Paper Number

Whole Lifecycle Electrical Design Analysis in Foresight Vehicle

N. A. Snooke, C. J. Price
Department of Computer Science, University of Wales, Aberystwyth, SY23 3DB, U.K.

D. Ellis
Ford Motor Company Limited, Room 15-3B/E-11, Dunton Research and Eng. Centre, Basildon, Essex, SS15 6EE

ABSTRACT

Design analysis such as Failure Modes and Effects Analysis (FMEA) or Sneak Circuit Analysis (SCA) is typically carried out once in the lifecycle of a product. This is likely to be late in the lifecycle, when all design information is available and the design is stable. The drawback of this is that problems discovered at this late stage can be very expensive to fix. On the other hand, performing the analysis earlier might miss some problems because they only become apparent once all information is available.

This paper describes tools for assisting engineers in performing design analysis early and efficiently repeating it whenever the design changes or extra information becomes available. These tools enable the engineers to obtain the best of both worlds. Information can be acted upon as soon as a problem becomes apparent, without tedious and expensive repetition of analysis by experts.

INTRODUCTION

Vehicle designs have been increasing in complexity for many years. As this has happened, it has become more difficult for designers to comprehend all the possible ramifications of a failure within their design, and to detect all of the possible interactions between parts of the design. In order to make sure that possible shortcomings of a design will be detected, a number of design analysis techniques have been developed.

FMEA. Failure mode and effects analysis considers the effect on an overall product of any (usually single) failure of part of the product.

FTA. Fault tree analysis highlights the combinations of failures that can affect the safety of a design.

Design verification. Given a formal description of the legal states in which a system can be, it is possible to analyze the operation of the design to ensure that the device cannot enter any illegal states.

Sneak circuit analysis. This identifies any unexpected interactions between systems within a product.

Breadboarding. Unlike most of the design analysis techniques mentioned here, this usually involves construction of a physical prototype. To ensure that the electrical systems of a product are designed correctly before constructing a complete prototype of a product, the electrical systems are pegged out on a large board and tested against expected behavior.

The overall effect of all of these design analysis techniques is to reduce the considerable risks involved in developing a new complex electro-mechanical product. Automated design analysis software has begun to make inroads into the difficult and tedious task of identifying potential problems in electrical and electronic systems. However, such software typically provides a snapshot analysis of the design at a point in time (when appropriate information is available), whereas design analysis is ideally performed iteratively throughout the design process. Early in the design, rough analysis can identify gross problems, whereas towards delivery time, detailed analysis can pinpoint complex problems that could not be identified precisely until enough information was available.

The Dougal project, part of the UK Government's Foresight Vehicle Initiative, has developed design analysis systems that can give progressively better design analysis results as more detail is available about a vehicle's electrical design. This has been achieved through developing a range of simulation models that can be automatically constructed from schematic information. Results of the simulations are linked to a common notion of system functionality, which allows the results of the different simulations to be compared, and

incremental changes to the results to be identified as the design evolves.

The benefit of this incremental design analysis is that instead of design analysis results being available only at one point in the development of a design (giving either early identification of significant problems, or detailed but late results), the designers always have access to the best results available given the known state of development of the design. These techniques have been applied to providing engineers with interactive simulation results, with automated failure mode and effects analysis reports, and with sneak circuit analyses.

AUTOMATED DESIGN ANALYSIS EARLY IN THE LIFECYCLE

A previous SAE World Congress paper [1] documented the use of electrical design analysis software to automate electrical design analysis techniques. The software documented in that paper was closely linked to the CAD software used by the engineers, so that once a schematic had been drawn, the software associated a component model with each drawn component, and could perform simulation of the whole system. In order to make the results of simulation comprehensible to users, two features are provided:

Visualization of results: Simulation colors the schematic within the CAD diagram, showing which parts of the circuit are active at any point in the simulation, so that the user can understand the effect of changing inputs. In addition to being able to observe which parts of the circuit are active by coloring wires, direction of current flow is indicated by arrows. This can be important. In a headlamp circuit, a particularly nasty set of results were achieved when a local ground to the left headlamp cluster was removed. Instead of the expected two lamps being illuminated, a total of 8 lamps were lit. The engineer's initial impression was that the modeling was in error. Close examination of the direction of current flows helped the engineer understand that it was a really nasty sneak effect involving currents running back to common fuses and switches that were not powered - all because of the lost ground. These visualization features are integrated with the other design analysis techniques, so that FMEA, for instance, can set up the circuit for simulation with specific faults induced on components, and visually demonstrate the effect of that failure on the circuit.

Abstraction of results via functions: The overall behavior of a circuit such as a door-locking system can often be summarized by a single label such as *locking* or *unlocking* or *locked*. For a cruise control system, the overall behavior might be summarized as *accelerating*, *decelerating*, *cruising* or *deactivated*. Most circuits will only need a few such functional labels. The software can determine the state of the overall system by examining the state of a small subset of the components in the circuit. The functional labels are used as the basis for written reports produced by the design analysis tools described in the next section.

The design analysis is based on the simulation, and can produce the following results:

What-if investigation: Once the schematic has been drawn, the engineer can alter inputs to the system, interactively flicking switches and activating sensors, and see the results of the simulation illustrated on the schematic. A good example of a what-if investigation occurred recently. The European Commission is introducing legislation to make day-time running lights (DTRL) mandatory for all new vehicles. There are a number of issues to take into account when meeting this legislation - negative effects on charge balance cycle, negative effects on headlamp warranty, extra costs for relays, resistance wires, interpretation of the homologation permitting optimization to offset these problems, etc. A headlight schematic without DTRL was modified to add it, and the simulation and visualization were used to run many different scenarios. Answers were found in a few hours to problems that might have otherwise taken weeks to solve.

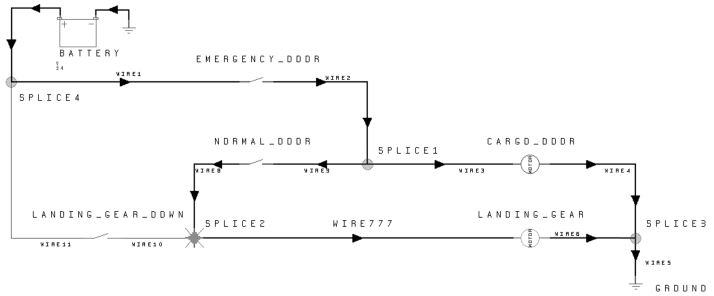

Figure 1: Extract from simulation

This kind of investigation could previously only be carried out by breadboarding a physical prototype. This virtual breadboarding can save significant time and effort for the engineers It is also a basis for automated design verification if there is a description of the intended behavior of the system, and all possible states are investigated.

The tool also allows us to ask what-if questions concerning destructive tests that may not be possible on a physical breadboard or real vehicle. In high-power circuits like electric windows, front-screen de-icers, etc, very large fault currents can flow. The cost and danger of testing these in real life rule them out. The version of the tool based on Saber (discussed later) makes it

possible to carry these tests out virtually. We can verify wire temperature and fuse relationships, failure mode management, etc, and make design revisions accordingly

Failure mode and effects analysis: The software is able to simulate operation of the schematic when one or more components have failed. An FMEA report is produced which gives in English the effect of each possible failure of each component in a schematic on the functioning of the whole circuit. These are presented to the engineers in a standard FMEA report format. Table 1 shows an undoctored example row of an FMEA report produced by the software. An example of the kind of problems that have been highlighted by this tool occurred in a lighting subsystem. Stop-lamps were driven by a lighting ECU module, and powered by the stop-lamp fuse input. The stop-lamp switch fed positive voltage to the ECU module when pressed. If the fuse failed, the ECU module would detect that braking was required but no power was available to supply the stop-lamps. It would alert the user that the stop-lamps were not available. In an early version of the lighting system, The FMEA software detected that when the stop-lamps did not work, no warning was issued. On examination, it turned out that this was because the stop-lamp switch was spliced to the fuse feed. When the fuse blew and the brake pedal was pressed, the ECU detected that there was no fuse feed, but did not detect that the brake pedal had been pressed, and so gave no warning. The software detected this early in development, and so saved a lot of money and cycle-time.

Assistance for FTA: One of the uses of fault tree analysis is to compensate for the shortcomings of manual FMEA. It is used to highlight all of the combinations of failures that will make a particular unwanted event occur. For example, such an event might be a vehicle's airbag firing when it should not. Alternatively, it might be to identify when the airbag will fail to fire. It is then possible to calculate an overall figure for how likely the unwanted event is to occur. Engineers calculate the dependencies in the fault tree by hand. The automated software can perform multiple failure FMEA. This provides all of the information that is needed to decide what combinations of failures can cause the unwanted event to occur. In addition, as vehicles become more complex, with ECUs programmed to mitigate the effects of known failures, it is likely to calculate the true effects of a combination of failures more accurately than an engineer mentally simulating circuit operation.

Sneak circuit analysis: In complex electrical systems, the interaction of several subsystems can cause further systems to be activated unexpectedly. A classic example is given in [2] of the cargo bay doors of a particular aircraft design, where operating the emergency switch for the cargo doors can cause the landing gear to lower unintentionally. Typically, such problems are caused when a wire, which was expected to provide current in one direction, is used in the opposite direction, causing a *sneak path*. A much more recent example seems to be given in [3], where an F-4EJ fighter discharged 188 cannon rounds unintentionally, because an abnormal electrical current that triggered the cannon system was generated when the control stick was inclined to the right past a certain point, if the cannon system was armed at the time.

Sneak circuit analysis (SCA) is the process of identifying and eliminating such sneak paths where they might occur. Where a wire is allowing current to flow in an unexpected direction, this can often be prevented by the addition of a diode to the design, but cost considerations mean that extra diodes should not be added to the circuit unless they are really needed.

We have implemented an automated sneak circuit tool capable of detecting classic sneaks [4]. The functions of the system will have already been declared for FMEA. It is necessary only to declare the combinations of inputs, which should activate each function. All combinations of inputs can then be tried in simulation in the circuit, and if unexpected functions occur for any combination of inputs, then they are due to a sneak.

Item/Fn	Potential Failure Cause	Potential Failure Mode	Potential Failure Effect	Sev	Occ	Det
(23)	The component UNLOCK_RELAY has failure switch stuck at contact2.	For the first time, the "doors unlocking" function was achieved. Finally, regardless of any event change, the "doors locked" function was never achieved, and the "doors unlocked" function was always achieved.	Doors started unlocking unexpectedly. Doors unlocked unexpectedly. Doors failed to lock.	6	3	2
(24)	The component DEADLOCK_RELAY has failure coil blown.	When DRIVER_KEY_SWITCH was set to lock (3) the "doors locked" function was achieved unexpectedly. Also, when DRIVER_KEY_SWITCH was set to neutral (4) the "doors locked" function was achieved unexpectedly.	Doors locked unexpectedly.	6	2	4

Table 1: Example output produced by FMEA tool

Unlike several other sneak circuit tools, it is not necessary to declare the direction in which current should flow through each wire (impossible for many wires in circuits such as central door-locking circuits, where current is allowed to flow both ways in many wires). Neither does the algorithm produce spurious sneaks. However, it does have drawbacks. It is necessary to draw a circuit including all of the subsystems that are suspected of interacting. It has detected sneaks in single complex systems that were drawn together as one design, but where subsystems interact, you would have to suspect the fact, and actively investigate it in order to find the interactions.

ADVANTAGES OF EARLY AUTOMATED DESIGN ANALYSIS

Design analysis can be performed with very little effort early in the design lifecycle, and gross errors detected and rectified. This is the time when it is cheapest to fix problems, and so is a great improvement over performing analysis much later in the lifecycle.

Engineers can explore possible technical solutions without physically building many prototypes - that only becomes necessary once the majority of the problems have been ironed out.

The software simulates current flow through the circuit using state-based descriptions of complex components, and idealized resistors (with values of zero, load or infinity). This means that early modeling of components is simple and components are very reusable. The library of components needed is much smaller than is the case for numerical simulators.

It provides the best results possible when all information on specific components used is not available.

DRAWBACKS OF EARLY AUTOMATED DESIGN ANALYSIS

Because only idealized resistors are used, it can be impossible to decide what will happen in a circuit. for example. if there is a short circuit, it is impossible to know whether a fuse will blow or wires melt unless the value of the fuse and the length and gauge of the wire are known. The early design analysis can only draw attention to a possible problem to be addressed when detailed design decisions are being made.

As extra information becomes available about the design, the engineers need to find other ways to check that problems raised by the early design analysis have been solved. For example, this might mean using the PSPICE simulator to get detailed results for a specific failure case. The need to be able to simulate with more detailed information when it is available has motivated the use of more detailed information where it is available within the software described above. The next section describes the different levels of information that become available, and how they are used to produce more precise versions of the results originally generated by the early design analysis.

IMPROVING ANALYSIS AS DESIGN INFORMATION INCREASES

The qualitative analysis outlined above works with very little information about the actual physical components used. The drawback of this is that some results are ambiguous, and some problems cannot be detected because the models of the components do not have detailed enough information. This drawback is a small price to pay for the ability to detect the majority of potential problems early in the design process with comparatively little effort.

The Dougal project has concentrated on how the analysis results can be gradually improved and tracked as extra information becomes available during the design process. For electrical systems, there are three further kinds of extra information that might become available:

- Knowledge of resistor levels in the circuit
- Knowledge of resistor values in the circuit
- Detailed numerical models for components in the circuit

KNOWLEDGE OF RESISTOR LEVELS

The qualitative simulation described in the previous section uses three levels of resistance - zero, load and infinite. These are not enough to distinguish between levels of current. For example, a trickle current through a device might be used to provide a signal, where it is not enough to activate the device. The qualitative simulation cannot distinguish between the two levels, and so either compromises must be made in the modeling or resolution of whether current levels are high enough for activation must be left to later in the design process.

Some ambiguous situations can be resolved by adding further levels of resistance. We have implemented a scheme which allows an arbitrary number of levels [5,6]. In practice, in present vehicles, a five level scheme gives some extra information in simulation. The levels are then: zero, low, medium, high and infinite. The presence of these distinctions allows the visualization to color the circuit with the different levels of activity in the circuit. In a vehicle with a 12 volt battery, the visualization shows three levels of activity as green, yellow and orange. These three levels correspond to information level flow (for activating ECUs), activation level flow (for activating relays), and power level flow (for activating motors). The correct results can be obtained in many of the cases mentioned above, without any modeling compromises.

KNOWLEDGE OF RESISTOR VALUES

Later in the design process, once decisions have been made about where to source components, precise values of resistors can be provided to the simulation, and the length and gauge of connectors will be known. Once that is the case, most of the short circuit cases that were identified in early design analysis can be resolved. Without numerical resistor values, it was impossible to tell whether a fuse would blow or a wire melt (if the fusing was wrong). Once resistor values are known, these ambiguous cases can be resolved.

DETAILED COMPONENT MODELS

For specific unresolved problems, or safety-critical systems, the engineers may choose to perform detailed numerical simulation using a tool such as PSPICE or SABER. We have interfaced the design analysis tools to SABER, abstracting the detailed numerical results given by SABER and producing the same English-level results that were provided by the qualitative simulator. As well as producing the type of design analysis results only previously available from the qualitative simulation, this work also provides a much more friendly interface to SABER for performing visualization work.

TRACKING ANALYSIS AS DESIGN DECISIONS ARE CHANGED

In the past, design analysis has usually been performed once during the development of a vehicle system. This would be towards the end of the product design lifecycle. Where changes were made to the design after the analysis had been carried out, it was not possible to completely repeat the analysis, and so engineers would estimate the effects of the change, and limit the analysis to the perceived influence of the change.

Once the design analysis is automated, it is very little effort to repeat the analysis whenever a change is made to the design. Similarly, when further information becomes available, such as knowledge of resistor values, then the analysis can be repeated with more detailed simulation, to provide more accurate results. However, that is not the end of the problem. The analysis is only useful because engineers look at the results, and take action on problems identified. A typical FMEA analysis might detail the effect of 500 different component failures, and so an engineer would not want to study the 500 results every time a small design change is made plus each time more information becomes available and it is possible to perform a more detailed simulation.

In order to address this problem, we have developed software to provide incremental FMEA results. When the automated FMEA is first performed, the engineer considers all results, and takes appropriate actions. When a change is made to the design, a new FMEA report is generated and the incremental FMEA software compares the new results with the previous set of results. Results which have changed are presented to the user, along with any new results (for example, failures on components which did not previously exist). Typically, for a simple change, a very small number of results will change.

The incremental FMEA also works to compare the results from the different types of simulation described in the previous section. This means that the implications of more detailed design decisions can also be tracked - as resistor values are decided or as resistor values change during the design process, the effects of those decisions on the design can be seen.

The potential of this facility has not been completely explored, but it provides the possibility of running design analysis each night on all systems where a change to the design has been made during the day, and providing a summary to the

engineers the next day of all implications of the design decisions made during the previous day. This would minimize the detection time for any decision which caused a new design problem.

CONCLUSION

Automated design analysis based on qualitative simulation provides a very valuable tool for assisting engineers in dealing with the complexity of modern vehicle design and producing robust designs under shorter timescales.

The work described in this paper improves that facility in three important ways:

- The integration of more detailed types of simulation with the design analysis tools provides more accurate results as more information becomes available.

- The provision of analysis at several stages of design means that the engineer has the best possible analysis available at any stage of the design process. With the exception of the SABER analysis, this is made available with very little extra effort from the engineer.

- The incremental FMEA enables the tracking of all changes to the design and improved information as the design evolves with minimum effort from the engineers.

ACKNOWLEDGMENTS

The research described in this paper was supported by the UK Foresight Vehicle program under EPSRC grant GR/N06052, and done in collaboration with FirstEarth Limited.

REFERENCES

1. D. D. Ward and C. J. Price. System functional safety through automated electrical design analysis. Procs of SAE World Congress, paper number 01PC-250, March 2001.
2. D. S. Savakoor, J. B. Bowles, R. D. Bonnell, Combining sneak circuit analysis and failure modes and effects analysis. Proc. Ann. Reliability and Maintainability Symp., Jan 1993, pp 199-205.
3. Aviation Week, July 9, 2001. page 17.
4. C. J. Price, N. Snooke, J. Landry, Automated Sneak Identification, Engineering Applications of Artificial Intelligence, vol 9(4), 1996 pp 423-427.
5. M. H. Lee. Qualitative modelling of linear networks in engineering applications. Procs ECAI-2000, 14th European Conf on Artificial Intelligence, pp161-165, Berlin, August 2000.
6. M. H. Lee, J. Bell and G. M. Coghill, Ambiguities and Deviations in Qualitative Circuit Analysis in proc. 15th International Workshop on Qualitative Reasoning, San Antonio, Texas, 2001. pp51-58

CONTACT

Neal Snooke, at address at top of paper, email: nns@aber.ac.uk.

DEFINITIONS, ACRONYMS, ABBREVIATIONS

ECU: electronic control unit

FMEA: failure mode and effects analysis

SCA: sneak circuit analysis