RISK ANALYSIS OF SATETY-CRITICAL CONTROL SYSTEMS

K. Rástočný

Department of Control and Information Systems, Faculty of Electrical Engineering, University of Žilina, Univerzitná 8215/1, SK-010 26 Žilina, Slovakia, Phone.: +421 41 513 3320, E-mail: karol.rastocny@fel.uniza.sk

Summary: This paper deals with problems associated with risks analysis of a safety-critical control system. In the paper there are introduced recommendations enabling practical enforceability of risk analysis by the assurance of sufficient objectivity level. In the initial phases of the system lifecycle risk analysis serves for a tolerable hazard rate definition for individual safety relevant functions. In the end of the control system development process the risk analysis (an analysis of failures consequences on system safety) serves for the verification of system safety attributes.

1. INTRODUCTION

There is a class of control systems (so-called safety-critical), whose faulty function can result in personal injuries, considerable material damages, environmental damages, or other undesirable after-effects. System like this has to be realized in such a way, that in the case of a failure-free operation it must perform exactly the specified functions (functional safety) and in the case of a failure occurrence it must either remain in a safe state (if the state in which the system is found doesn't endanger the controlled process), or proceed to a predefined safe state (technical safety).

It's obvious, regard to the knowledge level, technological level and limited financial resources, that it is not possible to calculate on the absolute safety (zero risk), but really it is necessary to assume the occurrence of an error, or a failure in the system, which can lead to a certain risk for the controlled process. Providing the evidence of safety requirements fulfilment and of a final risk acceptability is possible only on the basis of the safety analysis. It's not possible to prove the strict safety requirements for the safety relevant system only by tests or praxis results.

Generally, safety of a system can be understood as a set of system properties. A certain dependency exists between these properties. The goal is to create a model, which enables to analyze the sensitivity of the system to particular factors influencing its safety attributes and to find a global optimum with the respect to these attributes, assuming an economical acceptability of the proposed solution. Accomplishment of this goal is related to the problems solving in the following areas:

- Risk analysis;
- Modelling of system RAMS parameters.

The fundamental international standard dealing with safety-critical control systems is the standard [12]. On the base of this standard some other application standards are derived, among them for example standards for railway applications [9], [10], [11] or industrial applications [13]. Depending upon requirements on system safety these standards define 4 safety integrity levels and for every safety integrity level (SIL) practices are recommended, that have to be performed in individual life-cycle phases of the system in order to achieve the ability of the system to fulfil required functions in regard to the Reliability, Availability, Maintainability, Safety (RAMS parameters) and their mutual effects.

These standards define common safety targets, recommend practices for achieving the required safety integrity level and methods for its evaluation, however definition of objectives is ambiguous and methodical directives for the safety evaluation are rather general. Negative influence also results from the fact, that a generally acceptable theoretical apparatus for a risk analysis and safety level evaluation is missing, which would objectify the whole process of safety consideration. Therefore a great attention is paid to this problem in international discussion forums (e.g. http://www.sipi61508.com), open specialised consortia (e.g. http://www.railwaydomain.org, http://www.fmeurope.org), projects (e.g. http://samnet.inrets.fr) and conferences (e.g. http://www.forms-format.net). It is pleasant, that by issuing of these standards the standardization process in safety critical control systems area is not finishing but overshooting the preparation of new standards and revision of already accepted standards.

Nowadays used or developed practises for safety attributes evaluation may be basically divided in two groups:

- Creation of the model, that provides the complex description of failure consequences on functional and technical safety; such a model could be usable for the risk analysis, specification of the functional requirements and verification of safety attributes of the system; on the basis of Petri nets such a model is developed within the project Thomason [6], [8];
- Using the combination of methods; special methods and models are used for the risk analysis (hazard graph, risk matrix, BP-risk, ..), other for specification and modelling of functional properties of the system (UML, finite automaton, Z-language, Petri nets, …), and another for modelling of RAMS parameters of the system (FMEA, FTA, Markov chains, Petri nets, ..) [3], [4], [7].

2. MODELLING OF RAMS PARAMETERS OF THE CONTROL SYSTEM

Since particular RAMS parameters influence each other, it is necessary to propose such a solution, which enables complex modelling of RAMS parameters. When modelling RAMS parameters, the factors affecting them must be respected, especially:

- Degree of redundancy applied in the system;
- Reliability of system components;
- Diagnostic coverage, fault detection-and-negation time;
- Recovery of availability of the system after failure.

In the case of complex RAMS parameters analysis the stochastic process is concerned for whose modelling for example Markov chains or Time Petri Nets can be successfully used. However, Markov chains have their limits. Their main disadvantage is that during modelling constant transition intensities are supposed (homogenous Markov chain). That means, that occurrence of events, which influence transitions between states, must be approximated by the exponential distribution, that mustn't always correspond to reality. Though non-homogenous Markov chains can be theoretically considered, but the solution is rather complicated.

Even though in the case of RAMS parameters analysis of the system, the Markov models have specific constraints, they are generally accepted. Basically, creation of such a Markov model may proceed in two ways:

- Logical consideration based on analyst's expert approach; this way tends to analyst's mistakes and therefore has limitations in respect of system's states quantity; nowadays it is a utilised method for diagrams creation;
- Automatic generation; automatic computer model generation leads to models with large number of states; this method requires the utilisation of quality computer equipment and specific software tools, which enable states number reduction and selection of an appropriate numerical method so that results can be obtained in real time with the sufficient precision; this practice is suitable for the analysis of system reliability attributes, but it is not used for the analysis of RAMS parameters.

Nowadays the project [5] is submitted; whose one of the goals is achieving an automatic generation of transition intensities matrix either in a universal way, or at least for some specific cases. Solution based on an atomisation of the system and a combination of different quantitative methods comes into account. Safety attributes on system's components level would be modelled using one method and bonds between components would be modelled using another method.

Analysis of stochastic models can be realised in several ways. They differ in the results precision, application options and computing demands. The following approaches are supposed:

- Simulation;
- Numerical solution;
- Analytical solution.

The use of an analytical solution in combination with the numerical solutions supported by an appropriate software tool seems to be the most suitable.

3. PROCESS OF THE RISK ANALYSIS OF THE CONTROL SYSTEM

Development of the safety-critical control system must be based on specification of the safety requirements, which are defined on the base of risk analysis associated with a controlled process. SIL of the system is proportional to a difference between calculated or estimated risk and acceptable risk. Nowadays there is no generally accepted unified method for risk analysis. There are numbers of methods and procedures for risk analysis (depending on an application area), which are usually based on a subjective evaluation of "sensitivity" of risk factors, what results in the fact, that different collectives of analysts may obtain significantly different results, even when using the same method. This problem comes into spotlight especially when malfunction of the control system can lead to human casualties (problem of an acceptable risk). Process of the risk analysis can be objectified only on the base of quantitative methods, which lean on the theoretical considerations and accident-events statistical data.

Risk analysis (even analysis of failure consequences on control system safety) can be realised using quantitative or qualitative methods, but more frequently by the combination of these methods [7]. Qualitative methods help to understand consequences of different failures of system components on the entire system and a logical structure of their mutual relations. Quantitative methods utilise available data about component failures, human mistakes, repair times, and so on and enable to determine the probability of a certain system's critical state occurrence [1].

Generally risk can be formulated as a combination of hazards rate and their consequences for a certain time unit. Therefore in the process of risk analysis it is necessary to define system's incidence boundaries, identify hazards, determine intensities of their occurrence, evaluate damages caused by individual hazards, and evaluate the overall risk associated with a controlled process. Based on knowledge of the overall risk and acceptable risk tolerable hazard rate (THR) can be derived and consequently SIL can be assigned to functions and components of the system.

Hazards identification is an important moment of the risk analysis (to create a hazard list). Hazard list may be created on the base of theoretical consideration and analyses or on the base of present experiences in an analogical system operation and statistical entries, but more often by proper

combination of these two possibilities. What is necessary to consider being hazard depends on system analysis level. Risk analysis result is not dependent on quantity of the hazards identification but thereon how the entire area of the hazardous states is covered. Individual hazards have to be independent to each other. It is desirable, if the hazard list copies list of safety relevant system functions (Fig. 1). For instance, if function F_1 states claim on performance of certain operation, then the hazard H_1 states faulty performance of this operation. This kind of the approach to hazards identification and to creation of bonds among hazards considerably simplifies the safety requirement definition process for individual modules of the control system. Definition of hazard rate is quite problematic and generally has to be accomplished on the base of the expert estimation (solution like this considerably impacts objectivity of quantitative analysis). The determination of hazard rate is inaccurate on the basis of statistical data about accidents, since not every hazard results in accident.

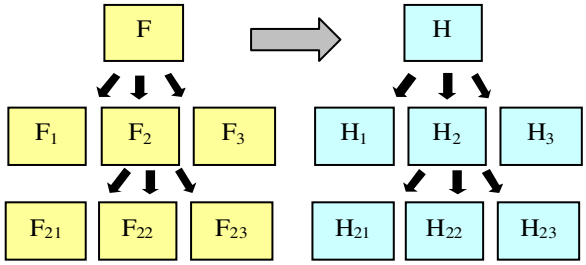

Fig.1 Relation between functions tree and hazards tree

Identification of the individual hazard results may be set on the basis of the practical experiences (statistical data) in the control process or on the expert estimations (mainly when there are processes without practical experiences). Problems are uprising if hazard may cause not only material damages but also human casualties.

Quantitative risk analysis requires material damages and human casualties transfer to a common unit (how to qualify human health?). In this case the following possibilities come into account:

- Material damages neglect, if hazard can result in a serious human health harm;
- Risk calculation particularly for material damages and particularly for human casualties.

By qualitative risk analysis simultaneously material damages and human casualties can be considered.

Consumer states range of acceptable risks in the case of material damages. Concerning human casualties the legal requests must be respected, which issue either from collective risk (for example GAMAB criteria) or from individual risk (for example MEM or ALARP criteria) [9]. In the practical life such an approach can be met when design of a new system results from statistical data related to an old (existing) system. The problem is that the set of the new and the old system functions have not to be identical on each other (for example if a new system contains a new function, necessary statistical data does not exist).

4. IMPLEMENTATION OF SAFETY REQUIREMENTS

Result of risk analysis is definition of THR for the individual safety relevant functions (F_1, F_2, ... F_m). It is necessary to realise the decomposition of the control system to individual modules (M_1, M_2, ... M_n) and these consequently identify with the realised functions. Nevertheless, one module can realise more functions or one function is realised by more modules (Fig. 2). Decomposition have to be realised in such a way, in order to modules could be independent on each other.

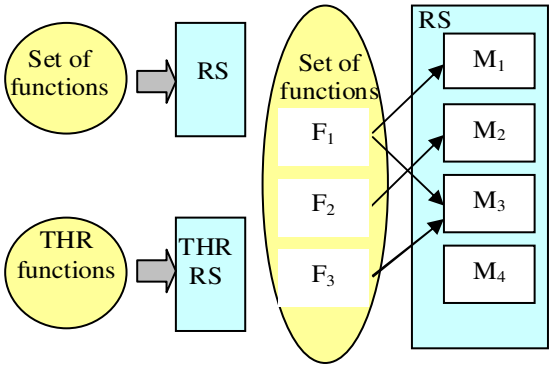

Fig. 2 Function assignment to system modules

Result of risk analysis is definition of THR for the individual safety relevant functions (F_1, F_2, ... F_m). It is necessary to realise the decomposition of the control system to individual modules (M_1, M_2, ... M_n) and these consequently identify with the realised functions. Nevertheless, one module can realise more functions or one function is realised by more modules (Fig. 2). Decomposition have to be realised in such a way, in order to modules could be independent on each other.

If the *i*-th function is realised only by the *j*-th module then holds:

$$THR_M \leq THR_F \ , \tag{1}$$

where THR_F is a tolerable hazard rate for given function and THR_M is a tolerable hazard rate for the given module.

If the function is realised by several modules (*n* modules), then holds:

$$THR_F \geq THR_{M1 \cap M2 \cap \ldots \cap Mn} \ , \tag{2}$$

where $THR_{M1 \cap \ldots \cap Mn}$ is an entire tolerable hazard rate of modules 1 to *n* considering realised function.

If the module realises several functions (*n* functions) then holds:

$$THR_M \leq THR_{F1 \cap F2 \cap \ldots \cap Fm} \ , \tag{3}$$

where $THR_{F1\cap..\cap Fm}$ is an entire tolerable hazard rate of functions 1 to *m* considering the module, that realises them.

If the module realises no safety relevant function, then no safety requirements are laid on it.

In connection with the dissemination of THR on individual parts of the system question of system structure is also necessary to be solved.

Selection of a system structure is one of the most important decisions during the development process. By choice of the structure it is necessary to progress very carefully, because a compromise between cost, SIL and availability of the system is concerned. The selection of the structure has to be done based on the results of RAMS parameters modelling. Created model enables choosing the most suitable solution so that customer's requirements on the individual RAMS parameters of the system will be respected. A model created in early phases of lifecycle can be progressively refined and utilised for the results verification obtained in particular phases of the development process.

5. CONCLUSION

Risk analysis has to be realised several times (with different depth) during the system development. In the initial system development phase it serves for a definition of tolerable hazard rates of the system or its individual parts. In other system development phases it serves for the control whether real values of the hazard rate of the system or its individual parts are acceptable.

In practical life we also often meet with demand for improving quality of services that have already been provided by an existing safety-related system (for example change of an existing function or implementation of a new function). To accept this demand means to implement a new module (hardware and/or software) into the system. Acceptable risk resulting from process control usually does not vary (is not increased) even though a new function has been implemented. On the contrary, implementation of a new function can cause increase of risk resulting from operation of a modified system. However, adding a new module (system) cannot bring increase of risk of the controlled process above the acceptable level. Therefore it is necessary to define not only functional but also safety requirements for this kind of module.

This work has been supported by the scientific grant agency VEGA, grant No. VEGA-1/0040/08 "Mathematic-graphical modelling of safety attributes of safety-critical control systems".

REFERENCES

[1] BRADLEY, J.: Elimination of Risk in Systems. Tharsis Books, 2002

[2] RÁSTOČNÝ, K. – JANOTA, A. - ZAHRADNÍK, J.: The Use of Development of a Railway Interlocking System. In Journal: Lecture Notes in Computer Science, Springer-Verlag Heidelberg, 2004, pages 174-198, ISSN 0302-9743

[3] RÁSTOČNÝ, K.: Model for safety analysis of the interlocking system. International scientific conference ELEKTRO ′99, 25 – 26 May 1999, Žilina, pp.13 – 18, ISBN 80-7100-602-5

[4] RÁSTOČNÝ, K.: Risk Analysis of a Railway Interlocking System. In: AEEE, No. 3 – 4 Vol. 2/2003, ŽU v Žiline, pp. 24 -29, ISSN 1336-1376 (in Slovak)

[5] RÁSTOČNÝ, K.: Mathematic-graphical modelling of safety attributes of safety-critical control systems. Project VEGA, No. 1/0040/08

[6] SLOVAK, R. et al.: Toolunterstützte Modellierung, Analyse und Synthese sicherheitsrelevanter Steuerungen für den Einsenbahnverkehr mit Petrinetztechnologie. Project Tomasen. TU Braunschweig

[7] ZAHRADNÍK, J. – RÁSTOČNÝ, K. – KUNHART, M.: Safety of Railway Interlocking Systems. EDIS, 2004, ISBN 80-8070-296-9 (in Slovak)

[8] ZAHRADNÍK, J. et al.: Tool-supported modelling, analysis and synthesis of railway safety systems by Petri nets technologies. Project No. 03 Cost 04 24/604, ŽU v Žiline

[9] EN 50126: Railway applications: The specification and demonstration of dependability, reliability, availability, maintainability and safety (RAMS)

[10] EN 50128: Railway applications: Communications, signalling and processing systems - Software for railway control and protection systems

[11] EN 50129: Railway applications: Safety related electronic systems

[12] EN 61508: Functional safety of electrical /electronic/programmable electronic safety-related systems

[13] EN 61511 Functional Safety. Safety Instrumented Systems for the Process Industry Sector