Operator's Influence on the Safety of the Controlled Process

Peter NAGY, Karol RASTOCNY

Department of Control and Information Systems, Faculty of Electrical Engineering,
University of Zilina, Univerzitna 8215/1, 010 26 Zilina, Slovak Republic

peter.nagy@fel.uniza.sk, karol.rastocny@fel.uniza.sk

DOI: 10.15598/aeee.v13i3.1248

Abstract. *An analysis of risks related to controlled process and related hazards identification is an important activity during the development of the safety related control system (SRCS). The mistake of the operational staff during the execution of the safety relevant operations related to controlled process can be the cause of hazard. Influence of the operator on controlled process safety depends on operation mode of the SRCS and on technical safety of the SRCS. This contribution deals with the issue of the safety assessment of the operator effect on the safety of the controlled process.*

Keywords

Human error, safety, safety assessment, safety function, safety related control system, SRCS.

1. Introduction

The SRCS is a technological device for controlling of safety-critical process and its role is to replace or supervise a human (operator) in applying the safety-critical operations related to control of the considered process. The aim of such replacement or supervising is contribute to safety of controlled process so that SRCS eliminates human (operator) errors. So that SRCS is a coupling device between the operator and controlled process.

Functions of the SRCS can be divided into Fig. 1:

- control functions without influence on the safety; it means functions the failure of which may cause operational problems, but cannot endanger safety of the controlled process,
- control functions with influence on the safety; it means functions the failure of which may cause not only operational problems, but can also endanger the safety of the controlled process,
- protective functions; it means functions, which do not participate on the process controlling, but their role is to supervise the state of elements that reduce the risk of damage to protected assets (people, environment, property, ...) located in the scope of controlled process.

Protective and controlled functions with influence on the safety are referred as safety functions (SF). SRCS can contain more safety functions; each safety function can be defined with different safety integrity level (SIL) [6].

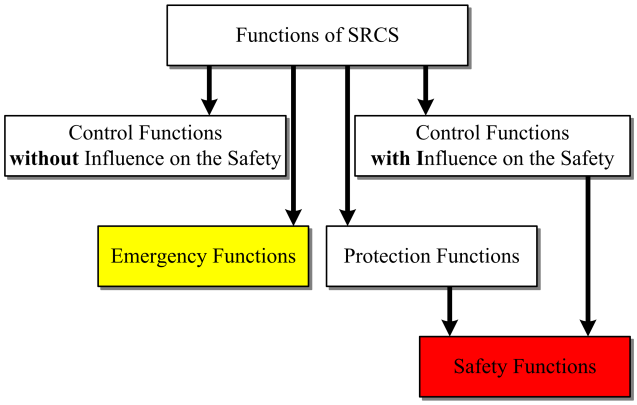

Fig. 1: Functions of the SRCS.

A specific position between SRCS functions have so-called emergency functions (EF), which do not participate on control of the process, but their role is to minimize thread of the controlled process safety due to operator error or failure of interface between the operator and SRCS (so-called Human-machine interface – HMI) during emergency operation (the operation when required safety function is not available). Due to the failure of the HMI can occur to falsification (modifi-

cation) of the operator's command. That means the failure of the HMI has the same impact on the safety of controlled process as the operator's error.

2. Error Rate of the Operator

It is very difficult task to evaluate reliability properties of the operator, because the operator does not behave always equally in the same situation. Moreover, the same traffic situation can be successfully resolved in many cases by the different ways. Human reliability can be described by the analogous parameters such as reliability of technical systems – human error probability (HEP), respectively probability of successful execution of the operation (human success probability - HSP).

There are used different methods in the world to estimate the human error probability. The following methods belong to the most frequently used methods of probabilistic estimation of human reliability [8]:

- THERP (Technique for Human Error Rate Prediction),
- SLIM (Success Likelihood Index Method),
- HRC (Human Cognitive Reliability),
- SHARP (Systematic Human Action Reliability Procedure).

Human error probability depends on the operator‘s behavior mode. Generally we can consider following behavior modes of the operator [9], [10]:

- skill-based behavior mode,
- rule-based behavior mode,
- knowledge-based behavior mode.

There is no clear boundary between these behavior modes and the operator usually combines individual behavior modes.

To minimalize operator error probability means to know causes of the errors occurring. The most frequent causes of the operator's error are:

- inattention,
- lack of the operator's specialized skills,
- work overload or time pressure,
- bad management of the operator.

3. Modelling of the Operator Effect on the Controlled Process Safety

Operator influences controlled process through the SRCS. Therefore influence of the operator on the safety of the controlled process can be evaluated only providing knowledge of functional and technical properties of the SRCS and knowledge of the operator's role in the controlled process. The operator role in the controlled process we can describe using different models. It is desirable to create each model so that describes specific monitored property and there should be respected mutual relations between individual models.

3.1. Object Model

The object model (Fig. 2) illustrates static relations between operator, SRCS and controlled process. The observed property is influence of the operator to the safety of the controlled process. For this reason there is not presented object realised functions without safety influence in the figure.

Ideally all commands to the controlled process state change are generated by the logic of the SRCS base on the state information on controlled process (information from sensors) and base on operator's commands. SRCS accepts command from the operator only if cannot the thread of controlled process safety occur and the hazard can arise only due to failure of the safety function (safety functions) of the SRCS. Tolerable intensity of safety function malfunction can be determined based on risk analysis.

In the case of continuous operation control, there is a need to ensure control the process by the operator in the case of partial or total failure of the SRCS too. The operator must supply safety functions which are not available (non-functional functions) and therefore must assume the responsibility for process control in this case. Operator issues safety critical commands based on state information of the controlled process, commands control the actuators. The operator can obtain state information of the process using HMI or by direct process observation. The operator can control actuators either directly or indirectly using emergency function (EF) depending on technical solution of the SRCS and depending on its failure range.

SRCS with safety functions with lover SIL (usually SIL 1) enables to operator during the fault-free operation and during the emergency operation interfere with process control without the check of his commands by the SRCS logic (Fig. 3). In this case, the operator is responsible for the safety of the controlled process in entirety.

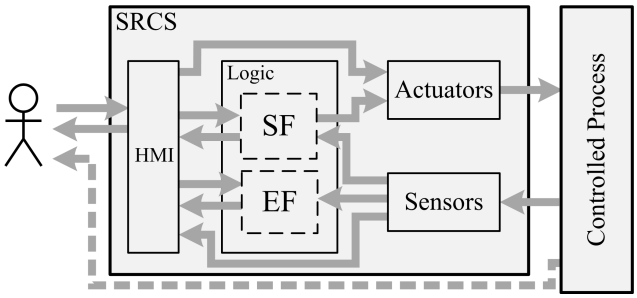

Fig. 2: Control of the process by the operator – SRCS with safety functions with higher SIL.

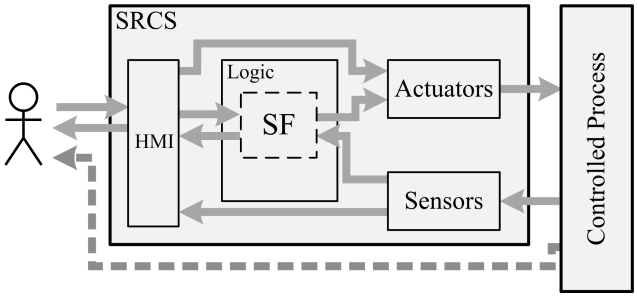

Fig. 3: Control of the process by the operator – SRCS with safety functions with lower SIL.

3.2. Sequence – Event Model (Sequence Diagram)

A sequence diagram describes interactions between the operator, SRCS and the controlled process.

In case of failure less operation of the SRCS (Fig. 4) a command entered by the operator (*Commd*) via HMI is transferred to object realising required safety function. If it is impossible to threat the safety of the controlled process, logic of the SRCS issues the command (*S_Commd*) for the actuator (actuators). This form of control is marked as o one-stage control.

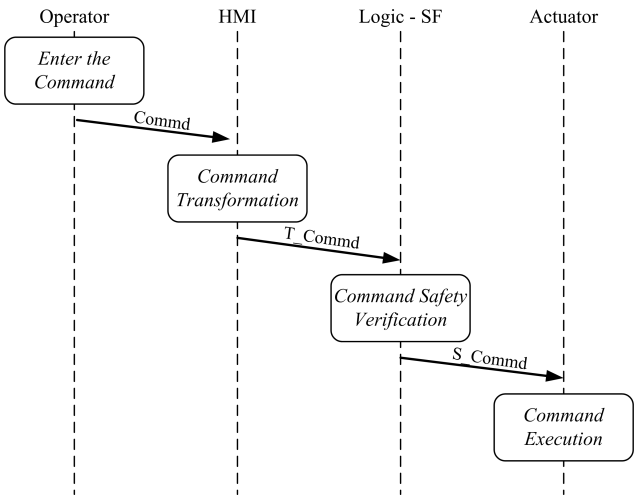

Fig. 4: Sequence diagram – failure less operation of the SRCS, one-stage control.

In case of emergency operation using one-stage control (Fig. 5), the command of the operator does not checked by the logic of the SRCS. The command is from HMI transferred directly to the actuator (actuators).

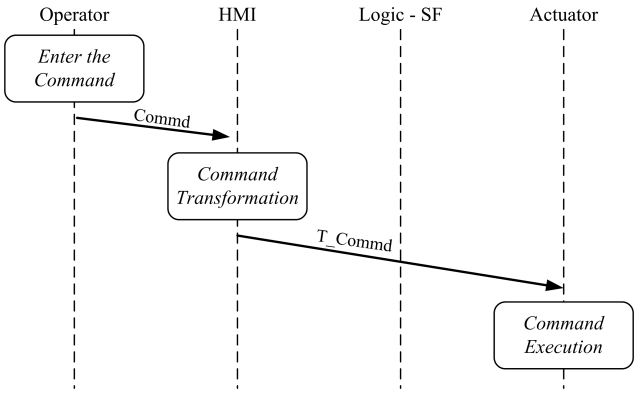

Fig. 5: Sequence diagram – emergency operation, one-stage control.

In case of multi-stage control (usually double-stage control), the operator must perform more actions in exactly defined sequence to command from the operator be accepted by the logic of the SRCS and then logic issues the order to change the state of the controlled process (through actuators control). Block EF checks correctness of the operator action in issuing the safety relevant command. Sequence diagram shown in Fig. 6 represents double-stage control principle. The SRCS logic (the block realized EF) after receiving command from the operator (*T_Commd*) backward informs the operator about required activity and asks the operator to confirm the command (message *Req_Ack*). The EF object subsequently after receiving confirmation sequence will check its accuracy (comparison of logical content of the *T_Commd* and *Ack* messages) and issues a command to the actuator (respectively commands to the actuators) [12].

3.3. State-Space Model

Different operational situations of the SRCS and the controlled process can be represented by the state-space model (Fig. 7). State space of the controlled process is generally formed by a set of safe states and a set of dangerous states (DSP). Safe states are considered states, in which there is no threat of assets related to control process (people, property, etc.). Dangerous states are considered states, in which occurs a treat to these assets. Similarly the state space of the SRCS is formed by set of:

- dangerous states (DSS),
- safety states which can be divided concerning of functionality of the SRCS to:

– states in which the SRCS is fully functional (FSS) – the SRCS has no failure,
– states in which the SRCS is partial functional (P-FSS) – SRCS has failed, thus there are not available all safety functions; the process is partially controlled by the operator using emergency services,
– state in which is the SRCS non-functional (N-FSS) – the process is fully controlled by the operator using emergency services.

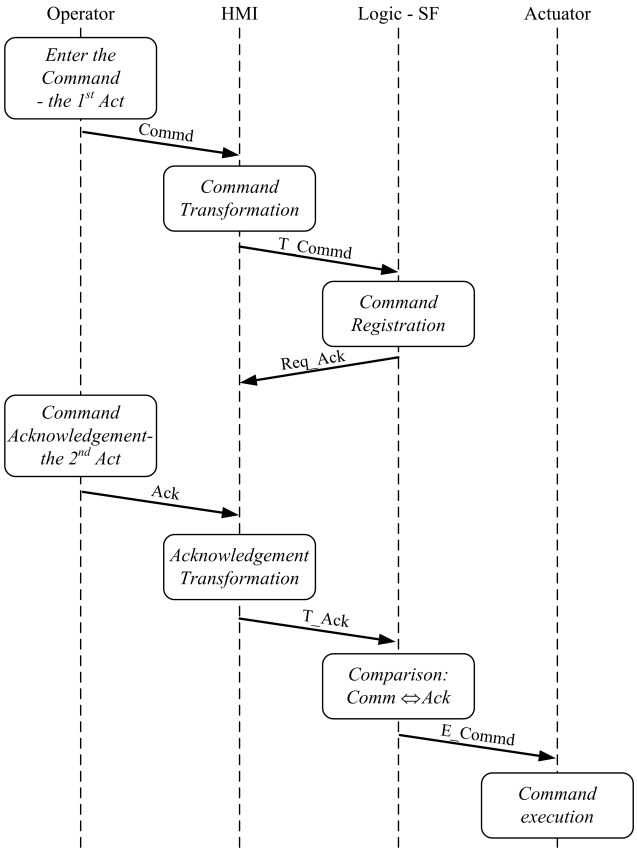

Fig. 6: Sequence diagram – emergency operation, double-stage control.

There are exist transitions between these states. Type of transitions and the intensity of these transitions depend on the specific design of the SRCS and on the actual controlled process. Transitions between SRCS state are represented by the dashed line in Fig. 7. Calculation of the probability (respectively intensity) of occurrence of the dangerous state of the controlled process due to SF malfunction is not the main subject of this paper. For this goal we can use information specified e.g. in [2], [3], [4], [5].

The most used method which allows analyzing the influence of multiple factors on the safety of the SRCS is actually Markov analysis. There can be properly used combination of Markov's chains with continuous time (CTMC) for description of stochastic processes

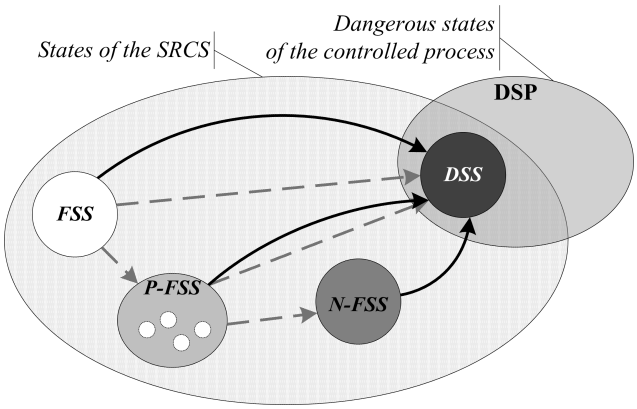

Fig. 7: State-space model of the SRCS and the controlled process.

and Markov's chains with discrete time (DTMC) for description of deterministic events, as well as for approximation of non-homogenous Markov process to homogenous Markov process [13].

To analyze of the influence of the operator's error on the safety of the controlled process we can accept following assumption: if the SRCS is in dangerous state, then the controlled process is in dangerous state too. There is no need to distinguish between dangerous state of the SRCS (DSS) and dangerous state of the controlled process (DSP) and these two states we can equated. Safe states of the control process are not relevant in terms of the safety analysis.

The dangerous state of the SRCS (DSS) can occur due to following hazards:

- failure of the considered safety function,
- error of the operator or HMI when entering the safety critical commands during normal (no-failure) operation of the SRCS if the operator controls actuators directly,
- error of the operator or HMI and simultaneous EF malfunction (if the SRCS disposes of them) when entering the safety critical commands during emergency operation of the SRCS.

Following transitions between states in Fig. 7 relate with hazards bound to the operator error:

- transition between FSS and DSS states; it is the transition which is applied during no-failure operation of the SRCS if the operator can control actuators directly; the intensity of the transition depends on the frequency of issuing such commands and on the operator error or HMI failure probability,
- transition between P-FSS and DSS states; it is the transition which is applied in case of partial

functional SRCS; transition intensity depends on applied mode of the emergency control (one-stage or double stage control), on the operator respectively HMI failure probability and on frequency of safety critical commands entering,

- transition between states N-FSS and DSS; it is the transition which is applied in case of the SRCS malfunction; transition intensity depends on mode of process controlling by the operator (single-stage or multi-stage control), on the operator error or HMI failure probability and on frequency of safety relevant commands entering (frequency of safety critical commands entering is higher than in transition between states P-FSS and DSS).

Safety analysis of the controlled process should be provided individually for each safety function realized by the SRCS.

For practical usable of the procedure described in this paper for safety assessment of the controlled process, it is necessary:

- to compile the state-space diagram describing dangerous state occurrence base on good knowledge of the specific SRCS and the controlled process; compiled diagram should respect not only factors influenced the safety of the SRCS (its architecture, reliability, diagnostic ...), but also the mode of SRCS operation and the role of the operator in control of the process,
- to determine the intensities of transitions between individual states of the model.

Determination of the transitions intensity (especially of the transitions related to human error and frequency of issuance of safety critical commands of the operator) is very difficult. It is necessary to use statistical data acquired from operation of such systems. Detailed information regarding human error of the operator and frequency of the safety critical commands used for control of the railway transport process were published in [7].

4. Conclusion

There is established indirect safety assessment of the controlled process using assessment of the technical measures (safety assessment of the SRCS) and organizational measures (among other things, measures to minimize probability of operator error) applied to eliminate the hazards related to the controlled process.

Operator error rate cannot be a quality criterion of the SRCS. In order to ensure objectivity of the safety assessment of technical design of the SRCS it is necessary to pay attention to the technical measures designed to eliminate potential operator error in an emergency operation. In this evaluation it is necessary to consider a nominal value of the HEP (for example statistically determined value for specific type of the controlled process).

There is not considered intentional threat of the controlled process by the operator in safety assessment of the process. Design of control systems resistant to operator bad motives would result in a significant increase of their price and operability reducing of such system also. Operability reducing would lead to serious problems in the controlling of processes which running cannot be interrupted.

Acknowledgment

This paper was supported by the scientific grant agency VEGA, grant No. VEGA-1/0035/15 “Analysis of operator – control system interaction effect on the controlled process safety”.

References

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

[2] RASTOCNY, K. and J. ILAVSKY. Quantification of the Safety Level of a Safety-critical Control System. In: *Proceedings of international conference on Applied Electronics 2010*. Pilsen: IEEE, 2010, pp. 285–288. ISBN 978-0-7043-865-7.

[3] ILAVSKY, J. and K. RASTOCNY. Comprehensive technical safety analysis approach including common-cause failures. In: *9th international conference ELEKTRO 2012*. Rajecke Teplice: IEEE, 2012, pp. 299–304. ISBN 978-1-4673-1180-9. DOI: 10.1109/ELEKTRO.2012.6225608.

[4] RASTOCNY, K. and J. ILAVSKY. What Is Concealed Behind the Hazardous Failure Rate of a System? In: *Proceedings 11th International Conference on Transport Systems Telematics, TST 2011*. Katowice: Springer Berlin Heidelberg, 2011, pp. 372–381. ISBN 978-3-642-24660-9. DOI: 10.1007/978-3-642-24660-9_43.

[5] RASTOCNY, K., J. ZDANSKY and P. NAGY. Some Specific Activities at the Railway Signaling System Development. In: *Proceedings of 12th International Conference on Transport Systems Telematics, TST 2012*. Katowice: Springer Berlin

Heidelberg, 2012, pp. 349–355. ISBN 978-3-642-34050-5. DOI: 10.1007/978-3-642-34050-5_39.

[6] RASTOCNY, K., L. PEKAR and J. ZDANSKY. Safety of Signaling Systems - Opinions and Reality. In: *Proceedings of 13th International Conference on Transport Systems Telematics, TST 2013*. Katowice: Springer Berlin Heidelberg, 2013, pp. 155–162. ISBN 978-3-642-41647-7. DOI: 10.1007/978-3-642-41647-7_20.

[7] NAGY, P. *Emergency operation of external elements of railway signaling systems.* Zilina, 2014. Ph.D. thesis. University of Zilina. Supervisor Karol Rastocny.

[8] STRAETER, O. Investigations on the Influence of Situational Conditions on Human Reliability in Technical Systems. In: *13th Triennial Congress of the International Ergonomics Association*. Tampere: IEEE, 1997, pp. 76–79. ISBN 978-9518021882.

[9] CHANDLER, F., I. A. HEARD, A. PRESLEY, A. BURG, E. MIDDEN and P. MONGAN. *NASA Human Error Analysis*. NASA [online]. 2010. Available at: `http://www.hq.nasa.gov/office/codeq/rm/docs/hra.pdf`.

[10] ZHIQIANG, S., X. HONGWE, S. XIUJIAN and L. FENGQIANG. Engineering approach for human error probability quantification. *Journal of Systems Engineering and Electronics*. 2009, vol. 20, iss. 5, pp. 1144–1152. ISSN 1004-4132.

[11] ZDANSKY, J. and J. HRBCEK. The choice of the appropriate structure of the control system with respect to the required availability and safety. In: *Proceedings of 5th international scientific conference: Theoretical and Practical Issues in Transport.* Pardubice: University of Pardubice, 2010, pp. 172–177. ISBN 978-80-7395-244-0. Available at: `http://dspace.upce.cz/handle/10195/37815`.

[12] ZDANSKY, J. Using PLC for control of safety-critical processes. In: *Proceedings of International conference OWD 2004*. Gliwice: Silesian University of Technology, 2004, pp. 421–426. ISBN 83-915991-8-3.

[13] ZDANSKY, J. Modeling of safety characteristics of control system with safety PLC. In: *Proceedings of International Scientific Conference Modern Safety Technologies in Transportation 2009*. Zlata Idka: Technical University of Kosice, 2009, pp. 303–308. ISBN 978-80-970202-0-0. Available at: `http://www.mosatt.org/archiv/mosatt2009/zbornik/303.pdf`.

About Authors

Peter NAGY was born in 1962 in Trutnov, Czech Republic. He received Ph.D. in 2014 at University of Zilina in the field of "Control Engineering". His professional orientation covers railway signaling systems, security systems and information system. His research activities are focused on safety issues of railway signaling systems and their safety assessment.

Karol RASTOCNY was born in 1958 in Setechov, Slovak Republic. He received his Prof. in 2009 in the field of "Control Engineering". His professional orientation covers solving problems of functional and technical safety, hazard analysis and risk analysis of safety-related applications, preferably oriented to railway domain.