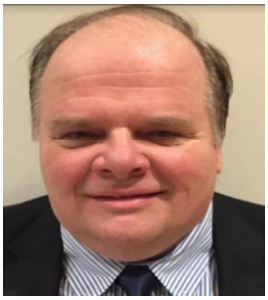
MEASURING RISK IN THE AUTOMOTIVE DESIGN PROCESS

RICHARD HARPSTER; PRESIDENT OF HARPCO® SYSTEMS INC;



Richard Harpster is president of Harpco® Systems Inc. which he founded in 1987. Harpco® Systems specializes in providing software, training and consulting for Risked Based Product Lifecycle Management (RBPLM®). Over the past 30 years Mr. Harpster has helped hundreds of companies implement improved risk-based design and manufacturing systems in a wide variety of industries. He is a recognized expert in the application of FMEAs and invented several new concepts including the linking of Design FMEAs to Process FMEAs in 1990 which became an automotive industry standard eighteen years later. His latest inventions in the field of RBPLM® include Requirements Risk Assessment™ (RRA®), Usage Risk Assessment (URA™), Multiple Integrated Cause Analysis (MICA™) and Rapid Integrated Problem Solving (RIPS®). He has published several papers on the topic of RBPLM®. Prior to starting Harpco® Systems, Richard spent 14 years at Ford Motor in a wide variety of positions including Plant Manager. His education includes a B.S.E.E. from Penn State University, M.S.E.E from the University of Detroit and an M.B.A. from Eastern Michigan University. He is a registered PE in the State of Michigan.

ABSTRACT

IATF 16949:2016, the automotive international quality standard for quality management, requires the use of risk-based thinking in the management of processes that have an impact on the quality of a company's products. Risk-based thinking is the use of risk to identify, prioritize and remove the sources of potential problems that expose the company and its customers to the greatest harm. To effectively implement risk-based thinking the company must be able to properly measure risk.

The design of products is an important process in the automotive industry where the proper implementation of risk-based thinking is critical. The purpose of this paper is to define:

1) what design risk is;
2) the accuracy of design risk measurement required;
3) the key steps to measuring design risk;
4) the role of the Design FMEA and design verification in design risk measurement;
5) common mistakes made in measuring design risk.

Keywords: Risk, Risk-based Thinking, Design FMEA, ISO 9001:2015, IATF 16949:2016, Prototype Control Plan, Design FMEA Severity of Effects Table, Class Symbol, Risk Matrix, Risk Policy, Design Control, Design Verification, Design Verification Plan.

INTRODUCTION

Since the release of ISO 9001:2015 and IATF 16949:2016 which requires compliance with IS0 9001:2105, risk-based thinking has received a lot of publicity in all industries including the automotive. Although the use of risk-based thinking has always been implicit in the two standards, proof of the use of risk-based thinking is now required.

Risk-based thinking can be used when making a wide variety of business decisions including pursuing new business opportunities, releasing product designs and modifying manufacturing processes. The good news is risk-based thinking is something most companies do automatically. If a company asks the question "What are the risks?" before taking an action, the company is using risk-based thinking. The bad news is that most companies do not use risk-based thinking as effectively as they could.

One of the main sources of a company's inability to effectively implement risk-based thinking is an inability to accurately measure risk. The purpose of this article is to examine how to measure risk in the design process. If a company can define the hardware specifications and software code (if applicable) that represent the greatest sources of risk, company resources can be targeted to make the necessary changes before design release to improve design performance and prevent future design failures.

KEY FACTOR IN DETERMINING REQUIRED RISK MEASUREMENT ACCURACY

For the sake of the discussion, we will assume the product has hardware and software components. The required accuracy of risk measurement is dependent on the type of decision one is trying to make. In the design process there are three decisions where using risk-based thinking can be extremely powerful.

The first decision is to define which hardware specifications and software code must be considered for possible change to reduce future design failures and thereby reduce risk. The second decision is the priority for working on the potential hardware specification and software code changes. The third and final decision is if or when the hardware specifications and software code should be released for manufacture. The ability to measure design risk must allow us to make these three decisions correctly.

DEFINITION OF RISK

Risk is comprised of two components. The first is the level of harm that can occur when an objectionable incident

occurs. The second component is the probability of exposure to the harm. The combination of both components is used to define risk.

DEFINING AND MEASURING THE HARM COMPONENT OF RISK

Harm occurs when an objectionable incident occurs. In the design process an objectionable incident is when the design fails to meet a design requirement. Various types of harm can occur at different probabilities when the design failure occurs. Although one can do a reasonable job identifying the different potential types of harm, knowledge of their individual probabilities can be lacking. For this reason, it is recommended that the worst-case harm be selected regardless of probability when determining the severity of harm for a design failure. The potential financial damage to a company due to overstating potential harm due to design failure is typically much less than understating it.

The Design FMEA is the most common tool used in the automotive industry to manage design risk. To assist in the measurement of harm, the Design FMEA has a Severity of Effects table identifying types of harms that can be experienced when the design fails. Design FMEA Severity of Effects tables can come in various sizes. Typical sizes are ten and five rows. The automotive industry uses 10 rows. Table 1 is a typical "Severity of Effects" table.

Description	Rating
Possibility of injury or violation of law without warning.	10
Possibility of injury or violation of law with warning.	9
Loss of primary function.	8
Reduction of primary function.	7
Loss of secondary function.	6
Reduction of secondary function.	5
Noise or appearance issue detected by customer that results in return.	4
Noise or appearance issue detected by customer that does not result in return.	3
Noise or appearance issues typically not detected by customer.	2
No effect.	1

Table 1: Severity of Effects

The Severity of Effects Table Rating indicates a relative ranking for each type of harm identified. Due to the need to identify ten different types of harm, it is not uncommon to see Severity of Effects Tables where individual harm types have the same cost impact. As an example, the cost of repair or replacement for a product that fails completely or partially are typically the same. In the Severity of Effects Table, the complete failure is typically given a higher rating than partial failure. Since they have the same financial impact, an additional grouping of the harm descriptions is required to assign a financial cost to the harm. Although there are ten different harm descriptions, it is not uncommon to see companies group them into three or four cost zones. Table 2 is a "Severity of Effects with Cost Zone" table that could be used to define the cost categories for the types of harm defined in Table 1.

Cost Zone	Description	Rating
Safety/Legal Zone	Possibility of injury or violation of law without warning.	10
	Possibility of injury or violation of law with warning.	9
Return Zone	Loss of primary function.	8
	Reduction of primary function.	7
	Loss of secondary function.	6
	Reduction of secondary function.	5
	Noise or appearance issue detected by customer that results in return.	4
Conditioned Response Zone	oise or appearance issue detected by customer that does not result in retur	3
	Noise or appearance issues typically not detected by customer.	2
	No effect.	1

Table 2: Severity of Effects with Cost Zone

Safety and legal issues are the most expensive problems that a company can have. The "Safety/Legal Zone" contains harm descriptions that describe physical injury or violation of a law.

The next cost zone is the "Return" zone. The harm descriptions contained in this zone involve harms that involve return of the product. Typical harm descriptions include loss or reduction of a primary function, loss or reduction of a secondary function or noise and appearance issues that result in a return. The multiple harm descriptions are placed in the same zone because their cost to the company to resolve are typically very close and are significantly less than Safety/Legal zone cost issues.

The final cost zone is the "Conditioned Response Zone". This zone includes harms that the customer is currently conditioned to accept as normal and consequently does not return the product for repair. The zone also includes problems with the product the customer may not be aware of. The is no cost of return of the product for repair or replacement for harms in this zone.

DETERMINING THE PROBABILITY OF HARM EXPOSURE COMPONENT

Once a measurement of harm is developed, the focus can be moved to determining the probability of harm exposure. Since it is being assumed that the worst-case harm will occur if the design fails, the probability of exposure to harm becomes the probability of the design failure creating the harm.

To determine the probability of design failure, one must first identify the potential root causes which are the hardware specifications and/or software code that if incorrectly specified can lead to the design failure. Once the potential root causes of the design failure are defined, a method or methods must be identified to determine the probability of the design failure due to the causes. The methods are called design verification controls.

The proper design of the design verification controls is the most important factor in accurately determining the probability of design failure. When designing a design

verification control, three key factors that must be considered.

It is important that the design control closely approximate the environmental conditions under which the objectionable incident is expected to occur during actual usage. It is not uncommon to find companies using methods that do not include expected conditions of usage that can play a significant role in the performance of a product. One example of this was a hydraulic component company that would do testing with clean hydraulic oil rather than oil that contained typical levels of contamination when they knew that the contamination could have a significant impact on the performance they were evaluating. When asked why they did not use oil with typical contamination levels to include actual usage conditions in the evaluation, they explained that the oil would contaminate their test equipment and they would have to clean it after each test.

When attempting to determine the risk due to a hardware specification, it is important to remember that you are trying to determine the probability of design failure when the product is built anywhere within the specification. Consequently, it is important that the products are evaluated at worst case specifications if possible. If physical prototypes are used, attempts should be made to build them to worst case for the hardware specifications being evaluated. If it is not possible to build prototypes to worst case, it is important that the hardware characteristics whose specifications are being evaluated for possible cause of design failure be measured so adjustments can be made in the actual test procedure or the analysis of the results to compensate for the measured values positions within their specification ranges. The Prototype Control plan is the key tool in accomplishing this task by requiring the measurement of the hardware characteristics to be evaluated during the prototype build.

The final key factor when designing design verification controls to determine the probability of design failure is sample size. The sample size has a direct impact on the confidence level one can have on the design control's ability to assess the adequacy of the hardware specifications and software code to prevent design failure.

While one would like to know the actual probability of design failure due to the failure cause being evaluated, it can be very difficult and sometimes impossible. The good news is that it is typically possible to define a confidence level that the design failure will not occur due to the cause. Consequently, when determining the probability of harm exposure to arrive at a risk measurement, it is not uncommon to use a combination of probability of failure data if available and confidence levels when probability of failure data is not available. Table 3 "Occurrence of FM Due to FC" is a table where either "probability of design failure due to the cause" or "confidence that design failure will not occur due to the cause" can be used to arrive at a rating that is indicative of probability of harm exposure.

Description	Rating
>/= 1 in 10; Confidence Level: <70%.	10
1 in 20; Confidence Level: 70%.	9
1 in 50; Confidence Level: 75%.	8
1 in 50; Confidence Level: 80%.	7
1 in 500; Confidence Level: 85%.	6
1 in 2,000; Confidence Level: 90%.	5
1 in 10,000; Confidence Level: 95%.	4
1 in 100,000; Confidence Level: 99%.	3
1 in 1,000,000; Confidence Level: 99.9%.	2
Failure is eliminated.	1

Table 3: Occurrence of FM due to FC

When a Design FMEA is being used, the rating from Table 3 is used to populate the Occurrence column. It is important to recognize that this table is providing a rating that is indicative of the probability that the design will fail due to the potential failure cause. It is not the probability of the potential failure cause occurring which the majority of FMEA reference manuals including the AIAG 4th Edition FMEA Manual and 2012 VDA FMEA manuals define it as. The probability of the potential failure cause occurring by itself is not a component of risk measurement.

When using design control results the challenge one faces is that a single design control typically is assessing the probability of a design failure due to multiple hardware specifications and/or software code when we want to know the risk impact due to individual hardware specifications and/or software code. Consequently, when design control results indicate an objectionable risk is present one must subjectively determine which of the hardware specifications and/or software code being evaluated by the design control they believe is most likely causing the design failure and perform the initial improvement activities on them while ignoring the potential causes that are deemed less likely. If it found that the selected hardware specifications and/or software code are not the source of the failure, the other potential causes are then evaluated.

DETERMINING TOTAL RISK

Once the severity of harm and probability of exposure to harm components are defined, the next step is to define the risk. A Risk Table (Table 4) must first be constructed. The Risk Table is matrix where the "Y" axis size is determined by the number of rows in the Severity of Effects Table (Table 1). The "X" axis size is determined by the number of rows in the Occurrence of FM Due to FC Table (Table 3). Symbols are defined to identify the cost zone that the severity rating falls in (S/L=Safety/Legal Cost Zone, R=Return Cost Zone). The appropriate cost zone symbol is placed in any combination of severity of harm (Severity

rating from Design FMEA) and probability of exposure to harm (Occurrence rating from Design FMEA) that the company identifies as unacceptable risk. The Risk Table cost symbol determined by the ratings is placed in the Class column of the Design FMEA. Table 4 is a typical Risk Table.

10		S/L	S/L	S/L	S/L	S/L	S/L	S/L	S/L	S/L
9		S/L	S/L	S/L	S/L	S/L	S/L	S/L	S/L	S/L
8				R	R	R	R	R	R	R
7				R	R	R	R	R	R	R
6				R	R	R	R	R	R	R
5				R	R	R	R	R	R	R
4				R	R	R	R	R	R	R
3										
2										
1										
Sev/ Occ	1	2	3	4	5	6	7	8	9	10

Table 4: Risk Table

USING RISK TO ANSWER THE THREE DESIGN PROCESS QUESTIONS

Design failure and cause combinations with cost zone symbols are issues that must be worked on because their risk is unacceptable. The priority on which they are to be worked on is based on the cost zone the combination occurs in and the Occurrence rating. Items in the highest cost zone must be worked on first (red zone). Items within a cost zone are to be prioritized based on the Occurrence rating with the highest ratings (lowest confidence factor) being worked on first.

The final question that must be answered is when the design can be released for manufacture. It is very difficult for a company to remove all sources unacceptable risk. Consequently, the company must define how much risk is acceptable. As a result, a risk policy must be developed. A typical risk policy may be "no designs may be released with design issues in the Safety/Legal cost zone or with design issues in the Return zone with Occurrence ratings greater than 4". Table 5 is a typical "Risk Policy" table that is a graphical representation of such a policy.

10		*S/L	*S/L	*S/L	*S/L	*S/L	*S/L	*S/L	*S/L	*S/L
9		*S/L	*S/L	*S/L	*S/L	*S/L	*S/L	*S/L	*S/L	*S/L
8				R	*R	*R	*R	*R	*R	*R
7				R	*R	*R	*R	*R	*R	*R
6				R	*R	*R	*R	*R	*R	*R
5				R	*R	*R	*R	*R	*R	*R
4				R	*R	*R	*R	*R	*R	*R
3										
2										
1										
Sev/ Occ	1	2	3	4	5	6	7	8	9	10

Table 5: Risk Policy (*=No Design release)

ROLE OF DESIGN FMEA COLUMNS IN MEASURING RISK

Table 6 shows the columns from the Design FMEA that are used to measure risk. When used correctly, the Design FMEA is very effective tool for managing risk and keeping a record of the current measured risk of the current hardware specifications and software code.

Column Headings	Item/ Requirement	Potential Failure Mode (FM)	Potential Effect(s) of Failure (FE)	Sev	Class	Potential Cause(s) of Failure (FC)	Occ	Design Prevention Controls	Design Detection Controls
Design FMEA Content	Product/Design Requirement	Objectionable Incident (Design Failure to Meet Design Requirement)	Description of Harm Due To FM	7	R	Improperly Defined Hardware Specification or Software Code	4	Method of Determining Probability of FM due to FC	Method of Determining Probability of FM due to FC

Table 6: Design FMEA Columns Used for Risk Measurement

The Class column is used to capture the risk symbol from the Risk Table. A common mistake made in the automobile industry when populating the Design FMEA is to determine the Class column entry only using the severity of harm.

The Det (Detection Rating) and RPN (Risk Priority Number) columns from the Design FMEA are not shown as being used for risk management. The reason for this is as follows. Unlike the Process FMEA where one can reduce harm by implementing a product inspection (Detection Control) to keep an out of spec product with a safety related defect from being shipped, there is no such type of control in the Design Process to contain a design failure due to the design. Once the design is released, there are no detection controls to revoke the design release. Since RPN uses the Detection Rating in its determination, it cannot be used for risk measurement.

The proposed AIAG-VDA FMEA Manual recently made available for public comment includes an Action Priority (AP) column for risk measurement in the Design Process. The AP rating includes the Detection Rating in its determination and thus should not be used for risk measurement.

CONCLUSION

Risk-based thinking can be a powerful tool for defining where company resources should be applied to provide the greatest design improvement. To effectively use the technique, one must be able to accurately measure risk. To accomplish this task, one must understand the impact of design failures, identify the hardware specifications and/or software code that cause designs to fail and possess a strong product design verification plan.