Availability as a Cloud Service for Control System of Critical Energy Infrastructure

Oleg Ivanchenko[1][0000-0002-5921-5757], Vyacheslav Kharchenko[2][0000-0001-5352-077X], Borys Moroz[1][0000-0002-5625-0864], Leonid Kabak[1][0000-0001-6267-1772], Kyrylo Smoktii[3][0000-0002-5647-1712], Yuriy Ponochovnyi[4][0000-0002-6856-2013]

[1] University of Customs and Finance, Dnipro, Ukraine

vmsu12@gmail.com, moroz.boris.1948@gmail.com, kabak.leo@gmail.com

[2] National Aerospace University "KhAI", Kharkiv, Ukraine

v.kharchenko@csn.khai.edu

[3] Vasyl' Stus Donetsk National University, Vinnytsia, Ukraine

smoktii@gmail.com

[4]Poltava National Technical University named after Yurij Kondratyuk, Poltava, Ukraine

pnch1@rambler.ru

Abstract. The increasing of energy consumptions and attempts to use Management and Control System based on cloud computing technologies for ensuring normal work of the critical energy infrastructure (CEI) are made serious demands for analyzing Infrastructure as a Service (IaaS) Cloud availability level. In this paper, a new perspective unified platform for determining of availability level of the IaaS Cloud pertaining to the information components of the CEI is described. In fact Semi-Markov Modeling Process for assess of overall availability level of the IaaS Cloud with multiple pools of physical and virtual machines based on a novel Availability as a Cloud Service platform in order to improve effectiveness of CEI was presented by authors.

Keywords: Infrastructure as a Service Cloud, Control System of Critical Energy Infrastructure, Availability as a Cloud Service.

1 Introduction

Nowadays cloud computing are improving the world by giving users powerful, scalable computer and information resources, flexible management, enormous storage units for big data etc. It is generally agreed today that migration process of information and computer resources from classical information technologies domain into clouds is the best way in order to achieve the positive results in science, education, production and business. This trend also continues for critical infrastructures (CIs).

One argument in support of cloud computing systems and technologies mission is leveraged two Amazon EC2 data centers and Amazon VPC in the GridCloud project sponsored by the U.S. Dept. of Energy, ARPA-E GENI program, Cornell University and Washington State University. In fact, group of scientists have applied Amazon cloud resource in order to ensure information canals between GridCloud cluster and data center [1,2]. Perhaps inspired by ARPA program, let's try to use this approach in order to solve task of effective usage of the critical energy infrastructure (CEI) based on perspective platform, which is seen as cloud service supporting the work of Control System of CEI. Our main assignment is ensuring of high availability level Infrastructure as a Service (IaaS) Cloud and Control System of CEI. Before begin to consider main theoretical and practical aspects of Availability as a Cloud Service (AaaCS) issue, we will perform analysis of works and achievements into cloud computing systems domain, including some possibilities of leveraging the cloud computing as a mission for CEI.

To begin with availability and reliability of CEI. In [3] authors performed analysis of different types of vulnerabilities and threats pertaining to the critical infrastructures components, authors offered quite effective measures in order to address those negative impacts. Specific emphasis was put on effectiveness of SCADA system and automation of management of the renewable energy devices based on wireless sensor networks. Relevant mathematical models based on the principles of analysis and availability assessments of critical infrastructures were presented by authors in [4]. Important aspects of determining availability level of software different systems, considering the rejuvenation policy based on Semi-Markov modeling process (SMP) are illustrated authors in [5]. Similar models can be used for determining availability level of CEI components.

It is clear that Non-Markovian approaches and models for assess of the availability level CEI and IaaS Cloud play an important role, because these infrastructures have complex regimes and states functioning of their components. Therefore, some groups of scientists' leverage SMP models in order to reliability and availability level for different systems in preference to Markovian approach. In [6] authors have described one of the most popular Non-Markovian approach, which researchers and specialists into domain of the critical computing can use in order to determining availability level of separate CEI components and as well as overall availability level of the CI.

Nowadays different deliberate malicious impacts are the biggest threat for cyber assets CEI and IaaS Cloud. In [7] different types of failures, including hidden failures for physical machines (PMs) of the IaaS Cloud with multiple pools have been modeled by authors in order to determine overall availability level of the cloud infrastructure. This task was being solved based SMP approach. In spite of the fact, that durations of time for CEI and IaaS Cloud are combination of random and deterministic values, one should, however, not forget that some experts point out that if the complex systems are components with a great variety of subsystems, then researchers can employ assumption that all times are exponential distributed. In this case researchers can be used Markov models. Turning to Markovian approach, take into account practical and theoretical significance of the work [8]. In this work authors have presented solution of the task pertaining to the overall availability level of IaaS Cloud with multiple pools of physical machines. Solution was gotten based on Continuous Time Markov Chains (CTMC). In this context, let's keep to consider researches relating to the survivability modeling of cloud service in distributed data center. In [9] authors performed analysis of cloud service survivability with the usage of closed-form solutions [8] based on CTMC. Experience availability pertaining to the software-defined cloud computing was submitted by authors in [10], too. At the same times the scientific paper [11] discussed the most important aspects of the implementation and submit of a graphical web-based application, that allows users and vendors of cloud computing systems to determine reliability level for different types of cloud using Monte Carlo simulation.

This paper was drafted according to the following structure. In Section II main theoretical aspects and practical provisions to develop and implement the cloud oriented service for critical energy infrastructure based on usage of definite Semi-Markov availability models are presented. Conclusions and discussions were set out in Section III.

2 Some Fundamental Provisions of Availability as a Cloud Service for Control System of Critical Energy Infrastructure

2.1 Overall Provisions of Availability as a Cloud Service

The initial purpose of the researches has been to get analytical product (PRDaaS) in order to create cloud service for control system (CS) of CEI. However, development trends of CEI and IaaS Cloud gave the opportunity to move on towards the procedure as a service (PRCaaS). After that users and researchers have detected serious issues as regards the availability for cloud infrastructure. For instance, events related to the disruption of Amazon Simple Storage Service (S3), Amazon Elastic Compute Cloud (EC2) and Amazon Elastic Block Store (EBS) in February 2017 [12] have confirmed our apprehensions. Since, nowadays largest cloud service providers consider availability is one of the most vital significant property of cloud infrastructure, let's also try to focus on this property. Next, the transition was implemented from Procedure as a Service to the Property as a Service (PRPaaS) and different combinations for PRPaaS were considered. Our logical chain for generalized service $XaaS$ can be written as:

$$XaaS = \{PRDaaS, PRCaaS, PRPaaS\}. \tag{1}$$

In accordance with (1), generalized operator X is given the following combination for set of products, observed processes, properties or attributes:

$$X = \{Product(Hardware, Software, Infrastructure, Platform), Process(Monitoring,$$

$$Testing, Technical\ and\ Information\ States\ Control, Communications), Property/$$

$$Attribute(Reliability, Faulttolerability, Availability, Security)\}. \tag{2}$$

Thus, our main goal is development of unified cloud oriented platform, that will work according to overall logical chain (1), (2). Where necessary, the logical chain (1), (2) can be extended and supplemented other products, procedures, processes and properties. For instance, according to (2) content of Product can be extended if vendor will try to take into account different critical systems, considering their how components of CEI.

2.2 Development of the Cloud Platform with Feature of Availability as a Service

Let's begin with considering of features' set, that should be performed by using cloud computing. Figure 1 shows taxonomy of ensuring the Availability as a Cloud Service for CS of CEI.

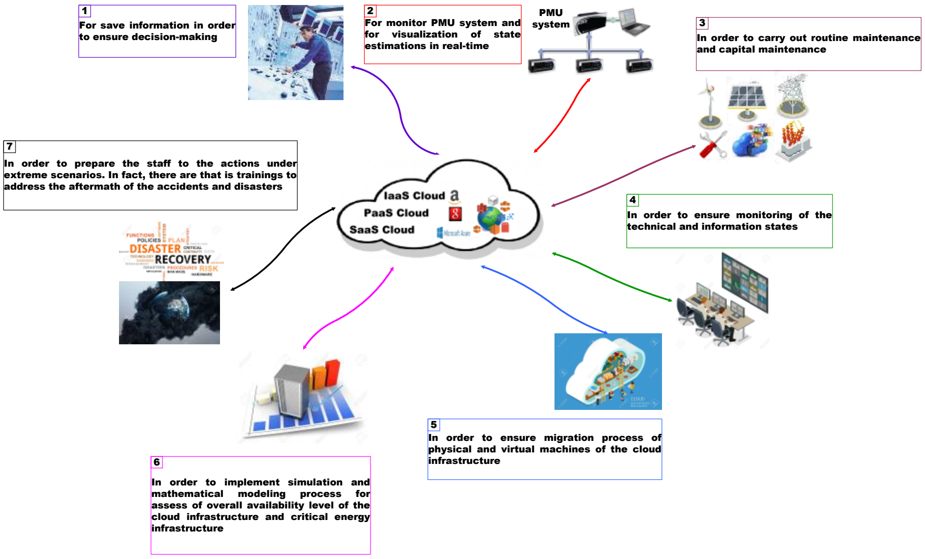

1
For save information in order to ensure decision-making
2
For monitor PMU system and for visualization of state estimations in real-time
PMU system
3
In order to carry out routine maintenance and capital maintenance
7
In order to prepare the staff to the actions under extreme scenarios. In fact, there are trainings to address the aftermath of the accidents and disasters
IaaS Cloud
PaaS Cloud
SaaS Cloud
4
In order to ensure monitoring of the technical and information states
DISASTER
RECOVERY
RISK
PLAN
POLICIES
FUNCTIONS
5
In order to ensure migration process of physical and virtual machines of the cloud infrastructure
6
In order to implement simulation and mathematical modeling process for assess of overall availability level of the cloud infrastructure and critical energy infrastructure

Fig. 1. Taxonomy of ensuring the Availability as a Cloud Service for CS of CEI

The architecture of cloud computing system should be built in accordance with the Fig. 1. However, the separation of features for cloud core (CLC) and cloud platform (CLP) is necessary and suitable. Indeed, better if researchers would be able to introduce the separation of features for cloud core and cloud platform in terms of ensuring availability requirements for control system of CEI and IaaS Cloud. Table 1 shows separation of features for CLC and CLP with availability as a service. Next step is representation of architecture in order to deliver availability as a service for critical energy infrastructure.

In order to develop concrete architecture familiar practical experience, related to implementation appropriate projects should be considered. Note that the division on types and models of the cloud computing systems in the field of scientific researches is acquired purely a formal character. It means that hardly worth following the strong rules and norms for building of cloud system's architecture. We consider, that in this case creative attitude is played large and important role.

Table 1. Separation of features for CLC and CLP with Availability as a Service

Number	Assignment of Features	Cloud Core	Cloud Platform
1.	In order to prepare the staff to the actions under extreme scenarios. In fact, there are that is trainings to address the aftermath of the accidents and disasters	✓	
2.	For save information in order to ensure decision-making	✓	
3.	For monitoring and visualization of states in real-time using Phasor Measurements Units (PMU) system	✓	
4.	In order to carry out routine maintenance and capital maintenance		✓
5.	In order to ensure monitoring of the technical and information states		✓
6.	In order to ensure migration process of physical and virtual machines of the cloud infrastructure		✓
7.	In order to implement simulation and mathematical modeling process for assess of overall availability level of the cloud infrastructure and critical energy infrastructure		✓

While developing the CLP with feature of AaaS, it is significant to be clear about which type of cloud computing system better to use for perform the features of CLC and CLP. Familiar experience prompt us that as a core can be used public cloud. At the same time, considering specific tasks and issues, as a platform can be leveraged private cloud. Perhaps inspired by investigations of the scientists from Washington State University and Cornell University [1,2], researches of availability based on hybrid cloud architecture will as well be tried to perform by us. Figure 2 is illustrated overall simplified architecture for this service. As indicated in Fig. 2 by applying both types of clouds, can be proceeded to the hybrid architecture. In this situation, hybrid cloud architecture provides more accurate and immediate decisions and as well supports authorized deduplication in order to ensure cybersecurity requirements [13]. What is more, famous decisions for hybrid cloud architectures embrace energy company's different applications and its need to protect cyber assets by using authentication procedure. The activity of cybersecurity partners also plays an important role for the promotion of quality of service for a lot cloud computing users. Nowadays most of all energy companies is vital part of critical energy infrastructure and need to solve serious problems, that related to the data processing. There are problems as follows: a) need to improve efficiency CEI based on implementations of big data procedures; b) management larger and larger information domains, such as IoT, PMU, wireless sensor network, SCADA system; c) number of information technologies and integration applications are climbing fast.

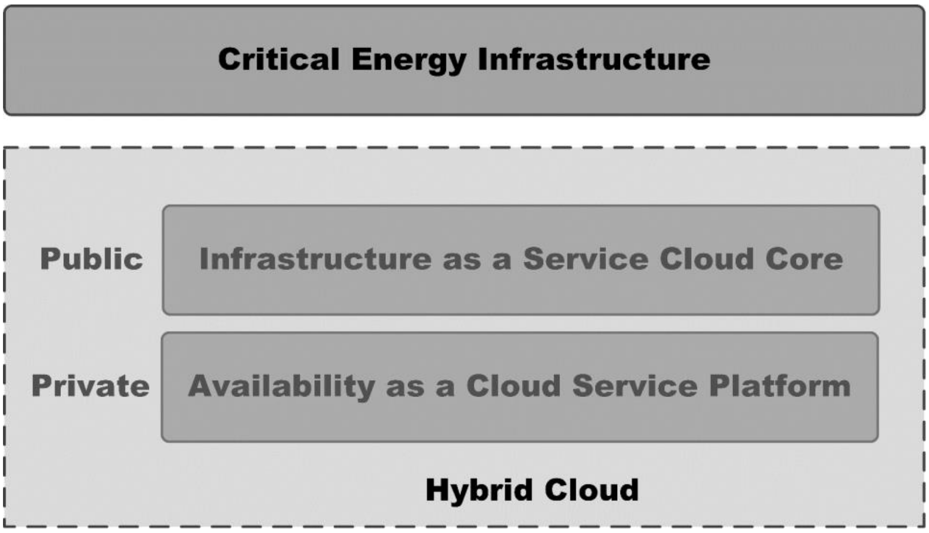

Critical Energy Infrastructure
Public
Infrastructure as a Service Cloud Core
Private
Availability as a Cloud Service Platform
Hybrid Cloud

Fig. 2. Overall simplified architecture of the Availability as a Cloud Service for CS of CEI

Figure 3 shows hybrid cloud architecture (HCA) with feature of Availability as a Service. In accordance with Fig. 3 HCA includes five clearly defined layers, namely Critical Energy Infrastructure, Microservice Operation System, Infrastructure as a Service Cloud Core, Application Program Interfaces, Availability as a Cloud Service Platform. Furthermore, Module of Authentication and Virtual Private Network are important components of the HCA. A summary of some of the characteristics is summarized below.

Control system of CEI contains as famous so new components. Traditionally, SCADA system is system which designed for supervision and data acquisition of substations of CEI located over large and distant geographic areas [3]. PMU consist of three applications, such as Power System Monitoring, Power System Protection and Power System Control [14]. In fact, PMU is system of accurate phase measurements. Nets of Internet of Things (IoT) and Wireless Sensor Network are constituted the basis of modern measurements technologies based on achievements of Internet. Digital information from these devices are inputted out into Service Router of the Microservice OS.

Microservice OS includes suite of some modular services in order to build quite large applications. Each module supports a specific business goal and uses a simple, well-defined interface to communicate with other sets of services [15]. Since cloud computing apply greater volumes of the information, therefore next component is servers for processing big data. Software (SW) Hadoop MapReduce is an open source implementation of MapReduce framework that processes vast amounts of data in parallel on clustered computers [16]. Hadoop Distributed File System, Kafka and Spark technologies belong to the Hadoop Big Data Platform and leverage for quick cloud computing operations. This platform solves different tasks based on SW Hadoop Map Reduce. Suppose, according to Figure 2 data stream from PMU are delivered to Amazon S3.

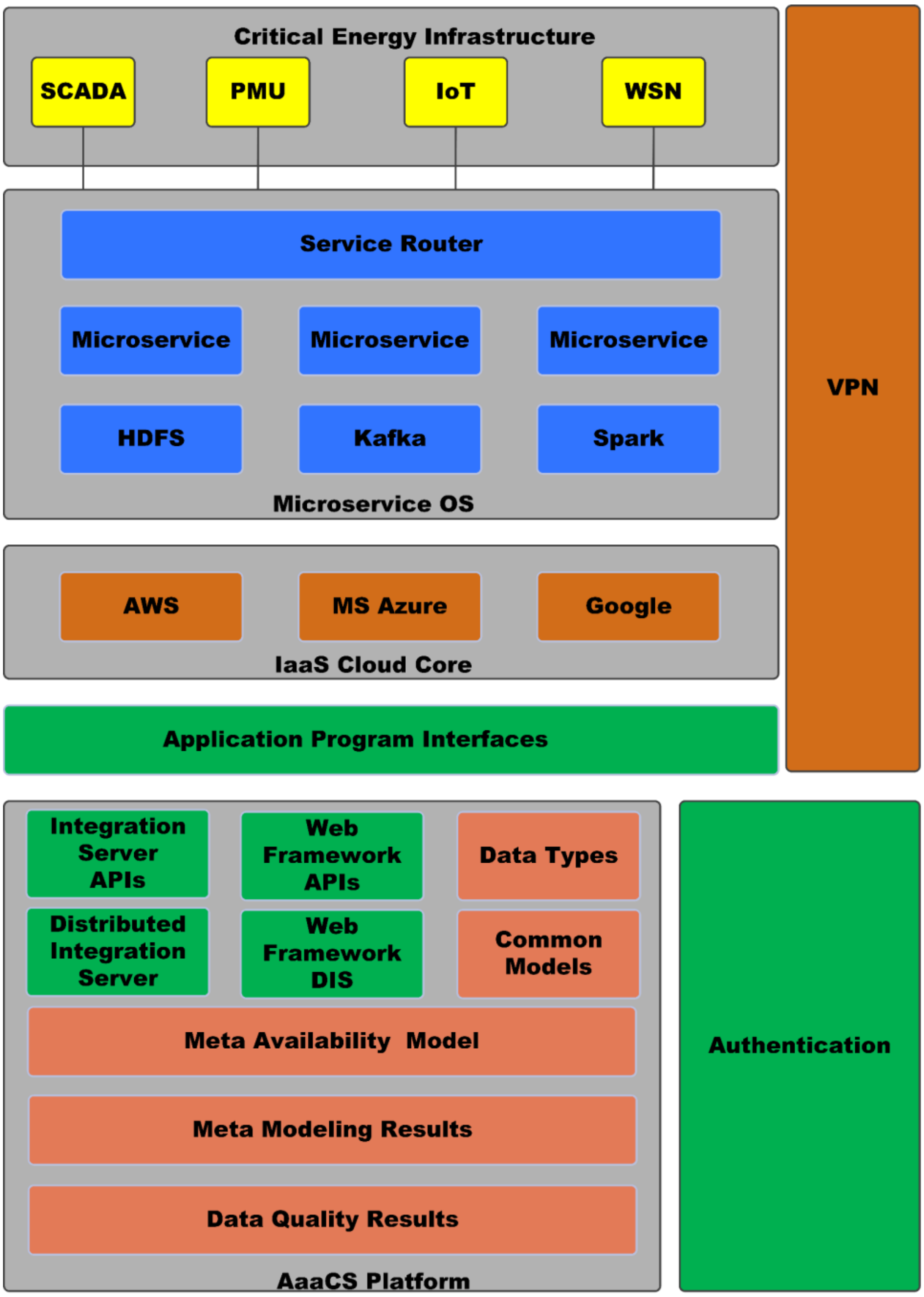


Fig. 3. Hybrid cloud architecture with feature of Availability as a Service

Services of Amazon S3, Amazon EC2 perform computations, taking place in the compute cloud and the results are delivered to the operational grid [2] of the Critical Energy

Infrastructure. Amazon Virtual Private Network (VPN) is used as transportation infrastructure. Furthermore, data stream as input dates is delivered through Application Program Interfaces (APIs) to the AaaCS Platform. Need also take into account, that access requirements for ensuring of appropriate cybersecurity level are supported by special authentication module.

Nowadays Disaster Recovery (DR) is as well one of the most widely submitted technique of ensuring availability requirement for IaaS Cloud. In this regard, replication of data from one cloud service provider (CSP) to the others is quite effective procedure for disaster recovery implementation. Therefore, if needed data stream can be delivered to storage units and cloud computing nodes of other CSPs, namely Microsoft and Google. Next, data stream transforms into special data types by using Integration Server APIs, Distributed Integration Server (DIS), Web Framework AIPs and DIS. These models are applied by staff of CS for CEI in order to solve tasks in accordance with Table 1 for Critical Energy Infrastructure's components. Tasks for overall CEI, including IaaS Cloud can be solved by using modules Meta Availability Model and Meta Modeling Results.

As a result, can be made a conclusion, that a quite large part of the Common Models module (Fig. 3) can be presented by Markov and SMP models. As an illustration, can be considered SMP approach based on familiar theoretical provisions pertaining to the usage embedded Markov chains [7,17]. Traditionally can be assumed that SMP availability model contains three pools of PMs [8]. The researchers can also be assumed, that cloud infrastructure is equipped with Technical and Information States Monitoring System (TIMS), which works in different regimes and can provide migration, repair operations for unavailable PMs. Indeed, in separate situations the TIMS system already the ability to perform functionalities of Physical Machines Monitor in order to detect different negative events pertaining to the deliberate malicious impacts. Determining the availability level as steady state probability for IaaS Cloud or CEI was conducted using a famous equation [6]:

$$A_{SS} = \sum_{i=1}^{m} \pi_i \, , \tag{3}$$

where π_i – steady state probability for available states of IaaS Cloud or CEI; m – overall number of available states of the IaaS Cloud or CEI.

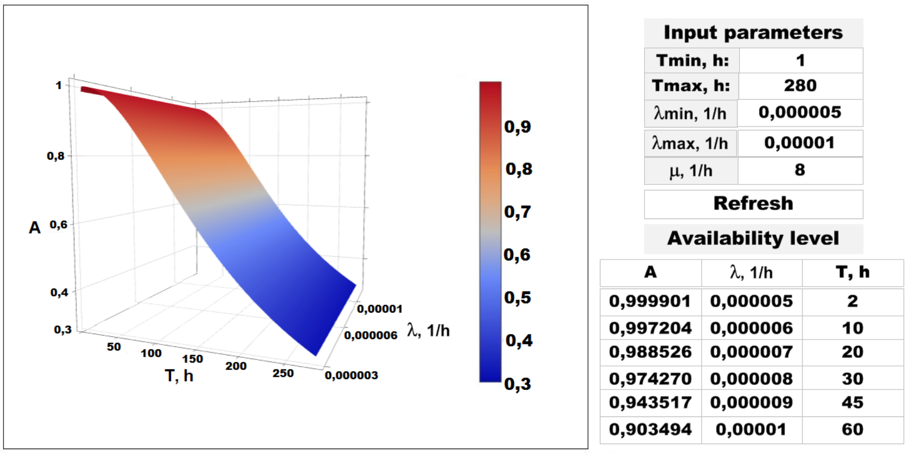
Intermediate parameters' values in order to determine steady state probabilities π_i can be written as [7,17,18]:

$$P_{ij}(\infty) = p_{ij} = \int_0^{\infty} \prod_{\ell \neq i} \left[1 - Q_{i\ell}(\theta)\right] \, dQ_{ij}(\theta), \tag{4}$$

$$h_i = \int_0^{\infty} \left[1 - F_i(\theta)\right] \, d\theta, \tag{5}$$

where p_{ij} – elements of transition probability matrix $P = \left| p_{ij} \right|$; h_j – mean sojourn times [19] for all states of SMP availability model; $Q_{i\ell}(\theta)$, $Q_{ij}(\theta)$ – cumulative distribution function for transition from state i to states ℓ and j for IaaS Cloud or CEI [18]; $F_i(\theta)$ – distribution function of sojourn time in state i for IaaS Cloud or CEI [18].

As an example, Figures 4, 5 are illustrated SMP modeling results for IaaS Cloud with multiple pools of physical machines.



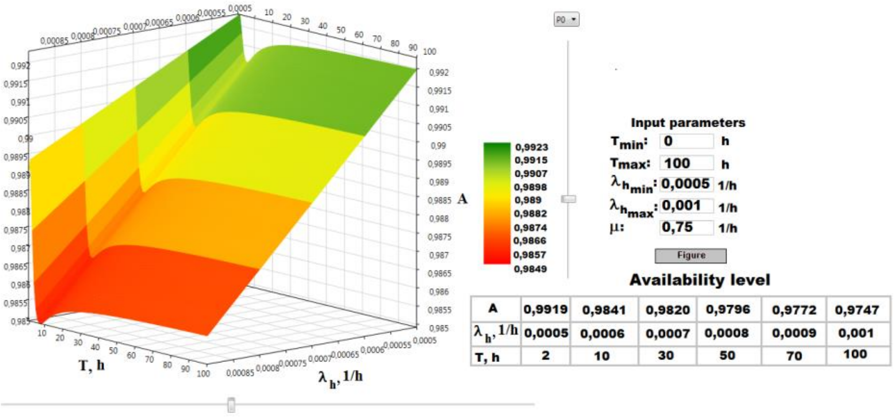
Input parameters	
Tmin, h:	1
Tmax, h:	280
λmin, 1/h	0,000005
λmax, 1/h	0,00001
μ, 1/h	8

Refresh

Availability level

A	λ, 1/h	T, h
0,999901	0,000005	2
0,997204	0,000006	10
0,988526	0,000007	20
0,974270	0,000008	30
0,943517	0,000009	45
0,903494	0,00001	60

Fig. 4. Availability modeling results for $T = 280$ h, $\mu = 8$ 1/h [7]



Input parameters

T_{min}:	0	h
T_{max}:	100	h
$\lambda_{h_{min}}$:	0,0005	1/h
$\lambda_{h_{max}}$:	0,001	1/h
μ:	0,75	1/h

Figure

Availability level

A	0,9919	0,9841	0,9820	0,9796	0,9772	0,9747
λ_h, 1/h	0,0005	0,0006	0,0007	0,0008	0,0009	0,001
T, h	2	10	30	50	70	100

Fig. 5. Availability modeling results for $T = 100$ h, $\mu = 0{,}75$ 1/h [17]

The special situations considering the deliberate malicious impacts on physical and information resources of the cloud infrastructure are as well as great interest, since preliminary mathematical modeling results can be employed in order to development of preventive measures both for IaaS Cloud and CEI. Take into consideration, that implementation of migration processes of the information resources for PMs based on using of monitoring system for IaaS Cloud and PMU system for CEI is one of the most effective measure for overcome issues pertaining to the deliberate malicious impacts. Figure 6 is presented modeling results of overall availability level for cloud infrastructure based on SMP which considers double deliberate malicious impacts on information resources of the PMs. Modeling results are received for IaaS Cloud with multiple pools of PMs for different rates λ_3 and λ_4 of double malicious impacts, namely 1 – when $\lambda_3/\lambda_4 = 0{,}2$; 2 – when $\lambda_3/\lambda_4 = 0{,}21$; 3 – when $\lambda_3/\lambda_4 = 0{,}22$; 4 – when $\lambda_3/\lambda_4 = 0{,}235$; 5 – when $\lambda_3/\lambda_4 = 0{,}25$ [20].

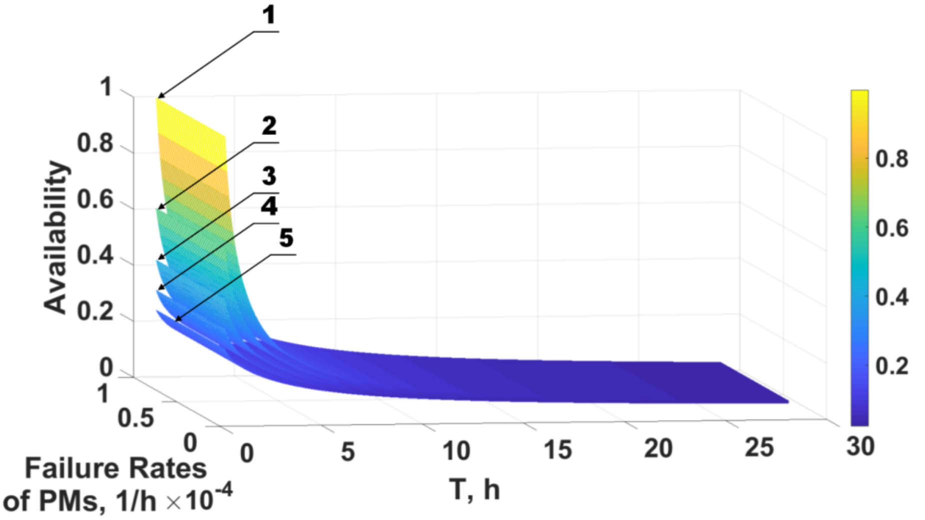


Fig. 6. Availability modeling results for double deliberate malicious impacts on information resources of the IaaS Cloud with multiple pools of PMs [20]

Thus, in order to assess overall availability level of CS for CEI, including IaaS Cloud, users and vendors of cloud services can leverage the web resource proposed, hosted on the AaaCS Platform.

3 Conclusions and Discussions

This paper explores a serious issue of ensuring availability of the Control System for Critical Energy Infrastructure considering different components that impact on effectiveness CEI. Cloud platform in order to assess overall availability of the CS for CEI was proposed by authors. Theoretical provisions of proposed cloud technology are based on famous mathematical and simulation modeling provisions. In spite of the fact, offered cloud platform was practically proposed for CEI, authors did not try to describe process of ensuring the close relationship between critical energy infrastructure and IaaS Cloud. Main task was considered as description of the concrete cloud platform architecture, presentation of mathematical availability modeling possibilities for IaaS Cloud based on SMP and as well as rationale of the appropriate future researches in this domain.

Some problems related to the optimization procedures of operational regimes and architecture IaaS Cloud can be overcome, using proposed toolkit. The described AaaCS platform will be extended to solve tasks pertaining to the other important properties of CEI and IaaS Cloud.

References

1. Bakken, D., Smart Grids: Clouds, Communications, Open Source, and Automation. CRC Press (2014).
2. Hauser, C., et al. Cloud Data Sharing Platform (S-67G). Final project report. PSERC Publication 16–05 (2016).
3. Alcaraz, C., and Sherali Z. Critical infrastructure protection: Requirements and challenges for the 21st century. In International journal of critical infrastructure protection, vol. 8, pp. 53–66 (2015).
4. Ivanchenko, O., Kharchenko, V., and Skatkov, A. Management of critical infrastructures Based on Technical Megastate. In an International Journal: Information and Security. Critical Infrastructures Safety and Security, vol. 28, no. 1, pp. 37–51 (2012).
5. Xie, W., Hong, Y., and Trivedi, K. Analysis of a two-level software rejuvenation policy. In Reliability Engineering & System Safety, vol. 87, no. 1, pp. 13–22 (2005).
6. Distefano, S., and Trivedi, K. Non-Markovian State-Space Models in Dependability Evaluation. In Quality and Reliability Engineering International, vol. 29, no. 2, pp. 225–239 (2013).
7. Ivanchenko, O., Kharchenko, V., Ponochovny, Yu., Blindyuk, I., Smoktii, O. Semi-Markov Availability Model for Infrastructure as a Service Cloud Considering Hidden Failures of Physical Machines. In Proceedings of the 13th International Conference on ICT in Education, Research and Industrial Applications. Integration, Harmonization and Knowledge Transfer, ICTERI, Kyiv, Ukraine, May 15-18, pp. 634–644 (2017).
8. Ghosh, R., Longo, F., Frattini, F., Russo, S., and Trivedi, K. S. Scalable analytics for IaaS cloud availability. In IEEE Transactions on Cloud Computing, vol. 2, no. 1, pp. 57–70 (2014).
9. Chen, Z., Chang, X., Han, Z., and Li, L. Survivability Modeling and Analysis of Cloud Service in Distributed Data Centers. In The Computer Journal, pp. 1–10 (2017).
10. Cai, B. L., Zhang, R. Q., Zhou, X. B., Zhao, L. P., & Li, K. Q. Experience availability: tail-latency oriented availability in software-defined cloud computing. In Journal of Computer Science and Technology, vol. 32, no. 2, pp. 250–257 (2017).
11. Snyder, B., Green, R. C., Devabhaktuni, V., and Alam, M. ReliaCloud-NS: A scalable web-based simulation platform for evaluating the reliability of cloud computing systems. In Software: Practice and Experience, vol. 48, no. 3, pp. 665–680 (2018).
12. Summary of the Amazon S3 Service Disruption in the Northern Virginia (US-EAST-1) Region, March 2018. [Online]. Available: https://aws.amazon.com/ru/message/41926/.

13. Li, J., Li, Y. K., Chen, X., Lee, P. P., & Lou, W. A hybrid cloud approach for secure authorized deduplication. In IEEE Transactions on Parallel and Distributed Systems, vol. 26, no. 5, pp. 1206–1216 (2015).
14. De La Ree, J., Centeno, V., Thorp, J. S., and Phadke, A. G. Synchronized phasor measurement applications in power systems. In IEEE Transactions on smart grid, vol. 1., no. 1, pp. 20–27 (2010).
15. How to explain microservices in plain English, March 2018. [Online]. Available: https://enterprisersproject.com/article/2017/8/how-explain-microservices-plain-english.
16. Machida, F., Xiang, J., Tadano, K., and Maeno, Y. (2012, November). Aging-related bugs in cloud computing software. In Software Reliability Engineering Workshops (ISSREW), IEEE 23rd International Symposium on, pp. 287–292 (2012).
17. Ivanchenko, O., and Kharchenko, V. Semi-Markov Availability Models for an Infrastructure as a Service Cloud with Multiple Pools. In Proceedings of the 12th International Conference on ICT in Education, Research and Industrial Applications, ICTERI, Kyiv, Ukraine, June 21-24, pp. 349–360 (2016).
18. Ivanchenko, O., Lovyagin, V., Maschenko, E., Skatkov, A., Shevchenko, V.: Distributed critical systems and infrastructures. National Aerospace University named after N. Zhukovsky “KhAI”, Kharkiv (2013).
19. Vinayk, R., Dharmaraja, S. Semi-Markov Modeling Approach for Deteriorating Systems with Preventive Maintenance. In: International Journal of Performability Engineering, vol. 8, no. 5, pp. 515–526 (2012).
20. Ivanchenko, O., Kharchenko, V., Moroz, B., Kabak, L. and Smoktii, K. Semi-Markov availability model considering deliberate malicious impacts on an Infrastructure-as-a-Service Cloud. In Advanced Trends in Radioelecrtronics, Telecommunications and Computer Engineering (TCSET), 14th International Conference IEEE, Slavske, Ukraine, February 20-24, pp. 570–573 (2018).