PRODUCED BY THE OPERATIONS DIRECTORATE OF ENERGY NETWORKS ASSOCIATION

Engineering Report 127

Issue 2 2013

Application of electrical, electronic, and programmable electronic systems in safety-related systems in the electricity industry

www.energynetworks.org

PUBLISHING AND COPYRIGHT INFORMATION

Operations Directorate
Energy Networks Association
6th Floor, Dean Bradley House
52 Horseferry Rd
London
SW1P 2AF

First published, April, 2004

Amendments since publication

Issue	Date	Amendment
Issue 2	January, 2013	Revision of Issue 1 to align with revision of BS EN 61508 and changes in reference BS and IEC Standards. Converted into the new ENA Engineering Report (EREP) template and updated in accordance with Engineering Recommendation G0 Issue 1 2012 *Rules for structure, drafting and presentation of ENA engineering documents*. This issue includes the following principal technical changes: Clause 3 Terms and definitions: New definitions clause added. Clause 4 Identification of safety-related systems: • New paragraph added relating to Substation Control Systems. • New requirements relating to bay controllers. • New explanatory paragraph for software interlocking. • Clarification that document does not cover malevolent or unauthorised actions. Clause 6 Basic risk assessment methodology: • Amended Table 1 and Table 2 column headings to align with equivalent tables in BS EN 61508-1. • Added notes in Table 1 and Table 2 to clarify PFD_{avg} and PFH. Clause 7 The safety life cycle: • Added note relating to systematic capability (SC).

Issue	Date	Amendment
		• Included requirement for functional safety assessment at various stages of life cycle. Annex A: Renamed/renumbered sub-clauses A.2.1, A.8.2, A8.3 and A.8.4. Clause A.5: Added requirement relating to safety integrity of data communications process. Clause A.9: • Incorrect answer for R_i of "0.019" corrected to "0.194". • Note added regarding clarification of "SIL 0". New Annex B added to show an example of interdependency between programmable electronic protection relays. Details of all other technical, general and editorial amendments are included in the associated Document Amendment Summary for this Issue (available on request from the Operations Directorate of ENA).

This page deliberately left blank

Contents

Tables

Foreword

This Engineering Report (EREP) is published by the Energy Networks Association (ENA) and comes into effect from date of publication. It has been prepared under the authority of the ENA Engineering Policy and Standards Manager and has been approved for publication by the ENA Electricity Networks and Futures Group (ENFG). The approved abbreviated title of this engineering document is “EREP 127”, which replaces the previously used abbreviation “ETR 127”.

This document cancels and replaces ENA ETR 127 Issue 1.

ETR 127 Issue 1 was prepared with particular reference to BS EN 61508, which sets out a generic approach for all safety lifecycle activities for systems comprised of electrical/electronic/programmable electronic (E/E/PE) elements that are used to perform safety functions. BS EN 61508-1 was revised in 2010 and relevant alterations and additions have been incorporated in this issue.

This document should be read in conjunction with BS EN 61508-1.

NOTE: Commentary, explanation and general informative material is presented in smaller type, and does not constitute a normative element.

This page deliberately left blank

1 Scope

This Engineering Report provides guidance on the approach in BS EN 61508, "*Functional safety of electrical/electronic/ programmable electronic safety-related systems*" and how this should be applied in ENA Member Companies with respect to electronic and programmable electronic (PE) systems for control, operation and protection of power systems.

2 Normative references

The following referenced documents, in whole or part, 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.

Standards publications

BS EN 61508 (all parts): 2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems*

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

3.1
continuous mode of operation
mode where a safety-related function is performed continuously in normal operation

3.2
dangerous failure
failure of an element/subsystem/system that prevents a safety-related function from operating when required (demand mode) or causes a safety-related function to fail (continuous mode) placing the equipment under control in a hazardous or potentially hazardous state

[BS EN 61508-4 Clause 3.6.7 amended]

3.3
electrical/electronic/programmable electronic (E/E/PE)
based on electrical (E) and/or electronic (E) and/or programmable electronic (PE) technology

NOTE: The term is intended to cover any and all devices or systems operating on electrical principles. E/E/PE devices include: electro-mechanical devices (electrical); solid-state non-programmable electronic devices (electronic) and electronic devices based on computer technology (programmable electronic).

3.4
high demand mode of operation
mode where a safety-related function is performed on demand at a frequency of demand exceeding once per year

3.5
HSE
Health and Safety Executive