SAFETY AND DEPENDABILITY ASSESSMENT OF AN INDUSTRIAL PROGRAMMABLE LOGIC CONTROLLER

Eugen Ioan Gergely

University of Oradea
No. 5, Armatei Romane str., Oradea, Romania
Phone: +4059432830, Fax: +4059432789
Email: egergely@uoradea.ro

Abstract. Computer based systems, which are devoted to control critical functions, may incur in safety and dependability problems. In the safety area a new standard is currently emerging, IEC 61508, which is intended to provide a unified framework which may deserve as guideline for the analysis of safety related systems. The present paper deals with the safety and dependability analysis of a Programmable Logic Controller (PLC) according to the requirements of IEC 61508.

Keywords: PLC, SIL, safety, dependability

1. INTRODUCTION

The present paper deals with a comparative dependability analysis of a typical industrial Programmable Logic Controller (PLC). The PLC is based on a (2:3) voting policy and is intended to be used for safety functions. An emergent standard in the safety area is IEC 61508. A very important concept in IEC 61508 is that of Safety Integrity Level (SIL).

SILs are used as the basis for specifying the safety integrity requirements for the safety. For the determination of the appropriate SIL, the IEC 61508 is based on the concept of risk and provides a number of different methods, both qualitative and quantitative. The comparative dependability analysis of the PLC refers to the SIL as defined by IEC 61508 standard. Starting from the PLC specification and available data on the failure rates, different probabilistic methodologies have been applied to evaluate various dependability measures related to the required SIL and compared. First a Fault-Tree (FT) analysis has been carried out. From the FT both an equivalent Bayesian Network (BN) model has been derived through automatic conversion algorithms [1] and a Stochastic Petri Net (GSPN) [2,10]. Furthermore, it is shown that the GSPN model can be further simplified by resorting to a Stochastic Well Formed Net (SWN) [10,4]. If constant transition rates are assigned to timed transitions, the stochastic behavior of the PN is mapped into a Continuous Time Markov Chain (CTMC).

The paper proceeds as follows. Section 2 points out some aspects of the IEC 61508 standard. Section 3 describes the PLC architecture while Section 4 describes the application of the different techniques and the obtained results. Section 5 concludes giving the main selection criteria of the presented modeling techniques.

2. THE IEC 61508 STANDARD AND THE SAFETY INTEGRITY LEVELS

Process industry requires that well defined safety prerequisites must be achieved, as hazards may be present in such installations [3, 5]. IEC 61508 introduces a principle with the name As Low As Reasonably Practicable (ALARP). ALARP defines the tolerable risk as that risk where additional spending on risk reduction would be in disproportion to the actually obtainable reduction of risk. The strategy proposed by IEC 61508 takes into account both random as well systematic errors.

Table 1. Safety Integrity Levels: Target Failure Measures

SAFETY INTEGRITY LEVEL	LOW DEMAND MODE OF OPERATION (Probability of failure to perform its design function on demand)	CONTINUOUS / HIGH DEMAND MODE OF OPERATION (Probability of a dangerous failure per hour)
4	$\geq 10^{-5}$ to $<10^{-4}$	$\geq 10^{-9}$ to $<10^{-8}$
3	$\geq 10^{-4}$ to $<10^{-3}$	$\geq 10^{-8}$ to $<10^{-7}$
2	$\geq 10^{-3}$ to $<10^{-2}$	$\geq 10^{-7}$ to $<10^{-6}$
1	$\geq 10^{-2}$ to $<10^{-1}$	$\geq 10^{-6}$ to $<10^{-5}$

IEC 61508 [5] has introduced the concept of Safety Integrity Level (SIL) attempting to homogenize the concept of safety requirements for the Safety Instrumented Systems. According to IEC 61508 the SIL is defined as *"one of 4 possible discrete levels for specifying the safety integrity requirements of the safety functions to be allocated to the safety-related systems. SIL 4 has the highest level of safety integrity, SIL 1 has the lowest*". The target dependability measures for the 4 SILs are specified in Table 1, for systems with low demand mode of operation and with continuous (or high demand) mode of operation.

The determination of the appropriate SIL for a safety-related system is largely related to the experience and judgement of the team doing the job. IEC 61508 offers suitable criteria and guidelines for assigning the appropriate SIL as a function of the level of fault-tolerance and on the coverage of the diagnostic.

3. DESCRIPTION OF THE PLC CASE STUDY

The PLC system consists of triplicated channels, that process the input signals, and of a (2:3) hardware voter which collects the channel results to produce the output. The block diagram of the PLC architecture is shown in Figure 1.

Table 2. Failure rates for PLC components

PLC elementary blocks	Failure rates [failures/h]
DI	$\lambda_{DI}=2.8\cdot10^{-7}$
CPU	$\lambda_{CPU}=4.82\cdot10^{-7}$
DO	$\lambda_{DO}=2.45\cdot10^{-7}$
I/O Bus	$\lambda_{I/O}=2.0\cdot10^{-9}$
Inter channel bus	$\lambda_{TB}=2.0\cdot10^{-9}$
Voter HW	$\lambda_{Voter}=6.6\cdot10^{-8}$
Power supply	$\lambda_{a1}=3.37\cdot10^{-7}$

For each channel (identified as A, *B* and *C,* respectively) a digital input unit *(D*I), a processing unit *(CP*U) and a digital output unit *(D*O) are employed.

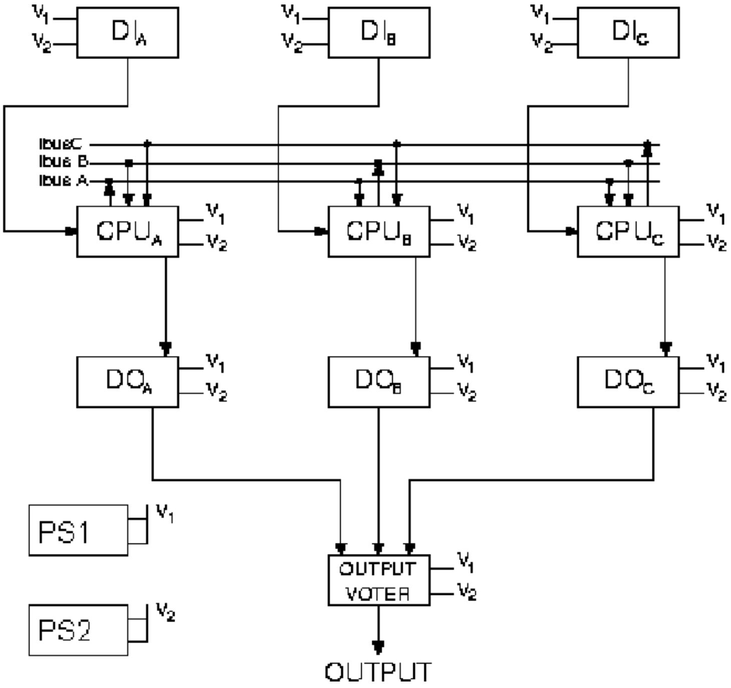

Figure 1. The PLC block diagram

Each *CPU* receives the signal to be elaborated from its *D*I, but it also receives a copy of the input signals from the other *CPUs* so that the actually elaborated input signal is the result of a software (2:3) majority voting. Finally, two independent power supply units *(PS 1* and *PS* 2) are connected in parallel redundancy to all the components, in such a way that only the breakdown of both *PS* units prevents the system to operate. The failure rates for PLC components are reported in Table 2.

The PLC works with continuous/high demand mode of operation and its safety function is the correct delivery of the digital output. According to the IEC 61508 indication and the PLC fault tolerant architecture and failure modes, SIL-2 seems the most appropriate level. The safety and dependability assessment of the PLC case study have been characterized by the following measures:
- *MTTF (Mean Time To Failure) for the system;*
- *the probability of failure of the PLC referring to SIL2 of IEC 61508 (Table 1);*
- *the most critical set of components responsible of the failure of the PLC..*

4. THE PLC MODELLING AND ANALYSING

The experience of assessing the PLC has started by building the FT model and then formally converting it into the more powerful methodologies, BN, GSPN and SWN.

4.1 The Fault Tree model of the PLC

Among combinatorial methodologies Fault Tree Analysis (FTA) has become very popular in dependability analysis and safety studies of large critical systems. The main weak point of FTA is the fact that events are considered as statistically independent, so that the methodology has a scarce modeling power counterbalanced by the ability to deal with large scale. The FTA is carried out in two steps: a qualitative step in which the list of all the minimal combinations of events (the Minimal Cut Set, MCS) leading to the TE is determined, and a quantitative step in which the probability of occurrence of the TE (and of any MCS) is calculated. The Top Event (TE) of the Fault Tree model represents the overall PLC failure and the primary events represent the failure of the elementary blocks. Implicit (2:3) gates are used in the construction of the FT. The following numerical results have been obtained using two different software tools, namely SHARPE [6] and Item-Software [7]:

Table 3. TE Unreliability and Average Unreliability vs time

Time t (h)	TE Unreliability (U)	Average Unreliability (U/t)
10,000	$8.295\ 10^{-04}$	$8.295\ 10^{-08}$
20,000	$1.993\ 10\ ^{-03}$	$9.965\ 10^{-08}$
50,000	$7.429\ 10\ ^{-03}$	$1.486\ 10^{-07}$
100,000	$2.253\ 10\ ^{-02}$	$2.253\ 10^{-07}$
200,000	$7.202\ 10\ ^{-02}$	$3.601\ 10^{-07}$
300,000	$1.407\ 10\ ^{-01}$	$4.690\ 10^{-07}$
400,000	$2.212\ 10\ ^{-01}$	5.25010^{-07}

- MTTF = 8.32 10 5 h (about 95 years)

*-The TE unreliability is given by the probability of reaching the TE and has been computed versus time from t=0 up to time t = 4*10^{5} hours. Some points are reported in the second column of Table 3. The third column reports the average unreliability (or.frequency of dangerous failure) as prescribed by IEC 61508 (see Note 5 to table 1 in IEC 61508). Since the prescribed SIL-2 in Table 1 requires that the average unreliability (or frequency of dangerous failure) should be less than 10^{-6} , it is seen from Table 3 that the predicted behavior of the PLC system s respects the SIL-2 specification.*

– The criticality of the PLC components has been evaluated by determining the MCSs of the FT. The FT has 59 MCSs, of which, one is of order 1 (corresponding to the failure of the voter) and the remaining 58 of order 2.

4.2 The Bayesian Network model of the PLC

In a BN [8] we can identify a qualitative part (the structure of the graph) and a quantitative part (the set of conditional probabilities). The quantitative part is specified by means of a Conditional Probability Table (CPT) assigned to each node. With respect to FT, BNs have the advantages [1] of allowing to include uncertainty in the model by means of probabilistic dependencies among components, to accommodate multivalued variables (instead of the binary variables of the FT) and to allow a backward diagnostic analysis that provide more significant criticality measures for each basic component or MCS.

The FT can be automatically converted into a binary BN by means of suitable conversion algorithms described in [2,10]. The measures that can be typically evaluated by means of a FT analysis, can be evaluated as well in the BN setting. However, the converse is not true.

Table 4. Posterior Probabilities for PLC Components

PLC elementary blocks	Post Failure Probability
CPU	0.38382
DO	0.20433
Power Supply	0.17603
DI	0.17167
Voter HW	0.11812
I/O Bus	0.00208
Inter channel bus	0.00175

As an example, from the BN representation, the posterior failure probability of each elementary component, given the TE failure has occurred, can be evaluated. This posterior probability is reported in Table 4, and provides a more accurate measure of the component criticality with respect to the prior probability.

4.3 The Generalised Stochastic and Well formed Petri Nets models of the PLC

Applying a conversion algorithm [2,10] to the FT, the Generalized Stochastic Petri Net model of the PLC can be easily obtained. However, the so obtained GSPN model results as a large model, with replicated subsets of elements to represent the replicated channels of the PLC. To make the model more compact, replicated elements may be folded and parameterized (colored), so that only one *representative* for each replicated class of objects is explicitly included in the model, while the identity of each replica is maintained through the parameter value (color) of the token. Stochastic Well Formed Nets introduce the new attribute, the “color”, to the tokens.

Applying SWN to the case study at hand, a single place represents a class of similar components *(DI, bus, CPU, DO, Alim*), and the identity of each specific component in each channel is preserved by assigning to the tokens an index *j (j=1,2,3)* to represent the channel The SWN model of the system can be derived automatically from the GSPN model or directly from the FT [2,10]. The main advantage of the SWN approach, is that the generated reachability graph has a reduced number of markings with respect to the corresponding GSPN, so that the Markov chain to be solved has a much smaller number of states. Table 5 shows the comparison between the number of states generated by the GSPN model and those generated by the SWN model.

Table 5. Comparison between the nbr. of states of GSPN and SWN models of the PLC

	Tangible states	Vanishing states
GSPN SWN	5639 707	45506 5400
Reduction factor	7.9	8.2

The table shows a coefficient of reduction in the number of generated states of about one order of magnitude.

5. CONCLUSIONS

Fault Tree analysis (FTA) has been completely adequate to perform the required PLC safety and dependability assessment, including the identification of PLC most critica components. FTA methodology is able to deal with large dimension problems and is often.cheap in terms of computational costs. A weakness of FTA is in considering statistically independent events. Modelling by Petri Nets allows an immediate representation of logical interaction among subsystems and of system activities (i.e. synchronisation, sequentially, concurrency). When system activities can be represented by exponential distributions, analytical solution of Petri Nets, is granted through the solution of the underlying stochastic process which is a CTMC. SWN versus GSPN can reduce the state explosion problem allowing to keep into account possible symmetries of the model, as in the case of PLC architecture, which relays on the replica of identical channels.

Other than proper probabilistic modeling methodologies, Bayesian Networks have been investigated. BN versus Fault Trees can answer some interesting questions allowing both forward and backward analysis; moreover BN are more suitable to represent local dependencies among components and to include uncertainty in modeling. On the other side, BN do not provide a direct mechanism to implement temporal dependencies, which are well implemented in Petri Nets.

Concluding, the selection of the most appropriate modeling technique depends upon on the compromise between the required modeling accuracy and the acceptable analytical complexity of the model.

REFERENCES

[1] A. Bobbio, L. Portinale, M. Minichino, E. Ciancamerla, (2001), Improving the Analysis of Dependable Systems by Mapping Fault Trees into Bayesian Networks, *Reliability Engineering and System Safety Journal*, No. 71/3, pp 249-260

[2] M. Malhotra, K. S. Trivedi, (1995), Dependability modeling using Petri Nets, *IEEE Transactions on Reliability*, Vol. 44, pp 707-714

[3] E. I. Gergely, (1997), Dependability analysis of distributed computing systems, *2nd Phd essay, University of Oradea*, pp 33-40

[4] G. Chiola and C. Dutheillet and G. Franceschinis and S. Haddad, (1993), Stochastic Well-Formed Coloured Nets for Symmetric Modelling Applications, *IEEE Transactions on Computers*, Vol. 42, pp 1343-1360

[5] S. Bologna, (1998), Safety applications of programmable electronic systems in the process industry: impact of emerging standards, *16th International System Conference*, Seattle, USA, pp 14-18

[6] R. Sahner, K. S. Trivedi, A. Puliafito, (1998), Performance and reliability analysis of computer systems – An example based approach using the Sharpe software package , *Kluwer Academic Publishers*

[7] Item Software "Fault Tree+ - Fault and Event Tree Analysis Program", (1998), *Isograph Ltd*, 1998

[8] Finn V. Jensen, (1996), An Introduction to Bayesian Networks, *UCL Press Limited*

[9] G. Chiola, G. Franceschinis, R. Gaeta, M. Ribaudo, (1995), GreatSPN 1.7: Graphical Editor and Analyzer for Timed and Stochastic Petri Nets, *Performance Evaluation*, Vol. 24, pp 47-68

[10] A. Bobbio, G. Franceschinis, R. Gaeta, L. Portinale, (1999), Exploiting Petri Nets to support Fault Trees Based Dependability Analysis, *8-th International Conference on Petri Nets and Performance Models - PNPM99*, pp 146-155