



SAFETY CRITICAL DEVICES

Doc 252/24

EUROPEAN INDUSTRIAL GASES ASSOCIATION AISBL



AVENUE DE L'ASTRONOMIE 30 • B – 1210 BRUSSELS

Tel: +32 2 217 70 98

E-mail: info@eiga.eu • Internet: www.eiga.eu





SAFETY CRITICAL DEVICES

Prepared by WG-21 – Process Safety
Published in July 2024

Disclaimer

All technical publications of EIGA or under EIGA's name, including Codes of practice, Safety procedures and any other technical information contained in such publications were obtained from sources believed to be reliable and are based on technical information and experience currently available from members of EIGA and others at the date of their issuance.

While EIGA recommends reference to or use of its publications by its members, such reference to or use of EIGA's publications by its members or third parties are purely voluntary and not binding.

Therefore, EIGA or its members make no guarantee of the results and assume no liability or responsibility in connection with the reference to or use of information or suggestions contained in EIGA's publications.

EIGA has no control whatsoever as regards, performance or non performance, misinterpretation, proper or improper use of any information or suggestions contained in EIGA's publications by any person or entity (including EIGA members) and EIGA expressly disclaims any liability in connection thereto.

EIGA's publications are subject to periodic review and users are cautioned to obtain the latest edition.

© EIGA grants permission to reproduce this publication provided the Association is acknowledged as the source

EUROPEAN INDUSTRIAL GASES ASSOCIATION AISBL
Avenue de l'Astronomie 30 B 1210 Brussels Tel: +32 2 217 70 98
E-mail: info@eiga.eu Internet: www.eiga.eu



Table of Contents

1	Introduction	1
2	Scope and purpose	1
2.1	Scope	1
2.2	Purpose	1
3	Definitions	2
3.1	Publication terminology	2
3.2	Technical definitions	2
4	Introduction on safety protection layers	4
4.1	IEC 61511 – Safety Instrumented Systems (SIS)	4
4.2	Safety Integrity Levels (SIL)	5
5	Site specific Safety Critical Devices	5
5.1	Identifying site specific SCDs	5
5.2	Operations and responsibility of management control	6
5.3	Qualification and training	6
6	Design rules for SCDs and SIFs	7
6.1	Design considerations for SCDs	7
6.2	Design considerations for SIFs	7
6.3	Design considerations for SIL	7
6.4	Modes of operation of a SIF	7
6.5	Robustness	9
6.6	Selection of components	9
7	Documentation of SCDs	9
8	Maintenance and testing of Safety Critical Devices	10
8.1	Maintenance management system	10
8.2	Visual inspection	10
8.3	Calibration	10
8.4	Proof testing and performance	11
8.5	Maintenance bypass	11
8.6	Performance indicators	12
8.7	Changes involving SCDs	12
9	References	12

Tables

Table 1 – Safety integrity requirements for demand mode (average PFD)	8
---	---

Figures

Figure 1 – Safety protection layers	4
Figure 2 – Identifying SCDs	6

1 Introduction

The concept of safety critical elements was introduced in the UK oil and gas sector by the legislation enacted following the Piper Alpha disaster in 1988. After this, the concept has been extended to the rest of process industries, including industrial gases.

A common practice to all process industries is that they manage the safety of their operations using Risk Based Process Safety Management Systems.

The main objective of Risk Based Process Safety Management Systems is preventing the occurrence of Process Safety Incidents (PSI), as defined in EIGA Doc 223, *Monitoring of Process Safety Performance* [1].¹

Safety critical devices (SCD) are defined specifically as instruments and equipment which mitigate against a safety risk, i.e. not a business or environmental risk. The safety risk should be credible in terms of probable likelihood and potential consequence.

The purpose of this publication is to provide industry guidance for the identification and management of SCD within the industrial and medical gases industry.

2 Scope and purpose

2.1 Scope

This publication provides guidelines for developing management procedures, training, proof testing and performance analysis to improve reliability of safety critical devices to prevent the occurrence of PSIs.

Control of major-accident hazards involving dangerous substances is governed in Europe by Directive 2012/18/EU *on the control of major-accident hazards involving dangerous substances*, that lays down rules for the prevention of major accidents which may result from certain industrial activities and the limitation of their consequences for human health and the environment [2]. This directive is known as Seveso III.

A particular case of PSIs are events related to serious injury or severe damage such as hazardous events as defined in IEC 61511, *Functional safety - Safety instrumented systems for the process industry sector*, Tier 1 incidents as defined by Center for Chemical Process Safety (CCPS) [3], or Tier 1 incidents defined by Conseil Européen de l'Industrie Chimique (CEFIC) [4, 5, 6].

IEC 61511 (adopted by CENELEC) was developed to provide good engineering practices for the application of Safety Instrumented Systems in the process industries sector in response to major incidents [4]. Some industry gas member companies have adopted the concept of IEC 61511 within their own standards and refer to these.

However, there are some industrial gases facilities, that either because of the amount (threshold value) or the nature of the handled products are out of the scope of these regulations and standards. This publication includes guidelines to extend the concept of some SCDs to all facilities.

This publication refers to some of the elements in EIGA Doc 186, *Process Safety Management Systems* [7].

2.2 Purpose

This publication:

- provides definitions of common terms used in safety systems in the process industry;

¹ References are shown by bracketed numbers and are listed in order of appearance in the reference section.

- provides a brief introduction to safety critical devices;
- gives guidance on how to identify SCDs on typical production plants in the industrial gas industry which provide safeguards to prevent PSIs;
- identifies operation, maintenance and testing requirements for SCDs;
- provides guidance on documentation of SCDs; and
- provides guidance related to instrumented protection outside the scope of IEC 61511 [4].

3 Definitions

For the purpose of this publication, the following definitions apply.

3.1 Publication terminology

3.1.1 Shall

Indicates that the procedure is mandatory. It is used wherever the criterion for conformance to specific recommendations allows no deviation.

3.1.2 Should

Indicates that a procedure is recommended.

3.1.3 May

Indicates that the procedure is optional.

3.1.4 Will

Is used only to indicate the future, not a degree of requirement.

3.1.5 Can

Indicates a possibility or ability.

3.2 Technical definitions

3.2.1 Administrative control

Training, procedures, policies, or shift designs that lessen the threat of a hazard to an individual. Administrative controls typically change the behaviour of people (for example factory workers) rather than removing the actual hazard.

3.2.2 Basic Process Control System (BPCS)

A system that responds to input signals from a process, its associated equipment, other programmable systems and / or an operator and generates output signals causing the process and its associated equipment to operate in the desired manner (IEC 61511-1) [4].

3.2.3 Process Safety Incident (PSI)

A release of energy or material in process involvement, with actual or potential consequences above a minimum reporting threshold.