On the availability of information exchange in radio notification transmission systems

A V Telny
Vladimir State University, city of Vladimir, Gorky Street, 6 str., 87, 600000, Russia
E-mail andre.izi@mail.ru

Abstract. This article presents the results of studies on assessing the availability of information exchange in radio transmission notifications system (RTNS) of various types. The author proposes to use indicators showing the probability of non-reception of alarm notifications at the scheduled time, the daily average probability of non-reception of data from RTNS, and the average daily occupancy of the RTNS radio channel as parameters for assessing the availability. The article introduces the expansion of the existing assessments of the information exchange availability not only in terms of test messages passing the radio channel control, but also taking into account possible internal time collisions associated with the transmission of service and alarm notifications to RTNS. The author proposes to expand the assessments of availability indicators not only for asynchronous RTNS, but also for combined asynchronous-synchronous systems with working frequency occupancy control, satisfying the conditions stating that the time window for the transmission of alarm and service notifications does not intersect with the time window of test messages for the radio channel control. The calculations show that the obtained estimates of availability are consistent with the established practice of RTNS operation.

Keywords: Centralized security point; Radio system for transmitting notifications; Object transceivers; Synchronous-asynchronous operation mode of the RTNS; Internal time collisions

1. Introduction
Radio systems for transmitting notifications are used for centralized protection and fire monitoring of facilities. Object complexes of security, alarm and fire alarms transmit service and alarm notifications about the state of the object to the centralized protection point (CSP) by means of RTNS. The number of transmitted messages is determined by the information content of RTNS, the tactics of protecting objects and the structure of RTNS. To control the integrity of the radio channel, the object blocks constantly send test messages. For different RTNS, test bursts can have a different set of durations, and the minimum burst period is usually defined as 12-15 seconds. The maximum polling time is limited, and at the same time, the fact of communication failure with each of the protected objects should be determined in a time of no more than 120 seconds. Depending on the hardware and circuitry implementation of RTNS, the duration of the test messages can be from 6 to 15 ms. The duration of a service notifications transmission from the object to the central (base) station for RTNS basically corresponds to the duration of alarm notifications and ranges from 30 to 50 ms, but alarms have a higher priority during transmission. The most significant factor determining availability in RTNS is the number of protected sites. Since all the object transmitters in RTNS operate at the same frequency, the filling of the operating frequency is determined by the number of the objects protected at the same. This factor
also affects time collisions in the operation of RTNS transmitters at other sites. Temporary collisions occur when service and alarm notifications from different objects overlap. As a result, the transmitted notifications disappear.

RTNS types are categorized by design into one-way RTNS (one-way notification, only a transmitter is installed at the site) and two-way RTNS, when the site has a receiver and a transmitter. In addition, in asynchronous RTNS, the transmission of all types of notifications is carried out in a randomly determined time interval and is not synchronized with the operation of other object transmitters. For this reason, all announcements in an asynchronous RTNS are repeated many times. Basically, an asynchronous RTNS transmits notifications either in bursts, with a constant time interval between messages in a burst, or random access to the data transmission channel is used, or mathematical laws are used to ensure the non-repeatability of the number series (for example, a number of primes are used) and to increase the delivery probability notifications. In synchronous notification transmission systems, the operation of object blocks is synchronized from the side of the centralized monitoring panel (each transceiver communicates after the synchronization signal, in its own time window, usually associated with the object number of the block). The transceiver can listen to the operating frequency for its busyness and get in touch after the end of the transmission from another unit. The test messages repetition rate determines the amount of information transmitted in the communication channel and affects the availability of information exchange and the possible number of protected objects, like the information content of RTNS.

The electromagnetic environment in the RTNS coverage area has a strong impact on the state of radio communications. This parameter can be both random (in case of natural interference), and targeted in case of deliberate interference or special purpose sabotage of RTNS. We do not take into account accessibility analysis sabotage performed by an intruder and the influence of external electromagnetic interference. Many publications are devoted to the functioning of various types of RTNS, for example, [1-13] and others. [1,2,3,14,16] deal with ensuring confidentiality of transmitted information, imitation security of RTNS transceivers and secrecy of information exchange. Work [15] is devoted to information exchange algorithms in RTNS and optimization of time windows of pauses in an asynchronous system. In this work, it is proposed to use a relative prime number generator that forms a time sequence with the smallest common multiple exceeding the channel control time. Items [4,8] consider the issues of using radio-technical methods of transmitting notifications with pseudo-random operational frequency readjustment with spreading of the spectrum in asynchronous RTNS, including the use of PROFR only for the choice of the carrier frequency, but also for the time intervals for sending messages. In [16], it is proposed to use the cellular principle of RTNS construction, while the objects transmit all information only to the central nodes of the “cell”, which control the communication channels to the objects in their “cells” independently. Only “cell” nodes transmit information to the CSP. The issues of the availability of information exchange for RTNS were directly considered in [17,18,19,20].

2. Problem statement

The availability of information exchange in radio systems for the transmission of notifications can be assessed as the probability of the system fulfilling its main functional purpose of transmitting alarm messages from any protected object to a centralized security point. Determination of availability for RTNS can be interpreted as the possibility of transmitting an alarm notification for a specified time. It is proposed to assess the availability of information exchange in radio systems for transmitting notifications according to the following generalized formula

$$A_D = \int_{t_{AL}}^{t_{AL}+T_D} A_F(\alpha(t), t) dt$$  \hspace{1cm} (1)

Here $A_D$ is the directive accessibility of the RTNS; $t_{AL}$stands for triggering time of technical means of security and alarm on the object device RTNS of a particular object; $T_D$ means directive (maximum possible) time during which it is necessary to transmit the alarm notification to the CSP; $A_F$ stands for actual availability of RTNS for data exchange at time $t$; $\alpha(t) = \varphi(F(t))$ shows a function of
dynamically changing factors; \( F(t) = (f_1(t); f_2(t); \ldots; f_k(t)) \) is a vector of factors that can be dynamic and change over time, be constants or random variables; \( f_1(t); f_2(t); \ldots; f_k(t) \) are factors affecting the availability of RTNS (the number of protected facilities, time collisions from the operation of RTNS transmitters at other facilities, the electromagnetic environment in the RTNS coverage area, RTNS type, nature of information exchange, RTNS architecture, duration of service and alarm notifications, RTNS information content, spectrum width, carrier frequency instability, etc.).

According to the Russian standards, the delivery time of an alarm notification for RTNS should not exceed 60 seconds, which is the directive time \( T_p \). The most promising direction in the development of RTNS is the creation of combined asynchronous-synchronous systems in which all service notifications are transmitted in their time windows, and alarm notifications are transmitted in a randomly determined time interval of a special time window. Alarms are repeated (duplicated) until an acknowledgment (notification of notification) is received from the central station to ensure the guaranteed transmission into the object's transmitters at other facilities, the electromagnetic environment is taken into account and do not affect the time synchronization of the RTNS; the probability of errors caused by incorrect transmission or reception of the object number is extremely small. To model the probability of passing notifications from an object to a CSP, it is proposed to use the Poisson distribution for the following reasons: the probability of overlapping notifications from object blocks (time collisions) depends only on the duration of notifications and does not depend on the time of their occurrence, and the notifications themselves are distributed on the time axis with the same average density; the probability of collisions occurring in the allocated time interval does not depend on the probability of overlapping notifications in another time interval; the probability of overlapping three or more notifications in a time interval equal to twice the duration of notifications is negligible compared to the probability of overlapping two notifications in this time interval.

### 3. Methodology for assessing the availability of information exchange in radio systems for transmitting notifications

We propose to use two indicators to analyze the availability in practical use. These are the messages non-reception probability (the probability of temporary collisions, overlapping messages) \( P_{not} \) and the maximum occupancy of the radio channel \( G_{max} \) at given levels \( P_{not} \) and the number of message repetitions \( b \). The number of message repetitions for different types of RTNS can be either the same or different for service \( b_{serv} \) and alarms \( b_{Al} \). Let \( b_{serv} = b_{Al} = 6 + 16 \).

According to [18,19,20] for asynchronous RTNS:

\[
P_{not} = 1 - \exp(-\frac{2\pi N}{\Delta t_{test}}) \tag{2}
\]

Here \( \tau \) is the duration of test messages (\( \tau \approx 6 \div 15 \) ms), \( N \) means the number of protected objects, \( \Delta t_{test} \) stands for repetition period between test messages. Typically, for RTNS, there are several sets of test transmission periods with a minimum of about 12-15 seconds. \( T_{contr} \) maximum time of polls, according to which the fact of communication with the object is established \( T_{contr} = 120 \) s. It is worth noting that formula (2) gives the probability of non-reception of only test messages and only two messages (one collision), it is possible to refine \( P_{not} \) both for test messages and for service and alarm notifications

\[
P_{not} = 1 - \exp\left(-\frac{2\pi N}{\Delta t_{test}} + \frac{2t_{max}(2N+k_{serv})b_{serv}}{T_{day}} + \frac{2t_{max}k_{Al}b_{Al}}{T_{day}}\right) \tag{3}
\]
Here $t_{mes}$ is the duration of alarm and service notifications ($t_{mes} \approx 30 \div 50$ ms), $T_{day}$ is a day ($T_{day} = 86400$ s), $k_{serv}$ and $k_{AL}$ are the average daily number of alarm and service (excluding commands to arm/disarm an object) notifications from RTNS respectively (this data can be obtained from the statistics of RTNS operation on the CSP). It is assumed that each object is armed and disarmed on a daily basis. For practical purposes of protecting objects [18], it is advisable to take the values $P_{Σnot} = 10^{-4} \div 10^{-5}$. The maximum occupancy of the radio channel $G_{max}$ for asynchronous systems according to [18] is defined as

$$G_{max} = \frac{-\ln(1-P_{Σnot})}{2}$$

(4)

Formula (4) is valid only for test messages. The average value of the average daily occupancy of a radio channel (for the time $T_{day} = 86400$ s) for asynchronous systems can be determined as

$$G_{mean} = \frac{1}{T_{day}} \left( t_{mes} + k_{AL} b_{AL} + t_{mes} k_{AL} b_{AL} + \frac{1}{2}(2N + k_{serv}) b_{serv} + t_{mes} b_{AL} b_{AL} \right)$$

(5)

The second term in formula (5) means the share of the radio channel occupation with test messages, the second term determines the share of occupation by the arming / disarming commands for each object and the average daily number of other service notices, and the third term determines the share of the radio channel occupation by the average daily number of alarm notifications. An important indicator is to determine the likelihood of non-receipt of exactly alarming notifications at the scheduled time. The number of repetitions of the transmission of alarm notifications for the directive control time $m = \frac{T_D}{ΔT_{AL}}$

Here $T_D = 60$ c according to [1], and $ΔT_{AL}$ is the repetition period between alarm messages. At the same time, $ΔT_{AL}$ is a random variable generated by special random number generators for many asynchronous RTNS [15]. In practice, for various types of RTNS, $ΔT_{AL} = 3 \div 30$ s. Since the overlapping of notifications on the time interval $ΔT_{AL}$ is assumed to be an independent event, the probability of non-receipt of alarm notifications at the scheduled time will be

$$P_{Σnot|T_D} = (P_{Σnot})^{\left( \frac{T_D}{T_{day}} - \frac{T_D}{T_{day}} \right)} = P_{Σnot}^m$$

(6)

In practice, for RTNS, the value $P_{Σnot|T_D}$ should be $P_{Σnot|T_D} \leq 10^{-6} \div 10^{-7}$ over the time period $T_D$. For combined asynchronous-synchronous systems with controlled working frequency occupancy, the availability parameters $P_{Σnot}$, $G_{mean}$, $P_{Σnot|T_D}$ depend greatly on architecture, operation algorithm and data format in RTNS data exchange protocols. In such systems, the transmission of test messages is synchronized and does not cause time collisions (if the equipment is functioning properly), and the transmission of alarm and service notifications from the facility is a random event. If we assume that the system has the following properties: all test messages are repeated once in the time window set for the object and no temporary collisions occur: the time window for the transmission of alarm and service notices does not overlap with the time window for test messages; only service and alarm notifications are acknowledged from the central station, and after receiving the acknowledgment signal, the object block does not perform further repetitions of notifications.

When these conditions are met for combined asynchronous-synchronous systems, $P_{Σnot}$ can be determined as follows

$$P_{Σnot} = 1 - \exp\left\{-\left(\frac{2(t_{mes} + τ_p) b_{serv} + τ_{ack})}{T_{day} p} + \frac{2(t_{mes} + τ_p) b_{AL} + τ_{ack}) k_{AL}}{T_{day} p}\right)\right\}$$

(7)

Here $τ_{ack}$ is the duration of acknowledgment notifications (confirmation of information receipt from the object unit from the central station to the central station) (usually $τ_{ack} = τ \approx 6 \div 15$ ms), $τ_p$ is the pause time for air control before transmitting each notification ($τ_p \approx (0,2 \div 0,3) t_{mes}$), $P$ stands for time fraction for service and alarm notifications transmission in the time cycle of information exchange between the object and the CSP. $P = \frac{T_{winAL}}{T_{winAL} + T_{winAl}}$, where $T_{winAL}$ is the duration of the time window for the transmission of alarm and service notices, $T_{winAl} -$ the duration of the time window for the transmission of test messages. $T_{winAL} + T_{winAl}$ - full period of the time cycle of information exchange with the CSP. $T_{winTest} = (t_{mes} + τ_p) N$. The minimum value stating the probability of non-receipt of alarms for combined asynchronous-synchronous systems at the scheduled time will be
\[ P_{\text{Σnot}|T_D} = (P_{\text{Σnot}})^{\left(T_D-T_{\text{win test}}\right)\Delta T_{\text{AL}}}(T_D/T_{\text{day}}P) \]  

(8)

The average value of the average daily occupancy of a radio channel (for the time \(T_{\text{day}} = 86400\) s) for combined asynchronous-synchronous systems with control of the working frequency occupancy can be determined similarly to (5) as follows:

\[ G_{\text{mean}} = \frac{1}{T_{\text{day}}} \left\{ (\tau + \tau_p) \left(\frac{T_{\text{day}}}{T_{\text{contr}}}\right) N + (t_{\text{mes}} + \tau_p)(2N + k_{\text{serv}})b_{\text{serv}} + (t_{\text{mes}} + \tau_p)k_{\text{AL}}b_{\text{AL}} + \right. \]
\[ \left. \tau_{\text{ack}}(k_{\text{serv}} + k_{\text{AL}}) \right\} \]

(9)

Taking into account the fact that after receiving an acknowledgment signal for alarms and service notifications, the object block does not perform further repetitions of the notifications transmission, the number of repetitions for service and alarm notifications will be lower for combined asynchronous-synchronous systems with control of the working frequency than for asynchronous systems.

4. Availability assessment comparison for asynchronous and combined asynchronous-synchronous RTNS

For comparison, let us assess the availability of information exchange by the indicators \(G_{\text{mean}}\) and \(P_{\text{Σnot}|T_D}\) for asynchronous RTNS (5), (6) and combined asynchronous-synchronous RTNS with control of the working frequency busy (8), (9). We will take a day \((T_{\text{day}}=86400\) s) as comparison time. The initial conditions for the systems are assumed to be the same. Let the combined system comply with the above conditions, and for each notification from the object, an acknowledgment follows. Let us take the following initial data for asynchronous RTNS: \(\tau = 10\) ms; \(T_D = 60\) s; \(b = 10\); \(b_{\text{serv}} = b_{\text{AL}} = 16; T_{\text{contr}} = 120\) s; \(\Delta t_{\text{test}} = 12\) s; \(\Delta T_{\text{AL}} = 12\) s; \(t_{\text{mes}} = 50\) ms; \(k_{\text{serv}} = 0,1N; k_{\text{AL}} = 0,05N\); modified parameter \(N = 10...410\) in increments of 20. Let us take the following initial data for the combined asynchronous-synchronous RTNS with control of the working frequency occupancy: \(\tau = 10\) ms; \(T_D = 60\) s; \(b_{\text{serv}} = b_{\text{AL}} = 2; T_{\text{contr}} = 120\) s; \(\Delta t_{\text{test}} = 12\) s; \(\Delta T_{\text{AL}} = 12\) s; \(t_{\text{mes}} = 50\) ms; \(\tau_{\text{ack}} = 15\) ms; \(\tau_p = 10\) ms; \(k_{\text{serv}} = 0,1N; k_{\text{AL}} = 0,05N; P = 0,1\); variable parameter \(N = 10...410\) in increments of 20. The calculation results are shown in Figure 1 and Figure 2.

Figure 1. Probability of not receiving alarms at scheduled times for different RTNS
5. Conclusion
The paper proposes an assessment methodology for the availability of information exchange in radio systems for transmitting notifications of various types, including asynchronous systems and combined asynchronous-synchronous ones with control of the working frequency occupancy. The approaches used can be partially applicable to notification transmission systems of a more complex architecture. Such parameters as the probability of non-reception of alarm notifications at the scheduled time, the average daily probability of non-reception of data from RTNS and the average daily occupancy of the RTNS radio channel are proposed to be used for assessing availability. The novelty in this work is the proposal to calculate the accessibility parameters not only by passing the test messages of the radio channel control, but also taking into account possible collisions associated with the transmission of service and alarm notifications.

The proposed methodology can be useful when comparing RTNS of various types and principles of operation, as well as to justify the maximum possible number of protected objects on one RTNS frequency. Based on the results of the calculations, we can conclude that the combined asynchronous-synchronous RTNS with control of the working frequency occupancy can be more effective than the asynchronous one in terms of the probability of non-receipt of alarm notifications at the scheduled time with a large number of protected objects.

6. Acknowledgment
The study was conducted as part of the implementation of the state task of Vladimir State University FZUN-2020-0013.

References
[1] Fedyaev S L, Maksimov V S and Fedyaev Yu S 2011 Patent for utility model No. 111938 RU G08B 21/00 27.12.2011. Radio channel alarm complex of protection
[2] Zavyalov S A, Isupov A V, Kosyih A V, Lepetaev A N, Tsibenko L V and Zavyalov N S 2008 Patent for utility model No. 74232 RU G08B 26/00 20.06.2008. Notification Radio System
[3] Pervuninskikh V A 2016 Patent for invention No. 2620239 RU G08B 13/00 23.05.2017. Wireless self-organizing network system of protected territory monitoring
[4] Ji S and Cai Z 2012 Distributed data collection and its capacity in asynchronous wireless sensor networks *Proceedings - IEEE INFOCOM* 2113–21

[5] Ji S and Cai Z 2013 Distributed data collection in large-scale asynchronous wireless sensor networks under the generalized physical interference model *IEEE/ACM Trans. Netw.* 21(4) 1270–83

[6] Zhang Y, Shum K W and Wong W S 2011 Completely irrepressible sequences for the asynchronous collision channel without feedback *IEEE Trans. Veh. Technol.* 60(4) 1859–66

[7] Shum K W, Wong W S, Sung C W and Chen C S 2009 Design and construction of protocol sequences: Shift invariance and user irrepressibility *IEEE International Symposium on Information Theory – Proceedings* 1368–72

[8] Wong W S 2007 New protocol sequences for random-access channels without feedback *IEEE Trans. Inf. Theory* 53(6) 2060–71

[9] Chen S, Wang Y, Li X Y and Shi X 2009 Order-optimal data collection in wireless sensor networks: Delay and capacity *2009 6th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks* pp 1–9

[10] Marler R T and Arora J S 2004 Survey of multi-objective optimization methods for engineering *Struct. Multidiscip. Optim.* 26(6) 369–96

[11] Chamberlain J F and Veeravalli V V 2007 Wireless sensors in distributed detection applications *IEEE Signal Process. Mag.* 24(3) 16–25

[12] Rani B S and Shyamala K 2019 Energy Efficient Load Balancing Approach for Multipath Routing Protocol in Ad Hoc Networks 2019 Second International Conference on Advanced Computational and Communication Paradigms (ICACCP), pp. 1–5

[13] Bishop A N, Fidan B, Anderson B D O, Doğançay K and Pathirana P N 2010 Optimality analysis of sensor-target localization geometries *Automatica* 46(3) 479–92

[14] Osipov D L, Zhuk A P and Gavrishev A A 2015 Patent for invention No. 2560824 RU H04L 9/20 20.08.2015. Apparatus for protection against imitation of controlled objects with high structural security of carrier signals

[15] Tsyibenko L V, Zavyalov S A and Tihonov S V 2008 Improving the algorithm of operation of security radios *The Journal Omsk Scientific Bulletin (Omsk: Publishing House of Omsk University)* 70(3) 126–29 (in Russian)

[16] Partyka A 2005 Patent for invention No. 6870875 US H04B 1/69 22.03.2005. Transmission of urgent messages in frequency hopping system for intermittent transmission

[17] Spiridonova N E and Zarubin V S 2017 The cellular principle of creation of perspective RSPI for the organization of the protection of stationary objects *Okhrana, bezopasnost, sviaz* (Voronezh: Publishing House of Voronezh Institute of the Ministry of Interior of Russia) 1–1 175–78 (in Russian)

[18] Zuev P I 2011 Funktsionalnyie vomoznosti asinhronno adresnyih radioohrannyih sistem *Algoritm Bezopasnosti magazine* 4 78–82 (in Russian)

[19] Zuev P I 2004 Veroyatnostnyiy analiz funktsionalnyih vozmozhnostey asinhronno-adresnyih radioohrannyih sistem *Algoritm Bezopasnosti magazine* 2 52–55 (in Russian)

[20] Belkin V. 2006 Veroyatnost dostavki soobscheniy v radiosistemah peredachi izvescheniy asinhronno-adresnogo tipa *Algoritm Bezopasnosti magazine* 2 60–62 (in Russian)