# Evaluation of availability of cluster distributed disaster tolerant systems for control and information processing based on a cluster quorum

**R Yu Tsarev[1], D V Gruzenkin[1], I V Kovalev[2], A V Prokopenko[1], A N Knyazkov[1]**
[1] Siberian Federal University, Russia
79, Svobodny Prospect, Krasnoyarsk, Russia
[2] Siberian State Aerospace University named after Academician M.F. Reshetnev
31 "Krasnoyarskiy Rabochiy" prospect, Krasnoyarsk, 660014, Russia

E-mail: rtsarev@sfu-kras.ru

**Abstract.** Control and information processing systems, which often executes critical functions, must satisfy requirements not only of fault tolerance, but also of disaster tolerance. Cluster architecture is reasonable to be applied to provide disaster tolerance of these systems. In this case clusters are separate control and information processing centers united by means of communication channels. Thus, clusters are a single hardware resource interacting with each other to achieve system objectives. Remote cluster positioning allows ensuring system availability and disaster tolerance even in case of some units' failures or a whole cluster crash. A technique for evaluation of availability of cluster distributed systems for control and information processing based on a cluster quorum is presented in the paper. This technique can be applied to different cluster distributed control and information processing systems, claimed to be based on the disaster tolerance principles. In the article we discuss a communications satellite system as an example of a cluster distributed disaster tolerant control and information processing system. Evaluation of availability of the communications satellite system is provided. Possible scenarios of communications satellite system cluster-based components failures were analyzed. The analysis made it possible to choose the best way to implement the cluster structure for a distributed control and information processing system.

## 1. Introduction

Developing modern control and information processing systems requires high dependability of both software and hardware. There are a lot of areas of science and industry where system failure can lead to essential economical loss and bring damage to people's health and lives [1]. These areas are banks and finance, space and defense industry, underwater and underground research, nuclear and chemical industries [2].

In this connection one of the main problems is elaboration of such approaches and techniques for control and information processing system design, that could provide system tolerance to software and hardware failures and guarantee fault tolerant solution, that main objective is to preserve data and continue functioning in conditions of mass and, probably, consecutive system failures [3], [4], [5].

The technology of failure handling in this case requires considering structure component interconnection and system ability to react specifically on possible sequence and combination of events leading to system failure with the purpose of providing maximum data security [6].

Wilkins et al. claim in [7], that clustering of computer systems to increase application availability has become a common industry practice. For accurate functioning of cluster distributed control and information processing systems used by big companies and corporations, disaster tolerant solution should be found. By "disaster tolerant solution" is meant the set of software and hardware configurations, settings parameters and organizational arrangements, that in total provide critically important data security and possibility for continuing the work of the system in case of occurring cataclysms leading to partial or complete destruction of the system [8], [9], [10]. As a rule, there are two (or more) datacenters for control and information processing connected by redundant communication channels and distributed into large distances which are enough for the possible catastrophe would not touch both datacenters at once. Configuration and structure of each datacenter's hardware and software can differ.

Design and development of control and information processing systems, the disaster tolerance of which is provided with the distributed cluster architecture, demands considering various parameters such as cost, which depends on configuration and geographical remoteness of datacenters, requirements to integrity and rate of the system recovery, frequency of inspections for compliance with system and procedures requirements [8], [10], [11].

In this work the problem of disaster tolerance assurance of distributed control and information processing system based on cluster system structure is considered. Here is presented the result of analysis of different failure scenarios of cluster distributed control and information processing system' components, which allows evaluating availability of the system and its disaster tolerance.

## 2. Concept of cluster quorum

In [12] cluster quorum is mentioned as a dynamic characteristic, the value of which presents the cluster integrity at the current moment. For the cluster structure of distributed control and information processing system let us define cluster quorum as a minimal integrity of the cluster, in conditions of which it remains operable.

Cluster quorum is a percentage characteristic, which implies minimal cluster part capable of coping with tasks given. If the value of cluster quorum is 40%, this means that if 60% of a cluster crush, the cluster is still able to work steadily. In that way, in the ideal case cluster quorum equals 0%.

For calculating cluster quorum value each cluster node is set a weight by an expert. After that according to the weights the "importance equivalent" is calculated for each node. Then the variants of cluster integrity disruption are composed with an appropriate workability value. Minimal operable integrity value is taken for cluster quorum.

## 3. Results and discussions

Availability analysis was implemented with the help of program complex for analysis of availability and control of the development of cluster structures for automated control systems designed by the authors [13]. This complex can be implemented for designing new cluster distributed control and information processing systems and for development cluster structures of currently existing systems. Functional purpose of the program complex is an analysis of different cluster structures of a distributed control and information processing system, detection of different system components' failure scenarios, and evaluation of availability of control and information processing systems and their disaster tolerance.

The purpose of the program complex is in designing and visualising of cluster structure of a distributed control and information processing system, analysis of different cluster structures of the system and providing support for decision making when choosing the cluster structure of the system.

Let us consider several cluster structure failure scenarios by the example of communications satellite system [14]. It is supposed that cluster structure of distributed control system for a communications satellite system with four datacenters is needed.

When designing and developing the cluster structure of a communications satellite system the most important parameters are dates and expenses spent on it. Two variants of implementation were considered.

According to the first one, the system includes four datacenters, in the first and the third of which there are three computer nodes, in the second and fourth of which there are two computer nodes and three arbitrators, the dates of realization – 365 days, budget – $1 500 000.

According to the second variant, the system includes four datacenters, in each of which there are two computing nodes, two arbitrators, construction period – 240 days, budget – $1 100 000.

Arbitrator is a full-function system, which is a part of a cluster; it accomplishes unity and synchronizing role for all other nodes [7]. Dynamic characteristic which is calculated every time when the cluster node fails is a cluster quorum defining cluster's integrity.

Table 1 presents some failure scenarios of components of the cluster distributed communications satellite system implemented according to the first variant. In Table 1 the column "Out of order" presents components unavailable for current scenario. Unfortunately, the article format does not allow presenting all the failure scenarios.

**Table 1.** Cluster distributed communications satellite system failure scenarios.

| Scenario number | Out of order | Failed components | Cluster integrity | Components left | Consequences |
|---|---|---|---|---|---|
| 1 | None | None | 100% | 13 out of 13 | |
| 2 | None | Arbitrator 1 | 92% | 12 out of 13 | No consequences |
| 3 | None | Arbitrator 2 | 92% | 12 out of 13 | No consequences |
| 4 | None | Arbitrator 1, arbitrator 2 | 84% | 11 out of 13 | No consequences |
| 5 | None | Arbitrator 2, arbitrator 3 | 84% | 11 out of 13 | No consequences |
| … | … | … | … | … | … |
| 959598 | Node 2, node 3, node 9, node 10, arbitrator 2 | Node 1, node 4, node 6, node 7, node 8, arbitrator 3 | 25% | 2 out of 8 | Cluster is stopped |
| 959599 | Node 2, node3, node 9, node 10, arbitrator 2 | Node 1, node 4, node 6, node 7, node 8, arbitrator 1 | 25% | 2 out of 8 | Cluster is stopped |
| … | … | … | … | … | … |
| 1594322 | Node 1, node 2, node 3, node 4, node 5, node 6, node 7, node 8, node 9, node 10, arbitrator 1, arbitrator 2 | Arbitrator 3 | 0% | 0 out of 1 | Cluster is stopped |
| 1594323 | Node 1, node 2, node 3, node 4, node 5, node 6, node 7, node 8, node 9, node 10, arbitrator 1, arbitrator 2, arbitrator 3 | None | 0% | 0 out of 0 | |

Analysis of two different variants of construction of cluster structure for the communications satellite system indicates that the first variant includes 1 594 323 different failure scenarios, in 239 748 of which a cluster stops working completely. This means that 15,04% of failure scenarios lead to the whole communications satellite system failure. The second variant includes 59 049 scenarios, 17 668 of which lead to cluster stopping, that makes 29,92% of scenarios. In the first variant $1 500 000 were spent, while in the second variant $1 100 000 were spent, which is 36,36% less. Thus, it is reasonable to implement cluster structure of the communications satellite system according to the first variant.

## 4. Conclusions

Ensuring disaster tolerance of control and information processing systems has been an important problem since the systems of this class began to be applied in critical areas. The use of cluster structure in control and information processing systems with geographically distantly located datacenters allows implementing its functional objectives even in case of catastrophic occasions leading to the failures of components or clusters of the system.

In this article the analysis of cluster distributed control and information processing system is presented. We considered a communications satellite system as an example of a cluster distributed control and information processing system.

The communications satellite system consisted of different computing nodes and datacenters. The analysis of communications satellite system availability was made with the program complex designed by the authors. On the basis of this analysis the more preferable variant of communications satellite system cluster structure can be selected.

The proposed technique for evaluation of availability of a cluster distributed control and information processing system can be applied in designing and modernizing different distributed systems for control and information processing, where disaster tolerance is required.

## 5. References


[1] Knight J C 2002 Safety critical systems: Challenges and directions *Proc. of Int. Conf. on Software Engineering* pp. 547-550

[2] Sommerville I 2011 *Software engineering* (New York: Pearson, Addison-Wesley)

[3] Fekih A 2015 Fault tolerant control design for complex systems: Current advances and open research problems *Proc. of the IEEE Int. Conf. on Industrial Technology* pp. 1007-1012

[4] Rehman S, Kriebel F, Shafique M and Henkel J 2014 Reliability-driven software transformations for unreliable hardware *IEEE Trans. Comput.-Aided Design Integr. Circuits Syst.* **33** 1597-1610

[5] Kulyagin V A, Tsarev R Yu, Prokopenko A V, Nikiforov A Yu and Kovalev I V 2015 N-version design of fault-tolerant control software for communications satellite system *Int. Siberian Conf. on Control and Communications, SIBCON 2015 - Proc.* art. no. 7147116

[6] Tekinerdogan B, Sozer H and Aksit M 2008 Software architecture reliability analysis using failure scenarios," *J. Syst. Software* **81** 558-575

[7] Wilkins R S, Du X, Cochran R A and Popp M 2002 Disaster tolerant Wolfpack geo-clusters *Proc. - IEEE Int. Conf. on Cluster Computing, ICCC* pp 222-227

[8] Nguyen T A, Kim D S and Park J S 2016 Availability modeling and analysis of a data center for disaster tolerance *Future Gener. Comp. Sy.* **56** 27-50

[9] Sen A, Mazumder A, Banerjee S, Das A, Zhou C and Shirazipourazad S 2015 Region-based fault-tolerant distributed file storage system design in networks *Networks* **66** 380-395.

[10] Yao W-B, Zhao L, Wang Z, Yao X and Han S 2015 Research on disaster tolerant information system modeling and simulation *Beijing Youdian Daxue Xuebao/Journal of Beijing University of Posts and Telecommunications* **38** 50-54

[11] Qiu Z and Perez J F 2015 Enhancing reliability and response times via replication in computing clusters *Proc. of IEEE INFOCOM* pp 1355-1363

[12] Özsu M T and Valduriez P 2011 *Principles of Distributed Database Systems* (New York: Springer-Verlag)
[13] Glotov A K, Kovalev I V, Tsarev R Yu, Zavyalova O I, Rusakov M A, Kapulin D V and Kovalev D I 2012 Program complex for analysis of dependability and control of the development of cluster structures for automated control systems *Federal service for intellectual property (Rospatent)* certificate no. 2012614895 31.05.2012 Moscow Russia.
[14] Chernigovskiy A S, Tsarev R Yu and Knyazkov A N 2015 Hu's algorithm application for task scheduling in N-version software for satellite communications control systems *Int. Siberian Conf. on Control and Communications, SIBCON 2015 – Proc.* art. no. 7147270