FUNCTIONAL, THERMAL AND EMC ANALYSIS FOR A SAFETY CRITICAL ANALOGUE DESIGN APPLIED TO A TRANSPORTATION SYSTEM

Jon del Portillo[1], Jaizki Mendizabal[1], Iñigo Adin[1], Juan Melendez[1], Joaquin de No[2] and Unai Alvarado[1]

[1] *CEIT and Tecnun, University of Navarra, Manuel de Lardizábal 15, 20018 San Sebastián, Spain*

[2] *Tecnun, University of Navarra, Manuel de Lardizábal 13, 20018 San Sebastián, Spain*

Keywords: Temperature, MTTF, THR, EMC, BIST, Requirements, Design parameters, Safety, Safety critical system.

Abstract: Safety-critical equipment depends on the study of functional, thermal, EMC (Electromagnetic Compatibility) and RAMS (Reliability, Availability, Maintainability and Safety) fields. The variation of one area characteristic could result in a failure to fulfil safety requirements. Traditionally, thermal, EMC or RAMS issues were only considered once the design was done. This paper proposes a novel analogue equipment design methodology by studying these areas dependently from the beginning of the design process. Each area requirements and design parameters and the relation among them are defined qualitatively and quantitatively. Based on these dependences among all the areas, the cross-influence of each parameter variation in other areas requirements is demonstrated. The obtained results are intended to aid the fulfilment of requirements of the design of any safety critical analogue circuit, and to help designers to know beforehand the consequences of any change in the design, saving time and money. The application of this methodology in a SIL 2 RF transmitter is shown and the improvement and worsening of requirements depending on the parameters variation is exposed.

1 INTRODUCTION

Signalling, communication and control systems are part of safety-critical systems included in a number of transport means, as aircraft and trains. Generally, from the design perspective there are four key areas for consideration in the design process of safety critical systems: functionality, temperature, EMC and RAMS.

The design methodologies described in the literature take into account different variables. Some define methodologies for safety and EMC (Alexandersson, 2008) (Armstrong, 2006), others optimise reliability and cost constraints (Zafiropoulos, 2007), and others focus their efforts on the functional capability (Gilbert, 2005). All of them are valid depending on the system requirements and even can be compatible, but this paper proposes a more complete analysis.

A new global methodology including temperature and EMC requirements, for reliability and safety critical systems is needed. This all-inclusive methodology for system designs completes the state of the art supporting the robust design literature for analogue hardware. The four areas need to be considered in parallel moving forward in the same direction: the consideration of the multidisplinary requirements and their fulfilment in a control manner.

The main goal of this work is to establish a design methodology to define and quantify the relation between the RAMS design parameters and requirements with the functional, thermal and EMC characteristics (Figure 1).

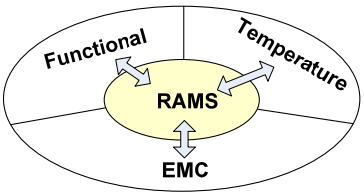

Figure 1: Relations between RAMS characteristics and functional, thermal and EMC characteristics.

In this paper, the group of functional, thermal and EMC fields are identified by FTE acronym. So,

del Portillo J., Mendizabal J., Adin I., Melendez J., de No J. and Alvarado U..
FUNCTIONAL, THERMAL AND EMC ANALYSIS FOR A SAFETY CRITICAL ANALOGUE DESIGN APPLIED TO A TRANSPORTATION SYSTEM.
DOI: 10.5220/0003571702190223
In *Proceedings of 1st International Conference on Simulation and Modeling Methodologies, Technologies and Applications* (SIMULTECH-2011), pages 219-223
ISBN: 978-989-8425-78-2

FTE-RAMS term would be related to FTE design parameters and RAMS requirements analysis, whereas RAMS-FTE term to RAMS design parameters and FTE requirements analysis.

This paper is organized as follows. Section 2 defines the four areas independently. Section 3 introduces RAMS equations, while section 4 analyses FTE-RAMS performance and RAMS-FTE analysis. The final equations of all these analyses are presented in section 5. Finally, section 6 describes the application of this methodology in the design of an RF transmitter, part of a safety critical system. And the conclusions are drawn in section 7.

2 DESIGN PARAMETERS AND REQUIREMENTS

In order to obtain the relationship among functional, thermal, EMC and RAMS parameters, it is first necessary to define the system requirements, and the design parameters of any analogue equipment.

The reliability requirement is the Mean Time To Failure (MTTF). Whereas, safety requirement is defined as Tolerable Hazard Rate (THR). The two RAMS design parameters that are the failure rate of the components and the use of safety improvement techniques, as table E.4 of standard EN50129 (CENELEC, 2005) defines. Two of these techniques are Built-In Self-Test (BIST) and redundancy. The former adds an extra parameter for the design: Mean Detection Time of the failure (MDT), and evidently, the reliability data of the components of the added topology have to be considered.

The functional parameters and requirements strongly depend on the designed equipment type. The design parameter that most affects the reliability is the architecture of the equipment. Thermal requirements are the maximum and minimum operating ambient temperature. And thermal design parameters are components thermal resistance between junction and air or maximum junction temperature. EMC requirements are divided into immunity and emissions / radiated and conducted. The radiated limits are defined as the maximum electric or magnetic fields. The EMC design parameters consist of components insertion as components to avoid conducted interferences.

3 RAMS ANALYSIS

This analysis defines the relation between the RAMS parameters and requirements described in section 2. In most cases, the transmitter or receiver consists of a main chain and it is assumed that a single failure causes a system failure (Smith, 2000). The system MTTF is inversely proportional to this failure rate.

In systems where no safety improvement technique is used, HR is equal to the failure rate of the safety function related to this hazard. Because of the high failure rate of some analogue components, it is usual not to accomplish at least one of the two RAMS requirements (MTTF and THR).

The system MTTF with BIST is worse than the one without and system. HR with BIST depends on the included components failure rate (λ_{iBIST}), MDT and the occurrence rate of the event (r_H) that can produce the hazard, as shown in (1) based on EN50129 (CENELEC, 2005).

$$HR = \left(\lambda_{system} + \Sigma\lambda_{iBIST}\right) MDT \cdot r_H \quad (1)$$

Another possible solution from the architecture point of view is the redundancy**.** The analyses of these architectures are done at length in different references, as in (Smith, 2000).

4 FTE-RAMS AND RAMS-FTE ANALYSIS

Once all the requirements are defined, the first stage of the system design is the architecture definition in order to fulfil functional requirements. System functionality can be achieved by means of different architectures. System failure rate of analogue equipment depends on the failure rate of each of its components. This information can be obtained from manufacturers or reliability databases (MIL-HDBK-217F 1991). These values provide the information to know if the equipment fulfils the RAMS requirements.

Thermal issues also affect system RAMS requirements, because depending on the operating temperature of the component its failure rate differs. The component failure rate is exponentially dependant on the junction temperature (Hnatek, 2003). And, as shown in (2), in the case of a heatsink, thermal resistance between junction and ambient (R_{JA}) is distributed among three thermal resistances ($R_{JC,}$ resistance between junction and case; R_{CH} between case and heatsink; R_{HA} between heatsink and ambient).

$$T_J = P_D \cdot \left(R_{JC} + R_{CH} + R_{HA}\right) + T_A \quad (2)$$

where P_D is the dissipated power.

All these parameters have a physical limit, therefore, once the best heatsink is chosen, the way to improve the resistance is the inclusion of air flow by means of a mechanical cooling system. The use of a fan is very common in this type of equipment, but the low MTTF of this type of components is its major drawback.

In order to fulfil EMC requirements, radiated and conducted interferences have to be eliminated by means of the inclusion of extra components. The conducted interferences are eliminated using bypass capacitors. ESD protections are needed in all the external connectors of the system. As said previously, the insertion of all these components worsens the system MTTF and HR.

It is crucial to know that the variations due to RAMS aspects affect the characteristics of the system regarding FTE performance (RAMS-FTE).

Safety-aimed changes must not vary the system main functionality, but the characteristics of the system blocks may be varied if the new architecture needs them. As explained previously, the two possibilities analyzed in this work to improve system safety are the BIST and redundancy. Both techniques affect system consumed power and transmitted or received RF signal power.

The need of including components in the transceiver chain results in a reduction of the transmitted power. Therefore, equipment characteristics need to be changed to obtain the same output power as in the absence of these techniques.

Either BIST or redundancy implies the insertion of new components in the system and hence, new signals. These generate two types of EMC issues, interferences to the environment and interferences within the components of the system; both of which must be avoided.

5 ANALYSIS RESULTS

Once the causes and consequences among FTE and RAMS characteristics have been analyzed, RAMS-FTE and FTE-RAMS (section 4) analyses results are gathered. Table 1 exhibits FTE-RAMS trends, where the columns show the requirements and the rows define the design parameters. The parameters trend is defined by means of – and +. The ↑ in the cells shows the improvement of the requirement while the ↓ the worsening.

In the case of BIST technology, the decrease of MDT (quantifiable parameter) makes the THR better, but, at the same time, the use of new components (non quantifiable) worsen some requirements. The advantage of BIST is the HR improvement, at the cost of worsening system MTTF.

System MTTF is inversely proportional to the sum of the components failure rate. Therefore, the lower the BIST and EMC solution components failure rate is, the lower its effect in MTTF. Although, as shown in the next section, these components usually have a very low failure rate.

Table 1: Effect on RAMS requirements.

			RAMS req.	
			THR	MTTF
Functional	Chosen architecture		↓	↓
Temp.	Thermal resistance	-	↑	↑
	Max junction temp	+	↑	↑
	Cooling mechanism	+	↓	↓
EMC	Filter	+	↓	↓
	Capacitances	+	↓	↓
	ESD protections	+	↓	↓

As shown in (1), HR strongly depends on the MDT and r_H. The shorter this period (MDT) the better the system HR, however the failure rate of the components included in the system is directly added to the failure rate of the system. So, a trade-off must be considered between the failure rate of the included components and the MDT.

6 SIL 2 RF TRANSMITTER

The methodology, based on studying functional, thermal, EMC and RAMS from the beginning is applied to a design of a SIL 2 RF transmitter.

The system to be designed is an analogue transmitter for a signalling system located in a high speed train. RAMS requirements are defined by the railway safety requirements (UNISIG 2009). The minimum MTTF limit is defined as $5 \cdot 10^5$ hours. Whereas the safety requirement of the transmitter is given by the THR related to the safety related hazard. This THR for the transmitter is $2.2 \cdot 10^{-8}$ dangerous failures per hour.

6.1 FTE-RAMS Analysis Results

The basic architecture for this type of transmitter is based on a signal generator and different amplifier stages. By means of the failure rate of every component at 25ºC and 60% confidence level, the reliability data calculation can be obtained. It shows that the proposed architecture (first line of Table 2)

accomplishes MTTF requirement, but HR is 10 times higher than the THR.

The environmental conditions (temperature) make the reliability data worse, as shown in the second line of Table 2. Moreover, other effect that must be included in the RAMS calculations is the inclusion of the components to mitigate interferences. These components effect is shown in the third line of Table 2, where MTTF and HR are 12.5% worse.

Table 2: Reliability data for four cases.

	HR (f/h)	MTTF (hours)
Tx @ 25ºC	$2.73 \cdot 10^{-7}$	$3.66 \cdot 10^{6}$
Tx @ 50ºC	$1.33 \cdot 10^{-6}$	$7.54 \cdot 10^{5}$
Tx @ 50ºC + EMC	$1.52 \cdot 10^{-6}$	$6.59 \cdot 10^{5}$
Tx @ 50ºC +BIST+EMC	$3.39 \cdot 10^{-9}$	$6.56 \cdot 10^{5}$

Due to that reason, BIST is introduced (the rate of hazard occurrence is 400 times per hour and the used MDT is 40ms). Therefore, the calculated system HR and MTTF are shown in the fourth line of Table 2. Both requirements are accomplished, although the MTTF is slightly worse. All the values fulfil the requirement, but the MTTF decrease with the temperature, BIST and EMC is clear.

Figure 2 shows the HR evolution, where the surface in the middle is THR. The lower surface is the HR with BIST and the one at the top HR without BIST. It can be seen that HR without BIST does not fulfil the requirement, while the BIST topology allows it be fulfilled. In both cases, HR value increases with temperature and the EMC solutions.

6.2 RAMS-FTE Analyses Results

From the RAMS-FTE analysis point of view, BIST technique implies the insertion of a power detector, which generates a power loss. So, it is necessary to increase the output power. Power consumption is also modified due to the components included and the need of transmitted power increases 3% the total consumption.

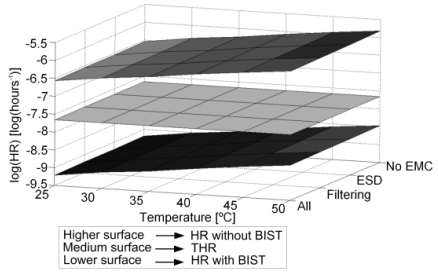

Figure 2: HR evolution and comparison with the requirement (THR).

The thermal characteristics due to the extra components included do not change significantly because the increase of the dissipated power is only 3% of the total dissipated power.

The last consequence of BIST technique is the variation of EMC characteristics. The self-test is done by means of digital systems, which may disturb the analogue system operation. In order to avoid any malfunction, capacitors have to be included.

7 CONCLUSIONS

In order to fulfil all the requirements that any safety critical equipment presents, this paper shows a design methodology that includes the study of functional, thermal, EMC and RAMS performance. This novel methodology allows the designer to avoid redesigns, due to non-considered issues, as typically happened with thermal and EMC matters.

RAMS requirements, THR and MTTF, depend strongly on the chosen architecture and the thermal resistances of the components, while EMC solutions have less effect. On the other hand, RAMS parameters variation showed slightly worse results in a slight worsening of functional, thermal and EMC requirements, but all of them accomplish the limits.

The proposed methodology is applied to a SIL 2 RF transmitter located in a signalling system of a high-speed train, where the BIST technique was needed to attain THR.

This design methodology was tested to use with a common goal: a safety-critical system global requirements fulfilment.

REFERENCES

S. Alexandersson. Functional safety and EMC for the automotive industry. *IEEE International Symposium on EMC, 2008*.

K. Armstrong. Design and mitigation techniques for EMC for functional safety. *2006 IEEE International Symposium EMC*.

EN50129. *Railway applications. Communication, signalling and processing systems.* AENOR; 2005.

J. M. Gilbert, I. M. Bell, D. R. Johnson. Circuit design optimization based on quality cost estimation. *Quality and reliability engineering international January 2005*.

E. R. Hnatek. *Practical reliability of electronic equipment and products*. Marcel Dekker, Inc; 2003.

MIL-HDBK-217F. *Reliability prediction of electronic equipment*. Department of Defense (US); 1991.

D. Smith. *Reliability*, *Maintanibility and Risk*. Butterworth-Heinemann; 2000.

Subset-036. Issue: 2.4.1. *FFFIS for Eurobalise*. UNISIG; 2007.

Subset-088. Issue: 2.2.10. *ETCS Application Level 1 - Safety Analysis. Part 0 to Part 3*. UNISIG; 2009.

E. P. Zafiropoulos, E. N Dialynas, Methodology for the optimal component selection of electronic devices under reliability and cost constraints. *Quality and reliability engineering international; May 2007*.