

# **Is there a Role for Third Party Software Assessment in the Automotive Industry?**

Roger Rivett  
Rover Group Ltd.

## **Abstract**

The use of third party assessment for software intensive safety related systems is often suggested by standards for higher integrity level systems. A recent European Esprit project, CASCADE, (Certification and Assessment of Safety-Critical Application Development) has devised a new assessment method addressing the certification and assessment of software intensive safety critical systems in the railway and automotive industries. While there has been much interest from the railway industry in the new method, this has not been the case within the automotive industry. This paper describes the automotive environment with regard to market, legislation, safety and validation and explains how these factors affect the use of third party validation for software based systems.

This report reflects work which is partially funded by the Commission of the European Communities (CEC) under the ESPRIT III programme in the area of Information Processing Systems, project no. 9032: "Certification and Assessment of Safety-Critical Application Development".

## **1 Introduction**

CASCADE (Certification and Assessment of Safety-Critical Application Development) is a multi-national project funded by the CEC under the ESPRIT III programme. CASCADE is addressing the certification and assessment of software intensive safety critical systems in the railway and automotive industries. [CASCADE]

The principal deliverable of CASCADE is the Generalised Assessment Method (GAM) for assessing software intensive safety critical systems. The GAM is

concerned with both process and product evaluation and addresses the following issues:

- Assurance of the correct integrity level of safety critical software.
- The role of a safety case and its contents.
- The types of demonstration (testing, proof, audit, inspection, etc) to be used for the assessment of safety-related software.
- The procedures, methods and techniques for software assessment.
- Common criteria and rules to adopt.
- Application proof of conformity to the relevant standards for certification purposes.

As the electronic and software content of vehicles is increasing it would seem that there is a need within the automotive industry for such a method. However it is apparent that there is less interest in the work of CASCADE in the automotive industry than in the railway industry.

This paper seeks to present an overview of the automotive industry and explain the legal, marketing, and design environment within which it operates. In particular the following topics are discussed:

- (i) The legal framework under which the automotive sector operates.
- (ii) Road transport safety issues.
- (iii) The general nature of the automotive market.
- (iv) The software content of vehicles.
- (v) The approach to software development and vehicle validation used in the automotive industry.

From this analysis the current and future roles of third party software assessment within the automotive industry is discussed.

## **2 The Law (UK Only)**

The first UK Road Traffic Act was passed around 1900. In subsequent years more acts were passed and by 1978 the whole of the UK automotive industry was governed by the Construction & Use Regulations and the Road Vehicle Lighting Regulations, two very slim volumes. Up to 1978, except for buses and London black cabs, the legislation applied to the driver of the vehicle, not the manufacturer.

### **2.1 1963: UN ECE 1958 Agreement**

In 1963 the UK signed the UN ECE 1958 Agreement on motor vehicle equipment and parts.

The Agreement was produced in 1958 by the United Nations Economic Commission for Europe, based at Geneva, in order to facilitate free trade in Europe. It was considered necessary because many countries had produced road traffic laws which, while broadly similar, were not identical and not recognised outside of their own national boundaries. This meant that motor manufacturers had to produce different versions of their vehicles for each different country.

The Agreement, which relates to parts and equipment for motor vehicles, is based on reciprocal recognition by signatory countries of approvals of motor vehicle parts included in the Agreement.

Since 1958 more and more countries have become signatories and the scope is European in its widest geographical sense, e.g. includes Russia and former communist countries. Currently there are about 28 signatories.

The agreement now includes approximately 100 different regulations. The parts and systems covered are wide-ranging and include lights, noise, radio interference, locks, exhaust emissions, seats, brakes and even motor-cycle riders' helmets and advance warning triangles. Some of them concern motorbikes, trucks or buses.

## **2.2 1978: Type Approval (Great Britain) Regulations**

As a result of becoming a member of the European Economic Community in 1973, in 1978 the UK introduced a type approval system for passenger cars; Type Approval (Great Britain) Regulations 1978.

This was necessary because in 1970 the Council of the European Economic Community adopted Directive 70/156/EEC - Type Approval of Motor Vehicles and their Trailers. This is a framework directive and references 44 partial directives. These partial directives are concerned with particular aspects of the vehicle and are similar to the individual regulations of the UN ECE Agreement.

Although 70/156/EEC is completely separate from the UN ECE Agreement, the two schemes do try to stay technically in step with each other.

The EEC created its own system in order that eventually it could become a means to facilitate free trade in new motor vehicles and new components for motor vehicles between the Member States of the Community.

From 1970 EEC Member States had to recognise type approvals of vehicle systems or components that were granted to any of the partial directives within the Directive 70/156/EEC framework. For political reasons related to the import of vehicles from non EEC countries, the total list of partial directives envisaged when directive 70/156/EEC was made were not all adopted. This is because it would have automatically triggered a whole vehicle type approval system with the Community.

To sell in an EEC Member State from 1970 manufacturers of vehicles have had the options of:-

1. satisfying the national requirements of that Member State alone;

or

2. satisfying the national requirements of that Member State, with some of those being substituted by EEC partial Directives or by any UN ECE Regulation which that Member State had adopted.

Notwithstanding that, from 1992 exhaust emissions Directives had become mandatory requirements across the Community.

### **2.3 1992: European Whole Vehicle Type Approval**

In 1992 the EEC adopted a Directive amending Directive 70/156/EEC which requires that any mass-produced M1 vehicles (passenger vehicles with up to 9 seats including the driver) type approved for sale within the Community after 1st January 1996 comply with that sub-set of the partial directives that apply to M1 vehicles. From January 1998 this requirement for compliance with European Whole Vehicle Type Approval (ECWVTA) will apply to all new mass-produced M1 vehicles sold and registered in the Community.

### **2.4 Type Approval (Homologation)**

Type Approval, also known as homologation, is the process of ratification by a third party that an article, or series of identical articles, meets the legal requirements to which it is subject prior to being placed on the market. The manufacturer, having obtained type approval, is committed to ensure that any further examples of the approved article are built in conformity with the approved type and generally has to attest to each article being in conformity by either applying a special marking to the articles and/or issuing a document, a certificate of conformity, with each individual article.

Another means of having a manufacturer declare that he is manufacturing articles to a particular set of requirements is "self-certification". Here, the manufacturer again attests that the individual articles comply but without there being any prior ratification by a third party. "Self-certification" is the method used in the USA to show compliance with the Federal Motor Vehicle Safety Standards.

It is common, both in markets where type approval applies and where self-certification applies, for the authorities to apply some form of after market sampling to ensure that the manufacturer's attestations of compliance are indeed true.

Type Approval is not unique to the automotive industry, for example it is used within civil aviation and telecommunications. An example of its use in telecommunications is that all telephones have a green stamp stating that the equipment is “approved for connection to telecommunication systems”.

Type Approval works by having regulations which apply to a particular component or system and which state the conditions under which that item is acceptable and how acceptance is to be determined. A manufacturer wishing to Type Approve an item under a particular scheme submits a production representative sample to an approved agent who determines whether or not it meets the regulation. Once a manufacturer has had an item Type Approved it can then be manufactured and sold in any country which is party to the scheme.

The advantage of type approval is that it allows manufacturers to design products and easily obtain approval to sell them in other countries, that is it facilitates free trade.

The details of type approval regulations can vary widely, e.g.:

- number of vehicles required for approval process
- whether approval process consists of checks and/or tests
- whether tests are conducted by the manufacturer or the assessor
- whether tests are conducted at the manufacturer’s premises or the assessor’s
- whether the approval process includes any examination of the manufacturing process

Even if the regulations do not explicitly include any check of the manufacturing process it is implicit that those parts made for production will be the same as those supplied for approval.

Legislation applies at three different levels of detail:

- Some legislation applies to particular components, for example horns, headlights, tyres, seat belts. Typically these components are fitted to many different vehicle models from different vehicle manufacturers. The

legislative requirements can usually be met without them being fitted to a vehicle.

- Some legislation applies to systems, for example braking. These systems often contain components which are subject to individual legislation but which now have to meet installation criteria as well.
- Some legislation applies to the whole vehicle, for example exhaust emissions and electromagnetic compatibility (EMC).

The legislation gives details of what is to be assessed, how the assessment is to be carried out and what constitutes a pass.

While some legislation gives quite detailed mechanical specifications, for example tyre minimum tread depth, none of the current legislation specifically mentions electronic components let alone the software they contain.

The system requirements are given and checked at a system level. Details of how the requirements have been met is outside the scope of the legislation.

The future for type approval schemes is for global harmonisation. This will be in the next century and has to overcome quite large global differences, e.g. self certification in the USA.

## **2.5 Conclusion**

Although there is much legislation with regard to the automotive industry, the current legislation does not require any third party assessment of software. This may reflect the fact that the legislation has largely been put in place to facilitate trade rather than in response to road transport disasters. This is perhaps in contrast to the legislation in other transport sectors.

## **3 Road Transport Safety**

In order to travel safely on the road it is not sufficient to consider only aspects of the vehicle design and construction, but also the design and construction of the road infrastructure, the ability and behaviour of the driver and societal attitudes in general.

Vehicle and road infrastructure design and construction are engineering issues and within these can be seen two

distinct categories of possible safety measures. Firstly there are measures taken to avoid the occurrence of accidents, often referred to as primary safety measures; and secondly measures taken to preserve human life and health in the event of an accident, often referred to as secondary safety measures.

Driver ability and behaviour together with societal attitudes are human factors issues, and while engineering measures can help ameliorate hazards arising from such issues, they can not address the root causes.

### **3.1 Social Aspects**

This relates to general road safety, for example as typified by the British 'Highway Code'. It includes things like the attitude to drinking and driving, the use of seat belts and speed limits. In general, society's attitudes of the day are reflected in legislation enacted by the government. However there is often widespread acceptance of the breaking of some laws, for example speed limits, probably stemming from some unarticulated notion of personal freedom.

### **3.2 Driver Ability/Behaviour**

With current vehicles, the driver is the principal controlling agent and the bulk of the responsibility for safety on the roads lies with them. Ensuring that drivers have sufficient competence and experience is achieved by the use of driving tests which are usually enshrined in government legislation. Driver behaviour is affected by legislation, for example requiring "due care and attention", and by societal pressure to conform to what is acceptable. However the driver remains the safety component with the greatest variability in the road transport system.

### **3.3 Road Infrastructure**

This aspect includes things like road layout design, road surfaces and road traffic signs. Once again the government is responsible for these via legislation or agencies which inspect completed roads. This appears to be the only aspect of the road transport system which regularly uses third party assessment of some sort.

### **3.4 Vehicle Design and Construction**

The vehicle manufacturer takes a whole vehicle approach to safety. This means considering both primary and secondary safety measures, for example:

- primary safety
  - ensuring robustness of design and manufacture
  - provision of good driver visibility
  - provision of good road handling characteristics
  - provision of good steering characteristics
  - provision of good braking characteristics
  - provision of ergonomically designed driver information systems
  - provision of comfortable internal environment
- secondary safety
  - deformation of vehicle body under crash conditions so as to protect the occupants
  - provision of seat belts
  - provision of air bags

In some of these areas the government sets minimum requirements and they are enforced in the ways described above (section 2 *The Law (UK Only)*). However in practice the performance of vehicles far exceeds that required by the regulations due to other pressures for increased safety, described below.

With regard to safety objectives and policies a hierarchical approach is taken. The senior management will set vehicle level objectives. Major sub-systems will then be the responsibility of a chief engineer who prescribes design guidelines and performance criteria for their sub-systems. At a component level the responsibility resides with a component engineer, who will decide the procedures and standards necessary in order to achieve the goals set by their own management. For current systems, the embedded software is contained within a single component and so decisions concerning issues like third party assessment are the responsibility of the component engineer, with help and guidance from company policies, standards and experts.

### **3.5 Pressures For Increased Safety**

Although, strictly speaking, vehicle design and construction is only governed by the Type Approval

regulations the real standards are set by pressure from other sources.

#### *3.5.1 Published reports*

These originate from a variety of sources and their purpose is to inform a potential buyer of how different vehicles compare with each other with regard to safety. Many also campaign for particular measures in advance of legislation.

*Which? Reports.* This is a consumer's magazine in the UK. It performs crash tests, feature specification analysis and design analysis in order to give a model a safety rating.

*Automotive Magazines.* These perform their crash tests on similar vehicles and publish comparative results.

#### *3.5.2 Insurance companies*

These analyse the actual injury related costs on a per model basis and publish the results. The results may affect insurance premiums. In the USA the Insurance Institute of Highway Safety (IIHS) perform their own high and low speed crash tests. Note - current legislation in the USA only requires high speed crash tests.

#### *3.5.3 Governments*

Some governments produce league tables of vehicle safety based on crash statistics from the police and other sources.

#### *3.5.4 New Car Assessment Programme (NCAP)*

This originated in the USA in the early 1980s. Since then Australia has introduced it, followed by the UK in 1995. It is likely that there will be a European community wide NCAP by the year 2000.

In the US scheme a government agency performs crash tests on a group of similar products and publishes the results in buyer's guides. The tests performed exceed the legal requirements and include front direct, front offset and side impacts. The performance of both the vehicle body and the restraint systems are assessed. The purpose of NCAP is to push vehicle crash performance standards ahead of legislation.

### *3.5.5 Competitors*

Each vehicle manufacturer is keenly aware of what safety features its competitors are offering and so comes under pressure to keep pace in order to maintain the same market image in the mind of its customers.

### *3.5.6 Product Liability*

The product liability legislation, which includes the concept of “strict liability”, states that meeting a legal requirement does not absolve the manufacturer of their responsibility. Ever conscious of this fact, the vehicle manufacturers strive to ensure that their vehicles are not vulnerable under this legislation.

## **3.6 Conclusion**

There are four aspects to road safety: design and construction of the vehicle; design and construction of the road infrastructure; the ability and behaviour of the driver; and societal attitudes in general. Of these, the automotive manufacturer can only address the first.

Manufacturers take safety very seriously and are keenly aware of the external pressures for measures over and above those required by legislation. However these external pressures have more bearing on secondary safety measures than primary safety measures. For software, the primary safety measures relate to the robustness of the design. Whereas responsibility for this generally resides with the component engineer, for future systems, with more and more integration by use of vehicle networks, the responsibility may move upwards from the component engineer to system-level chief engineer.

The obvious weak links in the chain at the moment appear to be the driver, whose poor driving is the cause of the majority of accidents, and the attitude of society at large which tolerates the current level of vehicle accidents due to poor driving.

## **4 The Automotive Market**

### **4.1 Market Size**

The automotive market is very large, for example the total number of cars sold throughout the world in 1995 was 34,614,000 [Worldcar 96]. The impact of the

automotive industry on a country can also be very large, for example it may contribute up to a sixth of a country's gross domestic product.

Most automotive manufacturers operate globally, in terms of both manufacturing and marketing. This is necessary to avoid being affected too much by local economic variations. In general, profit margins are low, say less than 2% on average. High investment is required in manufacturing plant. The lead times for new product introduction are high. In order to help cut costs there are collaborative ventures, for example the use of common components. All these factors combine to make the industry very cost conscious with respect to both product development and sales price.

Although the automotive industry is global, it is currently dominated by the three mature markets of West Europe, North America and Japan who together account for about 75% of all world sales( see Table 1).

<b>Market</b>	<b>Sales(1000s)</b>	<b>PercentageO f World Market</b>
West Europe	11,996.90	35%
North America	9,397.10	27%
Asia (inc. Japan)	7,149.10	21%
Latin America	1,963.40	6%
East Europe	1,581.20	5%
Other	2,526.40	7%

Table 1: World Cars Sales 1995 [Worldcar 96]

A mature market is one where car ownership is unlikely to increase much, the majority of cars being bought on a replacement basis only. Little substantial growth is expected over the next 10 years, say only 2-3 % per annum.

## 4.2 Market Segments

All manufacturers divide the market into different segments, for example small cars, medium cars, executive cars. The definitions for each segment vary from manufacturer to manufacturer and from market to market but the figures shown in Table 2 for 1995 are indicative.

<b>Market Segment</b>	<b>Percentage of World Sales</b>
Basic	4%
Small	13%
Lower Medium	23%
Upper Medium	24%
Executive	19%
Luxury	2%
Multi Purpose Vehicle	4%
Leisure	10%

Table 2: World Production by Market Segment 1995  
[Worldcar 96]

## 4.3 Conclusion

Electronic and software systems are usually introduced into the upper medium, luxury or executive segments first, and then migrate into the other segments as they get market acceptance. The higher selling price of the high end vehicle helps cover the costs associated with introducing the new technology. This means that in terms of production volumes the growth of new systems is relatively slow.

Although most aspects of the vehicle have software based systems associated with them (see below) the percentage of vehicles fitted with many of them is small, being restricted to the high end segment vehicles. So future growth for current systems can be expected as they get fitted to lower end segment vehicles and as the overall market grows outside of the mature markets.

## 5 The Product

## 5.1 Current Software Applications

Applications to date have tended to replace or supplement traditional functions, for example see Table 3 (this is not an exhaustive list).

Powertrain Systems	engine management cruise control transmission control
Body Systems	exterior lighting wiper systems central locking security systems electric seat controls electric windows
Chassis Systems	anti-lock brakes active suspension
Other	occupant restraint systems e.g. air bags instrument pack heating and ventilation radio

Table 3: Current software applications

Although the use of electronics is obviously increasing rapidly there does not appear to be any documentation recording this growth or predicting future growth. Some simple analysis is attempted in section 4.3 *Conclusion* above. One figure much used, but un-attributed, is that by the year 2000 the electronic content of a medium-segment vehicle will account for 30% of its value.

Going hand in hand with this growth in electronics is a growth in the use of software, but again this growth has not been documented.

From Table 3 it will be seen that systems which replace or supplement existing functions within the vehicle are approaching saturation point, i.e. there is little scope for new application areas.

## 5.2 Current Integrity Levels

Most of the current systems do not add new hazards to those which can occur anyhow through mechanical failure. For example vehicles have always exhibited the following failure modes: loss of engine power due to lack of fuel; loss of vision due to loss of windscreen wipers or lights; difficulty in steering due to a burst tyre. Most electronic systems controlling these functions do not introduce new hazards.

None of these could be said to be in the highest safety criticality level. Of the current applications it is perhaps only full authority throttle control which introduces new hazards.

As long as systems are confined to the operation of a single vehicle and primary control remains with the driver, the potential for injury to people is confined to that possible for a small number of vehicles carrying up to four or five people. This puts an upper bound on the integrity level of these systems.

So while current vehicle systems are obviously safety related, in the main they are not at the highest integrity levels and the need for third party assessment is correspondingly low, for example a recent draft of IEC 1508 highly recommends assessment by an independent organisation for safety integrity levels 3 and 4, at Automotive Group McGraw-Hill

[IEC 1508].

### **5.3 Future Trends**

While systems have been designed which replace or supplement existing functions, only some of these (e.g. engine management, air bags) are standard fit. The others are only fitted on vehicles sold in the more expensive market segments. So one future trend will be the use of more of these systems on vehicles in more market segments.

A trend which is already well established is the use of networks to connect control systems together. This started with the use of diagnostic buses, e.g. ISO9141, which allow a single point connection between all vehicle systems and the service diagnostic equipment. Other buses, e.g. CAN (Controller Area Network), are being used to pass data between control systems. While

the use of buses does not necessarily create new functionality it does add to the complexity of the design.

Now that existing vehicle functions have been incorporated into software, future growth will be in the development of new functions only made possible by the use of electronics and software. Examples include use of local radar linked to the cruise control to ensure the maintenance of safe stopping distances. Many of these are likely to take advantage of the networking of systems together. Some new functions may arise just out of the ability of control systems to communicate.

The area with the largest potential growth is that of telematics. These are distributed systems involving central computers analysing data about traffic flow, weather conditions, and communicating with many vehicles via road side transponders. It may also involve vehicle to vehicle communication with corresponding modification of vehicle behaviour, with or without driver intervention. These type of systems require a major change to the road infrastructure and will be impossible without government initiatives and support. The current use of vehicle radios which automatically change station for road traffic announcements is perhaps a tentative step in this direction. An internet address for every vehicle is perhaps the future nightmare that awaits us!

#### **5.4 Future Integrity Levels**

Systems which take actions which affect the control of the vehicle without driver intervention are much more likely to be placed in higher safety integrity levels. Similarly, systems which communicate with many vehicles and affect vehicle control, either directly or indirectly, are also likely to be in higher integrity levels.

#### **5.5 Conclusion**

Although the current vehicle systems are in the main in lower integrity levels, future systems are quite likely to be in the higher levels. Therefore the requirement for third party assessment, while currently small, is likely to grow.

## **6 Software Development**

### **6.1 The Developers**

Although some vehicle manufacturers develop their own software, most software is written by component suppliers.

There are several tiers of component suppliers with first tier suppliers sub-contracting to second tier suppliers and so on. Component suppliers with a mechanical background who find they now have to incorporate electronic controllers into their products will often subcontract this work to an electronics company who may then subcontract the software development. The number of suppliers involved in software development is still a small percentage of the total component supplier base.

Like the vehicle manufacturers, many of the first tier suppliers are large international companies which manufacture and sell in all major markets and to all major manufacturers. Some have a very wide product portfolio whereas some tend to specialise. Often the company, or a particular division of a company, will work exclusively for the automotive industry. This reflects the specialised nature of the work, the need for close co-operation between manufacturer and supplier, and the size of the market.

The majority of the component suppliers have a mechanical engineering background reflecting the historical nature of the industry. More recently companies have developed electrical and then electronic engineering skills. Software engineering skills are the most recent and the least widespread. Most staff involved in software development are more likely to be electronic engineers than computer scientists. This does mean that they are able to relate well to high speed real-time applications.

### **6.2 Standards**

#### *6.2.1 ISO9000/TickIT*

In common with many other industrial sectors, there is widespread adoption of the ISO9000 quality standard within the automotive industry. Some manufacturers use the straight ISO9000 standard while others have derived

sector specific versions of it. Once the vehicle manufacturers started to adopt it they then encouraged their suppliers to adopt it. More recently, in the UK, software suppliers are starting to obtain ISO9000 certification under the TickIT scheme. Overall the introduction of the ISO9000 quality standard has had a beneficial effect on all aspects of the automotive business.

#### *6.2.2 MISRA Guidelines*

Published in 1994, the MISRA Guidelines (Motor Industry Reliability Association) represent the current definition of what is “best practice” in the UK for automotive software development and have authority due to the large number of companies and organisations which endorse them. They were produced voluntarily due to an industry perception that it must improve the general standard of its software development and anticipate the potential need for self regulation in the future. The development of the Guidelines was initiated in response to the UK Safety Critical Systems Research Programme, supported by the Department of Trade and Industry and the Engineering and Physical Sciences Research Council.

The MISRA consortium is still active in promoting the Guidelines with both workshops and a user's forum. The Guidelines have had a major impact on promoting good software engineering practice in the automotive industry both in the UK and the wider world.

### **6.3 Conclusion**

As there is no legislative requirement for the use of particular development procedures current practice is very varied.

With the advent of ISO9000/TickIT and the MISRA Guidelines a more standard approach is increasingly being taken. While some suppliers are undoubtedly very good, these are usually first tier suppliers; some of the second and third tier suppliers have greater scope for improvement.

The growing awareness of software standards will also bring greater awareness of the role of third party assessment.

## **7 Vehicle Validation**

The automotive industry is fortunate in being able to perform extensive testing of the finished product which samples the full range of the vehicle's intended application domain. This testing, traditionally known as vehicle validation, is taken very seriously by the automotive manufacturers and a large amount of effort is expended in performing it. Historically software based systems have benefited from this vehicle validation and the good track record of the use of software in the automotive industry probably owes a great deal to this.

This section will give an overview of durability and reliability validation testing, but is not intended to be a comprehensive description. Other tests, which are not going to be elaborated here, are also performed. These are:

- Exhaust Emissions
- Electromagnetic Compatibility (EMC)
- Crash worthiness

It will be seen in what follows that the automotive use of the term “validation” is different to that of the software engineering.

### **7.1 Mechanical Approach to Design & Validation**

The automotive industry is by tradition a mechanical based enterprise. Design proceeds by producing mechanical drawings. These were formerly paper based but are now produced by the use of CAD and supplemented by the use of finite element analysis. Designs are subject to review and FMEAs are performed to check for design correctness and to highlight possible reliability problems. Prototype components are made by machining metal directly. Later on press tools are constructed which produce the production parts.

In order to validate the design the following validation exercises are performed:

- Component validation for functionality, durability & reliability
- Whole vehicle validation for durability & reliability

Typical figures for whole vehicle validation for the introduction of a new vehicle are 5 million miles. In any one year, across the whole of its product range, a company may perform 12-14 million miles (new vehicles, facelifts, etc.). These figures show that this technique is taken very seriously.

## **7.2 Test Configuration Selection**

It is in the nature of the automotive industry to have many variants of each product. These are generated by:

- Model variants, e.g. 3 door, 5 door
- Trim levels, e.g. base model to top of the range
- Customer options, e.g. air conditioning, manual/automatic transmission

This leads to there being hundreds, if not thousands, of possible combinations for the final product. Obviously it is not possible to validate every possible combination so a choice has to be made. Typically only 5 to 10 different vehicle derivatives will be tested. The choice will include those with the largest anticipated sales volume and those which are worst case in terms of the number of components or complexity.

## **7.3 Test Coverage**

For a new model the full validation programme will be performed.

Most models have several model year facelifts during their life. These may be major changes, e.g. different engine fitted, or quite minor relating to the visual appearance only.

The degree to which validation is repeated depends on:

- whether or not it is a carryover component, i.e. already used in production on another model
- the degree to which new technology is being introduced

The powertrain (engine/gearbox/transmission) is considered to be critical and a major change to this is likely to lead to all the reliability tests being repeated.

Other changes are judged on a case by case basis.

## **7.4 Durability Testing**

This tests the structural integrity under normal operation and in crude terms can be said to check that the powertrain does not break and that the body does not fall apart.

Vehicles are built to production specification, but not with production parts, i.e. parts not necessarily manufactured using a production process.

This exercise validates the design of the vehicle. This activity is carried out according to company proprietary standards but it typically involves driving a number of vehicles a total of 100,000 miles.

## **7.5 Reliability Testing**

In contrast to the durability tests which are looking for gross mechanical failures, reliability testing is aimed at achieving reduced customer dissatisfaction and warranty costs.

This is performed on vehicles built with off-tool parts, i.e. parts manufactured using a production process, and effectively validates the manufacturing process.

There are many different types of test which use company proprietary standards and endeavour to simulate 2 years of use. There are three different categories of test: extremes, typical and specific.

## **7.6 Reliability Testing: Extremes**

### *7.6.1 Pavé*

This involves driving the vehicle over various rough road surfaces which has the effect of inducing a wide range of chassis and engine vibrations.

### *7.6.2 High Vehicle Speed*

This has the effect of inducing the maximum oil temperature and engine stress conditions. This particular test represents the majority of the miles driven for reliability testing.

### 7.6.3 Environment

This involves subjecting the vehicle to extremes of ambient temperature, e.g. -40 degrees C and 50 degrees C, and humidity, e.g. water splash tests.

## 7.7 Reliability Testing: Typical

Great effort is put into matching the test conditions with real customer usage profiles and problems that they experience. This information is gathered by:

- Customer Quality Tracking Surveys  
This involves contacting the customer directly during the first 18 months of ownership. Sometimes it is performed on 5 vehicles which are 5 years old.
- buyer surveys
- market research
- instrumenting customer's vehicles and letting them drive for a week while data logging key vehicle parameters. This is often done in the context of fault finding
- analysing warranty return data
- analysing different market requirements.  
This is done on a model by model basis. Even so there is no set usage cycle for a model but each one has a range. For example a 4x4 vehicle may be used as a mobile office by a builder out in all weathers, road conditions and times, or by a teacher who only drives 5 miles a day back and forth to school.

## 7.8 Reliability Testing: Specific tests

Test specifications are supplied by a component area to test a specific aspect of their component. This may be a new technology or design feature or possibly something which arose out of an FMEA.

## 7.9 Problem Reporting & Resolution

Drivers and technicians who perform tests are required to complete logs at the end of the shift. From the shift logs Problem Reports are raised as necessary and sent to the corresponding component area who will investigate and correct the problem. A Problem Report can not be closed down without a sign-off by the Validation area.

A reliability growth curve is produced for each vehicle development phase. There are company standards giving the expected profile and acceptable production values.

### **7.10 Vehicle Validation in the Future**

Greater complexity of vehicle systems will make it harder to test all possible combinations, driving conditions and fault conditions. Therefore all available feedback mechanisms will be used to target the testing most effectively.

The trend will be to use more rig tests, as the component areas do at present, and to focus tests more on customer usage as opposed to tests specified by engineering.

The validation department will be more involved with component areas, participating in design reviews and FMEA exercises, and with manufacturing, performing methods build assessment and failure analysis. This approach will enable validation to be targeted towards the safety-critical aspects of the system.

### **7.11 Conclusion**

Validation activities are taken very seriously and will be targeted more closely to critical parts of the systems, including safety requirements. The question is, will this be sufficient on its own as systems get ever more complex?

## **8 Discussion**

Although there is much legislation with regard to the automotive industry, the current legislation does not require any third party assessment of software. Anticipated work on Type Approval would appear to be concerned with increasing its breadth rather than its depth, so a major impact on third party assessment is unlikely.

As long as society is prepared to tolerate the current level of accidents due to poor standards of driving, any problems that may occur with existing systems will be lost in the noise. Consumer pressure on manufacturers is unlikely to materialise unless an accident does occur that which is directly attributed to software.

The current vehicle systems are in the main at the lower integrity levels. But if telematic systems come into

common use then it is likely that the average safety integrity level will increase. This is because the overall system would then consist of more than a single vehicle, maybe hundreds of vehicles, and the potential for accident severity would start to approach that of civil aircraft or railways.

With the advent of these type of telematic systems even comprehensive validation activities will need additional measures to ensure adequate safety levels.

## **9 Conclusion**

Is there a Role for Third Party Software Assessment in the Automotive Industry?

There is a small role at the moment for the highest integrity level systems, for example full authority throttle control.

Where new systems take away more of the primary control from the driver, or connect more than one vehicle together in a manner which affect vehicle control, then the role for third party assessment will increase, possibly becoming mandatory for the worst case automatic or multi-vehicle systems.

The need for third party assessment will be driven by the higher integrity levels involved and the inability of traditional vehicle validation to provide sufficient confidence.

Legislation may follow but this is not obvious at the moment.

## **References**

[CASCADE] CASCADE Summary.  
Ricardo Hetherington (Lloyd's Register).  
February 7 1996, ref. CAS/LR/RHZ/R480/2 - Public.

[Worldcar 96] World Car Industry Forecast Report,  
February 1996.  
Data Resource Inclusive, Global Automotive Group  
McGraw-Hill

[IEC 1508] Draft IEC 1508 - Functional safety: safety-related systems - June 1995. Ed.1  
Geneva: International Electrotechnical Commission (IEC reference 65A Secretariat 123)