Functional safety analysis of control systems consisting of programmable units for using in transportation

Wojciech Romański*, Kazimierz Kosmowski,**
Piotr Gappa, Andrzej Powarunas**, Marcin Śliwiński****

* AREX, Gdansk, Poland
wojciech.romanski@arex.pl

** Gdansk University of Technology, Gdansk, Poland
kazimierz.kosmowski@ely.pg.gda.pl, msgdw@wp.pl

Abstract - **Nowadays a trend is observed in designing the control system to equip them with programmable electronic units. The application of programmable electronic units in safety – related systems implicates the requirements for safety integrity level (SIL) and a high availability factor. A real control system for road transportation is described, which controls the signaling lights and monitors its operation. This system is designed using programmable logic controllers. In the paper the reliability analysis of the control system is carried out. Two methods have been used that are available in the CARE software system, namely FMEA (Failure Mode and Effect Analysis) and RBD (Reliability Block Diagram) to analyses potential failure modes of units and subsystems and to asses levels of safety and availability of the road transportation control system. The results of analyses and assessments enabled to formulate several conclusions how to improve the safety and availability of the system under consideration.**

1. Introduction

It is hard to imagine life in modern world without road communication. Road infrastructure of cities is an important element of their proper development. Functioning of city agglomeration is impossible without efficient road traffic signaling. Bad functioning of road traffic signaling causes burdensome hindrances in everyday life of cities. The first light road traffic signaling systems were constructed basing on the use of transmitters. These systems have many advantages, but there exists a substantial difficulty in modifying the controlling algorithm. The development of motorization has caused arising need to create systems of road traffic signaling control to make possible modifying the controlling algorithms.

The development of electronics caused appearance of programmable controllers used widely in modern systems. The use of controllers enables elasticity in changing the program servicing the traffic controlling. The use of systems equipped with programmable units enables creating the area systems having possibility of full city road traffic control, including adaptation of the road traffic signaling according to changes in street traffic volume.

Intelligent road traffic control, consisting in constant adapting of the algorithm "accommodation" to changes in street traffic volume allows for discharging traffic-jams of given road infrastructure. It is very useful, however, it involves much more complex architecture of the control systems, consisting of logic controllers, and communication

between those controllers. The functional safety of modern road traffic signaling systems depends both on hardware and software

2. Description of the structure of the examined system

Road traffic signalling control system consists of a computer controlling the net of crossroads grouped in controlled areas. The control over a crossroad is performed by controllers of road traffic signalling. System controller is responsible for optimisation of traffic lights work in the area. On a base of traffic measurements (traffic volume, flow ratio, queue length) and data coming from neighbouring controllers it determines the controlling parameters (cycle length, split, offset).

There is a communication between controllers working at the very area. Due to this communication there takes place exchange of information on the state of road traffic density at crossroads grouped in the area. In fully developed system comprising the whole city there is possible full exchange of information between areas and the central point, in aim of full control of the road traffic controlling. Due to it there is possible to achieve bigger road flow capacity for the same road infrastructure. Additionally it allows to control the state of the road traffic at roads of the whole city and it reduces also time of eliminating failures.

Due to control from the central point there is possible setting to controllers the change of algorithm settings in aim to reduce flow ratio at the specific area, or enabling free ride for a privileged vehicle. During normal work controllers perform an algorithm of green extension in depends on traffic at peculiar intersections. In our considerations concerning functional safety we performed analytic tests on a model, which block scheme is shown on Fig. 1. There were analysed different configurations of communication net between controllers.

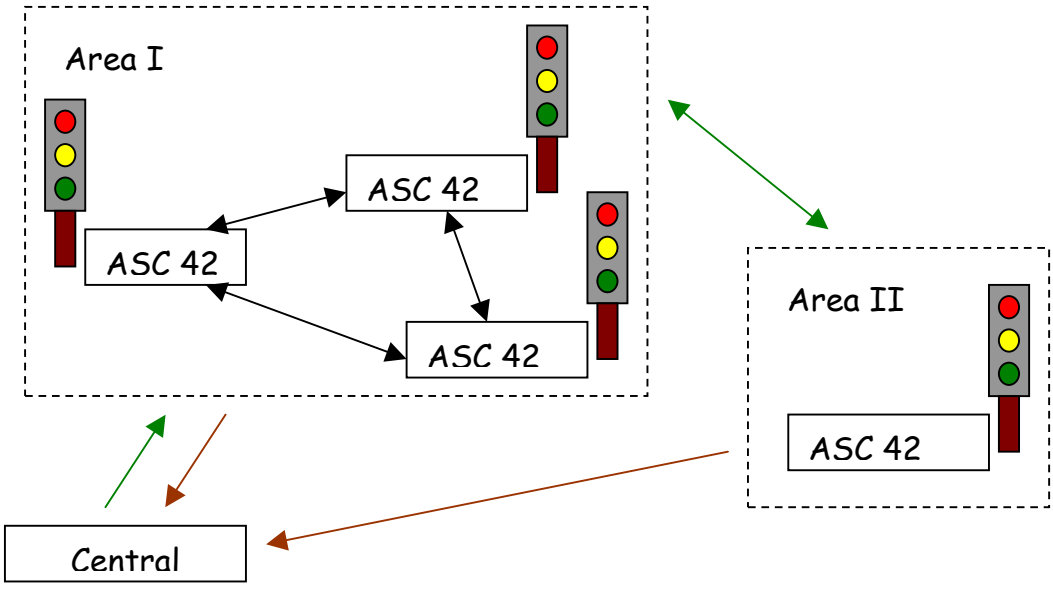

Fig. 1. Block scheme of an area road traffic controlling system

3. Construction of a controller and a communication network

Analysed controller of a road traffic signalling is destined for group controlling the road traffic signalling at crossroads. It enables performing both simple and complex controlling

algorithms. It has possibility to memorise tens of programmes. The controller is equipped with two independent processors.

Module of central unit – MCU-19 is responsible for performing controlling algorithm and communication with local modules. This module controls state of all controlling circuits and detectors. All detected failures are stored in an archive. The second processor is placed in conflict and intergreen time detection module MDC – 01. It is equipped in a "watch – dog" units and performs inspection of a controller.

Switch module MS-41 performs directly switching light circuits and inspecting their state. It is equipped with five independent switches of lights red, amber, green and conditional arrow and failure state switch – amber flash lights.

Two-state input-output module MIO – 88 enables connection to the controller of 8 input signals and 8 two-state outputs. The inputs can be used for servicing outside traffic detectors, co-ordination signals of other controllers or for servicing push-buttons for pedestrians.

Vehicle detection module MIL – 81 is used for detecting vehicles by means of induction loops. It is possible to connect 8 independent loops to the module. In case of a failure the loop is switched off and every minute there is made test of its circuit. When the failure passes the loop comes back to normal work.

Power supplier module MZ – 120 is three-phase impulse supplier supplying all the remaining electronic units with 12 V current. This power supplier enables automatic choose of the active phase.

Permanent communication between controllers inside an area is necessary for correct working of the control optimisation algorithm. The permanent communication between areas and the central point is not required and e.g. PSTN connections can be used. Connections between areas are not required. However this connections can affect better control quality in many cases.

Network structure depends on roads infrastructure and area partition. Technical and financial possibilities are also very important. It means there is not possible to find one universal network structure for all cases. Always an analysis should be done in order to obtain the best possible solution. In communication network design two basic advices can be used:

- controllers in neighbourhood on the same road should be directly connected,
- loops should be created when it is possible.

Disconnections in communication inside the area doesn't cause the serious failure of the all traffic lights. However it makes impossible the data exchange between controllers and optimisation of the traffic control in the area. Traffic light controllers are working at that time in local mode and optimising the control only in one intersection.

4. FMEA analysis of a controller

There was made FMECA analysis for a single controller. It is an analyse of kinds, results and criticality of failures. FMECA is an induction method of non-failure and safety analysis of a system. It defines results and sequence of events caused by identified kinds of failures. It enables classification and grouping of identified failures according to possibility of their detection, diagnosis, testing or exchange of elements. It also values levels of criticality for specific kinds of elements failures or whole distinguished units and evaluates possibility of failure occurrence. The aim of criticality analyse is scheduling potential kinds of failures

identified according to FMEA rules, on a base of criticality levels and probability of occurrence [1].

The controller was modelled in CARE programme. The tree of functional dependence for FMEA analysis is shown in Fig. 2.

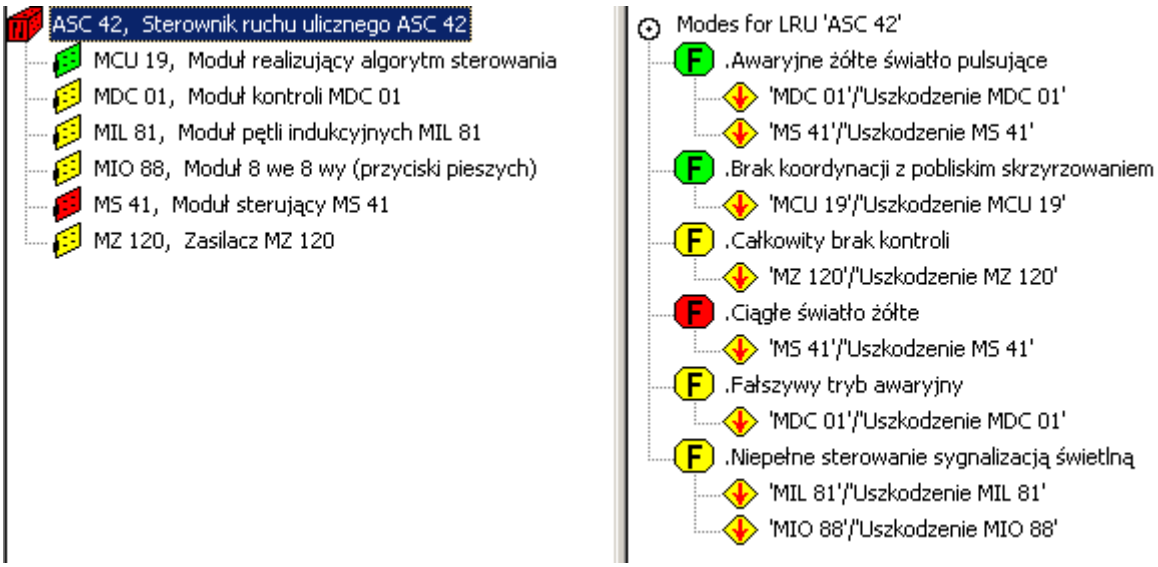

Fig. 2. FMEA tree of the controller

The analysis was performed on a base of real data on failures of the controller elements. In the above fig. Particular colours define kinds of failures. The red colour defines the most critical failures, which are the most dangerous for the considered object. The yellow colour defines kinds of failures having medium influence on proper work of the considered system. The green colour implies low harmfulness of the specific failures. As it can be observed on the fig., the most critical failure is a breakdown of the controlling module MS – 41., causing occurrence of specific kind of a failure – continuous yellow light.

Table 1. presents failure modes qualitative criticality matrix for failures occurring in system of a controller. Table 2. presents list of kinds of failures with assigned to them level of criticality.

Table 1: Failure Modes Qualitative Criticality Matrix

Failure Modes Qualitative Criticality Matrix (Quantity for Internal Causes only)					
CRITICALITY	**SEVERITY**				
Group Description	**V**	**IV**	**III**	**II**	**I**
[A]-Frequent	0	0	0	0	0
[B]-Reasonably probable	0	0	0	0	0
[C]-Occasional	0	0	1	3	1
[D]-Remote	0	1	1	2	0
[E]-Extremely unlikely	0	0	0	0	0

Table 2: Qualitative Critical Failure Mode List

Qualitative Critical Failure Mode List (Full Report for Internal Causes only)						
Region	**Sev**	**Critic. Group**	**Blk#**	**RefDes**	**Function**	**Failure Mode Name**
2	I	C	6	MS 41	Moduł sterujący MS 41	Uszkodzenie MS 41
	II	C	4	MIL 81	Moduł detekcji pojazdów MIL 81	Uszkodzenie MIL 81
			5	MIO 88	Moduł WE/WY dwustanowych	Uszkodzenie MIO 88
			6	MS 41	Moduł sterujący MS 41	Uszkodzenie MS 41
	III	C	6	MS 41	Moduł sterujący MS 41	Uszkodzenie MS 41
3	II	D	3	MDC 01	Moduł kontroli kolizji i czasów międzyzielonych	Uszkodzenie MDC 01
			7	MZ 120	Moduł zasilacza MZ 120	Uszkodzenie MZ 120
	III	D	3	MDC 01	Moduł kontroli kolizji i czasów międzyzielonych	Uszkodzenie MDC 01
	IV	D	2	MCU 19	Moduł jednostki centralnej	Uszkodzenie MCU 19

On a base of data presented in above tables it can be stated, that in considered configuration the controller is a safe system, because combination of criticality and frequency of kinds of controller modules failures is not situated in the most critical area – the red colour area. It is however alarming thing that there were obtained five kinds of modules failures in medium area of criticality – the yellow colour area. In Table 3. There are shown probabilities of occurrence of kinds of failures and criticality of those failures. The most critical final result – "continuous yellow light" has low probability of occurrence 0.0087 what gives good prognosis for the whole controller. In Table 4. there was shown criticality indicator. Possibility of occurrence of an event which would end in catastrophic results is for the considered system very low 0.875. It is 0.87% of the whole number of failure events.

Table 3: Qualitative Critical Failure Mode List

##	End Effect Name	Severity	System Failure Rate [F/10^6Hrs]	End Effect Ratio (Alpha)	End Effect Rate [F/10^6Hrs] F=D*E	End Effect Ratio for Severity	End Effect Probability H=exp(-F*t)
1	Ciągłe światło żółte	I	100.9	0.008672	0.875	1.000000	0.00871183
2	Fałszywy tryb awaryjny	II	100.9	0.296705	29.9375	**0.572009**	**0.258719**
3	Niepełne sterowanie sygnalizacją świetlną	II	**100.9**	**0.202180**	**20.4**	**0.389778**	**0.184538**
4	Całkowity brak kontroli	II	**100.9**	**0.019822**	**2**	**0.038214**	**0.0198013**
5	Awaryjne żółte światło pulsujące	III	**100.9**	**0.314049**	**31.6875**	**1.000000**	**0.271578**
6	Brak koordynacji z pobliskim skrzyżowaniem	IV	**100.9**	**0.158573**	**16**	**1.000000**	**0.147856**
Total				**1.000000**	**100.9**		

Table 4: Criticality indicator

Severity	Severity Rate [F/10^6Hrs]	Ratio [%]	Severity Description
I	0.875	0.87	Catastrophic - A failure which may cause death or system loss.
II	**52.3375**	**51.87**	Critical – A failure which may cause severe injury, major property damage, or major system damage which will result in mission loss.
III	**31.6875**	**31.40**	Marginal - A failure which may cause minor injury/property/system damage which will result in delay or lost of availability or mission degradation.
IV	**16**	**15.86**	Minor - A failure not serious enough to cause injury, property damage, or system damage, but which will result in unscheduled maintenance or repair.
V	**---------**	**------**	User defined.
Total	**100.9**	**100.00**	

5. RBD analysis of the controller

During further works there was performed RBD (Reliability Block Diagram) analysis of the road traffic signalling controller, the obtained results were used for performing an analysis of the system of road traffic controlling. RBD analyse is a graphic presentation of non-failure of the system [2,3]. It shows logic connections of elements ensuring the work of the system. After performing RBD analyse we obtain the following numerical data, characterising the considered object:

Reliability (R) – the probability of failure absence during a defined operation time (reliability definition time, T) after starting the operation.

R(t) - reliability curve - the probability of failure absence for any t.

Availability (A) (for repairable blocks only) – the probability of a block to be good at a defined moment of time.

MTTCF – the **M**ean **T**ime (hours) **T**o (the first) **C**ritical **F**ailure. The failure is critical when the block cannot perform its function. **RBD** operates with critical failures only.

MTBCF (for repairable blocks only) - the **M**ean **T**ime **B**etween **C**ritical **F**ailures.

FPMH – the number of **F**ailures **P**er **M**illion **H**ours. **FPMH = 10^6/MTBCF**

MTTR – **M**ean **T**ime **T**o **R**epair (the average repair time after a failure).

Down Time (DT) – the average total repair time during T [4,5].

Block scheme of the considered controller is shown at Fig. 3.

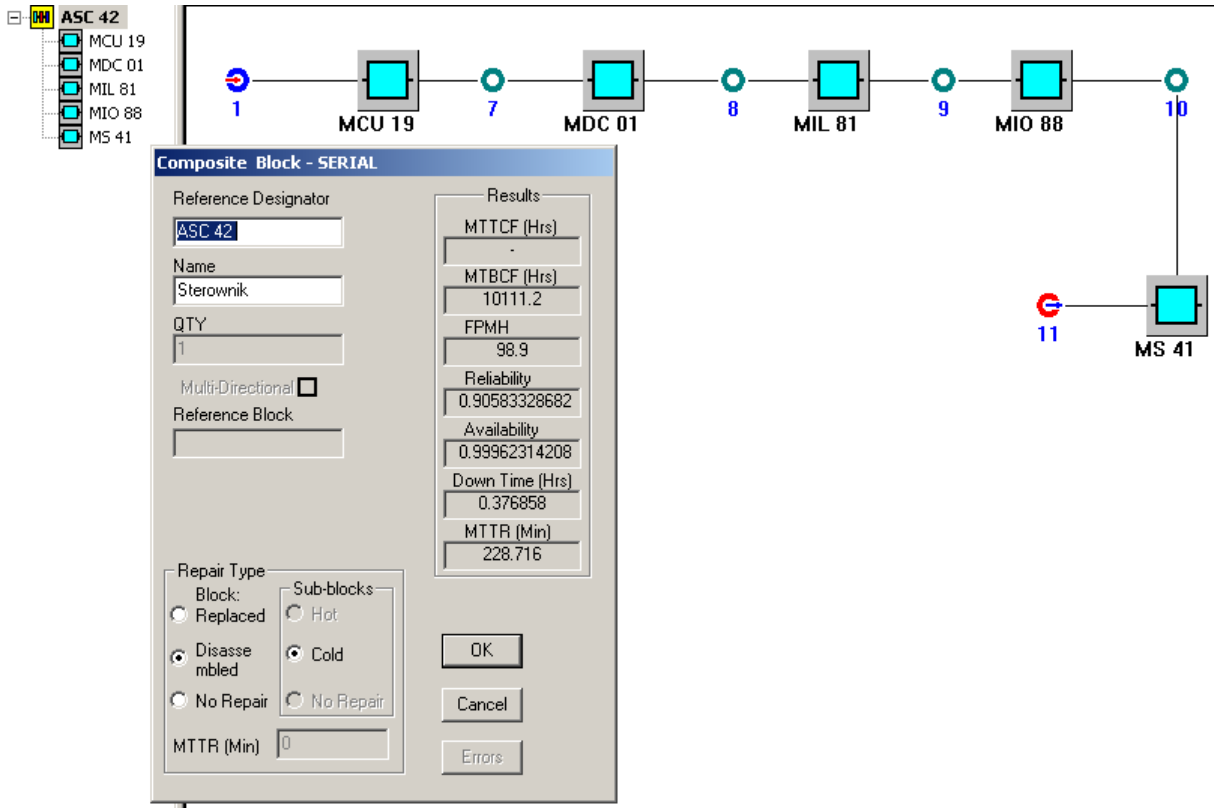

Fig. 3. Block scheme of the road traffic signalling controller

As it can be observed in the fig., the controller was modelled as a series structure. To ensure proper work of the controller there is required functioning of all its modules, which were described above.

From the performed analyse there results, that reliability of the controller equals R = 0.906, availability A = 0.999623 and number of failures per million of hours FPMH = 98.9. Reliability data considered in the analyse were obtained during observation of a real object.

6. RBD analysis of an area road traffic controlling system

The aim of performed examinations, which results are shown in this chapter, is determining the best configuration of the system shown in Fig. 1. Proper work of the considered system consists in adaptive controlling the road traffic by light road traffic signalling, supervised from central unit. Analysed system is a two-area one. In area I there are placed three controllers ASC 42, while area II is serviced by one controller. Inside area communication between controllers is a system with cold reserve. Communication between central unit and areas is performed by an unit with redundancy 1 with 3. The work of the whole system is supervised from central unit. It can decide upon change of the controlling road traffic signalling programme, what makes possible real-time reaction for changes in traffic density. The work of the system may be fully automatic, the central unit performs function of monitoring the state of traffic on the roads. In such a case net of controllers, by means of information exchange, controls by itself the density of the traffic in the city, not allowing for traffic jams creation.

Following are schemes of models which were analysed.

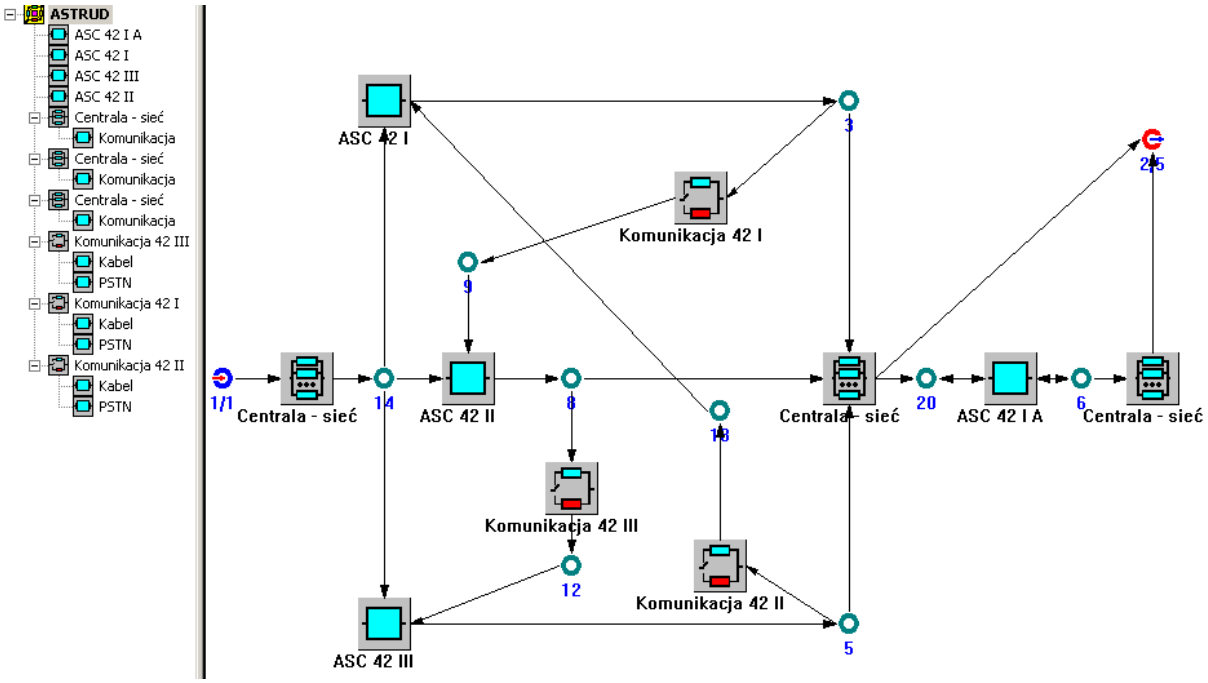

Fig. 4. Block scheme of an area road traffic controlling system. System I

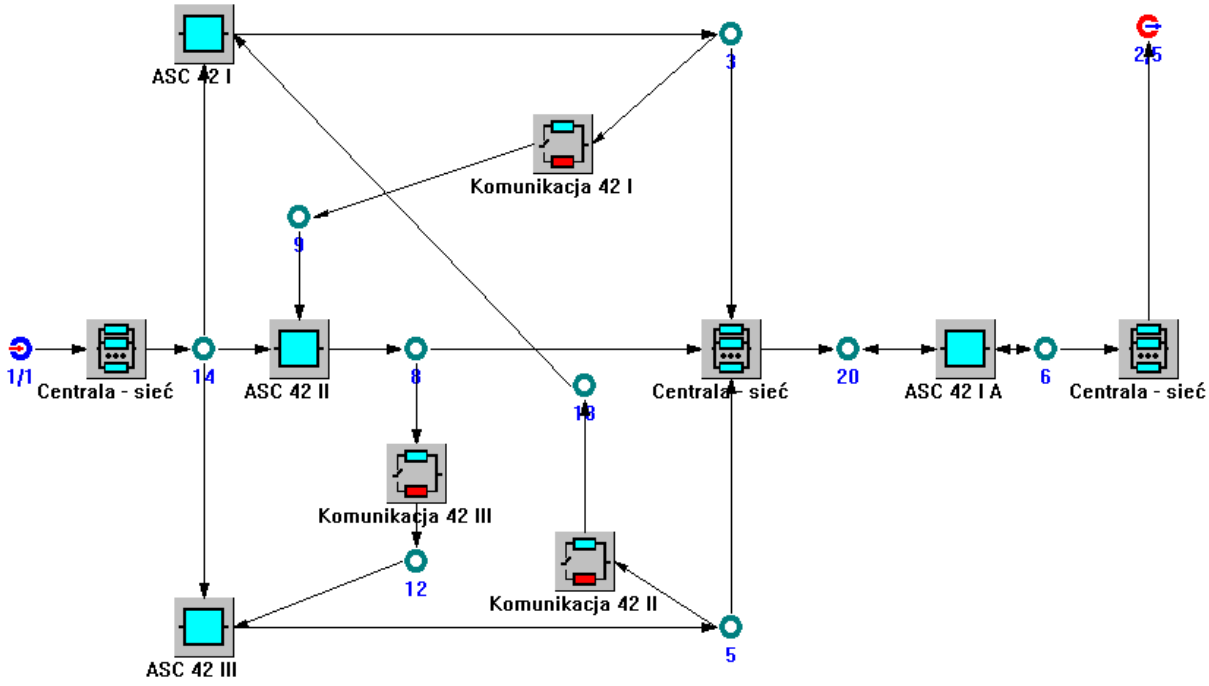

Fig. 5. Block scheme of an area road traffic controlling system. System II

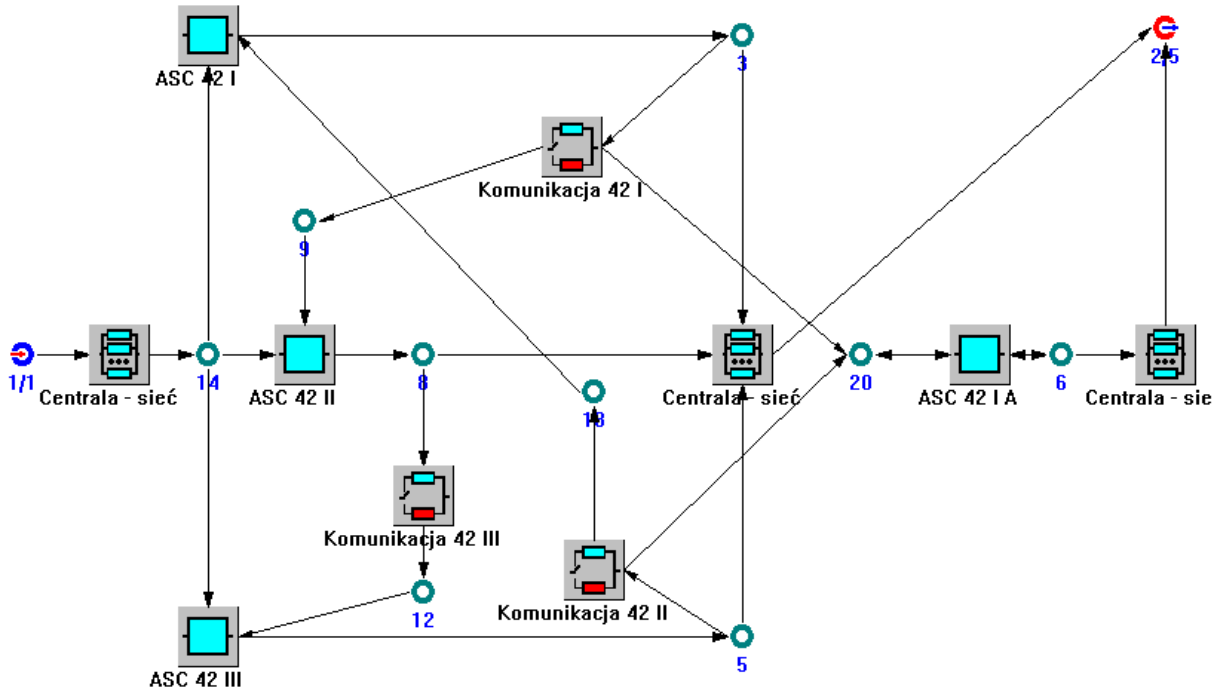

Fig. 6. Block scheme of an area road traffic controlling system.. System III

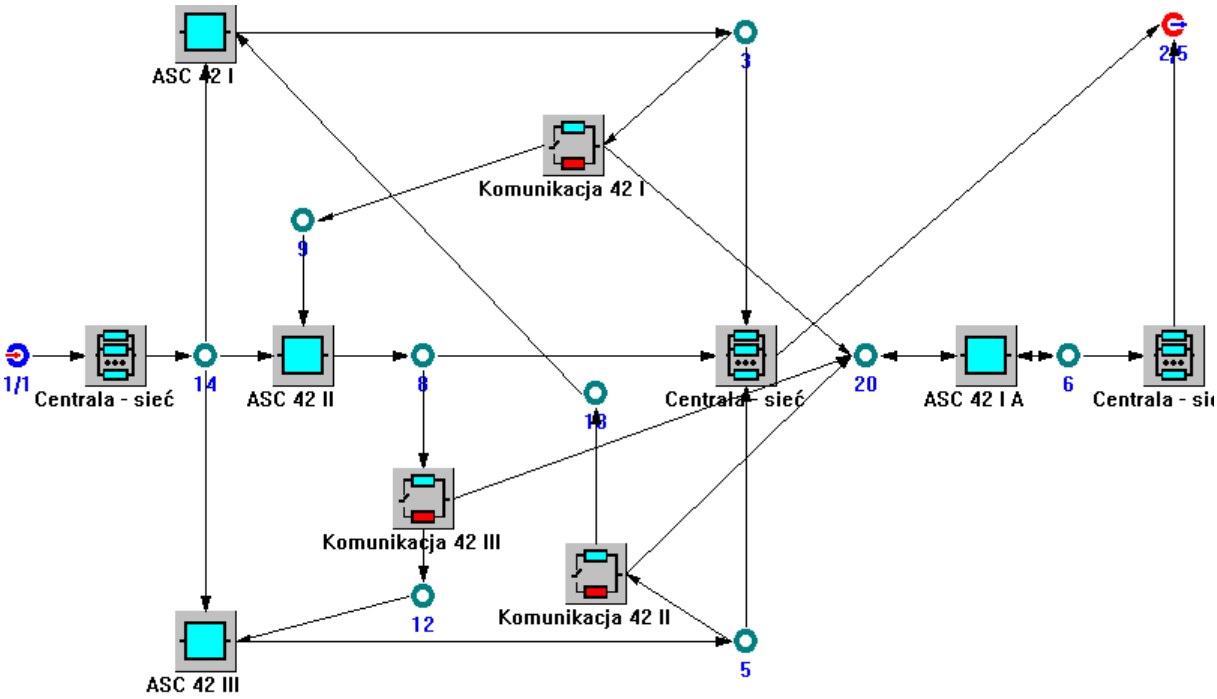

Fig. 7. Block scheme of an area road traffic controlling system. System IV

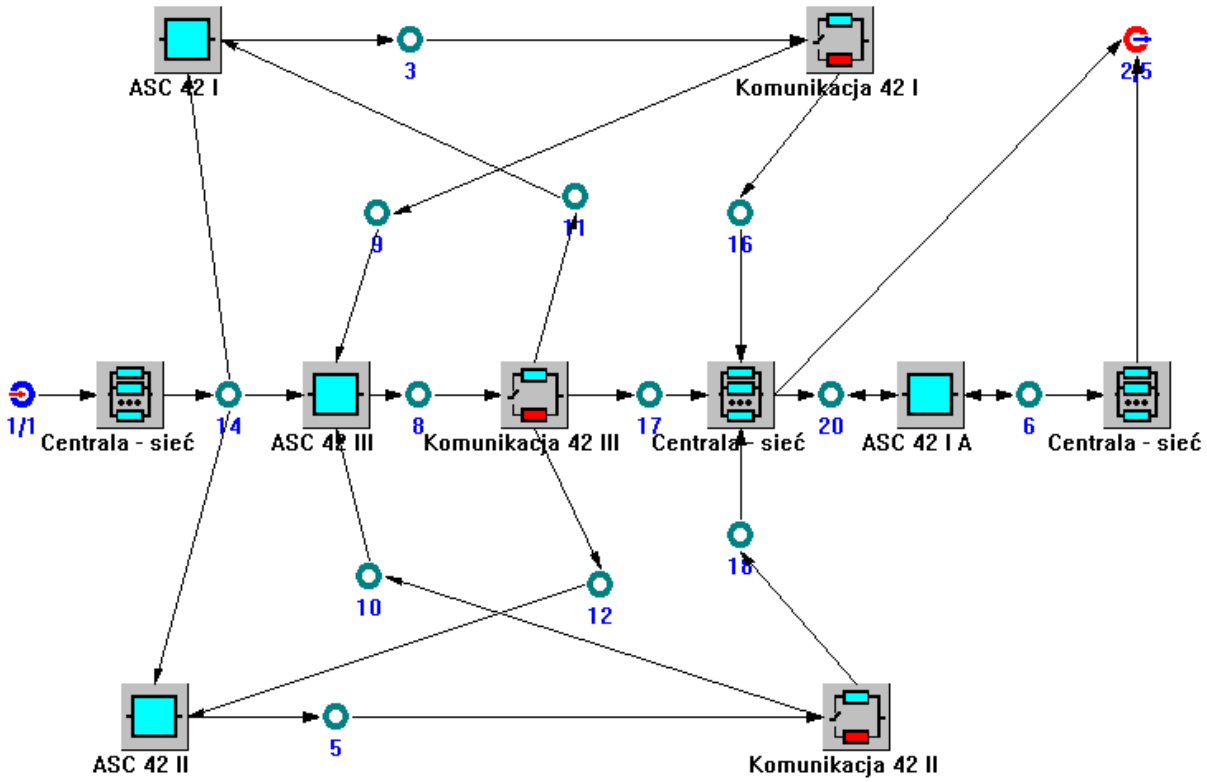

Fig. 8. Block scheme of an area road traffic controlling system. System V

At the Fig.4 we have to do with situation where at area I the controllers were joined into loop.

From the central unit there are transmitted data to every controller in first area, every one of controllers has communication with central unit. Output signal is transmitted directly to central unit or indirectly through area II, however by means of the same communication way. Fig. 5, in contradistinction to previously described situation, the output from the area I to the central unit is performed through the area II. At Fig. 6 we consider situation in which connection between area I and II is performed through two inner connections of an area I. Outside output net connects the area I exclusively with the central unit. Fig. 7 shows situation, when every controller of the first area communicates with the area II through inner net. At Fig. 8 there is presented situation, in which controllers of the area I have direct communication between themselves. Signal to the central unit goes from the area I through the outside net and through second area. In table 5. there were placed comparative results for configurations described above.

Table 5: Results of tests

Układ	MTBCF (h)	FPMH	MTTR (min)	Reliability	Availability
Controller	10111.2	98.9	228.716	0.905833	0.999623
System I	**11963.8**	**83.5852**	**800.305**	**0.960062**	**0.998886**
System II	5423.6	184.379	627.167	0.852395	0.998076
System III	9815.97	101.875	951.584	0.96	0.998387
System IV	9917.68	100.83	1077.96	0.960307	0.998192
System V	8086.89	123.657	1120.21	0.925012	0.997697

From the above table there appears that the best configuration of an area road traffic controlling system is the one shown at Fig 4 (system I). There results from analyses that increasing number of communication connections does not always influence increase of reliability. It can be observed on an example shown in Fig. 6 (system III) and Fig. 7 (system IV). Increasing the number of connections from two to three only insignificantly improves obtained results. In spite of expectations connecting in area I one controller to each other (see Fig. 8) did not improve results – on the contrary, it caused worsening of results. Comparing Fig 4 and Fig 5 one can observe, that there is indispensable direct communication between area I and central unit. It influences significantly for improving the results of obtained reliability indicators of the considered system. On a base of performed analyses there appears that system I is the best solution. Exchange of information between controllers is performed on a base of a loop. Every controller sends information outside area I through outside communication (1 from 3). Moreover there exists double exchange of data from the area I to the central unit. It goes directly through outside net and area II.

7. Summary

In this article the results of tests performed for the controller of road traffic signalling and area road traffic controlling system are presented. For the controller of the road traffic signalling two analyses using FMEA and RBD methods were performed.

From the FMEA analysis it results that the most neuralgic element of the controller is the module MS41. Its failure can cause most critical consequences. For improving the functional safety of this controller the frequency of this element failures should be decreased and / or the redundancy of this module could be considered. The most dangerous potential situation, the case of appearance of two green lights on crossing ways of traffic, never took place thanks to designing the configuration of three elements described above, and it would be associated with total failure of these elements in an unheard-of mode. This protection is performed both by hardware and software.

From the RBD analysis the results are as follows. The controller reliability point value R is equal to 0.906, while the number of failures per million of hours (FMPH) is equal 98.9; which is relatively a good result for this kind of systems.

From the RBD analysis for the area model of road traffic controlling system the conclusions have been reached that very important is to ensure good communication between controllers working in one area (inside area network) and between controllers and central controlling unit. Connections between areas are not so critical but can improve reliability of the system. The RBD analysis for communication network can be very useful in practice. It can help to select the best solution assuring required safety level.

In the analyses carried out the reliability indicators of the analyzed object and systems are high. However, there should be remembered that these results were obtained for the hardware part only. In these analyses there were not considered causes of failures associated with software for the controllers and the net. Worsening of obtained results could have connection with potential faults in the software.

7. References

[1] PN-IEC 812.: Analysis techniques for system reliability – Procedure for failure mode and effect analysis(FMEA), 1994.

[2] PN-IEC 300-3-1.: Dependability management – Part 3: Application guide – Section 1: Analysis techniques for dependability: Guide on methodology, 1994.

[3] IEC 61508.: Functional safety of electrical/electronic/programmable electronic safety related systems, 1997.

[4] LEZION R.: Care reliability planning and simulation tools, BQR Reliability Engineering Ltd, 2000.

[5] BQR CARE.: Computer aided reliability engineering – Reliability block diagram, BQR Reliability Engineering Ltd, 2002.

[6] KOSCIELNY J.M.: Diagnosis of automated industrial processes (in Polish), Warszawa: EXIT 2001.