



Developing advisory software to comply with IEC-61508

Prepared by **Adelard**
for the Health and Safety Executive

**CONTRACT RESEARCH REPORT
419/2002**



Developing advisory software to comply with IEC-61508

P Froome & C Jones
Adelard
Drysdale Building
Northampton Square
London EC1V 0HB
United Kingdom

This report gives constructive technical guidance on how to develop advisory software so as to achieve compliance with IEC 61508 “Functional safety of electrical/electronic/programmable electronic safety-related systems”.

This guidance defines the scope of a limited class of safety-related advisory software, explains in a software context what IEC 61508 is trying to achieve at each key point of the safety lifecycle.

Two practical illustrations are given of quality management procedures to collect compliance evidence. The first is a quality management system (QMS) which is 3rd party certified to ISO 9000-3. The second recognises that many software developers will not have a 3rd party certified QMS, and even fewer specifically for software development.

This report and the work it describes were funded by the Health and Safety Executive (HSE). Its contents, including any opinions and/or conclusions expressed, are those of the author alone and do not necessarily reflect HSE policy.

© Crown copyright 2002

Applications for reproduction should be made in writing to:
Copyright Unit, Her Majesty's Stationery Office,
St Clements House, 2-16 Colegate, Norwich NR3 1BQ

First published 2002

ISBN 0 7176 2304 1

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording or otherwise) without the prior written permission of the copyright owner.

FOREWORD

This report gives technical guidance to software developers on how to comply with IEC 61508, but solely for the limited class of safety-related advisory software. Explicitly excluded is software that has any degree of online control over machinery or plant. This guidance should be used in conjunction with IEC 61508.

It is recommended that developers familiarise themselves with “The Engineer’s Responsibility for Computer Based Decisions”, published by The Institution of Chemical Engineers, Geo. E. Davis Building, 165–171 Railway Terrace, Rugby, CV21 3HQ, UK.

The developer’s goal is to produce advisory software of demonstrable safety integrity, assessed on the basis of recorded evidence that the requirements of IEC 61508 have been met. An explicit quality management approach is recommended to facilitate the systematic gathering of compliance evidence to make possible the assessment of software safety integrity. The developer will need to develop suitable quality management procedures, or adapt existing procedures, to ensure that the evidence, illustrated in Appendices 1 and 2, is collected in a manner suitable for the assessment process.

HSE invites comments on the practicality and effectiveness of the recommended approach, and on any other significant aspect of the safety integrity of advisory software. Please send your comments to

Edward Fergus
Technology Division
357 Magdalen House
Stanley Precinct
Bootle
Merseyside
L20 3QZ.

CONTENTS

FOREWORD	iii
CONTENTS	v
EXECUTIVE SUMMARY	vii
1. ADVISORY SOFTWARE.....	1
1.1 SAFETY ASPECTS OF ADVISORY SOFTWARE	1
1.2 CHARACTERISTICS OF ADVISORY SOFTWARE	1
2. IEC 61508 FUNDAMENTALS, AND ADVISORY SOFTWARE	3
2.1 FUNCTIONAL SAFETY, SAFETY INTEGRITY, AND sil.....	3
2.2 FUNCTIONAL SAFETY OF AN ADVISORY SOFTWARE SYSTEM.....	4
2.3 SIL ASSESSMENT	4
2.4 THE SOFTWARE DEVELOPER’S ROLE IN SIL ASSESSMENT.....	5
3. THE ORGANISATION OF IEC 61508.....	7
3.1 MANAGING AND ASSESSING FUNCTIONAL SAFETY	7
3.2 HARDWARE ISSUES FOR ADVISORY SOFTWARE.....	8
3.3 THE IEC 61508 SAFETY LIFECYCLE	8
4. PLANNING AND ASSESSING FUNCTIONAL SAFETY	15
5. SOFTWARE QUALITY MANAGEMENT	17
6. DOCUMENTATION.....	19
7. COMPLIANCE MATRIX	21
Appendix 1: IEC 61508 compliance illustrated using a certified QMS	23
Appendix 2: IEC 61508 compliance using a non-certified or non-software QMS.....	33
Appendix 3: Generic SIL assessment of advisory software	45

EXECUTIVE SUMMARY

The Health and Safety Executive both develops safety-related software internally and also commissions software from external developers. Safety-related software must achieve an adequate standard of safety integrity. HSE has adopted the international standard IEC 61508 “Functional safety of electrical/ electronic/ programmable electronic safety-related systems” as one acceptable criterion of safety integrity.

This report relates to a limited class of software – an offline advisory system which assists a human expert in some well defined way to assess risk arising from a hazardous industrial installation or activity.

The Health and Safety Executive has developed technical guidance to indicate to developers how to comply, for this limited class of software, with IEC 61508 to achieve adequate software safety integrity.

Two detailed illustrations are given of how to use quality management procedures to collect compliance evidence. The first uses a quality management system (QMS) which is 3rd party certified to ISO 9000-3. The second recognises that many software developers will not have a 3rd party certified QMS, and even fewer specifically for software development. Dr. Peter Froome and Dr. Claire Jones of Adelard provided these two illustrations and the “safety justification” documentation scheme, based on Adelard’s practical experience of developing and assessing high integrity software.