Usage of Service-Oriented Architecture for Developing Prototype of Intelligence Information System

Jugoslav Achkoski [1], Vladimir Trajkovik[2]

[1]*Military Academy "General Mihailo Apostolski", str. Vasko Karangeleski bb, 1000 Skopje, Macedonia*
[2] *Faculty of Computer Science and Engeneering, str. Rugjer Boshkovikj 16, P.O. Box 393 1000 Skopje, Macedonia*

***Abstract* – The level of technological development in society has influence on implementing contemporary technologies because benefits of using ICT make pressure on increasing level of development in society.**

In this paper we propose key points of usage of Service-Oriented Architecture for Developing Prototype of Intelligence Information System.

***Keywords* – Service-oriented architecture, Model of Intelligence Information System, Security standards, Metrics for service availability, service reliability and service response time, Intelligence.**

1. Introduction

Intelligence, as a public service, has a great significance for a country [1], [2]. Frequently used information systems, which support intelligence activities, have high influence in the decision making process. Contemporary information technology considerably contributes to the processes' (activities) improvement by supporting intelligence cycles (planning, collecting data, analyzing data and dissemination). Although, there is constant improvement in the field of information technology, significant advancement in the quality of work in the field of intelligence has not taken place in the last ten years [3], [4], [5].

According to NATO Glossary of Terms and Definitions (AAP-6) [6], processes or phases that are going in Intelligence are shown on Figure 1:

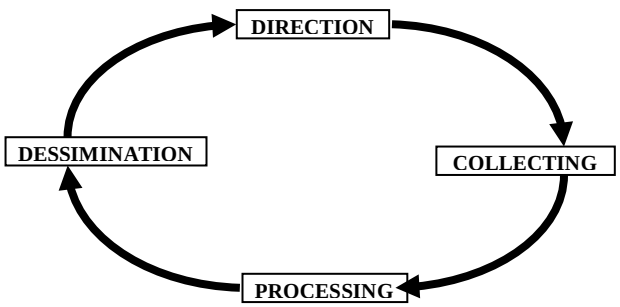


Figure 1. Intelligence cycle

Implementation of Service Oriented Architecture – SOA, [7] i.e. the usage of SOA provides possibilities for making new opportunities in the form of expanded solutions for designing intelligence [8], [9], [10], [11], [12] information systems, regarding the more efficient management of information, as well as their use by the end users for whom hum they are intended. In order to keep up with the pace with contemporary development, planning on short, medium and long term is needed for development of information systems for supporting intelligence [13], [14], [15], in relation to IT development.

Nowadays, as a response of challenges and better coordination, contemporary intelligence agencies have established teams for monitoring and responding on events to different locations with usage of modern IT solutions.

After the changing of the traditional hierarchical model in the target-centric model of intelligence, intelligence analysts as a part of the intelligence community are facing the need of new IT solutions, with one goal – achieving better intelligence products.

This contribution is divided on several sections. In the section 2 is presented concept for Intelligence Information System development using SOA. The section 3 and 4 explain our approach for developing metrics to evaluate services and information in information system. Also, we propose metrics for service availability and service reliability. In the section 5 are given concluding remarks.

2. Service-oriented architecture concept for Intelligence Information System development

Every modern intelligence system is based on some type of information system [18]. Usage of contemporary technology, especially Information Communication Technology (ICT), is giving more efficient execution of all phases of the intelligence service.

Such IIS achieves minimum requirements for designing services that are needed to be implemented in intelligence process with internal functions which can be processed from external IIS peer [19].

As result of system complexity solution is realized as a layer architecture model [20].

Web services are a possible solution to integration problems [7]. Information systems can be integrated, depending on the aim and function, with different web services they create. Web services are presented

with WSDL that firmly define communication interface [12], [21]. Web services are anticipated to be used in information systems integration on the method of peer-to-peer connecting.

The enterprise application integration usually means the sum of technologies that support the interoperability of separate information systems. The principal use of this concept is based on the integration of different enterprise applications and process automation. Because of that, the service oriented architecture represents the main platform for the existing application integration solutions [5], [22]. Application integration means building a system which consists of different software components which communicate among each other via standardized messages. Certain components of that system are called adapters and use the external components, which need to be integrated in the system.

The key difference between the broker architecture, which uses hub-and -spoke topology, and the bus topology is that the integration component, which performs the message transformation and their delivery, is distributed into the application adapters; also the bus architecture requires the application adapters to use the same platform as the original applications [3].

The figure (Figure 5) bellow shows one possible solution for Information Systems integration with the Intelligence Information System (IIS) [16].

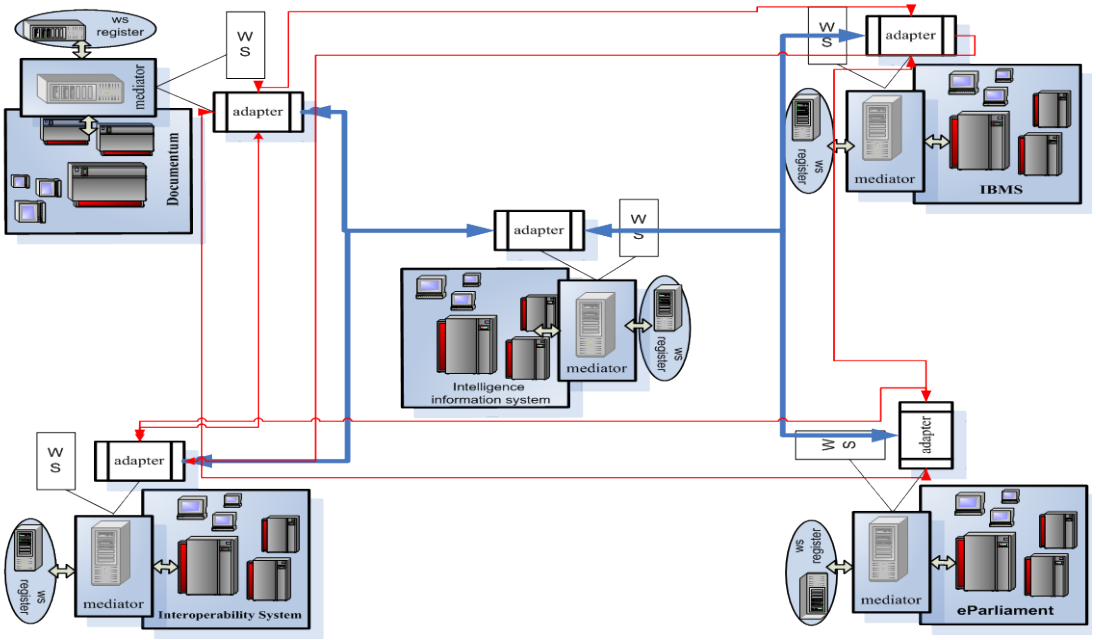


Figure 5. Information systems integration according to the peer-to-peer model

2.1 Model of Security Solution for Intelligence Information System-Based on SOA

Our model of security solution for intelligence information system-based on SOA [23], [24] is proposed on Figure 6. Figure 6 also presents: control flow (blue direction) and data flow (red direction)of the data in our model. XML Signature standard is used in control flow to validate security policies. XML Encryption is used in data flow to validate security policies.

In both cases information flow through three phases:

1. Request phase – identifying information requester and registering request with the purpose of establishing security mechanism;
2. Verification phase – identifying requester and its security mechanisms are appropriate for gaining response according to security policies related to information;
3. Notification phase – according to security mechanisms and policies, requester for information is notified for access to use information form services or requester is notified that access is denied sending forward cause in terms of security policy.

Requested information flows form source to the information requesters, going to mediation component which serves for connecting and formatting security systems in institutions. Mediation component is important for IIS, because it can be connected to more information systems which are embedded in heterogonous environment. Requested information is encrypted and it has unique security policy. Although IIS Center and System registry are not involved, they play important roles in control flow.

Control flow establishes three functions:

1. Recording information requester in terms of date and time, location and type of user who requests for information;

2. Validation to security policy of user type called requester of information and security policies attached to the information;
3. Recording each request which is not followed with information at moment of request. This third function is interested for information system designers on future services.

Highly structured suggested model of Security Solution for Intelligence Information System not only interpolates security a mechanism also provides by following:

- Effective data transmission endorsing data encryption and data formatting on appropriate level;
- Recording each request whether it is inserted in database or not, furthermore it has appropriate security policy or not. This supports recording possible disruption of security policy.
- Flexible scalable mechanisms and mechanisms for extending services which are located in IIS Registries.

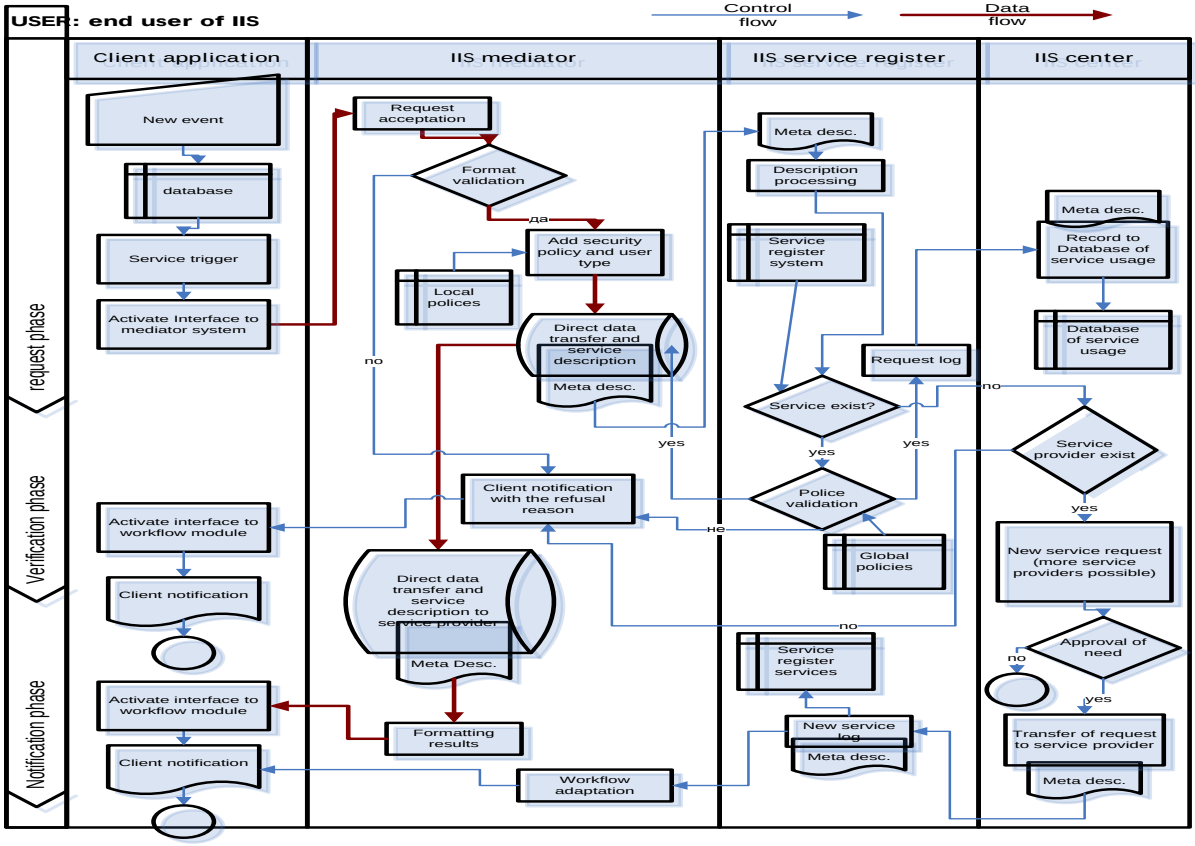


Figure 6. Model of Security Solution for Intelligence Information System

3. Metrics for intelligence information system model based on SOA

In order to conduct a proper service evaluation, appropriate methods for measuring should be used [25],[26]. The value that is obtained as a result of the measuring should be used as a referent parameter, indicating the size of the measured quantity.

Based on [25],[26], we define unifying metrics that will allow evaluation of some selected principles in SOA, such as unique categorization, discoverability, loose coupling and autonomy. These principles are typical for developing services in SOA. In the same context we introduce separate metrics for evaluating accessibility to certain intelligence information, assessment of intelligence information reliability and assessment of cost of information acquisition.

3.1 Metrics for Evaluating Services in SOA

A. Unique categorization is analyzed through four service indicators: business-oriented or technical functionality BT(s), agnostic and non-agnostic functionality AN(s), data superiority DS(s) and common business entity usage CB(s) [25]. Taking into consideration the desirable values of the given indicators, we introduce a unifying metric for services (or in a phase of service design, for service candidates), also called unique categorization K(s). The equations refer to each of the following four cases of functionality preferences:

A.1.Business-oriented BT(s), agnostic functionality AN(s):

$$K(s) = \frac{BT(s) + AN(s) + DS(s) + CB(s)}{4} \qquad (1)$$

A.2.Technical-oriented functionality BT(s), agnostic functionality AN(s):

$$K(s)=\frac{1-BT(s)+AN(s)+DS(s)+CB(s)}{4} \quad (2)$$

A.3.Business-oriented BT(s), non-agnostic functionality AN(s):

$$K(s)=\frac{1+BT(s)-AN(s)+DS(s)+CB(s)}{4} \quad (3)$$

A.4. Technical-oriented functionality BT(s), non-agnostic functionality AN(s):

$$K(s)=\frac{2-BT(s)-AN(s)+DS(s)+CB(s)}{4} \quad (4)$$

In each of these cases, the value of K(s) will be interpreted in the interval [0,1]. Furthermore, the desirable value for K(s), according to the preferred functionality, is the maximal value of 1.

B. *Discoverability*, in addition to being related to unique categorization, is described by the following indicators: *functional naming FN(sc)*, *functional naming compatibility CFN(sc)* and *information content IC(sc)*. These indicators are relevant for the process of service design, so they can only apply to service candidates. In order to define a discoverability metric **D(sc)** that will unify all of the mentioned indicators, we will firstly define the middle values for FN(sc) and CFN(sc) taking into account the appropriate values in relation to the *roles (R), operations (O), parameters (P), data types (T)* and *interfaces (I)*. We have:

$$FN(sc)=\frac{1}{5}[FN_R(sc)+FN_O(sc)+FN_P(sc)+FN_T(sc)+FN_I(sc)] \quad (5)$$

The discoverability metric for D(sc) can now be defined by:

$$D(sc)=\frac{FN(sc)+CFN(sc)+IC(sc)}{3} \quad (6)$$

The values of service candidate discoverability D(sc) will be interpreted in the interval [0,1]. A values of indicates that maximal service candidates discoverability D(s) has been achieved. On the other hand, a value of 0 indicates that discoverability is nonexistent.

C. *Loose coupling* is another principle in service oriented architecture. It contributes to increased scalability, flexibility, fault tolerance and maintainability of the architecture. Indicators that are relevant in this context are: *asynchronity of long-runing operations AS(s), common data types complexity CCT(s), abstraction of knowledge related to operations and parameters implementation AN(s)* and *(non)compensation of operations NC(s)*. Using these indicators, we define the unifying loose-coupling metric LC(s) in SOA by:

$$LC(s)=\frac{AS(s)+CCT(s)+AN(s)+NC(s)}{4} \quad (7)$$

We should note that here, is the middle value of the abstraction metrics, as calculated separately for the operations and the parameters.

The quality of loose coupling is maximal when the value of the given metric LC(s) is 1.

D. The quality of autonomy of services can be described by the indicators of direct service dependency SD(s) and functionality overlap FO(s). Since the degree of autonomy is reversely proportional to the values of service dependencies SD(s) and functionality overlap FO(s) metrics, we define the autonomy metric AU(s) in the following manner:

$$AU(s)=\frac{SD(s)+FO(s)}{SD(s)\cdot FO(s)} \quad (8)$$

The values for AU(s) that we obtain in this manner will be in the interval $[1,\infty]$. A value of 1 for AU(s) indicates lowest level autonomy. The greater the value of AU(s), the greater is the autonomy of the service. We should stress here that the value of AU(s) is unbounded from above.

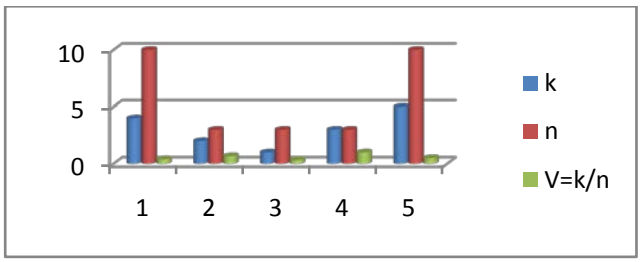
3.2 Metrics for Evaluating Services in Intelligence Information System

The reliability V of information collected by a certain service can be defined as the probability of accuracy for the particular information. It can be determined empirically according to:

$$V=\frac{k}{n} \quad (9)$$

Table 1. Reliability V of information collected by a certain service

k	n	V=k/n
4	10	0.40
2	3	0.67
1	3	0.33
3	3	1.00
5	10	0.50



where **n** presents the total number of information collected by designated service during some past period of time (consisting of one or more intelligence cycles) and **k** is the number of accurate (proven) information among them. It is clear that the possible values of **V** lie in the interval [0,1]. Given as such, V can be also considered as reliability of the service in question.

We are considering a SOA based information system that consists of **m** services with mutually independent functionality. The reliability of information in this system depends on the reliability of each of the services that information is collected from. If particular information is obtained from at least one of the previously activated services in the intelligence cycle, its *maximal reliability* V_{max} can be expressed as:

$$V_{max} = \max_{\substack{\chi(i)=1 \\ i=1,m}} \left\{ \chi_A(i) \cdot \frac{k_i}{n_i} \right\} \tag{10}$$

Here, the action of the authorities is presented by $\chi(i)$, the characteristic function of service activation,

$$\chi(i) = \begin{cases} 1 & \text{if the service is activated} \\ 0 & \text{if the service is not activated} \end{cases}$$

and $\chi_A(i)$ is the binary characterization function of the particular information

$$\chi_A(i) = \begin{cases} 1 & \text{if the information is obtatned by service "i"} \\ 0 & \text{if the information is not obtained by service "i"} \end{cases}$$

In order to optimize reliability analysis of collected data, the summary information should be broken down to elementary pieces of information. As previously, we express the emergence of elementary information by the binary characterization function. Thus, we evaluate *average reliability* V_E of each elementary information by the following equation:

$$V_E = \frac{\sum_{i=1}^{m} \chi(i) \chi_A(i) \cdot p_i}{\sum_{i=1}^{m} \chi(i)} \tag{11}$$

It can easily be noticed that values obtained in (10) and (11) depend on the set of activated services. This points that the reliability of collected information is significantly influenced by the decision process that precedes the activation of services. Namely, in order to increase the expected accuracy of the information, it is desirable to introduce criteria that will be applied in the process of decision making related to this issue.

A part of these criteria is the *information accessibility* of a service, which we will denote by **d.** The value of **d,** which belongs to the interval $[0,1]$, is estimated empirically using previous observations, assessments and known facts. A value of 0 for d indicates that the information in question is estimated to be unavailable for the service, and if $d = 1$ then information is estimated to be fully available for that service. Using this estimation, we can evaluate the a priori reliability AV_i for receiving accurate information from service **i**, according to the following formula:

$$(AV)_i = d_i \cdot p_i = \frac{d_i \cdot k_i}{n_i} \tag{12}$$

The maximal reliability for collecting accurate information by service **i** can be expressed as:

$$(AV)_{i\_max} = \max_{\substack{\chi(i)=1 \\ i=1,m}} \left\{ \frac{d_i k_i}{n_i} \right\} \tag{13}$$

while the expectation of getting accurate information from active services is given by:

$$V_E = \frac{\sum_{i=1}^{m} \chi(i)\, d_i\, p_i}{\sum_{i=1}^{m} \chi(i)} \tag{14}$$

The problem of maximal accuracy and accessibility of information by activating **s** out of **m** services is formalized by the following optimization problem:

$$\max_{\substack{S \in 2^m \\ |S|=s}} \left\{ \frac{1}{s} \cdot \sum_{i \in S} \frac{d_i k_i}{n_i} \right\} \tag{15}$$

where 2^m is the power set of $\{1,2,\ldots,m\}$.

The comparisons of the results from (1) and (3), and respectively from (2) and (4), can give a useful indication about the correctness of the decisions that have been made.

Another element that should be taken into consideration during the development phase is the *cost of information acquisition*. Its assessment should include not only the resource requirements, but also risks that can emerge during the process. For service **i,** it can be nominally expressed by a number $\mathbf{U_i}$. For more convenience these numbers can be normalized to u_i, thus having their values in [0,1]. Now we formulate $k_i = d_i / u_i$ as a *coefficient of acquisition* and apply it the following maximization program:

$$\max_{\substack{S\in 2^m \\ |S|=s}} \left\{ \frac{1}{s} \cdot \sum_{i\in S} \frac{d_i k_i}{n_i u_i} \right\} \quad (16)$$

The solution of this problem will yield the group of **s** services that can provide an optimal combination of accessibility and cost, in respect to the reliability of a certain elementary information.

Finally, Table 2 allows concluding that usage of services with the highest value for expectation of getting accurate information and the service with the highest value for information reliability is not always best approach for collecting information. These values refer to different service, respectively if one service has maximal value for information reliability, the same service does not have maximal value for expectation of getting accurate information.

Table 2. Calculation of the reliabilities for a received elementary information A

сервис	n_i	k_i	V_i (Vmax)	$\chi(i)$	$\chi_A(i)$	V_E	d_i	$(AV)_i$	$(AV)_E$
1	2	3	4=3/2	5	6	7=∑4/1	8	9=8*3/2	10=∑9/1
1	10	8	0.80	1	1		0.7	0.56	
2	9	5	0.56	1	0		0.85	0.47	
3	7	6	0.86	0	1		0.5	0.43	
4	5	2	0.40	1	1		0.3	0.12	
5	8	5	0.63	0	1		0.95	0.59	
6	2	1	0.50	0	0	**0.59**	0.9	0.45	**0.41**
7	6	4	0.67	1	0		0.95	0.63	
8	10	1	0.10	1	1		0.7	0.07	
9	3	2	0.67	0	1		0.4	0.27	
10	4	3	0.75	1	0		0.7	0.53	

n_i – total number of information received by service i
k_i – number of accurate information received by service i
V_i – reliability of the service i
$\chi(i)$ – activation indicator function of the service i (1= active, 0= inactive)
$\chi_A(i)$ – information receiving indicator function for the service i (1 = yes, 0 = no)
V_E – expected reliability of the information
d_i – accessibility of information for service i
$(AV)_i$ – probability for acquiring of accurate information from service i
$(AV)_E$ – expectance of acquiring accurate information from active services

To avoid existed shortcomings in Intelligence Information System, principle of Intelligence should be used. This principle refers to check reliability of collected Intelligence information from minimum three different sources of information. In our case, sources of intelligence information corresponded to services for collecting information in Intelligence Information System. Services that should be used in planning process for collecting information have to be selected in accordance with criteria for maximal value of expectation of getting accurate information.

However, it should be stressed that optimal usage of services in terms of probability of getting accurate information from certain services and information reliability as a product in analyzing process do not correspond with exploiting services that have maximal value by both parameters.

4. Metrics for service availability and service reliability development

Practical and expanded usage of SOA in software developed application is needed to avoid existing shortcomings. One solution is to define metrics for measuring performance of services.

However, current researches for service performance are not enough precise to be used in effective diagnoses that refer to SOA performance [27], [29].

As a result in the section are defined set of precise and practical metrics for measuring service performances. In order to be shown applicability and usefulness of these metrics they are implemented in a Intelligence Information System.

Defined metrics in this section refer to set of metrics for service availability and reliability that are part of Intelligence Information System. Metrics answer on users requirements when they sent a query to services for particular information.

4.1 Service States in Information System - Based on SOA

Generally, each information system that is based on service-oriented architecture depends of services states in particular time moment.

Term service state can be defined as a service activity when request from user/users is sent to service provider for using services. According to this, it is possible to be introduced measurement that can measure service activity. If a service is active then can be used measurement "1". If service is not active then can be used measurement "0".

When request is received by the service provider and service responses on received request then service state is defined as an active state of service and service has activity "1". If service does not response on received request, that state is defined as an inactive service state and service has activity "0".

Number of states in information system that is based on SOA, no matter where they are implemented and what is the purpose of the system, it depends of services state on each separately service that is a integral component of information system.

In order to be estimated number of possible services states in an information system, that depends of service state whether it has activity "1" or "0", we can introduce equation of variation:

$$V_n^k = n(n-1)\dots(n-k+1) \qquad (17)$$

$n -$ number of services in infromation system
$k -$ number of service states [0,1]

If equation (17) is used for presenting information system that is composed of services that can be in both states [0,1], as an example can be introduced following equations:

$$n = 3 \text{ и } k = [0,1]; \qquad V_3^2 = 3(3-1) = 12$$

$$n = 5 \text{ и } k = [0,1]; \qquad V_5^2 = 5(5-1) = 20$$

$$n = 7 \text{ и } k = [0,1]; \qquad V_7^2 = 7(7-1) = 42$$

Elaborated example allows to be concluded that possible states of services grow exponentially depending of number of active services when client request are received.

Importance of determining number of services states has influence on analyzing QoS metric in service-oriented information system.

4.2 Service Availability

Availability is service attribute that describes whether or not service is active or available after received request by a user. More precise estimation of service availability can be done on services that are frequently exploited in short time intervals [28].

Unavailability of services in service-oriented information system is related to different type of errors, failures, fixing computer networks, changing software components that are used from service provider or service [30]. Presumption that information system or services in certain period of time are founded in one of numerous service states whether or not services are unavailable or available allows implementing Markov' models. Markov' models are functions that have two variables: service state X(t) and observation time "t" of information system. Depending of variable values and variable types – discrete or continual – Markov' models can have different character (Markov' chains and Markov' processes). To determinate service availability and reliability, Markov' processes should be composed of variable for service state X(t) that should be of discrete type and time variable "t" that should be of continual type.

In order to analyze service availability, we introduce Markov' models that have countable number of states. Examples of this type of model are the processes of dying and thriving that are used as a model for describing different natural and technical systems.

Analysis for service availability can be based on assumption that availability for services is defined with discrete service states X(t) which means that probability of service transition in other state is equal to result of multiplication by constant λ with time interval Δt when services is founded in state "i" in the time moment t and it transfers in state "j" in time moment t+Δt. Constant "λ" represents number of events in time unit. In a case of service reliability and service availability "λ" is intensity of unavailability or number of service unavailability in time unit.

In the same manner, it is possible to define probability of returning in the previous service state. For example, if services were in state "j" in time interval t, then probability of services to be in state "i" in time interval t+Δt is equal to multiplication of constant μ and time interval Δt. Constant μ represent intensity of availability or number of service availability in time unit.

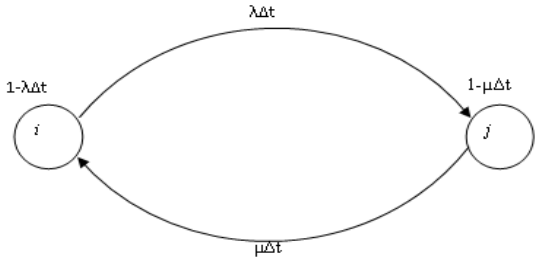


Figure 7. Diagram of transition using different states

Probability in certain time interval that refers to not happen events or service is still in a state "i" after time interval Δt is equal to sum of probability between probability when service was in state "i" in

time moment t ($P_i\ (1 - \lambda\Delta t)$) and probability when service transits from state "j" in time moment t in state "i" in time moment t+Δt ($P_j(\mu\Delta t)$).

$$P_i\ (t + \Delta t) = P_i\ (t)\ (1 - \lambda\Delta t) + P_j\ (t)\mu\Delta t \qquad (18)$$

Probability when service is in state "j" in time interval t+Δt is equal to sum of probability when services was in state "j" in moment "t" ($P_j\ (1 - \mu\Delta t)$)and probability when service transits from state "i" in time moment t, in state "j" in time moment t+Δt ($P_i\ (\lambda\Delta t)$)

$$P_j\ (t + \Delta t) = P_i\ (t)\ (\lambda\Delta t) + P_j\ (t)(1 - \mu\Delta t) \qquad (19)$$

We are planning to research service availability in certain time interval [0, t], where numerous requests are received from different users.

We introduce assumption that service can be found in both states where states can be modeled with Markov' models. First service state refers to assumption that service can respond to client request or more request in certain time moment "t". According to this assumption, service is available or active for using by the service clients. That service state can be marked as an "i".

If service transits in inactive state and it is unavailable for service clients then service state can be marked as "j". (see Figure 7)

Both cases refer to service states marked as "i" and "j" when service is available or unavailable for using. For better presentation of service availability in service-oriented information systems, it is needed to be introduced more service' states for explaining service behavior on appropriate manner.

Service states that can be explained refer to state which services can be found in certain time moment when probability of receiving service response is equal to probability that service does not receive service response. For that reason, we are introducing state "z" that refers to service state when service processing request from service client. As a result of service transitions from one state to another state, it is possible to be concluded that probability of service to be found in state when service response to client request is equal to probability that client does not receive response from service. If client receives service response then service is founding in state "x". If service client does not receive service response then service is founding in state "y" and service transits from state "z" to state "y".

According to previously mentioned, transition states can be represented by diagram presented on Figure 8.

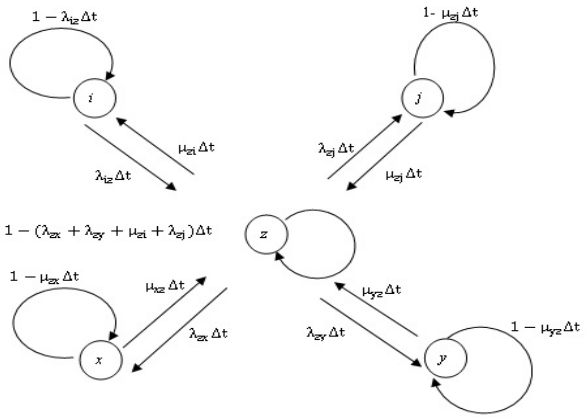


Figure 8. Diagram of transition for service availability

Because state "x" is identical with state "i" which means that service transits from state "z" in certain time moment in active state and it is available for using. As a result both states are overlapping between each other. According to this, state "x" can be replaced with state "i"

State "y" is identical to state "j" which means that service transits from "z" in certain time moment in inactive state and it is unavailable for using. As a result both states are overlapping between each other. In that case, state "y" can be replaced with state "j".

Replacing states afford optimization of transition diagram. There is possibility to avoid complex equations that are created as result of using Markov' models. Simplified transition diagram is given on Figure 9.

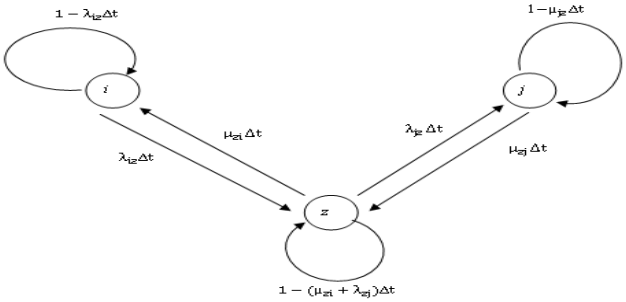


Figure 9. Simplified diagram of transition for service availability

Using simplified transition diagram, equations for probabilities $P_i(t + \Delta t)$, $P_z(t + \Delta t)$ and $P_j\ (t + \Delta t)$ when services are found in different states can be described with formulas (20),(21) and (22).

*)$P_i(t + \Delta t)$, when service is in state "i",

$$P_i\ (t + \Delta t) = (1 - \lambda_{iz}\Delta t)P_i\ (t) + P_z\ (t)\mu_{zi}\Delta t \qquad (20)$$

*)$P_z(t + \Delta t)$, when service is in state "z",

$$P_z(t + \Delta t) = P_i(t)\ \lambda_{iz}\Delta t + P_z\ (t)\big(1 - (\mu_{zi} + \lambda_{zj})\Delta t\big) + P_j\ (t)\mu_{zj}\Delta t \qquad (21)$$

*)$P_j\ (t + \Delta t)$, when service is in state "j",

$$P_j(t+\Delta t) = P_z(t)\,\lambda_{jz}\Delta t + P_j(t)(1-\mu_{jz}\Delta t) \qquad (22)$$

Function for service availability in certain time moment is presented by following equation:

$$A(t) = \left(1 - \frac{\lambda_{iz}\lambda_{jz}}{r_2 r_1}\right) - \frac{\lambda_{iz}\lambda_{jz}}{r_1 - r_2}\left(\frac{e^{r_1 t}}{r_1} - \frac{e^{r_2 t}}{r_2}\right) \qquad (23)$$

4.3 Service Reliability

Function of service reliability represents probability of service processing in certain time interval [0,t]. Intensity when service is not available for using can be presented with constant value λ=const.

A Usage of Markov' model is the most convenient for examination service reliability. Service states where service can be found are "i" and "j". When service is in state "j", it is inactive or unavailable for using. When service is in state "i", it is active or available for using. We exanimate service reliability in time interval [0,t].

Probability that service can be found in state "i" in time moment (t+Δt) is equal to multiplication of probability $P_i(t)$ which means that service can be found in state "i" in time moment "t" and probability of service when it is available for using in time interval "Δt" or "1-λΔt" .

$$P_i(t+\Delta t) = (1-\lambda\Delta t)P_i(t) \qquad (24)$$

Probability that services in time moment (t+Δt) can be found in state "j" is equal to sum of probabilities that services can be found in state "i" in time moment "t" with probability$P_i(t)$, and multiplication of probability "λΔt"that service is unavailable for using in time moment "Δt" and probability $P_j(t)$ that means service can wait in state "j" when it is in time interval "Δt"

$$P_j(t+\Delta t) = \lambda\Delta t P_i(t) + P_j(t) \qquad (25)$$

Our research refers to examination of service reliability and availability in certain time interval [0, t], when numerous request are received in information system from different users.

We use assumption that service can be found in both states where states can be modeled with Markov' models. First service state refers to assumption that service can respond to client request or more requests in certain time moment "t". According to this assumption, service is available or active for using by the service clients. That service state can be marked as an "i".

If service transits in inactive state and it is unavailable for service clients then service state can be marked as "j".

Both cases refer to service states marked as "i" and "j" when service is available or unavailable for using which are mentioned in previous section. For better presentation of service reliability in service-oriented information systems, we need to introduce more service states for explaining service behavior on appropriate manner.

Service states that can be explained refer to state which services can be found in certain time moment when probability of receiving service response is equal to probability that service does not receive service response. For that reason, we are introducing state "z" that refers to service state when service processing request from service client. As a result of service transitions from one state to another, it is possible to be concluded that probability of service to be found in state when service response to client request is equal to probability that client does not receive response from service. If client receives service response then service is found in state "x". If service client does not receive service response then service is found in state "y" and service transits from state "z" to state "y". State "x" is identical with state "i" which means that service transits from state "z" in certain time in active state and it is available for using. As a result both states are overlapping each other. According to this, state "x" can be replaced with state "i"

State "y" is identical to state "j" which means that service transits from "z" in certain time in inactive state and it is unavailable for using. As a result both states are overlapping each other. So that, state "y" can be replaced with state "j".

By using approach similar to the one we used for service availability, transition states can be represented by diagram given on Figure 10:

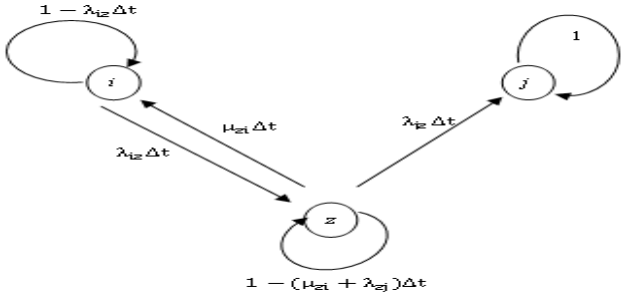


Figure 10. Diagram of transition in case of service realibility

Therefore equations for probabilities $P_i(t+\Delta t)$, $P_z(t+\Delta t)$ and $P_j(t+\Delta t)$ when services are found in different states should be resolved by following:

*)$P_i(t+\Delta t)$, when service is in state "i",

$$P_i(t+\Delta t) = (1-\lambda_{iz}\Delta t)P_i(t) + P_z(t)\mu_{zi}\Delta t \qquad (26)$$

*)$P_z(t+\Delta t)$, when service is in state "z",

$$P_z(t+\Delta t) = P_i(t)\,\lambda_{iz}\Delta t + P_z(t)\left(1-\left(\mu_{zi}+\lambda_{zj}\right)\Delta t\right) \quad (27)$$

*)$P_j(t+\Delta t)$, when service is in state "j",

$$P_j(t+\Delta t) = P_z(t)\,\lambda_{jz}\Delta t + P_j(t) \quad (28)$$

Function for service reliability in certain time is presented by following equation:

$$R(t) = \frac{r_1+\mu_{zi}+\lambda_{zj}+\lambda_{iz}}{(r_1-r_2)}e^{r_1 t} - \frac{\mu_{zi}+\lambda_{zj}+r_2+\lambda_{iz}}{(r_1-r_2)}e^{r_2 t} \quad (30)$$

Business process (Figure 11) that is used for presenting functionality of Intelligence Information System shows that intelligence operation should not be launched if in the information system does not have approval for launching that operation. Approval should be authorized by Intelligence authorities or other stakeholders in Intelligence community according to Intelligence procedures and law.

If intelligence operation is not approved by authorities then it finishes immediately, because of sensitivity in Intelligence.

If Intelligence operation is approved by authorities for certain Intelligence target then business process continues on next steps. Next step is determination of position and time on Intelligence target. In our case study, Intelligence operation refers to follow Intelligence target.

Position of Intelligence target can be determinate when services that are components of Intelligence Information System or peers of external service providers are activated.

Other services can be exploited to determinate target positions that are used as an external peer of Intelligence Information System. Using services from external peers refers to future of Intelligence which means that in a future is possible to be exploited services that will be on a higher level than at this moment.

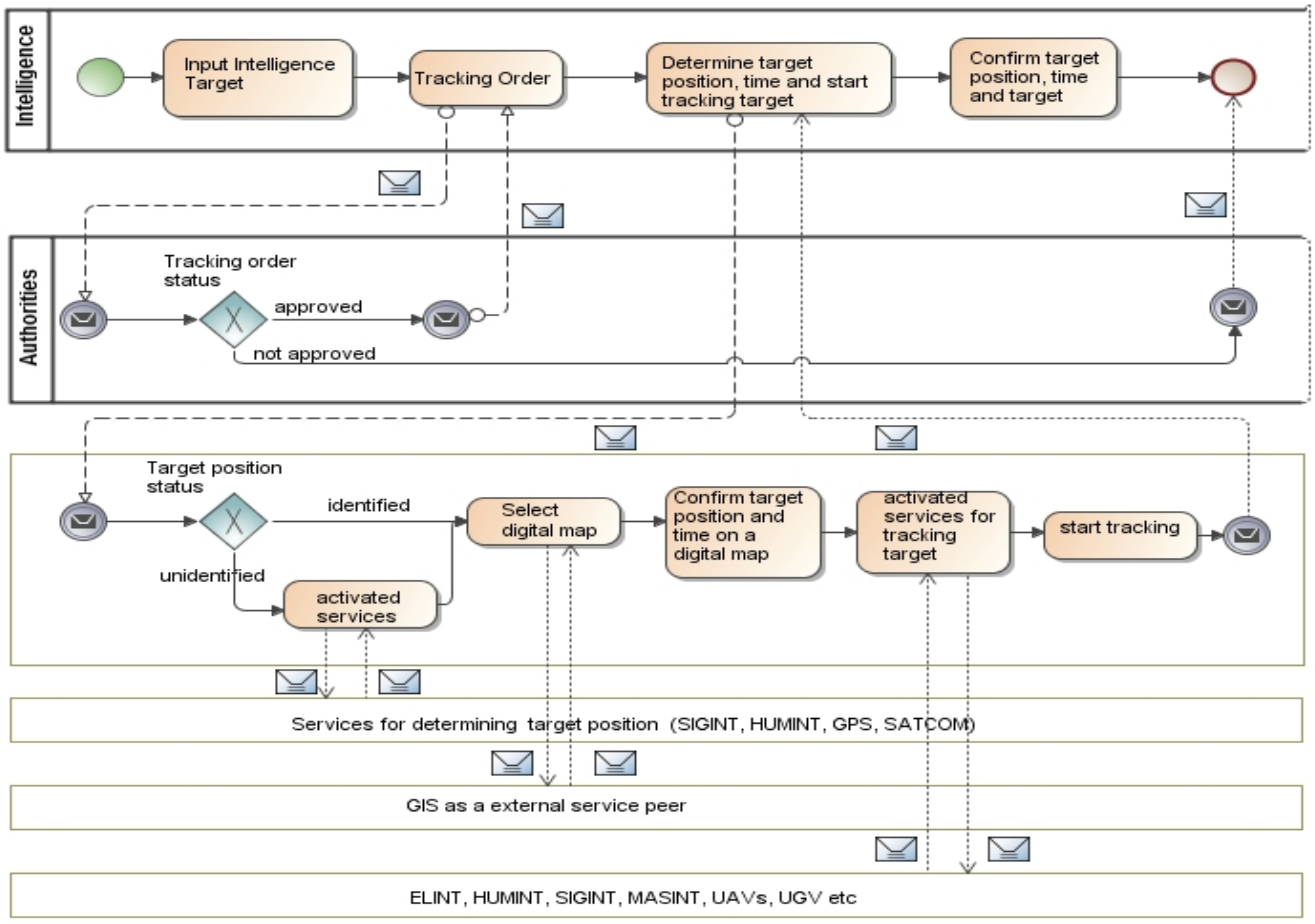


Figure 11. Business process for following Intelligence object

Position of Intelligence target can be marked on digital map which allows implementing Geographic Information System (GIS) as a service. This allows different scenarios for Intelligence target to be created. Also, routes can be estimated and should be used by the Intelligence target.

Services for following target are activated immediately when position of Intelligence object is marked on a digital map.

Common characteristic for previously mentioned services is probability that refers to service availability in certain time during Intelligence

operation. Also, zones (green, yellow, red) for determining functions of probability can be introduced (see figure 12).

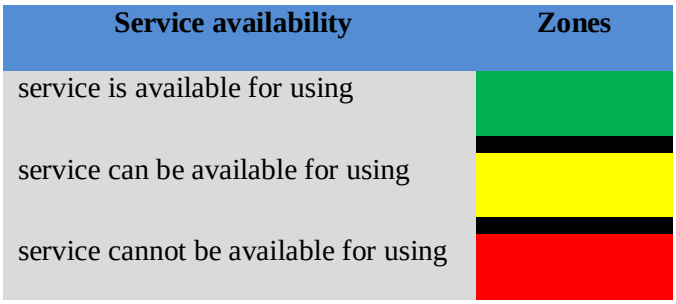


Figure 12. Service availability that is related to appropriate zones

Probability value of service availability allows selecting services that can be exploited in certain Intelligence operation in certain time. Introduced zones contribute to select services that can respond on the most appropriate manner.

5. Conclusion

Intelligence Information System Model gives contribution in Homeland Security and Civil Military Emerging Risks assessment through the possibility of providing information in the appropriate way by implementing pushing and pulling mechanisms into information systems, and then by selection of data and creation of information from raw data, that can be used in creating intelligence products and dissemination reports to the authorities. In this contribution, this is done by IIS based on SOA which follows the five postulates that enables flexible and secure design of IIS.

In this contribution we show that Information system integration should be based on assumption which refers to information sharing between users of information system. Additionally, service-oriented information systems are based on assumption which means sharing information between numerous clients through services.

Presented security approach about Intelligence Information system based on SOA provides secure data stream through services and also it provides strict security policies as a Authentication, Authorization, Privacy, Integrity and Non-repudiation.

We suggest two sets of metrics. The first one is a unifying general metrics that can be used for evaluating services in information system based on service-oriented architecture. The second metrics are information specific metrics that are used for evaluating the informative quality operation of services that are part of the proposed model. Together, they can give a thorough description of the established system of information procurement and quantify various aspects of its structure and operation. An advantage of the suggested metrics is their adoptability, i.e. they can be applied on all services and service compositions that are part of a service-oriented architecture.

Service attributes are important features for services. Developing metrics for service attribute allows determining services that are the most convenient for executing one Intelligence operation. In order to be presented functionality of Intelligence information system through estimation of probability for services in certain time moment, we have developed metrics for determining service reliability and service availability. Assessment of service attributes contributes to be exploited service-oriented systems on most appropriate manner and also it allows to be achieved high optimization in Intelligence processes.

References

[1]. Air Combat Command, - Version 2, *CONOPS UAV*, Section 6 - Communication Integration and Interoperability, http://www.fas.org/irp/doddir/usaf, US Air Force; 3 Dec 1996.

[2]. A. Goel, *Enterprise Integration EAI vs. SOA vs. ESB*, http://hosteddocs.ittoolbox.com/Enterprise%20Integration%20%20SOA%20vs%20EAI%20vsESB.pdf, consulted of January 2011.

[3]. F. Sanati, Jie Lu., *A Methodological Framework for E-government Service Delivery Integration*. Faculty of Information Technology, University of Technology, Broadway NSW. 2007.

[4]. P. Baglietto, M. Maresca, et al.. *Stepwise deployment methodology of a service oriented architecture for business communities* Journal: Information and Software Technology 47(6): 427-436. 2005.

[5]. F. Belanger, and L. D. Carter, *U-government: a framework for the evolution of e-government*, International Journal: Electronic Government 2(4): 426-445. 2005.

[6]. NATO Standardization Agency (NSA), *AAP-6(2002) NATO Glossary of Terms and Definitions*; http://www.nato.int/docu/stanag/aap006/aap6.htm, 2002.

[7]. M. Hepp, *Semantic Web and Semantic Web Services*, IEEE Internet Computing. 2006.

[8]. R. R. Burk, *Enabling Citizen-Centered Electronic Government 2005-2006 Action Plan*,USA, Office of E-Government and Information Technology. 2005.

[9]. M. H. Burstein, *Dynamic Invocation of Semantic Web Services That Use Unfamiliar Ontologies*, IEEE Intelligent Systems (July/August). (vol. 19 no. 4) 2004.

[10]. Castellano, M.. "An e-Government Cooperative Framework for Government Agencies". 38th Hawaii International Conference on System Sciences. Hawaii, IEEE. 2005.
[11]. S. Arroyo, M.-A. Sicilia, et al.. *Choreography frameworks for business integration: Addressing heterogeneous semantics*, Journal: Computers in Industry.2006.
[12]. Yu, K., X.L. Wang and Y. Zhou, *Underlying techniques for web services: a survey*, Journal of Software, 15(3), 428. 2004.
[13]. *IEEE Recommended Practice for Architectural Description of Software-Intensive Systems*, IEEE Std 1471-2000, September, 2000.
[14]. *Ministry of Defence Architecture Framework (MODAF)*, UK, version 1.2, http://www.modaf.org.uk accessed on 15 August 2008.
[15]. *NATO Architecture Framework*, version 3, AC/322-D0048. 2007.
[16]. A. Cernicki - Mijic, A. Martini, *Integracija aplikacija u elektroprivredama*, 7. simpozij o sustavu vodenja EES-a Cavtat, Dubrovnik, 5. - 8. studenoga 2006.
[17]. D. Pintar, *Implementacija stvarnovremenskog skladištenja podataka na temelju principa integracije poslovnih aplikacija*, FER e-Campus, 05.06.2008. http://www.fer.hr/_download/repository/kval_clanak_pintar.pdf
[18]. *Exploring New Command and Control Concepts and Capabilities Final Report*, NATO SAS-050, January 2006.
[19]. J. Achkoski, V. Trajkovik , and M. Dojcinovski "SOA Approach in Prototype of Intelligence Information System" ICT Innovations 2010, Web Proceedings, ISSN 1857-7288 pp. 149-160. 2010.
[20]. J. Achkoski, Vladimir Trajkovik and Danco Davcev: *Service-Oriented Architecture Concept for Intelligence Information System Development*; The Third International Conferences on Advanced Service Computing SERVICE COMPUTATION 2011 (IARIA), Rome, Italy, September 25 - 30, 2011.
[21]. J. Achkoski, V. Trajkovik: *Intelligence Information System Integration*, The 8th International Conference for Informatics and Information Technology (CIIT 2011), Bitola, Macedonia, March 2011.
[22]. J. Achkoski, V. Trajkovik, *Intelligence Information System (IIS) with SOA-based Information Systems*, 33rd International Conference on Information Technology Interfaces, IEEE, Cavtat/Dubrovnik, Croatia, June 27 - 30, 2011.
[23]. J. Achkoski, Vladimir Trajkovik and Danco Davcev, *Security Issues for Intelligence Information System based on Service-Oriented Architecture*, International Conference ICT Innovations 2011, Skopje, Macedonia, September 14 – 16, 2011.
[24]. J. Achkoski, V. Trajkovik and M. Dojchinovski, *An Intelligence Information System based on Service-Oriented Architecture: A Survey of Security Issues*, Information & Security: An International Journal, vol. 27: 91-111, 2011.
[25]. M.Gebhart, & S. Abeck, *Metrics for Evaluating Service Designs based on SoaML*, International Journal on Advances in Software, 4(1&2), 61-75. Retrieved from http://iariajournals.org/software/, 2011.
[26]. M. Gebhart, M. Baumgartner, S. Oehlert, M. Blersch and S. Abeck, *Evaluation of Service Designs based on SoaML*, In Proceedings of the Fifth International Conference on Software Engineering Advances (ICSEA) (Hall J, Kaindl H, Lavazza L, Buchgeher G, And Takaki O), p 7, Nice, France. 2010.
[27]. D. A. Menascé, *Response-Time Analysis of Composite Web Services*, Journal IEEE Internet Computing, Vol. 8, No. 1., pp. 90-92. 2004.
[28]. S. Kalepu, S. Krishnaswamy, S. W. Loke: *Verity: A QoS Metric for Selecting Web Services and Providers*. Proceeding WISEW'03 Proceedings of the Fourth international conference on Web information systems engineering workshops IEEE Computer Society Washington, USA, 2003.
[29]. R. M. Ramović., *Skripta - Pouzdanost sistema elektronskih, telekomunikacionih i informacionih*, Katedra za Mikroelektroniku I tehnicku fiziku, Univerzitet u Beogradu, Elktrotehnicki fakultet, 2005.
[30]. W. Xie†, H. Sun‡, Y. Cao† and Kishor S. Trivedi† *Modeling of Online Service Availability Perceived by Web Users*

Corresponding author: **Jugoslav Achkoski**
*Institution:***Military Academy "General Mihailo Apostolski", Skopje Macedonia**
E-mail: **jugoslav_ackoski@yahoo.com**