Journal of Loss Prevention in the Process Industries 43 (2016) 488–502

Contents lists available at ScienceDirect

Journal of Loss Prevention in the Process Industries

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

New considerations for SIL verification of functional safety fieldbus communication

Long Ding [a, *], Hong Wang [a], Aidong Xu [a], Shixing Li [b]

[a] Key Laboratory of Networked Control Systems, Chinese Academy of Sciences, Shenyang Institute of Automation (SIA), University of Chinese Academy of Sciences (UCAS), 114 Nanta Street, Shenyang, 110016, PR China
[b] North Automation Control Technology Institute, 351 Tiyu Road, Taiyuan, 030006, PR China

ARTICLE INFO

Article history:
Received 5 March 2016
Received in revised form
21 June 2016
Accepted 11 July 2016
Available online 15 July 2016

Keywords:
Safety integrity level
Functional safety fieldbus communication
Residual error probability
Residual error rate
Safety communication layer
Safety instrumented system

ABSTRACT

Safety integrity level (SIL) verification of functional safety fieldbus communication is an essential part of SIL verification of safety instrumented system (SIS), and it requires quantifying residual error probability (*RP*) and residual error rate of function safety communication. The present quantification method of residual error rate uses *RP* of cyclic redundancy check (CRC) to approximately replace the total *RP* of functional safety communication. Since CRC only detects data integrity-related errors and CRC has intrinsically undetected error, some other residual errors are not being considered. This research found some residual errors of the present quantification method. Then, this research presents an extended new approach, which takes the found residual errors into account to determine more comprehensive and reasonable *RP* and residual error rate. From perspective of the composition of safety message, this research studies *RP*s of those controlling segments (sequence number, time expectation, etc.) to cover the found residual errors beyond CRC detection coverage, and the influences of insertion/masquerade errors and time window on *RP* are investigated. The results turn out these residual errors, especially insertion/masquerade errors, may have a great influence on quantification of residual error rate and SIL verification of functional safety communication, and they should be treated seriously.

1. Introduction

Ever since IEC 61508 (IEC, 2010a) was published, many safety standards for process industry have been developed and published, such as IEC 61131-6 and IEC 61511. Safety PLC (Programmable Logic Controller) and safety instrumented system (SIS) which are compliant with these safety standards are being released in the world. In a SIS, functional safety fieldbus performs transmission of safety data. Sufficient reliability of the functional safety fieldbus is vital for the safety function of SIS, Cauffriez et al. (2004) discussed different aspects linked to the design and assessment of intelligent distributed control systems, in particular the communication function, from a dependability point of view. Safety integrity level (SIL) verification of functional safety fieldbus communication is an indispensable step in the integral SIL verification of safety-related system (SRS). However, in the past, almost all attention on SIL verification has been paid to hardware and system level of SRS, and this is reflected in IEC 61508-6 (IEC, 2010b), ISA-TR84.00.02 (ISA, 2002) and scientific literatures (Liu and Rausand, 2011; Jin et al., 2011; Kim and Kim, 2013; Ding et al., 2014; Wang and Rausand, 2014).

IEC 61784-3 is the international standard of functional safety fieldbus communication. According to IEC 61784-3-0 (IEC, 2010c), SIL verification of functional safety fieldbus communication means calculation of residual error rate, and residual error rate of safety fieldbus should be less than 1% of the maximum *PFD* or *PFH* corresponding to target SIL, see Section 2.4. Residual error rate is calculated from residual error probability (*RP*) and transmission rate of safety messages. *RP* is called undetected error probability (P_{ue}) in the context of error control theory. There are several different methods proposed in literatures related to various aspects of calculation of P_{ue}, including *direct code analysis* (Wolf and Blakeney, 1988), *transformed code analysis* (Wolf and Blakeney, 1988), *recursive method* (Agarwal and Ivanov, 1992), *Special Hardware* (Chun and Wolf, 1994), *Bayesian inference* (Wacker and Börcsök, 2007a), *probabilistic method* (Wadayama, 2010) and *the Monte-Carlo-simulation*. The difference between P_{ue} and *RP* is that, P_{ue} is only determined for certain error detection code in the

* Corresponding author.
E-mail address: dinglong@sia.cn (L. Ding).

http://dx.doi.org/10.1016/j.jlp.2016.07.013
0950-4230/

context of error-control theory, while generally, *RP* is determined for superimposed safety data integrity assurance mechanism including error detection code.

In recent years, some works have been done on the dependability evaluation of systems using fieldbus-based devices. Portugal and Carvalho (2004a) presented a hierarchical modeling approach using stochastic Petri Nets to evaluate dependability of fieldbus networks, and Portugal and Carvalho (2004b) evaluated dependability of PROFIBUS-DP networks by using the approach. Lei et al. (2010) presented a novel network reliability assessment method that provides diagnostic and prognostic information for DeviceNet. Langeron et al. (2011) used stochastic Petri nets to implement a model for dependability assessment of network-based SRS. Mkhida et al. (2014) used Monte-Carlo method to assess the dependability parameters of SIS in compliance with IEC 61508 & IEC 61511 using fieldbus-based instruments. However, those work are not focus on SIL verification of functional safety fieldbus communications.

Some research works have also been done on *RP* of functional safety communications. Using *direct code analysis*, Börcsök, Schwarz and Wacker et al. did some work related to P_{ue} of functional safety communication, including requirements and specifications to be considered for SRS (Börcsök and Schwarz, 2006), dual code of CRCs (Wacker and Börcsök, 2007b), weight distribution of proper linear codes (Wacker and Börcsök, 2008), P_{ue} calculation of redundant data transmission (Börcsök et al., 2006), residual error rates for safety-critical communications (Börcsök and Hannen, 2007). Frank Schiller and Tina Mattes et al. did some work on CRC for safety-critical communications and presented three methods to ensure a low *RP*, including combinations of CRC (Mattes et al., 2007), nested CRC (Mattes et al., 2008), CRC concatenated with parity bits (Mattes and Schiller, 2010), and they presented a new method to determine *RP* of safety-critical communications by means of *deterministic and stochastic automata* that handles the polynomial complexity since determination of the characteristics of a polynomial is usually very complex (Schiller and Mattes, 2007). The good news is that, these work related *RP* with functional safety communications; regrettably, these work talked about research on the P_{ue} of CRCs within error detection coverage of CRCs, no research work has been done on the residual errors beyond error detection coverage of CRCs which is the topic of this research.

IEC 61784-3 adopts *direct code analysis* to quantify *RP* of safety communication, however, it uses the P_{ue} of CRC to approximately replace *RP* of superimposed safety data integrity assurance mechanism used in safety communication. In the authors' opinion, that approximate replacement is not proper, since CRC error detection code only considers data integrity of the whole message and CRC has intrinsically undetected errors.

This research found some residual errors beyond the error detection coverage of CRC, which should be taken into account for *RP* quantification of safety communication since they may have a great influence on quantification of residual error rate and SIL verification for functional safety communication.

In order to quantify *RP* and residual error rate for safety communications more comprehensively and reasonably, from perspective of the composition of message, this research studies *RP*s of those controlling segments (sequence number, time expectation, etc.), which still have some residual errors beyond the data integrity-related errors checked by CRC. This research also takes into account insertion/masquerade errors and time window errors for timeliness-related error-control measures. Based on decomposition of the message and corresponding *RP*s, the results obtained in this research is more comprehensive and reasonable than the present method. And the results turn out these residual errors, especially insertion/masquerade errors, may have a great influence on quantification of residual error rate and SIL verification of functional safety communication, and they should be taken into account seriously. Besides, it is a reminder that more attention should be paid to the quantification of residual error rate of safety fieldbus communication.

The rest of this paper is organized as follows. Preliminaries and basic assumptions are presented in Section 2. Section 3 analyses defect of CRC. In Section 4, proposed quantification approach for *RP* and residual error rate is presented. Section 5 gives results and discussion. Conclusions are given in Section 6.

2. Preliminaries and basic assumptions

2.1. Error detection performance of linear codes

Let C be a linear $[n, k, d_{\min}]_q$ code over the finite field of q elements $GF(q)$ (Galois Field), with minimum Hamming distance d_{min}. Suppose C is used for error detection on a q-ary symmetric channel with q inputs and q outputs, and ε is bit error probability. Any symbol transmitted has a probability $1-\varepsilon$ of being received correctly and a probability $\varepsilon/(q-1)$ of being transformed into each of the $q-1$ other symbols, it is natural to assume that$0 \le \varepsilon \le (q-1)/q$.

The P_{ue} of C is the probability that undetected errors occur and denoted by$P_{ue}(C, \varepsilon)$. This probability is expressed in terms of weight distribution $\{A_i, 0 \le i \le n\}$ of C or weight distribution$\{B_i, 0 \le i \le n\}$ of$C^{\perp}$, the dual (orthogonal) code of C, as

$$P_{ue}(C,\varepsilon) = \sum_{i=1}^{n} A_i \left(\frac{\varepsilon}{q-1}\right)^i (1-\varepsilon)^{n-i} \tag{1}$$

This formula is exactly the *direct code analysis* method, where.

A_i = weight distribution of C code = number of codewords of weight i (weight = number of bits equal to 1)
ε = bit error probability (bit error rate, BER)
q = elements number of Galois Field
n = bit length of block

Using the MacWilliams Identity,

$$q^k B(x) = [1+(q-1)x]^n A\left[\frac{1-x}{1+(q-1)x}\right] \tag{2}$$

Where$A(z) = \sum_{i=0}^{n} A_i z^i$, $B(z) = \sum_{i=0}^{n} B_i z^i$,$P_{ue}(C, \varepsilon)$ can be expressed in another formula,

$$P_{ue}(C,\varepsilon) = q^{-(n-k)} \sum_{i=0}^{n} B_i \left(1 - \frac{q\varepsilon}{q-1}\right)^i - (1-\varepsilon)^n \tag{3}$$

This formula is exactly the *transformed code analysis* method, where.

B_i = weight distribution of dual code $C^{\perp}$ = number of code words of weight i
k = number of information bits in a codeword

However, since $\{A_i, 0 \le i \le n\}$ of a code and $\{B_i, 0 \le i \le n\}$ of its dual are very difficult to calculate with increase of n, many research works have been published to find alternative solutions for calculation of $P_{ue}(C, \varepsilon)$ (Agarwal and Ivanov, 1992), or find upper and lower bounds for $P_{ue}(C, \varepsilon)$ (Wolf et al., 1982), or find simpler calculation methods for weight distributions $\{A_i, 0 \le i \le n\}$ and $\{B_i, 0 \le i \le n\}$ (Kim and Lee, 1996).

The formulae (1)–(3), and more detailed knowledge of linear codes, $GF(q)$, Hamming distance and q-ary symmetric channel can