Theoretical and Applied Informatics
ISSN 1896-5334
Vol. 25 (2013), no. 3-4
pp. 183 – 200
DOI: 10.2478/thai-2013-0014

Information security and business continuity issues and solutions with OSCAD - case studies in public administration

ANDRZEJ BIAŁAS

Instytut Technik Innowacyjnych EMAG
ul. Leopolda 31, Katowice, Poland
a.bialas@emag.pl

Received 25 July 2013, Revised 26 November 2013, Accepted 2 December 2013

Abstract: The paper features some aspects of providing information security and business continuity to public administration by means of an integrated computer-aided management system OSCAD. The system is based on international standards ISO/IEC 270001 and BS 25999 (ISO 22301). First, the significance of information security and business continuity issues in public administration was presented along with a short introduction to the applied standards. Then the possibilities of the OSCAD system were discussed together with the examples how the system can solve the problems encountered by public administration.

Keywords: Information security, business continuity, public administration, risk management, computer support.

1. Introduction

In every country there are a number of institutions whose competence is to implement the government policy in different realms of political, economic and social activities, to develop and maintain policies, and to provide decisions which ensure that the government is able to operate. This way government-level objectives are brought to details in everyday lives of citizens and the state can operate efficiently. These institutions are: ministries, parliament, courts, state administration on different levels, local self-government, educational institutions, public health service, central offices and inspectors, institutions of control, guards, service, agencies, and all sorts of non-government organizations. They share the following characteristics:

1. The public administration institutions have to function on a stable, suitably high level of efficiency. Every disturbance can lower the efficiency of an institution and its co-operating organizations, and this way has a negative impact on the state as a whole, and on its image among the citizens. Therefore there is a strong need in the public administration to ensure operational continuity identified with the term of business continuity.

The functioning of organizations is perceived through their business processes. The terms such as business process or business continuity, commonly understood as characteristic of commercial, profit-oriented organizations, can be applied to institutions which render public services for citizens too. Public administration units carry out these processes for the state, its organs, social groups and citizens. There are many factors that can disturb business continuity of public administration. It is necessary to identify these factors, apply proper measures and get prepared to deal with the related crisis situations. The continuity of business processes conducted by public administration units is a protected asset.

2. Today's public administration units make an extensive use of information technologies. Complex IT systems working in such institutions need proper security measures to process, transfer and store sensitive information. That is why information security has a key significance here.

Information systems produce, process, store, and transfer a huge amount of information about the state and its citizens. The network for transferring this information is the backbone of the state. It is vital to ensure the integrity of this information in order to protect it against the activities of unauthorized subjects that falsify or destroy it, intentionally or by mistake. A part of this information are confidential data that have to be protected for the benefit of the state and its citizens. Additionally, it is important to protect personal data of citizens, stored in central repositories or transferred through the network. Public administration units have at disposal and use certain information. What is more, they provide it to other institutions. This process is the basis for both strategic decisions concerning the state or social groups and decisions concerning individuals. These decisions can be made only if the information is available (in due place and time, of proper quality) to authorized decision makers. The necessity to protect information attributes, such as integrity, confidentiality or availability, means that public administration units are strongly oriented to ensure information security. There are many factors which may breach the integrity, confidentiality and availability of information. For this reason the organizations should identify these disturbing factors, apply adequate security measures and get prepared for the related crisis situations. A protected asset is understood here as information whose integrity, confidentiality and availability have to be maintained.

Business continuity and information security issues are tackled differently by different institutions, depending on the operating level and specifics of the given administration unit. For example, the protection of state registers is different than the protection of state critical infrastructure or providing preparedness of rescue services.

The paper gives an introduction to information security and business continuity issues with brief presentation of the related international standards. Afterwards, the results of the targeted project OSCAD, completed recently by the author's institute, are presented. This project is focused on solving business continuity and information security issues in different kinds of organizations, including public administration. The key section features a few examples showing how to solve these issues. Finally, the author summarizes the achieved results and presents development and implementation plans for the near future.

2. Introduction to information security and business continuity

Ensuring business continuity and information security in an institution requires that suitable management systems should be implemented, i.e. Business Continuity Management System (BCMS) and Information Security Management System (ISMS), and embedded into the whole management system of the institution.

The paper concerns the implementation of two world-known standards into one integrated IT system:

- BS 25999 [1], [2] concerning the development of *Business Continuity Management Systems (BCMS)* in organizations (replaced by ISO 22301 recently [3]),
- ISO/IEC 27001 [4], [5] concerning the development of *Information Security Management Systems* (*ISMS*) in organizations.

Business Continuity (BC) is understood as a strategic and tactical ability of the organization to [1], [2]:

- plan reactions and react to incidents and disturbances in business operations with a view to carry on these operations on an accepted, previously agreed level,
- reduce losses in case incidents or other disturbances occur.

Information Security (IS) is related to the protection of information against the breach of its attributes, such as integrity, confidentiality and availability.

Ensuring business continuity and information security is based on risk management [6], [7] which starts from risk analysis. For the protected assets (business processes or information) the following are identified:

- factors that are breaching assets, i.e. threats,
- factors facilitating the breach, i.e. vulnerabilities and,
- different kinds of results of the breaches are estimated, i.e. impacts.

The core of the risk management process are certain operations undertaken for each risk case. The risk can be mitigated by means of different kinds of security measures, can be transferred to an insurance agency or business partner, or can be accepted if it is not too high and there are rational reasons to accept it.

Risk management is an interdisciplinary process as it comprises organizational, personal and technical issues, including IT.

3. Integrated, computer aided system OSCAD for business continuity and information security management

The OSCAD system was developed at the Institute of Innovative Technologies EMAG within a project co-financed by the National Centre for Research and Development (NCBiR). The project acronym means “Open, scalable, and integrated, computer aided system for business continuity and information security management”.

The objective of the OSCAD project was to develop an integrated, computer aided system of business continuity and information security management which ensures the following:

- monitoring factors which cause crisis situations in institutions, i.e. when the continuity of business processes is disturbed or information security is breached by threats which exploit certain vulnerabilities,
- ability to reduce negative impact of business continuity disturbances or information security breaches (consequences),
- ability to recover business processes to their original form after different types of incidents.

A business continuity management system and information security management system, similarly to other standardized systems (quality management, IT services management, occupational health and safety, environmental management system), are developed on the basis of the Deming cycle [8]. The cycle is also called PDCA (Plan-Do-Check-Act) as it divides management processes into four phases:

- Plan: processes related to the development of a project plan concerning the management on the basis of the developed method;
- Do: processes concerning a trial implementation of a plan and implementation of the method;
- Check: processes which assess whether the new method gives better results;
- Act: if a new method gives better results it should be considered as a standard (valid procedure), standardized, monitored and improved.

The “Act” phase includes the detection of inconsistencies between the management system and the current situation in the institution and its surroundings., The inconsistencies may emerge from organizational changes in the IT infrastructure or in the method of carrying out business processes. Additionally, new forms of threats make the management system incompatible with the new situation and require that it should be adapted to it. The postulated adaptation changes should be planned, fulfilled, checked and implemented for exploitation. This way the PDCA system shows its ability for self-adaptation.

Both management systems (BCMS and ISMS), based on the Deming cycle, were integrated with the use of a concept presented in [9]. The so called Integrated Security Platform (ISP) was introduced. The platform makes use of the common data base CMDB (Configuration Management Database) used in IT services management systems. The ISP platform ensures that management systems are integrated in their IT-related aspects (data and functions). The British standard BS PAS 99 [10] has been applied to deal with organization and procedures. The requirements of the standard assume that a common part of the management systems co-existing in an institution should be identified. This common part is implemented in the same way for all integrated systems. Elements which are specific for particular systems are implemented separately for each system. The objective of the management systems integration is to lower the costs and improve management efficiency (fewer procedures and less information generated by particular systems).

The OSCAD project [11] is patterns-based, i.e. a set of design patterns was prepared to develop BCMS/ISMS systems. It was assumed that OSCAD would not be a product dedicated to one concrete client but a set of pre-defined modules (patterns) each time adapted to the previously identified needs of the client. This way the solution was more open and scalable, yet it required a special method. The method had to determine how to build a concrete system, for a concrete client, out of predefined modules. In particular, the following products were developed within the OSCAD project:

- methodology of building an open, framework-based, integrated system for business continuity and information security management, making use of pattern modules,
- methodology of implementing a system, based on the identification of the needs and requirements of a client who plans the implementation and on the development or adaptation of pattern modules into the form of final modules based on these needs and requirements,
- software supporting the implementation process and then the exploitation of the integrated system for business continuity and information security management,
- software for building a system for the collection, analysis and access to statistical information about threats, vulnerabilities and incidents which disturb business process of an institution,
- knowledge necessary to implement and use such a system.

The OSCAD project developed the following products: knowledge, software, patterns, and a method to use these patterns to build a system for the given institution. Apart from a general-purpose version, there are dedicated versions of the system for particular application domains.

The general diagram of the integrated system can be seen in Fig. 1. In the central part there is the main OSCAD component which offers role-dependent interfaces (shown on the left side of the figure) for different users: managers, people who conduct analyses, particularly risk analysis, people who manage incidents, prepare reports, and maintenance personnel.

OSCAD communicates with the surroundings by means of different interfaces which transfer warning messages (lower part of the figure):

- from ERP systems (Enterprise Resource Planning), e.g. about the decreasing number of components for production,
- from SCADA systems (Supervisory Control and Data Acquisition) which supervise the automated production process, e.g. about events occurring in the production process,
- from systems monitoring the functioning of IT infrastructure and other technical infrastructures, e.g. about IT-related breakdowns and other incidents,
- from anti-burglar exchanges, e.g. about breaches in limited access zones,
- from fire detection alarms, e.g. about fire symptoms,
- from other OSCAD systems operating in the organizations functioning within the supply chain.

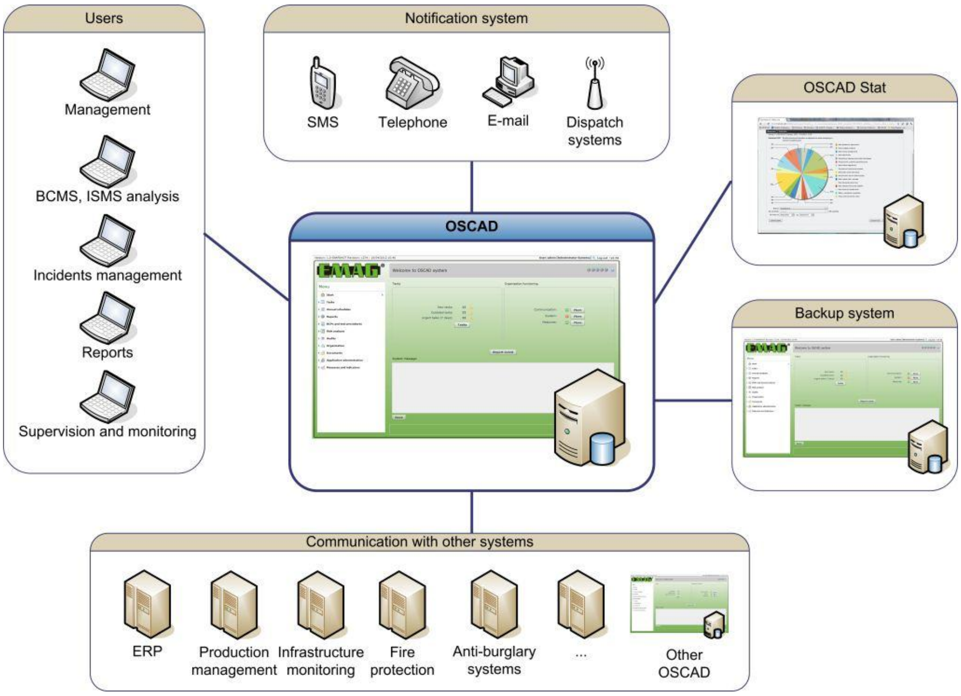


Fig. 1. Diagram of the OSCAD system
Source: EMAG's documentation, 2012

Each OSCAD has its own communication system (e-mail, mobile devices, telephone, etc.) for receiving and sending warnings and messages about tasks assigned to the managing personnel (upper part of the figure).

If there is a threat to the OSCAD system itself, the system gets switched to the OSCAD backup system. During the standby phase the backup system signals its readiness by means of a special signal (heart beat) and updates its data base following the changes in the base of the main system.

An extra element of the system is the OSCAD-STAT component. OSCAD-STAT receives information about completed incidents from one or a few OSCAD systems, prepares statistics which can be accessed by managers of the institutions and managers of OSCAD systems, and serves as an informational portal. Statistical data are the basis for corrections and improvements in management systems and can be helpful during the risk analysis.

The OSCAD system performs many functions which can be divided into several groups.

The **general-purpose functions** comprise the following:

- system management and data storage functions, including: management of users' roles and accounts, management of data describing the institution, its organizational structure, business processes, vocabulary, standards, patterns, etc.;
- documentation management functions responsible for the management of all documents produced or registered in the system, either as e-forms or files attached

to the system; all documents have identification numbers to enable their management;

- external communication functions making use of all sorts of communication interfaces for information exchange:
  - with other OSCAD systems, e.g. owned by institutions co-operating within a supply chain,
  - with the OSCAD-STAT system which collects and analyzes statistical data about incidents and gives access to these data in the form of statistics,
  - with the OSCAD backup system,
  - with different systems working in the institution's business surroundings,
  - with mobile phones access points.
- task management functions co-ordinate the performance of tasks assigned to people who play certain roles in the system; all management operations in the system are treated as tasks to be fulfilled; the tasks may be grouped in time in the form of timetables;
- reporting functions are responsible for making different types of reports; they support other usability functions of the system.

Risk management functions serve to:

- identify and specify the institution's business processes, taking into consideration information groups related to the fulfillment of particular processes;
- conduct an analysis of harmful influence of losing a continuity attribute on business processes and harmful influence on losing integrity, availability and confidentiality of information assets related to the given process; this type of analysis is called BIA (Business Impact Analysis) and corresponds to HLRA (High Level Risk Analysis); processes with critical significance for the institution are identified;
- collect detailed information about the institution's assets which need to be protected and are related to the fulfillment of business processes; these are functions conducted by the assets inventory;
- conduct LLRA (Low Level Risk Analysis) which allows to determine the risk value for each triple asset-threat-vulnerability; taking into account the existing security measures, their technical advancement and implementation level;
- select security measures which reduce the risk volume; security variants are defined; the most beneficial variant is considered for implementation, i.e. the one which can reduce the risk and implementation costs the most.

Incident management functions register events coming from different sources (simple forms filled by the users, SMSes, e-mails, ERP, monitoring systems which function in the surroundings, other OSCAD systems, etc.). Then each event is assessed by a responsible person. Events which are identified as potentially harmful are qualified as incidents and, depending on their kind and importance, adequate actions are undertaken – even up to initializing the business continuity plan. After the incident is finished, it is assessed, closed, reported and, after anonymization, can be registered by the OSCAD-STAT system. There are always conclusions drawn from incidents. This helps to avoid them in the future.

Audit and review functions manage information about conducted compliance audits or reviews; they generate reports and support the process of the reports acceptance. OSCAD has at its disposal a number of audit lists to get compliance with basic standards and laws. The lists facilitate the auditing process and half-automatic generation of reports. Timetabling functions are used to plan audits or reviews.

BCP (Business Continuity Plan) management functions support the user in the preparation, maintenance and testing of business continuity plans. The plans are developed for business processes which are critical for the institution's functioning. The plan indicates the assets necessary for its fulfillment, the environment of the fulfillment, list of contact persons engaged in the process, and operations to be carried out. The plans have to be periodically tested by the institution's employees. Tests are planned on the basis of timetabling functions.

Measures and indicators servicing functions allow to define and manage the measures and performance indicators as well as use them to improve the efficiency of operations (process improvement) and to conduct a risk analysis.

During the project it was assumed that Web browsers would be used as software interface and Java client-server architecture would be applied. The software was developed in two language versions – Polish and English.

4. Using OSCAD system to solve selected problems in public administration

In the course of the project there were a number of sample applications proposed which go beyond the original framework of the project (BCM/ISM). OSCAD can be a BCMS, an ISMS, or an integrated system playing these two roles simultaneously. Some OSCAD's elements support other management systems, particularly quality management (ISO 9001). A basic BCM/ISM version was developed, along with different sets of input information for this version (vocabulary, documents, roles, and other data). This allowed to make several sample domain versions and carry out feasibility studies for them:

- for a small production and services company (information security in business),
- for a middle-size research institute (information security in business),
- for a design office involved in the development of IT security according to the requirement of ISO/IEC 15408 Common Criteria (protection of sensitive data related to conducted projects),
- for a middle-size logistics company working in a supply chain (business continuity),
- for a middle-size town hall (information security in public administration),
- for a health service unit (business continuity of a health service unit and protection of data managed by the unit).

The system proved to be very flexible and configurable. Thanks to these features it can be used in different applications beyond the range stipulated by BS 25999 and ISO/IEC 27001. Thus the project team decided to go in for more complex and untypical applications for which it was necessary not only to acquire specific input data but also to partially modify the menu and contents of the messages sent to the user (without changing the software functions). The following feasibility studies were prepared in this respect:

- business continuity and protection of production assets of a coal mine (miners, machines, equipment, infrastructure, mining facilities, mining processes, personnel security, etc.),
- managing the preparedness of rescue services (considered as the protection of business continuity of these services) in a fire brigade and mining rescue team (under development),
- protection of an area against flood (English language version, FP7 ValueSec project [12], risk assessment for different types of anti-flooding security measures used in Germany, in the basins of the Elbe and Mulde rivers).

These examples show that the system is highly flexible and open to different applications (going beyond business continuity provision and information assets protection).

There are vast possibilities to use the OSCAD system and the related methodology in the public sector. First of all, these possibilities are related to typical applications described in standards. In public administration units it is necessary to provide business continuity and there are huge amounts of information which need to be protected.

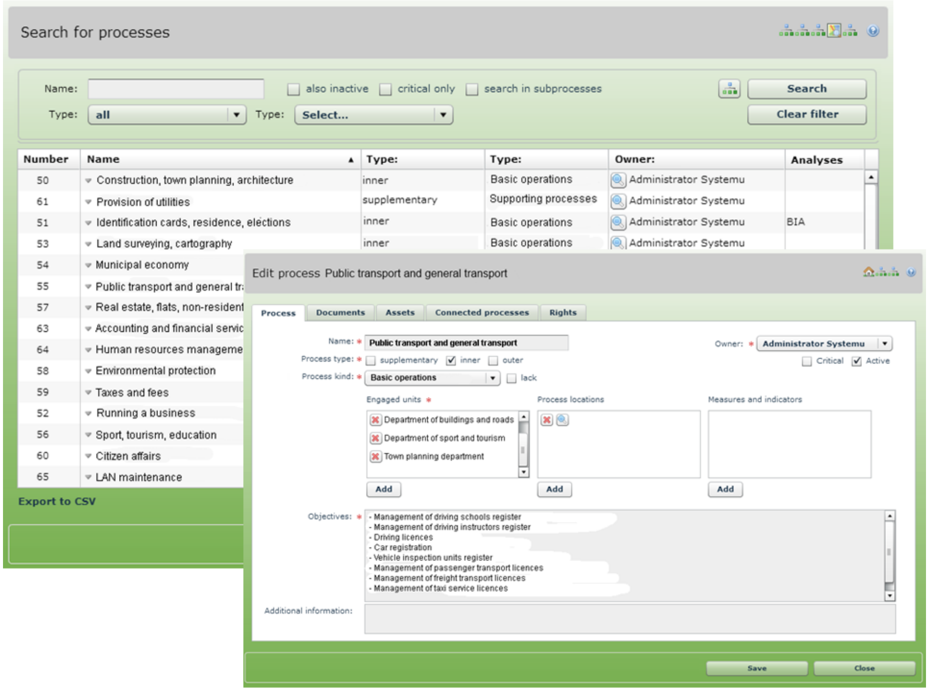
Public administration units of different levels are strongly dependent on information technology in their business operations. There is a strong need for interoperability and change management, along with a strong pressure to implement state-of-the-art information technologies. These factors speak the most for the need to provide secure, well managed solutions.

In the further part of the paper there are selected examples presented on the OSCAD methodology in the public sector.

4.1 Information security and business continuity in a middle-size town hall

Town halls tend to have problems in providing business continuity of processes responsible for public administration services for the citizens. There is also an issue of protecting huge amounts of information, including personal data. The solution to these issues may be the implementation of the integrated BCMS/ISMS based on the OSCAD system.

The system version for public administration was based on the analysis of issues typical for a public administration unit (on the example of a middle-size town hall). Additionally, the selected representative elements of such an office were implemented.



Search for processes

Name: □ also inactive □ critical only □ search in subprocesses [Search]

Type: all ▾ Type: Select... ▾ [Clear filter]

Number	Name ▲	Type:	Type:	Owner:	Analyses
50	Construction, town planning, architecture	inner	Basic operations	Administrator Systemu	
61	Provision of utilities	supplementary	Supporting processes	Administrator Systemu	
51	Identification cards, residence, elections	inner	Basic operations	Administrator Systemu	BIA
53	Land surveying, cartography	inner	Basic operations	Administrator Systemu	
54	Municipal economy				
55	Public transport and general tr				
57	Real estate, flats, non-resident				
63	Accounting and financial servic				
64	Human resources manageme				
58	Environmental protection				
59	Taxes and fees				
52	Running a business				
56	Sport, tourism, education				
60	Citizen affairs				
65	LAN maintenance				

Export to CSV

Edit process Public transport and general transport

Process | Documents | Assets | Connected processes | Rights

Name: * Public transport and general transport

Owner: * Administrator Systemu ▾

Process type: * □ supplementary ☑ inner □ outer

□ Critical ☑ Active

Process kind: * Basic operations ▾ □ lack

Engaged units *
- Department of buildings and roads
- Department of sport and tourism
- Town planning department

[Add]

Process locations

[Add]

Measures and indicators

[Add]

Objectives: *
- Management of driving schools register
- Management of driving instructors register
- Driving licences
- Car registration
- Vehicle inspection units register
- Management of passenger transport licences
- Management of freight transport licences
- Management of taxi service licences

Additional information:

[Save] [Close]

Fig. 2 OSCAD for public administration – business processes
Source: EMAG's documentation, 2012

The following operations were carried out:

- analysis of the organizational structure (organizational units, positions),
- analysis how a public administration unit functions with a view to determine typical processes and process groups in this unit,
- analysis of the key assets indispensable for the unit to carry out its key processes,
- assessment and selection of typical business threats for the functioning of public administration units,
- analysis how public administration units function with respect to information processed in them, determination of typical groups of the processed information,
- analysis and selection of threats and vulnerabilities typical in public administration units.

Based on the collected information, the selected and representative elements related to public administration units were expressed in the dedicated OSCAD system. Sample screens of the OSCAD version for public administration can be seen in Fig. 2.

In the background screen there is a list of business processes indentified in a public administration unit, while in the foreground – an edition window of a process with the data concerning "Public transport and general transport".

The conducted case study shows how to develop a computer-aided integrated (BCMS/ISMS) management system which fulfills all requirements of the BS25999-2 and ISO/IEC 27001 standards in middle- and high-level public administration units. To implement the system in small units, a preliminary analysis is required along with the adaptation to the conditions of a small community. The system needs to be simplified in the range of the policy, roles, procedures, documents, and performed functions.

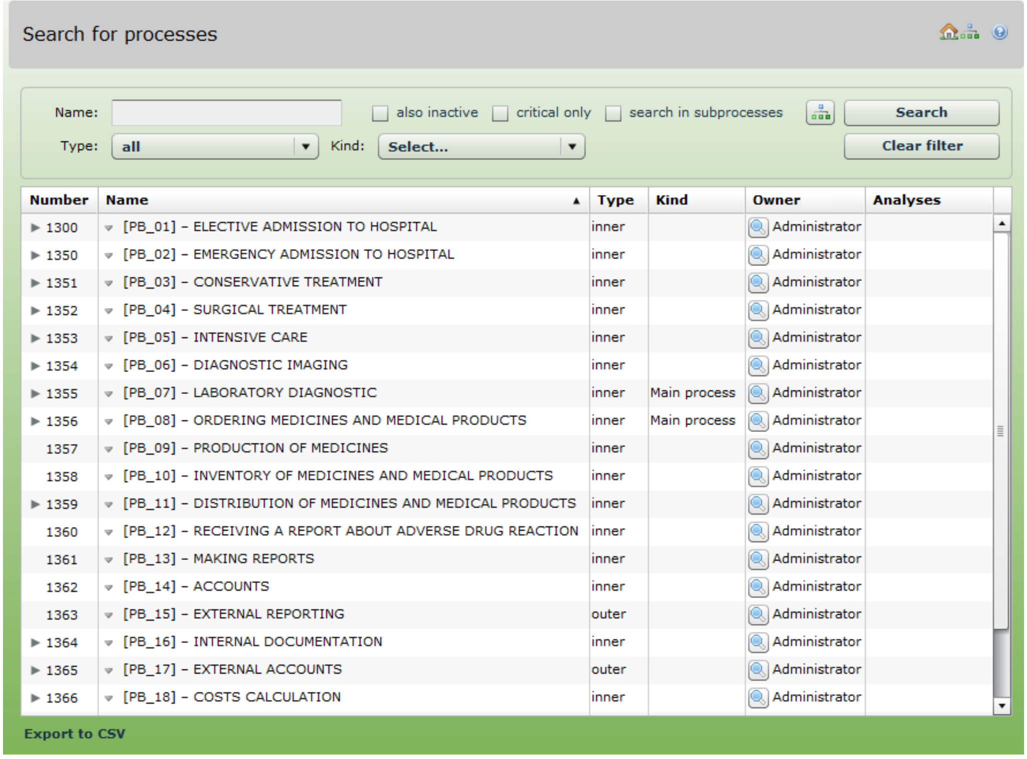
4.2 Information security and business continuity in health service and public insurance organizations

There is a common need to protect information and provide business continuity in the health service sector, however, the needs of national health service units and social insurance units are different in this respect than those of hospitals and doctors' surgeries.

The case study was conducted for a large hospital. First the departments and organizational units of the hospital were identified (director's office, reception, surgery wards, operating theatre, diagnostics, etc.). Then, a list of key positions was prepared for each organizational unit. Key processes and protected assets were identified, along with the related sample threats, vulnerabilities and proposed security measures.

After the analysis of a health service organization, the collected data were entered into the OSCAD system. Figure 3 features an example of such data, i.e. a list of business processes identified in a typical hospital.

A BIA analysis [13] was conducted for selected processes, as well as a detailed risk analysis with respect to business continuity and protection of the patients' medical data.



Search for processes

Name: ▭ □ also inactive □ critical only □ search in subprocesses Search

Type: all ▾ Kind: Select... ▾ Clear filter

Number	Name ▲	Type	Kind	Owner	Analyses
▶ 1300	[PB_01] – ELECTIVE ADMISSION TO HOSPITAL	inner		Administrator	
▶ 1350	[PB_02] – EMERGENCY ADMISSION TO HOSPITAL	inner		Administrator	
▶ 1351	[PB_03] – CONSERVATIVE TREATMENT	inner		Administrator	
▶ 1352	[PB_04] – SURGICAL TREATMENT	inner		Administrator	
▶ 1353	[PB_05] – INTENSIVE CARE	inner		Administrator	
▶ 1354	[PB_06] – DIAGNOSTIC IMAGING	inner		Administrator	
▶ 1355	[PB_07] – LABORATORY DIAGNOSTIC	inner	Main process	Administrator	
▶ 1356	[PB_08] – ORDERING MEDICINES AND MEDICAL PRODUCTS	inner	Main process	Administrator	
1357	[PB_09] – PRODUCTION OF MEDICINES	inner		Administrator	
1358	[PB_10] – INVENTORY OF MEDICINES AND MEDICAL PRODUCTS	inner		Administrator	
▶ 1359	[PB_11] – DISTRIBUTION OF MEDICINES AND MEDICAL PRODUCTS	inner		Administrator	
1360	[PB_12] – RECEIVING A REPORT ABOUT ADVERSE DRUG REACTION	inner		Administrator	
1361	[PB_13] – MAKING REPORTS	inner		Administrator	
1362	[PB_14] – ACCOUNTS	inner		Administrator	
1363	[PB_15] – EXTERNAL REPORTING	outer		Administrator	
▶ 1364	[PB_16] – INTERNAL DOCUMENTATION	inner		Administrator	
▶ 1365	[PB_17] – EXTERNAL ACCOUNTS	outer		Administrator	
▶ 1366	[PB_18] – COSTS CALCULATION	inner		Administrator	

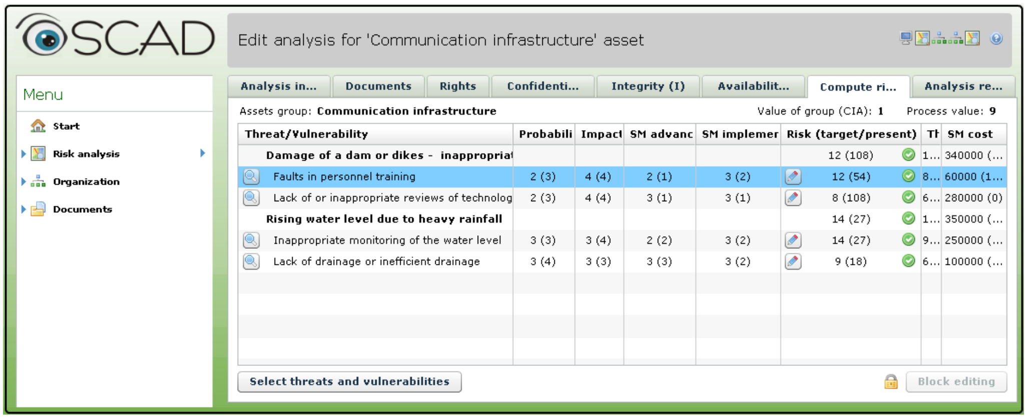
Export to CSV

Fig. 3 OSCAD for a health service organization – business processes
Source: EMAG's documentation, 2012

The case study showed that the OSCAD system can be used to protect business continuity of a hospital and the patients' data processed by the hospital.

4.3 Selecting security measures to reduce the risk of flood

This is not a typical example of OSCAD's application. It is related to EMAG's participation in the EU FP7 project "ValueSec – Mastering the Value Function of Security Measures", carried out with partners from Germany, Norway, Spain, Finland, and Israel. The objective of the project is to support the users in the range of the selection and assessment of planned security measures. The assessment is usually made with respect to the results of conducted analyses of losses and benefits, risk analyses, business impact analyses. Therefore the project consortium decided to use OSCAD (along with three other tools) in the ValueSec system as a component of conducting the risk assessment and providing risk assessment results. These results are then used as input data for the ValueSec software for further analysis and selection of security measures (taking into consideration the costs, benefits and quality criteria).



Edit analysis for 'Communication infrastructure' asset

Assets group: **Communication infrastructure** Value of group (CIA): **1** Process value: **9**

Threat/Vulnerability	Probabili	Impact	SM advanc	SM implemer	Risk (target/present)	Th	SM cost
Damage of a dam or dikes - inappropriat					12 (108) ✓	1...	340000 (...
Faults in personnel training	2 (3)	4 (4)	2 (1)	3 (2)	12 (54) ✓	8...	60000 (1...
Lack of or inappropriate reviews of technolog	2 (3)	4 (4)	3 (1)	3 (1)	8 (108) ✓	6...	280000 (0)
Rising water level due to heavy rainfall					14 (27) ✓	1...	350000 (...
Inappropriate monitoring of the water level	3 (3)	3 (4)	2 (2)	3 (2)	14 (27) ✓	9...	250000 (...
Lack of drainage or inefficient drainage	3 (4)	3 (3)	3 (3)	3 (2)	9 (18) ✓	6...	100000 (...

Fig. 4 OSCAD in the field of communal security – anti-flood measures based on risk analysis
Source: EMAG’s documentation, 2013

The English version of the OSCAD software was prepared for the ValueSec project. This way the system could be presented outside Poland. The expanded functionality of the software was reduced to risk management functions. This was achieved by defining proper roles in the system with the rights restricted to risk management (Fig. 4 – left-side menu).

OSCAD – Risk manager was used in one of five application domains (contexts) of ValueSec. One of these applications is communal security, particularly “Flood use case”. EMAG, in co-operation with the Fraunhofer Institute for Factory Operation and Automation IFF (FhG/IFF) from Germany, prepared input data for this use case based on the flood reports of the Elbe and Mulde rivers basin and information obtained from German institutions: Ministerium für Inneres und Sport des Landes Sachsen-Anhalt and Ministerium für Landwirtschaft und Umwelt des Landes Sachsen-Anhalt.

Based on the collected data a risk analysis was conducted. The figure shows the analysis for the “communication infrastructure” asset which is protected against flooding. The analysis for each risk case enabled to further analyze five different security variants and assess their risk reduction ability. The selected most efficient variant is submitted to further analysis which is carried out in other ValueSec framework components (Cost-Benefit Analysis, Qualitative Criteria Analysis). This is the basis to recommend security measures which reduce the risk, are cost-effective and have restrictions accepted by decision makers.

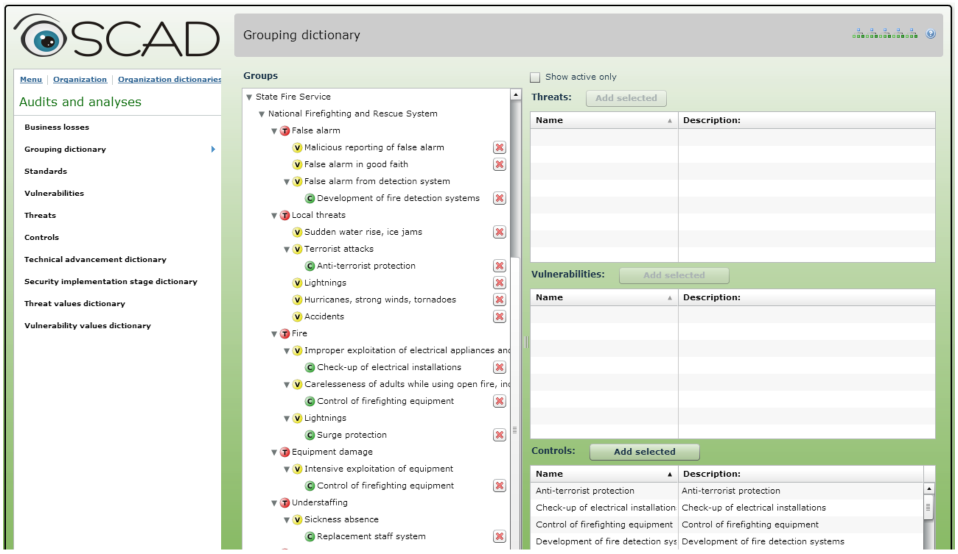
Additionally, management processes responsible for anti-flood protection were identified and the risk analysis concerning their continuity was conducted. Yet this issue is not applicable to the ValueSec project.

At the moment the first stage of the validation has been completed based on the data from reports and from the above mentioned institutions. Next, OSCAD will be validated with the participations of experts from these institutions.

While preparing a case study, a different approach was necessary for a new application domain. For example, instead of information assets there are physical assets that are protected against the flood, such as human health and lives, property, transport infrastructure, etc. That is why the data operated by the OSCAD system had to be changed, along with the language to communicate with the user – it had to be adapted to a different application domain. Operation mechanisms did not change thus the logic of the software remained the same.

4.4 Management of rescue services preparedness and risk in fire brigades

There was a strong analogy observed between business continuity and preparedness of different kinds of rescue services (readiness to assist in need). For example, an incident for a fireman is not a fire as such but something that disturbs its extinguishing – this situation breaches the fireman's preparedness to operate.



☐ Show active only

- State Fire Service
  - National Firefighting and Rescue System
    - T False alarm
      - V Malicious reporting of false alarm
      - V False alarm in good faith
      - V False alarm from detection system
        - C Development of fire detection systems
    - T Local threats
      - V Sudden water rise, ice jams
      - V Terrorist attacks
        - C Anti-terrorist protection
      - V Lightnings
      - V Hurricanes, strong winds, tornadoes
      - V Accidents
    - T Fire
      - V Improper exploitation of electrical appliances and
        - C Check-up of electrical installations
      - V Carelesseness of adults while using open fire, inc
        - C Control of firefighting equipment
      - V Lightnings
        - C Surge protection
    - T Equipment damage
      - V Intensive exploitation of equipment
        - C Control of firefighting equipment
    - T Understaffing
      - V Sickness absence
        - C Replacement staff system

Threats:

Name	Description:

Vulnerabilities:

Name	Description:

Controls:

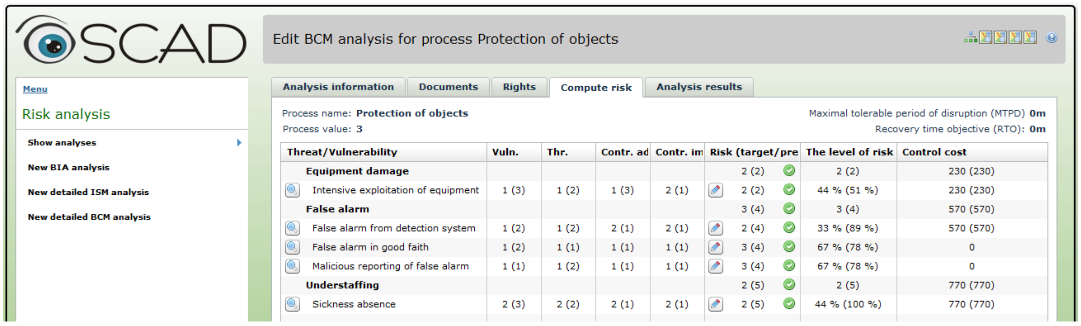
Name	Description:
Anti-terrorist protection	Anti-terrorist protection
Check-up of electrical installation	Check-up of electrical installations
Control of firefighting equipment	Control of firefighting equipment
Development of fire detection sys	Development of fire detection systems

Fig. 5 OSCAD for fire protection – defining domain vocabulary
Source: EMAG's documentation, 2013

This is another example of an untypical application domain, requiring to have a communication language between the software and its user. At the same time OSCAD can be used to conduct a risk analysis for assets that are threatened by a fire. There were dictionaries of threats, vulnerabilities and security measures developed for a version for the fire services, similarly to other dedicated versions, as demonstrated in Fig. 5.

During the risk analysis there were two cases considered:

- analysis of threats disturbing the continuity of the process "Protection of objects" understood as the preparedness for a rescue operation; in the OSCAD system it is a BCM analysis (Fig. 6).
- analysis of threats to protected facilities, e.g. public utility buildings; in the OSCAD system it is an ISM analysis (Fig. 7).



Edit BCM analysis for process Protection of objects

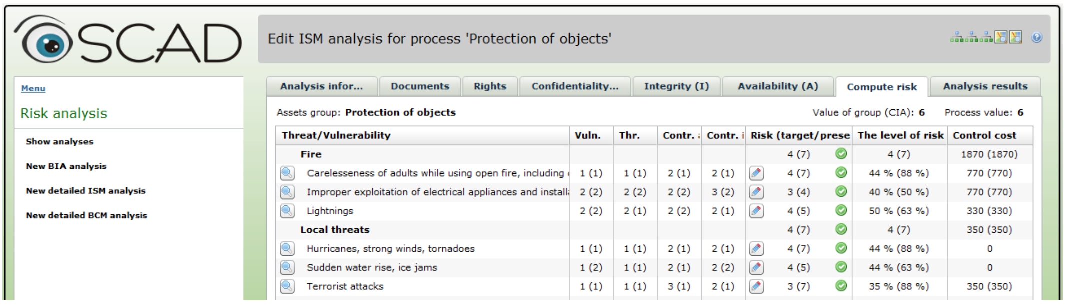
Process name: **Protection of objects**
Process value: **3**

Maximal tolerable period of disruption (MTPD) **0m**
Recovery time objective (RTO): **0m**

Threat/Vulnerability	Vuln.	Thr.	Contr. ad	Contr. im	Risk (target/pre	The level of risk	Control cost
Equipment damage					2 (2) ✓	2 (2)	230 (230)
Intensive exploitation of equipment	1 (3)	1 (2)	1 (3)	2 (1)	2 (2) ✓	44 % (51 %)	230 (230)
False alarm					3 (4) ✓	3 (4)	570 (570)
False alarm from detection system	1 (2)	1 (2)	2 (1)	2 (1)	2 (4) ✓	33 % (89 %)	570 (570)
False alarm in good faith	1 (2)	1 (1)	1 (1)	1 (1)	3 (4) ✓	67 % (78 %)	0
Malicious reporting of false alarm	1 (1)	1 (2)	1 (1)	1 (1)	3 (4) ✓	67 % (78 %)	0
Understaffing					2 (5) ✓	2 (5)	770 (770)
Sickness absence	2 (3)	2 (2)	2 (1)	2 (1)	2 (5) ✓	44 % (100 %)	770 (770)

Fig. 6 OSCAD in fire protection – risk analysis concerning preparedness for operation
Source: EMAG's documentation, 2013

The conducted case study was restricted to the risk analysis process in the two above cases.



Edit ISM analysis for process 'Protection of objects'

Assets group: **Protection of objects**

Value of group (CIA): **6**
Process value: **6**

Threat/Vulnerability	Vuln.	Thr.	Contr. a	Contr. i	Risk (target/prese	The level of risk	Control cost
Fire					4 (7) ✓	4 (7)	1870 (1870)
Carelessenes of adults while using open fire, including	1 (1)	1 (1)	2 (1)	2 (1)	4 (7) ✓	44 % (88 %)	770 (770)
Improper exploitation of electrical appliances and install	2 (2)	2 (2)	2 (2)	3 (2)	3 (4) ✓	40 % (50 %)	770 (770)
Lightnings	2 (2)	2 (1)	2 (2)	2 (1)	4 (5) ✓	50 % (63 %)	330 (330)
Local threats					4 (7) ✓	4 (7)	350 (350)
Hurricanes, strong winds, tornadoes	1 (1)	1 (1)	2 (1)	2 (1)	4 (7) ✓	44 % (88 %)	0
Sudden water rise, ice jams	1 (2)	1 (1)	2 (1)	2 (2)	4 (5) ✓	44 % (63 %)	0
Terrorist attacks	1 (1)	1 (1)	3 (1)	2 (1)	3 (7) ✓	35 % (88 %)	350 (350)

Fig. 7 OSCAD in fire protection – risk analysis for a fire-threatened facility
Source: EMAG's documentation, 2013

The work is underway on a more extensive use of OSCAD, i.e. to register incidents and create a statistical data base for them.

5. Conclusions

The above examples show that OSCAD's products are useful to solve information security and business continuity issues in different types of public administration units, in compliance with ISO/IEC 27001 and BS 25999.

During the validation works the flexibility and openness of OSCAD's products were observed. Thanks to that, these products were applied in domains which had not been considered previously. The results of these experiments are encouraging and may extend the range of the project application. This is important as the recently completed project has just entered the phase of intensive implementation works.

So far the focus has been on simple applications, based on one software instance. Vast possibilities of connectivity enable to build more complex OSCAD systems which can solve business continuity and information security issues for several public administration units with backup systems. There is an analogy here to a supply chain in production facilities. The administration units can communicate messages, including warnings, and can build and use a common statistical data base about incidents.

Acknowledgements

The author wishes to thank the members of the OSCAD project team who were engaged in the fulfillment of the case study and preparation of the dedicated software versions.

References

[1] BS 25999-1:2006 Business Continuity Management – Code of Practice.

[2] BS 25999-2:2007 Business Continuity Management – Specification for Business Continuity Management.

[3] ISO 22301:2012 Societal security – Business continuity management systems – Requirements.

[4] ISO/IEC 27001:2005 Information technology – Security techniques – Information security management systems – Requirements.

[5] ISO/IEC 27002 Information security – Security techniques – Information security management systems – Code of practice.

[6] ISO 31000:2009 – Principles and Guidelines on Implementation.

[7] ISO/IEC 27005:2008 Information technology – Security techniques – Information security risk management.

1 http://pl.wikipedia.org/wiki/Cykl_Deminga

2 Białas A.: *Development of an Integrated, Risk-based Platform for Information and E-services Security*. In: Górski J.: Computer Safety, Reliability, and Security, 25th International Conference SAFECOMP2006, Springer Lecture Notes in Computer Science (LNCS4166), Springer Verlag Berlin Heidelberg New York 2006, ISBN 3-540-45762-3, pp. 316-329.

3 BS PAS 99:2006, Specification of common management system requirements as a framework for integration.

4 Computer-supported business continuity management system – OSCAD project reports, Instytut EMAG, Katowice, 2010-2012 (in Polish), http://oscad.eu

5 FP7 ValueSec: http://valuesec.eu

6 Bagiński J, Rostański M.: *The modeling of Business Impact Analysis for the loss of integrity, confidentiality and availability in business processes and data.* Theoretical and Applied Informatics, Vol. 23 (2011), no.1, pp. 73-82. ISSN 1896-5334.

Bezpieczeństwo informacji i ciągłość działania w administracji publicznej

Streszczenie

Artykuł przedstawia wybrane aspekty zarządzania bezpieczeństwem informacji i ciągłością działania w administracji publicznej na przykładach zastosowań zintegrowanego, wspomaganego komputerowo systemu OSCAD. Na wstępie zwrócono uwagę, że jednostki administracji publicznej dysponują ogromnymi zasobami informacji o strategicznym znaczeniu, a także realizują odpowiedzialne zadania na potrzeby państwa, grup społecznych i poszczególnych obywateli. Implikuje to zarówno potrzebę zapewnienia bezpieczeństwa informacji, jak również zapewnienia ciągłości działania w tych jednostkach.

OSCAD opracowano na podstawie międzynarodowych standardów zarządzania opartych na cyklu Deminga: ISO/IEC 27001 dotyczącego bezpieczeństwa informacji oraz BS 25999 (ISO 22301) dotyczącego zagadnienia ciągłości działania. Produkty projektu OSCAD to: wzorce budowy komponentów systemów zarządzania, metodyka ich przystosowania do potrzeb danej instytucji wdrażającej, oprogramowanie wspomagające oraz wiedza potrzebna do budowy tego typu systemów zintegrowanych.

Przedstawiono budowę oprogramowania OSCAD (Fig. 1), wskazując komponent podstawowy, zapasowy oraz serwer danych statystycznych. Przedstawiono bogate możliwości komunikacji między systemami OSCAD, ich użytkownikami i otoczeniem. W zarysie scharakteryzowano funkcjonalność systemu, zwracając uwagę na jego możliwości w zakresie zarządzania ryzykiem, incydentami, dokumentami, audytami, przeglądami, planami i zadaniami. Poza tymi typowymi funkcjami, oprogramowanie OSCAD jest wyposażone w rozbudowany podsystem raportowania oraz podsystem mierników i wskaźników kontrolujących efektywność procesów zarządzania, jak również procesów w samej instytucji, w przypadku szczególnym rozumianej jako jednostka administracji publicznej.

System ma charakter otwarty i podczas wdrożenia wymaga przystosowania do realiów instytucji, w tym identyfikacji potrzeb instytucji, opracowania słowników, miar ryzyka, dokumentów, procedur, itp. Artykuł prezentuje w zarysie wersję systemu OSCAD dedykowaną dla miasta średniej wielkości (Fig. 2) oraz wersję dla większego szpitala (Fig. 3). W toku procesu walidacji systemu OSCAD zauważono możliwości jego zastosowania wychodzące poza zakres opisany w normach będących podstawą projektu (ochrona zasobów informacji i procesów działania). Opracowano kolejne wersje, z których dwie pokazano w niniejszym artykule. Fig. 4 przedstawia system OSCAD przystosowany do ochrony przeciwpowodziowej (wykorzystany w ramach EC FP7 ValueSec). Tu zasobami chronionymi jest ludność, dobytek, zwierzęta i infrastruktura na określonym obszarze państwa (w tym przypadku Niemiec). Opracowano również wersję systemu służącą do analizy ryzyka wybuchu pożaru w określonym obiekcie (Fig. 7) oraz do analizy ryzyka utraty gotowości do działania służb ratunkowych (Fig. 6). Każda wersja dedykowana wymaga opracowania słownictwa (Fig. 5), różnych miar i innych danych, specyficznych dla dziedziny zastosowań.

W podsumowaniu zwrócono uwagę na dużą otwartość i elastyczność oprogramowania. W zasadzie żadna z wersji dedykowanych nie wymagała zmiany kodu oprogramowania, a samo przystosowanie ograniczało się do słownictwa i danych dziedzinowych.