IGEM
Institution of
Gas Engineers & Managers

IGEM/SR/15 Edition 5 - with amendments December 2015
Communication 1784

Integrity of safety-related systems in the gas industry

This publication is produced for the sole use of the licensee.

Use by any unauthorised party in either electronic or hard copy format is not permitted.

Founded 1863
Royal Charter 1929
Patron: Her Majesty the Queen

ISBN 978 1 905903 60 3
ISSN 0367 7850
Published by the Institution of Gas Engineers and Managers

Previous Publications:
Communication 1419 (1989) – 1st Edition
Communication 1581 (1994) – 2nd Edition
Communication 1649 (2002) – 3rd Edition
Communication 1711 (2005) – 4th Edition
Communication 1746 (2010) – 5th Edition

For information on other IGEM Standards, visit our website, www.igem.org.uk

CONTENTS

TABLES

SECTION 1 : INTRODUCTION

1.1 This Standard supersedes IGE/SR/15 Edition 5, Communication 1746, which is obsolete.

1.2 This Standard has been drafted by an Institution of Gas Engineers and Managers (IGEM) Panel, appointed by IGEM's Gas Transmission and Distribution Committee, and has been approved by IGEM's Technical Co-ordinating Committee on behalf of the Council of IGEM.

1.3 The purpose of this Standard is to provide recommendations for the design and implementation of safety-related systems. The contents will be of most relevance to managers, engineers and technicians with responsibility (particularly for design and/or safety assessment) during the appropriate phases in the lifecycle of a control or safety system.

1.4 The Standard is intended to satisfy the need for industry specific guidance to supplement BS EN 61508. Other supplementary documents are described in Appendix 5 and listed in Appendix 2. In particular IEC 61511 is frequently invoked in respect of this industry (See Appendix 5). This fifth edition continues to update the recommendations and reflects that the principles of BS EN 61508 are not confined to programmable equipment.

1.5 Major differences between Editions 4 and 5 are the revision of the targets relating to maximum tolerable risk, enhancements to the Section on integrity targeting and revision of the material relating to life-cycle activities (in particular with regard to the 2010 issue of BS EN 61508). Specific examples of the latter include an alternative to the safe failure fraction metric, the use of safety manuals etc.

1.6 Any system is deemed to be safety-related where a failure, singly or in combination with other failures/errors, could lead to death or injury or damage to the environment. An application cannot be excluded from this category merely by identifying alternative means of protection. A formal safety integrity assessment, as described in Section 10, is required in order to establish if a piece of equipment can be categorised as "not safety-related". Therefore, the presence of over-rides or alternative forms of protection, for example pressure relief, does not, of itself, render other equipment "not safety-related".

The same techniques given in this Standard can be applied to design systems to protect property.

1.7 This Standard applies to both new equipment under design and to existing equipment. The targets, in both cases, will be the same but the means of assessment may differ. Existing equipment may well be assessed by "proven-in-use" historical data (Sub-Section 6.10) whereas new designs will require the use of predictive techniques.

1.8 Functional safety involves identifying specific hazardous failures which lead to serious consequences (for example, death) and then establishing maximum tolerable frequency targets for each mode of failure. Equipment whose failure contributes to each of these hazards is identified and usually referred to as "safety-related".

1.9 In practice, a hazard analysis of the plant, system or site, for example a Hazard Identification Study (HAZID), will have identified the hazardous failure mode(s). More formal hazard identification is often carried by means of a HAZOP (Hazard and Operability Study). In consequence, further studies may be needed to assess the adequacy of the control and safety systems and a safety integrity assessment would normally follow. Any HAZOP will need to take account of the

possibility that non-hazardous systems might become hazardous as a result of foreseeable modifications or abnormal operation. HAZOPs vary from formal (detailed) studies of plant performance to broad overviews of the hazards perceived. In practice, for the majority of gas installations, the hazardous conditions are generally "high or low pressure", "high or low flow", "high or low temperature" or "overfill or underfill". The HAZOP need not always be arduous since it can be based on experience of a large number of similar studies, addressing similar hazards.

1.10 Functional Safety is the term used to refer to the Integrity (expressed both quantitatively and by means of safety integrity levels (SILs) called for in respect of safety-related systems).

➤1.11 Over the last few years there has been a dramatic proliferation of industry and sector specific guidance documents. These now occupy three chapters of Reference Appendix 2.5 item 1 (now version 4.0) which is itself by no means a total coverage.➤

1.12 This Standard makes use of the terms "should" "shall" and "must" when prescribing particular requirements. Notwithstanding Sub-Section 1.14:

- the term "must" identifies a requirement by law in Great Britain (GB) at the time of publication
- the term "shall" prescribes a requirement which it is intended will be complied with in full and without deviation
- the term "should" prescribes a procedure which, it is intended, will be complied with unless, after prior consideration, deviation is considered to be acceptable.

Such terms may have different meanings when used in legislation, or Health and Safety Executive (HSE) Approved Codes of Practice (ACoPs) or guidance, and reference needs to be made to such statutory legislation or official guidance for information on legal obligations.

1.13 The primary responsibility for compliance with legal duties rests with the employer. The fact that certain employees, for example "responsible engineers", are allowed to exercise their professional judgement does not allow employers to abrogate their primary responsibilities. Employers must:

- have done everything to ensure, so far as it is reasonably practicable, that "responsible engineers" have the skills, training, experience and personal qualities necessary for the proper exercise of professional judgement
- have systems and procedures in place to ensure that the exercise of professional judgement by "responsible engineers" is subject to appropriate monitoring and review
- not require "responsible engineers" to undertake tasks which would necessitate the exercise of professional judgement that is not within their competence. There should be written procedures defining the extent to which "responsible engineers" can exercise their professional judgement. When "responsible engineers" are asked to undertake tasks which deviate from this, they should refer the matter for higher review.

1.14 It is widely accepted that the majority of accidents in industry can be primarily attributed to human factors because hazards may not have been foreseen, risks may have been inadequately assessed, safety system designs may have significant limitations and working practices may be flawed.

It is therefore necessary to give proper consideration to the management of these human factors and the control of risk. To assist in this, it is recommended that due regard be paid to HSG48.

1.15 Notwithstanding Sub-Section 1.11, this Standard does not attempt to make the use of any method or specification obligatory against the judgment of the responsible engineer. Where new and better techniques are developed and proved, they should be adopted without waiting for modification to this Standard. Amendments to this Standard will be issued when necessary, and their publication will be announced in the Journal of the Institution and other publications as appropriate.

1.16 Requests for interpretation of this Standard in relation to matters within its scope, but not precisely covered by the current text, should be addressed in writing to Technical Services, IGEM, IGEM House, High Street, Kegworth, Derbyshire, DE74 2DA and will be submitted to the relevant Committee for consideration and advice, but in the context that the final responsibility is that of the engineer concerned. If any advice is given by or on behalf of IGEM, this does not relieve the responsible engineer of any of his or her obligations.

1.17 Amendments are shown throughout the document by ➤ ➤.

1.18 This Standard was published in December 2015.

SECTION 2 : SCOPE

2.1 This Standard is applicable to safety-related control and protection systems in the gas and process industries, including gas terminals, transmission, distribution and storage and industrial, commercial and domestic gas installations. It is also relevant to offshore installations. In view of the general similarity of equipment in its many applications, this Standard is considered to be suitable for wider application in the process industries.

2.2 The scope of this Standard embraces the whole of the control or safety system concerned. It extends from field sensors (or other input devices) through to the field devices (for example, valves, pumps, fans) and includes human factors. The term process refers to all the equipment of the physical process together with the control and protection systems.

2.3 This Standard applies to all electrical and electronic systems. Although not specifically included in BS EN 61508, the principles can also be applied to mechanical and/or pneumatic items. Some equipment configurations (for example, IGEM/TD/13) have been formally assessed and shown generally to meet current risk targets (however, see A2.5 (4)).

2.4 The term "programmable electronic system" (PES) is the generic description used for all electronic control systems which employ digital computing. PESs consist of both electronic hardware and software code which provides the functionality.

2.5 An assessment includes the following elements:

- identify hazards and establish maximum tolerable risks so as to target appropriate SILs for safety functions
- establish if the hardware reliability meets the requirements implied by the integrity targets
- ensure that the principle that risks need to be shown to be "as low as reasonable practicable" (ALARP) has been applied to the reliability assessment
- establish if the architectures, i.e. measures associated with redundancy and proportions of hazardous failures, have been met
- demonstrate that the life-cycle methods and controls have been applied appropriate to the SIL in question
- show that all the organizations (from user to equipment supplier) have suitable functional safety competence.

2.6 The content of this Standard is largely aimed at designers and safety assessors but, nevertheless, some essential aspects of operation and maintenance are included.