Guidance on safety integrity level determination for safety instrumented systems in support of IEC 61511

energy institute

GUIDANCE ON SAFETY INTEGRITY LEVEL DETERMINATION FOR SAFETY INSTRUMENTED SYSTEMS IN SUPPORT OF IEC 61511

First edition

January 2020

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 (EI) is the chartered professional membership body for the energy industry, supporting over 20 000 individuals working in or studying energy and 200 energy companies worldwide. The EI provides learning and networking opportunities to support professional development, as well as professional recognition and technical and scientific knowledge resources on energy in all its forms and applications.

The EI's purpose is to develop and disseminate knowledge, skills and good practice towards a safe, secure and sustainable energy system. In fulfilling this mission, the EI addresses the depth and breadth of the energy sector, from fuels and fuels distribution to health and safety, sustainability and the environment. It also informs policy by providing a platform for debate and scientifically-sound information on energy issues.

The EI is licensed by:
- the Engineering Council to award Chartered, Incorporated and Engineering Technician status, and
- the Society for the Environment to award Chartered Environmentalist status.

It also offers its own Chartered Energy Engineer, Chartered Petroleum Engineer, and Chartered Energy Manager titles.

A registered charity, the EI serves society with independence, professionalism and a wealth of expertise in all energy matters.

This publication has been produced as a result of work carried out within the Technical Team of the EI, funded by the EI's Technical Partners. The EI's Technical Work Programme provides industry with cost-effective, value-adding knowledge on key current and future issues affecting those operating in the energy sector, both in the UK and internationally.

For further information, please visit **http://www.energyinst.org**

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

BP Exploration Operating Co Ltd
BP Oil UK Ltd
Centrica
Chevron North Sea Ltd
Chevron Products Company
Chrysaor
CLH
ConocoPhillips Ltd
DCC Energy
EDF Energy
ENI
E. ON UK
Equinor
ExxonMobil International Ltd
Innogy
Kuwait Petroleum International Ltd
Nexen CNOOC
Ørsted
Perenco
Phillips 66
Qatar Petroleum
Repsol Sinopec
RWE npower
Saudi Aramco
Scottish Power
SGS
Shell UK Oil Products Limited
Shell U.K. Exploration and Production Ltd
SSE
TAQA Bratani
Total E&P UK Limited
Total UK Limited
Tullow Oil
Uniper
Valero
Vattenfall
Vitol Energy
Woodside
World Fuel Services

However, it should be noted that the above organisations have not all been directly involved in the development of this publication, nor do they necessarily endorse its content.

ISBN 978 1 78725 106 9

Published by the Energy Institute

Hard copy and electronic access to EI and IP publications is available via our website, **https://publishing.energyinst.org**.
Documents can be purchased online as downloadable pdfs or on an annual subscription for single users and companies.
For more information, contact the EI Publications Team.
e: **pubs@energyinst.org**

CONTENTS

Page

Contents continued

Contents continued

LIST OF FIGURES AND TABLES

Page

Figures

List of figures and tables continued

Page

Tables

FOREWORD

Most process plants are controlled by complex process control systems; there is increasing dependence on safety instrumented systems (SISs) to carry out safety instrumented functions (SIFs). Process industry incidents, such as those occurring at petroleum refineries and bulk storage facilities, have focused attention on the design and maintenance of functional safety for SISs to ensure that the target risk levels (e.g. tolerable) are to be achieved.

After applying inherently safer design (ISD) principles to the fundamental process plant design, residual process plant hazards should be properly controlled and have effective risk reduction measures (RRMs) in place to achieve target risk levels. Equipment on the process plant and the process control system may provide some risk reduction, but these do not usually provide sufficient control for all the identified hazardous events. Consequently, to achieve target risk levels, and as part of a balanced approach to risk reduction, additional RRMs may be necessary. Such RRMs could include SISs to carry out SIFs. These are protection layers (PLs) that are intended to detect abnormal conditions on the process plant and prevent the hazardous event (PL(prevention)), or to mitigate the consequences of the hazardous event (PL(mitigation)). SISs comprise electrical, electronic or programmable electronic systems. SIL determination therefore contributes to defining RRMs, and its findings should be part of a demonstration of safe operation to competent authorities.

The objective of safety integrity level (SIL) determination is, for a specific hazardous event, to:

– Determine whether it is necessary to employ a SIS, to carry out a specific SIF, where there is a shortfall in the risk reduction already achieved by RRMs to meet a target risk.
– Determine the SIL of the SIF where it has been determined that there is a shortfall in the risk reduction needed to meet the target risk.

This technical publication supports practical application of the following clauses of IEC 61511-1:

– clause 8 Process [hazard and risk assessment] H&RA, and
– clause 9 Allocation of safety functions to protection layers.

It does so by providing guidance on:

– SIL determination of SIFs associated with SISs within the scope of IEC 61511.
– Identifying the SIFs to be carried out by one or more SISs.
– Illustrating several SIL determination methods available for ensuring that an appropriate SIL is selected for each SIF.
– The team-based workshop methodology.
– Setting a target risk comprising target harmful event frequencies for the specified consequences (e.g. safety and environment).
– Justifying the basis on which the target harmful event frequencies for specified consequences are set.
– Having a rational basis for claims made for the risk levels that are achieved.
– Ensuring that the assumptions relating to the risk reduction parameters that impact on the amount of risk reduction that is being claimed for a particular PL are based on robust evidence and are managed throughout the safety life cycle of the process plant.

Guidance is provided on some key principles and requirements for effective functional safety management (FSM), including:

- Setting a target risk comprising target harmful event frequencies for the specified consequences (e.g. safety and environment).
- Justifying the basis on which the target harmful event frequencies for specified consequences are set.
- Having a rational basis for claims made for the risk levels that are achieved.
- Ensuring that the assumptions relating to the risk reduction parameters that impact on the amount of risk reduction that is being claimed for a particular PL are based on robust evidence and are managed throughout the life of the process plant.

The focus of this technical publication is safety and environmental risk, but the guidance may also be used for other risks (e.g. as a basis for asset protection). Excluded from the scope is guidance on other key steps of the SIS safety life cycle, from SIS design and engineering through installation and commissioning to decommissioning. For guidance on taking forward the findings of SIL determination, see EI *Guidance on achievement, operation and maintenance of functional safety employing safety instrumented systems in support of IEC 61511*.

The intended applications of this technical publication are:

- the process industry sectors (e.g. nuclear processing, offshore and onshore oil and gas sectors, and the chemical manufacturing industry);
- SIFs operating in any mode of operation (i.e. low demand, high demand or continuous mode), and
- new process plant design, but also legacy systems where modifications are being considered or undertaken.

This technical publication should be relevant to:

- Persons who require a basic understanding of the key concepts and terminology of SIL determination, e.g. to make them competent 'intelligent customers';
- Persons who need to have a comprehensive understanding of SIL determination;
- Persons who wish to further develop their competence in the key technical concepts, and
- Senior managers who have responsibility for functional safety.

Comments or suggestions for improvement should be sent to:
Technical Department,
Energy Institute,
61 New Cavendish Street,
London,
W1G 7AR,
UK.
e: technical@energyinst.org

ACKNOWLEDGEMENTS

The need for this technical publication was identified by the EI's Process Safety Committee (PSC). Developmental work was contracted to Engineering Safety Consultants Ltd. (ESC Ltd.): Ron Bell was the main author; Dr Fan Ye, Ken Simpson and David Green assisted.

The project to develop this technical publication was directed by EI's SILs/LOPAs Working Group, which is a PSC working group, whose members during the project comprised:

Paul Lucas (Chairperson)	ABB
Dr Alan King	ABB
Chris Venn	Chevron
Toby St Leger	ConocoPhillips
Dr Mark Scanlon (Secretary)	Energy Institute
Dr Mike Nicholas	Environment Agency
Tom Ramsay	ExxonMobil
Ron Bell	ESC
Ed Fergus	Health and Safety Executive
Andy Fewster	Health and Safety Executive
Chris Wheeler	InSite Technical Services
Ian Bradby	Jacobs Consultancy
King Lee (former Chairperson)	Lloyd's Register
Dylan Peters	Murco Milford Haven Refinery
Peter Davidson	Tank Storage Association

The EI acknowledges their direction and technical contributions to the project. The listing refers to the representatives' last affiliation whilst participating. In addition, the EI acknowledges the following who provided significant comments during the stakeholder technical review that facilitated consensus building:

Dr Alan King	ABB
Stephen Clarke	BP
Neil Macnaughton	BP
John Gould	Centrica Energy
Sander Makop	Centrica Energy
Mark Thompson	Centrica Energy
Chris Venn	Chevron
Toby St Leger	ConocoPhillips
Dr Mark Scanlon	Energy Institute
Dr Mike Nicholas	Environment Agency
Tom Ramsay	ExxonMobil
Ed Fergus	Health and Safety Executive
Andy Fewster	Health and Safety Executive
Richard Gowland	Independent consultant
Chris Wheeler	InSite Technical Services
Clive de Salis	Murco Milford Haven Refinery
Dylan Peters	Murco Milford Haven Refinery
Peter Davidson	Tank Storage Association
Amol Deshpande	Total

The listing refers to the representatives' last affiliation whilst participating.

The Environment Agency is acknowledged for kindly making available from their internal training resources the worked example presented in Annex E.2.

The author thanks the International Electrotechnical Commission (IEC) for permission to reproduce information from its International Standards. All such extracts are copyright of IEC, Geneva, Switzerland. All rights reserved. Further information on the IEC is available from www.iec.ch. IEC has no responsibility for the placement and context in which the extracts and contents are reproduced by the author, nor is IEC in any way responsible for the other content or accuracy therein

Dr Mark Scanlon managed the technical development project.

1 INTRODUCTION, SCOPE AND APPLICATION

1.1 INTRODUCTION

Most process plants are controlled by complex process control systems; there is increasing dependence on safety instrumented systems (SISs) to carry out safety instrumented functions (SIFs).

After applying inherently safer design (ISD) principles to the fundamental process plant design to eliminate hazards as the first priority, residual process plant hazards should be properly controlled and have effective risk reduction measures (RRMs) in place to achieve target risk levels. Equipment on the process plant and the process control system may provide some risk reduction, but these do not usually provide sufficient control for all the identified hazardous events. Consequently, to achieve target risk levels, and as part of a balanced approach to risk reduction, additional RRMs may be necessary. Such RRMs could include SISs to carry out SIFs. These are protection layers (PLs) that are intended to detect abnormal conditions on the process plant and prevent the hazardous event (PL(prevention)), or to mitigate the consequences of the hazardous event (PL(mitigation)). SISs comprise electrical, electronic or programmable electronic systems.

To achieve target risk levels, the approach should involve (in order of priority):

- Applying ISD principles (also in order of priority):
  - elimination of hazards, and
  - control and minimisation of risk at source using physical engineering controls (e.g. by increasing separation distances).
- Providing PLs (prevention) that reduce the specific hazardous event frequency (HEF). These may include systems and functions that are intended to detect abnormal conditions on the process plant and prevent the hazardous event.
- Providing PLs (mitigation) that mitigate the consequence of the specific hazardous event. These may include systems and functions that are intended to mitigate the consequences of the hazardous event.

For a specific hazardous event, the objective of SIL determination is to:

- Determine whether it is necessary to employ a SIS to carry out a specific SIF, where there is a shortfall in the risk reduction already achieved by RRMs to meet a target risk.
- Determine the SIL of the SIF where it has been determined that there is a shortfall in the risk reduction needed to meet the target risk.

An example of a hazardous event is 'Rupture of pressure vessel and release of flammable gas at high pressure leading to an extensive gas cloud.'

Whilst the guidance provided in this technical publication relates to the required performance of the SIFs to be implemented by PLs to prevent hazardous events or to mitigate the consequences of hazardous events, selecting SIFs and determining their performance requirements should be part of a balanced approach to risk reduction.