Reliability and Availability of the Vessel Traffic Management and Information Systems

Pančo Ristov, Pavao Komadina[a], Vinko Tomas[a]

This paper presents an approach to the reliability and availability of Vessel Traffic Management and Information Systems through the analysis of hardware, software and human reliability. The paper analyzes the critical subsystems and modules on the basis of the reliability theory, in order to achieve and ensure the availability of systems, i.e. to increase the safety of maritime traffic and the protection of the sea and marine environment. The paper discusses some of the techniques and mechanisms of hardware and software redundancy, as well as the activities that result in increasing the reliability of man.

KEY WORDS:
~ Reliability
~ Availability
~ Hardware
~ Software
~ Humans
~ Vessel Traffic Management and Information Systems

University of Split, Faculty of Maritime Studies, Zrinsko-Frankopanska 35, HR-21000 Split, Republic of Croatia

e - mail: panco.ristov@pfst.hr

a. University of Rijeka, Faculty of Maritime Studies, Studentska 2, HR-51000 Rijeka, Republic of Croatia

e - mail: komadina@pfri.hr

e - mail: tomas@pfri.hr

1. INTRODUCTION

Computers and all their associated equipment present the technical foundation of modern information and communication systems. Computer technology is experiencing a rapid development geared towards the increasing miniaturization and mobility, increasing processing speed, increasing capacity of the main and secondary memory. This development is also geared towards the use of all media designed for receiving and storing data, greater compatibility, continuous price cuts, etc. The size and complexity of computer systems have dramatically increased in the last decade and the trend is likely to continue in the future. Contemporary examples of complex computer systems can be found in all sectors of economy, in all maritime systems, as well as onboard ships and in supervising, managing and organizing the maritime transport.

In order to improve the safety and efficiency of maritime transport and the protection of the sea and marine environment, it is inevitable to use modern information and communication technologies when collecting, storing, processing, presenting and distributing relevant data and information to the participants in maritime transport. These are the essential characteristics of the system called *Vessel Traffic Management and Information System* - VTMIS.

A common structure of the VTMIS system consists of the VTMIS functions and VTMIS subsystems. VTMIS functions are grouped into operational and complementary roles, while VTMIS subsystems include *sensors* (a marine radar subsystem and the automatic identification subsystem), *communication and computer networks, operator consoles, servers, databases, video*

walls, system software, application software and web services. VTMIS systems are flexible, open and have modular architectures that allow upgrading using standard computer and communication components. In other words, a VTMIS system is a distributed architecture which is: *distributed, decentralized, networking, multi-layered, hierarchical and open.*

A VTMIS system is based on a *client-server architecture,* where the server provides services to a client whose work at the computer is most of the time disconnected from the server. The client-server architecture provides a clear separation between the server and client processes and their autonomy.

The distributed database is a relational database that is not entirely situated on just one server (SQL Server – Structured Query Language). SQL servers are based on a client-server concept with highly standardized application interface, defined by the SQL standards and communication standards with databases known under the abbreviation ODBC (*Open Data Base Connectivity*).

VTMIS systems include hardware and software, and they include the man as an important participant. Hence, it is necessary to analyze the reliability of all these system elements.

Generally speaking, a computer system failure can be caused by *hardware failure, software failure, human error, or by variables from the environment* (fire, power failure, lightning, etc.). Unlike hardware failures that have been extensively analyzed, along with various techniques and mechanisms for their solving, software failures and failures caused by the man followed by an adequate analysis of reliability and availability, did not attract much attention during the research and development of professional systems. However, as the implementation of computer systems grew, the analysis and study of the software and man-induced failures gained impetus, especially when it became evident that the computer system failure occurs mostly due to software failure resulting from the operator's error. In addition, it was considered for a long time that the concept of reliability and failure rate can not apply to software because the latter cannot be physically degraded over time and because of stressful environmental influences. Practice has shown that such considerations were wrong. In many applications, there are serious consequences caused by errors or software failures that result in huge economic losses and/or loss of human life (e.g. sinking of the British destroyer HMS Sheffield by the Argentine Air Force in the Falklands War in 1982; the aircraft crashing into a mountain in Antarctica because of computer errors in determining flight coordinates).

The development of information technology enables the development, implementation and use of increasingly complex computer systems in off-line and on-line applications. All these applications require that the operation of hardware and software should be failure-free, i.e. that computers work without error or fault. In this regard, IT companies have begun to design, deploy and use computer systems that are tolerant to failures. Failure tolerance is one of the techniques to achieve the target reliability of a computer system. Other techniques include: *avoiding failures* (preventing the occurrence or introduction of faults), *troubleshooting* (reducing the number or the magnitude of faults), *and dodging the issue* (predicting / estimating the malfunction and its consequences if it occurs).

The reliability theory shows that fault tolerance can be achieved by using redundancy, which can be: *hardware, software, information and time redundancy*. Hardware and software redundancy are carried out by multiplication of hardware and software at all levels of complexity. Information redundancy is adding bits to data, which enables the detection and/or correction of errors. The codes of parity represent the simplest form of information redundancy. Time redundancy implies the repetition of certain operations during program performance. In addition, the systems tolerant to failures are often designed using reconfiguration strategy. Reconfiguration strategy can be implemented in various ways, including logical or physical removal of faulty elements. The techniques that are used to identify faulty elements and methods that are used to fix the system are quite different and may lead to complex reliability models.

There are two basic strategies of reconfiguration: *degradation* and *replacement with a grain of salt*. Methods of degradation include the continuous removal of faulty elements without repair. A reconfigured system continues to operate with reduced elements. The other method implies removing faulty elements and their replacement with the correct ones, or repairing the defective element; see (Tomas, 2004; Kirrmann, 2005; Shooman, 2002).

2. AVAILABILITY OF VTMIS SYSTEMS

In the national and international scientific and technical literature there has been a growing interest of computer companies in expressing the quality of their products through their *reliability, availability, safety, integrity and functional suitability*. The number and types of quality indicators depend on the complexity of the information system.

The VTMIS system reliability is defined as the probability that the system will function without failure during a specific period of time under certain conditions. In other words, it is the probability that the failure time *T* will occur after the observed time *t*. Reliability is a complex feature and is an indicator of quality. Mean Time Between Failure (MTBF) is the most common indicator of quality.

Availability is defined as the probability that a system will be available at any point in time, i.e. that it will be able to work or to get started, provided it is used under specific conditions.

Availability may be defined in various ways: it may be defined by the manufacturer (inherent availability - A_i) and, on the other hand, as the operational availability (A_o) (Pokorni, 2002).

The inherent availability can be calculated with the aid of the relation:

$$A_i\,[\%] = \frac{MTBF}{MTBF + MTTR} \cdot 100 \qquad (1)$$

Where: MTBF is Mean Time Between Failure and MTTR is Mean Time To Failure.

The operational availability can be calculated by using the relation:

$$A_0\,[\%] = \frac{t_{ur}}{t_{ur} + t_{uo}} \cdot 100 \qquad (2)$$

Where: t_{ur} is the total or average time in the operational work and t_{uo} is the total or average time of failure.

The relation (1) shows that an increased availability can be achieved by higher MTBF (higher reliability) or lower MTTR. A higher MTBF is achieved by higher reliability of the elements that are installed in the computers (servers), but also through redundancy. In computer systems, the MTTR is, in fact, the mean time to the restoration of service, rather than the mean time to repair or replace faulty modules, and the restoration of services includes the following activities: detection of failure / error, reporting the problem, communication between the operator and his own maintenance service or the technical service provided by the system manufacturer, repairing / replacement, restarting the computer system.

MTTR for critical modules of the VTMIS system ranges from 2 to 4 hours, while with non-critical modules it lasts between 24 to 48 hours. Relying to our own experience and technical literature, MTTR can be reduced down to 50% if the user of a VTMIS system is supported by trained and skilled personnel for maintaining computer equipment, if he/she has necessary maintenance equipment and a number of critical spare modules.

On the basis of our own data (Command, Control, Communications and Intelligence system) and data gathered from the literature (Struk, 2012), the availability of computers in different architectures is presented in Table 1.

Table 1.
Availability and the time of failure of computers in the course of one year.

Availability	Failure	Example
90 %	> 1 month	Unattended PC
99 %	~ 3 days 16 hours	Maintained PC
99,9 %	~ 9 h	Cluster
99.99 %	~ 57 min	Mainframe
99.999 %	~ 5 min	Onboard computer to the PC platform
999.999 %	~ 30 s	Installed on a dedicated PC platform

In the Resolution A.915 (220 Ref.40) the International Maritime Organization (IMO) defines the availability as "the probability that the system provides a needed service under the specified conditions. Unavailability can be caused by the planned and / or unforeseen interruption". International Association of Marine Aids to Navigation and Lighthouse Authorities (IALA) recommends three availability levels: *basic, standard* and *target (advanced)* (IALA Recommendation V-128 Edition 3.0: Operational and Technical Performance Requirements for VTS Equipment, 2007).

Companies that produce VTMIS systems adhere to the IALA recommendations and launch into the market VTMIS systems that are configured to provide availability of 99.9%, which means that a subsystem or the system as a whole is not available approximately 9 hours per year; see (Norcontrol IT AS – Vessel Traffic Management & Information System – VTMIS 5060, 2006; CoastWatch VTMIS, 2012).

Table 2.
Availability of radar subsystems as recommended by IALA.

Availability of radar subsystems			
	Levels of availability		
	Basic	Standard	Advanced
Recommended availability for radar subsystems	99 %	99.6 %	99.9 %

In the simplest case, where a failure of any hardware, software, or man / operator leads to a system failure (block diagram of the three elements connected in series), and provided that their failures are independent, the reliability of such a system is obtained by the relation (Shooman, 2002):

$$R_S = R_H \cdot R_{SF} \cdot R_O \tag{3}$$

where:

- R_S – system reliability,
- R_H – hardware reliability,
- R_{SF} – software reliability, and
- R_O – operator reliability.

In VTMIS systems using virtual private networks (VPN), based on TCP / IP technology, it should be taken into account that the system failure or system availability reduction may occur due to the channel failure, network congestion, viruses or attacks referring to rejection of services etc. According to (Hussain, 2005), there may be various reasons for communication network failure: in 32% of cases the failure is due to the connecting paths (links), 25% because of the directors, 36% resulting from maintaining and configuring the network, and 9% due to other communication problems.

In order to increase availability, almost all manufacturers of VTMIS systems install self checking devices in their subsystems. Checks performed during the operation (*functional control*) continuously monitor the operation of the subsystems to detect errors in the software, hardware faults or mistakes made by the operator. Checks performed out of the operational work (*functional testing*) are done with the aim of finding the components that are broken and need to be repaired / replaced. This inspection is carried out by the maintenance personnel (own maintenance, dealers or service agents authorized by the system manufacturer).

Functional monitoring generates two types of warnings that are displayed and logged into a separate file (*log file*):

- system's response – if the operator, during normal operation, enters a wrong command or inadequate information in certain forms, the system responds by generating an adequate warning;
- technical warning – if the functional monitoring diagnoses a failure / error in a module, the subsystem's technical console receives an adequate warning.

A detailed analysis of the reliability and availability of the elements of the VTMIS system is presented in the following chapters.

3. RELIABILITY OF HARDWARE IN VTMIS SYSTEMS

VTMIS systems feature a great variety of subsystems, consisting of a large number of hardware modules. This method of designing a system provides great advantages with regard to redundancy, maintenance and training.

Simple and complex hardware modules that are installed in all control centers and sensors feature an open architecture design in order to meet the new requirements. In control centers the main (critical) modules are VTS server (*Track Management Server*), SQL server and LAN (Local Area Network) networks. In sensor subsystems, the main modules (transmitters, radar extractor, pointing elements...) are under the direct control of the microprocessor. All modules are usually characterized by the so-called failure rate (λ), a general relation for hardware reliability $R(t)$ being:

$$R_H(t) = e^{-\int_0^t \lambda(t)\,dt} \tag{4}$$

Formula (4) is the first law of reliability, which is used to determine of reliability when is a known function of the failure rate. When the failure rate does not change over time, i.e. λ = const, the formula for reliability takes the form:

$$R_H(t) = e^{-\lambda t} \tag{4.1}$$

Formula (4.1) is called the exponential law of reliability. If the failure rate in the formula (4.1) is expressed in the unit (1/h), then the time should be included in hours (h). Formula (4.1) is valid for the second period (the period of normal use) as shown in Figure 1.

Figure 1 shows that there are three characteristic periods within the hardware failure rate: the early failure period, the period of normal use and the period *of aging (wear).*

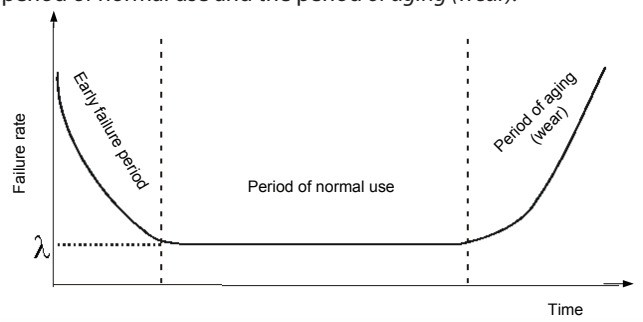

Figure 1.
Failure intensity of hardware elements

In professional systems, such as VTMIS systems, the early failure period (the period of childhood diseases) is conducted by the manufacturer of the system (except for the failures that occur during transport, transfer or installation of the system). At the beginning of the third period, when components are subject to aging and wear, the systems are removed from service for safety reasons because of major material / financial losses that may result from their failure, or due to high maintenance costs.

Reliability indicators are normally used in the second period, i.e. during normal operation. This period is the longest and for personal computer systems may range from 2 to 5 years.

Computer technology provides four ways to ensure the reliability of hardware: *through installing reliable elements* (CPU, RAM, disk drives, etc.), *designing the systems* in such a way that the failure of an individual module cannot lead to the breakdown of the entire system; *purchasing the elements from multiple sources;* and *installation of redundant elements* allowing fast switching to a secondary or redundant element.

Each module whose failure may reduce the system's availability must have its redundant module. Almost all manufacturers of VTMIS systems use the classical form of redundancy for critical modules. This form includes two identical components connected in parallel, where both modules perform the same functions, and each is capable of functioning independently in the system. Both modules are connected to the mechanism for automatically switching from the primary module to the secondary one in case of failure. The secondary module can function in the following conditions: *cold standby reserve, hot standby reserve and fault-tolerant operation.*

VTMIS subsystems use the fault-tolerant operation which means the extension of hot reserve, since the secondary module operates as a "mirror" of the primary module. Both modules handle the same data, so that there is no loss of data or information in case of failure of the primary and switching to the secondary module. In addition, each module has a built-in ability to detect errors. Therefore, adding just one module can be sufficient to achieve the desired reliability. Additional hardware resource management allows the computer system to increase its ability to continue operating.

Figure 2 shows the schematic presentation of a redundant radar transmitter. In addition to the radar transmitter, the radar extractor and microprocessors may be duplicated in some configurations to improve reliability.

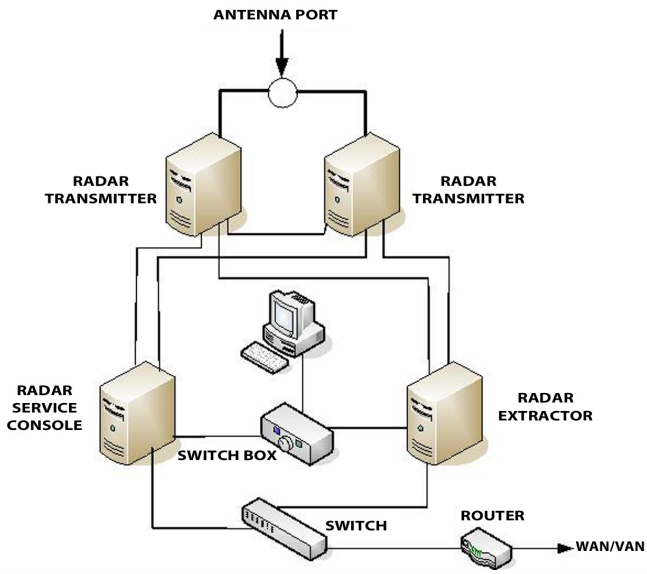

Figure 2.
Redundancy in radar subsystems.
Source: SAAB Systems - CoastWatch VTMIS

In control centers of the VTMIS systems, critical redundant modules include: VTS server, database server (SQL server) and LAN networks; see (Norcontrol IT AS – Vessel Traffic Management & Information System – VTMIS 5060, 2006; CoastWatch VTMIS, 2012).

All computer equipment in VTMIS subsystems is connected to devices for uninterruptible power supply (UPS), with the provision that in the event of a prolonged interruption of power a diesel generator cuts in. This form of redundancy is ensured because power failures make 26% of total failures in computer systems.

There are several mechanisms for monitoring hardware modules. The simplest way is to monitor functional safety and it involves checking the hardware modules with the aid of other

hardware modules and using test programs. The performance of test programs does not affect normal functions of the software. When functional monitoring detects an error, a warning is sent to the technical service console and is recorded in the log file.

In order to further increase the availability of the VTMIS system, i.e. the availability of control centers, the hardware and software of all consoles are configured to perform the same functions, which means that the failure of one operator console will not affect the other.

In order to increase the reliability of the VTMIS system, nominal environmental conditions must be met: atmospheric pressure of 1024 hPa, relative humidity of 70%, rainfall at 5 mm/hr, air temperature 25°C, sea temperature 18°C, salinity of 35‰ and sea state up to 3.

Redundant modules have proved to be the best solution for improving the overall availability of subsystems and the VTMIS system as a whole. Installing the most trusted module can be a more expensive and less reliable solution than installing the two cheaper and less reliable modules that operate in parallel with negligible time of switching and restarting.

4. RELIABILITY OF SOFTWARE IN VTMIS SYSTEMS

As a result of the increasingly important role of software in professional systems, including VTMIS systems, software errors have a significant share in the total number of failures. This, in turn, has forced professional system manufacturers to pay more attention to the software reliability and availability, i.e. to the overall quality of their systems.

VTMIS software system is based on common modules that are harmonized with the functions. These "modules" are called systemic functions because each systemic function performs one of the many functions that the systemic software should do. The rest of the modules (programs) in the VTMIS system, i.e. the utility tools, are not essential for the operational reliability of the system.

Depending on the VTMIS manufacturer, the systemic functions are grouped into several categories. Here is one of the possible categorizations:

- *systemic application functions* - are functions that perform the functional requirements of operators;
- *systemic functions for sensor control* – are functions for handling the sensors for data acquisition and basic information processing;
- *systemic communication functions* – are functions ensuring the interaction with the operator, the communication within each subsystem and for communication between subsystems;
- *auxiliary systemic functions* – are used by other functions to fulfill their tasks;
- *basic systemic functions* – are functions without which the other systemic features could not work; they include the operating system functions, data management, functional monitoring and functional verification.

Such a division of VTMIS software systems into systemic functions makes the software consistent, effective, reliable, and easy to understand, maintain and upgrade.

Ensuring a high reliability of the software depends on the parameters of the software quality in each stage of the development cycle. Each stage requires parameters used to measure the quality characteristics. The IEEE 982.2. standard defines in detail the characteristics of each stage, with particular attention paid to: user requirements, design, implementation and *testing* (IEEE Std. 982.2.-1988: IEEE Guide for the Use of Standard Dictionary of Measures to Produce Reliable Software, 1988).

The assessment of the reliability of software is done using various measures (Jiantao, 1999): *the finished product value* (referring to the complexity of the software, i.e. the number of lines of the software code), *project management value* (referring to the relationship between the development process and the project feasibility in a defined period of time and at acceptable quality level), *software development process* (referring to the measures taken to produce a quality software), *error and failure ratio* (referring to the MTBF and reliability of the software calculated on the basis of information on errors obtained from users), and *reliability requirement factor* (which implies that the specification of user requirements cannot contain ambiguous phrases, requests with multiple meanings, and the like).

According to ANSI, the software reliability is defined as the probability of a successful software operation over a period of time in a particular environment. In other words, software reliability is a function of a successful software operation dependent on the time and the environment:

$$R_{SF} = f\,(rbo, so, ov) \tag{5}$$

where:

- *rbo* – operation without failure,
- *so* – specific environment, and
- *ov* – specified time.

The evaluation of reliability and the hardware reliability itself are based on the analysis of failure, i.e. software errors and their impact on the overall system. Software error may be the result of errors in the code, misuse, misinterpretation of specifications that the software should satisfy (incompetence of programmers), the application of inappropriate tests or other unforeseen problems.

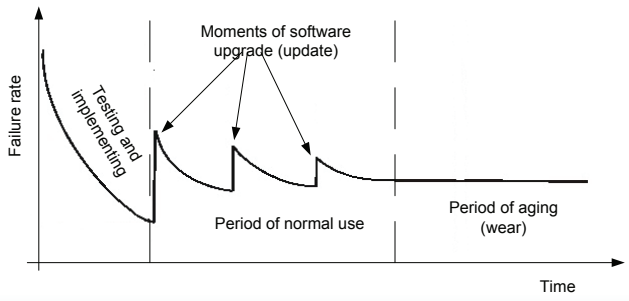

Figure 3.
The function of the failure rate of software.

Comparing the hardware failure rate curve (Figure 1) and the software failure rate (Figure 3), two main differences can be noticed:

- during aging (wear) there is no increased error intensity, nor decreased reliability, because software does not require updating;
- the software failure rate during normal use features a number of peaks indicating an increasing number of failures due to upgrades (updates) of the systemic or user software, as it is likely to make mistakes during the process.

Similar to VTMIS hardware systems, many techniques that are designed for detection and fault tolerance can be applied to the software. Redundant software can be implemented in multiple forms, and it is not necessary to replicate the entire modules to obtain redundancy. Software redundancy can be achieved by using additional parts of programs (from using several software modules to the use of programming procedures), or through additional data storage, where several software support tools may be used.

The simplest mechanism for checking software is the use of time clocks or monitoring clocks (programmable timers, counters that normally reset the programs that are being executed before reaching zero when counting backwards). If the program is terminated due to an error, the countdown timers will not be reset on time, and functional control will send a technical warning to the service console and enter it in the log file.

In order to increase the availability of software subsystems, there has been an increased use of software agents, i.e. systems for automatic installation and configuration of software support modules on remote PCs. Software agents can perform the installation of operating systems or modules of systemic functions. The RMS (Remote Maintenance Stell) is such an example. The RMS system allows fully automated remote management of software support on a large number of nodes in the IP network.

In the beginning of modern VTMIS system development, the operating systems Windows NT, Windows 2000 and Windows XP were used. Today, Microsoft operating systems are increasingly replaced with open source solutions (UNIX, Linux, etc.), in particular for server applications.

5. RELIABILITY OF MAN

At the dawn of development of complex technical systems, the manufacturers of computer systems usually determined the reliability of their system by taking into account only the reliability of the hardware (and later, the reliability of the software). From the practical point of view, the reliability defined in such a way presents just approximate information about the reliability of the system where a man inevitably takes part. The first attempts to determine the reliability of man assumed the application of the same concepts and methods that were used by the hardware reliability theory, considering the man / operator as a separate element of the system. Thus, it was possible to form the function of operator errors analogous to the function of the hardware failure rate. When the operator starts working (not being familiar with the current state of maritime traffic), the number of errors is usually high, to be soon reduced and become relatively small and approximately constant. After a while, the number of errors increases due to fatigue. The human error rate curve is analogous to hardware failure rate (Figure 1). The only difference lies in the observation period: for the hardware it is equal to the time of use (for a PC 2 to 5 years), and for humans the observation period covers an operator's shift or working hours.

Significant factors affecting the reliability of the human being are: *stress, time, training, conditions (ergonomics), procedures, etc.*

Man, as part of the system, may take a number of roles that directly or indirectly affect the availability of the system. In VTMIS systems, man can take the role of a VTS operator, VTS supervisor, VTS instructor, VTS manager, he/she may become a service provider (maintenance) or a service user.

IALA Recommendation V-103, entitled "Standards for Training and Certification of VTS Personnel", provides a set of requirements for courses and standards for certification of VTS personnel. A VTS operator must hold a certificate that includes the provision of information services, provision of navigation assistance and traffic organization services, and – if necessary – a VTS supervisor license (Recommendation V-103 Standards for Training and Certification of VTS Personnel, 2009).

Each VTS center should ensure a detailed VTS operator's job description that is in line with the provided services, equipment and coordination with other participants in maritime traffic.

For VTS personnel educational purposes a simulation function is used. The function should be in accordance with the IALA V-103 recommendations. Simulated maritime vessels move in line with the pre-programmed trajectories that are similar to those used for showing the movement of objects. On simulated

maritime facilities an operator can use most of the functions within the VTMIS system in the same way he/she uses the functions of the real-life marine facilities.

In order to increase the reliability of VTS operators, it is necessary to develop the ability of simultaneous acting which implies the human activity involving the simultaneous receiving and processing information from multiple independent sources or the simultaneous performance of two or more tasks. The term "simultaneous" should not be taken literally (parallel processing of information), but rather in a broader sense as a fast switching of focus from one task to another.

Problems that affect the reduced reliability of operators include:

- *arm muscle strain* – which largely depends on the design of the keyboard, mouse or control surface; strain of other muscles of the body (general fatigue and pain in the lower back) depends on the design of operator and service console;
- *visual comfort in using the console monitors* – is related to the features of the characters and the background on the console monitor and video terminals (size, contrast, brightness and color); in addition, the visual comfort is affected by monitor resolution, monitor size and speed of exchanging letters;
- *ergonomic design of interfaces* – the interface should allow the operator to focus on the task to be performed and be done in an intuitive way, the user's interface is actually a window providing a view into the application.

It is obvious that man as a part of the system can increase the reliability of the system, but also reduce it if his/her reliability is low. Therefore, the reliability of the man in VTMIS systems should be taken into careful consideration. There are human reliability models that have been designed specifically to serve the purpose.

6. CONCLUSION

Safe navigation of vessels is increasingly required in today's global maritime transport, especially in the control and organization of maritime transport. This is achieved through reliable operation of information and communication systems that provide timely, accurate and reliable data and information to the master and other participants in the maritime traffic. Low reliability and availability result in endangered safety of the ship, master's dissatisfaction (due to undelivered goods or services) and lead to pollution of the sea and marine environment. These consequences generate considerable material and financial losses. The reliability and availability of a VTMIS system must be calculated by taking into account the reliability of the hardware, the reliability of the software (as there is no component of the system which does not feature a built-in software), but also the reliability of the man / operator, particularly in supervision systems where human component takes part in all operations.

All manufacturers of VTMIS systems can achieve the availability of at least 99.9% for devices, subsystems and the system as a whole by combining hardware, software, information and time redundancy. The introduction of redundancy leads to complex and expensive configurations of the subsystems. For this reason, the designers and users of professional systems including VTMIS systems introduce redundancy only into the modules that are critical for the system, i.e. into the modules that require an extremely high level of reliability and availability, such as the VTS server and SQL server.

An increased availability of VTMIS systems inevitably implies investment in VTS human resources. The personnel engaged should have IT knowledge, hold VTS certificates, be able to act simultaneously, and be trained to perform all procedures and critical events with the aid of the simulator which is in compliance with the IALA V-103 recommendations.

REFERENCES

Hussain, I., (2005), Understanding High Availability of IP and MPLS Network, Indianapolis: Cisco Press.

IEEE Std. 982.2.-1988: IEEE Guide for the Use of Standard Dictionary of Measures to Produce Reliable Software, (1988), available at: http://standards.ieee.org/findstds/standard/982.2-1988.html, [accessed, 07 September 2012.].

IALA Recommendation V-128 Edition 3.0: Operational and Technical Performance Requirements for VTS Equipment, (2007), available at: http://www.tidelandsignal.com/web/information/IALA/Recommendations/V-128-Ed2-2007.pdf, [accessed 07 September 2012.].

Jiantao, P., (1999), Software Reliability, Carnegie Mellon University, available at: http://www.ece.cmu.edu, [accessed 07 September 2012.].

Kirrmann, R., (2005), Fault Tolerant Computing in Industrial Automation, 2nd Edition, Baden: ABB Research Center.

Norcontrol IT AS – Vessel Traffic Management & Information System – VTMIS 5060, (2006), product data sheet, available at: http://www.aatash.com/website/aatash-norcontrol/pdf/VTMIS5060.pdf, [accessed 07 September 2012.].

Pokorni, S., (2002), Pouzdanost i održavanje tehničkih sistema, (in Serbian), Beograd: Military academy.

IALA Recommendation V-103: Standards for Training and Certification of VTS Personnel, 2009.

CoastWatch VTMIS, User Guide, SAAB SYSTEMS, http://www.caclase.co.uk/Products/Documents/391/CoastWatch.pdf, [accessed 07 September 2012.].

Shooman, M. L., (2002), Reliability of Computer Systems and Networks: Fault Tolerance, Analysis, and Design, New York: J. Wiley & Sons.

Struk, V., Pouzdanost računalnih sustava, (in Croatian), lectures, Faculty of Electrical Engineering and Computing, University of Zagreb, available at: http://www.fer.unizg.hr/_download/repository/prs_01%5B1%5D.pdf, [accessed 07 September 2012.].

Tomas, V., (2004), Tehnike toleriranja kvarova u dijagnostičkom sistemu, in Croatian, Pomorstvo, 18(2004), pp. 137-146.