Time response of safety function realised by decentralised SRCS with safety PLC

Juraj Ždánsky
University of Žilina, Faculty of Electrical Engineering
Department of Control and Information Systems
Univezitná 8215/1, 010 26 Žilina, Slovak Republic
juraj.zdansky@fel.uniza.sk

Jozef Valigurský
University of Žilina, Faculty of Electrical Engineering
Department of Control and Information Systems
Univezitná 8215/1, 010 26 Žilina, Slovak Republic
jozef.valigursky@fel.uniza.sk

Abstract –**Guaranteed response time of a control system is a primary assumption for correct function of the system. This parameter is ever more important in case of a safety related control systems (SRCS). We have to determine a maximal response time of the realised safety functions to reach required safety parameters (it means that we have to assume the worst case of SRCS behaviour). This time depends not only on parameters of the SRCS but also on its architecture. This paper deals with influence of the above mentioned factors to response time of safety functions realised by a decentralised SRCS.**

Keywords - response time; safety PLC; SRCS; safety function

I. Introduction

Safety PLCs are common used for realisation of safety related control systems (SRCS). The safety PLCs are primary intended for industrial applications, but their use can be found in transport applications (for example: MODEST system from the company 1. Signální, ELEKSA system from Siemens, the SPA 4 system from Bombardier Corporate, etc.). We have to guarantee required safety integrity level (SIL) of realised safety function (SF) or functions (SFs) for every application. Safety integrity of hardware can be provided by suitable hardware components, architecture and diagnostics. Systematic safety integrity is possible to be provide by using methods that minimize systematic failure occurrence when we design the system [3].

For design of SRCS which realises SF or SFs with required SIL it is necessary to create a detailed specification which includes the description of their function and response time of every SF realised by SRCS. Because the response time of SF is dependent on the SRCS architecture, it is necessary to adapt this architecture in some case. We must also remember that architecture adaptation can worsen hardware safety integrity which must not exceed maximal tolerable level.

Response time will be longer in case that SF is realised by a decentralised SRCS. It is caused, besides other thing, by communication among decentralised parts of SRCS and degree of decentralisation which can causes longer delays. Influence of safety related communication is detailed described in [4, 5, 6].

This paper analyses influence of some decentralised architectures of SRCS on response time of realised SF.

II. Response Time

From a comprehensive point of view on the controlled system we have to assume that response time of safety function is the time from dangerous event occurrence until the controlled system gets into a safe state.

For mechanical devices with moving parts it is the time from sensor detection (for example light curtain, emergency stop button, etc.) to safe state (stop or slow down moving parts). Standard [7] defines an overall system stopping performance (total time to system stop) by formula:

$$t_{SFM} = t_{SRCS} + t_M, \qquad (1)$$

where t_{SFM} is an overall system stopping performance, t_{SRCS} is a response time of SRCS and t_M is a maximal time to termination of the dangerous function of the machine after the stop command is issued. Time t_M can be significantly affected by inertia of the machine´s moving parts.

Distance l between a sensor, which detects peoples entrance, and the potentially dangerous zone must be:

$$l \geq v_{max}.t_{SFM}, \qquad (2)$$

where v_{max} is a maximal assumed speed of the person (or part of body).

In industrial processes it is unlikely for the moving parts of the mechanical devices to be the source of the source of potential danger, which usually is the controlled process (for example a chemical reaction). In this case the following must apply (according to [8]):

$$t_{SFP} \leq t_{max}, \qquad (3)$$

where t_{max} is the maximal admissible time of controlled process to reach a safe state. Response time of safety function is possible to be described similarly as response time of mechanical devices. We can divide this time into two parts:

$$t_{SFP} = t_{SRCS} + t_P, \qquad (4)$$

where t_P is a maximal time of reaching safe state of the controlled process.

The response time of a safety function (formula (1) and (4)) is a part of the industrial process control regardless of the controlled process.

ISBN 978-80-261-0722-4, © University of West Bohemia, 2018

A. *Response time of centralised SRCS*

Response time for centralised SRCS can be described as:

$$t_{SRCS} = t_S + t_{sPLC} + t_A, \qquad (5)$$

where t_S is sensor (or sensors) response time, t_{sPLC} is response time of safety PLC and t_A is an actuator (or actuators) response time.

Response time values of sensors and actuators must be determined by manufacturer. Safety PLC is a modular system, which can be composed from different parts. Every part of the system can influence the response time of safety PLC. Parameters of safety PLC modules and their influence on response time of SF are detailed described by [9].

B. *Response time of decentralised SRCS*

Unlike the centralised SRCS in a decentralised SRCS we have to assume communication time influence on the response time of SRCS. We can describe this time for decentralised SRCS by formula:

$$t_{dSRCS} = \sum_{i=1}^{n} t_i + k.t_{com}, \qquad (6)$$

where t_{dSRCS} is a response time of distributed SRCS, t_i is a response time of hardware components which provide safety function by distributed SRCS, n is a components count, t_{com} is communication time between two parts of SRCS and k is a count of sequential two bounds transfer for SF realisation.

We cannot neglect communication time of decentralised SRCS (regardless of today´s high speed industrial networks) because application protocols are used for safety related communication. These protocols process data in an application program, which means that communication speed is not depend on cycle of data transfer via communication network only, but it also strongly depends on time period of application program. We can explain this issue on an example below.

Let´s assume that SF is realised by two safety PLCs, sensor S and actuators A_1 and A_2 (fig. 1). Safety PLC1 (sPLC1) monitors people entry by sensor S. In case of people entry detection, information is send to a safety PLC2 (sPLC2), which processes this information and changes state of actuator A_2. Then sPLC2 sends information about state change of actuator A_2 to safety PLC1. When sPLC1 receive this information, it will change state of actuator A_1. We assume that safety function was executed when state of both actuators was changed after entry detection.

We can determine response time of SF by formula (6), where $k = 2$. Communication time (t_{com}) depends on:

- used instruction sequence in safety program;
- period of operating cycle execution of safety PLC1 and safety PLC2;
- watchdog timer values of safety PLC1 and safety PLC2;
- phase shift between operating cycles of safety PLC1 and safety PLC2 (phase shift can be variable in time);
- scale of safety programs;
- communication bus speed.

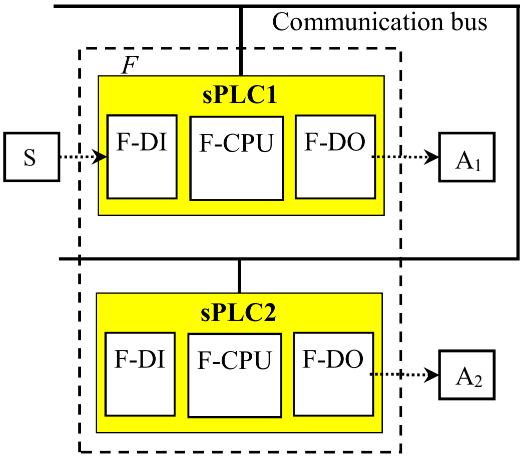

Figure 1. Safety function realised by simple decentralised SRCS

We can influence some of these factors (for example: sequence of safety program instructions). Other factors have to be assumed for the worst case, which can occur during lifetime of SRCS (for example: phase shift between operating cycle of sPLC1 and sPLC2).

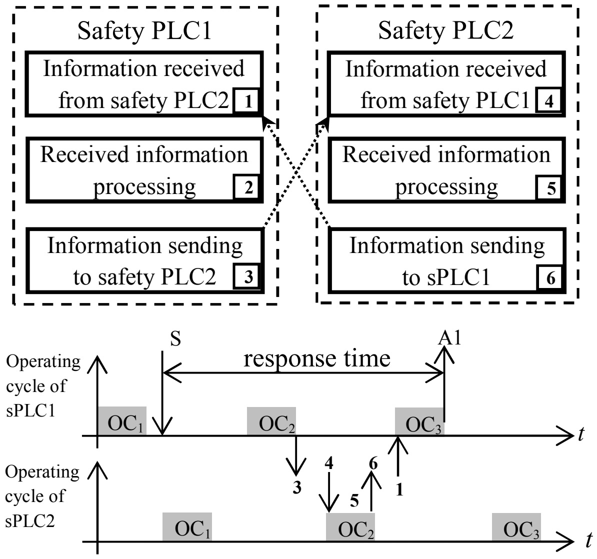
Safety PLC1
Information received from safety PLC2 1
Received information processing 2
Information sending to safety PLC2 3
Safety PLC2
Information received from safety PLC1 4
Received information processing 5
Information sending to sPLC1 6
Operating cycle of sPLC1
S
response time
A1
OC1
OC2
OC3
t
3
4
5
6
1
Operating cycle of sPLC2
OC1
OC2
OC3
t

Figure 2. Execution of SF by simple decentralised SRCS

In the Fig. 2 we can see representation of safety function execution (from detection by sensor to state change of actuator A_1) in case of optimal controlled instructions of safety program. In the fig. 2 we can see parts of safety program which are marked by numbers. Time sequence of execution parts of the program is shown in the graph. If an event occurred, the information about sensor state is transmitted to PLC2 as soon as next safety program is executed (OC_2 of safety PLC1). sPLC2 receives this information, process it and send to safety PLC1 during one operating cycle (OC_2 of the safety PLC2). Safety PLC1 changes state of actuator A_1 after it receives information from sPLC2 (during operating cycle OC_3).

III. APPLICATION EXAMPLE

Text above shows that architecture of decentralised SRCS has a significant influence on response time. This is mainly caused by important communication among parts of SRCS. This fact is described on an example below.

We assume that production line consists of three cells which do sequential tasks (every product eventually goes through every cell). Each cell is equipped by a safety PLC, which provides safety functions. Product line can also be operated by a wireless control panel (OP).

We will assume this definition of safety functions:

Name	Safety function
*F*1	First cell has to stop execution of operation after emergency stop button ES1 is pressed.
*F*2	First and second cell have to stop execute operations after press emergency stop button ES2.
*F*3	All cells have to stop executing of operations after emergency stop button ES3 is pressed.
F4	All cells have to stop execution of operations after emergency stop button ES4, which is situated on wireless control panel, is pressed.

With respect to scope of this paper, only emergency stop functions of the production line (or its parts) will be discussed further. These emergency stops will occur after emergency stop button is pushed. Of course, the conclusions of this example can be generalized for any other safety functions.

Mentioned SFs can be realised by different architectures of SRCS. Architecture of SRCS depends not only on realised SF, but also on usage of safety PLC for realisation of common control functions (functions not relevant for safety; safety PLC can work in parallel as a standard PLC for realisation of other complex functions, for example [10]). Two different architectures of decentralised SRCS, which can be used to realise said SFs, are shown in fig. 3 and fig. 4.

When we evaluate response time of safety functions, it is necessary to take into account that safety communication is possible only between two devices (model producent-consument is not supported). Therefore, from a safety relevant communication point of view, not only the network topology but primarily the configuration and programming of logical relations. These relations usually depend on safety PLC manufacturer and used hardware components. Safety relevant communication between device couples are represented in the fig.3 and fig.4 by arrows with dashed lines.

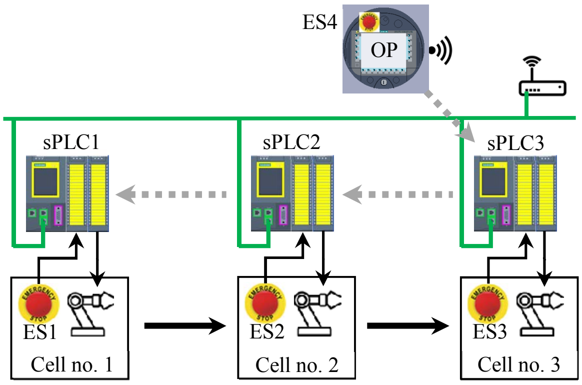

Figure 3. Production line with one- level decentralised SRCS

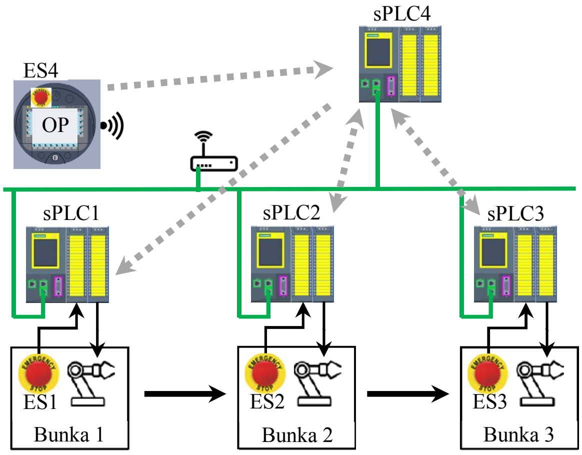

Figure 4. Production line and two-level decentralised SRCS

A. Influence of architecture of decentralised SRCS on real response time of safety functions

Response time of SFs realised by decentralised SRCS was measured under the following assumptions:

- safety PLC used for realisation of decentralised SRCS (fig. 3 and fig. 4) are from series Simatic S7-1500 (F-CPU 1516F-3PN/DP) and ET200SP (F-DI 8x24VDC, F-DO 4x24VDC/2A);
- used parameters of each modules of safety PLC are equal for every together related measured case (with respect to scope of this paper, detailed parameters are not included);
- sensors, actuators and product lines response times are not included in measured SFs response time of SRCS (excluded time parameters are independent on watched properties – influence of architecture and parameters of safety PLC on SFs response time).

Measured response times of SFs are shown in tab. 1 (all times are stated in ms). This table shows measured response times for architectures shown in fig. 3 and fig. 4. On the left side of the table we can see SFs response times for these architectures when manufacturer pre-set (default) values are used. The right side of the table shows measured response times for the same architectures in case of using optimised values compliant with [9]. Because the response time is variable, for each case a set of 10 measurements was conducted. Tab. 1 shows the average and maximal measured values.

TABLE I. RESPONSE TIME OF SFs – MEASURED VALUES

SF [ms]	Preset values of sPLC				Optimalised parameters of sPLC			
	fig. 3		fig. 4		fig. 3		fig. 4	
	avg	max	avg	max	avg	max	avg	max
*F*1	97	131	84,8	128	32,9	39	28,7	34
*F*2	129,2	190	168,2	220	34,2	37	35,4	44
*F*3	169,9	201	227	258	40	46	35,7	41
*F*4	158,4	208	109,9	158	37,4	45	23,6	28

B. *Influence of architecture of decentralised SRCS on maximal response time of safety functions*

It is evident (based on tab. 1) that architecture of decentralised SRCS and parameters optimalisation has influence on SFs response time. From the safety point of view, we cannot calculate with measured SFs response times because these times do not represent the worst possible case (for example we cannot assume measured response times to determine distance according to (2)). It is not possible to determine the worst case by measuring because we have to take into an account many different factors and their combinations which have influence on the response time. Some of factors with influence on response time can be simulated, but simulation of their combination is very difficult (or impossible). Therefore, response time has to be determined by theoretical analysis.

Maximal SFs response times for decentralised SRCS, which were shown in fig. 3 and fig. 4, are shown in the tab. 2 (all values are in milliseconds and determined by theoretical analysis by [11]).

TABLE II. MAXIMAL RESPONSE TIME OF SFs

SF [ms]	Preset values of sPLC		Optimalied parameters of sPLC	
	fig. 3	fig. 4	fig. 3	fig. 4
*F*1	174	154	61	60
*F*2	298	558	72	93
*F*3	364	558	85	93
F4	364	452	85	80

IV. EVALUATION OF EXPERIMENTAL RESULTS

In the tab. 2 we can see longer maximal response time of SFs – *F*2, *F*3 and *F*4 (safety functions which require safety relevant communication) in case of two level decentralised SRCS (fig. 4). The reason is, that for these safety functions, safety relevant communication has to run two times. For example: for realisation *F*3 it is necessary to send information about ES3 state change to sPLC4 and then send from sPLC4 to sPLC1 and sPLC2. Communication from sPLC4 to sPLC1 and sPLC2 can be parallel, but to determine maximal response time we have to assume the worst possible case – the biggest time shift among operating cycle starts of each safety PLC. This is one of the reasons, why the real response time (tab. 1) and maximal response time (tab. 2) are so different.

One solution how to reduce maximal response time is making a new relation among sPLC. For example: in case of existing relation between sPLC3 and sPLC1 and also relation between sPLC3 and sPLC2 (fig.4), information about ES3 change state could be send directly without mediated communication via sPLC4. We also have to assume other impacts of this solution. One of the impacts is longer safety program execution (secondary impact is again prolongation of response time) and, depending on a manufacturer, it could require addition of new hardware components (which are necessary for safety relevant communication).

V. CONCLUSION

Generally, it can be said that higher complexity of SRCS raises the response time of safety functions. This time can be reduced by changing the architecture or parameters optimisation for individual sPLC. With respect to the fact, that architecture of SRCS is not only dependant on safety function realisation, but also on common control functions realised by the same PLC for better utilization of the sPLC, then parameters optimisation is the better option. This paper shows the possibility to significantly reduce response time of safety functions without SRCS architecture modification thanks to parameters optimalisation of safety PLC.

ACKNOWLEDGMENT

This paper has been supported by the Educational Grant Agency of the Slovak Republic (KEGA) Number: 034ŽU-4/2016: Implementation of modern technologies focusing on control using the safety PLC into education.

REFERENCES

[1] J. Ždánsky, K. Rástočný, J. Hrbček, “Influence of Architecture and Diagnostic to the Safety Integrity of SRECS Output Part,” 20th International Conference on Applied Electronics, AE 2015; Pilsen, Czech Republic, September 8-9, p. 297-301, ISBN 978-802610385-1.

[2] M. Rousand, “Reliability of Safety-Critical Systems, Theory and Applications,” Published by John Wiley & Sons, Hoboken, New Jersey, 2014, ISBN 978-1-118-11272-4.

[3] N. He, V.Oke, G, Allen, “Model-based Verification of PLC programs using Simulink Design,” International Conference on Electro Information Technology 2016, Univ N Dakota, Grand Forks, May 19-21, p. 211-216, ISBN 978-1-4673-9985-2.

[4] K. Rástočný, M. Franeková, P. Holečko, I. Zolotová, “Modelling of Hazards Effect on Safety Integrity of Open Transmission Systems,” Computing and Informatics, Volume 35, Issue 2, p. 470-496, 2016, ISSN 1335-9150.

[5] K. Rástočný, M. Franeková, I. Zolotová, et al. “Quantitative assessment of safety integrity level of message transmission between safety-related equipment,” Computing and Informatics, Volume 33, Issue 2, 2014, ISSN 1335-9150.

[6] M. Franeková, K. Rástočný, “Safety evaluation of fail-safe fieldbus in safety related control system,” Journal of electrical engineering, Volume 61, Issue 6, p. 350-356, 2010, ISSN 1335-3632.

[7] EN ISO 13855, “Safety of machinery.Positioning of safeguards with respect to the approach speeds of parts of the human body,“ 2010.

[8] EN 61511, “Functional safety – Safety instrumented systems for the process industry sector,” 2017

[9] J. Ždánsky, K. Rástočný, “Influence of Safety PLC Parameters to Response Time of Safety Functions,” Proceedings of International Conference Applied Electronics, AE 2013, Pilsen, Czech Republic, Sep 10-12, p. 327-330, ISBN 978-80-261-0166-6, ISSN 1803-7232.

[10] J. Hrbček, P. Božek, J. Svetlík, V. Šimák, M. Hruboš, D. Nemec, A. Janota, E. Bubeníková, “Control system for the haptic paddle used in mobile robotics,” International Journal of Advanced Robotic Systems, Sage journals, Vol. 14, No. 5, 2017, p. 1 – 11, ISSN 1729-8814

[11] Maximal response time calculator, avaible at https://support.industry.siemens.com/cs/attachments/93839056/s7safety_rttplus.xlsm, reviewerd 9.2.2018