GUIDANCE ON ASSESSING THE SAFETY INTEGRITY OF ELECTRICAL SUPPLY PROTECTION

GUIDANCE ON ASSESSING THE SAFETY INTEGRITY OF ELECTRICAL SUPPLY PROTECTION

September 2006

Published by
ENERGY INSTITUTE, LONDON
The Energy Institute is a professional membership body incorporated by Royal Charter 2003
Registered charity number 1097899

The Energy Institute gratefully acknowledges the financial contributions towards the scientific and technical programme from the following companies:

BG Group
BHP Billiton Limited
BP Exploration Operating Co Ltd
BP Oil UK Ltd
Chevron
ConocoPhillips Ltd
ENI
ExxonMobil International Ltd
Kuwait Petroleum International Ltd
Maersk Oil North Sea UK Ltd
Murco Petroleum Ltd
Nexen
Shell UK Oil Products Limited
Shell U.K. Exploration and Production Ltd
Statoil (U.K.) Limited
Talisman Energy (UK) Ltd
Total E&P UK plc
Total UK Limited

ISBN 9780 85293 468 8
Published by the Energy Institute

Further copies can be obtained from Portland Customer Services, Commerce Way,
Whitehall Industrial Estate, Colchester CO2 8HP, UK. Tel: +44 (0) 1206 796 351
email: sales@portland-services.com

CONTENTS

Contents Cont.... **Page**

Tables

Figures

FOREWORD

The increasing use of microprocessor and programmable devices for protection of electrical supply requires an understanding of their functional safety. IP *Guidance on assessing the safety integrity of electrical supply protection* provides guidance on applying an efficient risk-based assessment methodology for determining safety integrity level (SIL) requirements and SIL allocations for the electrical protection function of various plant items. The methodology applies the safety integrity principles of IEC 61508/IEC 61511 to the protection of equipment and systems that are used in electricity supply, including the machinery involved.

By applying the methodology and guidance provided in this publication, electrical practitioners in the petroleum industry (both onshore and offshore) and allied process industries should be able to design, install, operate, modify and evaluate new and existing electrical supply protection equipment and systems using the safety integrity principles of IEC 61508/IEC 61511. In doing so, they should test their schemes (especially where they differ from previous practices due to new technology) to confirm they have not unknowingly raised the SIL provided to 1 or higher. This contrasts sharply with the expectations of engineers using IEC 61508/IEC 61511 for process control schemes where SIL 1 or higher is not uncommon or unexpected.

Whilst written in the context of the UK legislative and regulatory framework, the principles set out in this publication can be similarly applied internationally providing that the pertinent national and local legislative and regulatory requirements are complied with. Where the requirements differ, the more stringent should be adopted.

The information contained in this publication is provided as guidance only and while every reasonable care has been taken to ensure the accuracy of its contents, the Energy Institute, nor the representatives listed in the Acknowledgements cannot accept any responsibility for any action taken, or not taken, on the basis of this information. The Energy Institute shall not be liable to any person for any loss or damage which may arise from the use of any of the information contained in any of its publications.

This publication may be reviewed from time to time. It would be of considerable assistance in any future revision if users would send comments or suggestions for improvement to:

Energy Institute
Technical Department
61 New Cavendish Street
London
W1G 7AR
e: technical@energyinst.org.uk

ACKNOWLEDGEMENTS

This publication was commissioned by the Institute's Electrical Committee and was prepared by Bob Fallaize (Consultant). Significant technical contributions were made by:

Jim Adams	BP
David Atkinson	BP
Joe Battle	Total
Steve Bowcock	BP
Duncan Crichton	BP
Robert Denham	Health and Safety Executive
Peter Freeman	Shell U.K. Oil Products Limited
Kevin Hailes	BP
Alan Jeater	BP
Thomas Liew	Shell E&P Europe
Tom Ramsey	Esso Petroleum
Paul Taylor	British Pipeline Agency Limited
Norman Turner	Health and Safety Executive
Stephen Wilkinson	ConocoPhillips

Affiliations refer to the time of participation.

Project co-ordination and technical editing was carried out by Alia Alavi (Energy Institute) and latterly by Mark Scanlon (Energy Institute).

The Institute wishes to record its appreciation of the work carried out by those listed above and those that provided technical comments during the development of the publication.

1

INTRODUCTION

Instrumentation systems have been used for many years for the protection of plant and equipment in all areas of industry. The development of more complex protective systems involving the use of microprocessor and programmable devices, together with a trend to address risk more rigorously, has led to an increasing need to address the reliability and security of equipment and systems.

IEC 61508 (published in 1998) provides a framework for the robust consideration of the safety risks associated with the use of such equipment in systems used for safety purposes. IEC 61511 (published in 2003) provides a process industry specific application. Although the underlying approach used within IEC 61508/IEC 61511 is specifically aimed at the protection issues surrounding process plant – handling, transporting and storage of products – it may also be applied to the protection of equipment and systems that are used as part of electricity supply, including the machinery involved in that process.

The driver for developing the risk-based assessment methodology to functional safety set out in this publication has been the increasing use of microprocessor and programmable devices for electrical protection. In addition, the risk assessment required by legislation such as the UK Control of Major Accident Hazards Regulations (COMAH) 1999 (as amended) should include power system integrity and plant shutdown scenarios.

This publication provides electrical practitioners with guidance on applying an approach to risk associated with the protection of electrical power supply equipment and systems, specifically those used within the petroleum industry (both onshore and offshore) and allied process industries. It considers the concepts developed in IEC 61508 and subsequently applied in IEC 61511 and develops these to make them more easily applicable to the protection of electrical power supply equipment and systems. The approach is not only applicable to microprocessor and programmable equipment deployed – or possibly to be deployed in future – in electrical systems, but offers benefit to the assessment of risk associated with protection based on electronic or electromechanical devices.

By using this publication, electrical practitioners should be able to design, install, operate, modify and evaluate new and existing electrical protection equipment and systems using the safety integrity principles of IEC 61508/IEC 61511.

Commercial and environmental risk may be assessed in a manner similar to that of safety. Where this is the case, the higher of the SILs identified should be adopted for the protection arrangements.

In using this publication, electrical practitioners should define tolerable risk criteria; in the UK safety risks should be made as low as reasonably practicable (ALARP). Generally, the protection requirement should not be greater than SIL 1; it has been found that following previous good practices in the design of protection equipment and systems, together with appropriate test, inspection and maintenance routines (to ensure failure rates are low) should achieve this aim in most instances.

2

SCOPE AND APPLICATION

2.1 SCOPE

This publication provides guidance on assessing the risk and the consequent SIL requirements of protection systems applied to electrical power equipment and systems used within the petroleum industry (both onshore and offshore) and the allied process industries.

The elements of achieving and maintaining a defined SIL applied to protection arrangements are that:

— Protection arrangements satisfy the requirements of a defined risk analysis.
— Hardware elements used in the safety function have a defined hardware fault tolerance.
— Processes are applied that should avoid those faults of a systematic nature that may only be eliminated by a change in system or procedure.

This publication sets out means to achieve these requirements.

Note that all of Section 4 should be satisfactorily addressed in order to achieve a SIL of one or above.

The approach to risk assessment in this publication addresses three fundamental requirements:

— The initial assessment of risk that must be undertaken in order to identify the level of reliability demanded of the protection function overall.
— The assessment and allocation to the protection function, of the SIL offered by the protection arrangements applied to the power system.
— The necessary management, maintenance, testing and recording framework that is necessary to support the integrity of the entire process of risk evaluation.

The electrical systems in scope of this publication are those used in the petroleum industry (both onshore and offshore) and allied process industries. Note that Annex C provides worked examples of risk reviews for similar equipment in both onshore and offshore environments; this illustrates the differences that may be encountered.

The techniques employed do not make a distinction between relay types; electromechanical, electronic and digital relay applications can be reviewed, managed and maintained using the methods recommended.

Whilst the publication focuses on safety as the key risk driver for determining SILs, it also offers guidance on determining SILs based on commercial and environmental considerations.

2.2 APPLICATION

This publication is applicable to the protection systems used for all electrical equipment. It is presented in a way that will enable its application to existing and to new plant. This section sets out how electrical practitioners should apply the guidance provided in this publication, including defining some pre-requisites, and what to apply it to.

Before a formal approach to risk assessment can be undertaken, the electrical power system should have in place the following basic elements: