Journal of Loss Prevention in the Process Industries 40 (2016) 461–470

Contents lists available at ScienceDirect

Journal of Loss Prevention in the Process Industries

journal homepage: www.elsevier.com/locate/jlp

Procedure for assessing hardware safety integrity in legacy systems

Gi Young Kim [a], Ki Hoon Yoo [a], Byung Gak Ko [b], Joong Soon Jang [a, *]

[a] Department of Industrial Engineering, Ajou University, 206 World Cup-ro, Yeongtong-gu, Suwon-si, Gyeonggi-do, Republic of Korea
[b] IT Safety Engineering Center, Korea Testing Laboratory, 199 Techno 2-ro, Yuseong-gu, Daejeon, Republic of Korea

ARTICLE INFO

Article history:
Received 26 February 2015
Received in revised form
30 November 2015
Accepted 23 January 2016
Available online 26 January 2016

Keywords:
Hardware safety integrity
Legacy system
Safety integrity level
Boiler control system
IEC 61508

ABSTRACT

Functional safety is related to the safety functions of a safety-related system that uses electrical/electronic/programmable (E/E/PE) devices such as sensors, logic solvers, and final elements. A legacy system is a safety-related system which offers safety functions but which was not designed to comply with the IEC 61508 standard. This paper presents a procedure for assessing the hardware safety integrity of a legacy system so as to confirm its functional safety. The procedure defines the systematic relationship between the safety function and hardware system using a function-structure map (FSM) and assesses the hardware safety integrity centered on the safety function. The proposed procedure is applied to a boiler control system of a fossil-fuel power plant.

1. Introduction

Functional safety is part of the overall safety relating to the equipment under control (EUC) and the EUC control system that depends on the correct functioning of the electrical/electronic/programmable electronic (E/E/PE) safety-related systems and other risk reduction measures (IEC, 2010c). Functional safety consists of a safety function and the safety integrity. A safety function is one which is implemented to reduce the risks to acceptable levels or eliminate them through hazard analysis. Safety integrity means the probability of an E/E/PE safety-related system successfully providing the specified safety function. The safety integrity level (SIL) is a critical measure for evaluating the integrity of a safety function. When a selected safety function is operated with the required level of safety integrity, the functional safety of a specific function is attained in the designated system.

Since SIL is an important parameter in the development of a safety-related system, several studies have been conducted to determine a means of evaluating the SIL. Echeverria et al. (2009) used graphical analysis to determine the SIL that is suitable for the safety-related function. Baghaei (2013) improved the parameters used in the risk graph, and employed this method to derive the target SIL. Hauptmanns (2004) and Dutuit et al. (2008) utilized fault tree analysis to obtain the required SIL in the design and development phases. Catelani et al. (2011) proposed a simple and effective SIL evaluation technique that is compliant with the requirements of the IEC 61508. Beckman (1998) proposed the SIL assessment procedure in accordance with IEC 61508.

Almost all of the functional safety standards, for example IEC 61508, IEC 61511, and ISO 26262, focus on SIL determination in the design and development of new safety-related systems. Previous studies have focused on a procedure for deriving a target SIL which is expected to achieve the required safety goal in the design phase. Although the previous SIL assessment procedure for safety functions was inappropriate for application to a legacy system, there has been no progress towards developing the SIL evaluation process for existing systems.

Some studies have conducted SIL assessment for the safety functions. Hietikko et al. (2011) performed hazard and risk analysis to evaluate the SIL based on safety functions. Since hazard analysis and risk assessment are closely related to the SIL determination, Baybutt (2012) presented the need for different approaches to execute accurate analyses. Other studies have performed SIL evaluation for safety-related systems. Kim and Kim (2013) carried out hardware SIL assessment for the flame scanner system which is part of the fossil-fuel power station. Lee and Yamada (2010) conducted risk analysis of the power-assist system and determined the SIL of the safety-related systems.

IEC 61508 has emphasized that SIL assessment should be applied to the safety functions for E/E/PE safety-related systems

* Corresponding author.
E-mail address: jsjang@ajou.ac.kr (J.S. Jang).

http://dx.doi.org/10.1016/j.jlp.2016.01.019
0950-4230/

(IEC, 2010a). Problems occur, however, when the SIL assessment is intended for safety-related systems. A safety-related system is typically responsible for several safety functions. In this case, when the SIL assessment is applied to a safety-related system, all of the safety functions return the same SIL value which is inaccurate. To prevent such errors, the object of SIL assessment must be the safety function.

Legacy systems which are safety-related but which were not developed in accordance with functional safety standards are found in various fields. While basic safety has been evaluated and verified, functional safety has never been identified for legacy systems. For this reason, accidents associated with functional safety continue to occur. Since the turn of the century, a number of people had been injured due to an explosion at BP Petroleum storage tank facility and explosion of a fuel gas tank of a bus in Republic of Korea. To prevent accidents caused by legacy systems, The 61508 Association (2011) published its safety management guidelines for legacy systems. The guidelines stipulate activities to maintain the functional safety of legacy systems.

The highest priority is to correctly identify the current SIL of the safety functions to ensure functional safety of the legacy system. However, the 61508 Association's guidelines do not provide information on SIL evaluation of legacy systems. SIL assessment for a legacy system enables the parties to determine whether the safety functions of existing systems satisfy the required performance and reliability criteria. If the legacy system satisfies the safety-related requirements, further action is not required to ensure functional safety. However, when the safety functions of the legacy system do not provide a sufficiently high level of performance, additional activities would be required to improve the reliability of the safety functions.

To solve these problems, this study proposes the procedure for assessing the hardware SIL based on the safety functions of a legacy system. Function analysis is performed on the legacy system. The identified functions are classified into safety functions and performance-related functions. A function-structure map (FSM) is used to respond effectively to the safety functions of the related hardware components. SIL assessment is done for the safety functions associated with the hardware components. To this end, the method of estimating the dangerous hardware failure rate and evaluating the architectural constraints is proposed. As a case study, the procedure is applied to the boiler control system of a fossil-fuel power plant.

2. Procedure for assessing hardware safety integrity

A legacy system is a safety-related system which is responsible for one or more safety functions as defined in IEC 61508, but which was designed before the publication and adoption of the IEC 61508 standard (The 61508 Association, 2009). Since the safety of a legacy system cannot be known without performing an evaluation, the SIL assessment is essential to recognizing the current state. If a legacy system proves to be sufficiently safe, additional actions are not required to enhance the system safety. However, the legacy system may not be safe enough. In this case, it is necessary to identify fundamental causes that adversely affect the safety of the existing systems. Root causes can be categorized into two types: absence of safety functions or lack of reliability. When hazard analysis reveals that safety functions are absent from a legacy system, additional safety-related systems are implemented to provide the required safety functions. If the safety functions are unreliable, techniques of reliability growth management are applied to the safety-related system.

In a functional safety concept, the scope of SIL assessment is the safety functions rather than the safety-related systems. If the object of SIL assessment is the safety-related systems, the determined SIL value will be inaccurate. A safety-related system performs several safety functions and each safety function is realized by different hardware and software components. In this case, when SIL assessment is performed for the safety-related systems, an error occurs in that all of the safety functions return the same SIL value. Since the smallest SIL among various values is selected as the overall value for the safety-related system, the SIL for the partial safety functions is estimated as a value that is lower than that acquired for each function. Therefore, the adequate safety functions can be evaluated as not satisfying the required SIL.

To solve the existing problems and perform hardware SIL evaluation, a detailed concept must be investigated for functional safety. SIL assessment of the hardware components requires a simultaneous evaluation of the system hardware failure rate and architectural constraints (IEC, 2010b). To evaluate these architectural constraints, the concepts of safe failure fraction (SFF), hardware fault tolerance (HFT), and the component types specified in IEC 61508 must be assessed. Depending on the operation mode of the safety function, appropriate parameters of the dangerous hardware failure rate must be decided. Fig. 1, below, shows the hierarchical relationship of these concepts using the fault tree.

The hardware safety integrity assessment procedure can be divided into three main parts. Fig. 2 shows the detailed flow of the process and the activities performed in each step. Hardware SIL assessment can be divided into the following: the basic assessment process; the architectural constraints assessment considering the hardware structural aspects; and the dangerous hardware failure rate assessment process. As a basis for assessing the hardware SIL, the basic assessment process consists of function analysis, hazard analysis and risk assessment, diagram generation, and failure rate estimation of the parts or components. Further qualitative and quantitative analysis of the hardware is then performed based on the information obtained in the basic assessment process.

2.1. Basic assessment procedure

In the basic assessment process, function analysis is performed using the system level requirements. The analysis lists the functions performed by EUC or EUC control systems and describes each function in detail. The structure block diagram (SBD) is generated based on the design drawings and the schematic diagram to show the system architecture. Then, the FSM is drawn to explain the systematic connection between the functions and the hardware components. Fig. 3 shows a typical FSM. The functions are categorized according to the functional level, and are listed on the left side. The right side shows the hierarchical structure of the hardware. Functions on the left and the required hardware components on the right are connected by a line. The FSM helps us to confirm which hardware may fail when a function on the left does not perform properly, thus enabling users to efficiently find the location and cause of the failure (Kmenta & Ishii, 1998).

Hazard analysis for the defined functions confirms which results may be caused by the failure of a function. The hazard and operability (HAZOP) study is one of the most commonly used methods for hazard analysis (Baybutt, 2015). A function is categorized as being a safety function if its failure could cause harm, or as a performance-related function if its failure would cause only performance degradation. If there is a case wherein a function belongs to two categories at the same time, it is then considered to be a safety function and is included in the scope of functional safety analysis. Only the safety functions among all the functions included in the FSM and the hardware connected to the safety functions are regarded as being within the scope of the following analysis. If a hardware component simultaneously performs both the