Effortless Incremental Design FMEA

Christopher J. Price • University of Wales, Aberystwyth

Key Words: FMEA, automated FMEA, incremental FMEA, functional reasoning, qualitative analysis.

SUMMARY & CONCLUSIONS

Design FMEA of electrical systems is a costly and labour intensive process. Ideally it would be done when the electrical system is first designed, and repeated whenever any change is made to the design. Because of the cost, this has not been possible in the past.

This paper describes about how an existing tool for automating electrical design failure mode and effects analysis (FMEA) can be augmented to make incremental design FMEA much less of a burden for the engineer. The tool is able to generate the effects for each failure mode and to assign significance values to the effects. The first time that it is run on a design, the engineer still has quite a lot of work to do, examining the results and deciding what actions need to be taken because of the FMEA.

When a change is made to the circuit, the engineer runs the FMEA tool again and receives a new report. Because of the uniformity of the reports provided by the FMEA tool, it has proved possible to write software which sorts out the failure effects which have changed from the previous analysis and only report those results to the engineer. This makes examination of the repercussions of the incremental FMEA much less effort for the engineer, and makes it feasible to perform an incremental FMEA every time the design is amended.

1. INTRODUCTION

Failure mode effects analysis (FMEA) of electrical designs is typically performed towards the end of the development cycle for a new car. This is not an ideal situation. There are financial advantages to performing an FMEA as early as possible in the development cycle. It identifies potential problem areas at the time when design changes can be made at minimum cost. In this way, FMEA becomes part of the development process instead of a last minute check.

However if design FMEA is performed early in the design cycle, then it needs to be repeated whenever the design is changed. This is very time consuming to do: the reliability engineer needs to look at every failure mode again, in order to check that the changes to the design have not altered the effects of that failure mode. The prohibitive cost of repeating the design FMEA several times is the reason why it is usually performed late in the development cycle.

Previous work described the content and benefits of the Flame system, an automated FMEA assistant (Ref. 1). This paper shows how such an assistant gives even greater leverage where a design FMEA needs to be repeated on an amended version of a circuit for which an FMEA has already been performed. It turns incremental FMEA from a task too costly to carry out into one that is almost effortless.

1.1 *Acronyms*

FMEA Failure mode and effects analysis
RPN Risk priority number

2. THE FLAME SYSTEM

This section summarises the FLAME system as described in detail in Ref. 1. The Flame system has been under evaluation by automotive engineers during the intervening year, and so this section also summarises the important alterations and additions that have been made since Ref. 1 was produced.

The Flame system uses a description of the structure of an electrical design and of the functions of the subsystem in order to generate the effects of each failure mode on the design. It can also assign RPN values to each failure effect, using values assigned to similar failures in previous model years where it is available, along with information about the circuit design and about the importance of different functions being available to the driver.

When the automatic generation of the FMEA is completed, an engineer interacts with a screen version of an FMEA form, checking significant values, filling in any values that the system is unable to assess, and annotating the form with relevant observations. For the engineer, this is the most time-consuming part of the process, but much less time-consuming than filling in the whole form manually.

The main improvements to the Flame system made over the past year are:

A more powerful structural circuit simulator. Libraries of reusable components have been developed covering a much wider range of components. The Flame system can now deal with electronic control units, different relay types, sensors, etc. New types of component can easily be added using the Circuit Builder tool (Ref 2), making the system much more extensible than was previously the case.

Easier acquisition of system descriptions. The structural circuit descriptions are now imported into the Flame system directly from an ECAD tool used by our industrial partners. Any unknown components are flagged, and the user can then provide a definition of how they work. The functional description has been much simplified, and so is much easier for engineers to produce. It is also much more reusable, and we have a library of such functions for the different

0-7803-3112-5/96/$5.00 © 1996 IEEE

subsystems in a car, so an engineer can usually reuse an existing description. Ref 3 describes the new functional representation in greater detail.

3. INCREMENTAL DESIGN FMEA

Further significant benefits can be obtained because of the consistency of the automated FMEA production. Examination of hand-generated FMEA forms shows that engineers describe the same effect with different words in different parts of the form, and also assign different RPN values to the same effect. That is not the case in the Flame system – the same problem in the same part of the circuit will always generate the same effect, and have the same RPN values.

The consistency provided by the automated FMEA assistant can be used to reduce the burden of performing incremental FMEA. When a change has been made to an electrical design, the changed circuit topology is given to the FMEA assistant, and the automatic generation of effects and RPN values is repeated. It is not necessary at this point for an engineer to repeat the inspection of every possible failure mode. The automated FMEA assistant compares the effects for each failure mode with the effects that were produced for the previous version of the circuit, and can filter out all of the failure modes for which the effects have not changed. The engineer then only needs to inspect the failure modes where the effect has changed. This saves a lot of unnecessary repeated work by the engineer. The next section provides an example illustrating this.

4. A SIMPLE EXAMPLE FOR A LIGHTING SYSTEM

Figure 1 shows a screen dump of the Flame circuit simulation tool containing the headlights of a car. In practice, a lighting subsystem would be likely to include many other bulbs, but for simplicity, it has been limited to the headlights. The engineer identifies the supplied functions of the subsystem (to provide main beam headlights and dipped headlights), and links the functions to particular states of the circuit. Simulation of a correct version of the circuit is carried out to decide when the different functions should occur.

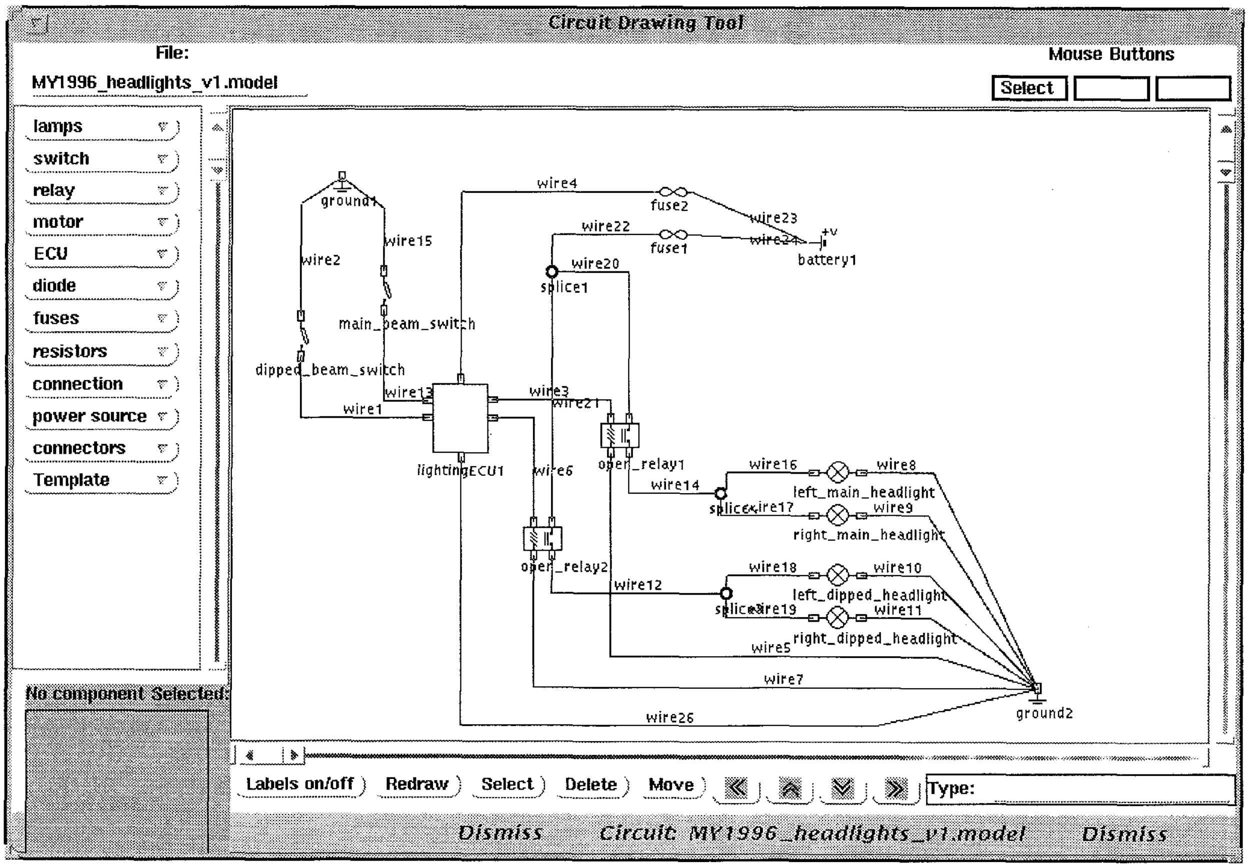

Figure 1: Example circuit to be analysed by FLAME system

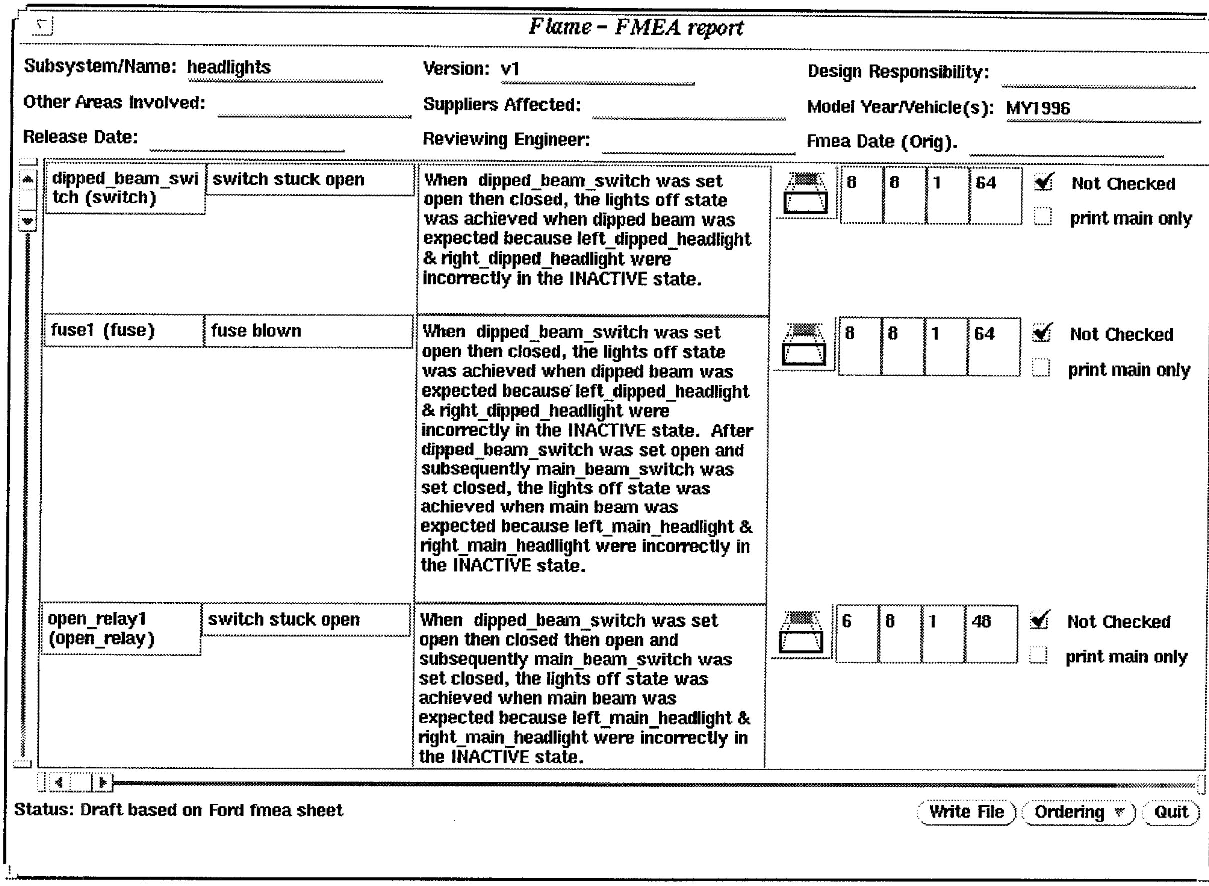

Figure 2: Interactive display of results of FMEA

Each type of component has a fixed list of failure modes. For example, the relay illustrated in the circuit could be stuck open or stuck closed. For each failure mode, the Flame system performs another simulation and records which functions occur in each state of the simulation, and assigns RPN values accordingly. For the circuit illustrated, 92 possible failure modes are investigated.

The results of the automated FMEA analysis can be examined interactively and annotated by the engineer, as illustrated by the screen dump in figure 2. When the engineer is happy with the report, it can be printed in a standard form and stored in the usual way.

Failure mode effects analysis is a design discipline which is intended to highlight problems with a design. Because of that, the FMEA report itself may prompt changes to the design, and that should be the case for this circuit. One problem that is shown clearly by this FMEA is that all failure modes which might blow the fuse will cause complete loss of all headlights. The engineer's response to this might be to fuse each set of headlights separately.

Having changed the design to add an extra fuse to the circuit, as illustrated in figure 3, the engineer needs to run the Flame system again. A complete analysis is produced for the new design and is available for examination by the engineer, but by default the engineer is just shown the effects that have changed from the previous version of the design. For the given change, there are 8 of those, and the engineer can see that the change to the circuit has reduced the RPN value in 4 cases because it has prevented complete failure of all headlights when a fuse blows. It has also introduced 4 new failures by adding a fuse and a new wire to the circuit. However, these failures are also less significant than the four they are replacing.

The incremental nature of the automated FMEA may well transform the use of the automated FMEA assistant from being a tool which is used after the engineer has decided on a design change into one which is used to perform "what-if" analysis as part of the process. It can be used to highlight what the reliability consequences of a proposed change might be, enabling the engineer to explore different alternatives.

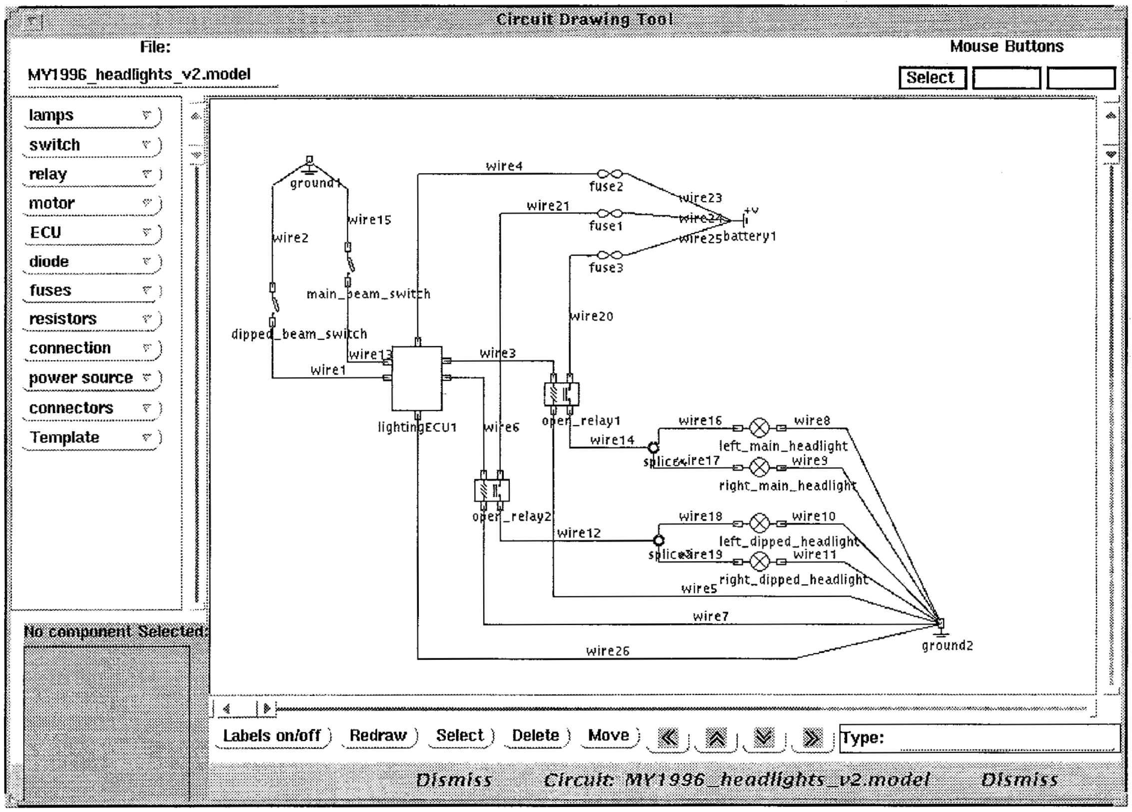

Figure 3: Amended circuit with separately fused lights

5. EFFECTIVENESS OF PERFORMING INCREMENTAL FMEA

This section looks at the difference that using the incremental FMEA tool described above would make to an engineer.

5.1 *Time taken without the Flame system*

The lighting circuit used as an example is a fairly trivial circuit, and yet a conservative estimate is that it would take a week to produce an FMEA report on the circuit without the use of a tool such as the Flame system. An update to the FMEA report could be produced more quickly, perhaps within a day, but the engineer would not look in detail at all the failure modes to produce it, just the ones that were most likely to be affected. Potentially dangerous effects could be missed by this partial FMEA.

5.2 *Time taken with the Flame system without incremental features*

The automated FMEA assistant speeds up the generation of an FMEA report significantly. Using the FLAME system to perform FMEA on the lighting subsystem is much quicker than doing it by hand. The lighting circuit will have been entered into the ECAD tool, and can be imported from there by clicking a couple of buttons. The reusable functional description of the lighting system can be verified and then linked to states of components in the circuit. This should only take a few minutes of the reliability engineer's time. The Flame system takes about 10 minutes on a Sparc 5 to identify all failure modes, generate all failure effects, and assign RPN values for each failure effect. While this does take some time, the engineer need not be present, and could be carrying out some other duty, or just taking a coffee break.

The major commitment of time comes during the interactive examination phase. The engineer will want to examine the results of the automated FMEA, and to study the significant failure effects in detail. The circuit simulator provides support for this, allowing the engineer to single step through the simulation of the circuit containing the failure mode under consideration. The engineer will also want to look carefully at cases where the Flame system was unable to decide on failure effects or to assign some of the RPN values. For a circuit of the complexity of the example, this process might take a couple of hours. Thus it can be seen that the FLAME system reduces the task of producing this FMEA report from one which previously took a week to one which can be performed within half a day at the most.

Without the incremental FMEA feature described in this paper, a repeat FMEA report on a changed version of the same circuit should take the same length of time, if the engineer gives the results of the FMEA the same level of study that was given the first time.

5.3 *Time taken for repeat FMEA using incremental features*

With the incremental FMEA feature described in this paper, a repeat FMEA report for a changed version of the same circuit takes very little of the engineer's time. The engineer needs to import the new version of the electrical design – a couple of clicks of a button. The engineer can again concentrate on other tasks while the machine is generating all failure effects (or can run the analysis overnight). Where the RPN values were not known on the first run and the effects have not changed, the Flame system can now reuse the values that the engineer assigned last time. The engineer could consider the complete FMEA report on-screen, but will usually only want to look at failure modes for which the effects have changed from the last time that FMEA was performed on this circuit. These are sorted out automatically by the system, and there are only a few of these, so the examination only takes a matter of minutes.

6. CONCLUSIONS

It can be seen that the Flame system reduces the amount of time needed to carry out an electrical FMEA by an order of magnitude. The incremental FMEA code reduces the effort required by engineers to perform a repeat FMEA for a minor change down to a few minutes.

The availability of almost effortless incremental FMEA should have a significant effect on the way that FMEA is practised. It makes it into a design analysis exercise which really can be performed concurrently with the design, and which can be repeated every time the design is changed, ensuring that design problems are detected early in the development lifecycle, and that problems introduced by late changes to the design are brought to light as part of a full FMEA.

ACKNOWLEDGEMENTS

This work has been supported by the UK Engineering and Physical Sciences Research Council (grant number GR/H96973), the Ford Motor Company Ltd, Jaguar Cars, the Motor Industry Research Association, and Integral Solutions Ltd, using the Poplog program development system.

REFERENCES

1. C. J. Price, D. R. Pugh, M. S. Wilson, N. Snooke, "The Flame System: Automating Electrical Failure Modes & Effects Analysis (FMEA)", Proc. Ann. Reliability and Maintainability Symp., 1995 Jan pp90-95.

2. D. R. Pugh, N. Snooke, "Dynamic Analysis of Qualitative Circuits for FMEA", accepted in abstract for Proc. Ann. Reliability and Maintainability Symp., 1996.

3. C. J. Price, D. R. Pugh, J. E. Hunt, "Development of a multiple model design analysis system", Proc. 3rd Intl Workshop on Advances in Functional Modeling of Complex Technical Systems, University of Maryland, 1995 Jun.

BIOGRAPHY

Christopher J. Price, *PhD, CEng*
Computer Science Department
University of Wales, Aberystwyth
Aberystwyth, Dyfed
Great Britain
Internet (e-mail): cjp@aber.ac.uk

Chris Price is Deputy Director of the Centre for Intelligent Systems at the University of Wales, Aberystwyth. His research interests include the application of model-based reasoning and case-based reasoning to engineering problems. He is Book Review Editor of Engineering Applications of Artificial Intelligence, and has published articles in Knowledge Engineering Review, Artificial Intelligence in Engineering, Engineering Applications of AI, Intelligent Systems Engineering Journal, Control Engineering Practice, Journal of Systems Engineering, Journal of Automobile Engineering.