LAWRENCE
LIVERMORE
NATIONAL
LABORATORY

UCRL-JC-154905

Use of Fault Tree Analysis for Automotive Reliability and Safety Analysis

H. E. Lambert

September 24, 2003

2004 SAE Society of Automotive Engineers World Congress, Detroit, Michigan, March 8 – 11, 2004

DISCLAIMER

This work was performed under the auspices of the U. S. Department of Energy by the University of California, Lawrence Livermore National Laboratory inder Contract No. W-7405-Eng. 48

Use of Fault Tree Analysis for Automotive Reliability and Safety Analysis

Howard Lambert
Risk Assessment Analyst
Lawrence Livermore National Laboratory

925-422-5195
Fax 925-422-2091
E-mail LAMBERT8@LLNL.GOV

Abstract

Fault tree analysis (FTA) evolved from the aerospace industry in the 1960's. A fault tree is deductive logic model that is generated with a top undesired event in mind. FTA answers the question, "how can something occur?" as opposed to failure modes and effects analysis (FMEA) that is inductive and answers the question, "what if?" FTA is used in risk, reliability and safety assessments. FTA is currently being used by several industries such as nuclear power and chemical processing. Typically the automotive industries uses failure modes and effects analysis (FMEA) such as design FMEAs and process FMEAs. The use of FTA has spread to the automotive industry. This paper discusses the use of FTA for automotive applications. With the addition automotive electronics for various applications in systems such as engine/power control, cruise control and braking/traction, FTA is well suited to address failure modes within these systems. FTA can determine the importance of these failure modes from various perspectives such as cost, reliability and safety. A fault tree analysis of a car starting system is presented as an example.

1.0 Introduction

Methods and tools to conduct reliability, safety and risk assessments evolved from the aerospace industry in the 1950's and 1960's. The US Air Force required failure modes and effects analysis (FMEA) in the 1950's. The Department of Defense (DOD) adopted this requirement for DOD defense contractors. The use of FMEA spread to other governmental agencies such as NASA and other industries such as the automotive, petrochemical and electric power. Automotive industry conducts process and design FMEAs, ref [1] and [2].

FMEA is an inductive analysis asking the question "what if." FMEA generally addresses hardware failure modes and determines the affect of these failures on the system. Other methods of inductive analysis include hazards analysis, Markov analysis, decision trees and event trees.

Fault tree analysis (FTA) evolved from the aerospace industry in the early 60's. The technique was used to analyze undesired events associated with Ballistic Missile systems such as "Failure to launch missile on demand" and "Inadvertent missile launch." As with FMEA, DOD recognized the usefulness of FTA and its use spread to other governmental agencies and other industries. FTA became an important tool for conducting probabilistic risk assessment.

FTA is a deductive analysis technique asking the question "How can something occur?" FTA is generated with a top undesired event in mind. The fault tree is a graphic and logical representation of the various combinations of possible events, both fault and normal, occurring in a system. These events are represented by the appropriate symbols that can be used as inputs and/or outputs of the standard AND and OR gates or other logic gates. The basic events that appear at the bottom of the fault tree represent the limit of resolution in the analysis. Basic events include component failures, human error, software failures and environmental conditions. The fault tree is built by construction rules that establish the procedures necessary at each gate to determine the type of gate to use and the inputs to the gate. Fault tree evaluation can be both qualitative and quantitative (probabilistic)

2.0 Fault Tree Analysis

Possible steps to conduct FTA are listed below. Some or all of these steps can be conducted depending upon the scope and extensiveness of the FTA.

Step 1 – Define the Undesired Event
Step 2 – Acquire an Understanding of the System
Step 3 – Establish Scope and Bounds of the Analysis
Step 4 – List Assumptions
Step 5 – Construct the Fault Tree
Step 6 – Perform Qualitative Analysis
    1. Find Single point failures
    2. Find Common cause failures
    3. Find Min cut sets
Step 7– Perform Quantitative (Probabilistic Analysis)
    1. Probability of the top event
    2. Importance of basic events/min cut sets
    3. Uncertainty analysis
Step 8 – Conduct Tradeoff Studies
Step 9 – Make Decisions, Recommendations and Results
Step 10 – Document Results
Step 11- Perform Peer Review

In this paper, we conduct a qualitative FTA and do not conduct a probabilistic analysis.

2.1 Fault Tree Undesired Events

There are basically two types of events in fault tree analysis -- normal and fault events. In turn there are two types of fault events:

Type I -- A system element fails to perform an intended function
Type II -- A system element performs an inadvertent function.

An example of a normal event is “rich gasoline mixture during vehicle startup.”

Example of type I fault events include:

1. Engine misfires – bumpy roads
2. Poor engine performance at high altitudes
3. Malfunction indicator light (MIL) is off – vehicle exceeds OBD-II limits (On board diagnostics) pollution limits (violation of federal law)
4. Air bag fails to employ when vehicle collision occurs
5. Car fails to start

Example of type II events include

1. MIL light is ON when OBD-II system gives a false indication of an OBD-II power train component (driver nuisance)
2. Inadvertent deployment of air bag
3. Car starts in gear

2.2 System Understanding

The fault tree analyst must understand how the systems works as well as understand the specific failure modes that cause the top event to occur. It is desirable to represent the system in terms of a diagram, flow sheet or logic diagram. Complex systems may have modes of operation that require separate fault trees. For example, a car engine has the following operating modes:

- Startup
- Run
- Load
- Coasting
- Limp-in.

Figure 1 shows a modern day block diagram of a car starting system, ref [3]. Figure 2 taken from ref [4], shows the four strokes of a typical modern gasoline fired-spark-ignition engine which are 1. intake, 2. compression, 3. power and 4. exhaust. The function of the car starting system is to crank the engine to a sufficient speed so that a self sustaining combustion reaction can occur. The charging

system will also be modeled in the fault tree since the car starting fault tree will also contain the event "Insufficient Power output from battery."

The engine control module (ECM) and the On Board Diagnostic System (OBD II system version two) are two electronic systems that can affect the “Starting System.” ECM is the brain of the power train system. OBD II is a monitoring and reporting system that acts as a watchdog in controlling the vehicle emission. In the OBD II, there is an oxygen (O2) sensor located in the exhaust pipe between the engine and the muffler. This (or these) sensor(s) will monitor the emission output from the engine and report to the ECM. If the O2 sensor failed then the engine controller will not allow the engine to start.

2.3 Scope and Bounds of the Analysis

Temporal and spatial bounds are considered in the analysis in this step. System environment is considered. For example, environments considered such as car starting in cold temperatures, engine operation on bumpy roads, engine coolant system in hot weather.

2.4 Assumptions

In this step, assumptions are made. For example we assume that the engine consists of four cylinders. In addition, we will assume that there is a warning alarm in the event that the driver leaves the headlights on when the ignition switch is turned off. In addition, we give credit to the driver to take action (i.e., bring car in for service) in the event that the charging current indicator reads low or that charging system warning light turns on. The fault tree will include driver error -- i.e, leaving headlights on, failing to take action etc.

2.5 Fault Tree Construction

Figure 3 shows the fault tree that was constructed for the car starting system. The circles and diamonds at the bottom of the fault tree represent basic events. Basic events represent the limit of resolution in the fault tree. A circle represents a random hardware failure or human error. A diamond is a basic event that is not developed further and is not a basic failure.

The top level of the fault tree describes the events that are to be considered in the analysis. One method to generate the top event structure is to define success criteria. Failure to meet the success criteria defines the top level events. For example, for a car to successfully start, requires two conditions –

- engine crankshaft rotates as intended

AND

- adequate combustion in all four cylinders.

To generate the top event we take the Boolean complement (change OR to AND gates, vice versa and change success description to failure description). The result is

- Engine crankshaft fails to rotate as intended

OR

- Inadequate combustion in any of the four cylinders.

Note that the success logic is all AND and that the failure logic is all OR.

This logic is shown in the top level OR gate in figure 3. The are two basic failure modes for cranking the engine

1. engine does not adequately crank (type I fault event)

or

2. ring gear fails to disengage (type II fault event).

The fault tree is constructed in a series of steps backwards through the components that are connected in series – i.e., ring gear, starter motor, starter relay, park neutral switch, ignition switch, controller, fuse, power distribution center and battery.

Redundancy/prevention is considered when we consider the battery system. For this system, AND gates are generated. The fault tree for the battery system is shown on page 2 of figure 3. We give credit to jumping the car with a donor battery. In addition, we give credit to the driver to observe warning lights and take action to the service the car to prevent the battery from draining power. In addition, the driver has to ignore warning light alarm in the event that the lights are left on in order to drain the battery.

Failure to achieve adequate combustion is shown on the top of page 2 in figure 3. These four branches are not developed. We can see that the fault tree for the entire car can be quite extensive.

2.6 Qualitative Analysis

Qualitative analysis entails finding the min cut sets. There are a total of 35 min cuts, there are 19 of order 1, 5 of order 2, 3 of order 3 and 8 of order 4. Order refers to the number of basic events in the min cut sets. Min cut sets of order 1 are

single point failures. Note that the failure of the park neutral switch is a single point failure. This is also true for the oxygen sensor – if it fails then the controller will not permit the engine to start. Note that the park neutral switch is a safety device that has an affect on reliability. The same is true for the oxygen sensor. Cut sets of order 2 or higher refer to the battery system failure in which we assume that we give credit for a donor battery.

3.0 Conclusions

In this paper, we conducted a qualitative FTA. The value of the fault tree is that it shows a logical progression of events and ties all the events together to show important system interactions that are not displayed in an FMEA. FMEA can identify undesired events for FTA. FTA can incorporate all the failure modes in a FMEA. FTA uses a graphical format. FTA can consider a wide range of basic events, i.e, failures related to hardware, software and humans. FTA can be used as an engineering design tool.

Acknowledgements:

Dr. Paul Hsieh of Pyramid Associates provided the block diagram in figure 1. He inspired the author to write this paper.

References:

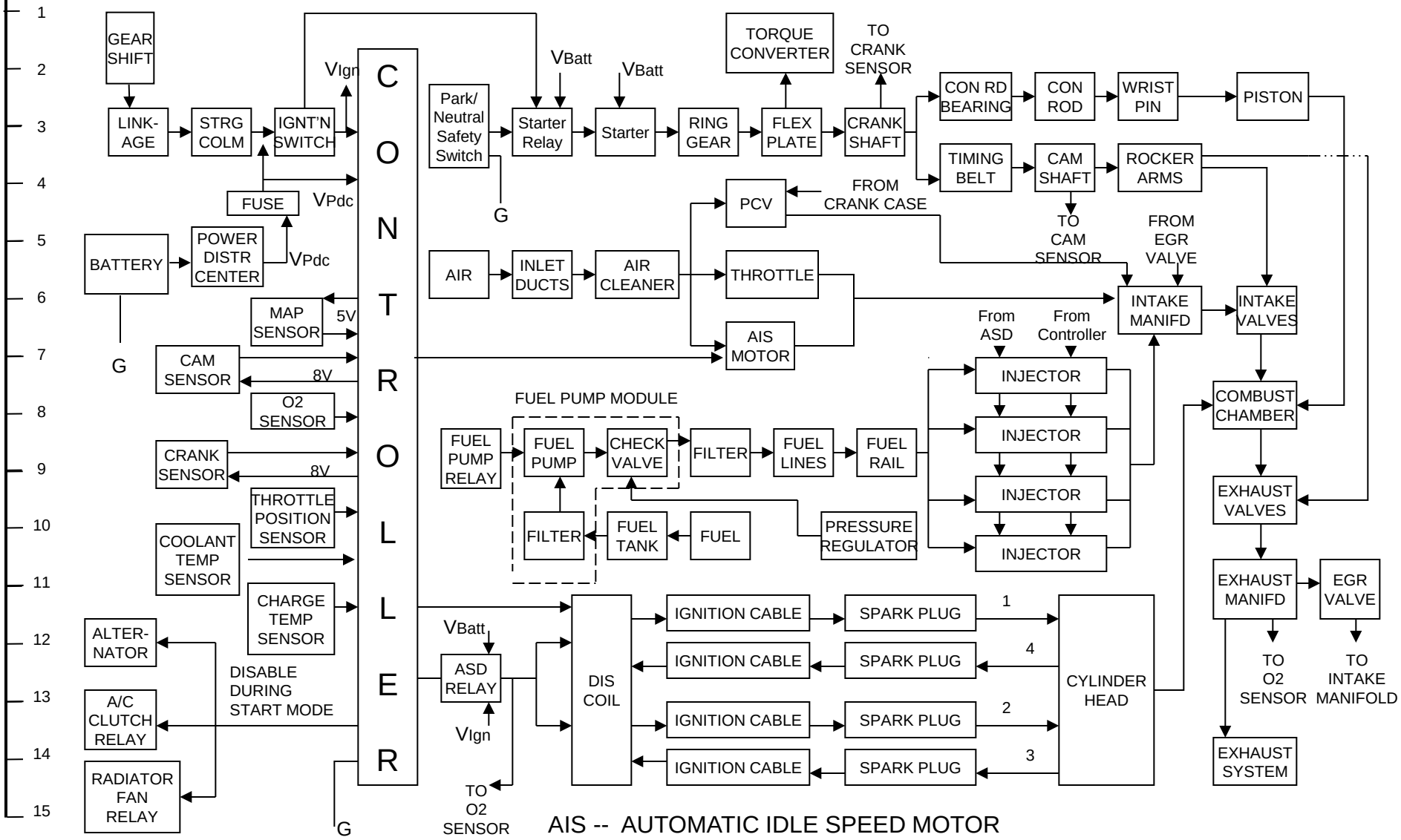
1. Process Failure Modes and Effects Analysis, Chrysler, Ford and Generator Motors.

2. Design Failure Modes and Effects Analysis, Chrysler, Ford and Generator Motors.

3. Dr. Paul Hsieh, Pyramid Associates, Michigan

4. William B. Ribbens, Understanding Automotive Electronics, Society of Automotive Engineers, Butterworth-Heinemann, 1998.

STARTING SYSTEM BLOCK DIAGRAM



AIS -- AUTOMATIC IDLE SPEED MOTOR
ASD -- AUTOMATIC SHUTDOWN RELAY
EGR -- EXHAUST GAS RECIRCULATION

Prepared by P. I. Hsieh
Pyramid Associates
May 22, 2003

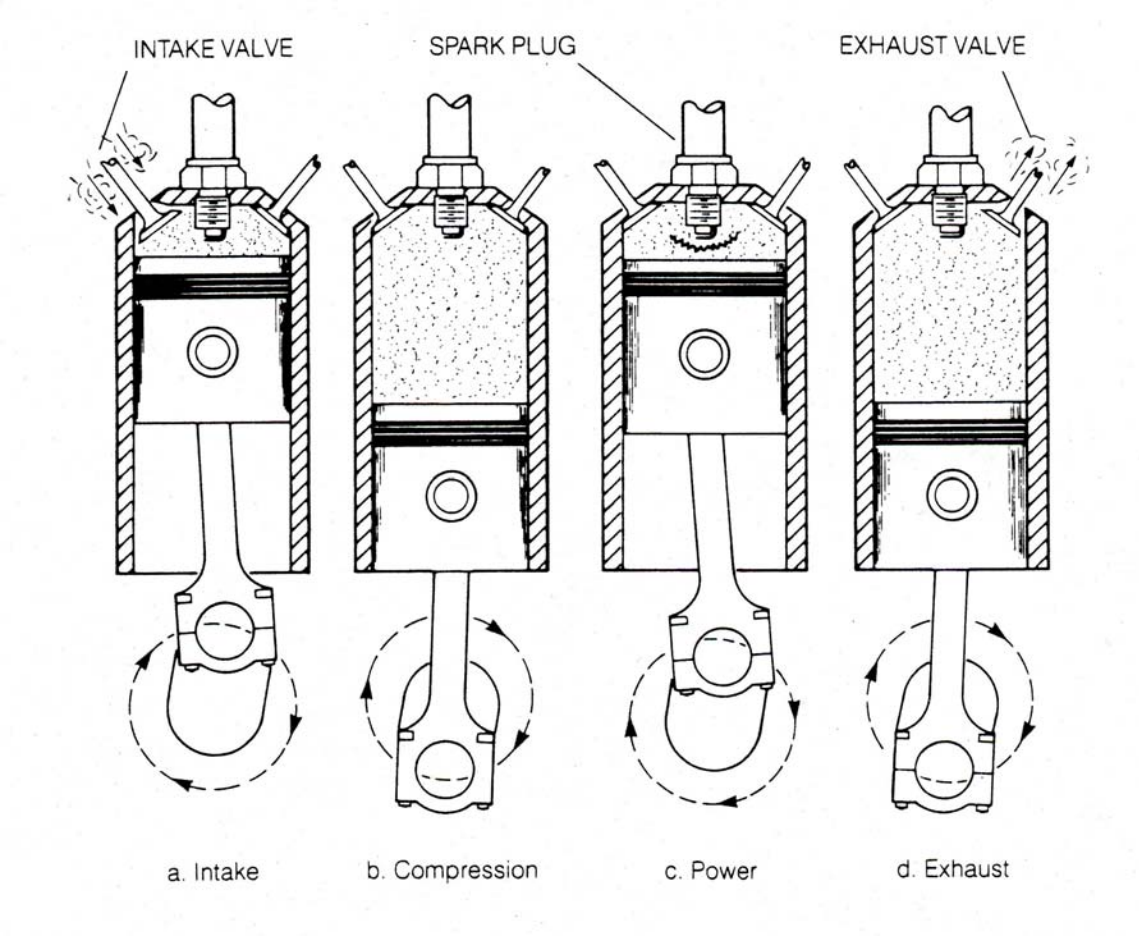


Figure 2 – Four Strokes of a typical Modern Gasoline Fueled Spark Ignition Engine

Figure 3 – Fault Tree for car starting system

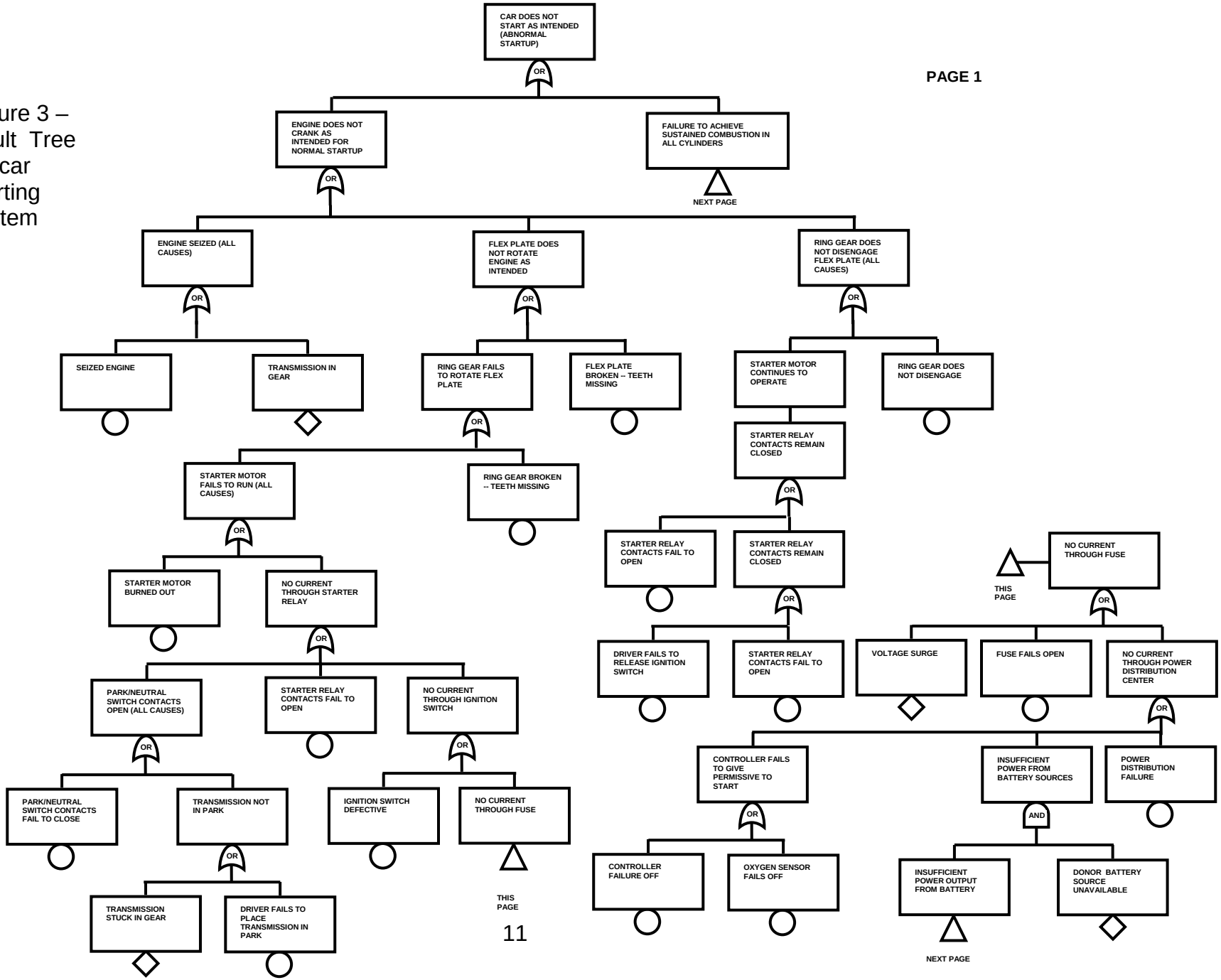
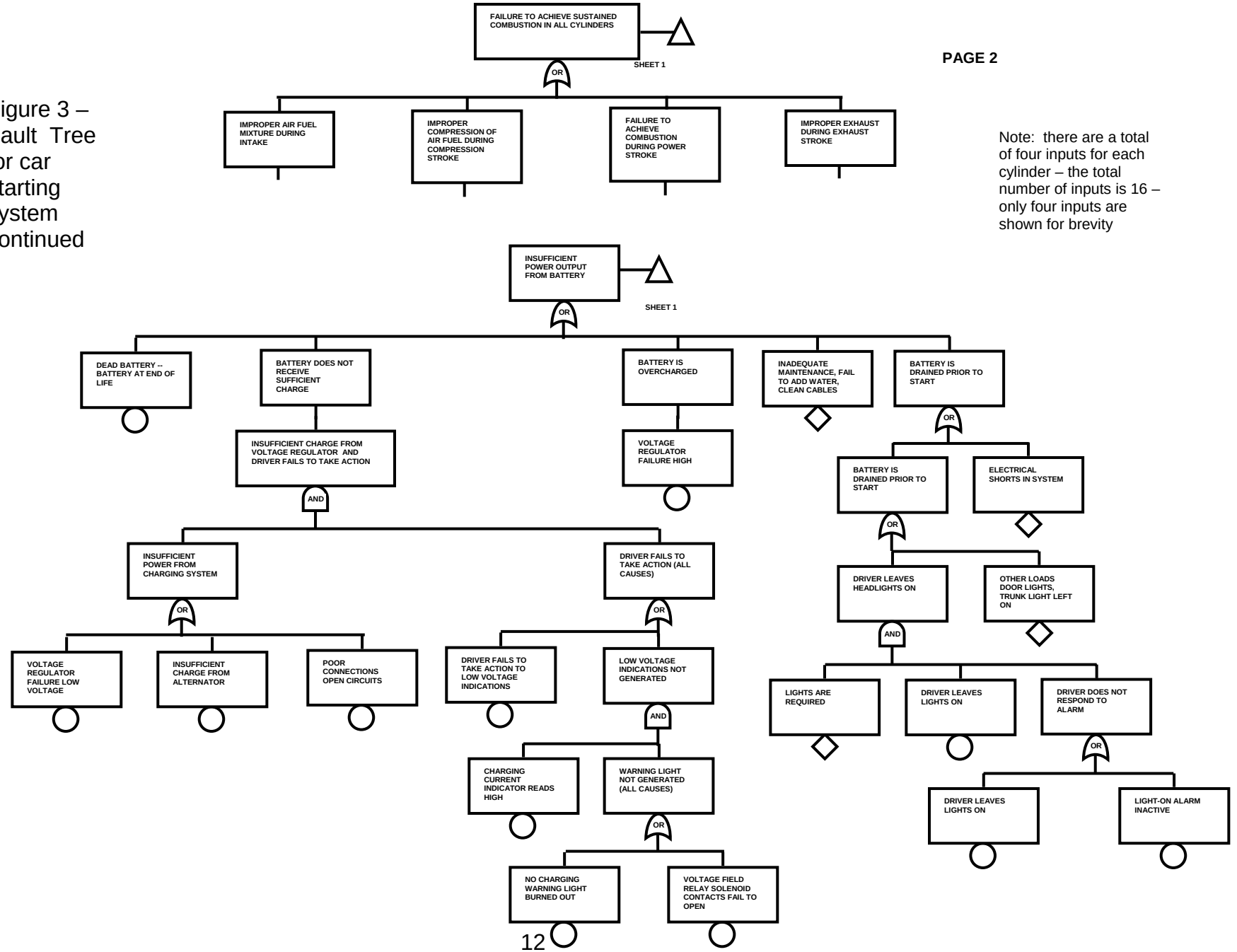


Figure 3 – Fault Tree for car starting system continued



Note: there are a total of four inputs for each cylinder – the total number of inputs is 16 – only four inputs are shown for brevity