failure mode and effects (FMEA) enables identifying of all potential and known modes of failure occurrences in system assemblies/parts, their causes, evaluation of consequences. Individual system elements can have several failure modes, since each stipulated function can have several failure modes. Failure modes are allocated, according to the required function, into three groups: complete function loss, partial function loss and wrong function, and this is important for conducting the analysis. For each failure mode, the possible effect (consequence) is analyzed at a higher level, i.e. at the whole system level.

It is stated that the mentioned method is appropriate mainly for non-redundant systems; however, analyses of partly redundant systems will be shown using this technique. This contradiction must be resolved by proper considerations, which are going to be presented. It should be noted that this systematic approach is only one possible solution and handles only

one failure at a time. Multiple failures can be handled by quantitative reliability analysis, which creates a fault model and contains the analysis of the model deductively. Fault trees provide a convenient symbolic representation of the combination of the events resulting in the occurrence of the top event and provide statement on the total failure risk.

It should be remarked that this analysis does not necessarily depend upon credible component failure rates to produce useful results. In the case of software modules or components with no sufficient history of use, such failure rates would be impossible or very difficult to obtain anyway. However, the logical reduction of fault trees into minimal cut-sets can still indicate single points of failure in the system and point out potential design weaknesses that may lead to useful design iterations.

Results show that even handling only one failure at a time is legally prescribed, hidden failures or failure combinations can cause unintended effects in systems operation despite of redundancy. That is why qualitative reliability analysis and its structural appearance can be systematic input for further needed quantitative reliability analysis.

SYSTEMATIC SET UP OF SYSTEM STRUCTURE AND FUNCTION

Before starting the FMEA it is worth deploying the related requirements to design specification level. For that purpose, several tools are available; one of them is the Matrix Analysis (MX FMEA) from Plato AG, which seems to be very powerful in safety-critical applications. The advantages of using matrix analysis over representing the system in a structure tree lie in the fact that the function, failure and system structures are set up almost simultaneously and that functional relationships are indicated within the matrix.

The system-level structure of each matrix is based on the answers to three questions:

- What is the system or product to be analyzed?
- What customer needs/expectations, regulatory requirements, standards, etc. are associated with such a system or product (functions and/or requirements)?
- What subsystems make up the system or product? And which functions correspond to these subsystems (directly or indirectly)?

The requirements that the relevant components must meet in order to fulfill a function are mapped at interfaces (Figure 3). An interface is both a means of separating system from design and a means of linking the two. Interfaces make it possible for the teams to work independently at different locations. Design and System FMEAs can run parallel to each other up to a certain stage of the development process and then the conception FMEA (how the whole complex system is influenced by each component) can be executed (1).

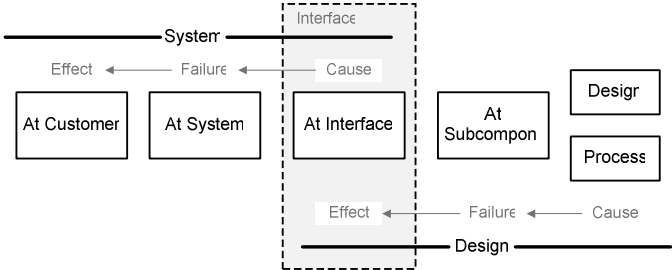
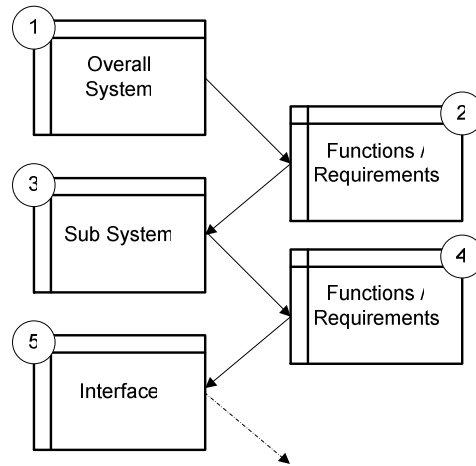


Figure 3. Representation of involved levels in System and Design FMEAs with defined interface

Question guideline concerning building up the matrix structure (Figure 4):

1. What is the overall system?

2. What do customers, laws, standards, etc. expect from such a system (functions/requirements)?
3. Of which sub systems the system should consist of? Which functions do they support?
4. Which functions should each sub system have? Which (external) functions/requirements do they support?
5. Of which interfaces each sub system should consist of? Which functions do they support?



1	2				
ABS System (Beispiel)	optimale Aktivierung des Rollwheels beim Bremsen	Fahrzeug Stabilität beim Bremsen erhöhen	Fahrzeug Lenkbarkeit beim Bremsen erhöhen	Traction beim Fahrzeug Beschleunigen erhöhen	Fahrzeugstabilität beim Fahren/ Bremsen/ Beschleunigen erhöhen
3	ABS [+]	x	x	x	
	ESP [+]		x	x	x
	ATC []			x	x
	BD				
	EBD				
		Fahrzeug Stabilität beim Bremsen erhöhen [ABS System (Beispiel)]	Fahrzeug Lenkbarkeit beim Bremsen erhöhen [ABS System (Beispiel)]	Fahrzeugstabilität beim Fahren/ Beschleunigen erhöhen [ABS System (Beispiel)]	Spurstabilität beim Fahren/ Bremsen/ Beschleunigen erhöhen [ABS System (Beispiel)]
	ESP		apply Brakepressure to specific wheels		apply Brakepressure to specific wheels
5	Drehzahlgeber []		x		x
					4

Figure 4. Matrix structure

Standard evaluation

Standard evaluation has its own rules how to apply. Evaluation begins after creating the FMEA form derived from the matrix. Two different aspects will be taken into account concerning the evaluation: whether the value refers to the failure effect or to the failure cause. The final value (RPN – Risk Priority Number) contains three factors:

- Severity (S), which always refers to the failure effect (FE)
- Occurrence (O) and Detection (D) for the failure cause (FC)

Multiplying these factors we get the RPN, which will be analyzed whether the corrective action is needed or not. The range for each value is 1 to 10 (including only integers).

Severity evaluation

The severity value is strictly not changeable not even in the optimization phase because the effect of the failure does not change during the analysis and this value refers only to the failure effect. It is classified once based on the evaluation catalogue to a specific value.

Occurrence evaluation

In case of occurrence evaluation if a preventive action can be implemented the originally determined value can be reduced the way as follows:

$O = O$ (FC)-P (evaluation of the preventive action - value of 'goodness')

These operations are applied during the automatic evaluation process.

Solving the optimization problem for the redundancy of the communication lines the following mathematical operation (1) was applied, which is analogue to the calculation of resistors connected in parallel:

$$O_2 = \frac{O_{1_preventive_action} \cdot O_{1_redundant_preventive_action}}{O_{1_preventive_action} + O_{1_redundant_preventive_action}} \quad (1)$$

Detection evaluation

In case of detection evaluation if a detective action can be implemented the originally determined value can be reduced the way as follows:

$D = 10 - C$ (evaluation of control action – value of 'goodness')

These operations are applied during the automatic evaluation process.

Since a better detectable (lower value) solution (2) provides the connection between the combination parts the basis for the detection value after optimization was its detection probability number.

$$D_2 = \min[D_{1_corrective_action}; D_{1_redundant_corrective_action}] \quad (2)$$

$RPN = S \cdot O \cdot D$. The RPN value was marked as critical at 100; corrective actions were carried out in all cases the value was above 100.

CONCLUSION

With improving or selecting suitable existing or even inventing new approaches the iterative steps of safety design can be reduced, which influences positively time and cost targets as well. The gist of conducting a qualitative reliability analysis is the good preparation for that, i.e. well-structured requirements/functions are presented from the top level until the analysis will be conducted and the same procedure for the system elements which are components of the required system.

REFERENCES

- (1) Dobry, A.: "Global denken, lokal handeln", Carl Hanser Verlag, München, Vol. 48, No. 11, pp. 1096-1097., 2003

- (2) Hedenetz, B., Schedl, A. V.: "Fault Injection and Fault Modeling for a Safety-critical Automotive Communication System", *Safety and Reliability*, Lydersen, Hansen & Sandtorv (eds), Balkema, Rotterdam, pp. 417-423., 1998
- (3) Pimentel, J. R.: "Verification, validation and certification issues of safety-critical communication systems", *Safety-critical automotive systems*, Ed. by J. R. Pimentel, Society of Automotive Engineers, Inc., pp. 3-12., 2006
- (4) Leveson, N. G.: *Safeware: "System safety and computers"*, Addison-Wesley, 1995.
- (5) Amberkar, S., D'Ambrosio, J. G., Murray, B.T., Wysocki, J., Czerny, B. J.: "A system-safety process for by-wire automotive systems", *Safety-critical automotive systems*, Ed. by J. R. Pimentel, Society of Automotive Engineers, Inc., pp. 13-18., 2006
- (6) "A Scientific Study 'ETAC' European Truck Accident Causation", *Executive Summary and Recommendations*, International Road Transport Union (IRU), 2007
- (7) Papadopoulos Y., Grante C., Wedlin J.: "Automating aspects of safety design in contemporary automotive system engineering", *FISITA Conference 2004*, Barcelona, Spain