Influence of Architecture and Diagnostic to the Safety Integrity of SRECS Output Part

Juraj Ždánsky, Karol Rástočný, Jozef Hrbček
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, karol.rastocny@fel.uniza.sk, jozef.hrbcek@fel.uniza.sk

Abstract – **This article deals with the achievement of safety properties of the output part of the safety-related electronic control system (SRECS) and refers to the impact of architecture and diagnostic of the SRECS output part to the required safety integrity level (SIL) SRECS.**

Keywords- SRESC, intensity of dangerous failures, SIL, diagnosis

I. INTRODUCTION

Control of so-called safety-critical processes requires a particular way in the design of the entire control system including sensors, actuators, mutual communication between individual parts of the control system and HMI (human machine interface). Designing of SRESC based on safety PLC is devoted e.g. in [1]. It is required to use the components and their interconnection to the control system that after a failure get into the pre-defined safe state. The safe state must be determined on the basis of risk analysis for each safety function [2], [3].

The result of risk analysis is not only the potential risks arising from the controlled process, but also the degree of effectiveness with which these risks should be eliminated. To express the effectiveness of measures against random failures of hardware it is used probabilistic approach. In this context, we are talking about the integrity of safety against random hardware failures and it is expressed by the dangerous failure rate [4].

View of the fact that the control system can perform more safety functions and also with them the conventional control functions, so that the dangerous failure rate cannot be related to the whole system, but must be always related to the particular safety function.

Therefore, the efforts of manufacturers of the control systems for implementation of the safety functions are creating (and subsequently offering to customers) as much as possible standardized solutions for the same type safety functions (some standardized solutions are given in [5]). Ensuring the required safety integrity of the safety function (or functions) also entails certain economic claims, which do not provide users direct economic return (giving him a sense of safety, which can be very difficult financial rate). Such solutions are profitable in many cases because it saves money spent on the design, implementation and safety analysis of implemented safety function. However, this is not valid always.

This article points out that the design for customized solutions is more preferably for particular application in some cases. This solution may take into consideration the specifics of given application and finally may lead to a simpler and economically more preferred to obtain the required safety integrity level. Among the specifics standardized solutions that aren't often taken under consideration include for example: required SIL, the required response time of the safety function, maximum intervals of changes the state of the output circuits etc.

II. SAFETY ASSESSMENT OF A SAFETY FUNCTIONS

Suppose the safety function which is realized by *n* components (e.g. sensors, control logic, actuators, etc.). If these parts are connected such that their impact on the dangerous failure of the safety function can be described by serial model, then dangerous failure rate of the safety function can be expressed by the formula:

$$\lambda_F^D(t) = \sum_{i=1}^{n} \lambda_i^D(t), \qquad (1)$$

where λ_i^D is the dangerous failure rate of the *i*-th part participating at the performance of the safety function.

Equation (1) is valid provided that the dangerous failure of any part may cause a dangerous failure of realized safety functions. The control system can also perform more safety functions where one part may also participate in the performance of several safety functions. The issue of the relationship between the dangerous failure rate of safety functions and dangerous failures rate of individual parts is devoted [6].

From equation (1) follows directly that the resulting dangerous failure rate of the safety function is determined by the dangerous failures rate of the individual parts realized the safety function. Assume that the safety function is realized by the parts of the SRECS according to Fig.1. Each part can consist of one or several components (e.g. in fig. 1, the input section consists of sensors (S) and the input interface (II), output section consists of output interface (OI) and actuators (A)). Then the dangerous failure rate of the safety function can be affected especially at the input and output of the SRECS, because the other components are typically pre-prepared and typically certified by the manufacturer for SIL 3 according to [4] (e.g. the control logic; SIL3 represents in common industrial applications the highest required SIL).

ISBN 978-80-261-0386-8,

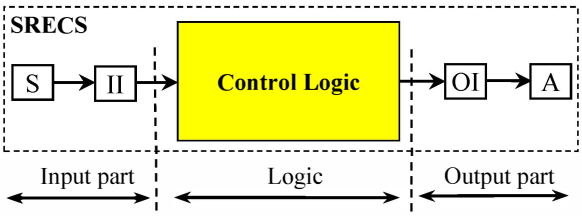

Figure 1. Basic SRECS components

A part of the SRECS components manufacturer's information is the dangerous failure rate of such a components and conditions of usage of component. Parameter setting extends the possibilities of component usage and must take into account the characteristics of the other parts of the SRECS if this component is configurable. Components of a modular safety PLC can be as examples of components suitable for the implementation to SRECS especially for industrial applications. The impact of parameters of safety PLC to the safety integrity of the safety function is discussed in detail in [7].

III. INPUT-OUTPUT INTERFACE OF SRECS

In the terms of achievement of the required SIL we need to pay attention to safety function especially to input and output of the SRECS as already follows from the foregoing. The next part of this paper will be focused only on the safety properties of different architectures of SRECS output interface, because it directly affects the safety properties of output part of SRECS.

A. Commonly used wiring of SRECS output interface

Fig. 2 shows a commonly used output interface wiring of SRECS. This is a two-channel connection of power components (in this case contactors) controlling the actuator. This wiring is appropriate, on the assumption that:

- safe state of controlled process can be achieved by disconnecting the actuator (A) from the power source;
- SRECS outputs, controlling the C1 and C2 are mutually independent (from the perspective of common causing failures);
- SRECS includes the application logic and controlling an output O1 and O2 at the same time, or also diagnostic applications for the evaluation of feedback signals.

The dangerous failures rate of the SRECS output interface can be calculated from the equation:

$$\lambda_O^D(t) = \frac{\frac{P_O^D(t)}{dt}}{1-P_O^D(t)}, \qquad (2)$$

where $P_O^D(t)$ is the probability of dangerous failure of output interface. Relation (2) is valid on the assumption that $P_O^D(t)$ has the characteristics of the distribution function, which is fulfilled in this case.

Probability of dangerous failure of the SRECS output interface according to fig. 2 can be expressed by the following formula:

$$P_O^D(t) \le P_{C1}(t).P_{C2}(t), \qquad (3)$$

where $P_{C1}(t)$ and $P_{C2}(t)$ are failure probability of contactors C1 and C2.

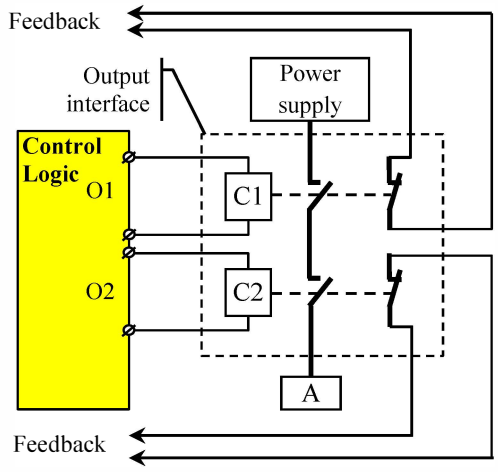

Figure 2. Commonly used output interface wiring of SRECS

Realistically can be assuming that the failure of connecting wires and connectors between logic and contactors C1, C2 have no impact on the probability of failure of SRECS output interface.

Based on formulas (2) and (3) and assuming the exponential distribution of failures, an equation can be derive for dangerous failures rate of the SRECS output interface with two contactors:

$$\lambda_{O1}^D(t) \le \frac{\lambda_{C1}e^{-\lambda_{C1}t}+\lambda_{C2}e^{-\lambda_{C2}t}-(\lambda_{C1}+\lambda_{C2})e^{-(\lambda_{C1}+\lambda_{C2})t}}{e^{-\lambda_{C1}t}+e^{-\lambda_{C2}t}-e^{-(\lambda_{C1}+\lambda_{C2})t}}, \qquad (4)$$

where, λ_{C1} is the failures rate of contactor C1 and λ_{C2} is the failures rate of contactor C2.

The dangerous failures rate of the SRECS output interface is time dependent. Provided that there is no diagnosis of sensors, it must be considered to determine the value of rate with time of the proof test and at the extreme case it must be considered with the time of the system working life. A significant reduction of the dangerous failures rate of SRECS output interface may be achieved by implementing the diagnostics. If the output interface is made by contactors, the diagnosis can be realized by scanning the state of the contactor via the auxiliary switch (this feedback is shown in fig. 2). The auxiliary contacts must be “so called” mirror contacts (the properties of such contacts are defined by the standard [8]). We may expect 100% diagnostic coverage provided the correct connection of auxiliary contacts on the SRECS input interface. In this case, in equation (4), we can presume a time of failure detection and negation (disconnect actuator from the power source). In general, the auxiliary contacts may be connected in series and connected to one input or can be connected to independent inputs alone. Connection type of auxiliary contacts depends on the requirements of diagnostic. More detailed information about diagnostics can be found in [9].

Fault detection of the contactors can be realized by functional diagnosis or test diagnosis. In the case of

realization the functional diagnostics for the fault detection time can be considered the maximum time between operating commands to change the status of contactors. For the fault detection time can be considered the maximum time between the implementation of testing procedures in the case of realization the test diagnostics.

Within a realization of the functional diagnosis is necessary to consider that the operating commands for changing the state of contactors are sporadic in generally (safety function solves critical situations which we are trying to avoid).

Among a general prerequisite for realization of application test diagnostic belongs:

- possibility to create the user application program triggered at a regular intervals (these intervals must be guaranteed in order to exclude potential threat of interval extension);
- realization of the test procedure must not affect so the actuator to cause an adverse reaction in a controlled process.

If the functional diagnostic or diagnostic test execution of SRECS output interface is impossible and the reduction of the dangerous failures is necessary, you can use one of the following options (or its combinations):

- use the better quality contactors (with lower failure rate);
- ensure the testing by organizational measures (e.g. the periodic exchange of contactors and diagnostics out of operation);
- use a more complex structure of the SRECS output interface.

B. The SRECS output interface wiring with three contactors

Fig. 3. shown a SRECS output interface with three contactor. This wiring is appropriate under the same assumptions as the wiring in Fig. 2, except that three mutually independent outputs for the contactor controls are necessary (from the perspective of the common causing failures).

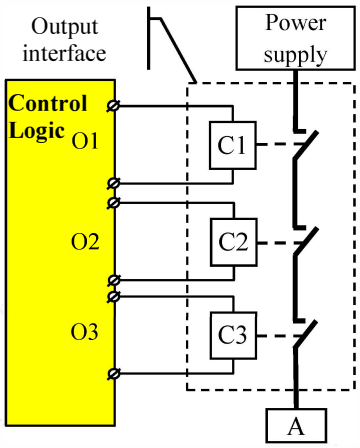

Figure 3. The wiring of the SRECS output interface with three contactors

Fig. 3 shows the wiring without the feedback. If a feedback is necessary it can be realized using auxiliary contactors contacts.

Probability of dangerous failure of a SRECS output interface with three contactors (Fig. 3) can be expressed by the formula

$$P_O^D(t) \leq P_{C1}(t).P_{C2}(t).P_{C3}(t). \quad (5)$$

The dangerous failures rate of the SRECS output interface with three contactors, assuming an exponential distribution of failures occurrence, will be:

$$\lambda_{O2}^D(t) \leq \frac{3\lambda_C e^{-\lambda_C t} - 6\lambda_C e^{-2\lambda_C t} + 3\lambda_C e^{-3\lambda_C t}}{3e^{-\lambda_C t} - 3e^{-2\lambda_C t} + e^{-3\lambda_C t}}, \quad (6)$$

where $\lambda_C$is the contactor failures rate. To simplify the formula (6) we assume that $\lambda_C = \lambda_{C1} = \lambda_{C2} = \lambda_{C3}$.

C. The SRECS output interface connections with four contactors

Fig. 4 shows a wiring of a SRECS output interface with four contactors. To contactors control required four mutually independent outputs in this case (from the perspective of the common causing failures).

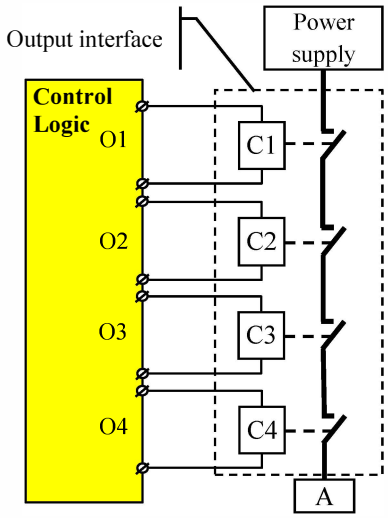

Figure 4. The wiring of the SRECS output interface with three contactors

Probability of dangerous failure of a SRECS output interface with four contactors (Fig. 4) can be expressed by the formula:

$$P_O^D(t) \leq P_{C1}(t).P_{C2}(t).P_{C3}(t).P_{C4}(t). \quad (7)$$

The dangerous failures rate of the SRECS output interface with four contactors, assuming an exponential distribution of failures occurrence, will be:

$$\lambda_{O3}^D(t) \leq \frac{4\lambda_C e^{-\lambda_C t} - 12\lambda_C e^{-2\lambda_C t} + 12\lambda_C e^{-3\lambda_C t} - 4\lambda_C e^{-4\lambda_C t}}{4e^{-\lambda_C t} - 6e^{-2\lambda_C t} + 4e^{-3\lambda_C t} - e^{-4\lambda_C t}}, \quad (8)$$

it is valid that $\lambda_C = \lambda_{C1} = \lambda_{C2} = \lambda_{C3} = \lambda_{C4}$.

IV. THE COMPARISON OF INTRODUCED WIRING OF THE OUTPUT SRECS INTERFACE

The Fig. 5 shows the time behaviors of dangerous failures intensity of the SRECS output interface according to Fig. 2 (curve 1), according to Fig. 3 (curve 2) and according to Fig. 4 (the curve 3). These

curves are built assuming that $\lambda_C = \lambda_{C1} = \lambda_{C2} = \lambda_{C3} = \lambda_{C4} = 1.10^{-5}$.

From Fig. 5 we can see that in the case of connection with three contactors (curve 2) or four contactors (curve 3), the failure detection and negation time to achieve the same SIL than in connection with a two contactors (curve 1) is significantly extended. For example, to achieve SIL 3 with connection of two contactors is needed to consider for failure detection and negation time up to 500 hours (about 21 days), but in connection with four contactors this time is up to 15,400 hours (about 1.75 years).

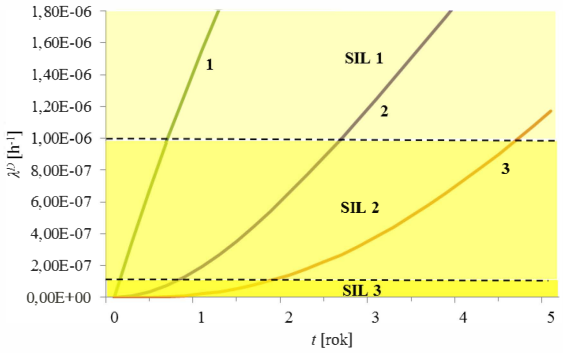

Figure 5. The dangerous failure rate of a SRECS output interfaces (1 - according to Fig. 2, 2 - according to Fig. 3, 3 - according to Fig. 4)

Necessary prerequisites for the realization of the application diagnostic of the output SRECS interfaces are as follows:

- use contactors with so-called mirror contacts (standard [8]);
- enough of SRECS outputs for connecting the contactors and enough SRECS inputs for sensing contactors state;
- SRECS allowing running the application program of test procedure in the required interval (in the case of diagnostic test realization);
- operational changes of contactors state shorter than the maximum interval for failure detecting and negation established with respect to the required SIL (for the implementation of functional diagnostics).

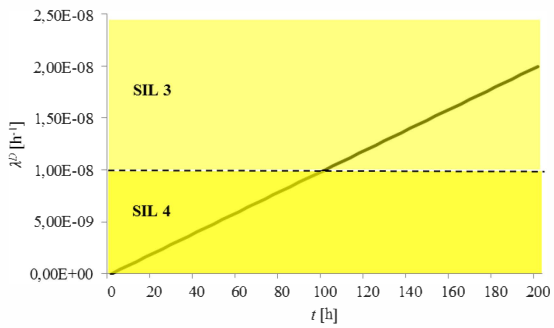

Figure 6. The dangerous failures rate of SRECS output interface according to Fig. 2

The relatively low dangerous failures rate of SRECS output interface can be also achieved with two contactors wiring by realization of functional or application diagnostic test, if these conditions are fulfilled. In Fig. 6 there is shown the curve of the dangerous failures rate of SRECS output interface connected according to Fig. 2, depending on the time of failure detection and negation. Curve is made provided that $\lambda_C = \lambda_{C1} = \lambda_{C2} = 1.10^{-5}$. Fig. 6 shows the range of dangerous failure rate defined for each SIL levels according to [4].

If the previously mentioned criteria for realization of the application diagnostic is problematic, then the output interface with three contactors may be used (Fig. 3), possibly with four contactors (Fig. 4). As we can see from the Fig. 5, in this case a maximum interval of failure detection and negation is substantially extended, which will allow us perform the diagnostics of contactors e.g. by the periodic maintenance of the system (e.g. once a year). In some cases (depending on of used contactors and the required SIL) the time of failure detection and negation can be identify with the planned working life of the system. In this case the contactors not need to have a mirrored contacts fulfilling the conditions of the standard [8] and we do not need more consider with the inputs for sensing the state of the contactors. On the other side, we need more independent outputs (from the perspective to common causing failures).

V. CONCLUSION

The SRECS consists of several parts as was noted in the introduction. Achieving the desired level of dangerous failures for the SRECS output interface is a prerequisite to achieve the required SIL of entire SRECS. However, we must also deal with the dangerous failures rate of other parts. The considerations set out in this article can be applied to achieving the desired safety properties of the sensors.

It would be appropriate to deal with the reliabilities characteristics of SRECS for the purpose of a comprehensive view to the system, but it has already beyond the scope of this paper. A comparison of reliability and safety features of some SRECS architecture with safety PLC can be found in [10].

ACKNOWLEDGMENT

This work has been supported by the Educational Grant Agency of the Slovak Republic (KEGA) Number: 010ŽU-4/2013: Modernization of didactic equipment and teaching methods with a focus on the area of robotics.

REFERENCES

[1] Hiroo Kanamaru, Tsuyoshi Mogi, Naoki Aoyama: Functional Safety Application Using Safety PLC. In: Proceedings of SICE Annual Conference 2007, p. 2489-2492, ISBN 978-4-907764-27-2 , September 17 – 20, Takamatsu, Japan, 2007

[2] Jianfeng Huang, Guohua Chen, Duomin Li: The SIS Improvement in Hydrogen Furnace Based on SIL. In: The Proceedings of 2012 International Conference on Quality, Reliability, Risk, Maintenance, and Safety Engineering, June 15-18, 2012, p.:1443 – 1447, IEEE Catalog Number: CFP1274P-ART, ISBN: 978-1-4673-0788-8, Chengdu, China, 2012.

[3] J. J. Sammarco, “Programmable electronic and hardwired emergency shutdown systems: a quantified safety analysis”, *Industry Applications, IEEE Transactions*, Volume: 43 , Issue: 4, DOI: 10.1109/TIA.2007.900477, Page(s): 1061 – 1068, 2007

[4] EN IEC 61508. Functional safety of electrical/electronic/programmable electronic safety-related systems. (2010).

[5] Ernesto Soressi: Introduction in Safety Rules EN954-1, EN13849 and EN62061. In: Proceedings of the 5th IET International System Safety Conference 2010, October 18-20, 2010.

[6] Rástočný, K., Ždánsky, J.: Specificities of safety PLC based implementation of the safety functions. In: Proceedings of International Conference Applied Electronics 2012. IEEE Cat.nr. CFP1269A-PRT, Pilsen 2012, pp. 229-232, ISBN 978-80-261-0038-6, ISSN 1803-7232, Czech Republic, 2012.

[7] Ždánsky, J., Rástočný, K.: Influence of safety PLC parameters to response time of safety functions. In: Proceedings of International Conference Applied Electronics 2013. IEEE Cat.nr. CFP1369A-PRT, Pilsen 2013, pp. 327-330, ISBN 978-80-261-0166-6, ISSN 1803-7232, Czech Republic, 2013.

[8] EN 60947-4-1. Low-voltage switchgear and controlgear.Part 4-1: Contactors and motor-starters.Electromechanical contactors and starters. (2013).

[9] Rounsand, Marvin: Reliability of Safety-Critical Systems, Theory and Applications. Published by John Wiley&Sons, New Jersey, ISBN 978-1-118-11272-4, 2014

[10] Ždánsky, J., Nagy, P.: Influence of the control system structure with safety PLC on its reliability and safety. In: Proceedings of the 9th international conference ELEKTRO 2012, IEEE Catalog Number: CFP1248S-ART, pp. TA4_25, ISBN 978-1-4673-1178-6, Rajecké Teplice, 2012.