Acta Univ. Sapientiae, Informatica **8,** 1 (2016) 82–95

DOI: 10.1515/ausi-2016-0005

Improving the effectiveness of FMEA analysis in automotive – a case study

Gábor VÁNYI
Eötvös Loránd University, Budapest
email: vanyig@ceasar.elte.hu

Abstract. Many industries, for example automotive, have well defined product development process definitions and risk evaluation methods. The FMEA (Failure Mode and Effects Analysis) is a first line risk analysis method in design, which has been implemented in development and production since decades. Although the first applications were focusing on mechanical and electrical design and functionalities, today, software components are implemented in many modern vehicle systems. However, standards or industry specific associations do not specify any "best practice" how to design the *interactions* of multiple entities in one model. This case study focuses on modelling interconnections and on the improvement of the FMEA modelling process in the automotive. Selecting and grouping software components for the analysis is discussed, but software architect design patterns are excluded from the study.

1 Introduction

Today, software working all over our vehicles, from sensors and cameras to navigation to infotainment systems to diagnostics. In 2001, cars had a minimal amount of code in them, nowadays, a new car has about 100 million lines of code. The increase of software parts reduces weight, involves cost optimization and decreases delivery time compared to similar complex mechanic

Computing Classification System 1998: G.2.2
Mathematics Subject Classification 2010: 46S99
Key words and phrases: FMEA, risk analysis, system modelling, automotive

or hardware changes in the development life-cycle. Complexity of hardware, software and mechanical systems exponentially increase with the possibility of harm and unwanted side effects. Hence, different standards implemented for reliability analysis and risk estimation.

The FMEA method was introduced in the automotive industry based on the results of the Apollo airspace program in 1970s [6]. It was the first time when this method could show opportunity to find possible failures in big and complex systems like a space shuttle. This method is widely used both in development and manufacturing. For the automotive industry the QS 9000 standard and the SAE J1739 defines the implementation. Effective analysis of software components remain a challenge, because it cannot be assessed like hardware. During the analysis a possible question can be: "what kind of harm can the development environment, programming language, compiler, coding method (pointer, timer or operator) cause?". If the functionality of software can be analysed by itself, it also generates questions like "what part of the code is a function?" and "what are the inputs and outputs of the given block?". And finally, "what kind of failures and causes can be considered during the analysis?". If a well-defined structure was used, then the effects of a failure can be traced back through the whole system. This streamlined approach can motivate technical risk analysis to handle each unwanted risk in full detail, hence project managers will see the quality and value together in their product.

2 FMEA overview

The following FMEA types are used in automotive: (1) system, (2) design and (3) process. These can be used in different logical levels. For example, system FMEA should be used for a subsystem, design FMEA for a simple screw, and process FMEA to evaluate risks in manufacturing. There is hierarchical relation between system, design and process FMEA (in this order). Two possible additional levels can be used to collect failure effects from the top level and one additional level on the lowest part (as cause level) which can be used as a failure cause catalogue.

The risk ranking is based on risk priority number (RPN), which can be calculated as the multiplication of parameters Severity (S), Occurrence (O) and Detection (D). The ranking process can be formal, since evaluating catalogues facilitates teams in finding the right risk evaluation values (see i.e. SAEJ1739, VDA, etc.). Moreover, proper structuring of technical systems and traceability of design changes is more challenging than risk evaluation. Former version of

VDA (released in 2009) required that every risk have to be mitigated, where RPN is larger than a certain threshold [9]. The newest version raises attention to S and O, thus, it defines a matrix of S and O for more detailed risk ranking. Many FMEA expert states that these matrices may not show the real practical risk. Multiplication of a high S value with a low O values means that very critical failure may not happen very often, but when it happens, it can cause high damage. Thus, some companies decided that they try to reduce their potential risks to as low levels as possible with different actions by tests, design changes or reviews together with their customers during development. A very important rule of thumb is to evaluate severity values on a highest level and inherit these to lower levels. This can ensure that a failure will have the same meaning of seriousness in the whole system and will be encountered and managed.

Beyond the effectiveness, sufficient level of technical content has significant differences from the quality point of view, because these depend on human factors. The electric, mechanic and electro-pneumatic systems have to be analysed by different methods of reliability and risk analysis in parallel. If these were coordinated as an unified systematic method, it would reduce capacity and time requirements. The FMEDA (Failure Mode and Effects and Diagnostic Analysis [8]) principles and purposes can be used in general FMEA as well. Many articles exist about software component analysis (see e.g. [4]), but these do not tend to explain how to connect software components with electrical hardware and mechanical interfaces.

3 Creating FMEAs

The “5 step method” is a well-known practice in the automotive industry. It has been introduced in the VDA standard [10][5]. This method prefers to start by creating hierarchical groups of system element networks, then connect functions to each system element, define the effects of failure operations, evaluate risks, and finally rank and mitigate risks. Although this method is well-known, the resource capacity is very high because of the high number of reviews for the newly developed product. Therefore ”best practices” and internal know-how have been used at many companies to quick start the process as a kind of template, but even in this case many redundant steps cannot be easily eliminated. Companies with many independent departments (or competent centres) usually use different strategies for system modelling and focuses different points of analysis. These methods generate latent quality gaps and

risks. Another problem comes, when different products or components connecting each other into one large system, thus FMEAs shall be connected as well. Fortunately, it is feasible to have a common consensus regarding which processes will be used on quality side. On engineering side, the modelling is supported by P-diagrams and boundary diagrams, which are introduced in QS 9000 standard [7]. Certain failures can be detected easier both by Fault Tree Analysis (FTA) or Functional Hazard Analysis (FHA) methods for the first step.

Hardware and mechanic elements can be analysed easier than software elements, because they can be bounded physically and standards support many methods for analysing. Software parts modelled mainly in Unified Modelling Language (UML) or flowcharts. Many tools support these forms but identifying safety gaps or risks are not so easy in safety critical or safety related modules and functions in the same way as estimating their effects in case of harms. Interfaces, built-in parameters and data layer functions can cause many exceptions if they have wrong values (programmed) or have been intentionally modified. Customers usually want to see identified risks under consideration, but it can be difficult to analyse and present thousands of combinations of values. An optimization strategy can be when software module analyses includes functional or logical grouped evaluation of interfaces. These cases are hard to find by tests of course, but FMEA should support identifying relevant requirements and functions which must be examined later.

A complex automotive system should be divided into hardware, software and mechanic components, since they cannot be analysed in the same time due to the different scheduling of development. The highest level is common, it is usually used for the effect level or system FMEA level. Using this common effect level has an advantage, since each severity number can be discussed with the customer, plus these failures can be guided easily through the system from top (requirement) down to an element (i.e. screw or software module). Later on, if an effect line of an identified risk was known, the failure network and function network would show these effect lines. If separated effect level was used only, it would cause quality gaps and shortcoming of risk evaluations on lower levels in the system.

System FMEA is the first point in the analysis where full risk evaluation is performed. There can be several system FMEA applied on the same level in parallel. This level lists the functions of the system. They are connected to one level higher to receive severity ranking for each failure as failure effect from the effect level.

One level below the design FMEAs can be found, where mechanical, elec-

trical elements and software components analysed in logical connection to the higher levels system FMEAs. This makes a logical network to overview which components participate in the given function. For example, the system level analysis may show an increasing pressure in chamber, the design level may connect a piston to a housing, etc., which are part of this function in the compressing air. If a system specialist was able to answer the question "what happens if this rod causes a failure?" then a failure network would help to see the points of possible failures and related functions up to the top-effect level. The last level is the process FMEA, which is used to evaluate the risk of components production.

Finally, the lowermost part is the cause level. It is not regularly used, but has many advantage if design or process failure causes are handled in a common failure catalogue.

3.1 Effect level

As it was discussed before, this is the top level in the FMEA, even if the three level rule is applied. Groups of the agreed first level requirements are listed in the function column. These are usually declarations of dimensions, some important internal requirements including internal lessons learned knowledge, specifications of standards, results of safety analysis (i.e. FHAs Top Effects) and regulations from relevant important laws. Possible failures and harms of requirement violation are evaluated in the next column. These are evaluated by system experts, safety professionals and the moderator. Usually ranked and evaluated the severity numbers together or at least reviewed with the customer who shall approve them. These targets of safety goals and functions shall be reached during the development. Safety is a killer criteria which shows how the unwanted actions are handled, since severity values cannot be lower than 9, but usually 10. Lower level (system) FMEA is connected to causes, these show the affected functions of each failure.

Functions	Potential failure	Ef-fect	S	Cause	O	P/D action	D
Braking	Speed is not reduced		10	ABS system			
Steering	Unintended maneuver		10	EPS system			
Comfort	Air conditioning fails		5	Cooling system			

Table 1: Effect level example

3.2 System FMEA levels

This is the first level where full risk analysis has to be performed. The risk assessment of system level shows weak points of system functionalities and helps to eliminate these gaps. This level usually has only one FMEA in case of less complicated systems with only a small number of functionalities and components. If the system has more advanced electronic, mechanical and software parts then various types of system FMEA have to be performed parallel in different content. This method will support sorting elements for a better system overview and handling scheduled delays according to different development life-cycles.

System level FMEA approach consists of two different contents. One of them focuses on components instead of functionalities, because production uses these information. Thus, the characteristics of strict suiting dimensions and material definitions have more value in labelling special characteristics (S/C or C/C) since these parts have more strict regulations for quality and product security. This approach should be applied for mechanical/pneumatic parts, in which case system level FMEA lists groups of mechanical functions (i.e. linkage group – containing functionalities for coupling two parts). One level below, the design FMEAs will list components which have different roles in this functionality. A component can be connected to more system FMEA if it is affected in that functionality.

Very significant difference from other mechanical FMEAs is declaring special characteristics on system levels. Because change of material, component or dimension will be traced easier on system level rather than design level, especially when design FMEA will be obsoleted or used in another production.

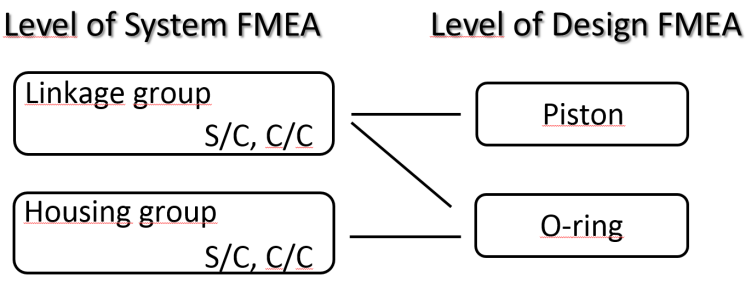

Figure 1: System FMEA connection to design FMEAs – mechanical and pneumatic components

The other approach is more beneficial for electronic and software components. This structure contains one system FMEA for electronic hardware and another one for software. If software components are too complicated then they should be divided into logical groups where each group has one common system FMEA.

One level below design FMEA is listed. Each component of an electronic circuit should be listed and connected to system level, showing which one participates in a given function. Usually short-cut, opening or missing component shall be examined. If these cases of failures examined, then they would have good input for FMEDA as well.

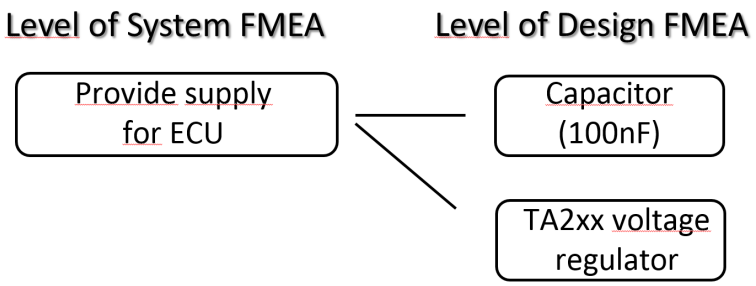

Figure 2: System FMEA connection to design FMEAs – electronic hardware

Software elements shall be analysed similarly, but the author experienced that three layers of software modelling will have more advantages. These free layers are (1) system level functions (high level functionality), (2) data transmission layer (communication arrays between modules) and (3) platform (low level functions, directly connected to hardware level). These are on the same level (design), but connected to each other via their interfaces.

Software modules are able to connect one element to more, thus the rule of the mechanic parts or hardware parts can be applied here. However, special characteristics (S/C, C/C) are not applicable because hardware components are examined for many times during the production (i.e. End–of–Line–Testing, testing each component at manufacturer, etc.), software parts are tested during development life-cycle and will have similar functionalities as have before in the production. Thus, final assembly test must validate that the assembled product is valid and working according to the specifications.

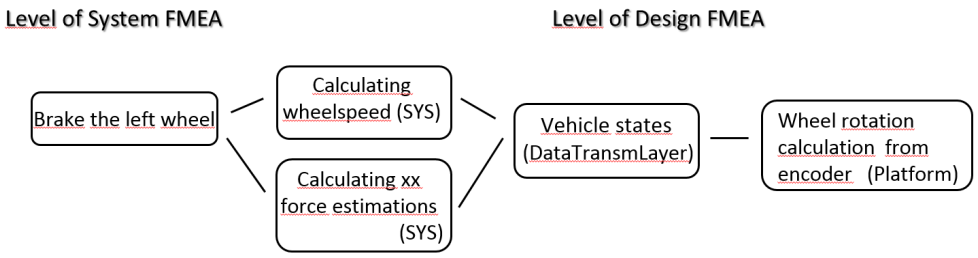

Figure 3: System FMEA connection to design FMEAs – software components

3.3 Design FMEA levels

This level is used for analysing disciplinary designs of hardware, mechanic, pneumatic or software components. Evaluation is made by technical experts, test engineers and an FMEA moderator. The notion "function" defines different meaning in each disciplines, but the top effect level can be similar. Full risk evaluation can be made on this levels as well.

In case of mechanical discipline for every element in the BOM (Bill of Material) a separate design FMEA have to be created. These elements related to the manufacturing process, thus data shall be assessable for production FMEA. Special characteristics such as S/C (Significant Characteristic) or C/C (Critical Characteristic) are identified for handling important dimensions or material definitions during manufacturing. The question is how special characteristics can be defined correctly, because there are no feedbacks from production of the given designs. A pre-defined a template with some technical points support this evaluation (see Table 2). The project team evaluates the template forms severity and occurrence values, then special characteristics are defined for the system level function, as it introduced earlier. This action makes easier to transfer the given function into the new product and supports to re-use them.

Hardware analysis is possible via the following the signal path from a single pin to the controllers software. It requires additional resources from software beside hardware developers. Analysis of electronic modules will have more advantage if FMEDCA (Failure Modes, Effects and Diagnostic Coverage Analysis) can be covered. PCB (Printed Circuit Board) contains many elements, hence these will make many extra work during the FMEA design process. Possible solution would be grouping them according to their functions, like power supply, etc. Short-cuts and cut in the circuit are usually analysed, failure cause

Function	Potential Failure
Ensure appropriate material properties	
	Wrong dilatation coefficient defined
	Wrong tribological properties defined
	Wrong E-modulis defined
	Wrong hardness defined
	Wrong braking strain defined
	Wrong Shore hardness defined
	Wrong glass transition temperature defined
	Wrong Poisson ratio defined
	Wrong Shear modulus defined
	Wrong property class defined
	Wrong compression set defined
	Wrong basic production technology defined
	Wrong Yield stress defined
Ensure appropriate geometrical properties	
	Wrong alignment relative to connecting components defined
	Wrong length relative to connecting components defined
	Wrong width relative to connecting components defined
	Wrong depth relative to connecting components defined
	Wrong thickness relative to connecting components defined
	Wrong diameter relative to connecting components defined
	Wrong greased area defined
	Wrong spring parameters defined
Ensure appropriate surface properties	
	Wrong surface coating defined
	Wrong roughness depth defined
	Wrong accuracy class for roughness
	Wrong surface treatment defined
	Wrong rill direction defined
	Wrong percentage contact area defined
Ensure appropriate connection of components	
	Wrong fastening element type selected
	Wrong numbers of fastening element defined
	Wrong fastening element distribution defined
	Wrong fastening torque defined
	Wrong fastening force defined
	Wrong fastening order defined
	Wrong connecting geometry defined

Table 2: Form sheet for mechanic design FMEA to support identification of special characteristics

catalogue on one level below supports finding design or other kind of possible failures.

Modelling the functionality of software modules is sometimes a kind of adventure. Teams usually facing with difficulties while performing analysis on pure software components, such as monitoring or continuously running routines. One of the lessons learned of FMEA moderation should be avoiding to create pure software FMEAs, because failure causes usually lead to the limits of programming language, edges of development environment or coding errors. Better if the analysis focuses on functionality of software modules. Requirements of the development level (RQ3 domain) are good starting points but calculations, actuations or any larger functionality should be considered. Causes of failures usually connected to other software modules, preventive actions usually refers violation of development processes or unintended failure of monitoring routines.

3.4 Cause levels

This is the bottom-most level of the FMEAs. The forms are not evaluated as design or system FMEAs, but they has been used for a kind of failure catalogue. Although, it also happens that this level is not used, but FMEA holds every necessary information and evaluation. We used this level to collect common disciplinary failures, like causes of design failures for evaluation support.

4 Increasing review efficiency

Motivating people to actively participate on FMEA review meetings is a big challenge. Finding the right information for FMEA and deciding if it is really the right one is also hard. The capacity usually limited and projects usually facing with time pressure, thus, FMEA meeting shall be optimized and speeded up to an efficient level. Minimal capacity of a meeting requires at least two experts of the given component for ensuring the right technical understanding and review each other. An FMEA moderator is usually necessary inviting test engineers for field experiences. Then, a thematic questionnaire and form sheets can support optimizing time and efficiency.

Typical questions are collected for thought-provoking here in order to support (i.e. software) FMEAs. General experience shows that developers are thinking usually in their modules inside, but has no idea what will they receive on input. Introducing or thinking over functionalities and newly devel-

oped or modified modules is a first step for placing this module in the system hierarchy. Then, the input and output of the given components can be examined, listening on keywords like "default value" and "NA" state. Afterwards questions can be stated about safe state if it is relevant or about scheduling operation. Thinking about these data the following questions will support you finding your own questions. Some examples were enumerated:

1. Assess the interfaces:
    - Which modules are using the output of this module and what are the input?
    - What are the default values, what happens if 0 or N/A occurs?
    - Is there any declaration for combination of value pairs on input or output?
    - Are there any configuration parameters which have been used for calculation?
2. Check the functionality of the module:
    - What kind of calculations have been made?
    - Is it possible that unintended overflow or underflow causing safety critical event?
    - Is it assured that unexpected values from other modules have been handled?
    - What thresholds have been examined or data comparison have been used?
    - What have been calculated and which functionality belongs to this calculation?
3. Safety of the module:
    - Are there any plausibility checks for calculated values?
    - Are there any check or monitoring for communication lines?
    - What kind of test or diagnostic function were implemented or used?
    - What is the scheduling period?

These questions have another benefits. If somebody has been interviewed about the development and requirement this person has to think what have been done and why? The final result of this thinking is also booked in the FMEA and assured that the right person has done the right development (other experts support this walk-through as well).

5 Conclusion

Risk evaluation of the designed functions has an increasing importance in automotive. Appropriate structuring brings better understanding of system functionality, and risk evaluation gives more precise feedback for developers. Re-using of earlier developed components can be supported by grouping the appropriate elements. The very first feedback shows that the production could connect their process FMEAs to design FMEAs easier due to the fact that functional grouping helps in understanding the component identification. Surveying other solutions, many articles just focus on the right risk evaluation [2] [3] using e.g. fuzzy logic in order to support risk ranking and the evaluation mechanism.

The presented system modelling method, particularly in software structuring and mechanical design grouping, will support the daily work better. Software FMEAs usually focus on evaluation of variables and equipment analysis [1]. This case study focused on structuring software and examined the interconnections among these structured levels instead. The usage of form sheets in mechanical design FMEA may reduce capacity demand due to answering similar questions at each component part. Experiences show that the cumulative meeting time frame of software FMEAs with questionnaires have been reduced from two months to two weeks, using a twice-per-week scheduling. On the other hand, the questionnaire supported the functionality review for developers and testers focusing on communication failures between modules and result of a calculation, scheduling interactions, safe states, etc. It is part of the software review at module test level of course, but not only one module have been inspected in this case. Re-using of former FMEA contents become easier in the newer generations and variants if unified structure and content were chosen.

Form sheets in design FMEA change the mindset for mechanical designers because they have to focus more on design points instead of ranking the levels of solutions. Hence, there is no need waiting for the feedback from production failures. Evaluating the right characteristics in the beginning shall be paid attention since it has influence on the cost of the product.

Designing mechanical connections is a baseline for production since processes are connected to design's result. Then, production is able to connect their FMEAs easier while they are able to identify the sources of special characteristics, such as material, mechanical connection, edges of the components connection, etc. Later, these technical information will support investigations in product modifications.

Motivating participants for an FMEA meeting is not an easy task under the pressure of deadlines. Making the evaluation time shorter and asking the right questions in right time definitely is a dream. If quality and daily practice meet in a well organized process and modelling method set then it can realize better quality and less postpones of production start and product recalls.

The reader shall decide how will implement these ideas in his or her FMEAs. Author just demonstrated a case study without any responsibility of insufficient use of these points.

6 Acknowledgements

I should like to thank János György and Sándor Drienyovszky for their ideas and experiences together with the result formed the concept of mechanical design FMEA part. I thank the referee for providing constructive comments and help in improving the contents of this paper. Finally, I should like to thank to my supervisor, Attila Kovács for his suggestions preparing this article.

References

[1] J. H. Craig, A software reliability methodology using software sneak analysis, SW FMEA and the integrated system analysis approach , in: *Reliability and Maintainability Symposium, 2003. Annual*, IEEE, 2003, pp. 12–18. ⇒93

[2] L. Pokorádi, T. Fülep, Reliability in automotive engineering by fuzzy rule-based FMEA, in: *Proceedings of the FISITA 2012 World Automotive Congress,* Volume 197 of the series Lecture Notes in Electrical Engineering, Springer Berlin Heidelberg, 2012, pp. 793–800. ⇒93

[3] L. Pokorádi, B. Szamosi, Fuzzy Failure Modes and Effects Analysis with Summarized Center of Gravity DeFuzzification, in: *16th IEEE International Symposium on Computational Intelligence and Informatics,* CINTI 2015 , IEEE, 2015, pp. 147–150. ⇒93

[4] K. H. Pries, Failure mode & effect analysis in software development, in: *Automotive Electronics Reliability,* edited by Ronald K. Jurgen, SAE International, PT-82, 1998, pp. 351–360. ⇒84

[5] P- Urban, DFMEA acc. to VDA - 5 steps approach, *OALC Reliability Blog.* 2011, http://www.opsalacarte.com. ⇒84

[6] Society for Automotive Engineers, Design Analysis Procedure For Failure Modes, Effects and Criticality Analysis (FMECA) 1967. ARP926. ⇒83

[7] Quality System 9000 Handbook, *Volume FMEA handbook* 2006. ⇒85

[8] TüV NORD, *Failure Modes Effects and Diagnostic Analysis* (2013), http://www.tuev-nord.de/. ⇒84

[9] Verband der Automobilindustrie, Qualitätsmanagement in der Automobilindustrie, Sicherung der Qalität vor Serieneinsatz, System FMEA *VDA QMC* 4 (2006) 124–139. ⇒84

[10] Verband der Automobilindustrie, Qualitätsmanagement in der Automobilindustrie, Produkt- und Prozess-FMEA, *VDA QMC* 4 (2006) 30–63. ⇒84

Received: March 4, 2016 • Revised: April 18, 2016