THE ASSOCIATION FOR THE BRITISH ELECTROTECHNICAL INDUSTRY

Edition – 9 November 2008

BEAMA Power Sector Position Paper:

RELATIONSHIP OF IEC 61508 TO T & D PRODUCTS INCLUDING SWITCHGEAR, MEASURING RELAYS AND PROTECTION & CONTROL EQUIPMENT, TRANSFORMERS AND ASSOCIATED EQUIPMENT

1. Summary

IEC 61508 is concerned with certain systems.

The performance of a system with regards to safety is not governed by the individual elements alone and is in fact the interaction of these elements. It is not necessary to have IEC 61508 at a product level to achieve a level of compliance appropriate to the installation.

System design principles will define the level of safety achieved i.e. including identification of the hazards and tolerable risk taking into account Regulatory requirements.

This position paper makes reference to key relevant issues.

2. Background

It is useful to make reference to the following extract from the Standard IEC 61508-1:1998

"This International Standard covers those aspects to be considered when electrical/electronic/programmable electronic systems (E/E/PESs) are used to carry out safety functions."

Publication of IEC 61508 (Parts 1 to 7) has resulted in some confusion, generally resulting from its attempted inappropriate application e.g. often the original scope and intention has not been followed. This can result in grossly misleading conclusions being drawn. In view of this, it is considered necessary to clarify here the relevance of IEC 61508 to T & D products and the related electricity system.

Furthermore, it is necessary to review the way in which safety is historically/currently achieved in the electricity transmission/distribution system.

3. Safety and the Electricity Transmission/Distribution System

Safety in the electricity system is achieved by system design principles and implementation of industry best practice.

> **The combination of system design principles/philosophy, specification of equipment, operational procedures and working practices define the safety level achieved. Historical experience and implementation of best practice is essential in the achievement and maintenance of the required safety level.**

The level of safety is defined by the system designer in choosing the level of redundancy and degree of back-up to be implemented. For example, in the case of a distribution system the operation of protective relays and switchgear will be determined through a protection grading system, with failure to operate of a relay or associated switchgear leading to operation of the next stage of graded protection. Graded and/or zoned protection ensures that if failure to operate of one (or more) Protection or Circuit breaker devices occurs that a fault will still be cleared in an acceptable time. The basis of this safe design concept is that a device will not operate when required to. Reliance is never placed on a single device. Hence the individual failure of equipment (although extremely rare) will be protected via the operation of back-up systems at the next protection stage. In a distribution system the fundamental protection process is likely to be determined through Overcurrent/time grading.

At transmission voltage levels where higher security levels are usually demanded, Distance protection may be backed-up by a zone, Differential protection, scheme operating in parallel i.e. a different protection principle operating in parallel redundancy mode with separate, independent, supply and Tripping circuits. Zone protection may also be applied in a distribution system, but it is much less typical (although available to the system designer).

The above has been given as illustrative examples. However it is essential that the system designer takes into account the system consequences which might vary considerably from inconvenience to major plant failure.

It is important to note that a 'false trip' is not a safety related issue i.e. it is solely an event affecting supply continuity.

The specification of equipment for use in the system is also significant in the level of safety achieved.

4. Specification of Individual Products Integrated within the System

The specifier of equipment for the system is responsible for ensuring that procurement specifications are consistent with the aims of the system design principles. It is essential that the specification is prepared ensuring the equipment can be fully integrated within the system design principles aspects relating to safety e.g. interlocking, isolation, and earthing to be compatible with work permits and 'gated control point' procedures which ensure safe system operation.

The above design principles aspects are likely to be defined to meet the specific requirements of the individual system. Additionally, the International product standards often require some certain safety aspects to be met. Some typical product standards which can be relevant are listed (non-exhaustively) in the Annex to this document.

Best practice is also essential with regard to individual products. Best practice includes the implementation of:

- Design principles review process and control
- 'failure/fault' analysis and corrective action
- Quality Assurance/Control (ISO 9001)
- Compliance with product standards

5. System Conditions

It is important to recognise that tripping and closing of circuit breakers initiated by protection schemes is not a safety issue, unless there is an abnormal system condition e.g. working on equipment temporarily taken out of service. Under such a situation it is the procedures, working practices and specified hardware features which will determine the safety level e.g. a permit to work system, removal of fuses, defined points of isolation e.g. racking out of Circuit Breakers, padlocking of equipment and application of earths etc.

Hence IEC 61508 does not offer a solution to assessment of the integrity of the safety level i.e. a SIL level defined against individual system components, as such an approach does not give meaningful information concerning the safety of the system.

6. Conclusion

The combination of system design principles/philosophy, specification of equipment, operational procedures and working practices define the safety level achieved. Historical experience and implementation of best practice is essential in the achievement and maintenance of the required safety level.

IEC 61508 is a standard dealing with systems rather than system components, and so its application to system components of an electricity system is inappropriate, and would result in grossly misleading conclusions being drawn.

Annex – Some Relevant International Product Standards

IEC 60255 – Series of standards - Measuring relays and protection equipment
IEC 62771 – Series of standards - High-voltage switchgear and controlgear
IEC 60076 – Series of standards - Power transformers
IEC 60044 – Series of standards - Instrument transformers
IEC 60099 – Series of standards - Surge arresters
IEC 60269 – Series of standards - Low-voltage fuses
IEC 60282 – Series of standards - High-voltage fuses
IEC 60137 – Insulated bushings for alternating voltages above 1000 V

THE BRITISH ELECTROTECHNICAL AND ALLIED MANUFACTURERS' ASSOCIATION
WESTMINSTER TOWER • 3 ALBERT EMBANKMENT • LONDON SE1 7SL
TELEPHONE: 020 7793 3000 • FACSIMILE 020 7793 3003 • EMAIL: info@beama.org.uk
WEBSITE: http://www.beama.org.uk
BEAMA LIMITED registered in ENGLAND • NO. 84313