Influence of Distributed SRCS Architectures on Dependability and Safety of Realised Safety Functions

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 – **Incessantly extending possibilities of safety PLCs allows usage not only in process level control but also in higher level of control. It means, that complex distributed control systems can be created. In case that safety functions are realised by these systems, architecture of control system can have an influence on safety and dependability parameters of functions. This paper deals with the influence of architecture and system realisation of safety functions on dependability and safety of these functions.**

Keywords-safety PLC; safety integrity level; safety function; failure probability; dangerous failure rate

I. INTRODUCTION

Control system can realise various functions. If a failure of some function could result in a significant damage to human health, the environment or major material damages, then the system is called safety related control system (SRCS) and function which can cause damage is called a safety function (SF). Most of industrial applications can be divided into common control functions and safety functions. Also control systems for industry are adapted for this fact. Mainly safety PLC (Programmable Logic Controller) which has capabilities to realise common control functions and also safety functions are used.

Safety PLC are modular control systems with many different communication interfaces and possibility of safety related communication. Relatively complex, distributed control systems can be realised thanks to wide communication possibilities. Using safety related communication, the realisation of distributed SF is also possible.

For realisation of SF (safety function) it is necessary to make safety analysis of this function for evaluation of SIL (Safety Integrity Level - Definition of SIL is described in [1]). Importance of dependability parameters evaluation is higher for more complex applications (e.g. distributed safety function). Architecture and way of realisation of distributed SRCS can have influence on safety and dependability parameters of realised SF. It is important for architecture composition to take into account the minimal required values of all defined parameters.

This paper deals with analysis of SRCS architecture and way of SRCS realisation on safety and dependability of realised SF.

II. SAFETY OF SAFETY FUNCTION

Required parameters of determined SIL must be respected during design and realization of centralised or distributed SRCS. SIL is determined on base of risk analysis. Result of risk analysis is risk identification and proposal of risk reduction measures. Measures can have technical or non-technical character (e.g. organization measure). Safety functions are technical measures for risks reduction related with controlled process. Risk reduction realised by safety function is directly proportional to SIL. If multiple safety functions are realised by the same SRCS, then SIL must be determined for each safety function.

SIL specifies the random hardware and systematic failure tolerance of safety function. Systematic safety integrity is non-quantifiable part of safety integrity and with respect to scope of this paper will not be discussed further. More detailed information about systematic safety integrity can be found in [2, 3].

Random hardware safety integrity can be quantitatively evaluated based on probability calculation. Standard [1] evaluates reached SIL according to one of two parameters. For systems with low demand mode, SIL evaluation is determined on SF average probability of dangerous failure. For systems with high demand mode SIL is determined on SF average frequency of dangerous failure.

Low demand mode is defined as safety function, which is executed only on demand and occurs less than one per year only. Most of safety functions work in high or continuous demand mode. This mode is also considered in this paper.

III. DEPENDABILITY OF SAFETY FUNCTION

Dependability is a general property of the object which ich based on ability to perform required functions in determined range of specified values and during specified time. An object can be considered a whole system or its elements. If these objects are parts of SRCS, which cooperate to realise the safety function, we can consider the dependability of safety function. Determination of this term is necessary for comparison of various SRCS architecture and their influence on relevant properties.

In the international electrotechnics dictionary [4] dependability is defined as a summary of terms used

ISBN 978-80-261-0812-2,

for description of availability and factors, which have influence on availability, maintainability and providing of maintenance.

Suitable parameters for quantitative evaluation of safety function dependability are various dependability indicators. For example: function of immediate availability, coefficient of mean availability or coefficient of asymptotic availability. Coefficient of average availability is an average value of immediate availability in a defined time range (t_1, t_2).

$$\overline{A(t_1,t_2)} = \frac{1}{t_2-t_1}.\int_{t_1}^{t_2} A(t).dt\ , \qquad (1)$$

where $A(t)$ is function of immediate availability.

In case, that some relevant conditions are met, for example, constant failure rate and restoration rate, then we can assume:

$$A = \frac{MUT}{MUT+MDT}\ , \qquad (2)$$

where *MUT* is mean up time and *MDT* is mean down time.

It is evident based on (2), that availability is dependent not only on parameters of SRCS but also on external parameters (e.g. time of unusability – dependent on recovery time, stock of replacement parts, etc.). This is the reason why quantitative parameters are more suitable (based on SRCS parameters only) for comparison of architectures. Suitable parameter for evaluation is for example probability of failure-free operation or failure probability. We can assume:

$$R(t) = 1 - F(t), \qquad (3)$$

where $R(t)$ is probability of failure-free operation and $F(t)$ is failure probability.

Supposing of exponential distribution of failure occurrence (generally accepted for electronic devices), failure probability can be described by:

$$F(t) = 1 - e^{-\lambda t}, \qquad (4)$$

where λ is failure rate of monitored object.

IV. ARCHITECTURE OF SRCS

A. Centralised architecture of SRCS

Example of centralised SRCS architecture is shown in fig. 1. More safety functions can be realised by this SRCS. When we assume, that dangerous failure of any element which cooperates on realisation of safety function will cause dangerous failure of SF (we can assume serial model of system elements), then dangerous failure rate can be express using equation:

$$\lambda_{SF}^{D} = \sum_{i=1}^{n} \lambda_i^D\ , \qquad (5)$$

where λ_i^D is dangerous failure rate of element *i* which cooperate on SF realisation and *n* is count of elements which realises SF.

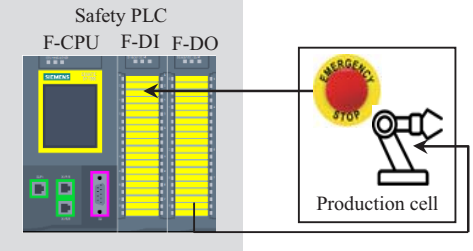

Figure 1. Example of centralised SRCS architecture

When SRCS is realising multiple SF, it is obvious that some elements (such as control logic) will be used to realize more than one SF. In this case we have to assume more pessimistic approach of evaluation, and dangerous failure rate is therefore assumed as a sum of separately determined dangerous failure rate of each realised SF. This issue is described in [5].

Equation (5) does not include some necessary components which have no influence on safety with assumption of correct application of used parts, (e.g. power supply).

Failure probability of SF which is realised by centralised architecture can be described by:

$$F_{SF}(t) = 1 - \prod_{i=1}^{n}(1 - F_i(t)), \qquad (6)$$

where $F_i(t)$ is failure probability of element *i* which cooperate on SF realisation and *n* is count of elements, which are realising SF.

Assuming that exponential distribution of failure occurrence has been used, formula (6) can be modified using formula (4):

$$F_{SF}(t) = 1 - \prod_{i=1}^{n} e^{-\lambda_i t}, \qquad (7)$$

where λ_i is failure rate of element *i* which cooperate for SF realisation. In equation (7), unlike equation (5), it is necessary to consider all elements of SRCS (such as power supply) which are necessary for SF realisation. The reason is that failure of each of these parts will cause SF failure (does not matter that some of theseare not dangerous).

$$\lambda_i = \frac{1}{MTBF_i}, \qquad (8)$$

where $MTBF_i$ is mean time between failure of used elements.

B. Distributed architecture of SRCS

In the fig. 2 we can see example of distributed SRCS architecture. Generally, this SRCS can be complex, multilevel distributed SRCS. For simplicity, in the fig. 2, only two-level architecture is shown. Input and output modules of safety PLC used in process level (sPLC1, sPLC2, ..., sPLCn) are directly cooperating with controlled technology. Safety PLC in higher control level (sPLCc) realises coordination of each task realised by PLC in lower level.

Architecture of SRCS is not dependent on realised SF only, but also on application of safety PLC for realisation of common control functions (safety non-relevant functions). Safety PLC can execute complex

control functions as is [6] (as standard PLC) and safety functions at the same time.

Because of necessity to evaluate safety and dependability parameters of SF realised by distributed SRCS, logical relation among elements used for SF realisation must be known. Logical relations can depends on specific properties given by manufacturers of safety PLC. Logical relation can depends also on used communication interface or other specific requirement of realisation (e.g. galvanic separation of communication networks). Example of logical relations among sPLC is shown in fig. 2 by arrows with dashed lines.

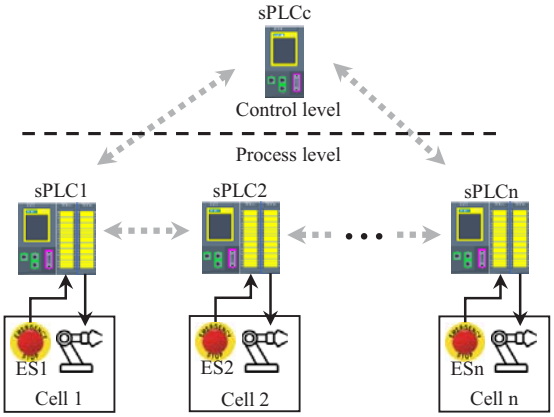

Figure 2. Two level distributed SRCS

We assume, that architecture shown in the fig. 2 realise SF. In case of execution request in a place A (e.g. pushed emergency button ES1) safety function will put a machine into safe state in a place B (e.g. disconnection a motor from power supply in cell n).

For realisation of SF mentioned above, safety related communication between sPLC1 and sPLCn is unavoidable. This communication is possible by two ways. First possible way is communication in process level realised among sPLC1 - sPLC2 - ... – sPLCn (this realisation of safety function will be labelled as SF_1). In this case the direct communication between sPLC1 and sPLCn could be the best solution. Unfortunately, this communication is impossible in practice, because of communication among other cells requires more communication elements (e.g. galvanic separation of networks). Application of additional elements, to allow communicate every cell with each other could be too expensive.

Second way of realisation is using elements in higher level of architecture. Data exchange is provided by communication realised via sPLC1 – sPLCc – sPLCn (this realisation of safety function will be labelled as SF_2).

In case that SF_1 and SF_2 are realised, dangerous failure rate can be determined by (5), what is given by serial model of used components for SF realisation. To the serial model must be included communication dangerous failure rate. Failure probability of SF can be determined by formula (6) or rather (7).

Another case of data exchange realisation is when we use communication via two parallel ways (safety function realised by this way will be labelled as SF_K). Reason why realise this solution is improving availability of SF. Advantage of this solution is that not additional hardware is required. Higher availability is reached thanks to software modification based on logical sum of received values in place B.

Failure probability of SF_K can be described by block diagram shown in fig. 3. This block diagram assume that modular system based on Simatic S7-1500 will communicate via Profinet and galvanic separation realised by PN/PN couplers has been used.

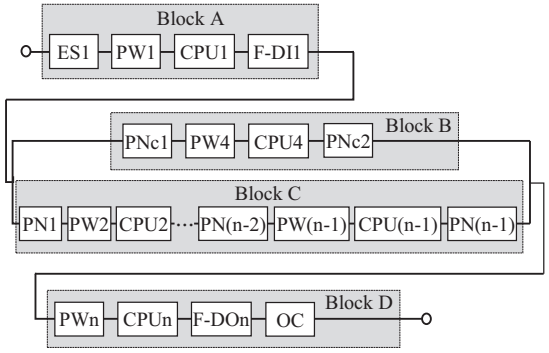

Figure 3. Failure occurence block diagram of two level distributed SRCS

Block description of blocks used in fig. 3 is in the tab. 1.

TABLE I. DESCRIPTION OF USED BLOCKS IN FIG.3

Block label without number	Block description	Failure rate symbol
ES	Emergency stop button	λ_{ES1}
PW	Power supply	λ_{PW}
CPU	Central processing unit of sPLC	λ_{CPU}
F-DI	Input module of sPLC	λ_{FDI}
PNc	PN/PN coupler which separate networks between process and control level	λ_{PN}
PN	PN/PN coupler which separate networks on the process level	λ_{PN}
F-DO	Output module of sPLC	λ_{FDO}
OC	Output circuit	λ_{OC}

It is possible to express equation for failure probability calculation of SF_K using block diagram in the fig. 3:

$$F_{SFK}(t) = 1 - \big(1 - F_A(t)\big)\big(1 - F_B(t)F_C(t)\big)\big(1 - F_D(t)\big), \quad (9)$$

where F_A, F_B, F_C and F_D is failure probability of A, B, C and D blocks.

Failure probability of A, B and D blocks can be determined by formula (6), or (7) because, each block consists of elements. Each element consists of parts which also use serial model of connection.

Supposing of identical elements used for realisation of SF_K in each cell, failure probability of block C (fig. 3) can be described by (10).

$$F_C(t) = 1 - \left(1 - F_{PN}(t)\right)^{(n-1)}\left(1 - F_{PW}(t)\right)^{(n-2)}\left(1 - F_{CPU}(t)\right)^{(n-1)}, \quad (10)$$

where F_{PN}, F_{PW} a F_{CPU} are failure probabilities of PN, PW and CPU blocks.

When we assume identical elements for each cell and also exponential distribution of failure occurrence. Using formula (7), (9) and (10) formula for calculation of SF_K failure probability can be derived (explanation of symbols used in (11) is shown in tab.1.):

$$F_{SFK}(t) = 1 - e^{-(\lambda_{ES1}+\lambda_{FDI}+\lambda_{FDO}+\lambda_{OC}+3(\lambda_{PW}+\lambda_{CPU})+2\lambda_{PN})t} - e^{-(\lambda_{ES1}+\lambda_{FDI}+\lambda_{FDO}+\lambda_{OC}+(n-1)\lambda_{PN}+n(\lambda_{PW}+\lambda_{CPU}))t} + e^{-(\lambda_{ES1}+\lambda_{FDI}+\lambda_{FDO}+\lambda_{OC}+(n+1)(\lambda_{PN}+\lambda_{PW}+\lambda_{CPU}))t}. \quad (11)$$

Danger failure rate of SF_K can be determined also by (5). It is important to assume all used elements in each way of communication because of fact, that each element providing information transfer (in first and also second way) can cause danger state.

V. EXPERIMENTAL RESULTS

In the fig. 4 waveforms of SF_1 failure probability (curve 4) and SF_2 for n=4, n=5 a n=7 (curves 3, 2 a 1) are shown.

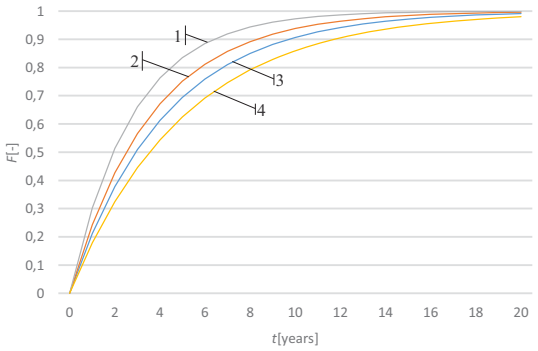

Figure 4. Failure probability of SF_1 and SF_2

In the fig. 5 waveform of SF_2 failure probability is shown. In the graph, 6 curves shows failure probability for n=4, n=5 and n=7 (curves 3, 2, 1) and SF_K, for n=4, n=5 a n=7 (curves 6, 5, 4).

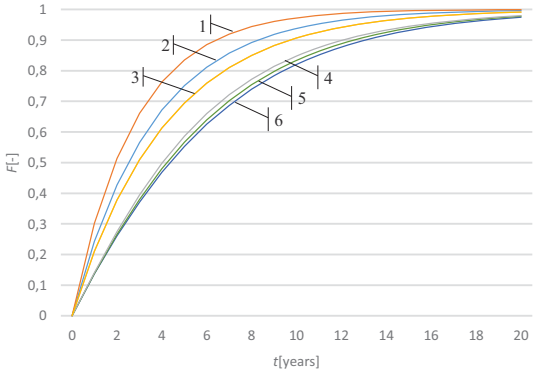

Figure 5. Failure probability of SF_2 and SF_K

In the tab. 2, we can see danger failure rate of SF_1, SF_2 and SF_K (it is average rate of dangerous SF failure for 20 years - it means, during lifetime of SRCS).

TABLE II. AVERAGE DANGER FAILURE RATE OF SF DURING LIFETIME OF SRCS

Safety function	n	λ_{SF}^{D}
SF_1	-	$1{,}29.10^{-8}h^{-1}$
SF_2	4	$1{,}49.10^{-8}h^{-1}$
SF_2	5	$1{,}69.10^{-8}h^{-1}$
SF_2	7	$2{,}09.10^{-8}h^{-1}$
SF_K	4	$1{,}69.10^{-8}h^{-1}$
SF_K	5	$1{,}89.10^{-8}h^{-1}$
SF_K	7	$2{,}29.10^{-8}h^{-1}$

Parameters used for calculation: availability factors according to [7], output circuit with two contactors without feedback according to [8] and safety factors include dangerous failure rate of communication according to [9]. With safety related communications deals detailed [10, 11].

VI. EVALUATION OF EXPERIMENTAL RESULTS

Waveforms shown in fig. 4 and fig. 5 compares dependability parameters of SF which are realised by different ways and by distributed SRCS with various complexity.

In the graph shown in fig. 4 it is evident that higher count of used cells in process level (fig. 2) will raise failure probability of SF_2. Reason of this occurrence is higher count of elements which can occurs failure of SF_2.

In the fig. 5 we can see redundancy influence on failure probability of SF_K. This influence is compared with equally complex distributed SRCS as used for realisation of SF_2. We must remember that it is realisation of the same SF by different ways. It is not primary target to create redundancy but only better use of exists hardware and software resources of distributed SRCS. In this example, redundancy is partial only (not all components of SRCS are redundant). It means that by suitable using of hardware and software resources only we can improve dependability of distributed SRCS.

It is necessary to keep on mind, that we realise SF and primary required aspect is safety. In the tab. 2 influence of each SF solutions on dangerous failure rate is shown. Because of facts mentioned above, safety parameters are worsening with higher count of elements which realises SF. It means, that for improving of dependability parameters we can worsen safety parameters. In any case, all required parameters must reach minimal required value.

VII. CONCLUSION

Realisation of SF by distributed SRCS has specific properties which must be taken into account during the selection of suitable architecture and way of SF realisation. In general, when the distributed SRCS is more complex, more ways of SF realisation exist. All required parameters must meet the minimum specified level for the considered architecture and solution choice. This paper deals with evaluation of safety and dependability parameters for safety functions only. Another important parameter, which has an influence on safety of SF is response time. The approach to realize a SF by a distributed SRCS with respect of response time is shown in [12].

ACKNOWLEDGMENT

This work has been supported by the Educational Grant Agency of the Slovak Republic (KEGA) Number 008ŽU-4/2019: Modernization and expansion of educational possibilities in the field of safe controlling of industrial processes using the safety PLC.

REFERENCES

[1] EN IEC 61508, "Functional safety of electrical/ electronic/programmable electronic safety-related systems," 2010.

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

[3] K. Rástočný, A. Janota, J. Zahradník, The use of UML for development of a railway interlocking system, Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics) Springer, Volume 3147, Pages 174-198. ISSN: 0302-9743, 2004.

[4] IEC 60050-191, "International Electrotechnical Vocabulary," Chapter 191: Dependability and quality of service, 2002.

[5] K. Rástočný, J. Ždánsky, P. Nagy, "Some specific activities at the railway signalling system development," Proceedings of the 12th International Conference Transport Systems Telematics 2012, Katowice, Ustroń, Poland, Volume 329, Telematics in the Transport Environment, Springer-Verlag, Berlin, pp. 372-381, ISSN 1865-0929, ISBN 978-3-642-34049-9, 2012.

[6] 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, p. 1 – 11, ISSN 1729-8814, 2017.

[7] Mean Time Between Failures (MTBF) - list for SIMATIC products, avaible at https://support.industry.siemens.com/cs/document/16818490/mean-time-between-failures-(mtbf)-list-for-simatic-products?dti=0&lc=en-WW, reviewerd 25.3.2019.

[8] J. Ždánsky, K. Rástočný, J. Hrbček, "Influence of architecture and diagnostic to the safety integrity of SRECS output part," Proceedings of international conference Applied Electronics, Pilsen, Czech Republic, 8 - 9 September 2015, pp. 297-301, ISBN 978-80-261-0385-1, ISSN 1803-7232, 2015.

[9] Safety Integrated – Overview of Safety-Related Parameters for Siemens Components in Accordance with ISO 13849-1 and IEC 62061, avaible at https://www.industry.siemens.nl/topics/nl/nl/safety-integrated/machineveiligheid/Documents/SIEMENS-producten_PFHd_SIL_PL_B10-waarden%20(EN).pdf , reviewerd 25.3.2019.

[10] K. Rastocny, M. Franekova, P. Holecko, et al., "Modelling of Hazards Effect on Safety Integrity of Open Transmission Systems," Computing and Informatics, Volume 35, Issue 2, Pages 470-496, ISSN 1335-9150, 2016.

[11] K. Rastocny, M. Franekova, I. Zolotová, et al., "Quantitative Assessment of Safety Integrity Level of Message Transmission between Safety-related Equipment," Computing and Informatics, Volume 33, Issue 2, Pages 343-368, ISSN 1335-9150, 2014.

[12] J. Ždánsky, J. Valigurský, "Time response of safety function realised by decentralised SRCS with safety PLC," Proceedings of the 23rd International Conference on Applied Electronics, Pilsen, Czech Republic, September 11-12 , pp. 179-182, ISSN 1803-7232, ISBN 978-80-261-0721-7, 2018.