Reliability Engineering and System Safety 152 (2016) 259–272

Contents lists available at ScienceDirect

Reliability Engineering and System Safety

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

Determining and verifying the safety integrity level of the safety instrumented systems with the uncertainty and security aspects

E. Piesik [a,*], M. Śliwiński [a], T. Barnert [b]

[a] Gdansk University of Technology, Poland
[b] Automatic Systems Engineering, Poland

ARTICLE INFO

Article history:
Received 21 February 2015
Received in revised form
16 March 2016
Accepted 24 March 2016
Available online 4 April 2016

Keywords:
Probabilistic modeling
Safety integrity level
Common criteria
Evaluation assurance level
Safety
Security
Uncertainty
Safety instrumented system

ABSTRACT

Safety and security aspects consist of two different group of functional requirements for the control and protection systems. In the paper it is proposed that the security analysis results can be used as a factor increasing or decreasing the risk level. It concerns a process of determining required safety integrity level of given safety functions. The authors propose a new approach for functional safety risk analysis. In this case the security factor influences the value of required safety integrity level SIL by changing the frequency of accident scenario. It can be done by using the methodology of modified risk graph. On the other hand there is a verification of required SIL fulfillment for designed safety-related system which implements safety function. In this case the result of security analysis is affecting uncertainty of probabilistic model parameters. The proposed method takes into consideration the sensitivity analysis of probabilistic models of E/E/PE or safety instrumented systems SIS as well as the uncertainty of probabilistic results. It uses differential factors, which are helpful for effective verification of required SIL of the E/E/PE or SIS systems taking into account results of sensitivity analysis and/or assessment of uncertainty ranges obtained from probabilistic models developed.

1. Introduction

Functional safety, which is a part of overall safety, is aimed at reducing the risk of a hazardous system operating to an acceptable or tolerable level by introducing a set of safety-related functions (SRFs). They are to be implemented by the control and/or protection systems which are usually operating in a computer network using the wire and/or wireless communication technologies. In functional safety analyses these aspects are sometimes neglected. The standard IEC 61511 does not indicate directly how to consider the safety of communication channels in the functional safety analysis. There is no doubt that it is a substantial problem, therefore in a new version of IEC 61511:2015 standard some additional requirements concerning the data communication channels in functional safety solutions are introduced [30,34,46].

One of the main objectives of functional safety analysis is determining of required safety integrity level (SIL) for the safety-related fun`ctions to be realized by safety-related systems. According to IEC 61508 to each SIL (1/4) the interval probabilistic quantitative criterion is defined. Functional safety analysis procedure usually does not include security aspects. But in case of distributed control and protection system it can have a practical significance [3–6]. It may affect the results of determining as well as verifying of SIL, taking into account functional safety analysis. The procedure of determination and verification of SIL is shown in Fig. 1.

In the paper an example of some analysis is described. It is based on a control and protection system architecture that consists of distributed control system with various communication technology. It is shown that performing of the security analysis for the control system can influence the results of determining required SIL. In this case hardware architecture of protection system (SIS) performing safety function should fulfill new requirements. In the process of verifying SIL for this architecture the security analysis can also play an important role. Its results can change the uncertainty boundaries in the probabilistic model of the safety-related system. The comparison of results obtained with including and excluding security aspects are presented and discussed.

2. Determination of the required safety integrity level

2.1. Functional safety and a general concept of risk reduction

The process of SIL determination is described in the standard IEC 61508 and it is based on the risk assessment. In this case the risk is understood as a combination of probability or frequency of dangerous

[*] Corresponding author.
E-mail address: emilian.piesik@pg.gda.pl (E. Piesik).

http://dx.doi.org/10.1016/j.ress.2016.03.018
0951-8320/© 2016 Elsevier Ltd. All rights reserved.

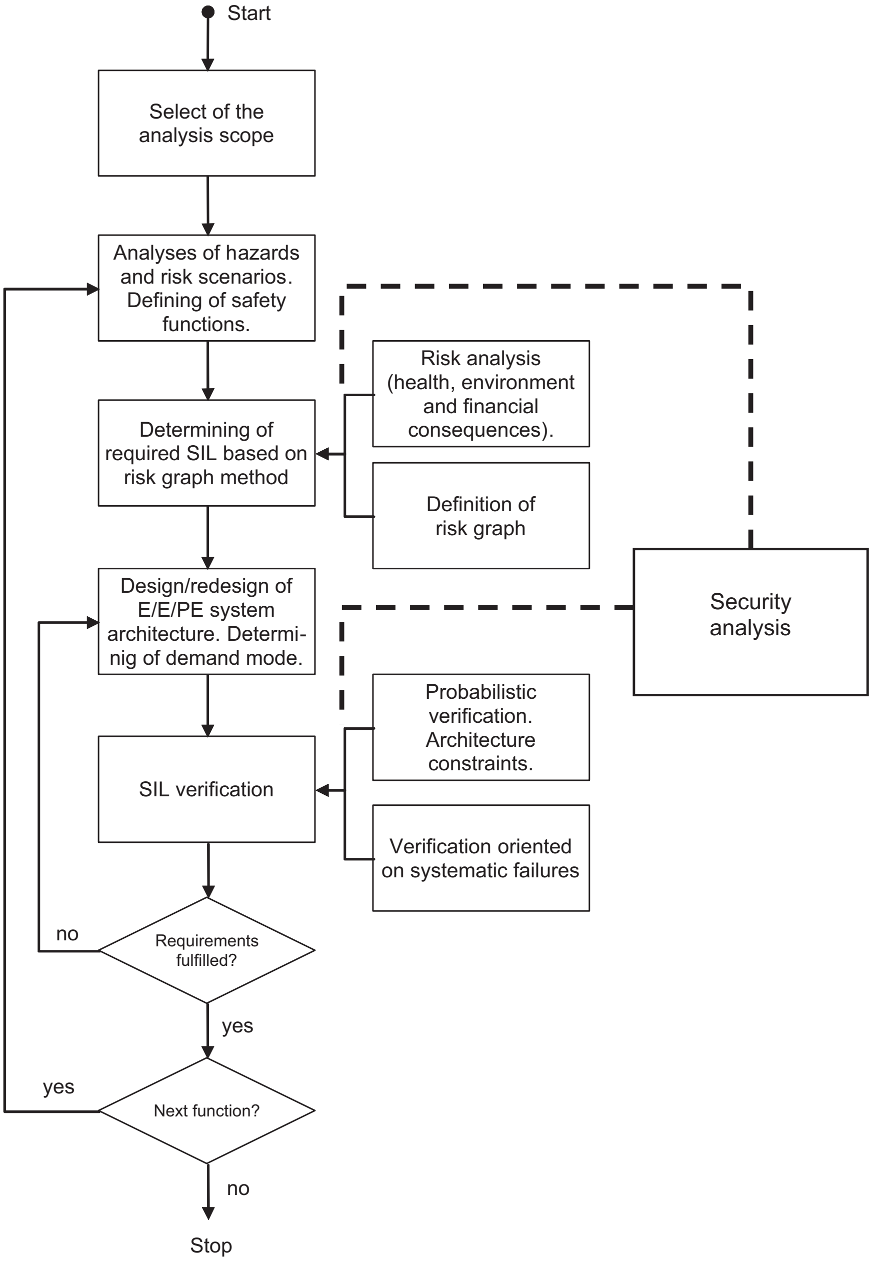
Start
Select of the analysis scope
Analyses of hazards and risk scenarios. Defining of safety functions.
Determining of required SIL based on risk graph method
Risk analysis (health, environment and financial consequences).
Definition of risk graph
Security analysis
Design/redesign of E/E/PE system architecture. Determi-nig of demand mode.
Probabilistic verification. Architecture constraints.
SIL verification
Verification oriented on systematic failures
no
Requirements fulfilled?
yes
yes
Next function?
no
Stop

Fig. 1. Functional safety analysis procedure [8].

event occurrence and its severity. It relies on information taken from a process of hazard identification as well as a further risk assessment for a designed or existing technical object as well as basic process control system. Some factors influence frequency and some are related to the consequences. The frequency parameter is basically associated with reliability of the object and control system equipment and also with some human factors.

If an EUC (equipment under control) risk is evaluated and tolerable level of risk is defined the necessary risk reduction to meet the requirement can be determined (see in Fig. 2). A basic concept of a functional safety analysis related to a process of determining required safety integrity level (SIL) is described as below:

- definition of a tolerable level of risk for the analyzed system,
- identification of the potential hazards,
- definition of the most important risk scenarios,
- definition of the safety functions,
- set an actual risk level for the analysed system,
- set a required risk reduction level for the defined safety functions, and
- express required risk reduction associated with the safety functions as a safety integrity levels.

The allocation of the necessary risk reduction using the E/E/PE safety-related system, other technology safety-related system or external risk reduction facility is achieved. The relative risk reduction (assuming that the consequence $N{=}const$) is evaluated from the formula

$$RRF = \frac{R_t}{R_{np}} = \frac{F_t}{F_{np}} \tag{1}$$

where F_t – a numerical frequency target (specified for a tolerable risk level); F_{np} – the frequency of a hazardous event that could occur without the protective system considered.