DRAFT FOR DEVELOPMENT

DD IEC TS
62143:2002

Electrical installations for lighting and beaconing of aerodromes — Aeronautical ground lighting systems — Guidelines for the development of a safety lifecycle methodology

ICS 29.140.50; 93.120

BSI
British Standards

National foreword

This Draft for Development reproduces verbatim IEC TS 62143:2002.

This publication is not to be regarded as a British Standard.

It is being issued in the Draft for Development series of publications and is of a provisional nature because the subject is still under technical development. It should be applied on this provisional basis, so that information and experience of its practical application may be obtained.

Comments arising from the use of this Draft for Development are requested so that UK experience can be reported to the international organization responsible for the Technical Specification. A review of this publication will be initiated not later than 3 years after its publication by the international organization so that a decision can be taken on its status at the end of its 3-year life. Notification of the start of the review period will be made in an announcement in the appropriate issue of *Update Standards*.

According to the replies received by the end of the review period, the responsible BSI Committee will decide whether to support the conversion into an international standard, to extend the life of the Technical Specification for another 3 years or to withdraw it. Comments should be sent in writing to the Secretary of BSI Technical Committee EPL/97, Aeronautical ground lighting, at British Standards House, 389 Chiswick High Road, London W4 4AL, giving the document reference and clause number and proposing, where possible, an appropriate revision of the text.

A list of organizations represented on this committee can be obtained on request to its secretary.

Cross-references

The British Standards which implement international publications referred to in this document may be found in the *BSI Catalogue* under the section entitled "International Standards Correspondence Index", or by using the "Search" facility of the *BSI Electronic Catalogue* or of British Standards Online.

This Draft for Development, having been prepared under the direction of the Electrotechnical Sector Policy and Strategy Committee, was published under the authority of the Standards Policy and Strategy Committee on 8 January 2003

Summary of pages

This document comprises a front cover, an inside front cover, the IEC TS title page, pages 2 to 25 and a back cover.

The BSI copyright date displayed in this document indicates when the document was last issued.

Amendments issued since publication

Amd. No.	Date	Comments

ISBN 0 580 41036 6

TECHNICAL SPECIFICATION

IEC TS 62143

First edition
2002-07

Electrical installations for lighting and beaconing of aerodromes – Aeronautical ground lighting systems – Guidelines for the development of a safety lifecycle methodology

Installations électriques pour l'éclairage et le balisage des aérodromes – Systèmes de balisage aéronautique au sol – Lignes directrices pour l'établissement d'une méthodologie pour le cycle de vie de sécurité

Reference number
IEC/TS 62143:2002(E)

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

ELECTRICAL INSTALLATIONS FOR LIGHTING AND BEACONING OF AERODROMES – AERONAUTICAL GROUND LIGHTING SYSTEMS – GUIDELINES FOR THE DEVELOPMENT OF A SAFETY LIFECYCLE METHODOLOGY

FOREWORD

1) The IEC (International Electrotechnical Commission) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of the IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, the IEC publishes International Standards. Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. The IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.
2) The formal decisions or agreements of the IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested National Committees.
3) The documents produced have the form of recommendations for international use and are published in the form of standards, technical specifications, technical reports or guides and they are accepted by the National Committees in that sense.
4) In order to promote international unification, IEC National Committees undertake to apply IEC International Standards transparently to the maximum extent possible in their national and regional standards. Any divergence between the IEC Standard and the corresponding national or regional standard shall be clearly indicated in the latter.
5) The IEC provides no marking procedure to indicate its approval and cannot be rendered responsible for any equipment declared to be in conformity with one of its standards.
6) Attention is drawn to the possibility that some of the elements of this technical specification may be the subject of patent rights. The IEC shall not be held responsible for identifying any or all such patent rights.

The main task of IEC technical committees is to prepare International Standards. In exceptional circumstances, a technical committee may propose the publication of a technical specification when

- the required support cannot be obtained for the publication of an International Standard, despite repeated efforts, or
- the subject is still under technical development or where, for any other reason, there is the future but no immediate possibility of an agreement on an International Standard.

Technical specifications are subject to review within three years of publication to decide whether they can be transformed into International Standards.

IEC 62143, which is a technical specification, has been prepared by IEC technical committee 97: Electrical installations for the lighting and beaconing of aerodromes.

The text of this technical specification is based on the following documents:

Enquiry draft	Report on voting
97/72/CDV	97/83/RVC

Full information on the voting for the approval of this technical specification can be found in the report on voting indicated in the above table.

This publication has been drafted in accordance with the ISO/IEC Directives, Part 3.

The committee has decided that the contents of this publication will remain unchanged until 2005-11. At this date, the publication will be

- reconfirmed;
- withdrawn, or
- replaced by an international standard.

INTRODUCTION

Aeronautical ground lighting (AGL) at an aerodrome or heliport provides the pilots of aircraft on approach to or take-off from an aerodrome, and pilots of aircraft or drivers of vehicles moving on the aerodrome surface, with location, orientation and alignment information. An AGL system therefore provides a safety-related service and functions. In order to assure that the safety of the service and functions provided by the AGL system is adequately addressed, specific safety assessments should be performed at various instances during the lifecycle of the system. This technical specification provides a methodology whereby this may be done.

This technical specification is primarily concerned with the safety lifecycle of aeronautical ground lighting (AGL) systems. To conform to this technical specification it should be demonstrated to the relevant bodies that the requirements have been satisfied and therefore that the clause objective(s) has been met.

NOTE 1 Examples of relevant bodies would include the following:

- aerodrome management;
- certification and licensing authorities;
- safety regulators;
- notified bodies for international or European directives;
- national standards bodies.

NOTE 2 This technical specification is based on the system and safety lifecycle methodology described in IEC 61508-1. IEC 61508, in all seven parts, provides a methodology to address the safety of safety-related systems and contains an abundance of guidance material, which may be applicable to an AGL system or may be of use to the reader of this technical specification. IEC 61508 contains requirements that are particularly relevant to risk reduction in a software-based AGL system.

ELECTRICAL INSTALLATIONS FOR LIGHTING AND BEACONING OF AERODROMES – AERONAUTICAL GROUND LIGHTING SYSTEMS – GUIDELINES FOR THE DEVELOPMENT OF A SAFETY LIFECYCLE METHODOLOGY

1 Scope

This technical specification:

– outlines a methodology to address the safety at all lifecycle phases of an AGL system, including the evaluation, design, procurement, manufacture, installation, commissioning, operational use, maintenance, modification, and decommissioning of the AGL system;

NOTE 1 This document contains guidelines of a high-level, objective-based, and non-prescriptive nature. This is intended to permit a flexible approach to meeting the requirements.

– applies to an AGL system at an aerodrome or heliport which provides visual guidance to a pilot and is provided, operated and maintained by the aerodrome authority;

NOTE 2 This document may apply to all or a part of an AGL system as required by the aerodrome authority. The equipment covered shall be defined and listed in the AGL safety case (see 5.6). Any subsequent addition or modification to the AGL system shall be notified as directed in 7.7.3.

– applies primarily to a new AGL system;

NOTE It may also be applied to an existing AGL system or to an existing AGL system that is being modified; however, the relevant documentation for the project phases may not be available. Therefore, retrospective action to cover the applicable lifecycle phases could be carried out or alternative means of providing safety information should be developed, e.g. historical data.

– covers all aspects of safety, including:

- operational (functional) safety of the AGL system;
- electrical safety for the installation, maintenance and decommissioning of the AGL system;
- environmental safety and electromagnetic compatibility (EMC);
- health and safety at work.

– supports a regulatory regime based on the auditing of a safety management system at an aerodrome, where the safety management system provides documented evidence that safety has been or is being addressed at all phases of the lifecycle. This applies equally to a project to install AGL or the routine operational use and maintenance of the AGL.

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

IEC 60300-3-9, *Dependability management – Part 3: Application guide – Section 9: Risk analysis of technological systems*

IEC 61508 (all parts), *Functional safety of electrical/electronic/programmable electronic safety-related systems*

IEC 61508-1, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 1: General requirements*

IEC 61508-7, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 7: Overview of techniques and measures*

IEC 61821, *Electrical installations for lighting and beaconing of aerodromes – Maintenance of aeronautical ground lighting constant current series circuits*

3 Definitions

For the purpose of this International Standard the following definitions apply.

3.1
aerodrome authority
organisation accountable for the safety and security of persons, aircraft operations and facilities at an aerodrome

3.2
AGL safety case
a controlled document, or set of controlled documents, which clearly and comprehensively presents sufficient arguments, evidence and assumptions that all foreseeable hazards have been identified and controlled for both engineering and operational areas to demonstrate that an AGL system is adequately safe

3.3
AGL system safety lifecycle
the safety activities involved in the implementation of an AGL system, occurring during a period of time that starts at the concept phase of the system and finishes when it is no longer available for use and has been decommissioned

3.4
hazard
potential source of harm

NOTE The term includes hazards to persons arising within a short time scale (for example, fire and explosion) and also those that have a long-term effect on a person's health (for example, release of a toxic substance).

3.5
hazard analysis
activity of identifying and evaluating those hazards, often following from some initiating event, that can lead to an accident

3.6
hazardous event
occurrence, with possible hazardous consequences, arising as the result of a hazardous condition

3.7
impact analysis
activity of determining the effect that a change to a function or component in a system will have on other functions or components in that system as well as on other systems.

3.8
safety audit
systematic and independent examination to determine whether the procedures specific to the safety requirements comply with the planned arrangements, are implemented effectively and are suitable to achieve the specified objectives

NOTE A safety audit may be carried out as part of a safety assessment.

[61508-4, definition 3.8.4, modified]

4 Competence of persons

4.1 Objective

The objective of this clause is to ensure that persons who have responsibility for any activity or are directly engaged in any aspect of the lifecycle of an AGL system are competent to discharge those duties or perform those tasks.

4.2 Requirements

4.2.1 It is recommended that the appropriate administration or aerodrome authority encourage the development of a formal and structured competency training programme(s). The training programme(s) should consist of multiple tiers that enhance progressively a person's skills and ensure a recognised level of competency for those persons who have satisfactorily completed the programme(s).

4.2.2 All persons involved in any activity, including management and maintenance activities, shall have the appropriate and verifiable training, technical knowledge, experience and qualifications relevant to the specific duties they have to perform. In particular, where involved in work on AGL equipment, they shall be knowledgeable of the specific risks and the safety procedures involved in the work. The training, experience and qualifications of all persons involved in any activity shall be justified taking into account all the relevant competence factors. The justification shall be recorded in appropriate documentation (see 5.3.2 g)).

NOTE The following competence factors should be addressed when assessing and justifying the competence of persons carrying out their duties:

- engineering appropriate to the application area;
- engineering appropriate to the technology (e.g. mechanical, electrical/electronic/software engineering);
- safety engineering appropriate to the technology;
- knowledge of the legal and safety regulatory framework;
- knowledge of the operational aspects related to the AGL system at the aerodrome;
- the consequences in the event of a failure of AGL equipment;
- the consequences of failure to adhere to safety procedures when working on AGL equipment;
- the novelty of the design, design procedures or application;
- previous experience relevant to the specific duties to be performed and the technology being employed;
- relevance of qualifications to the specific duties performed.

5 AGL safety management

In order to prepare and deploy an AGL system fit for operational use at an aerodrome, it is essential that safety is implicit throughout the lifecycle of the system. It is also essential that the organisations involved in all phases of the lifecycle have an embedded culture that addresses safety at all levels of management and work. It should be reminded that technical protection devices do not guarantee a level of safety and, in being able to prevent an accident from occurring, that there is no substitute for safety procedures, and the competence and vigilance of the persons involved. The following subclauses outline those aspects of a safety management system that should, at minimum, be in place within any organisation associated with the lifecycle of an AGL system.

5.1 Objective

The objective of this clause is to define and document all management and technical activities during the AGL system safety lifecycle (clause 6) that may have a direct impact on the operational safety at aerodromes and to ensure the safety of personnel engaged in those activities.

5.2 Documentation

5.2.1 The documentation developed as suggested by this technical specification shall be controlled by an appropriate document control scheme. The development of the documentation shall be initiated before the completion of the evaluation phase of the AGL system safety lifecycle and each document shall be reviewed, amended and approved by the aerodrome authority as necessary throughout the entire lifecycle.

5.2.2 For the purpose of audit, it is essential that all activities required by this technical specification be documented. The documentation produced shall:

a) suit the purpose for which it is intended;

b) comprehensively describe the safety assessment, test, system or equipment and the use of it;

c) be accurate, concise and easy to understand;

d) be assessable and maintainable.

NOTE The majority of the documentation should be considered as “live” documents, i.e. they are subject to review and revision throughout the lifecycle of the AGL system.

5.2.3 The documentation shall have:

a) unique identities so it will be possible to reference the different parts;

b) titles/names as specified in this technical specification;

c) a revision index (version numbers) to make it possible to search for relevant information. It shall be possible to identify the latest revision (version) of a document or set of information.

NOTE 1 The physical structure of the documentation will vary depending upon a number of factors such as the size of the system, its complexity and the organisational requirements.

NOTE 2 If relevant, other documents, such as applicable regulations and other standards, should be referenced.

5.3 AGL safety plan

5.3.1 An AGL safety plan shall be prepared by the aerodrome authority that outlines the responsibilities and procedures to be undertaken by management and staff engaged in the design, installation or maintenance of an AGL system or its components.

NOTE The AGL safety plan focuses on safety. It may be included in:

- a section in the Quality Plan entitled “AGL Safety Plan”,
- a separate document entitled “AGL Safety Plan”,
- several documents which are referenced in either of the above (e.g. one document could be for the overall AGL system or one document for each component (e.g. CCR), or
- an overall aerodrome safety management system.

5.3.2 The AGL safety plan shall define all management and technical activities for the design, installation or maintenance of an AGL system or its components. In particular the following items shall be specified or referenced in the AGL safety plan:

a) the scope of the AGL safety plan;

b) the policy and strategy for achieving safety, together with the means for evaluating its achievement, and the means by which this is communicated within the organisation to ensure a culture of safe working;

c) the person nominated by the aerodrome authority as responsible for the AGL system and owner of the AGL safety plan;

d) identification of the persons, departments, organisations or other units which are responsible for carrying out and reviewing safety procedures and their applications in each phase (including where relevant, licensing authorities and safety regulatory bodies) and a description of the relationship between them;

e) a description of the safety procedures to be applied;

f) the appropriate safety assessment processes as contained in the AGL safety assessment plan (see 5.4) for activities within the relative AGL system safety lifecycle phase;

g) the procedures for ensuring that all staff involved in the design, installation or maintenance of the AGL system are competent to carry out activities for which they are accountable. In particular the following shall be defined:

   1) the training of persons in diagnosis and repair of failure and in system testing;

   2) the training of operations staff;

   3) the re-training of staff at periodic intervals or after prolonged absence from duty;

   4) the plans for identifying and dealing with cases of diminished capacity to perform activities necessary for achieving safety;

h) the procedures which ensure that hazardous incidents or incidents with potential to create hazards are analysed and recommendations made such that the probability of repeat occurrence is minimised;

i) the procedures for analysing operations and maintenance performance. In particular:

   1) procedures for recognising systematic failures and faults;

   2) procedures which ensure that demand and failure rates during operation and maintenance are recorded in a suitable log and are compared with the predicted or assumed conditions made during the system specification and design phases. Such comparison will enable a judgement to be made as to whether the actual levels of dependability being achieved are less than required;

j) the requirements for periodic reviews or audits of procedures required to ensure safety. In particular, these requirements will define:

   1) the procedures to be reviewed;

   2) the required independence of the reviewers;

   3) the procedures for initiating reviews (including routine, essential and emergency);

   4) the minimum frequency of review for each activity;

   5) the procedures for the analysis of the results;

   6) the procedure for recommending corrective actions;

k) the required safety approval process and authority for modifications;

l) the procedures for initiating modifications as a result of recommendations arising from:

   1) analysis of hazardous events or incidents with potential to create hazards, including the procedures for ensuring prompt follow-up and satisfactory resolution of recommendations arising from

      i) incident reports;

      ii) any safety assessment;

      iii) verification activities;

      iv) validation activities;

      v) configuration management and change control procedures;

   2) performance below the specified level of safety (i.e. the actual performance gives rise to a risk level above that necessary to meet the level of safety);

   3) systematic fault experience (both hardware and software);

   4) new or amended safety legislation;

   5) modifications to the AGL system or its use;

   6) modification to any safety requirement;

   7) analysis of maintenance and operations performance which indicates that the required level of safety is not being achieved;

   8) routine safety reviews;

m) the procedure for maintaining accurate documentation on potential hazards;

n) the procedure for configuration management of the AGL system, including the following activities:

   1) the phase at which configuration control is to be implemented;

   2) the procedures to be used for uniquely defining all constituent parts of an item (hardware and software);

   3) the procedures to prevent unauthorised items from entering operational service;

o) where appropriate, the provision of training and information for relevant external organisations, for example, the emergency services in the safety procedures and hazards they may encounter.

5.3.3 Each of the components of the AGL safety plan shall be formally reviewed by the organisations concerned and agreement gained on the contents.

5.3.4 All those involved in implementing the AGL safety plan shall be informed of responsibilities assigned to them under the plan.

5.4 AGL safety assessment plan

5.4.1 An AGL safety assessment plan shall be developed as a means of co-ordinating, conducting, and determining the objectives of the assessments of the safety of the AGL system or one of its components.

5.4.2 The person nominated in 5.3.2 c) shall approve the AGL safety assessment plan.

5.4.3 An AGL safety assessment plan shall be provided that identifies

- the scope of the safety assessment;
- the safety assessment schedule;
- the appropriate safety assessment that shall be carried out at all phases throughout the AGL system safety lifecycle;
- the outputs from each safety assessment at each lifecycle phase;
- the safety assessment team, including the nominated leader;
- the level of independence of the assessors within the safety assessment team;
- the competence of the assessors relative to the application;
- the safety bodies and other participants involved;
- the resources required.

5.4.4 The typical safety assessments at each defined AGL system safety lifecycle phase shall

a) consider any work done since the last safety assessment was performed and the extent to which changes, as a result of that safety assessment, have been made to the system and/or the strategy for implementing further safety assessments;

b) identify the hazardous events, and the event sequences or failure modes of the AGL system that could lead to the hazardous event, under all reasonably foreseeable circumstances;

c) consider all relevant human factor issues;

d) evaluate the frequencies (or probabilities) of the hazardous events for the conditions specified;

e) evaluate the potential consequences associated with the hazardous events identified;

f) assign a level of safety (or risk criticality classification) for each hazardous event;

g) determine the safety requirements.

NOTE 1 The frequency of the events or other criteria may be specified quantitatively or qualitatively.

NOTE 2 There are many forms of safety assessment available. The type of safety assessment chosen shall be appropriate for the scope of the task, the technology involved and the required deliverables. Throughout this technical specification, a specific safety assessment may be given a specific name (e.g. preliminary hazard analysis); however they are all essentially a "hazard analysis" and this generic term is often used. IEC 60300-3-9 outlines the type of safety assessments that are appropriate for technological systems and IEC 61508-7 contains many examples and guidelines on safety assessments.

NOTE 3 The type of accident-initiating events that need to be considered include component failures, procedural faults, human error, and dependent failure mechanisms that can cause accident sequences to occur.

5.4.5 Consideration shall be given to the elimination of hazards. Risk reduction exercises shall be carried out in order to achieve or reduce the level of safety for each identified hazard.

NOTE Where sufficient mitigation of identified hazards by system design is considered unfeasible, the use of operational procedures should be investigated as an alternative means of reducing the level of risk.

5.4.6 The safety assessment team leader shall approve the results acquired from a safety assessment.

5.4.7 The information and results acquired in subclauses 5.4.4 and 5.4.5 shall be documented in the AGL safety case (see 5.6).

5.4.8 The person nominated in 5.3.2 c) shall consider the activities carried out and the outputs obtained during each phase of the AGL system safety lifecycle, and judge the extent to which the objectives have been met. The results of this exercise shall be recorded in the AGL safety case in the form of a verification report (see 5.5.4).

5.5 Verification plan

5.5.1 A verification plan shall be established, concurrently with the development, for each phase of the AGL system safety lifecycle and detailed in the appropriate and relevant documentation.

5.5.2 The verification plan shall provide and document or refer to the criteria, techniques and tools to be used in the verification process.

NOTE The selection of techniques, tools, etc., will depend upon a number of factors, including:

a) the size of the project;

b) the degree of complexity;

c) the degree of novelty of design;

d) the degree of novelty of technology.

5.5.3 Each verification process shall be performed in accordance with the verification plan.

5.5.4 A verification report shall be provided that contains evidence to show that the phase being verified has, in all respects, been satisfactorily completed.

5.6 AGL safety case

5.6.1 An AGL safety case document shall be developed that contains a history of every safety assessment that has been performed on the AGL system.

NOTE A safety case is sometimes presented in four parts that cover the following four aspects of the lifecycle: operational requirements, system design and manufacture, installation and commissioning, and operations.

5.6.2 For each safety assessment, the AGL safety case shall record the following information:

a) where the safety assessment is used to determine safety requirements:
   1) a description of the identified hazards, failure modes, etc.;
   2) the determined risk and tolerability;
   3) the safety requirements;
b) where the safety assessment is used to validate that safety requirements have been met:
   1) whether the safety requirements have been met or not;
   2) evidence, or a reference to the source of the evidence, to support any safety claims in the bullet above, or tests that have been performed;
   3) if the safety requirements have not been met, the proposed mitigation or further action required;
c) verification that the safety assessment has been done according to the AGL safety assessment plan (a verification report).

5.6.3 The AGL safety case shall be maintained and, when applicable, shall be updated with the following information:

a) the results of any additional safety assessment;
b) a record of any extra demands on the AGL system and any failures found during routine maintenance;
c) the time and cause of all extra demands on the AGL system together with the performance of the AGL system when subject to those demands;
d) a record of modifications that have been made to the AGL system as a result of, or which may have an impact on hazards in the AGL safety case.

6 AGL system safety lifecycle

The AGL system safety lifecycle (see Figure 1) outlines, in the chronological order of typical project and operational procedures that an AGL system will undergo throughout its life, the safety assessments that shall be conducted in order to determine the safety requirements and procedures that provide safe AGL equipment and an acceptable level of safety for personnel engaged in AGL activities and aerodrome operations supported by the AGL system.

The AGL system safety lifecycle phases can be divided into discrete processes. These processes are illustrated by specific boxes numbered 1 to 12 in Figure 1 and are described in detail in subclauses 7.1 to 7.8 inclusive and summarised in Table 1.

6.1 Objectives

6.1.1 The first objective of this clause is to structure, in a systematic manner, the phases in the overall safety lifecycle for an AGL system in order that safety is shown to be addressed at each phase.

6.1.2 The second objective of this clause is to determine the key information relevant to the safety aspects of the AGL system that shall be recorded throughout its lifecycle.

6.2 Requirements

6.2.1 The AGL system safety lifecycle that shall be used, as the basis for claiming conformance with this technical specification, is that specified in Figure 1. If another lifecycle is used it shall be defined in the AGL safety plan and all the objectives and requirements in each clause in this technical specification shall be met.

6.2.2 Unless exempt, each phase of the AGL system safety lifecycle shall be addressed and the requirements met. Justification for any exemption shall be recorded in the appropriate documentation.

6.2.3 Each lifecycle phase addresses

- the objectives of the phase;
- the requirements in order to meet the objectives of the phase;
- the scope of the phase;
- the inputs to the phase;
- the outputs required to meet the objectives of the phase.

6.2.4 Each phase of the AGL system safety lifecycle shall be divided into elementary tasks with a well-defined input, output and activity for each phase.

6.2.5 The outputs for each phase of the AGL system safety lifecycle shall meet the objectives and requirements specified for each phase.

6.2.6 The AGL system safety lifecycle shown in Figure 1 indicates the safety assessments and safety procedures that shall be performed in each of the following lifecycle phases:

– Phase 1 – the *evaluation* phase (box 1), where initial system designs and concepts are evaluated and a preliminary hazard analysis determines the mandatory or statutory safety requirements that take into consideration the design concepts, environmental factors, regulations and standards;

– Phase 2 – the *technical solution* phase (boxes 2 and 3), where the AGL system operational requirements are analysed and design safety requirements are derived by means of a hazard analyses for the overall AGL system and allocated to individual components;

– Phase 3 – the *realisation* phase (box 4), where the safety requirements are verified in the design and manufacture process. Also in phase 3 is the *planning* phase (boxes 5, 6 and 7), where the hazards involved in the installation, commissioning and operation of the AGL system are determined;

– Phase 4 – the *installation* phase (box 8), where the AGL system installation safety requirements and safety procedures are employed to protect the installer and the operational environment;

– Phase 5 – the *commissioning* phase (box 9), where the AGL system commissioning safety requirements are used in the commissioning of the system and the operational requirements are shown to be met;

– Phase 6 – the *operations* phase (boxes 10 and 11), where operational and maintenance safety requirements and safety procedures are implemented to protect the user (both direct and indirect) and maintainer and where appropriate measures are invoked in order to maintain the level of safety during any modification, which may include re-commencing all or part of the lifecycle;

– Phase 7 – the *decommissioning* phase (box 12), where safety procedures are determined to protect aerodrome operations and staff dismantling the AGL system or a component of it.

6.2.7 The AGL system safety lifecycle shown in Figure 1 is a simplified view of reality and, as such, does not show all the aspects of the safety assessments and procedures relating to a specific phase or between phases of the development of safety assurance for the AGL system.

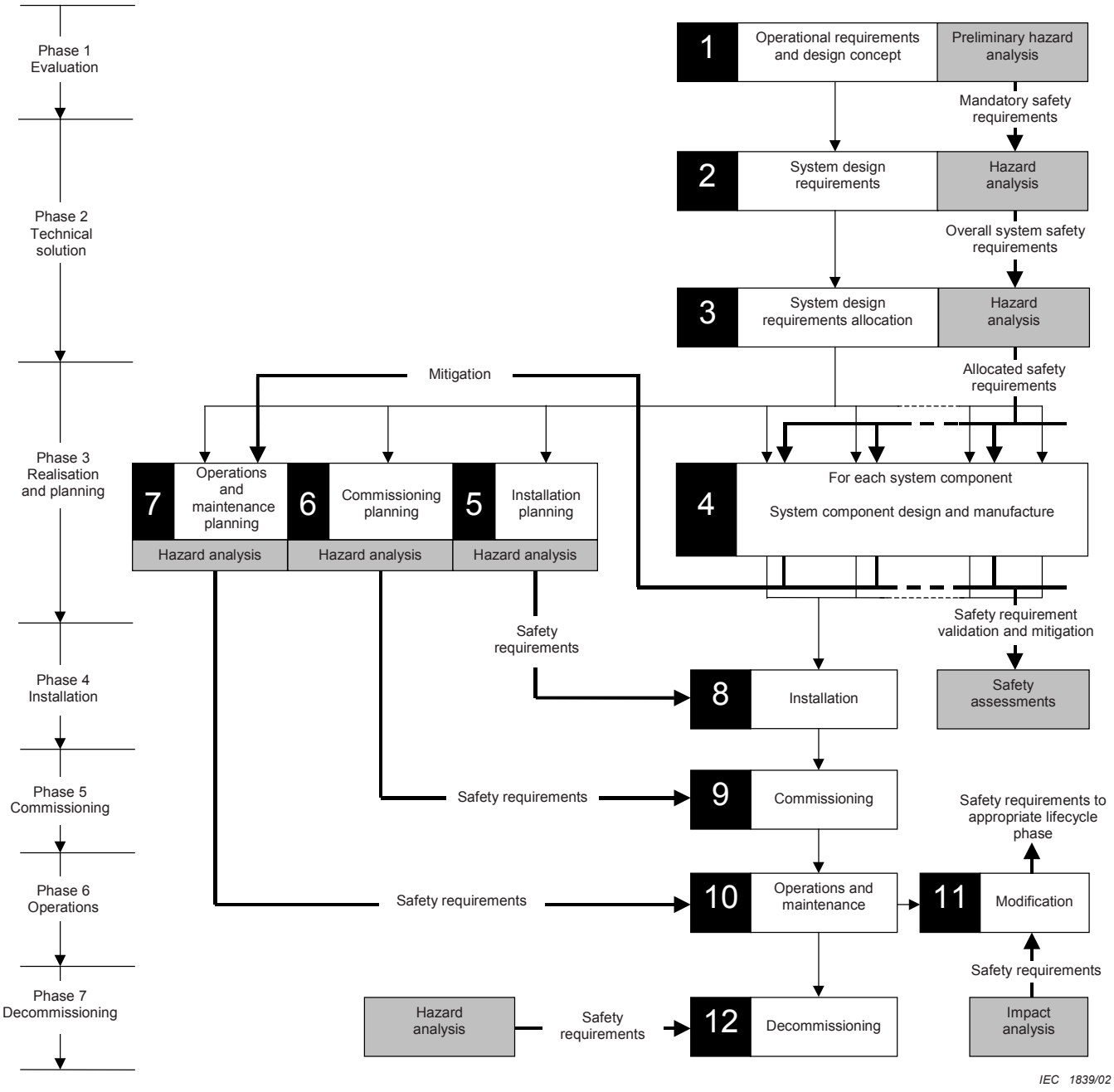

Figure 1 – AGL system safety lifecycle

7 AGL system safety lifecycle phases in detail

Subclauses 7.1 to 7.8 relate to specific boxes shown in Figure 1. Each box represents a process within the lifecycle; therefore, there will be certain inputs, actions and outputs associated with each process. For each process, subclauses 7.1 to 7.8 provide detailed information on the inputs, actions (including safety assessments) and outputs required at each phase of the lifecycle. Table 1 provides a summary of the objectives and requirements of all the clauses.

NOTE Statutory and local regulations (e.g. air navigation regulations) may apply; therefore it is of advantage to include the relevant regulatory authority in the safety lifecycle process at the earliest opportunity.

7.1 Evaluation

(See Box 1 of Figure 1)

7.1.1 Objectives

7.1.1.1 The first objective of this subclause is to describe fully the purpose of the AGL system in its intended environment (operational, physical, social, political and legislative) to enable the other lifecycle activities to be satisfactorily performed.

7.1.1.2 The second objective of this subclause is to identify the hazards associated with the operational use of the AGL system, and the event sequences leading to the hazards, in all modes of operation and all reasonably foreseeable circumstances.

7.1.1.3 The third objective of this subclause is to develop the initial safety requirements for the AGL system, including the mandatory or statutory requirements that shall apply.

7.1.2 Requirements

7.1.2.1 A thorough understanding shall be acquired of the AGL system, or component as appropriate, and its operational purpose.

7.1.2.2 In accordance with the AGL safety assessment plan, the likely sources of hazards within the scope of the AGL system shall be identified by a preliminary hazard analysis.

7.1.2.3 Information about the following aspects shall be obtained:

a) current and applicable safety regulations (national and international);

b) current and applicable air navigation regulations (national and international);

c) current and applicable local and aerodrome regulations;

d) environmental factors, including

   i) operational;

   ii) physical;

   iii) social;

   iv) political;

   v) legislative.

7.1.2.4 The operational requirements, including the level and characteristics of the AGL, shall be defined, and shall consider:

a) the intended aerodrome operational capability (weather, flight operations minima and facilities)

b) where taxiway guidance is required, the intended levels of aerodrome traffic flow (aircraft movement rates).

NOTE The maintenance of the information and results from the identification of the operational requirements is the principal means of establishing progress on the resolution of hazard and risk management issues contained in the AGL safety case.

7.1.2.5 Hazards due to interaction with other systems (installed/to be installed) in the proximity of the AGL system or component, as appropriate, shall be considered.

7.1.2.6 The preliminary hazard analysis shall determine the mandatory or statutory safety requirements for the AGL system.

7.1.2.7 The information and results acquired in subclauses 7.1.2.1 to 7.1.2.6 shall be documented in the AGL safety case.

7.1.2.8 A verification report shall be provided that contains evidence to show that the phase has, in all respects, been satisfactorily completed. The verification report shall be documented in the AGL safety case.

7.2 Technical solutions

(See Boxes 2 and 3 of Figure 1)

7.2.1 Objective

7.2.1.1 The first objective of this subclause is to develop the safety requirements for the AGL system.

7.2.1.2 The second objective of this subclause is to allocate specific safety requirements to each component of the AGL system.

7.2.2 Requirements – System design requirements

7.2.2.1 In accordance with the AGL safety assessment plan, a hazard analysis shall be performed to identify the safety requirements for the AGL system.

7.2.2.2 The hazard analysis shall consider the following aspects:

a) the mandatory safety requirements determined in the evaluation phase;

b) the safety functions necessary to ensure safety for each identified hazard;

c) each failure mode that may cause a hazardous event;

d) risk reduction measures (that are included in the AGL system design and manufacture);

e) safety levels may be assigned (see IEC 61508).

7.2.2.3 The actual type of AGL system might not be known at this phase of the lifecycle. However, since the AGL is to be used by aircraft and vehicles and operated by a person(s) with defined responsibilities at the aerodrome, there are several generic hazards associated with the AGL system, including

a) the display of an incorrect or misleading pattern, including colours;

b) an unexpected or unintended change in luminous intensity from maximum to minimum or vice versa;

c) an unintended activation or deactivation of the AGL, especially AGL associated with a runway.

NOTE The hazards listed above apply to the entire AGL system. Other hazards may exist that depend upon the type of control system, the technology employed and its complexity.

7.2.2.4 These generic hazards relate to the operational requirements of the safe movement of aircraft and vehicles at the aerodrome. They should be assessed in the hazard analysis within the context of the operations at the aerodrome and safety requirements for the AGL system should be derived.

7.2.2.5 The measures taken and methods used to develop the AGL system safety requirements (including risk reduction) shall be documented in the AGL safety case.

7.2.2.6 The AGL system safety requirements shall be documented in the AGL safety case.

7.2.2.7 A verification report shall be provided that contains evidence to show that the phase has, in all respects, been satisfactorily completed. The verification report shall be documented in the AGL safety case.

7.2.3 Requirements – System design requirements allocation

7.2.3.1 The safety functions necessary to achieve safety of the AGL and derived from the AGL system safety requirements shall be allocated to the designated AGL system components.

7.2.3.2 In accordance with the AGL safety assessment plan, a hazard analysis shall be performed to determine and allocate specific safety requirements to the designated AGL system components.

7.2.3.3 Safety assessment techniques, including availability, reliability and redundancy calculations, shall be employed in order to ensure that the allocation of system safety requirements has not degraded the required overall level of safety.

7.2.3.4 The measures taken and methods used to develop the allocated safety requirements shall be documented in the AGL safety case.

7.2.3.5 The safety requirements allocated to each AGL system component shall be documented in the AGL safety case.

7.2.3.6 A verification report shall be provided that contains evidence to show that the phase has, in all respects, been satisfactorily completed. The verification report shall be documented in the AGL safety case.

7.3 Realisation

(See Box 4 of Figure 1)

7.3.1 Objective

The objective of this subclause is to create an AGL system that conforms to all the applicable safety requirements and will satisfy the intended operational requirements.

7.3.2 Requirements

7.3.2.1 In accordance with the AGL safety assessment plan, hazard analyses shall be performed for each component of the AGL system to identify or confirm

a) conformance to all design and manufacturing standards that are applied;
b) test procedures as part of the commissioning phase for hazards and failure modes that can only be performed in the factory or by simulation;
c) new hazards and risks in the realisation process;
d) each failure mode that may cause a hazardous event;
e) the success of risk reduction measures;
f) safety levels may be assigned (see IEC 61508).

7.3.2.2 Safety assessments shall be performed as necessary in order to ascertain whether the overall system safety requirements and the allocated safety requirements have been met. Mitigation by alternative means shall be determined where any safety requirements cannot be met by the system design.

7.3.2.3 The information and results acquired in subclauses 7.3.2.1 and 7.3.2.2 shall be documented in the AGL safety case.

7.3.2.4 A verification report shall be provided that contains evidence to show that the phase has, in all respects, been satisfactorily completed. The verification report shall be documented in the AGL safety case.

7.4 Planning

(See Boxes 5, 6 and 7 of Figure 1)

7.4.1 Objectives

7.4.1.1 The first objective of this subclause is to develop the safety requirements and procedures for the installation of the AGL system.

7.4.1.2 The second objective of this subclause is to develop the safety requirements and procedures for the commissioning of the AGL system.

7.4.1.3 The third objective of this subclause is to develop operational and maintenance safety requirements to ensure that the safety of the AGL system (and its operational use by aircraft) and personnel engaged in activities with the AGL system is maintained during operation and maintenance.

7.4.2 Requirements – Installation planning

7.4.2.1 In accordance with the AGL safety assessment plan, an AGL installation plan shall be developed and shall describe

a) the installation schedule;

b) the allocation of roles and responsibilities;

c) the results of a hazard analysis performed in order to address potential hazards in the installation process;

d) the procedures for the installation (including the identification of operational and health and safety procedures and potential hazards);

e) the procedures for the resolution of failures and incompatibilities;

f) the criteria for declaring the installation complete.

7.4.2.2 A verification report shall be provided that contains evidence to show that the phase has, in all respects, been satisfactorily completed. The verification report shall be documented in the AGL safety case.

7.4.3 Requirements – Commissioning planning

7.4.3.1 In accordance with the AGL safety assessment plan, an AGL commissioning plan shall be developed and shall describe

a) details of when the commissioning shall take place;

b) the allocation of roles and responsibilities;

c) the results of a hazard analysis performed in order to address potential hazards in the commissioning process;

d) the procedures for the commissioning (including the identification of operational and health and safety procedures, potential hazards and how the commissioning will impact on aerodrome operations);

e) the commissioning strategy and techniques;

f) the scope of the commissioning exercise, including those parts of the AGL system that need to be validated before commissioning commences, and the relevant modes of operation of the AGL system;

g) the procedures for the resolution of failures and incompatibilities;

h) the criteria for declaring the commissioning complete (all relevant safety requirements have been met).

7.4.3.2 A verification report shall be provided that contains evidence to show that the phase has, in all respects, been satisfactorily completed. The verification report shall be documented in the AGL safety case.

7.4.4 Requirements – Operations and maintenance planning

7.4.4.1 In accordance with the AGL safety assessment plan, an AGL operations and maintenance plan shall be prepared.

NOTE See IEC 61821 for the maintenance requirements of an AGL constant current series circuit.

7.4.4.2 The AGL operations and maintenance plan shall specify

a) the results of a hazard analysis performed in order to determine the routine actions and safety requirements which need to be carried out to maintain the “as designed” safety of the AGL system and its operational use;

b) the actions and constraints that are necessary to prevent an unsafe state or to reduce the likelihood of an accident;

c) the records that need to be maintained;

d) the scope of the maintenance activities, including safety requirements;

e) the actions to be taken in the event of hazards occurring.

7.4.4.3 The AGL operations and maintenance plan shall be agreed with those responsible for the operation and maintenance of the AGL system.

7.4.4.4 The information and results acquired in 7.4.4.2 shall be documented in the AGL safety case.

7.4.4.5 A verification report shall be provided that contains evidence to show that the phase has, in all respects, been satisfactorily completed. The verification report shall be documented in the AGL safety case.

7.5 Installation

(See Box 8 of Figure 1)

7.5.1 Objective

The objective of this subclause is to ensure that the AGL system is installed in a safe manner.

NOTE Operational safety matters, such as clearances and procedures required in the vicinity of aircraft movements, should be addressed.

7.5.2 Requirements

7.5.2.1 Installation of the AGL system shall proceed according to the AGL installation plan (see 7.4.2.1).

7.5.2.2 The AGL safety case shall be updated if different or additional hazards become apparent as a result of the installation process.

7.5.2.3 A verification report shall be provided that contains evidence to show that the phase has, in all respects, been satisfactorily completed. The verification report shall be documented in the AGL safety case.

7.6 Commissioning

(See Box 9 of Figure 1)

7.6.1 Objective

The objective of this subclause is to ensure that the AGL system is validated and that the applicable AGL system safety requirements are met.

7.6.2 Requirements

7.6.2.1 Commissioning of the AGL system shall proceed according to the AGL commissioning plan (see 7.4.3.1).

NOTE Certain AGL facilities may require verification of operational performance and/or approval for operational use by a regulatory authority.

7.6.2.2 When discrepancies occur between expected and actual results that have an effect on safety, the analysis made and the decisions taken on whether to continue the commissioning process or issue a change request and return to an earlier part of the system lifecycle shall be documented in the AGL safety case.

7.6.2.3 A verification report shall be provided that contains evidence to show that the phase has, in all respects, been satisfactorily completed. The verification report shall be documented in the AGL safety case.

7.7 Operations

(See Boxes 10 and 11 of Figure 1)

7.7.1 Objectives

7.7.1.1 The first objective of this subclause is to operate and maintain the AGL system such that the designed level of safety is maintained.

7.7.1.2 The second objective of this subclause is to ensure that the level of safety is maintained during and after modification to the AGL system.

7.7.2 Requirements – Operations and maintenance

The AGL operations and maintenance plan and any other relevant procedures shall be implemented. Implementation shall include

a) the following of operational safety procedures relevant to the AGL system;

b) the following of maintenance schedules, including maintenance safety procedures;

c) the maintaining of records;

d) the carrying out, periodically, of audits in order to ensure that safety is maintained (see 5.3.2 j)).

7.7.3 Requirements – Modification

7.7.3.1 The modification phase shall only be initiated under the procedures specified in the AGL safety plan (see 5.3.2 k)) which details the following items:

a) the identified hazards that may be affected;

b) the proposed change;

c) the reason for change.

NOTE The reason for a modification could be because

a) the AGL system fails to meet the specified level of safety;
b) of systematic fault experience;
c) of the outcome of a periodic safety audit;
d) of new or amended safety legislation;
e) of planned modifications to the AGL system;
f) of modification to the overall system safety requirements.

7.7.3.2 In accordance with the AGL safety assessment plan, an impact analysis shall be carried out on the impact of the modification and the results shall be documented in the AGL safety case.

7.7.3.3 All modifications that are assessed to have an impact on the level of safety of the AGL system shall initiate a return to the appropriate phase of the AGL system safety lifecycle. All subsequent phases shall be completed in accordance with the procedures specified in this technical specification.

7.7.3.4 A verification report shall be provided that contains evidence to show that the phase has, in all respects, been satisfactorily completed. The verification report shall be documented in the AGL safety case.

7.8 Decommissioning

(See Box 12 of Figure 1)

7.8.1 Objective

The objective of this subclause is to ensure that the level of safety is maintained during and after the decommissioning process of the AGL system or part thereof.

7.8.2 Requirements

7.8.2.1 In accordance with the AGL safety assessment plan, a hazard analysis shall be carried out on the impact of the decommissioning and the results shall be documented in the AGL safety case.

7.8.2.2 Prior to decommissioning taking place an AGL decommissioning plan shall be prepared.

7.8.2.3 The AGL decommissioning plan shall include safety procedures for

a) the removing from operational service of the AGL system or component thereof;
b) safeguarding the operational environment;
c) dismantling and disposal of the decommissioned system.

NOTE The safety requirements of the decommissioning phase may be different from those required during the operational phase.

7.8.2.4 If the decommissioning process involves a part of the AGL system and has an impact on the level of safety of the rest of the AGL system, this shall initiate a return to the appropriate phase of the AGL system safety lifecycle. All subsequent phases shall be completed in accordance with the procedures specified in this technical specification.

7.8.2.5 A verification report shall be provided that contains evidence to show that the phase has, in all respects, been satisfactorily completed. The verification report shall be documented in the AGL safety case.

Table 1 – Summary of the AGL system lifecycle requirements

AGL system safety lifecycle		Objectives	Scope	Inputs	Outputs
Phase	**Title** Box No. in Figure 1				
1	**Evaluation** 1 – Operational requirements and design concept	To describe fully the purpose of the AGL system in its intended environment (operational, physical, social, political and legislative) to enable the other lifecycle activities to be satisfactorily performed. To identify the high-level hazards of the AGL system, and the event sequences leading to the hazards, in all modes of operation and all reasonably foreseeable circumstances. To develop the initial safety requirements for the AGL system, including the mandatory or statutory requirements that shall apply.	Operational/physical/social/ political/legislative environment. The operational requirements, physical equipment and the aerodrome environment.	All relevant information necessary to meet the requirements of the clause, including standards, regulations, environmental factors AGL safety plan AGL safety assessment plan Verification plan	Mandatory safety requirements Verification report [AGL safety case]
2	**Technical solution** 2 – System design requirements 3 – System design requirements allocation	To develop the safety requirements for the AGL system. To allocate specific safety requirements to each component of the AGL system.	The AGL system, the AGL and human factors.	AGL safety plan AGL safety assessment plan AGL safety case Verification plan	AGL system safety requirements Specific safety requirements (allocated) Verification report
3	**Realisation** 4 – System component design and manufacture	To create an AGL system that conforms to all the applicable safety requirements and will satisfy the intended operational requirements.	AGL system and/or components	AGL safety plan AGL safety assessment plan AGL safety case Verification plan	AGL system safety requirement validation Mitigation Verification report
	Planning 5 – Installation 6 – Commissioning 7 – Operations and maintenance	To develop the safety requirements and procedures for the installation of the AGL system. To develop the safety requirements and procedures for the commissioning of the AGL system. To develop operational and maintenance safety requirements to ensure that the safety of the AGL system (and its operational use by aircraft), and personnel engaged in activities with the AGL system is maintained during operation and maintenance.	The AGL system, its components, the operation and maintenance of the AGL, aerodrome operations, health and safety regulations, and human factors	AGL safety plan AGL safety assessment plan AGL safety case Verification plan	AGL installation plan AGL commissioning plan AGL operations and maintenance plan Verification reports

Table 1 – *(continued)*

AGL system safety lifecycle		Objectives	Scope	Inputs	Outputs
Phase	**Title** Box No. in Figure 1				
4	**Installation** 8 – Installation	To ensure that the AGL system is installed in a safe manner.	The AGL system, its components, the operation and maintenance of the AGL, aerodrome operations, health and safety regulations, and human factors	AGL safety plan AGL safety assessment plan AGL safety case AGL installation plan Verification plan	[AGL safety case] Verification report
5	**Commissioning** 9 – Commissioning	To ensure that the AGL system is validated and that the applicable AGL system safety requirements are met.	The AGL system, its components, the operation and maintenance of the AGL, aerodrome operations, health and safety regulations, and human factors	AGL safety plan AGL safety assessment plan AGL safety case AGL commissioning plan Verification plan	[AGL safety case] Verification report
6	**Operations** 10 – Operations and maintenance 11 – Modification	To operate and maintain the AGL system such that the designed level of safety is maintained. To ensure that the level of safety is maintained during and after modification to the AGL system.	The AGL system, its components, the operation and maintenance of the AGL, aerodrome operations, health and safety regulations, and human factors	AGL safety plan AGL safety assessment plan AGL safety case AGL operations and maintenance plan Verification plan	AGL safety case Verification report
7	**Decommissioning** 12 – Decommissioning	To ensure that the level of safety is maintained during and after the decommissioning process of the AGL system or part thereof.	The AGL system, its components, the operation and maintenance of the AGL, aerodrome operations, health and safety regulations, and human factors	AGL safety plan AGL safety assessment plan AGL safety case AGL operations and maintenance plan Verification plan	AGL safety case AGL decommissioning plan Verification report

Bibliography

IEC 61508-4, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 4: Definitions and abbreviations*

IEC 62144, *Electrical installations for lighting and beaconing of aerodromes – Aeronautical ground lighting control and monitoring systems – System requirements*[1]

_____

[1] Under consideration.

BSI — British Standards Institution

BSI is the independent national body responsible for preparing British Standards. It presents the UK view on standards in Europe and at the international level. It is incorporated by Royal Charter.

Revisions

British Standards are updated by amendment or revision. Users of British Standards should make sure that they possess the latest amendments or editions.

It is the constant aim of BSI to improve the quality of our products and services. We would be grateful if anyone finding an inaccuracy or ambiguity while using this British Standard would inform the Secretary of the technical committee responsible, the identity of which can be found on the inside front cover. Tel: +44 (0)20 8996 9000. Fax: +44 (0)20 8996 7400.

BSI offers members an individual updating service called PLUS which ensures that subscribers automatically receive the latest editions of standards.

Buying standards

Orders for all BSI, international and foreign standards publications should be addressed to Customer Services. Tel: +44 (0)20 8996 9001. Fax: +44 (0)20 8996 7001. Email: orders@bsi-global.com. Standards are also available from the BSI website at http://www.bsi-global.com.

In response to orders for international standards, it is BSI policy to supply the BSI implementation of those that have been published as British Standards, unless otherwise requested.

Information on standards

BSI provides a wide range of information on national, European and international standards through its Library and its Technical Help to Exporters Service. Various BSI electronic information services are also available which give details on all its products and services. Contact the Information Centre. Tel: +44 (0)20 8996 7111. Fax: +44 (0)20 8996 7048. Email: info@bsi-global.com.

Subscribing members of BSI are kept up to date with standards developments and receive substantial discounts on the purchase price of standards. For details of these and other benefits contact Membership Administration. Tel: +44 (0)20 8996 7002. Fax: +44 (0)20 8996 7001. Email: membership@bsi-global.com.

Information regarding online access to British Standards via British Standards Online can be found at http://www.bsi-global.com/bsonline.

Further information about BSI is available on the BSI website at http://www.bsi-global.com.

Copyright

BSI
389 Chiswick High Road
London
W4 4AL