THE SAFETY ASSURANCE OF THE AJV8 ELECTRONIC THROTTLE

Ian Kendall MA (Cantab) MSc CEng MIEE

Electrical Engineering, Jaguar Cars Ltd.

ABSTRACT

Electronic throttle is a major innovation of the AJV8 engine in the XK8 vehicle. Although essentially transparent to the driver, it moves Jaguar into new territory, and has often been referred to in the past as "drive-by-wire". Jaguar, in partnership with the Denso Corporation, has developed a system that, while still offering a simple mechanical solution to assuring overall safety, also recognises the importance of the increased criticality placed on computer controls. This paper will discuss both the system safety concepts, and describe the state-of the-art methods that have been used throughout the development of the XK8.

INTRODUCTION

The all new Jaguar AJV8 engine, which powers the XK8, has many new advanced features. Electronic throttle is the application of computer control to replace the traditional mechanical throttle cable, enabling the engine power to by determined electronically, based on sensors that measure driver demand. Hence the term "drive-by-wire".

Generally speaking, computers used to control anything can give rise to two extreme opinions. At one extreme is the view that computers are infallible, and offer vastly superior functionality and intelligence in the way a system behaves - the "technophile's view". The opposing view is that computers are unreliable, and very difficult to diagnose when they go wrong - the "technophobe's view". Which view you take depends on a) what experiences you have had with computers, and b) how much you know about designing computer control systems. When computer control has safety implications, these views can become sharply polarised.

The reality is that computers can, and do, offer greatly enhanced functionality, reliability and safety to many products in everyday use - provided they are designed to do so. This paper offers an insight into the techniques used to provide Jaguar XK8 customers with all the features and performance associated with a computer controlled throttle, while maintaining the very high standard of safety which they are entitled to expect.

Safety can be thought of as an aspect of quality. It has been suggested that if quality is defined as "fitness for purpose" and "meeting the needs of a customer" then a high level of quality also implies a high level of safety. The XK8 electronic throttle therefore needs to exhibit high quality and safety to meet the targets set for the programme. In achieving this, we have relied on several new approaches, along with many tried and tested ones, and subjected everything to independent assessment and audit by Lloyds Register, who are one of the leading safety assurance organisations.

This paper describes the design of the electronic throttle system, the safety features it includes, and the engineering process used to assure the safety and quality.

THE ELECTRONIC THROTTLE SYSTEM DESIGN FOR AJV8

The electronic throttle is an integral part of the engine management system, and is supplied to Jaguar by Denso Corp. according to Jaguar specifications. In the early stages of the project, Jaguar sought the advice of Denso Corp. on how to tackle the issue of safety on such a system. They offered the approach of "evolution" rather than "revolution", which allowed the system to be designed such that that it offers

the benefits associated with electronic throttle, while maintaining the safety characteristics of a conventional mechanical throttle. This is achieved by ensuring the electronics do not have full authority over the movement of the throttle valve blade. The mechanical parts, which are based entirely on current, well understood and accepted designs, provide a physical protection barrier and a limp-home facility. The effect of this is that the electronics cannot give rise to a throttle position far above that which the driver intends.

The electronic part of the system features sensors to measure the driver's demand using the accelerator pedal position; sensors to determine the actual position of the throttle valve blade; an electrical motor which drives the throttle valve blade via a reduction gear; and electronics which are part of the Engine Control Module (ECM). The mechanical components consist of a conventional cable linking the accelerator pedal to the throttle body on the engine, a "mechanical guard", a diaphragm vacuum actuator and associated switching valves and vacuum tank, and several springs. (See Figure 1).

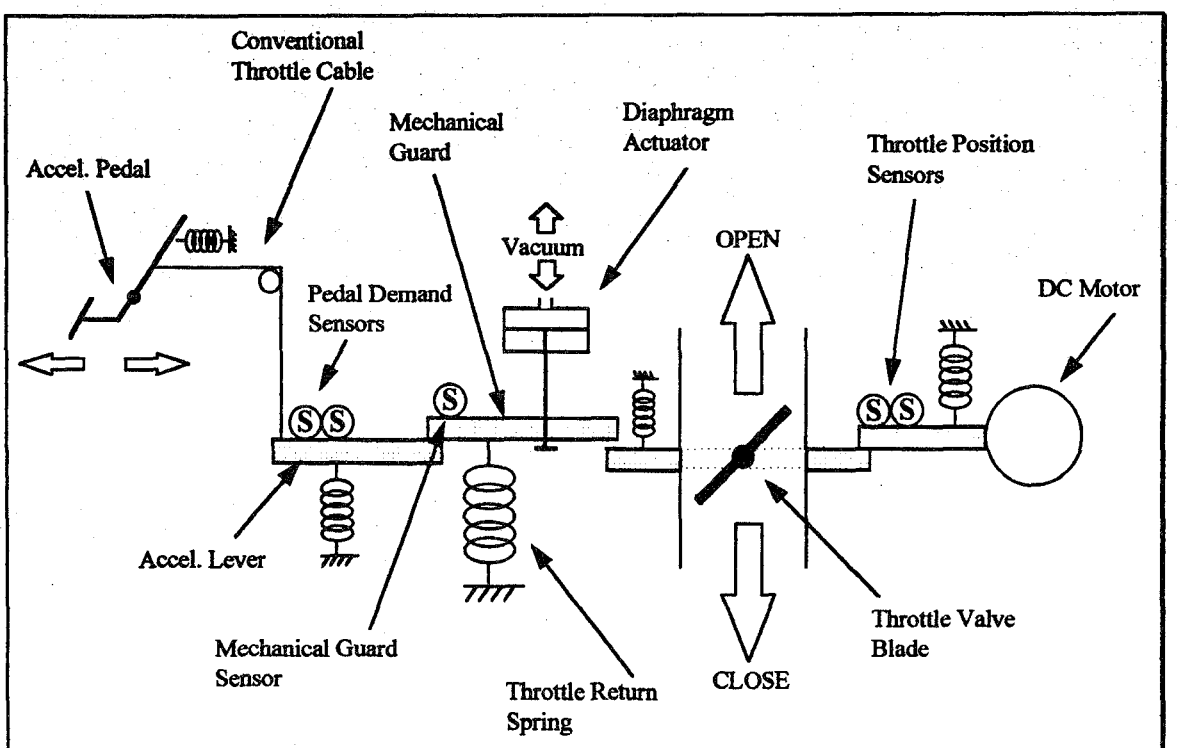

Figure 1 - AJV8 Electronic Throttle Body - Main Components

THE MECHANICAL GUARD

One of the most significant aspects of the electronic throttle design for AJV8 is that it does not seek to replace the mechanical throttle cable, but rather supplements it. The accelerator pedal under the driver's foot is still connected to a cable, and that cable still transfers the physical motion to the throttle body on the engine itself - all totally conventional. However, the motion of the cable does not act directly on the throttle valve blade, it acts on a device we call the mechanical guard. The throttle valve blade, which regulates the amount of air going into the engine, and hence its power output, is actually controlled below the mechanical guard position by an electrical motor. In essence the mechanical guard puts a physical barrier in place, such that the authority of the electronic control is always less than that allowed by the mechanical range. If the driver takes his foot off the pedal, the mechanical guard will close in the same way as a conventional throttle, and except in cruise control (see later), it will always override the electrical motor (i.e. the mechanical guard spring force > the throttle spring force). The mechanical guard therefore plays an essential role in assuring safety by limiting the authority of the

electronic/computer controlled elements, behaving in an obvious and predicable way as in any conventional throttle system.
The mechanical guard, of course, is subject to failure modes the same as any other mechanical component (breaking, jamming, etc.), but these can be predictably analysed for their effects, and monitoring functions provided by the computer can warn the driver before safety is affected. Hence this provides an enhancement of the safety performance of system through the functionality made possible by the electronic control system.

THE CRUISE CONTROL SYSTEM

When the driver selects the cruise control function, the system maintains the vehicle speed at what ever it was at the instant the "SET" button is pressed. The driver can then increase or decrease this using the "ACCEL/INCH-UP" and "DECEL/INCH-DOWN" buttons. The function is usually cancelled by slightly depressing the brake pedal, although there are many other ways in which control can be returned to the driver. Once cancelled, if the "RESUME" button is pressed, the vehicle will return smoothly to whatever the set speed was before it was cancelled.

The cruise function is realised by the electronic throttle, however we have said that the opening of the throttle valve blade is constrained by the mechanical guard. In most circumstances in cruise control, the driver will have his foot off the accelerator pedal, and hence the guard will be closed. This situation is handled by the diaphragm actuator, which uses the inherent vacuum available on the engine inlet manifold to withdraw the mechanical guard, via a series of valves under the control of the ECM. The safety integrity of the electronic throttle in cruise control, is thus a special case. The mechanical guard is not fully opened, but only as far as is required according to the throttle position needed to maintain speed (e.g. it will open more when going up hill, as the throttle must open to provide more engine power). In addition, there are several features that ensure that if the driver cancels the cruise function, the vacuum will be released, allowing the mechanical guard to close. This is achieved with redundant Vacuum Switching Valves, or VSV's, one of which is operated via the ECM control software, the other is directly switched electrical via the brake switch circuit. The circuits and valves are configured such that they always fail safe, i.e. always releasing the vacuum, closing the mechanical guard. (See Figure 2).

FAIL-SAFE DESIGN AND REDUNDANT ARCHITECTURE

The whole electronic throttle is designed such that it always fails safe. This requires that critical components should be supported by redundancy. Redundancy enables the detection of malfunction in one component using the other, and increases system availability. In the case of sensors, it is possible to use one sensor to check the reading from the other (e.g. dual throttle position sensors), or to "vote" the majority if there are more than 2 (e.g. dual driver demand sensors plus the mechanical guard sensor). In some cases it is possible to estimate a value from other related sensor data. For actuators, redundancy can provide back-up that can be used in the event of the primary component failing (e.g. the DC motor and Mechanical Guard/Throttle Return Spring) or be combined such that either or both must operate to produce the required action. In North America, regulations require that there shall be two means of returning the throttle to idle. The XK8 complies with this by considering the Mechanical Guard and Throttle Return Spring as one means, and the DC motor as the other, as both mechanisms can close the throttle even when the other has failed.

The Electronic Control Module (ECM), which contains two 16-bit microprocessors. The throttle is controlled by only one of the processors (actually called the Sub CPU), but the other (the Main CPU,

so called because it manages fuelling and ignition) contains diverse software that monitors the throttle function calculation in the Sub CPU for malfunction.
Other examples of redundancy are:

- Dual circuits within the wiring harness for the DC Motor connections and sensor power and ground connections,
- The power to the DC motor can be cut by switching off the power drive circuit in the ECM or by an external relay,
- Return springs on both the accelerator pedal and the throttle body,
- Dual brake pedal switches, one normally open, one normally closed,
- A total of 31 separate means of cancelling cruise control,
- Two valves that can independently release the vacuum on the diaphragm actuator.

The question that needs to be answered is how can we be sure that we have done everything practical to ensure a safe system. To answer this we need to explore the safety engineering process and how this was supported by Lloyd's Register, who were contracted to oversee and support the design and development activities, both at Jaguar and Denso Corp.

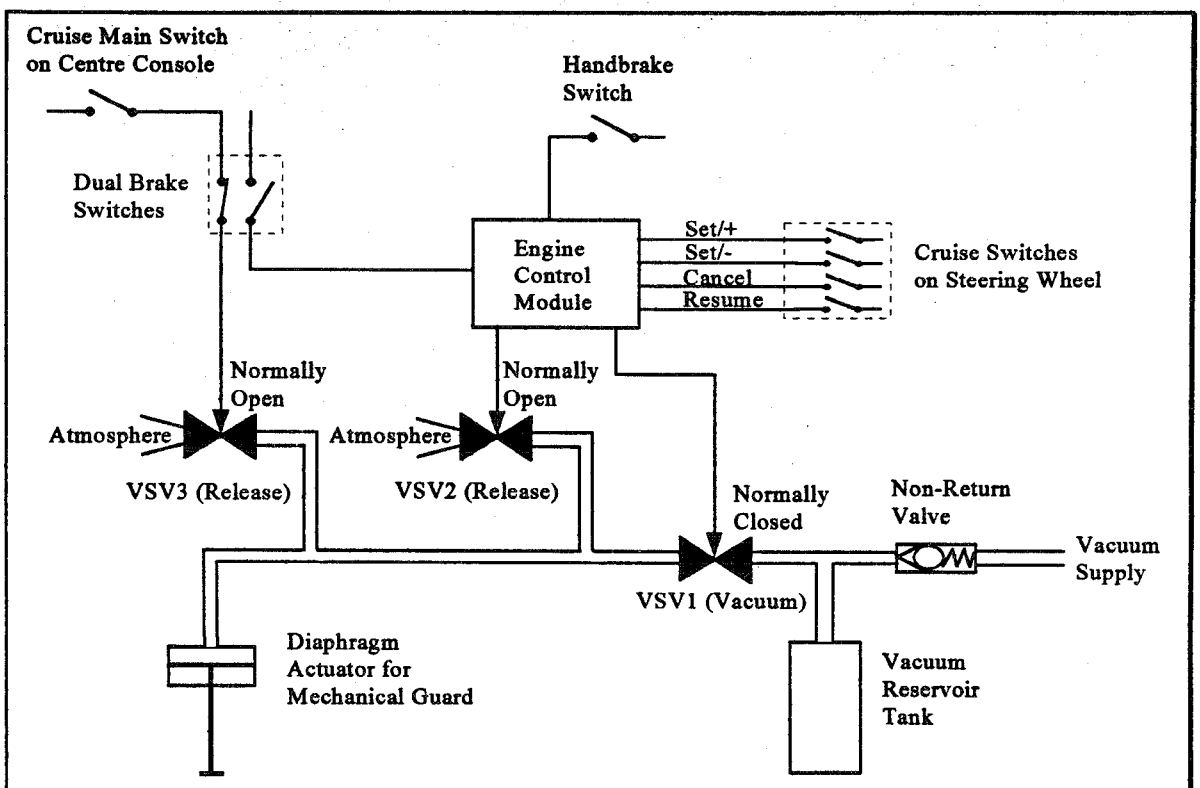

Figure 2 - Cruise Control System - Main Components

THE SAFETY ENGINEERING PROCESS USED ON THE XK8

Around the time work started on the AJV8 engine, the International Electronic Technical Commission published a draft standard on the subject of "Functional Safety", now called IEC 1508 [Ref 1]. It is also noteworthy that, in the UK, the motor industry formed a research consortium (MISRA) which, with DTI funding, published "Guidelines for the development of vehicle based software" [Ref 2]. This focused strongly on safety-related design within the automotive sector. Jaguar was a key member of this group and was keen to use many of the MISRA ideas at the earliest opportunity. Jaguar sought Lloyd's

Register's advice on how to address these emerging standards issues to ensure a state-of-the-art approach on AJV8 [Ref 3]. The remainder of this paper describes the work that has been done to achieve this.

THE SAFETY OBJECTIVES/SAFETY MISSION

In the early stages of the project, Jaguar defined the specific safety objectives for the system. These we based on IEC 1508 that identifies 4 classes of risk, which are known as: Class I (Intolerable), Class II (Undesirable), Class III (Tolerable) and Class IV (Negligible). Class I therefore represents the highest, intolerable, risk, and Class IV represents the lowest possible risk. The concept of a risk-based approach uses the principle that risk is a combination of how serious an event is, and the chances of it happening, i.e. RISK = SEVERITY OF CONSEQUENCES x PROBABILITY OF OCCURRENCE.

The main mission was to design the electronic throttle such that it only had a risk class of IV, i.e. negligible. In order to demonstrate this we had 3 main objectives:

- There shall be no hazardous single point failure modes.
- The likelihood of there being any multiple-point hazardous failure modes, shall be shown to be in accordance with risk class IV (Negligible).
- Any safety-related software is developed to an appropriate standard (appropriate process).

Lloyds Register's role was to assist us in achieving these objectives.

PRELIMINARY HAZARD ANALYSIS

One of the most important safety engineering activities is to identify the potential consequences associated with the failure modes of the system, and to categorise them according to their importance. This is often called Preliminary Hazard Analysis. In IEC 1508, a "hazard" is defined as "a situation with potential for human harm". Our first task to work together with Lloyd's Register and Denso Corp. to list all the situations we could think of which would allow the electronic throttle system to generate a hazard. Each of these was categorised according to the MISRA severity scale [Ref 2] as follows:

- **Uncontrollable**. Failures whose effects are not controllable by the driver. The outcome cannot be influenced by a human response.
- **Difficult-to-control**. Failures whose effects are not normally controllable by the vehicle occupant but could, under favourable circumstances, by influenced by a mature human response.
- **Debilitating**. Failures whose effects are usually controllable by a sensible human response.
- **Distracting**. Failures which produce operational limitations, but a normal human response will limit the outcome.
- **Nuisance**. Failures where safety is not normally considered to be affected.

REVIEW OF INTERNAL STANDARDS AND PROCEDURES

Lloyd's Register were asked to review the design standards, component test specifications, vehicle test specifications, and management procedures at Jaguar and Denso Corp. and to concur that they were suitable for the electronic throttle system. It was concluded that they were in line with the emerging standards and practices in other industry sectors such as defence, and aerospace, which have been tackling complex, safety-related control systems for many years.

AUDITS OF SOFTWARE DEVELOPMENT PROCESS

Lloyd's Register made several visits to Japan to audit Denso Corp. against their software development process to ensure that they were following it. They used "TickIT" methods [Ref 4], which support ISO 9000-3 (specifically for software), however the intention was not to certificate Denso Corp., but to ensure that the software development process was appropriate for this project. This a very important activity as it is well accepted that software cannot to shown to be suitable for is intended use by testing alone, as the number of test configuration combinations which even simple software exhibits becomes very large indeed. Software robustness must be demonstrated by ensuring the process used to develop it is appropriate, and that this process is rigorously followed. This work has proved extremely valuable in ensuring we have the necessary confidence in the software. However, it must be remembered that the software criticality is reduced by the presence of the mechanical guard, which ensures that, if it malfunctions, the throttle opening is restricted to only slightly above the driver's demand on the accelerator pedal.

FAILURE MODES AND EFFECTS ANALYSIS (FMEA)

This technique has been established practice in the automotive industry for many years. The technique is to consider each component in the system, analyse each of its individual failure modes, identify the possible causes, attempt to predict the effect, and recommend design improvement and development action to avoid problems before they happen [Ref 5]. FMEA's can be performed at several different levels of detail. For the electronic throttle system, several FMEA's were performed independently throughout the programme by Denso Corp., by Jaguar and by Lloyd's Register. At Jaguar the analysis is extended to "Failure Mode, Effect and CRITICALITY Analysis" (FMECA). The result of the FMEA's was to demonstrate successfully the safety objective that there shall be no single-points of failure leading to a hazardous state.

FAULT TREE ANALYSIS (FTA)

FTA is inverse of, and is used to complement, FMEA [Ref 6]. Instead of starting with single-point failure modes and working towards the effect, here the starting point is the effect, which for safety analysis is the hazard, and then work down towards all the possible causes. This captures combinations of faults that can lead to a hazard, otherwise known as multiple-point failure modes, as well as confirming that there are no single-point failures. Fault trees were constructed both by Jaguar in the early stages of the project, and later independently by Lloyd's Register, to show that the combinations of faults that had to occur before a hazard arises were highly unlikely. By refining the fault tree analysis down to component failures, we could estimate the probability of a hazard.

MARKOV MODELLING

This was performed by Lloyd's Register as an alternative to the quantified fault tree produced by Jaguar. A Markov model breaks the system into states, the most relevant ones being the "normal" state and the "failed" state, and assigns a probability for moving between states based on the likely reasons for doing so [Ref 5]. The net result is that this technique can also produce an estimate of the probability of a hazard occurring over the design lifetime of the vehicle. Both Jaguar's quantified FTA and Lloyd's Register's Markov Model are used to demonstrate the second safety objective, i.e. that the probability of a hazard was in accordance with risk Class IV (Negligible).

SOFTWARE DOCUMENTATION REVIEW

The software is written by Denso Corp., to Jaguar's specification. Lloyd's Register were asked to review this specification, and the documentation generated by Denso Corp. for both the software requirements and design. The main result was to identify those areas within the software relating to safety, ignoring the fact other system components in the overall design such mechanical guard, provide a higher level of protection. It was also possible to examine these areas of the software in more detail and formulate "Safety Properties" in relation to the hazard analysis mentioned earlier.

PROOF OF SOFTWARE SAFETY PROPERTIES

The safety properties of the software were initially identified in descriptive English text. The word "proof" implies some form of mathematical manipulation that asserts a true fact. Hence, it is first necessary to translate the safety property statements into a mathematical representation that lends itself to manipulation, and secondly to relate this to the software code. This is a highly specialised task, and again we relied on Lloyd's Register's expertise to perform it. They were able to mathematically manipulate of the resulting equations to show whether a property was fulfilled or not. At first, in some instances, a property could not be shown to hold in all conditions, but by reviewing these in detail with Jaguar and Denso Corp. experts on throttle control and vehicle design, it was possible to show that the "exceptions" were all valid conditions that were entirely consistent with design intention.

SAFETY VALIDATION TESTING

Jaguar is responsible for ensuring that the XK8 vehicle meets all the requirements of its test specifications, which in turn are aimed at reflecting customer usage patterns. Throughout the entire programme, even on the first prototypes there is validation. Cars are taken out to Timmins in northern Canada in the winter to do "Cold Environmental Tests", where the temperature is well below -30°C, and to the Arizona desert for "Hot Environmental Tests" where is often exceeds +50°C. We do whole vehicle Electro-Magnetic Compatibility (EMC) test to meet very strict standards as well as all international regulations. We have many tests for durability, driveability, vibration, thermal shock, resistance to fluids, etc. etc. All of this ensures that when the vehicle is signed-off for production, we have been as exhaustive as possible. The electronic throttle gets subjected to all of these vehicle test conditions as it is an integral part of the car. However, we also identified the need to perform specific safety validation tests. The difference is that the majority of the "standard" validation suite considers only normal operation, safety validation must consider the effect of the vehicle under as many failure conditions as is possible to generate. For single points of failure, we aimed to show that each failure would cause the vehicle correctly to enter one of the seven possible default modes. These are:

- Redundancy Mode - no effect at all, driver warning only.
- Cruise Control Inhibited Mode - cruise control function cancelled and disabled.
- Mechanical Guard Mode - Throttle deactivated completely, runs using mechanical guard, and with "fuel intervention" that partially cuts fuel to individual cylinders.
- Full Authority Mode - Mechanical guard failed, throttle still active but with a vehicle speed limit to reflect the loss of safety margin.
- Gearbox Protect Mode - Throttle opening limited to 30 degrees, for gearbox failure and in reverse gear.
- Fixed Idle Mode - Throttle closed to give a "high" engine idle.
- Engine Shutdown Mode - Engine cuts out by stopping fuelling completely.

Jaguar also checked that the correct warning was given to the driver on the instrument cluster, which include "Check Engine", "General Red" and "General Amber" warning lights, together with a text message on the LCD display.

For the multiple failure modes, combinations of the faults were considered. For two point failures this was achieved by combinations of the seven main default modes. Some three-point failures and one four-point failure were also checked.
Lloyd's Register were invited to witness some of the test work, the majority of which was carried out at the MIRA Proving Ground, where each failure situation could be safely evaluated. It was shown that the testing was suitable for its intended purpose in demonstrating the overall safety of the electronic throttle at the vehicle level.

SUMMARY

The aim was to ensure that the electronic throttle on the AJV8 engine in the XK8 has been engineered to a standard of excellence befitting such a feature on a passenger car. We believe that state-of-the-art engineering methods were used to design, analyse, test and assure the system. The main facts to support this claim are:

- Highly capable, world-class quality supplier.
- Robust, high reliability mechanical design, which "guards" the authority of the control system and provides limp-home facility.
- Application of safety engineering techniques, following emerging standards such as IEC 1508 and the MISRA Guidelines.
- Extensive third party expert independent technical assessment and audit.
- Identification and management of potential hazards and technical risks throughout the development.
- The setting of safety targets and ensuring they are met.

The evolutionary design facilitated by the mechanical guard has resulted in a final product that has all the benefits of advanced computer controls, while maintaining the high level of safety and predictability of conventional mechanical throttle actuation.

REFERENCES

1. IEC1508 (Draft). Functional Safety: Safety Related Systems. The International Electrotechnical Commission. June 1995.

2. Guidelines for the Development of Vehicle Based Software. The Motor Industry Software Reliability Association. MIRA, Nuneaton. November 1994.

3. Safety: A Modern Approach for Modern Vehicles. R S W Allen, A C Ashworth and W A Hoskins, Lloyds Register, UK. C498/1/178. Proceedings from Autotech 95, IMechE.

4. The TickIT Guide. A Guide to Software Quality System Construction and Certification using ISO 9001:1994. The DISC TickIT Office, London. 1995.

5. Failure Mode and Effects Analysis Handbook. Automotive Safety and Engineering Standards. Ford Motor Company, 1995.

6. Reliability and Risk Assessment. J.D. Andrews and T.R. Moss. Longman Scientific and Technical. 1993.

ACKNOWLEDGEMENTS

The author would like to thank all involved at Denso Corp. and at Lloyd's Register for the excellent work described in this paper.