KAPITEL 3 / *CHAPTER 3* [3]
AN APPROACH TO ASSESSING THE OPERATIONAL RELIABILITY OF REAL-TIME SYSTEMS AT THE STAGE OF CONCEPTUAL DESIGN

DOI: 10.30890/2709-2313.2023-22-01-029

Introduction

When designing computer control systems for cyber-physical and technological objects, an important stage is the stage of conceptual (architectural or early) design, when the main hardware and software solutions of RTCS are formed [1, 2]. The complexity of design and research works of the architectural stage lies in the unreliability of initial data for decision-making. This also applies to the task of software reliability assessment [3, 4, 22, and 23]. The main features of early software reliability assessment are described in [6, 13]. Neural networks [7], fuzzy logic [5], behavioral models [29] are used to solve this task. However, these approaches are difficult to apply in the early stages of design, especially for real-time systems [27]. Despite the successful testing and debugging of CS software and hardware in stationary laboratory conditions, when they operate in real technological processes under the influence of radio magnetic electronic fields, there are many perturbations in the processing of external events. Avionics and aerospace control systems are examples of such systems [12, 15, 21, 25 and 28]. This is because in processors of any federated or backbone architecture [17], the probability of failure increases by almost an order of magnitude [19, 26], which is equivalent to the loss of functional reliability under limiting conditions. These conditions can be quite severe in many control system time scales. This system belongs to the HRT (Hard Real-Time) class. Hard Real-Time software systems have a set of hard deadlines, and missing a deadline is considered a system failure [29, 30, and 31]. Examples of Hard Real-Time systems are sensors and autopilot systems for aircraft, spacecraft and planetary rovers [12, 15, 21, 25, and 28]. For such systems, it is important to fulfil a number of requirements including quality of service: Overall network performance includes factors such as throughput, bandwidth, availability as well as jitter, delay and error rate. In this regard, for such systems it is reasonable to use such a reliability indicator as the probability of system failure-free operation during the lifetime of an r-transaction [1, 2, and 14]. By lifetime we mean the marginal processing time of an r-transaction. Therefore, this paper proposes an illustration and numerical example from a preliminary design to apply a set of simple heuristic models to describe the operation of a marshaling yard RTCS and its software

[3]**Authors:** *Kosolapov Anatoliy, Egorov Oleg, Sokur Maria, Parpolita Alexander, Belyaev Nikolai*

under real-time constraints [2] and simple methods for calculating software stability at the conceptual design stage of real-time systems (Figure 1).

3.1. The main heuristic models

The presented complex structural scheme of the automated control system of the marshalling yard contains the control object - the marshalling yard with cars (uncouplers) on it and territorially distributed information and control RTCS. This system includes terminals of operating personnel K1…Kx, workstations, server and communication devices with the object.

Object communication devices (OCD) are designed to generate a set of signals about the state of the equipment on the hill and to issue control actions to the actuators.

The central processor part of the RTCS performs signal processing, forms and issues control actions to the OCD, interacts with the central database arrays, and issues information messages to the workstations.

The system processor realises the execution of a set of tasks in the form of a sequence of functional program blocks (FPB) or r-transactions. Two main parts can be distinguished in the processor: the phase of dispatching requests and the phase of processing the selected r-transaction. The dispatching phase consists of the work of the buffering manager and the work of the service manager.

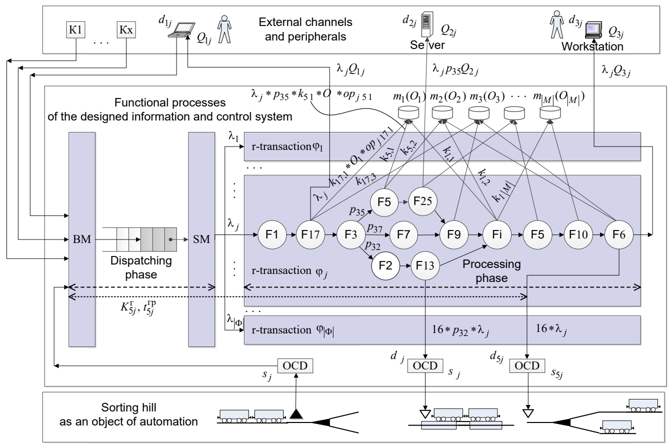

Figure 1 - Functional scheme of the distributed computer control system of the marshaling yard in real-time

We assume that RTCS performs a set of r-transactions

$$R = \{r_i,\ i = \overline{1, N_r}\} \tag{1}$$

on the initiative signals

$$S = \{s_i,\ i = \overline{1, N_r}\} \tag{2}$$

received in RTCS from sensors of ObjW [2] and culminating in the issuance of control actions (signals) *U:*

$$U = \{u_k,\ k = \overline{1, N_u}\} \tag{3}$$

to actuators of automation and (or) messages to peripheral equipment X to the operational personnel of the ObjW:

$$X_d = \{x_{dl},\ l = \overline{1, N_d}\} \tag{4}$$

Let's consider the features of r-transactions. Example of r-transaction r_i is shown in Fig. 1.:

1) A r-transaction in RTCS consists from an indivisible and non-recoverable sequence of tasks (functional-algorithmic and program blocks - FPB):

$$\overline{F} = \{\mathrm{F}_j,\ j = \overline{1, N_{\mathrm{F}f}}\} \tag{5}$$

2) FPBs are characterized by a set of parameters, which are presented in Table 1;
3) Each r-transaction has a time limit for its execution (deadline)

$$\overline{T}_{dl} = \{t_{dlk},\ k = \overline{1, N_u}\} \tag{6}$$

4) The r-transaction is started at a certain intensity, which is determined by the dynamics of ObjW [2]:

$$\overline{\Lambda} = \{\lambda_i,\ i = \overline{1, N_r}\} \tag{7}$$

5) And the r-transaction can be estimated execution time (processing) on the microprocessor μ for all variants of its completion

$$\overline{T}_{\mathrm{o}\mu} = \{t_{oi\mu\mathrm{k}},\ k = \overline{1, N_u}\} \tag{8}$$

6) Each r-transaction uses information from the database of RTCS, which consists of m_i arrays of O_i MB each.

$$D = \sum_{g=1}^{G_m} m_g(O_g) \tag{9}$$

When a r-transaction is executed, each of its FPBs (5) accesses to arrays of database and the volume of data used for the k-th output of the i-th r-transaction is d_{ik} which is part of the total size D. The diagram in Fig. 1 shows examples of computing J r-transaction and examples of related information flows:

- information flows associated with certain FPBs to database arrays,

$$\lambda_j * p_{35} * k_{5,1} * O_1 * op_{j,5,1} \tag{10}$$

$$\lambda_j * k_{17,1} * O_1 * op_{j,17,1} \tag{11}$$

ISBN 978-3-949059-99-5

- information message flows to workstations

$$\lambda_j p_{35} Q_{2j}, \quad \lambda_j Q_{1j}, \quad \lambda_j Q_{3j} \tag{12}$$

- signal flows through OCD

$$16 * p_{32} * \lambda_j, \quad 16 * \lambda_j \tag{13}$$

Comments to formulas 10-13:

- Q_{1j} is the volume of the information message in bytes;
- $k_{17,1}$ - utilization factor of the part of the array Q_1 FPB F17;
- 16 bits - control action coding

3.2. A numerical example

The reliability of the RTCS application software, i.e. FPB, in the process of operation under interference conditions will be estimated by the probability of failure-free/problem-free execution of each r-transaction *i* for each variant *k* of its completion. It is taken proportional to the duration of execution of each command in tacts.

For example, the register command mov, is executed for one clock, and its failure rate is assumed to be equal to the failure rate of one chip. The failure rate of other commands will be calculated according to the scheme of the clock cycle (Table 1).

Thus, the reliability of the application software is possible to calculate as

$$p_{ik}(t_{oik}) = k_{\text{av}ik} = k_{ik}^{db} \times (1 - \exp(-\alpha_{ik} \times t_{oik})) - \tag{14}$$

As a rule, when designing a RTCS indicates the required values of the availability factors $\tilde{k}_{\text{av}ik}$, at the same time, the condition $k_{\text{av}ik} \geq \tilde{k}_{\text{av}ik}$ must be met.

For the entire system (for a microprocessor μ), the following expression is true

Three types of microprocessors with different clock speeds on a set of commands differing in the number of processor clock cycles were investigated. The single-cycle command error rate was selected on the basis of the data set out [11, 12, 18] (Table 2).

In an architectural project [1] for a real-time computer system for an automated control system for a marshalling yard (Figure 1), the algorithms for its operation were described using several thousand *r*-transactions.

Each *r*-transaction consisted of several dozen tasks, the complexity of which was assessed by the number of the four main types of machine instructions. In the example three independent *r*-transactions were chosen, each with a deadline time limit set by the experts (Table 3).

 ISBN 978-3-949059-99-5

Table 1 - Initial Characteristics of the FPB

Command Set	Number of Commands in FPB of β				Number of Cycles and Failure Rate of Commands α_η
	F1	***F2***	**…**	F_{N_f}	
1. mov	k11	k21	…	kN_f1	$1(\alpha_{\min})$
2. add	k12	k22	…	kN_f2	$1(\alpha_{\min})$
3. mult	k13	k23	…	kN_f3	18 $(n3\times\alpha_{\min})$
4. div	k14	k24	…	kN_f4	24 $(n4\times\alpha_{\min})$
β …	…	…	…	…	$n\beta$ $(n\beta\times\alpha_{\min})$ …
K_{com}….	k1 K_{com}	k2 K_{com}	…	kN_f K_{com}	$nK_{com}\times\alpha_{\min}$

Table 2 - Characteristics of microprocessor commands

Commands	**Number of command execution cycles** $\alpha_{\eta=1,2,3,4}$		
	μ_1	μ_2	μ_3
1. mov	1	1	1
2. mult	13	10	10
3. div	24	20	20
4. add	1	1	1
ω_μ, (MHz)	400	1400	2400
Single-cycle command failure rate (1/hour)			0,0007

Conclusions

The proposed set of basic simple table heuristic models for assessing the stability of real-time control systems operating under conditions of external radio-electronic interference can serve as a basis not only for assessing the stability of systems but also for solving other optimization problems.

Table 3 - Number of commands per r-transaction (4)

r_i	r_{i+1}	r_{i+2}
3 999 391	2 531 928	6 071 863
r-transaction processing time (µs)		
8362	7226	8230
Number of clock cycles per r –transaction (1/sec)		
3 999 391	2 531 928	6 071 863
12 700 600	8 811 109	20 048 451
10 298 987	5 152 149	11 853 051
6 768 295	3 819 965	6 328 894
Total number of short commands		
33 767 272	20 315 150	44 302 259
Deadline time (µs)		
184000	237000	217000
Probability of transaction execution file without failures		
$p_{1k}(t_{o1k})$	$p_{2k}(t_{o2k})$	$p_{3k}(t_{o3k})$
0,946579	0,971861	0,931557
0,986590	0,993031	0,982910
0,992155	0,995929	0,989995

The question of optimization of *r*-transaction structures remains open. In the literature, there are known methods of solving such problems for algorithmic structures. However, their application is problematic at the early stages of control system design due to the complexity of processing a large number of r-transactions and the lack of accurate algorithms for FPB implementation. The table formalisation of models proposed in this paper allows us to automate the process of preliminary assessment of the stability of real-time control system operation under electromagnetic interference conditions.

Acknowledgment

The presented work was approbated in the process of implementation of a number of projects, in the development of which the masters of the Department of Computer Systems and Technologies of the Dnepropetrovsk Institute of Infrastructure and Transport, which is a part of the Ukrainian State University of Science and Technology, took part. The collection and design of research results and multiple editing of the text was helped by Pavlo Ivin, senior lecturer of the Department of Electronic Computing Machines, for which the authors express their gratitude. The authors are grateful for the support of the work to the Dean of the Faculty of CTS, Associate Professor Vladimir Malovichko.