Automotive Functional Safety and Robustness - Never the Twain or Hand in Glove?

Roger Rivett, Ibrahim Habli, Tim Kelly

Automotive Functional Safety and Robustness

Never the Twain or Hand in Glove?

Roger Rivett[†‡], Ibrahim Habli[†], Tim Kelly[†],
University of York[†]
Jaguar Land Rover[‡]

***Abstract*—The FMEA/FMECA analysis technique has been used for over 30 years in the automotive industry in the context of product quality and robustness. More recently the discipline of functional safety has been adopted by the industry for analysing software-based control systems. Both of these approaches seek to predict undesirable outcomes that may occur and then take steps to avoid them. Despite these similarities, and their joint use within the industry, the quality and robustness process and the functional safety process have very little alignment in terms of risk assessment and mitigation. This paper makes the case for a better alignment and proposes a means of achieving it.**

Keywords—quality engineering, FMEA/FMEA, robustness, failure mode avoidance, risk, functional safety, safety case.

I. INTRODUCTION

Man-made machines suffer from malfunctions. Malfunctions are undesirable for end users for many reasons, e.g. loss of service, inconvenience or injury. Malfunctions are undesirable for the manufacturer as they may lead to damaged reputation, loss of sales and court cases. As a response to the potential negative consequences of malfunctions, manufacturers have developed an approach to anticipating and preventing malfunctions under the general heading of *Quality Engineering*. *Quality Engineering* can refer to a set of techniques, but it can also be used to refer to a whole quality management framework such as Six Sigma or Total Quality Management (TQM) [15]. Failure Mode Effects Analysis (FMEA) / Failure Mode Effects Criticality Analysis (FMECA) is a quality technique that is included in these quality management frameworks, but is also sometimes used to refer to a whole quality management framework. This is often the case in the automotive industry. In mechanical systems where the functionality is constrained by the continuous nature of physical properties and there are only a few modes of operation it has generally been the case that quality techniques have been sufficient to also address the safety issues. This is in stark contrast to the software aspects of of software-based control where there are typically many modes of operation and the control algorithm is not constrained by physical properties.

With the growing use of software based control systems the inadequacy of relying upon a reliability-oriented approach has become apparent. This has led to the development of new disciplines such as functional safety, promoting new safety management frameworks and standards such as IEC 61508 [1] and ISO 26262, [2]. In these standards FMEA/FMECA is referenced as one of the many possible analysis techniques.

The motivation for this paper is borne primarily out of experience, justifying the safety of systems comprising both mechanical and software-based systems. We provide a brief history of the development of the FMEA/FMECA technique, its use in the automotive industry and the recent trend towards its use for failure mode avoidance in a quality and robustness engineering context (Section II). We then describe the process implied by the automotive functional safety standard ISO 262626 (Section III). In section IV the functional safety and FMEA/FMECA processes are compared and a case for the alignment of the two is made. Section IV concludes with a proposal for how this alignment may be realised.

II. FAILUDRE MODE AVOIDANCE

A. Early use of FMEA

The first standard for FMEA was issued in 1949 by the US Armed Forces, [3]. The Ford Motor Company started to use FMEA in the late 1970s, [4], as did many other automotive companies. In 1994, SAE published J1739, [5], which was jointly developed by Chrysler Corporation, Ford Motor Company and General Motors Corporation. The use of J1739 was required by QS9000, which until 2006, was widely used as the automotive version of ISO 9000. QS9000 has now been replaced by ISO/TS 16949, [6], which also requires the use of J1739.

B. FMEA Process Steps

All of the FMEA standards mentioned in section A describe the process in a number of steps. The steps are largely the same but differ to some extent in wording or order. For the sake of comparison the following generic set of process steps is defined, Fig. 1.

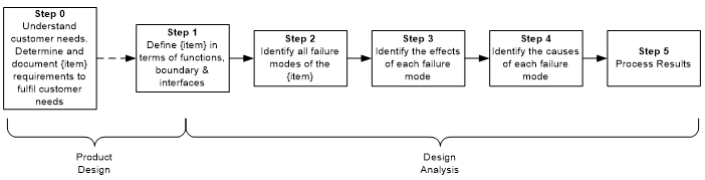

Fig. 1. Generic FMEA/FMECA Process

FMEA/FMECA-Step 0 is intended to represent the first task of product creation. It corresponds to the *Voice of the customer* level of abstraction and is only relevant if the FMEA is performed at the concept level.

FMEA/FMECA-Step 1 defines the object of the analysis. This definition will differ depending on the level of abstraction at which the analysis is being performed. If performed at the Concept level, then the FMEA is often referred to as a Concept FMEA. If it is performed at any of the lower levels then it is referred to as a Design FMEA (DFMEA). The material used in this step is intended to be produced as part of the regular product design work and collated in FMEA/FMECA-Step 1 as a reference for the analysis. When performed at the Concept level this step will help ensure that the concept is properly documented. The remaining steps are discussed below. The main variations arise in how FMEA/FMECA-Step 5 is performed. This is discussed in the next section.

C. Processing Failure Modes, Affects and Causes

In the 1980 version of Mil 1629, [7], FMEA/FMECA-Steps 1 to 4 are part of Task 101 and FMEA/FMECA-Step 5 is Task 102. Task 101 is referred to as an FMEA and its purpose is "*to study the results or effects of item failure on system operation and, to classify each potential failure according to its severity*". Task 102 is referred to as Criticality Analysis and its purpose is "*to rank each potential failure mode identified in the FMEA Task, according to the combined influence of severity classification and its probability of occurrence based upon the best available data*". Criticality Analysis has two methods: qualitative and quantitative. The significance of the failure mode, referred to in this paper by the generic term, consequence ranking, and in Mil 1629 as the Criticality Number, is arrived at by taking account of the severity of the outcome and the probability of the occurrence of the failure mode. The quantitative method uses failures rates and follows a reliability engineering approach. After determining the Criticality Number, Mil 1629 requires the identification of means to eliminate the failure or control the risk, e.g. failure detection methods and compensating provisions, corrective design, redundant items, safety devices, backup systems and logistics support.

J1739 takes the conventional approach of estimating the potential severity, S, of the outcome and the likelihood that the outcome will occur. However, the likelihood is split into two aspects:

- The likelihood that the failure mode that leads to the undesired outcome will occur, O; and
- The likelihood that the failure mode will be detected before the undesired outcome occurs and hence the undesired outcome will be prevented from occurring, D.

To capture the assessed value of each of the three aspects, three scales are defined taking values in the range of 1-10. These scales are a ranking based on an informal description which captures the intuition of greater severity and higher probability. The scales represent a relative ranking within the scope of the individual FMEA. The overall consequence ranking can be arrived at in a number of different ways. A classification may be assigned based on the values of Severity, Severity & Occurrence or Severity & Detection. Alternatively, or as well as, the 3 values are multiplied together to produce a Risk Priority Number (RPN). This approach has been criticised on the basis that the scales are ordinal and that an interval scale is required in order for the multiplication operation to be valid [8].

For countermeasures, J1739 calls for the use of prevention and detection controls that are used in the same or similar designs. Prevention controls describe how a cause, failure mode or effect is prevented, e.g. published design standard, design redundancy, corporate best practice standard design, system detection and driver notification for service and system detection and operational status displayed to driver. Detection controls describe how a cause and/or failure mode is detected before the item is released to production, e.g. Computer-Aided Engineering analytics, tolerance stack analysis and validation testing (fatigue, water intrusion, vibration, ride and handling, etc.). Finally actions may be recommended to reduce the likelihood of failure and/or improving the ability to detect failures, e.g. revised design geometry and/or tolerances, revised material specification, design of experiments, revised test plan and confirmation/verification of information.

D. Criticisms of a Reliability Approach

In striving for better performance of the FMECA/quality approach one could try to move more to the reliability approach, i.e. use component failure rates, notionally making more use of real world data and less use of judgement. However, there is large uncertainty concerning the nature of the environment in which the product will be used. Brown, [9], highlights the problem of knowing the stated conditions and specified period of time which would have to take into account the field usage, speeds, loads, duty-cycle of loads, temperature dynamics, humidity, corrosive environments and shock loads. Davis [10] highlights the lack of closed-loop feedback from units in the field when data outside the warranty period is not collected.

E. Alternative Approaches

Given the criticisms noted above, there has been a move away from reliability to an approach known variously as *Robustness Engineering* and *Failure Mode Avoidance (FMA).*

FMA has its roots in the work of Taguchi, [11]. Taguchi defines robustness as the "*state where the technology, product, or process performance is minimally sensitive to factors causing variability (either in the manufacturing or user's environment) and aging at the lowest unit manufacturing cost*". Robustness recognizes 2 types of quality: customer quality, i.e. features the customer wants, and engineered quality, i.e. features the customer does not want. Robustness is about engineered quality, i.e. removing the features that the customer does not want such as failures, noise, vibrations, unwanted phenomena and pollution. It does this by identifying the "ideal function" and then selectively choosing the best nominal values of design parameters that optimise performance reliability at lowest cost. The classical metrics for quality/robustness, e.g. failure rate, are considered to come too late in the product development. The Taguchi measure for robustness is signal-to-noise ratio. The signal-to-noise ratio measures the quality of energy transformation as expressed by *Level of performance of desired function / variability of desired function*. The signal-to-noise ratio is increased by reducing variability and specifying nominal values of the design parameters such that the design is

insensitive to noise factors, e.g. the customer environment, aging and wearing and manufacturing variations. In reducing variability in this way the Robustness approach has some similarities with the Six Sigma approach.

Clausing [12] has suggested a new definition for reliability, "*reliability is failure mode avoidance*", with failure being any customer perceived deviation from the ideal condition. As reliability is being equated to failure mode avoidance it is necessary to a have a way of measuring it. Clausing proposes the "operating window", (OW) as a metric for robustness. The OW is the range in some input noise that produces a fixed failure rate in the failure modes.

Davis [10] accepts Clausing's view of reliability as failure mode avoidance and proposes a robustness metric called the "*distance from the failure mode*". The distance is captured as measurements of physical properties in SI units, the greater the distance the higher the reliability.

III. Functional Safety / ISO 26262

The main automotive standard for functional safety is currently ISO 26262 [2]. This standard defines a process for functional safety engineering and management. A simplified description of this process is shown in Fig. 2. The process description is shown in a similar manner to that of the FMEA/FMECA process for ease of comparison.

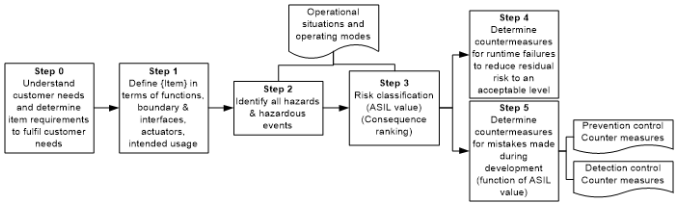

Fig. 2. Simplified ISO 26262 Process

ISO-26262-Step 0 is very similar to FMEA/FMECA-step 0 at the concept level.

ISO-26262-Step 1, referred to as the Item Definition in ISO 26262, is always defined at the vehicle level and includes some specification of the actuation, and so is similar, but not identical, to FMEA/FMECA-step 1 for a concept FMEA.

ISO-26262-Step 2 is performed using an inductive method of analysis on the Item Definition and does not assume an implementation except for some specification of the actuation. The purpose is to determine what vehicle level behaviour, if any, related to the item under consideration can initiate a sequence of events that results in harm to people. The analysis considers all the vehicle lifecycle phase, e.g. manufacturing, normal usage, servicing/repair, emergency services rescue and vehicle disposal. For normal usage the analysis considers the operational situations and operating modes, which may include current vehicle state and manoeuvre, the user state, the vehicle surroundings and external environment.

ISO-26262-Step 3 is equivalent to the consequence ranking. It considers the severity of the injuries that may be incurred; the qualitative probability that the vehicle may be in the lifecycle phase and operational situations and operating modes when vehicle level behaviour occurs (exposure); the qualitative probability that the persons at risk can avoid the harm by their own actions (controllability). This produces a value on the scale QM, ASILA, ASILB, ASILC and ASILD, where QM stands for Quality Management and ASIL stands for Automotive Safety Integrity Level. Unlike the FMEA/FMECA scales, this scale is defined industry-wide and applies to every automotive electrical and/or electronic (E/E) system.

ISO-26262-Step 4 produces a hierarchy of safety requirements from initial high-level safety goals, through implementation-independent design (functional) safety requirements, down to technical hardware and software safety requirements.

ISO-26262-Step 5 is comparable to the use of prevention and detection controls in the FMEA/FMECA process. Guidance on these as a function of ASIL value forms a large part of the standard. ISO 26262 has more steps than given here, including verification and validation but these are outside the scope of this paper.

ISO 26262 recognises FMEA/FMECA as an inductive analysis method [ISO 26262-9:2011, Clause 8] and the use of inductive analysis is specifically required at the system, hardware and software levels.

These analyses do not use FMEA/FMECA-step-5. The criticality analysis is not used as this comes from the risk assessment in ISO26262-step-3. For the prevention controls, error detection and reaction are a part of the ISO 26262 safety requirements process. For detection controls, design practice, further analysis and testing are part of the ISO 26262 process measures as shown in ISO26262-step-5.

ISO 26262 also acknowledges that FMEA/FMECA may play a part in hazard identification, safety requirements determination and safety validation. It is also used for assessing random hardware failures.

IV. Alignment of Functional Safety & Robustness

For a defined vehicle level E/E feature/system, following ISO 26262 will result in the following:

- a set of risk assessed hazardous events;
- safety requirements at different levels of abstraction from system to hardware and software intended to mitigate the risk associated with the hazardous events;
- verification evidence that safety requirements implemented and achieve risk mitigation; and
- evidence of having used appropriate processes, based on risk, for deriving, implementing and verifying the safety requirements

Having produced the above, it is possible to present an argument that the safety issues related to the E/E feature/system will not occur in service [13] [14]. By meeting the requirements of ISO 26262, this argument can be presented with a level of confidence that is commensurate with the risk associated with the safety issues. The formal requirement in ISO 26262 is for the creation of a safety case. This is defined

as an "*argument that the safety requirements for an item are complete and satisfied by evidence compiled from work products of the safety activities during development*". Whether or not the level of confidence at the time of product release was justified or misplaced can only be determined once the product has been in service for its design lifetime.

For a defined mechanical component/system, if the FMEA/FMECA is followed, then, the result will be a set of failure modes, set of causes, set of effects and a set of countermeasures for each cause.

The quality issues may include issues that functional safety would consider to be hazards. Having produced the above, it would be possible to present an argument that the quality issues related to mechanical component/system will not occur in the field. At present this is not done as it is not called for by any standard. This also means that there are no criteria concerning the level of confidence it is necessary to achieve.

Many, if not most, of the E/E control systems have an associated mechanical component/system. If a user is injured by the product when it is in service, it could be due to a failure of the mechanical component/system part *or* the E/E /system part. The distinction between the two is irrelevant from the perspective of the user who will only focus on the injury and not the cause of the injury. There is an obvious question of whether the level of confidence achieved by following the functional safety process is commensurate with the level of confidence achieved by following the robustness approach. Intuitively one would expect them to be commensurate if the risk was the same. At present it is not possible to answer this question. The task is made more difficult as the two use different approaches to consequence ranking and one is target-oriented and the other is achievement-oriented.

A. Way Forward

One means of aligning the functional safety process with the quality and robustness process is to extend the safety case required by the functional safety process, perhaps using the generic term 'assurance case', so as to include the argumentation and evidence emerging from the robustness process. ISO 26262 notes that the safety case could be extended to cover issues beyond the scope of the standard.

A prerequisite is to find a way of aligning the consequence ranking of FMEA/FMECA with that of ISO 26262. This task should be made easier as the quality process adopts a more failure mode avoidance approach. It will also be necessary to have a good knowledge of the current FMEA/FMECA practice and the underlying rationale by which the work is judged to be sufficient. This underlying rationale can then be captured in the argument of the extended safety case.

In addition to an argument that covers both the E/E system and mechanical components there are many potential benefits of aligning the functional safety process and the robustness process. An alignment at the processes level could improve the efficiency of functional safety and quality processes by reducing duplication of effort, or through producing work products that can be used by both disciplines. Alignment could bring greater consistency in the engineering effort expended in handling safety issues that arise from the failure of E/E systems or from failure of mechanical components. Alignment could also lead to improved ability to assess confidence in the results of the quality process. Finally, it may provide a more transparent and rational way of assessing the quality of the FMEA based on the reasoning and evidence that it produces.

REFERENCES

[1] IEC, "61508-3: Functional safety of electrical/electronic/programmable electronic safety-related systems. Software requirements,", 1998.

[2] ISO, "ISO 26262 Road Vehicles -- Functional Safety," ed, 2011.

[3] U. S. D. o. Defense, "MIL–P–1629 : Procedures for Performing a Failure Mode, Effects and Criticality Analysis," ed, 1949.

[4] F. M. Company, "Instruction Manual Process FMEA," ed, 1988.

[5] S. o. A. Engineers, "SAE Reference Manual J1739, Potential Failure Mode and Effects Analysis in Design and Manufacturing," 1994.

[6] ISO, "TS 16949 Quality management systems. Particular requirements for the application of ISO 9001:2008 for automotive production and relevant service part organizations," ed, 2009.

[7] U. S. D. o. Defense, "Military Standard Procedures for Performing a Failure Mode, Effects and Criticality Ananlysis AMSC N3074 MIL-STD-1629A," ed, 1980.

[8] W. Gilchrist, "Modelling Failure Modes and Effects Analysis," *International Journal of Quality & Reliability Management*, vol. 10, 1993.

[9] S. Brown, "Probabilistic Reliability vs. Failure Mode Avoidance Methodologies Within the Automotive Industry," presented at the 2004 SAE World Congress, Detroit, US, 2004.

[10] T. P. Davis, "Science, engineering, and statistics," *Appl. Stochastic Models Bus. Ind.*, 2006.

[11] G. Taguchi, S. Chowdhury, and S. Taguchi, *Robust Engineering*: McGraw Hill, 2000.

[12] D. P. Clausing, "Operating Window: An Engineering Measure for Robustness," *Technometrics*, vol. 46, 2004.

[13] J. Birch, R. Rivett, I. Habli, B. Bradshaw, J. Botham, D. Higham, P. Jesty, H. Monkhouse, R. Palin, "Safety Cases and their Role in ISO 26262 Functional Safety Assessment", SAFECOMP 2013, France, September 2013.

[14] J. Birch, R. Rivett, I. Habli, B. Bradshaw, J. Botham, D. Higham, H. Monkhouse, R. Palin, "A Layered Model for Structuring Automotive Safety Arguments", EDCC 2014, UK, May 2014.

[15] A. V. Feigenbaum: *Total quality management*. John Wiley & Sons, Inc., 2002.