FUNCTIONAL SAFETY – SAFETY INSTRUMENTED SYSTEMS FOR THE PROCESS INDUSTRY SECTOR –

Part 1: Framework, definitions, system, hardware and software requirements

1 Scope

This International Standard gives requirements for the specification, design, installation, operation and maintenance of a safety instrumented system, so that it can be confidently entrusted to place and/or maintain the process in a safe state. This standard has been developed as a process sector implementation of IEC 61508.

In particular, this standard

a) specifies the requirements for achieving functional safety but does not specify who is responsible for implementing the requirements (for example, designers, suppliers, owner/operating company, contractor); this responsibility will be assigned to different parties according to safety planning and national regulations;

b) applies when equipment that meets the requirements of IEC 61508, or of 11.5 of ~~IEC 61511-1~~ ANSI/ISA-84.00.01-2004 Part 1 (IEC 61511-1 Mod), is integrated into an overall system that is to be used for a process sector application but does not apply to manufacturers wishing to claim that devices are suitable for use in safety instrumented systems for the process sector (see IEC 61508-2 and IEC 61508-3);

c) defines the relationship between ~~IEC 61511~~ ANSI/ISA-84.00.01-2004 (IEC 61511Mod), and IEC 61508 (Figures 2 and 3);

d) applies when application software is developed for systems having limited variability or fixed programmes but does not apply to manufacturers, safety instrumented systems designers, integrators and users that develop embedded software (system software) or use full variability languages (see IEC 61508-3);

e) applies to a wide variety of industries within the process sector including chemicals, oil refining, oil and gas production, pulp and paper, non-nuclear power generation;

NOTE Within the process sector some applications, (for example, off-shore), may have additional requirements that have to be satisfied.

f) outlines the relationship between safety instrumented functions and other functions (Figure 4);

g) results in the identification of the functional requirements and safety integrity requirements for the safety instrumented function(s) taking into account the risk reduction achieved by other means;

h) specifies requirements for system architecture and hardware configuration, application software, and system integration;

i) specifies requirements for application software for users and integrators of safety instrumented systems (clause 12). In particular, requirements for the following are specified:

– safety life-cycle phases and activities that are to be applied during the design and development of the application software (the software safety life-cycle model). These requirements include the application of measures and techniques, which are intended to avoid faults in the software and to control failures which may occur;

– information relating to the software safety validation to be passed to the organization carrying out the SIS integration;

Copyright 2004 ISA. All rights reserved.

- preparation of information and procedures concerning software needed by the user for the operation and maintenance of the SIS;
- procedures and specifications to be met by the organization carrying out modifications to safety software;

j) applies when functional safety is achieved using one or more safety instrumented functions for the protection of personnel, protection of the general public or protection of the environment;

k) may be applied in non-safety applications such as asset protection;

l) defines requirements for implementing safety instrumented functions as a part of the overall arrangements for achieving functional safety;

m) uses a safety life cycle (Figure 8) and defines a list of activities which are necessary to determine the functional requirements and the safety integrity requirements for the safety instrumented systems;

n) requires that a hazard and risk assessment is to be carried out to define the safety functional requirements and safety integrity levels of each safety instrumented function;

NOTE See Figure 9 for an overview of risk reduction methods.

o) establishes numerical targets for average probability of failure on demand and frequency of dangerous failures per hour for the safety integrity levels;

p) specifies minimum requirements for hardware fault tolerance;

q) specifies techniques/measures required for achieving the specified integrity levels;

r) defines a maximum level of performance (SIL 4) which can be achieved for a safety instrumented function implemented according to this standard;

s) defines a minimum level of performance (SIL 1) below which this standard does not apply;

t) provides a framework for establishing safety integrity levels but does not specify the safety integrity levels required for specific applications (which should be established based on knowledge of the particular application);

u) specifies requirements for all parts of the safety instrumented system from sensor to final element(s);

v) defines the information that is needed during the safety life cycle;

w) requires that the design of a safety instrumented function takes into account human factors;

x) does not place any direct requirements on the individual operator or maintenance person.

y) <u>For existing SIS designed and constructed in accordance with codes, standards, or practices prior to the issue of this standard (e.g., ANSI/ISA-84.01-1996), the owner/operator shall determine that the equipment is designed, maintained, inspected, tested, and operating in a safe manner.</u>

Copyright 2004 ISA. All rights reserved.