Software simulator for property investigation of document management system with RFID tags

Maciej Kiedrowicz[1], Tadeusz Nowicki[1,a], Robert Waszkowski[1], Zbigniew Wesołowski[1], Kazimierz Worwa[1]

[1]*The Faculty of Cybernetics, Military University of Technology, 00-908 Warsaw, Kaliskiego 2, Poland*

Abstract. The study outlines the method for examining the properties of the RFID-tagged document management system. The system is composed of computers, where the software for supporting processes of the RFID-tagged documents was installed. Furthermore, the system cooperates with many other elements of the secret office (cabinets, sluices, photocopiers, desks). The examination of the properties of the RFID-tagged document management system is, in this case, complex due to the number of a possible examination scenarios. The simulation method for examining the system properties was proposed. It allows to conduct the examination of the properties in a short period of time for numerous testing scenarios.

1 Introduction

The flow of paper documents in public administration, commercial companies and other organizations is connected with the registration of many important legal deeds or personal documents, administrative decisions, bank decisions, etc. It is also worth mentioning that even though such documents are more and more often replaced by their electronic equivalents, the paper documentation is still required from the formal point of view. At different levels of public administration, the secret offices are established to collect the documents for the purpose of their efficient archivization and quick identification of their properties in that respect.

For some time now, the RFID (radio-frequency identification) (Heinrich [6]) tags have been used for the document flow processes. It is of great importance for both the public administration (Maniva et. al. [8]) and other organizations (Bose et. al. [4]), including health care (Wang et. al. [13]), logistic (Whang [14] and Stambaugh et. al. [12]), production (Araújo Filho et. al. [2]) and other institutions.

The technology allows to permanently attach the RFID markers (labels, tags) to documents, which - when subject to radiation from waves generated by appropriate antennas - send signals from such markers registering their presence in a certain distance from the antennas. Thus, the RFID-tagged documents are passive objects. If there is no radiation from the antennas, they do not send any signals across the ether. If the antennas work properly, the reading system allows identification of many tags present at the same time within the reading field.

It is also worth adding that, nowadays, the RFID tags are not something much different from traditional documents, without such markers. The RFID tags have recently undergone a substantial transformation in terms of their size. The RFID-tagged document shown in Fig. 1 does not differ much from a traditional document, and the size of the RFID tag is getting smaller and smaller, to approximately 10 square centimeters.

However, when bearing in mind the fact that the RFID antennas send signal with certain frequency, it is possible to establish a modern system for managing the RFID-tagged documents. Such system allows to register a number of events in a room, where the RFID-tagged document management system with the RFID antennas is located. The basic events include:

- occurrence of new documents with the RFID tags,
- taking away of a single RFID-tagged document or a package thereof outside the area of the antennas,
- relocation of the RFID-tagged document within the area of operation of the antennas,
- registration of new documents with the RFID tags,
- etc.

The implementation of the RFID-tagged document management system requires specialist environment, composed of a couple of elements, which creates a computer-assisted identification process of the document flow within a certain predefined area.

One of the most important examination of the properties of the RFID-tagged document management system consisted in developing a number of scenarios of events, which may appear during the operation of the system. There may be many of such scenarios. It must be remembered that in the course of the examination, the following should be taken into consideration:

- the number of the RFID-tagged documents may be changed,

[a] Corresponding author: tadeusz.nowicki@wat.edu.pl

- the location of the documents in particular cabinets may be each time different,
- the changes of location of the RFID-tagged documents may be subject to various activities of their users,
- different activities are registered in many locations in the databases of the system,
- every activity is the implementation of the adopted business processes,
- some new RFID-tagged documents appear in the system and some of them disappear from the system.

All of this creates an increase of the different variants of examining the properties of the system. The examination would entail a large number of the scenarios of activities of the system users. The examination of the properties would last too long. It also should be remembered that some of the characteristics of the use of the RFID-tagged documents are not homogeneous in time. They change quite often, which is caused by the fact that some RFID-tagged documents disappear from the system and the new ones appear. The frequency of use of particular documents also changes, since their relevance changes. It means that after some time, the examination of the system properties should be repeated.

Therefore, a concept of building a simulator (Fishman [5] and Perros [9]) of signals informing about different activities of the users of the RFID-tagged document management system emerged. The simulator may operate in the network environment (Sinclair [11]). It allows to prepare a number of program scenarios of physical implementation of activities of the users. The program scenarios of activities may be generated automatically. Their number is not limited, since what will be examined are the reactions of the RFID-tagged document management system, which takes place in a practically insignificant period of time. Such examination of the system properties is usually performed when we deal with the research into the IT systems with a large number of possible external and internal events.

The study outlines the simulation method for examining the properties of the RFID-tagged document management system, allowing to conduct complex research into its significant user features in a relatively short period of time.

2 Environment of the RFID-tagged document management system

We assume that the registration of the RFID-tagged documents is within the area of the widely understood secret office of the public administration. We may attempt to outline the structure of such secret office. Its elements, apart from the typical components, using the RFID technology, are the following:

- entrance sluice with the RFID antennas as the access terminal to the secret office,
- cabinets with the RFID antennas with the control unit,
- cabinets with the RFID antennas without the control unit,
- reading tunnel for the RFID-tagged documents,
- RFID tray reader,
- specialist photocopier with the RFID module,
- printer server,
- software server for registering RFID tags,
- software server of the RFID-tagged document management system.

The entrance sluice with the RFID antennas is for registering the documents brought into or taken away from the secret office. The person entering or leaving the secret office also has the RFID tag in the form of a special personal chip. The cabinets with the RFID antennas are natural storage for the documents in the secret office. The reading tunnel for the documents is used by the users of the secret office to file the documents brought and left in the office, including removal of the already held documents from the catalog. Similarily, the tray reader is used for registering single documents with the RFID tags. The specialist RFID printer registers the fact of copying a document. Thanks to its in-built verification system, it may check whether the document can or cannot be copied, by whom and in which number of copies.

Fig. 1 presents the architecture of the model execution environment for the computer RFID-tagged document management system. At the bottom of the figure, some symbolic external devices with the RFID-tagged documents are presented. They include:

- computer workstation for an employee of the secret office,
- cabinets with the RFID antennas with the control unit,
- cabinets with the RFID antennas without the control unit,
- reading tunnel for the RFID-tagged documents,
- RFID tray reader,
- specialist photocopier with the RFID module,
- entrance sluice to the secret office,
- manual RFID tag reader,
- and printer server.

All these devices connect with the RFID-tagged document management system via a computer network controlled by the network router.

The RFID-tagged document management system is composed of the following elements:

- Aurea BPM server describing potential activities of the system users,
- Cosmos server responsible mainly for the printer (photocopier) operations in the system,
- Nofilis server allows to configure the system (indication of the compatible devices in the secret office) and receive signals from the devices with the RFID-tagged documents.

The servers create a computer environment responsible for the RFID-tagged document flows in the system. The server software is the result of the work of the designers of the RFID-tagged document management system.

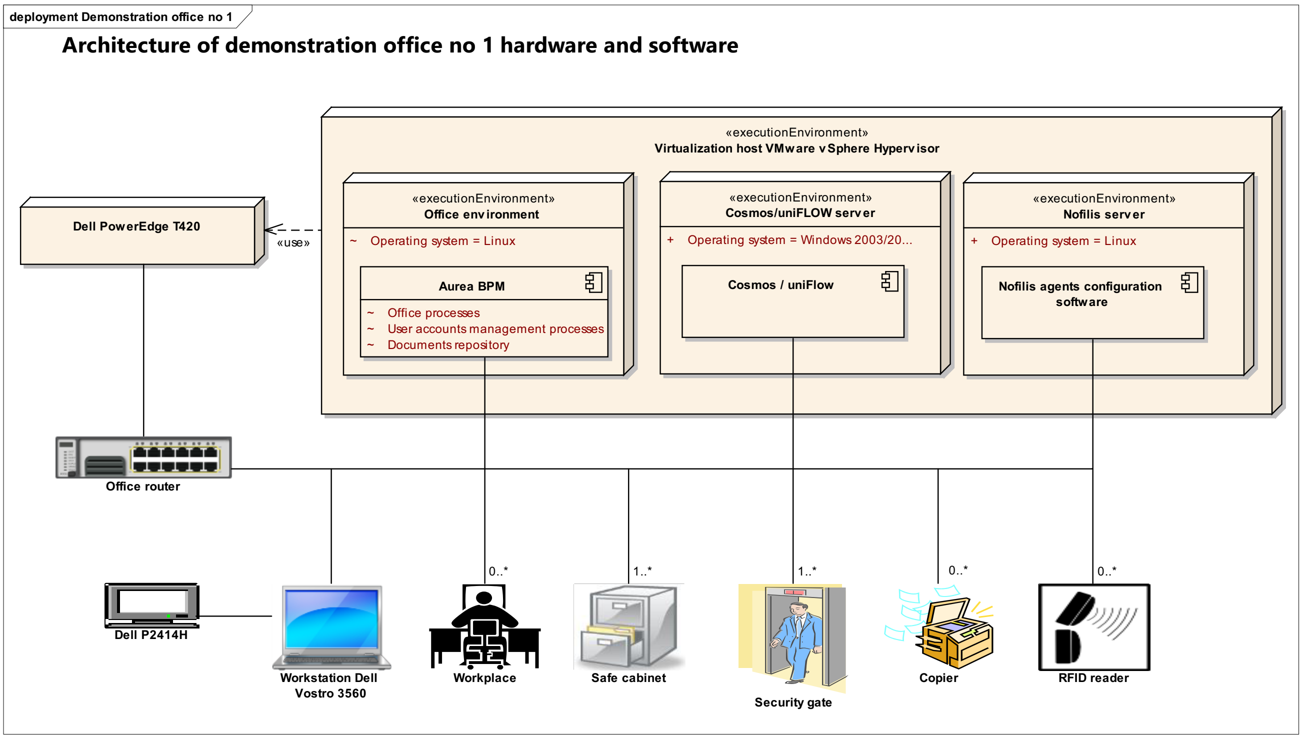
deployment Demonstration office no 1
Architecture of demonstration office no 1 hardware and software
«executionEnvironment»
Virtualization host VMware vSphere Hypervisor
Dell PowerEdge T420
«use»
«executionEnvironment»
Office environment
~ Operating system = Linux
Aurea BPM
~ Office processes
~ User accounts management processes
~ Documents repository
«executionEnvironment»
Cosmos/uniFLOW server
+ Operating system = Windows 2003/20...
Cosmos / uniFlow
«executionEnvironment»
Nofilis server
+ Operating system = Linux
Nofilis agents configuration software
Office router
0..*
1..*
1..*
0..*
0..*
Dell P2414H
Workstation Dell Vostro 3560
Workplace
Safe cabinet
Security gate
Copier
RFID reader

Fig. 1 Model execution environment of the computer RFID-tagged documents management system. Source: own elaboration.

The manner of communication between the devices of the servers of the system needs to be explained. CrossTalk is responsible for such communication. Every device in the secret office is accompanied by the CrossTalk agent, which sends the information to the system in case of any action involving the RFID-tagged documents or other action, such the opening or closing of the cabinet, entering of the user to the sluice, copying of the document, etc.

The messages are in the form of XML character strings. The XML documents in CrossTalk are used to describe the data and events in the system. They are sent over the network to the Aurea server. The server identifies and archives the documents in its database. Fig. 2 shows an example of the XML message.

```
<?xml version="1.0" encoding="UTF-8"?>
<events>
<event type="com:nofilis:crosstal
k:event:tag-observation"
timestamp="1417780363293"   uuid="CCDEDBCA-
6D07-2076-5CAE-C1DBC42DEE5D"          loca-
tionId="CABINET_3.R" objectId="C01B2916">
<id="first-read" value="1417780363291" />
<id="last-read" value="1417780363291" />
<id="observationUUID" value="73B00D24-C3B6-
25FB-CFD1-F59157FC3856" />
<id="reads" value="1" />
</event>
</events>
```

Fig. 2 Model XML documents defining the manner of handling an event

The XML message attributes, including their values, are contained in the following table.

Table 1. Descriptions of attributes of the XML documents defining the manner of handling an event

N o.	Attribute	Description of the attribute value
1	timestamp	The value of this attribute is a timestamp of the RFID tag reader of the document. The value of the timestamps is expressed in the Unix time.
2	uuid	The value of this attribute is an event identifier - *tag-observation*.
3	objectId	The value of this attribute is the RFID tag of the document.
4	locationId	The values of this attribute are names of storage locations of the RFID-tagged documents and names of operations performed on these documents. The value of *[Cabinet name].A* means that from the cabinet called*name* the RFID tag of the document was read. The value of this tag is saved in the form of the value of attribute *objectId*. The value of*[Cabinet name].R* means that from the cabinet called *name*the RFID-tagged document was removed, whose value is equal to the value of attribute *objectId*.

5	id="first-read"	The value of this attribute is the timestamp of the read-out of the first RFID tag of the document from the set of documents located in a place defined by the value of attribute *locationId*. The value of the timestamps is expressed in the Unix time.
6	id="last-read"	The value of this attribute is the timestamp of the read-out of the RFID tag of the document from the set of documents located in a place defined by the value of attribute *locationId*. The value of the timestamps is expressed in the Unix time.
7	id="observationUUID"	The value of this attribute is the identifier of the read-out session of the RFID tags of the documents located in a place defined by the value of attribute *locationId*.
8	id="reads" value="1"	The value of this attribute is the number of read-outs of single RFID tags executed by technical devices included in the RFID cabinet. The default value of this attribute is 1.

The XML messages are the only results, from the point of view of the system, of the activities of the user in the secret office, involving the RFID-tagged documents. Therefore, the generation of the XML messages from the simulator and sending them to Aurea will make the system register the activities of the users in the secret office, even though they have not actually occurred.

It will allow to quickly examine the practical and functional properties of the RFID-tagged document management system, without the necessity of undertaking long-term activities by the users, hence developing complex and numerous scenarios of the functioning of the secret office. This is the approach applied by the simulation method for examining the properties of the RFID-tagged document management system.

3 Workflow processes in the secret office with the RFID-tagged documents

The fundamental concept of executing the computer system supporting the RFID-tagged document flow management is based on the definition of the business processes related to the document flow in the secret office. Development of the models of the document flow processes allows to automate the registration procedure in the secret office. Thanks to a user-friendly interface of the system, the employees of the secret office, do not need to fill out any detailed forms related to the receipt, issuance, creation, etc. of the documents, but only select and tick certain options available in the graphic user interface. Any entries made into the system with respect to the description of the operations made on the documents, their names, purpose, flow history, modifications, moments of incorrect identification, etc., are automatically implemented by the system.

The case models concerning document flows also allow to monitor the status of the RFID-tagged documents held in the secret office. It is possible to turn on the frequency option for monitoring the document status in the secret office, which will be automatically initiated from time to time. In case of any irregularities, the alarm signal will be sent. Obviously, at the beginning of the operations of the secret office, when the personnel is not sufficiently trained, such signals will occur on a daily basis. However, with time, they should be completely eliminated.

The process models related to the flow of the RFID-tagged documents may be also used for examining the characteristics of the document flow, which is the main issue discussed herein. It should be also stressed that at the stage of defining the document flow processes, no significant features are noticeable with respect to the capacity and reliability of the support system in the secret office.

The main business processes related to the functioning of the secret office in terms of the RFID-tagged documents, include the following:

- acceptance or the RFID-tagged document or documents from a natural person,
- acceptance of the parcel including the RFID-tagged documents, bearing some traces of opening,
- performance of standard activities when accepting the RFID-tagged documents,
- registration of correspondence in the form of the RFID-tagged documents,
- inclusion of a confidentiality clause in the RFID-tagged documents,
- registration of the created RFID-tagged documents,
- processes related to the storage of the RFID-tagged documents,
- preparation of the RFID-tagged documents for sending,
- sending of the RFID-tagged documents by a carrier,
- sharing of the RFID-tagged documents,
- destruction of the RFID-tagged documents.

The procedure of accepting the parcel containing the documents may be a good example of the business process related to the functioning of the secret office. The example was presented in Fig. 3

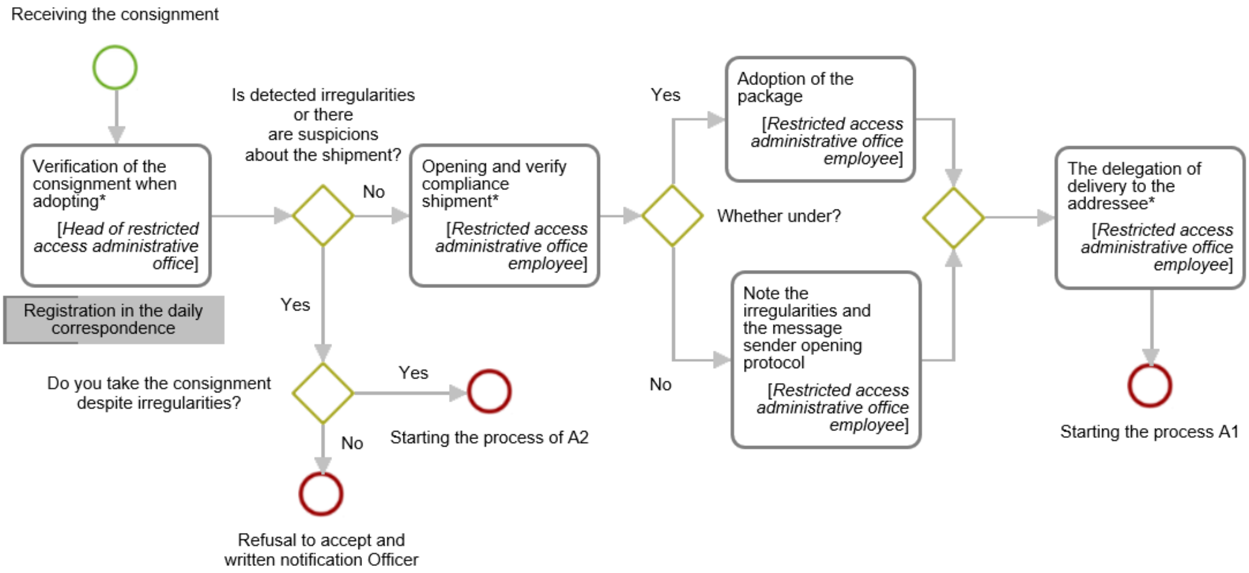
Receiving the consignment
Verification of the consignment when adopting*
[Head of restricted access administrative office]
Registration in the daily correspondence
Is detected irregularities or there are suspicions about the shipment?
No
Yes
Opening and verify compliance shipment*
[Restricted access administrative office employee]
Do you take the consignment despite irregularities?
Yes
No
Starting the process of A2
Refusal to accept and written notification Officer
Yes
No
Whether under?
Adoption of the package
[Restricted access administrative office employee]
Note the irregularities and the message sender opening protocol
[Restricted access administrative office employee]
The delegation of delivery to the addressee*
[Restricted access administrative office employee]
Starting the process A1

Fig. 3 Acceptance of the parcel containing the RFID-tagged document. Source: own elaboration.

The process is based on the following steps, which must be performed by an employee of the secret office. The process is initiated at the time of accepting the parcel by the employee of the secret office, who enters the date of receipt in the initial form and puts other information in the book of deliveries/list of delivered parcels, and approves the action. Subsequently, the Manager of the SO accepts the parcel and checks its contents. The Manager enters the information on the sender and recipient, confirms safe receipt of the parcel and includes the information about checking the compliance of the parcel. The Manager of the SO checks if any irregularities were found during the verification procedures or whether any suspicions exist with respect thereto. If so, the Manager decides on whether the parcel should be accepted, despite such irregularities, or not (If not, the Manager refuses to accept the parcel and informs thereof a responsible person in writing. The end of the process. If yes, the process of "acceptance of the parcel including the RFID-tagged documents, bearing some traces of opening" is initiated). If not, the Manager provides the employee of the secret office with the parcel. The employee of the secret office must open the parcel and check its contents in terms of the serial numbers listed in the inside envelope. The employee must verify which documents in the parcel already have the RFID tags. The employee must verify the number of pages, appendices and pages of appendices in accordance with the number indicated on particular materials. If the employee finds any irregularities, (s)he will make a relevant entry in the parcel opening report, defining the defects and making a comment about this fact in the correspondence logbook. Subsequently, the employee must attach the aforesaid reports and send them to the sender. The employee must accept the parcel. If necessary, the employee must put the RFID tags on the documents, which lack such markers, but should have them. The employee of the secret office must send the parcels to the addressees in different manners, depending on whether the matter is urgent or not. The process of the "registration of correspondence in the form of the RFID-tagged documents" is initiated. The employee must put a note about this fact in the "Comments" of the recording device. The process of the "registration of correspondence in the form of the RFID-tagged documents" is initiated.

To illustrate the complexity of the RFID-tagged document flow processes in the secret office, we may show the procedure related to the registration of the RFID-tagged documents in administrative office (Fig. 4).

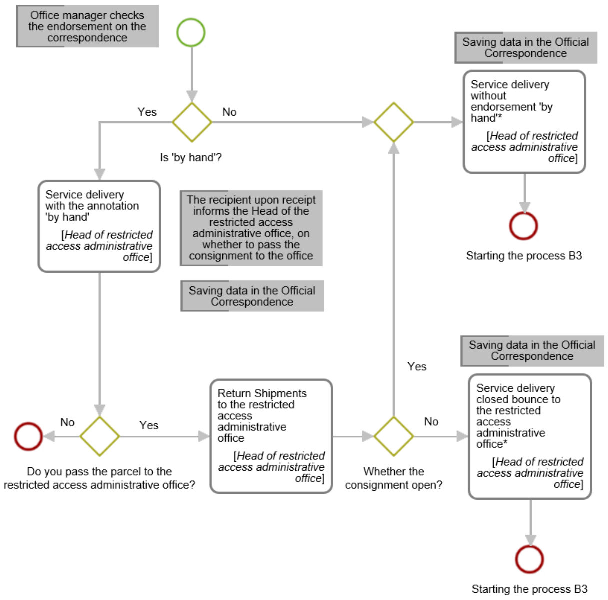
Office manager checks the endorsement on the correspondence
Yes
No
Is 'by hand'?
Saving data in the Official Correspondence
Service delivery without endorsement 'by hand'* [Head of restricted access administrative office]
Starting the process B3
Service delivery with the annotation 'by hand' [Head of restricted access administrative office]
The recipient upon receipt informs the Head of the restricted access administrative office, on whether to pass the consignment to the office
Saving data in the Official Correspondence
Saving data in the Official Correspondence
Yes
No
Yes
Return Shipments to the restricted access administrative office [Head of restricted access administrative office]
No
Do you pass the parcel to the restricted access administrative office?
Whether the consignment open?
Service delivery closed bounce to the restricted access administrative office* [Head of restricted access administrative office]
Starting the process B3

Fig. 4 Process related to registration of the RFID-tagged documents in administrative office.
Source: own elaboration.

4 Investigation of the workflow processes of the RFID-tagged document management system

The main issue concerning the examination of the characteristics of the document flow processes is to define the capacity and reliability properties on the support system implemented in the secret office. In natural conditions, the examination of the software properties would be very time-consuming. However, it is necessary before the accepting the system for use.

The basic features subject to the examinations and the capacity and reliability properties. As part of the examination of capacity and reliability,using previously developed methodologies and reliability characteristics, the following will be subject to examination:

- remote identification of documents and media, open and classified, in locations of storage and real-time work,
- automatic inventory of documents and media, open and classified, stacked up,
- automatic detection of relocation of marked documents and media,
- control system of the document and media flow,
- verification of the procedures and mechanisms for authentication of persons and documents,
- electronic system for protecting documents and media against unauthorized relocation and identification of documents and media at workplaces,
- method of protection against multiple copying of documents and printing with a limited number of copies,
- identification of location of a single document and medium with predefined accuracy,
- proper functioning of the sluice.

As part of the capacity examination, among other things, the following will be checked:

- efficient volume (number) of sets of marked documents in the selected procedures of their flow,
- duration of identification of the set of the marked documents and media in the selected procedures of their flow,
- analysis of significance of the impact of typical and random changes of the system working conditions (disruptions) on its correct functioning.

5 Simulation method for examining the workflow processes

To achieve this objective, the original working environment of the secret office was changed, according to Fig. 5. In such case, it would be necessary to implement a number of scenarios of events related to the messages sent between the RFID software agents from the third party device to the RFID system server. Furthermore, it would be indispensable to track the reactions of the server of the document flow system to the occurring events. The number of the examined scenarios, together with their internal diverse repeatability, would be so large that the study would take months.

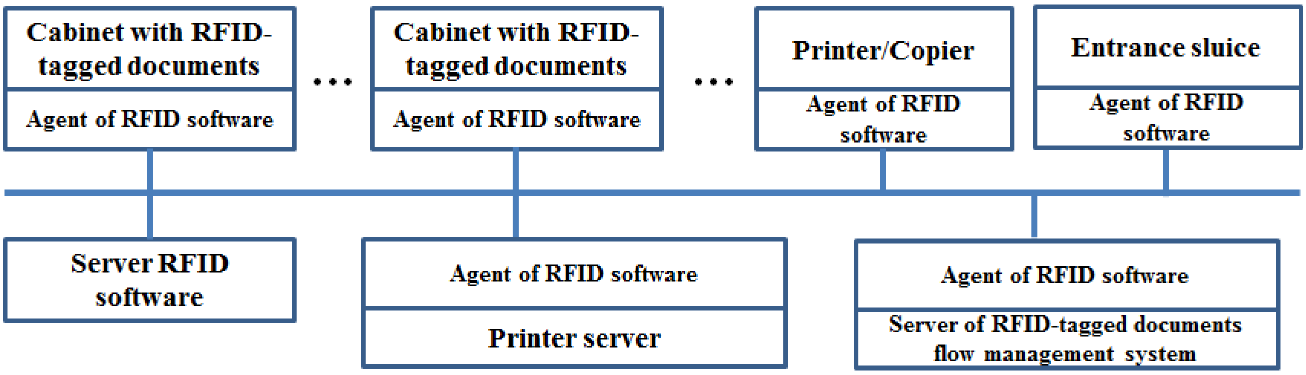

Fig. 5 System supporting the RFID-tagged document flow. Source: own elaboration.

It was decided to apply an innovative method of examination of the reliability and capacity properties of the system. We constructed a simulator imitating the events related to the document flow and - in this case - generating the signals about the change of the location of RFID-tagged documents in the system of the secret office. The event simulators imitating the functioning of the technical system were described, among other things, in terms of a model in the monograph (Fishman [5]) or (Ross [10]), and in terms of implementation - in (Abu-Taieh et. al. [1]) and (Sinclair [11]).

Normally, the RFID server is only used for the purpose of configuration of the environment, where the devices being the components of the secret office, are defined. On the other hand, the existence of the RFID-tagged documents are registered thanks to the fact that the RFID antennas send messages to the RFID software agents, which in turn send the signals to the document flow system. The messages are in the form of XML character strings. Therefore, the idea to build the simulator of the XML messages, imitating the existence or non-existence, or relocation of the documents in the system, was conceived.

The support system for the RFID-tagged document flow was thus transformed from Fig. 5 to artificial environment illustrated in Fig. 6.

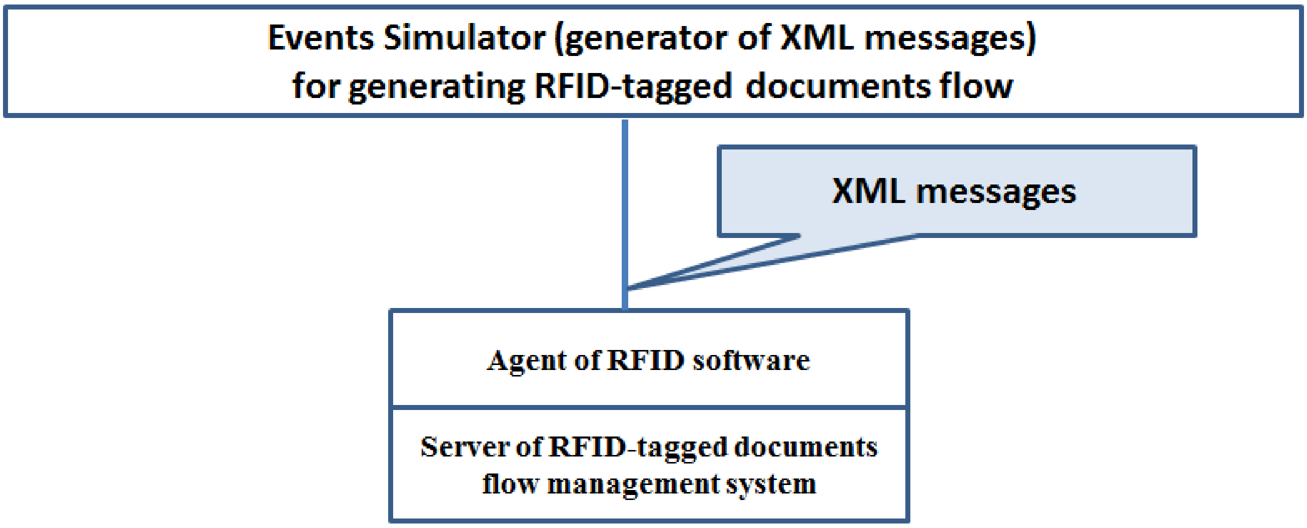
Events Simulator (generator of XML messages) for generating RFID-tagged documents flow
XML messages
Agent of RFID software
Server of RFID-tagged documents flow management system

Fig. 6 Process related to the storage of the RFID-tagged documents Source: own elaboration.

It created a possibility of earlier creation of the scenarios related to the examination of the RFID-tagged documents held in the secret office, including their location. In such a way, it is possible to examine - in a definite and short period of time - the capacity and reliability properties of the system in the secret office, in terms of the application software of the document flow management server and correct functioning of the entries in the database. Without the aforesaid modification, the examination of such properties would be very time-consuming.

Obviously, the examination of the proper functioning of some peripheral devices, such as the cabinets, printer, sluices, etc. is performed in a standard manner, yet the number of experiments is relatively small and takes little time. The structure and basic functionality of the simulator was shown in Fig. 7.

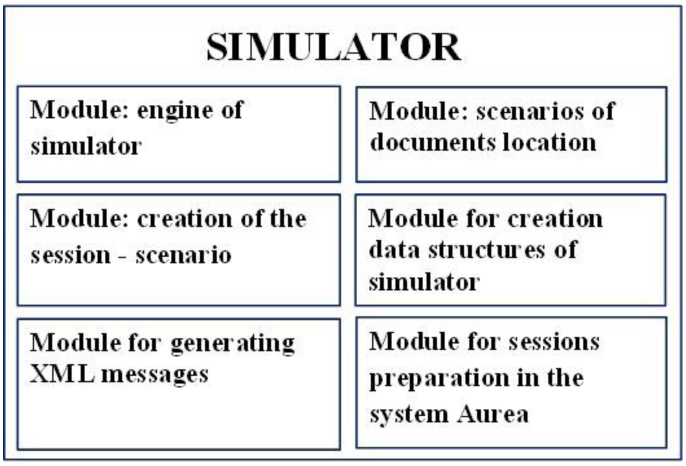
SIMULATOR
Module: engine of simulator
Module: scenarios of documents location
Module: creation of the session - scenario
Module for creation data structures of simulator
Module for generating XML messages
Module for sessions preparation in the system Aurea

Fig. 7 Structure of the simulator for the information flow about the documents. Source: own elaboration.

6 Conclusions

The main functions of the suggested solution include the RFID-tagged document flow management , access control to the documents and supervision of their copying, as well as access management. The additional benefit of the designed solution, apart from the better control of the document storage and access, will be a possibility of tracking the flow paths of the open and classified media and documents between the safety zones, with the indication of persons authorized to use the documentation. Obviously, the main users of the system will be public administration units, including those subordinate to the Ministry of Defense and the Ministry of the Interior and Administration. An important field of interest as regards the results of the discussed project will be also the area of justice and health care institutions.

The implementation of the results will contribute to the development and increase of competitiveness of the sector of document flow in Poland, mainly because such advance solutions, based on radio and automatic identification of the documents, are not available in Europe. Thanks to the said technology, many Polish institutions and enterprises, not only state-owned, but also private, may become the leading suppliers of the subject solutions on the European market and later - also worldwide.

References

1. E.M. Abu-Taieh, A.A.R. El Sheikh, *Handbook of research on discrete event simulation environments: Technologies and applications*, IGI Global, Hershey, New York (2010)
2. F.W.C.Araújo Filho, X.L. Travassos, P.S. Figueiredo, *Use of the RFID technology to overcome inefficiencies in the production process: an analysis of a microcomputer company in Ilhéus – Bahia*, Journal of Information Systems and Technology Management. Vol. 11, No. 1, pp. 65-84 (Jan/Apr., 2014)
3. D. Barnard-Wills, D. Ashenden, *Public sector engagement with online identity management*, Identity in the Information Society, Volume 3, Issue 3, pp. 657-674 (December 2010)
4. I. Bose, E.W.T. Ngai, T.S.H. Teo, S. Spiekermann, *Managing RFID projects in organizations*, European Journal of Information Systems 18, pp. 534-540 (December 2009)
5. G.S. Fishman, *Discrete event simulation. Modeling, programming and analysis*, Springer, New York, (2001)
6. C. Heinrich, *RFID and Beyond*. Wiley Publishing, Indianapolis (2005)
7. J. Kannry, S. Emro, M. Blount, M. Ebling, *Small-scale Testing of RFID in a Hospital Setting: RFID as Bed Trigger*, AMIA Annual Symposium Proceedings Archive, pp. 384–388 (2007)
8. T. Maniva, H. Sugano, M. Kato, *Mass Data Read/Write Technology for UHF-Band RFID Tags*, Fujitsu Sci. Tech. J., 43,4,p.464-468 (October 2007)
9. H. Perros, *Computer simulation techniques – the definitive introduction*, North Carolina State University, Raleigh (2009)
10. S. M. Ross, *Simulation*, Elsevier Inc. (2006)
11. B**.** Sinclair, *Simulation of Computer Systems and Computer Networks: A Process-Oriented Approach*, University Press, Cambridge UK (2004)
12. C.T. Stambaugh, F.W. Carpenter, *Wireless innovation in inventory monitoring and accounting*, Strategic Finance, Vol. 91(6), pp. 35-40 (2009)
13. S. Wang, W. Chen, C. Ong, L. Liu, Y. Chuang, *RFID Application in Hospitals: A Case Study on a Demonstration RFID Project in a Taiwan Hospital*, In Proceedings of the 39th Annual Hawaii International Conference on System Sciences - Volume 08, (4-7 January 2006)
14. S. Whang, *Timing of RFID Adoption in a Supply Chain*, Management Science, vol. 56, No. 2, pp. 343-355 (2010)