PANČO RISTOV, Ph.D.
E-mail: panco.ristov@pfst.hr
University of Split, Faculty of Maritime Studies
Zrinsko-Frankopanska 38, 21000 Split, Croatia
PAVAO KOMADINA, Ph.D.
E-mail: komadina@pfri.hr
VINKO TOMAS, Ph.D.
E-mail: tomas@pfri.hr
University of Rijeka, Faculty of Maritime Studies
Studentska 2, 51000 Rijeka, Croatia

Information and Communication Technology
Review
Accepted: Oct. 2, 2012
Approved: May 23, 2013

MODEL FOR RELIABILITY, AVAILABILITY AND SAFETY OF THE CONTROL CENTRES OF VESSEL TRAFFIC MANAGEMENT AND INFORMATION SYSTEMS

ABSTRACT

The quality of Vessel Traffic Management and Information Systems depends on the quality of all subsystems, in particular the quality of control centres. The most commonly used quantitative indicators of the control centres' quality are: reliability, availability, safety, and system failure. Therefore, a block diagram of reliability and the model for reliability / availability (Markov model) have been created in this paper and a detailed analysis and calculation of the quantitative indicators of critical components (servers) of the control centre have been performed. The quality functioning of the control centres will enable gathering, processing, storing and dissemination of timely, safe, and reliable data and information to the services in charge of monitoring and management of maritime traffic.

KEY WORDS

control centre, model, reliability, availability, safety, server, failure rate, repair rate

1. INTRODUCTION

Information technology is experiencing a rapid development so that the size and complexity of computer systems have increased considerably, and the trend will surely continue in the future. This has resulted in using computer systems in all spheres of society, including the maritime systems on modern ships, as well as in supervising, monitoring, managing and organizing the maritime traffic.

In order to improve the safety and efficiency of maritime traffic and to protect the sea and the marine environment, it is inevitable to use modern information and communication technologies for gathering, processing, distributing and presenting the relevant data and information to the participants in maritime transport.

The full application of computer equipment is essential in the VTS (Vessel Traffic System) systems, in the processes of gathering, processing, storing and sharing data and information among the participants in maritime transport. The main function of the VTS system is to increase maritime safety and the protection of the sea and the marine environment.

Following the positive sides of the VTS systems and the development of other maritime systems, scientific and expert considerations have been given to the integration of maritime systems into a single system for monitoring and management of maritime traffic (Vessel Traffic Management and Information System - VTMIS). Integration of maritime systems enhances the efficient, safe and reliable exchange of data and information at the national, regional and international levels, the effective management of maritime traffic and the preservation of the sea and the marine environment. The integration of maritime systems is in accordance with IMO (The International Maritime Organization) Resolutions, SOLAS (Safety of Life at Sea) Convention and IALA (International Association of Lighthouse Authorities) Recommendations [1]. Direct benefits of the integration of maritime systems include increased maritime safety and, consequently, reduced costs due to fewer collisions, groundings, accidents and incidents.

The manufacturers of information and communication systems usually present the quality of their products by highlighting the reliability, availability and

safety of the computer resources. The reliability and availability of computer systems can no longer be determined by the reliability of the hardware alone. One must also take into account the reliability of the software (there are practically no systems without built-in software support), but also the reliability of humans, depending on the nature and the purpose of the system, especially when performing tasks where a human is a part of the system or is activated in the event of failure of hardware and software modules.

Reliability of a computer system refers to the ability of an operating system to work without delay or to prevent the downgrade of the characteristics over a given period of time. The mean time between failures is usually given as the reliability indicator. Availability of a computer system refers to the system's ability to provide defined services at any point in time, and the mean time for repair is often given as an availability indicator.

The overall availability of a VTMIS system is an integral part of the availability of all its subsystems. The better the quality of computing resources, the better its subsystem or the control centre. Based on the technical literature, manufacturers' manuals and the recommendations of the IALA, the overall failure rate of computer equipment and VTMIS system as a whole may increase from 8.7 hours to 3 days per year, i.e. the availability ranges from 99.0% to 99.9% [2]. If it is assumed that the failure time amounts to 48 hours a year, the obtained availability is 99.4%. Low levels of reliability and availability result in endangered safety of the ship, dissatisfaction of the master and other participants in maritime transport due to undelivered goods or services and higher maintenance costs, etc. Apparently, the availability of 99.4% is not acceptable for VTMIS systems. Values amounting to 99.999%, where the system failure time is around 5 minutes per year, are the values to be strived for in the exploitation of the systems.

2. CONTROL CENTRES

A common structure of a VTMIS system consists of VTMIS functions and VTMIS subsystems. VTMIS functions are grouped into operational and complementary roles, while VTMIS subsystems include sensors, communication and computer networks, operator consoles, servers, databases, video walls, system software and Web services [3].

The VTMIS division is based on a broad range of subsystems. The subsystems are divided into levels (national, regional, local), according to their function within the overall function of the VTMIS. Each subsystem consists of hardware, software and communication components and VTS personnel. Control centres are the heart of the entire VTMIS: they include the national control centre, sector control centres and local control centres.

Servers are the main computer components of all control centres. Their number depends on the control centre level, i.e. on the amount of data, information and services provided. For a reliable and safe operation of the servers some form of redundancy is used. Depending on their application and configuration, the most common control centre servers are:

- *VTS (Vessel Track Handler) server* - generates a systematic trace of an object which is displayed on the console screen and recorded in the server for logging and repetition. The inputs in the VTS server come from one or more radars (radar trace of an object) in the same VTS area, AIS (Automatic Identification System) system (AIS track facility) and other external sources such as underwater systems and GSM/GPERS systems. VTS server generates system trace object that is displayed over a computer network on the console screen (actual picture of maritime traffic) and writes to SZP server (the history of the building).
- *Server database (SBP server/SQL server)* - where a distributed relational database is implemented. SQL (Structured Query Language) servers are based on a client/server concept with highly standardized application interface standards defined by SQL standards and standards on communication with databases. The SQL server has the exclusive right to manipulate the database physically. The SQL server has two basic components: a backend (provides functions for defining data, data integrity and protection, data manipulation, data management, etc.) and frontend (application interface that receives requests for manipulating data, and sends a response to the given requirements).
- *The logging and repetition server (SZP server)* – used for logging the data on objects which are used for analysis, evaluation and learning, i.e. training of the operators. Logging facilities involve recording vessels' positions, courses and speeds at regular intervals. In addition, every event that changes the data is logged into the data table of the object. For the purpose of VTS personnel training, the rollback is displayed on the corresponding operator consoles when planning a performance to be carried out in similar situations.
- *Warning Server (SU server)* – used to record the operator's and technical alerts generated by the diagnostic programs that are built into all process modules of the control centres, radars, AIS National server and VPN (Virtual Private Network) network.
- *Firewall (network barriers)* - involves the use of a proxy server to allow communication with the Internet. Administration of the firewall enables certain inputs (ports), or partially or totally disables some of them. A part of the protection is performed by

the configuration of the router, whereas another part is ensured by assigning appropriate rights to certain contents of the servers. The proxy server is required in all control centres.

- *Web (World Wide Web) server* - is a computer program or a computer that receives HTTP (HyperText Transfer Protocol) requests from various clients, such as user agents or Web browsers, and responds to them by sending HTTP replies along with the data that are commonly HTML documents and associated objects (images, etc.). Web technology as the basis for browsing documents and communication is not dependent on the platform on which it is used, and because of its flexibility, it ensures the interconnection of different systems.
- *Streaming server* - is the name of the infrastructure that broadcasts streaming audio and video materials (also known as web radio and web TV). It implies simultaneous reception and playback of audio and video data over the computer network. It provides live data (signals from the camera or radio) or the data containing recorded maritime events which are delivered to the user upon request. This means that the server features a software application for recording voyage data (Voyage Data Recorder), which continuously records the selected data and output data concerning the ship or any process at sea as designated by the head of the centre.

The servers that are essential for providing services to maritime subjects include VTS server, SBP server, SZP server and SU server; they can be considered as critical components of the control centres.

3. BASE MODEL FOR THE CONTROL CENTRE

3.1. Methods for determining the reliability and availability

Well-known methods for determining the reliability include reliability block diagrams, fault tree method, method of analyzing the types of failures and effects, the Markov method, etc. Here are the methods used in this paper:

- Reliability block diagram (RDB) is a graphical tool for creating and calculating the reliability of complex systems. Using RDB we can create complex systems (serial and parallel structures) and, using certain methods, we are able to determine the reliability, failure rate, availability, and mean time between failures of such systems.
- Markov method is an analytical method for determining the reliability of systems. Markov method consists of designing a state graph, determining the coefficients of transitional probabilities between the states and setting up and solving the systems of differential equations. This paper uses Markov processes which are functions of two random variables: the state of the system and the period of observation.

There are several recommendations that will be used during the development of a model for the control centre:

- subsystem boundaries with the environment must be selected so that its model includes only the variables that are relevant to the analysis,
- model should neither be too complex nor detailed. It should contain only relevant subsystem variables,
- on the other hand, the model must not excessively simplify the reality,
- when developing the model, it is recommended to use some of the verified methods for developing the algorithms and software packages, and
- a complete, logical and quantitative verification of the model is required.

The modules of moderate reliability are used for the calculation and analysis of quality indicators: microprocessor, working memory, disc drive of 500 GB capacity, SCSI controller, RAID controller, I/O controller, 80 GB streamer and power supply. The calculation and analysis will use the following failure rates: VTS server ($235.23\ 10^{-6}h^{-1}$), SBP server ($235.38\ 10^{-6}h^{-1}$), LAN network ($1.25\ 10^{-6}h^{-1}$), SZP server ($239.38\ 10^{-6}h^{-1}$), SU server ($242.75\ 10^{-6}h^{-1}$) and the coverage factor C=0.98 [4, 5, 6, 7]. The Mean Time to Repair (MTTR) is the average period of time spent on the actual repair of a software or hardware module.

3.2 RDB of the control centre

The control centres at the same levels are completely identical regarding their hardware, software and personnel characteristics, so that this paper will deal with the quality indicators of only one centre. The configuration of the VPN network allows any control centre at the same level to take over the monitoring of maritime traffic in any VTS sector, i.e. each control centre at the same level is redundant to one another, thus increasing the overall availability of VTMIS.

The RDB of the control centre includes the critical components (marked by *) and the components that are required to provide the defined functions of the control centre, as shown in *Figure 1*.

RDB shows the active and backup VTS servers, four identical operator consoles (OK_1, OK_2, OK_3 and OK_4), active and backup SBP server, SZP server, SU server, LAN network, communication subsystem (KS), three radars (R3, R2 and R1) and AIS national server.

In the control centres, the VTS servers, SBP servers and LAN networks have redundant systems with hot reserve, i.e. the backup server operates as a “mirror” of the primary server. Both servers handle the same

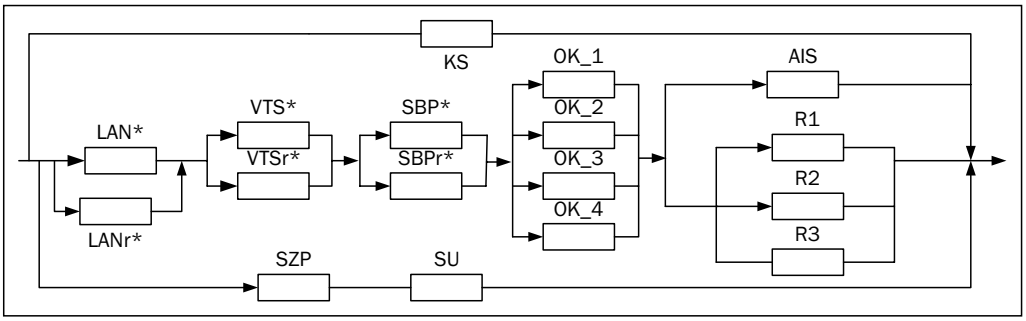


Figure 1 - RDB of the control centre

data, so that there is no loss of data or information in case of failure of the primary and switching to the secondary server. In addition, each module has a built-in ability to detect errors (diagnostic programs); therefore, adding just one module can be sufficient to achieve the desired reliability and availability.

From the configuration and functional aspects, the operator consoles are exactly the same. Normal monitoring of the safety of maritime traffic requires two consoles, i.e. one operator and one supervisory console. Hence, when analytically considering the availability, reliability and safety of the control centres, a 100% reliable console is assumed.

On the basis of professional and practical experience, one of the main problems of a computer system is the power supply and power failures which make 26% of the overall failures. Modern power supply system uses uninterrupted power supply (UPS) which supplies the system until diesel generator starts. Therefore, when analytically considering the quality indicators of the control centres, a 100% reliable supply is assumed.

3.3 Markov model for reliability and availability

Markov model for the reliability of critical components containing six states is shown in *Figure 2* (without intermittent arcs). State 1 shows a case where all the servers and LAN networks function properly. This state is a perfect state in which the system starts working and is called the "fully operational state". In State 2 a standby VTS server is activated, a failure is detected on the primary VTS server and the repairs are under way. In state 3 the standby SBP server is activated, a failure is detected on the primary SBP server and the repair is under way. State 4 shows a situation where the backup LAN is activated, a failure on the primary LAN has been detected and the network is being repaired. The state of safe failure (SO) implies a safe failure of a server, i.e. a problem has been detected and a transition to that state is performed in accordance with the procedure for shutting down the server as recommended by the equipment manufacturer. The state of unsafe failure (NO) is a system failure without implementing standard procedures for shutting down the server, i.e. the problem that initiated the unsafe failure has not been detected. Such events may result in serious problems associated with the open files (loss of data); they may stop the performance of systemic functions or cause unexpected hardware and/or software problems.

Let us analyze the transitions that may occur between servers and LAN networks under certain conditions:

1. Failure rates (λ) and repair rates (μ) of a module are constant and not dependent on time. The failure rate of VTS and SBP servers represents an overall rate of hardware failure (λ_h) and the software error rate (λ_s), i.e. $\lambda = \lambda_h + \lambda_s$.
2. All failures are mutually independent, i.e. any failure is independent of other failures.
3. The probability of occurrence of two or more failures in the time interval Δt is negligible.
4. The system starts in a completely proper operating condition where all system modules operate properly.

Transitions from state to state are shown in *Figure 2*; the transition from State 1 to State 2 will occur when the self-checking devices of the primary VTS server detect a failure and initiate an automatic transfer of

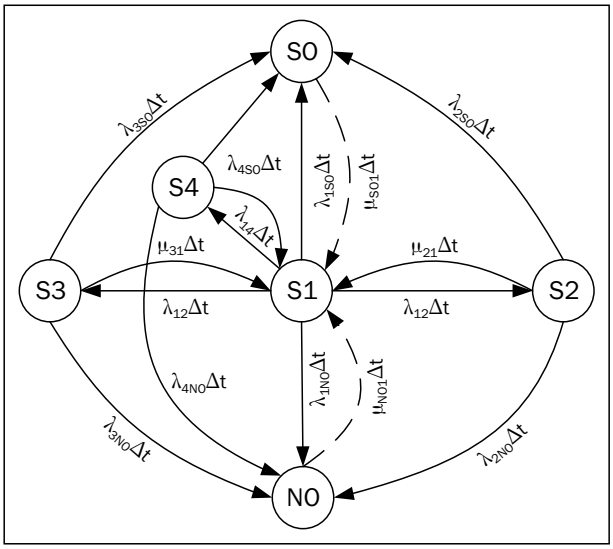


Figure 2 - Markov model for the reliability and availability of critical components of the control centre

functions to the VTS backup server. The transition from State 1 to State SO will take place when the self-checking devices detect a failure of any server or LAN network; the diagnostic program generates a technical failure alert and the operator or technical personnel undertake defined procedures for safe shutdown of the server.

The system is safe but not operational. The transition from State 1 to State NO occurs when a malfunction is not detected, and it is not known which of the servers or LAN is defective, i.e. the server simply "freezes". The transition from State S2 to State SO will take place if the repair of the primary VTS server is not completed, and the self-checking devices of the backup VTS server detect a failure so that the diagnostic program generates an alert and the operator or technical personnel undertake defined procedures for a safe shutdown of the system. The transition from State 2 to NO will occur if the self-checking diagnostic programs do not detect a failure in the backup VTS server and the server "freezes".

The analysis of the transition from State 1 to State 3 (SBP server) and the transition from State 3 to State SO or to State NO is completely analogous to the analysis of the VTS server, so there is no need to repeat it. Likewise, the analysis of the transition from State 1 to State 4 (LAN) and the transition from State 4 to State SO or to State NO is completely analogous to the analysis of the VTS server and SBP server so that there is no need to repeat it.

Equations for the Markov reliability model can be written in the matrix form:

$$P_{RSS}(t+\Delta t) = T_{RSS} \cdot P_{RSS}(t),$$

where each element of $P_{RSS}(t)$ represents the probability that the redundant servers with hot reserve and the LAN network are in a particular state at time t. Each element of the $P_{RSS}(t+\Delta t)$ represents the probability that the system is in an appropriate state at time $t+\Delta t$, where TRSS is the state transition matrix. Accordingly, it can be written as follows:

$$P_{RSS}(t+\Delta t) = \begin{bmatrix} P_1(t+\Delta t) \\ P_2(t+\Delta t) \\ P_3(t+\Delta t) \\ P_{SO}(t+\Delta t) \\ P_{NO}(t+\Delta t) \end{bmatrix}, \quad P_{RSS}(t) = \begin{bmatrix} P_1(t) \\ P_2(t) \\ P_3(t) \\ P_{SO}(t) \\ P_{NO}(t) \end{bmatrix} \quad (1)$$

$$T_{RSS} = \begin{bmatrix} -(\lambda_{12}+\lambda_{13}+\lambda_{1SO}+\lambda_{1NO})\Delta t & \mu_{21}\Delta t & \mu_{31}\Delta t & 0 & 0 \\ \lambda_{12}\Delta t & -(\lambda_{2SO}+\lambda_{2NO}+\mu_{21}) & 0 & 0 & 0 \\ \lambda_{13}\Delta t & 0 & (\lambda_{3SO}+\lambda_{3NO}+\mu_{31})\Delta t & 0 & 0 \\ \lambda_{1SO}\Delta t & \lambda_{2SO}\Delta t & \lambda_{3SO}\Delta t & 1 & 0 \\ \lambda_{1NO}\Delta t & \lambda_{2NO}\Delta t & \lambda_{3NO}\Delta t & 0 & 1 \end{bmatrix}$$

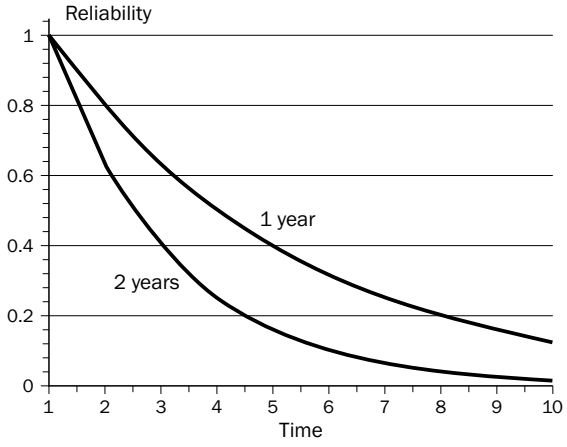
By replacing the corresponding values for the failure and repair rates and by solving the matrix equation of the Markov model, values for $P(\Delta t)$ can be obtained through multiplying the vector of initial values $P(0)$ by the matrix transition T_{RSS}, and values for $P(2\Delta t)$ through multiplying $P(\Delta t)$ by the transition matrix T_{RSS}. The general solution to the Markov model equation is given as

$$P_{RSS}(n \cdot \Delta t) = T^n P(0)$$

The reliability of redundant servers with hot reserve, LAN, and built-in diagnostic program at time t implies the probability that the computer equipment functions properly from starting the server and the LAN to time t. According to the Markov model for the reliability of the observed equipment, it is probable that the system is in State 4, State 3, State 2 and State 1; these states being the only states where the observed components work properly. This means that the reliability can be expressed as

$$R_{RNS}(t) = P_1(t) + P_2(t) + P_3(t) + P_4(t)$$

Figure 3 shows the reliability of servers and LAN network of the control centre as a function of the value of the servers' failure rate, the servers' repair rate, coverage factor and time. The presented reliability is the reliability of the system after 8,766 hours and 17,532 hours without changing state from S0 to S1 and N0 to S1. The given results are gained without maintenance of the system.



Label	Time (h)	
	1 year	2 years
1	0	0
2	974	1,948
3	1,948	3,896
4	2,922	5,844
5	3,896	7,792
6	4,870	9,740
7	5,844	11,688
8	6,818	13,636
9	7,792	15,584
10	8,766	17,532

Figure 3 – Reliability of the servers and the LAN network of the control centre

Graphic presentation of the Markov model for the availability of critical components is made in a completely analogous way. This presentation is shown in *Figure 2* (with intermittent arcs). The states of SO and NO are no more final; after restarting the system or repairing the hardware and/or software modules, the system returns to State S1, i.e. all the servers and LAN networks are fully operational.

The availability of all major computer components of the control centre is:

$$A_{RNS}(t) = P_1(t) + P_2(t) + P_3(t) + P_4(t)$$

The equations for $P_1(t)$, $P_2(t)$, $P_3(t)$ and $P_4(t)$ can be written in matrix form:

$$P_{RSS}(t + \Delta t) = T_{RSS} P_{RSS}(t)$$

where

$$P_{RSS}(t + \Delta t) = \begin{bmatrix} P_1(t) \\ P_2(t) \\ P_3(t) \\ P_4(t) \\ P_{SO}(t) \\ P_{NO}(t) \end{bmatrix}, \quad P_{RSS}(t + \Delta t) = \begin{bmatrix} P_1(t + \Delta t) \\ P_2(t + \Delta t) \\ P_3(t + \Delta t) \\ P_4(t + \Delta t) \\ P_{SO}(t + \Delta t) \\ P_{NO}(t + \Delta t) \end{bmatrix} \quad (2)$$

$$T_{RSS} = \begin{bmatrix} [-(\lambda_{12}+\lambda_{13}+\lambda_{14})+(\mu_{21}+\mu_{31}+\mu_{41}+\mu_{SO1}+\mu_{NO1})]\Delta t & \mu_{21}\Delta t & \mu_{31}\Delta t & \mu_{41}\Delta t & \mu_{SO1}\Delta t & \mu_{NO1}\Delta t \\ \lambda_{12}\Delta t & -(\lambda_{2SO}+\lambda_{2NO}+\mu_{21})\Delta t & 0 & 0 & 0 & 0 \\ \lambda_{13}\Delta t & 0 & -(\lambda_{3SO}+\lambda_{3NO}+\mu_{31})\Delta t & 0 & 0 & 0 \\ \lambda_{14}\Delta t & 0 & 0 & -(\lambda_{4SO}+\lambda_{4NO}+\mu_{41})\Delta t & 0 & 0 \\ \lambda_{1SO}\Delta t & \lambda_{2SO}\Delta t & \lambda_{3SO}\Delta t & \lambda_{4SO}\Delta t & -\mu_{SO1}\Delta t & 0 \\ \lambda_{1NO}\Delta t & \lambda_{2NO}\Delta t & \lambda_{3NO}\Delta t & \lambda_{4NO}\Delta t & 0 & -\mu_{NO1}\Delta t \end{bmatrix}$$

The initial conditions at $t = 0$ are:

$$P_1(t) = 1,\ P_2(t) = 0,\ P_3(t) = 0,\ P_4(t) = 0,$$
$$P_{SO}(t) = 0,\ P_{NO}(t) = 0.$$

Table 1 shows the availability of the system, the system in the period of failure and the operation of critical components of the control centre as a function of values of failure rates, repair rates, coverage factor and time. The presented availability is the availability of the observed equipment of the control centre at several characteristic repair rates after 8,766 hours of operation.

The system's safety is the probability that the critical components will either perform their functions or terminate their functions in a safe manner. In accordance with the Markov model in *Figure 2* the observed equipment will be safe as long as it is in one of the five states: State 1, State 2, State 3, State 4 or in State SO. Hence, the safety of the observed equipment of the control centre can be expressed as

$$S_{RSN}(t) = P_1(t) + P_2(t) + P_3(t) + P_4(t) + P_{SO}(t)$$

Sometimes the VTS server gets overloaded, e.g. due to activating more than two radars, microprocessor overheating or faulty operator procedures. In such situations, the active and standby servers VTS simply "freeze" so it is necessary to reboot the server or the entire VTS system. According to our own experience (use of C3I systems), specialized literature and other sources provided by the equipment manufacturers and the analysis of error codes of application servers, VTS failures are, in most cases, the result of software errors, while sometimes they are due to microprocessor failures (overheating of microprocessors). In such situations, the failure rate of the VTS server rises up to 40%. The result of the increased failure rate is the reduced reliability and availability of the equipment, which eventually leads to inefficient monitoring of the maritime traffic. If VTS server failures are the consequence of transient or intermittent faults, it is just necessary to restart the VTS server, while the lasting failures require rebooting of the entire system. An analysis using the Markov model for availability in *Figure 2* was made to demonstrate the impact of the VTS server on the availability of other computer equipment of the control centre. The analysis was based on the

Table 1 – Available servers and redundant LAN network of the control centre

	$\mu = 10$	$\mu = 4$	$\mu = 2$	$\mu = 1$	$\mu = 0.2$	$\mu = 0.125$
Availability	0.999908	0.999769	0.999538	0.999077	0.995419	0.992711
The system in failure (h)	0.81	2.03	4.05	8.09	40.14	63.84
The system in operation (h)	8,765.19	8,763.97	8,761.95	8,757.91	8,725.86	8,702.16

Table 2 - Safety of the servers and redundant LAN network for different repair rates

	$\mu = 10$	$\mu = 4$	$\mu = 2$	$\mu = 1$	$\mu = 0.2$	$\mu = 0.125$
Safety	0.999998177	0.999995767	0.999990949	0.999981567	0.999906	0.994495

Table 3 - Quality indications of the redundant components of the control centre as a result of the VTS server overload

	$\mu = 10$	$\mu = 4$	$\mu = 2$	$\mu = 1$	$\mu = 0.2$	$\mu = 0.125$
Availability	0.9998880	0.9988800	0.9994390	0.9988800	0.9944440	0.9911650
Safety	0.9999982	0.9999944	0.9999891	0.9999779	0.9998871	0.9998213
The system in failure (h)	0.98	2.46	4.92	48.70	48.70	77.45
The system in operation (h)	8,765.02	8,763.54	8,761.08	8,756.18	8,717.30	8,688.55

Table 4 - Quality indicators for the observed equipment when the repair is done by one person

	Mean Time To Repair			
The quality indic.	μ = 10	μ = 4	μ = 1	μ = 0.2
Availability	0.999857	0.999644	0.998578	0.992954
Safety	0.99999716	0.99995312	0.99997111	0.99781165
The system in failure (h)	1.25	3.12	12.48	61.77
The system in operation (h)	8,764.75	8,762.88	8,753.52	8,704.23

Table 5 - Quality indicators for the observed equipment when the repair is done by two persons

	Mean Time To Repair			
The quality indic.	μ = 20	μ = 8	μ = 2	μ = 0.4
Availability	0.999929	0.999822	0.999288	0.996456
Safety	0.9999981	0.9999962	0.9999288	0.9999288
The system in failure (h)	0.63	1.56	6.24	31.07
The system in operation (h)	8,765.37	8,764.54	8,759.76	8,734.93

VTS server failure rate of 329.32 10^{-6} and the same repair rates as in the previous analysis. The quality indicators for the observed equipment are shown in *Table 3*.

It can be taken into consideration that it is possible that two persons may participate in repairing the modules, i.e. that they may try to eliminate the failure together. Ideally, the mean time to repairs will be reduced by half, i.e. μ will be doubled: $\mu' = 2\mu$. In another case, μ will increase by at least 1.5 of its normal value. The calculation of the quality indicators of the control centre is done for both situations: when the repair is carried out by one and by two persons. The calculation results are shown in Tables 4 and 5.

4. ANALYSIS OF THE RESULTS

When studying the tables of the quality indicators for the observed equipment of the control centre, the following can be found: the availability, the safety, and the system in failure *increase*, whereas the system in operation *decreases* if the mean time to repair - MTTR is increased, i.e. if the repair rate is reduced. The quality indicators of the control centre were observed after 8,766 hours of operation. The best values referring to the availability (0.999908), the safety (0.999998177) and the system in failure (0.81 h) are obtained for the MTTR of 10 min (μ = 10). The MTTR of 10 min can be achieved only if the repair is performed by VTMIS technical staff with the telephone or Internet support provided by an authorized service in the Republic of Croatia; this refers to occasional and/or transient failures only. A satisfactory availability that is in accordance with IALA recommendations is obtained when the repair rate ranges from μ = 4 (MTTR = 15 min) to μ = 1 (MTTR = 1 hour). This range of MTTR value can be achieved only if the repair is performed by VTMIS technical staff with the telephone or Internet support provided by an authorized service; this refers to occasional, transient, and permanent failures which are dealt with appropriate hardware and software tools. If the failure cannot be repaired by the VTMIS technical personnel, the intervention of an authorized service provider is required. MTTR ranges from 5 h to 8 h, depending on the type of failure. In this case the equipment availability drops below 99.27%, which means that the system is in failure 63.84 hours or more. The calculation is performed using the failure/error coverage factor of 0.98.

It is interesting to compare the indicators of the VTS operation quality when the server is under load. *Table 3* shows that the VTS server strongly affects the availability of other computer equipment. We analyzed the case when the failure rate (λv) of the VTS server was increased by four times the normal overload. Comparing the data from Tables 1 and 3 we can see that all indicators of the loaded server are lower than indicators of quality when the VTS server is under normal load. Similar information would be obtained if we analyzed a loaded SBP server because it continuously communicates with the VTS server and stores the data of vessels in real time.

When observing Tables 4 and 5 it can be noticed that the time of the system in failure is by half shorter when the repair of a faulty hardware and/or software is carried out by two persons.

5. DETERMINING CRITICAL COMPONENTS AND MEASURES FOR IMPROVING THE AVAILABILITY OF CONTROL CENTRES

When implementing the defined functions of a control centre it is essential to ensure that a failure of any system module does not lead to the unavail-

ability of the services provided by the control centre to the participants of maritime traffic. During the analysis of the system quality indicators, critical modules/devices were identified and special attention was paid to such components. It can be easily concluded that the peripheral computer equipment of the control centre (terminals on consoles, video wall, keyboards, mouse, printer, etc.) have minimal impact on the reliability and availability of the system, because failure of a peripheral component reduces only the functionality of subsystems but does not cause their failure. In addition, sufficient quantity of spare peripheral units can be kept in reserve and the faulty ones can be quickly replaced to restore full functionality of a subsystem. On the other hand, critical components in control centres are unquestionably the units where the data are processed, stored and distributed, including servers with disk arrays, such as VTS server, SBP server and LAN network. Specifically, these are server motherboards, i.e. microprocessors and memory as the main modules.

The reliability and availability in the exploitation process of the control centres can be increased by the following measures:

- Organizing exploitation and maintenance on a scientific basis;
- Ensuring skilled technical staff at each control centre;
- Quality power supply (redundant power supply);
- Proper preparation and a continuous improvement of the technical personnel training and their skill, so that the repair rate is two times higher than the failure rate of critical components;
- Redundant ventilation and air conditioning at constant temperature;
- Recording and proper storing of data backups;
- Continuous updating of data in CMMS (Computerized Maintenance Management System);
- Continuous monitoring of log files;
- Upgrade of computers with modules that increase the operation speed and the server stability;
- Detecting the causes of computer system failures, replacement of faulty modules and testing them;
- Installing the antivirus and protection software;
- Detailed elaboration of procedures for repairing major components of the subsystems;
- Ensuring a minimum amount of critical modules of the system;
- Updated technical documentation;
- Continuous forecasting of failures of modules, devices...

These measures ensure high level of reliability, availability and safety of critical components of the subsystems.

6. CONCLUSION

The important features of the VTMIS control centres result from the quality of the hardware and software modules, and the diagnostic programs in each module, i.e. system. Almost all of the hardware and software modules are able to tolerate failures. In order to achieve this, various techniques are applied including, most commonly, the use of hardware, software, time and information redundancy. By combining these techniques the target reliability and availability of the control centres can be achieved. The maintenance strategy, i.e. the quality of the maintenance management information system, has a major influence on the availability of the control centres.

These results can be achieved and maintained only if the maintenance of computing resources is performed by qualified staff at the VTMIS technical department. This means that each control centre must be continually manned by a trained and skilled technician who can at any moment respond to any hardware and/or software problem related to the operation of computing resources. If an authorized service is engaged and if real reaction procedures are met when responding to the alert (MTTR is usually 5 hours or more), then the system quality indicators drop below the values recommended by IALA (the availability of the control centre falls below 98.39%).

The safety of the server corresponds to the level of highly safe systems where values range from 0.999998177 to 0.994495. The high values of computer equipment safety result from the quality of the diagnostic programs (error coverage factor is 0.98). The diagnostic programs allow safe transition to the state of safe failure.

Dr. Sc. **PANČO RISTOV**
E-mail: panco.ristov@pfst.hr
Sveučilište u Splitu, Pomorski fakultet
Zrinsko-Frankopanska 38, 21000 Split, Hrvatska
Dr. Sc. **PAVAO KOMADINA**
E-mail: komadina@pfri.hr
Dr. Sc. **VINKO TOMAS**
E-mail: tomas@pfri.hr
Sveučilište u Rijeci, Pomorski fakultet
Studentska 2, 51000 Rijeka, Hrvatska

SAŽETAK

MODEL POUZDANOSTI, RASPOLOŽIVOSTI I SIGURNOSTI UPRAVLJAČKIH CENTARA SUSTAVA ZA NADZOR I UPRAVLJANJE POMORSKIM PROMETOM

Kvaliteta sustava za nadzor i upravljanje pomorskim prometom ovisi o kvaliteti svih podsustava, posebno o kvaliteti upravljačkih centara. Najčešće korišteni kvantitativni pokazatelji kvalitete upravljačkih centara su: pouzdanost, raspoloživost, sigurnost i sustav u otkazu. Stoga je u radu kreiran blok dijagram pouzdanosti i model pouzdanosti/raspoloživosti (Markovljev model) te je izvršena detaljna analiza i proračun kvantitativnih pokazatelja kritičnih komponenti (serveri) upravljačkog centra. Kvalitetno funkcioniranje upravljačkih centara omogućit će prikupljanje, obradu, spremanje i distribuiranje pravovremenih, sigurnih i pouzdanih podataka i informacija službi nadzora i upravljanja pomorskim prometom.

KLJUČNE RIJEČI

upravljački centar, model, pouzdanost, raspoloživost, sigurnost, server, učestalost otkaza i učestalost popravke.

REFERENCES

[1] European Commission, *"Integrated maritime policy for the EU"*– working document III on maritime surveillance systems, 2008

[2] IALA Recommendation V-128 Edition 3.0, June 2007: *"Operational and Technical Performance Requirements for VTS Equipment"*

[3] **Ristov, P.**: *"Doprinos pouzdanosti i raspoloživosti sustava nadzora i upravljanja pomorskim prometom na Jadranu"*, doctoral dissertation, Faculty of Maritime Studies, University of Rijeka, Croatia, 2012

[4] **Tomas, V.**: *"Model distribuiranog dijagnostičkog sistema brodskih elektroenergetskih postrojenja"*, doctoral dissertation, Faculty of Maritime Studies, University of Rijeka, Croatia, 2003

[5] **Budny, T.**: *"Two various approaches to VTS Zatoka radar system reliability analysis"*, in: RTA # 3-4, 2007, Faculty of navigation, Gdynia, Poland

[6] Intel® Server System, *"Calculated MTBF Estimates"*, Rev 1.0, March 2009.

[7] **Shooman, M. L.**: *Reliability of Computer Systems and Networks: Fault Tolerance*, Analysis, and Design, J. Wiley & Sons, 2002