

Guidelines for management of safety critical elements (SCEs)

GUIDELINES FOR MANAGEMENT OF SAFETY CRITICAL ELEMENTS (SCEs)

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

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.

Copyright © 2020 by the Energy Institute, London.

The Energy Institute is a professional membership body incorporated by Royal Charter 2003.

Registered charity number 1097899, England

All rights reserved

No part of this book may be reproduced by any means, or transmitted or translated into a machine language without the written permission of the publisher.

ISBN 978 1 78725 155 7

Published by the Energy Institute

The information contained in this publication is provided for general information purposes only. Whilst the Energy Institute and the contributors have applied reasonable care in developing this publication, no representations or warranties, express or implied, are made by the Energy Institute or any of the contributors concerning the applicability, suitability, accuracy or completeness of the information contained herein and the Energy Institute and the contributors accept no responsibility whatsoever for the use of this information. Neither the Energy Institute nor any of the contributors shall be liable in any way for any liability, loss, cost or damage incurred as a result of the receipt or use of the information contained herein.

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
Foreword	7
Acknowledgements	9
1 Introduction, scope and application	10
1.1 Introduction	10
1.2 Development approach and key technical changes	11
1.3 Scope	13
1.4 Application	13
1.4.1 Relationship of <i>El Guidelines for management of safety critical elements (SCEs)</i> to <i>El High level framework for process safety management</i>	14
2 Key SCE management issues	16
2.1 Safety management system	16
2.2 Goal setting versus prescriptive legislation and regulation	17
2.3 SCE management across facility life cycle phases	17
2.4 Scope of SCEs	19
2.5 Major accident hazards (MAHs)	19
2.6 Applying inherently safer design principles	19
2.7 SCE identification	20
2.7.1 Types of SCEs	22
2.8 Role of human and organisational factors in managing SCEs	23
2.9 Role of change in managing SCEs	24
3 SCE PSs	27
3.1 Introduction	27
3.2 Functionality, availability, reliability, survivability and interactions and dependencies (farsi) criteria	28
3.2.1 Functionality	29
3.2.2 Availability	30
3.2.3 Reliability	30
3.2.4 Survivability	30
3.2.5 Interactions and dependencies	31
3.3 Defining performance standard (PS) criteria	31
4. SCE management – implementation of integrity assurance	33
4.1 Introduction	33
4.2 Assurance activities	34
4.2.1 Assurance activities for initial suitability of SCEs in design projects	35
4.2.2 Assurance activities for ongoing suitability of SCEs in operate phase	36
4.3 Management of change (MoC) in projects and operate phase	36
4.4 Configuring a maintenance management system for SCE management in operate phase	36
4.4.1 Managing SCEs at system, equipment and component levels	37
4.4.2 Ranking SCEs by criticality	39
4.5 Implementation of SCE assurance in operate phase	40
4.5.1 Inspection, maintenance and testing	40

Contents continued

	Page
4.5.2 Recording and reporting of SCE assurance data	41
4.5.3 SCE remedial work – Managing repairs and practical repairs procedures. . .	41
4.5.4 Managing temporary equipment	42
4.5.5 Managing spare parts.	43
4.5.6 Managing impaired SCEs – deferment, failure, degradation and unavailability	43
4.5.7 Deviations from SCE PSs.	46
4.5.8 Managing bypass or inhibit of SCEs	48
4.5.9 Unplanned demands on SCEs.	48
4.5.10 Human and organisational factors in SCE assurance.	49
5 Verification of SCE integrity	51
5.1 Introduction	51
5.2 Verification scheme	52
5.3 Verifier selection criteria.	53
5.3.1 Verifier independence	53
5.3.2 Verifier competency	53
5.4 Verification activities	54
5.4.1 Verification activities for initial suitability of SCEs in design projects	56
5.4.2 Verification activities for ongoing suitability of SCEs in operate phase. . .	57
5.4.3 Verification activities for change.	57
5.5 Verification activity frequency	58
5.6 Verification sample sizes	58
5.7 Critical function tests.	59
5.8 Verification recording and reporting.	60
6 Measurement of SCE performance, review and continual improvement	62
6.1 Measurement of SCE performance	62
6.2 Review of SCE performance.	63
6.3. Managing SCE ageing, obsolescence and life extension.	64
6.4 Continual improvement of SCE management	65
 Annexes	
Annex A Glossaries	67
A.1 Introduction	67
A.2 Glossary of terms	67
A.3 Glossary of abbreviations and acronyms	74
A.4 Glossary of symbols	78
Annex B References and bibliography.	79
Annex C Typical examples of MAHs.	83
Annex D Typical SCEs.	85
Annex E Example PSs	88
E.1 Introduction	88

Contents continued

	Page
E.2 Example PS – Emergency lighting for a fixed offshore exploration and production (E&P) installation	88
E.3 Example PS – Hydrocarbon containment for an offshore E&P installation	92
Annex F Using safety integrity level (SIL) determination outputs to manage safety instrumented system (SIS) SCEs by setting and measuring PS performance targets	105
Annex G Example method for maintenance management system designation of SCEs at equipment/system tag level	107
Annex H Example method for SCE safety criticality ranking	109

LIST OF FIGURES AND TABLES

	Page
Figures	
Figure 1: SCE management process	11
Figure 2: Safety management system based on Deming cycle applied to SCE management . .	16
Figure 3: SCE management activities mapped against facility lifecycle phases	18
Figure 4: Standard bow tie diagram	22
Figure 5: Relationship between SCE goals, PSs and SCE management (assurance and verification)	29
Figure 6: Example ESD loop showing maintenance tasks and disciplines	39
Figure 7: Process for managing SCE deviations – Risk assessment, deferred assurance and remedial work	47
Figure D.1: Typical SCEs for an offshore E&P facility	86
Figure D.2: Typical SCEs for an onshore petroleum refinery	87
Figure F.1: Using SIL determination outputs to manage SIS SCEs by setting and measuring PS performance targets	106
Figure G.1: Decision flowchart to ascertain whether an item of equipment/component is itself a SCE	108
Tables	
Table 1: Overview of typical assurance activities for initial and ongoing suitability	34
Table 2: Overview of typical verification activities for initial and ongoing suitability of SCEs .	55
Table C.1: Typical MAHs for offshore and onshore facilities	83
Table H.1: Scoring system for SCE MAH management functional role	109
Table H.2: Scoring system for SCE consequence of failure	110
Table H.3: Scoring system for SCE redundancy	110
Table H.4: SCE criticality ranking	110

FOREWORD

The process industries, including energy industry sectors such as oil and gas exploration and production (E&P), petroleum refining and bulk storage, and conventional (thermal) power generation, manage the safety of their operations using risk management processes, which include having safety management systems with a proportionate focus on process safety so as to identify hazards and manage risks throughout the life cycle of a facility. Of particular concern are major accident hazards (MAHs), which include events with safety-related consequences such as structural failure, fire, explosion, or loss of containment of a dangerous substance that cause, or have a significant potential to cause, death or serious personal injury to multiple persons.

The purpose of this technical publication is to provide 'industry' guidance for the management of safety critical elements (SCEs). An SCE is any part of a facility, plant, or computer program, the failure of which could cause, or contribute substantially to, an MAH; or the purpose of which is to prevent or limit the effect of an MAH.

The scope focuses mainly on assurance and verification aspects of SCE management.

Whilst the principles set out in this technical publication are written for SCE management where the potential impacts are to safety, the principles also should be applicable to broader safety and environmental critical element (SECE) management.

This 3rd edition has updated the 2nd edition so as to:

- Capture experience in SCE management.
- Make it applicable to a wider range of facilities.
- Recognise the range of maturity of international legislation and competent authority requirements for SCE management, which include some that mandate verification through to those with little specific requirement for MAH management.

In doing so, it provides:

- new guidance on SCE development and management in project phases, from initial SCE suitability through to ongoing SCE suitability;
- new guidance on the role of human and organisational factors in SCE management;
- new guidance on the role of change, which is a challenge to SCE management;
- additional guidance on developing performance standards (PSs);
- new guidance on using safety integrity level (SIL) determination to set and measure performance targets in PSs;
- additional guidance on assurance aspects of SCE management, to rectify an imbalance with the amount of guidance on verification in the 2nd edition;
- new guidance on implementation of SCE integrity assurance, such as its interface with maintenance management;
- new guidance on SCE management at system, equipment and component levels;
- new guidance on determining SCE criticality;
- new guidance on SCE performance, review and continual improvement, and
- new guidance on managing SCE ageing, obsolescence and life extension.

In addition, the 3rd edition provides practical examples to support the guidance.

The 3rd edition therefore provides a robust and updated 'industry' benchmark of good practice in managing SCEs for organisations operating in the high hazards industrial sectors. Adopting its guidance should enable industry operating companies to ensure initial and ongoing suitability of SCEs, and so contribute to improving their process safety management (PSM) capability.

The information contained in this publication is provided as guidance only. Whilst every reasonable care has been taken to ensure the accuracy of its contents, neither the Energy Institute (EI), nor the representatives listed in the Acknowledgements, can accept any responsibility for any actions taken, or not taken, on the basis of this information. The EI shall not be liable to any person for any loss or damage that may arise from the use of the information contained in any of its publications.

The intent is to review and where necessary update this technical publication periodically. Comments or suggestions for improvement (e.g. relevant project experience) should be sent to:

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

ACKNOWLEDGEMENTS

The 3rd edition of *El Guidelines for management of safety critical elements (SCEs)* was commissioned by the El's Process Safety Committee (PSC) and authored under the direction of a collaborative Working Group by David McLean and colleagues (Lloyd's Register). Working Group members during the project comprised:

Trudy Dymock	BP
Chris Bradley	BP
SreeRaj Nair	Chevron
Toby St. Leger (later Chairperson)	ConocoPhillips
Dr Mark Scanlon	Energy Institute
King Lee (initial Chairperson)	Lloyd's Register
Paul Irvine	Nexen CNOOC
Dr Keith Lewis (R.I.P.)	Total

El acknowledges their direction and technical contributions to the project, which includes providing experience and documentation.

El also acknowledges the following reviewers who provided significant comments during the stakeholder technical reviews that facilitated content consensus building:

Peter Gedge	BP
Dr John Morgan	DNV-GL
Ahmed Omar	Eni Engineering
Dr Andy Rushton	ESR Technology
Dave Mansfield	ESR Technology
John Briggs	Kuwait Petroleum International
Dr David Piper	Total

Several of those reviewers were members of the Oil and Gas UK (O&GUK) Major Hazards Work Group or the International Association of Oil and Gas Producers (IOGP) Process Safety Sub-Committee.

The listings refer to representatives' last affiliation whilst participating.

LR is acknowledged for providing some research funding to co-fund the technical development project to revise this technical publication.

The National Archives is acknowledged for use of public sector information licensed under Open Government Licence v3.0.

Dr Mark Scanlon (El) managed the technical development project and technically edited this technical publication.

Contents continued

	Page
E.2 Example PS – Emergency lighting for a fixed offshore exploration and production (E&P) installation	88
E.3 Example PS – Hydrocarbon containment for an offshore E&P installation	92
Annex F Using safety integrity level (SIL) determination outputs to manage safety instrumented system (SIS) SCEs by setting and measuring PS performance targets	105
Annex G Example method for maintenance management system designation of SCEs at equipment/system tag level	107
Annex H Example method for SCE safety criticality ranking	109

1 INTRODUCTION, SCOPE AND APPLICATION

1.1 INTRODUCTION

The process industries, including energy industry sectors such as oil and gas E&P, petroleum refining and bulk storage, and conventional (thermal) power generation cannot be absolutely safe. Organisations in those sectors manage the safety of their operations using risk management processes, which include having safety management systems with a proportionate focus on process safety so as to identify hazards and manage risks throughout the life cycle of a facility. Of particular concern are MAHs, which include events with safety-related consequences such as structural failure, fire, explosion, or loss of containment of a dangerous substance that cause, or have a significant potential to cause, death or serious personal injury to multiple persons. It should be noted that in some countries there is no established requirement for MAH management; also, where established, there are differences in what constitutes an MAH for different competent authorities around the world.

The purpose of this technical publication is to provide 'industry' guidance for the management of SCEs, focusing mainly on assurance and verification aspects. Following the guidance provided here should ensure that SCEs are identified, operated, inspected, tested and maintained in an appropriate way to the integrity of their operation and of the people that they protect.

An SCE is any part of a facility, plant, or computer program, the failure of which could cause, or contribute substantially to, an MAH; or the purpose of which is to prevent or limit the effect of a MAH. Examples of SCEs are ignition control/prevention and escape routes. Some SCEs are system based and may comprise a set of safety critical equipment or components; for example, a fire and gas (F&G) detection system SCE may comprise a set of individual gas or fire detectors (as sensor subsystems) and a logic solver subsystem (a.k.a. controller subsystem). This in turn may link to an emergency shutdown (ESD) system SCE.

For effective SCE management, a robust and appropriate process for MAH identification and risk assessment should be used. The process should include the use of a set of methodologies to identify MAHs, assess risks, and identify risk reduction measures to reduce risks, including defining appropriate SCEs. Whilst SCE selection is not the main focus of this technical publication, some guidance is provided on issues that should be considered in an MAH identification and risk assessment process.

Prior to selecting SCEs designers and operating companies should have implemented inherently safer design principles by adopting a hierarchy of measures (a.k.a. hierarchy of controls) that avoid MAHs instead of reducing risks from them.

EU Directive 2013/30/EU of the European Parliament and of the Council of 12 June 2013 on Safety of Offshore Oil and Gas Operations (a.k.a. OSD) promotes the wider term SECE, rather than SCE. This reflects the potential for MAHs to have environmental consequences (i.e., as major environmental incidents (MEIs)) as well as safety consequences. The focus of this technical publication is safety to people and therefore it purposely focuses on SCEs. Whilst the principles set out in this technical publication are written for SCE management, they also should be applicable to broader SECE management. It is likely that many SCEs also are SECEs.

Environment, reputation and asset protection aspects also may drive risk management. For environmental protection and mitigation, measures similar to SCEs are termed environmental critical elements (ECEs); for specific guidance see *EI Guidelines for the identification and management of environmentally critical elements*.