TECHNICAL REPORT

ISO/TR 15497

First edition
2000-11-01

Road vehicles — Development guidelines for vehicle based software

Véhicules routiers — Guide pour le développement de logiciels installés à bord de véhicules

Reference number
ISO/TR 15497:2000(E)

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.ch
Web www.iso.ch

Printed in Switzerland

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 3.

The main task of technical committees is to prepare International Standards. Draft International Standards adopted by the technical committees are circulated to the member bodies for voting. Publication as an International Standard requires approval by at least 75 % of the member bodies casting a vote.

In exceptional circumstances, when a technical committee has collected data of a different kind from that which is normally published as an International Standard ("state of the art", for example), it may decide by a simple majority vote of its participating members to publish a Technical Report. A Technical Report is entirely informative in nature and does not have to be reviewed until the data it provides are considered to be no longer valid or useful.

Attention is drawn to the possibility that some of the elements of this Technical Report may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights.

ISO/TR 15497 was prepared by the United Kingdom Motor Industry Software Reliability Association (MISRA) as guidelines published in 1994, and was adopted (without modifications except those stated in clause 2 of this International Standard) by Technical Committee ISO/TC 22, *Road vehicles*, Subcommittee SC 3, *Electrical and electronic equipment*.

Road vehicles — Development guidelines for vehicle based software

1 Scope

This Technical Report provides safety-related guidelines for the development of vehicle based software.

2 Recommendations

The technical recommendations are those made in the following publication (reproduced on the following pages), which is adopted as a Technical Report:

Development Guidelines for Vehicle Based Software, Motor Industry Software Reliability Association (MISRA), United Kingdom, 1994.

For the purposes of international standardization, the modifications outlined below shall apply to the specific clause and paragraphs of the MISRA publication.

Page i to iv (of the MISRA publication)

This is information relevant to the MISRA publication only.

Page 73-75

Clause 6

Substitute the following for the corresponding references.

[10] ISO 9001, *Quality systems — Model for quality assurance in design, development, production, installation and servicing*.

[15] ISO 11748 (all parts) —[1)], *Road vehicles —— Technical documentation of electrical and electronic systems*.

[25] ISO 11898, *Road vehicles — Interchange of digital information — Controller area network (CAN) for high-speed communication*.

[26] ISO 11519 (all parts), *Road vehicles — Low-speed serial data communication*.

[29] ISO 14230 (all parts), *Road vehicles — Diagnostic systems — Keyword Protocol 2000*.

Insert the following reference.

[24] EMC standards and technical reports applicable to road vehicles:

ISO 7637 (all parts), *Road vehicles — Electrical disturbance by conduction and coupling* ;

ISO /TR 10305, *Road vehicles — Generation of standard EM field for calibration of power density meters from 20 kHz to 1 000 MHz* ;

ISO/TR 10605, *Road vehicles — Electrical disturbances from electrostatic discharge* ;

1) To be published.

ISO 11451 (all parts), *Road vehicles — Vehicle test methods for electrical disturbances by narrowband radiated electromagnetic energy* ;

ISO 11452 (all parts), *Road vehicles — Component test methods for electrical disturbances by narrowband radiated electromagnetic energy*.

3 Revision of the MISRA publication

It has been agreed with the Motor Industry Software Reliability Association that ISO/TC 22/SC 3 will be consulted in the event of any revision or amendment of the MISRA publication. To this end, the British Standards Institution (BSI) will act as a liaison body between MISRA and ISO.

First published November 1994
by The Motor Industry Research Association
Watling Street
Nuneaton
Warwickshire
CV10 0TU

http://www.misra.org.uk

ISBN 0 9524156 0 7

British Library Cataloguing in Publication Data.

A catalogue record for this book is available from the British Library.

The Motor Industry Software Reliability Association

Development Guidelines For Vehicle Based Software

November 1994

Foreword

As coordinator of the Safety Critical Systems Research Programme, supported by the Department of Trade and Industry and the Engineering and Physical Sciences Research Council, I am pleased to support the publication of these guidelines.

In this programme we have been concerned to ensure that the results of research should not be buried in learned papers, but promulgated in ways which will affect practice in industry. We have therefore sought the involvement of user organizations so that the work based on an understanding of their real industrial needs, and so that the results will be credible to their peers. The MISRA Study, with its combination of vehicle and equipment manufacturers, has admirably realized that ambition.

The voluntary nature of the guidelines is important. They were produced voluntarily, for the benefit of both the industry and the public. Their adoption will also be voluntary. This has encouraged the MISRA consortium to develop guidelines which offer genuine benefits for their users, rather than burdensome restrictions.

The renowned cost-consciousness of the automotive industry might be thought by some to diminish its contribution to technological development. On the contrary: while this industry is properly cautious in the interests of safety, the fiercely competitive market and the public exposure of any problems ensures that the commercial value of new technology is thoroughly evaluated. This sector is a hard proving-ground for technology. So, while many of the issues on which the MISRA consortium has concentrated are specific to vehicles, other sectors might do well to see what they might glean from the trends here.

Bob Malcolm
DTI-EPSRC Safety Critical systems

Foreword (continued)

The motorist gains many benefits, including enhanced safety features, from advances in vehicle electronics.

The development of software is a specialized and often complex area where much relies on an effective approach by those directly involved. I welcome MISRA's initiative and efforts in developing these safety related guidelines and advice under a joint DTI, EPSRC and industry funded programme. The guidelines reflect a responsible and serious industry attitude to safety issues.

Malcolm Fendick BSc CEng FIMechE
Chief Mechanical Engineer
Department of Transport

The use of electronic systems in vehicles has increased significantly over recent years and will continue to increase. Much time and resources are being committed by vehicle manufacturers to deal with the compatibility of such systems in particular the problem of interference from external sources.

The vehicle owner expects his vehicle to be reliable and safe, and this includes the electronic systems. Electronic systems are dependent on the software provided by the manufacturer. The greater complexity of such systems is increasing the need to maintain software quality and reliability. This has resulted in the need for a unified approach to software design. It is therefore pleasing that an independent group has produced these guidelines on vehicle-based software which will be of benefit to the Motor Industry and also more importantly the motorist.

K B Barnes
Head of Engineering
SMMT

Acknowledgements

The MISRA consortium would like to thank the following organizations for their support of the study that produced these Guidelines:

AB Automotive Electronics Ltd	(CM)
AP Borg & Beck	(CM)
Delco Electronics	(CM)
Department of Trade and Industry	
Department of Transport	
Ford Motor Company Ltd	(CM)
Jaguar Cars Ltd	(CM)
Lotus Engineering	(CM)
Lucas Electronics	(CM)
Rolls-Royce and Associates Ltd	(C)
Rover Group Ltd	(CM)
The Centre for Software Engineering Ltd	(C)
The Motor Industry Research Association	(PM, C)
The Society of Motor Manufacturers and Traders Ltd	
The University of Leeds	(C)

Key

CM	controlling member of the MISRA consortium
PM	project manager
C	consultant

The MISRA consortium would like to thank the following individuals for their contributions to these Guidelines:

Alex Abbot	Vivien Hamilton	Frank O'Neill
Klaus Allen	Nick Heatley	Dave Perry
Neil Andrewartha	Keith Hobley	Mike Radford
Nigel Barrett	Peter Jesty	Roger Rivett
Terry Beadman	Edward Jones	Steve de la Salle
Nick Bennett	Ian Kendall	Chris Shakespeare
Colin Bowles	Keith Longmore	Heather Storey
Tom Buckley	Paul Manford	Ian Stothers
John Comfort	Chris Marshall	Lloyd Thomas
Nick Dunn	Josh McCallin	David Ward
Paul Edwards	Tom Monk	Brian Whitfield
Simon Farrall	Tony Moon	Anthony Wood
John Fox	Dave Newman	Marco Zasiura

Contents

Contents (continued)

1. Introduction

1.1 Statement of mission and objectives

1.1.1 The purpose of these Guidelines is to provide assistance to the automotive industry in the creation and application within a vehicle system of safe, reliable software.

1.1.2 There has been much recent growth in the quantity and complexity of electronic controls on motor vehicles. The greater the complexity, the harder it is to maintain the software quality and reliability the customer has come to expect. A unified approach to software development, using agreed techniques, is desirable across the automotive industry. This will enable the driver or owner to have continued confidence in complex electronic systems.

1.2 Benefits to the end customer

1.2.1 The public exposure to software in applications with safety implications is increasing. It may be through vehicles that the majority of the public will encounter such software. Therefore, it is vital that such software is both correct and perceived to be correct.

1.2.2 The record of the automotive industry in regard to software is good. The application of these Guidelines will maintain the industry's confidence in the quality of the software used in its products as the complexity increases.

1.3 The MISRA consortium

1.3.1 The MISRA consortium was formed 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, and consisted of eight controlling members, four consultants and a project manager (see Acknowledgements page).

1.3.2 The consortium initially conducted a survey of existing work, both in the automotive sector and in other industrial sectors.

1.3.3 The consortium then formed eight subgroups to research specific issues relating to automotive software:

- diagnostics and integrated vehicle systems
- integrity
- noise, EMC and real-time
- software in control systems
- software metrics
- verification and validation
- subcontracting of automotive software
- human factors in software development.

Introduction (continued)

1.3.4 Each group produced a report [1]–[8] that provides more detailed supporting information, and recommendations that have been incorporated into these Guidelines.

1.3.5 The results of the survey were continually updated throughout the study [9].

1.3.6 The eight reports and the survey report are available separately [1]–[9]. These reports provide additional background, more detailed recommendations and additional references that will be invaluable to the specialists in the field.

1.3.7 For the sake of brevity, the Guidelines do not always justify recommendations. The eight reports [1]–[8] contain the background material and justifications where appropriate.

1.4 Background

1.4.1 There are important differences between software and other forms of automotive engineering and components:

(a) Software is primarily a design, with no manufacturing variation, wear, corrosion or ageing aspects.

(b) It has a much greater capacity to contain complexity.

(c) It is perceived to be easy to change.

(d) Software errors are systematic, not random.

(e) It is intangible.

1.4.2 There are differences between automotive applications and applications in other industrial sectors:

(a) Production volumes are high (leading to manufacturing variation), related mechanical components are subject to wear and maintenance levels are difficult to assure. Therefore automotive software has an emphasis on data driven algorithms, parameter optimization, adaptive control and on-board diagnostics.

(b) Passenger car drivers receive little or no training compared with other users of computer-based products and services. Therefore automotive software requires an emphasis on failure management techniques based on the controllability of the vehicle.

(c) Traditional automotive test environments use real vehicles and components, as well as simulations. These are available to test systems and software extensively and safely before they reach the customer.