Certificating a safety related part of a control system

Marita Hietikko, Mika Riihimaa
VTT Expert Services Ltd, P.O. Box 345, FI-33101 Tampere, Finland
Tel: +358 20 722 111, E-mail: marita.hietikko@vtt.fi, mika.riihimaa@vtt.fi, www.vttexpertservices.fi

KEY WORDS functional safety, certification, logics, safety functions, machinery

ABSTRACT

Certification is used for proving that a product is designed, manufactured and validated according to standards. This paper highlights the significance and advantages of utilizing third-party certification services to prove the functional safety of programmable electronic system or a safety related part of a control system or a safety related control functions of machinery or other automation systems. Activities and important issues relating to hardware and software safety life cycle process are discussed, based especially on the requirements of IEC 61508 and ISO 13849-1. The focus is especially on the logic units intended to use for safety functions.

1 INTRODUCTION

Certification is a written evidence for indicating that an object, person or organization has certain characteristics and fulfils certain national or international requirements. There are three different types of certifications. In the first-party certification, the product manufacturer or service provider offers assurance that certain requirements are fulfilled. In second-party certification, an association to which the organization or individual belongs can provide the compliance assurance. Third-party inspection and certification includes an independent assessment which declares that specified requirements relating to a product, person, process or management system have been met.

Accreditation is an indication that the inspection body is competent and reliable party to make assessments in accordance with the requirements. The inspection body may issue a certificate of inspection as witness of conformity. These certification and inspection services are intended to ensure and assess compliance to the previously defined standards and regulations, but also to provide an official certification. A notified body normally accepts the official accredited third party inspections and certifications without questioning as part of demonstration of compliance with requirements. A notified body which is nominated by the national authority can make the official conformity inspection and can provide e.g. a type examination certificate.

For the safety related part of a control system specified requirements are set out in functional safety standards (e.g. IEC 61508, ISO 13849-1). Certificate is an easy way to prove that product, system or person meets the requirements of standards. Without certification there is always need to prove conformity to standards separately case by case.

The logic units to ensure safety functions (safety logic units) are among the common components to which manufacturers have applied for certifications. The use of certificated components makes the design work of a safety related control function easier. Chapter 2 of this paper highlights what are logic units to ensure safety functions and why this issue is discussed. Chapter 3 describes the procedure what is necessary to do by the designer to get the safety function certified according to ISO 13849-1. The advantages of the certification are highlighted in Chapter 4 of this paper.

2. LOGIC UNITS TO ENSURE SAFETY FUNCTIONS

At the end of 2009 the application of the new Machinery Directive 2006/42/EC (called MD in this text) became mandatory. There are several differences between the former and the new MD. One of these relates to control systems and concerns "logic units to ensure safety functions". These products are nowadays stated in Annex IV of the new MD. This Annex includes products which due to their function are a source of particularly high hazards in the event of a fault. Accordingly, stricter requirements apply to the conformity assessment method. Products are affected by this new provision if they are safety components designated by the MD and if they are "logic units to ensure safety functions" in accordance with Annex IV (No. 21) of MD.

"Safety component" in accordance with the MD means a component

- which serves to fulfil a safety function
- which is independently placed on the market
- the failure and/or malfunction of which endangers the safety of persons, and
- which is not necessary in order for the machinery to function, or for which normal components may be substituted in order for the machinery to function.

According to MD, a safety PLC is classified as a safety component. The definition applies both to products which are employed solely for safety functions and to products which at the same time fulfil both safety functions and machine functions. An indicative list for determining whether a component is a safety component can be found in Annex V of the MD.

The inclusion of these components (logic units to ensure safety functions) in Annex IV of MD is based on the growing use of functional safety products in machine controls. There is no definition for "logic units to ensure safety functions" in MD. Among the safety professionals the following definition has been suggested: *"Logic units to ensure safety functions" are devices, assemblies or components intended to be applied in safety-related parts of control systems to realise - solely or amongst others - safety functions and which generate the output signal(s) based on an internal logic operation with the input signal(s)".*

According to the MD Recommendation for Use (RFU) document, logic units to ensure safety functions according to Annex IV, 21 include, for example:

- Proximity devices for safety functions (for example, PDF-X according to EN 60947-5-3);

- Interlocking devices with electromagnetic guard locking (e.g. locking by magnetic force as opposed to locking with a bolt) for safety functions according to EN ISO 14119 (for protection of persons);
- Trapped-key interlocking systems for safety functions, where the algorithm is included in the system;
- Protective devices for indirect detection of the presence of persons, for example, by the use of RFID technology;
- Protective devices for the detection and deactivation of possible hazards (not a warning system only), such as the detection of laser radiation;
- Safety control units, for example, for the monitoring of speed, vibration, torque, temperature, pressure, force, guards, emergency stop devices, two-hand control devices, enabling devices, rotary encoders, length measuring devices, braking control units;
- Safety PLCs;
- Power Drive Systems (for example, PDS(SR) according to EN 61800-5-2) with one or more integrated safety functions (e.g. STO, SS1, SS2, SLS, SBC), e.g. frequency inverters, servo converters;
- Time delay devices for safety functions;
- Devices for the logical processing of safety-related signals of safety bus systems; excluding devices/components to be applied in "black channels" according to EN 61784-3 (black channel is a communication channel without available evidence of design or validation according to IEC 61508);
- Banks of valves with self-contained logic combination of safety relevant signals, for example, a safety valve block for presses.

All devices are intended to be applied in performing a safety function(s). The manufacturer must give at least one of the following product characteristics: Performance Level (PL) or Safety Integrity Level (SIL).

Position switches (with direct opening action, interlocking devices with mechanical guard locking, emergency stop devices, enabling switches, relays/contactor relays with mechanically linked contacts, contactors with mirror contacts, contact expansion modules (enhancement to safety switchgear), devices for under-voltage release for supply disconnecting devices (main switches) intended for use in safety functions (for example to prevent restarting following power restoration), brake assemblies, valves with additional means for failure detection intended for the control of dangerous movements on machinery, equipment for protection against overpressure (e.g. pressure valves), equipment for stopping of movement (e.g. resettable check valves) and safety clamps for piston rods of hydraulic or pneumatic cylinders are considered **not to be a logic unit** to ensure safety functions according to Annex IV of MD, because they do not perform logic operations for the control of a safety function(s).

Article 12 of the MD lists various ways for the demonstration of a product's conformity with the provisions of the MD. In this Article Paragraphs 3 and 4 are relevant for the "logic units to ensure safety functions" that are mentioned in Annex IV of MD. The following conformity assessment procedures are possible (see Figure 1):

a) Conformity assessment by the manufacturer in accordance with Annex VIII (only where manufacture is fully in compliance with the harmonised standards)

b) EC type examination in accordance with Annex IX by a notified body and internal checks on the manufacture in accordance with Annex VIII, No. 3

c) Full quality assurance in accordance with Annex X

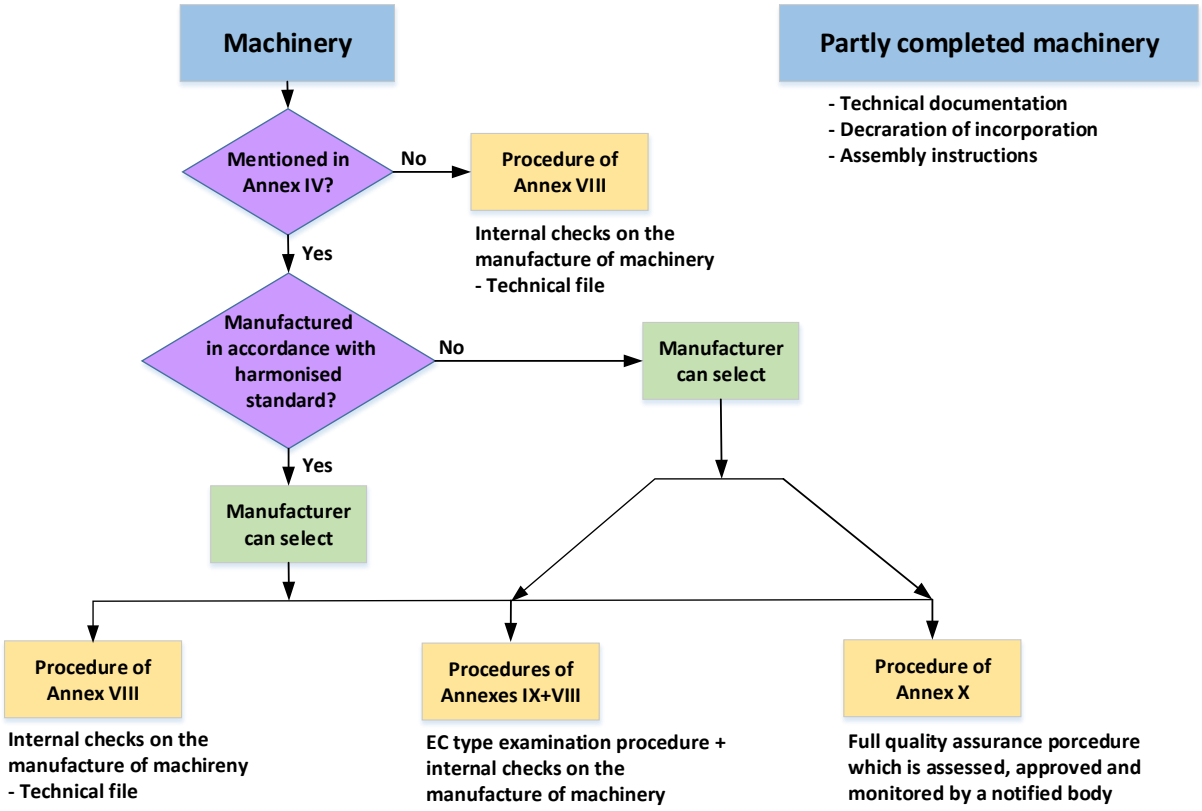

Figure 1. Conformity assessment according to Machinery Directive 2006/42/EC.

3. CERTIFCATION OF A SAFETY FUNCTION

It is important to first identify and specify the safety functions of a safety related control system. This is done by the safety related control system designer and it is more described e.g. by Hedberg et al. For each selected safety function it is necessary that the required performance level (PLr) has been defined, based either on a C type machinery safety standard, if available, or using a risk analysis. A risk graph method described, for example, in ISO 13849-1 (See Figure 2) is one technique for defining PLr for a safety function. In the risk graph method the PLr is defined by estimating the following parameters: the severity of possible injury, frequency and/or exposure to hazard and the possibility of avoiding hazard or limiting harm. A safety function, including component and architecture selections, is designed so that the defined PLr is fulfilled. The designer has to consider and document the following list of measures when designing safety functions so that they fulfil PLr's and if the designer's employer will apply certification for the safety functions (see also Figure 2):

- A safety block diagram for each safety function; preferably utilising designated architectures of ISO 13849-1 so that input-logic-output structure can be clearly identified. The safety block diagram consists of only those components that participate in the execution of a safety function. Safety block diagram

typically consists of input (e.g. sensors, limit switches etc.), logic (e.g. programmable logic controller, i.e. PLC) and output (e.g. actuators, contactors etc.) components (into which also cables and connectors are included). The safety function can be either single channel solution or duplicated one.

- The category of each safety function can be estimated based on safety block diagrams.
- Mean time to failure (MTTF) or mean time to dangerous failure (MTTFd) values of components that are parts of the safety functions. MTTF or MTTFd values are typically gathered from component data sheets or asked from the component manufacturers' representatives.
- Diagnostic coverage (DC) for input, logic and output parts of the safety functions. Diagnostic coverage (DC) is a measure for the effectiveness of diagnostics. It can be determined as a ratio between the failure rate of detected dangerous failures and the failure rate of total dangerous failures, and it is expressed as percentage units. There are two methods available for estimating DC: FMEA and Annex E of ISO 13849-1.
- Common cause failures (CCF). CCF is defined as failures of different items that result from a single event, but these failures are not consequences of each other (Annex F of ISO 13849-1)..
- Measures against systematic failures (Annex G of ISO 13849-1).
- Software (embedded / application); information required in Chapter 4 of ISO 13849-1 and IEC 61508 parts 3 and 7, which give additional information for software-specific issues.

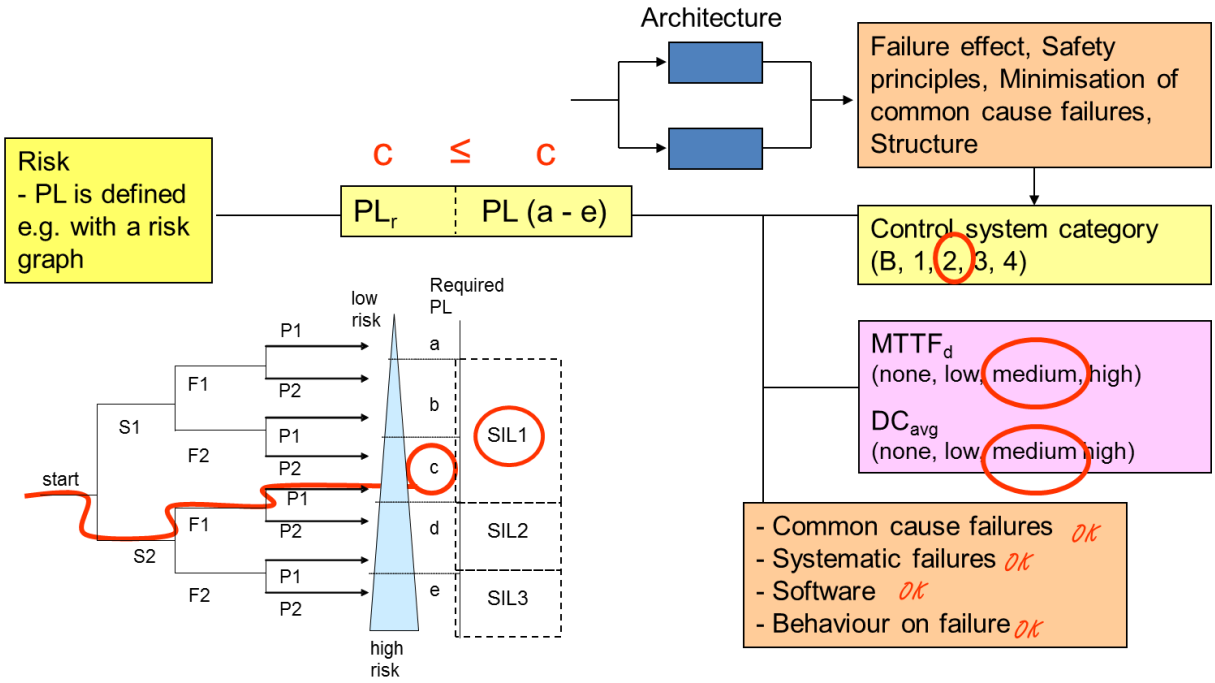

Figure 2. Definition of the required performance level (PLr) with graph. The right part of the figure shows the principles of inspecting that the required PL has been achieved.

PL for each safety function can be estimated using a graph or table of ISO 13849-1. It is important that the things mentioned in the list above are carefully documented if a certification will be applied for the safety functions.

4 DISCUSSION

The advantages of certification can be seen on the decrease of non-conformities in all phases of a product life cycle and shortened time to market process. Certification makes easier to sell product and may open totally new markets for product. Processes, tools and procedures in accordance with the safety standards requirements simplify and systemize all activities. The use of certified safety components decreases needed work in all phases but especially in requirements specification, design, testing, verification, validation and commissioning phases. Machine manufacturers' work became easier if they use certificated safety functions, logics and components in machine control systems. Also buying machines including certificated control system safety functions makes the work of the customer easier, because it is not necessary to clarify all the details of safety related components. This is remarkable issue for machine line manufacturers or integrators. Certification makes the system safety cooperation easier between suppliers and subcontractors. This also increases the speed of deliveries. It is also easier to address the competence and the fulfilment of legal requirements. Customer satisfaction and business will increase. Certification also makes for products or companies easier to access to the international market or suppliers for safety critical industries.

5 REFERENCES

Hiles A. Business Continuity Management: Global Best Practices. Edited by Noakes-Fry K. 4th ed. Rothstein Publishing, 2014. 443 p.

IEC 61508:2010. Functional safety of electrical/electronic/programmable electronic safety-related systems. Parts 1-7.

ISO 13849-1:2015. Safety of machinery. Safety-related parts of control systems. Part 1: General principles for design. 3. Ed.

Machinery Directive, 2006/42/EC.

BGIA. Logic units to ensure safety functions. 9 p. www.dguv.de/bgia

Recommendation For Use (RFU), CNB/M/11.045/R/E Rev 05. 2011. 2 p.

Hietikko M, Malm T, Alanen J. Functional safety of machine control systems. Instructions and tools for the creation of standard safety process. VTT Research notes 2485. 2009. 75 p + app. 14 p.

Hedberg J, Söderberg A, Tegehall J. How to design safe machine control systems—a guideline to EN ISO 13849-1. SP REPORT 2011:81, Borås; 2011. 78 p. ISBN: 978-91-87017-14-8.

Hietikko M, Malm T, Saha H. Comparing performance level estimation of safety functions in three distributed structures. Reliability Engineering and System Safety 134(2015) 218–229.