dr hab. inż. ANDRZEJ BIAŁAS
Instytut Technik Innowacyjnych EMAG

Management of business continuity, information security and security of other assets in the mining industry

The paper discusses the methods to solve selected issues of business continuity and protection of assets, including information assets, in mining companies with the use of an integrated computer-aided management system OSCAD. The system is based on international standards BS 25999/ISO 22301 (business continuity) and ISO/IEC 270001 (information security). First, the structure and possibilities of the tool was presented, with focus on these functions which, according to the author, are most useful in the conditions of a mine, i.e. analysis of incidents and resulting losses, preparation of related statistics, analysis of security parameters and production parameters, and finally risk management. The data collected during these analyses can be used by the mine's managers to improve production processes and safety of the mining personnel. The issues discussed in the article concern the mine (mining process) and, partly, companies which coordinate the work of the mine (management processes). In the summary, the author pointed at other potential applications of the OSCAD software in the mining industry.

1. INTRODUCTION

Ensured business continuity and protected assets of an organization are the factors which positively impact the efficiency of its operations. This objective is fulfilled by monitoring the factors which may disturb proper functioning of the organization or threaten its assets. During the risk analysis process harmful factors are predicted and, when they actually take place, there is a planned reaction aimed at reducing the losses and recovering the organization's business processes to a required level.

These issues are solved differently in different business domains, depending on business requirements, the organization's specifics and the nature of harmful factors. The article presents these issues with respect to a mining company, on two levels:

- business level, with respect to a company which coordinates the work of mines; here it is important to note that business operations of the company are similar to the operations of other companies, working outside the mining industry;
- level of the coal extraction process carried out in the mine; here we encounter issues characteristic of the mine.

The article shows how these issues can be solved by applying the products of the recently completed specific-targeted project OSCAD (Open, scalable, integrated, computer-aided system for business continuity management) which was co-financed by the National Centre for Research and Development (NCBiR) and the Institute of Innovative Technologies EMAG [1]. The OSCAD project has the following results:

1. A set of design patterns for establishing and implementing a business continuity and information security management system in an organization. It includes a system framework where management processes, compliant with the standard requirements, are placed. The design patterns concern: the specification of the management process, security and business continuity requirements, instructions and other documents.
2. A methodology of implementing a business continuity and information security system in differ-

ent types of organizations. It determines how to build, based on the above mentioned patterns, a management system for the given organization and comprises: examination of the organization's business structure; elaboration of information security management policy and business continuity management policy, with assumptions for the system documentation; analysis of business processes; preparation of business continuity plans; analysis of business needs and risks of the given organization; selection of security measures with the method of their implementation, maintaining and monitoring the achieved security and business continuity levels, including audits and reviews.

3. OSCAD software supporting the implementation process and then the exploitation of the system for business continuity and information security management. The tool is equipped with a server providing information about incident statistics – OSCAD-STAT.
4. Knowledge necessary to implement a business continuity and information security system; the knowledge has been included in manuals how to use, administer and implement the OSCAD system.

The basic version of OSCAD, worked out in the course of the specific-targeted project, was developed based on the following world standards:

- BS 25999 [2], [3], concerning the development of business continuity management systems (BCMS) in organizations; recently this standard has been replaced by ISO 22301 [4] (an extended version with a wider international impact);
- ISO/IEC 27001 [5], [6] concerning the development of information security management systems (ISMS) in organizations.

Business continuity [2], [3] is defined as a strategic and tactical ability of the organization to:

- 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.

The availability of processes (or services) is understood as business continuity. In the conditions of a mine the issue of business continuity is present both on the level of the coordinating company and the mine level. Yet, there are different disturbing factors in each case.

Information security [5], [6] is the protection of information against the breach of its basic attributes, such as integrity, confidentiality and availability – irrespective of the information form and place (information processed, stored, transferred by systems, printed, voiced, pictured). Ensuring the integrity of information should be understood as a set of operations aimed at preventing its forgery or deletion. Protecting the availability of information (process, service) means that the information should be available in the planned time solely to an authorized subject. In the case of confidentiality, the objective is to ensure that the information is not disclosed to unauthorized subjects.

In the conditions of a mine, the issue of information security is present on both levels considered in this article, however, the nature of information security is different in each case.

As it was mentioned before, information is an asset which can be protected according to ISO/IEC 27001. In the course of the OSCAD project it was observed that there are similarities between the protection of information and the protection of other assets. In general, an asset should be always protected against threats which may exploit its vulnerabilities (weak points of the protection system), thus leading to consequences (losses). Some of these events may not be very harmful, therefore are not taken into account. Others may result in significant losses and then are called incidents. In the systems designed to protect different types of assets there is a risk that the threats will materialize as incidents [7], [8]. The use of security measures allows to reduce the risk. An extensive presentation of risk analysis and risk management issues can be found in the monograph [9]. The protection methods of different types of asses were analyzed. This was the basis to develop different versions of OSCAD, dedicated to other applications, i.e. to protect assets other than information assets.

One of the dedicated versions was prepared to protect the production assets of a mine. The assets are technologies and personnel involved in the mining process. The protection of such assets can be looked at from the point of view of integrity and availability, as confidentiality is not applicable here.

Other examples of dedicated versions are the following: to plan and support operations related to the risk of fire [10] and to protect people, property and infrastructure against floods [10]. The latter dedicated version (the so called OSCAD-Flood) is used as a risk assessment component in protection against floods occurring in the land of Saxony-Anhalt, Germany – this is one of five use cases of the EC FP7 ValueSec project [11].

OSCAD is an integrated system, which means that it concerns more than one management aspect of the

organization (here: business continuity and information security) with a possibility to extend it by other aspects (quality, environment, occupational safety, etc). Such systems are built in compliance with popular standards (ISO 9001, ISO 14000, ISO 18000) based on the so-called Deming cycle (PDCA – Plan-Do-Check-Act) [12]. The integration of such systems on the organizational and procedural level is carried out with the use of the British standard BS PAS 99 [13].

OSCAD is a computer-aided system as it comprises both the level of procedures and organization and the level of software for supporting management processes. From the point of view of IT, the integration was performed on the level of a common data base [14]. The most complex, repeatable or laborious operations are carried out with the use of this specialized software. The achieved benefits are similar to the benefits from CAD/CAM systems for computer-aided design or production.

OSCAD is an open system that can be applied in organizations of different sizes and profiles. However, as it was mentioned before, each time the system has to be somehow adapted to the needs of the given domain. In typical applications, within the ranges covered by ISO 22301 and ISO/IEC 27001, the adaptation range is smaller. It is limited to the preparation of dictionaries, roles, documents, standard assets lists, threats, and vulnerabilities in the course of the risk analysis process. In the case of the so called dedicated version, e.g. the version for mines, the adaptation range is wider. It can include the preparation of data for the domain description, specific external interfaces, and even modified captions in software menus and messages.

The article presents briefly the functionality of the OSCAD system, identifies the issues of business continuity and assets protection on the level of the coordinating company and the mine. Then the proposals are given how to solve the most important problems on these two levels. The author indicates a few possible tasks which can be fulfilled with the use of the OSCAD system. In the summary some other possibilities of OSCAD application in the mining industry are mentioned.

2. OSCAD ARCHITECTURE AND FUNCTIONS OF THE OSCAD SOFTWARE

The diagram of the OSCAD system, based on the client-server approach, can be seen in Fig. 1. The users contact the server by means of web browsers.

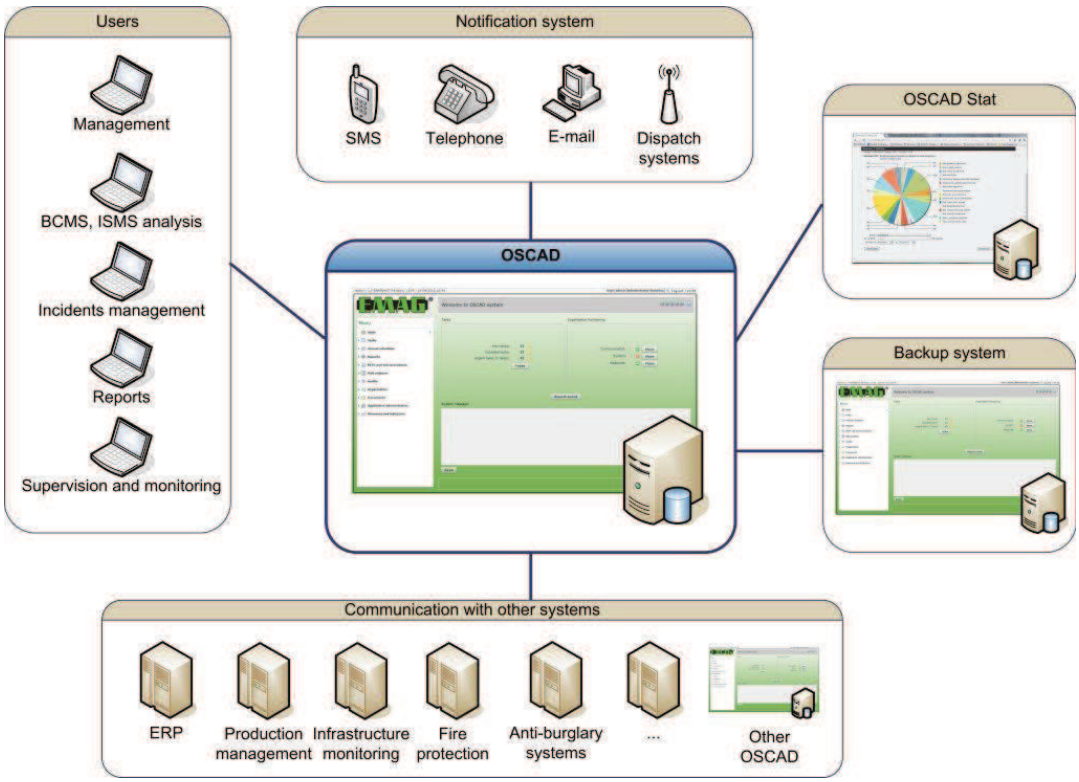

Fig. 1. Diagram of the OSCAD system
Source: EMAG's documentation

The diagram is general enough to suit both the basic version of the system and dedicated versions. In the middle there is the main OSCAD component which offers interfaces for different users according to their roles: for administrators, for managers, for people conducting analyses – particularly risk analyses, for incident management staff, for people who prepare reports, and for maintenance personnel. In the case of dedicated versions there are specific roles defined, i.e. those related to certain functions. For example, in the version for mines these can be: a supervisor, foreman, occupational safety inspector.

The OSCAD system was equipped with a number of interfaces to communicate with the surroundings. The interfaces are to collect information, including warning messages from the environment, particularly:

- from ERP systems (Enterprise Resource Planning), e.g. reporting the decreasing number of production components,
- from SCADA systems (Supervisory Control and Data Acquisition) which supervise the automated production process, e.g. about events which occur in the manufacturing process,
- from systems monitoring the functioning of IT infrastructure and other technical infrastructures, e.g. about breakdowns in IT infrastructure and other incidents,
- from anti-burglar exchanges, e.g. about breaches in restricted-access zones,
- from fire detection alarms, e.g. about fire symptoms.

The given OSCAD component communicates (e.g. by sending warnings about threats and vulnerabilities) with other OSCAD components working in companies which function within the given supply chain. This possibility can be used for communication between the OSCAD component of the coordinating company and the OSCAD components of the mines.

In the case of the mine-dedicated version, it is possible, through the available interfaces, to connect with the systems existing in the mine. Now there is a connection with the SD 2000 supervision system which monitors production and security parameters. Connections with similar systems are possible too, e.g. with the THOR system made by SEVITEL.

Each OSCAD component was equipped with a communication subsystem (e-mail, mobile devices, telephone, etc.) for receiving and sending warnings and messages about tasks assigned to the managing personnel. Here it is possible to connect OSCAD with mining telecommunications and communication systems.

If there is a threat to the OSCAD component, the system is switched to the OSCAD backup component. It is possible due to the fact that during routine work the backup OSCAD replicates data bases and exchanges the standby signal.

A significant element of the system is the OSCAD-STAT module which receives information about completed incidents from one or a few OSCAD components, prepares statistics which can be accessed by managers of the organizations and managers of OSCAD systems. Statistical data are used to make corrections and improvements in management systems. They are also helpful during the risk analysis process (for periodic verification of risk prognoses). These operations facilitate expanded reporting functions. In the case of the version dedicated to the mine these can be any defined statistics about safety, downtimes, breakdowns, etc. It is enough to have one OSCAD-STAT component for the whole organization. Collecting extensive information about incidents and their causes allows to improve security systems, management- and maintenance processes.

The OSCAD system performs several groups of functions. **General-purpose functions** comprise the following:

- administration and data storage functions for: management of users' roles and accounts, management of data describing the organization, its structure, business processes, vocabulary, standards, patterns, etc.;
- documentation management functions; all documents produced or registered in the system have their identification numbers to enable their management; the documents can be e-forms or files attached to the system;
- external communication functions: all sorts of communication interfaces for information exchange;
- task management functions; they 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 and have to be fulfilled; the tasks may be grouped in time in the form of timetables;
- reporting functions responsible for generating different types of reports, including comparative reports.

Risk management functions are responsible for the following:

- identification and specification of the organization's business processes, with consideration of information groups related to the fulfillment of particular processes;

- conducting BIA (Business Impact Analysis); the consequences of losing the availability attribute of a given process are examined in terms of several time horizons, along with the consequences of losing the integrity, availability and confidentiality attributes of information assets (integrity and availability for other assets); the consequences determine harmful influence of this situation on the organization's functioning; this type of analysis is called HLRA (High Level Risk Analysis); processes with critical significance for the organization are identified and maximum tolerable unavailability periods are determined for particular processes; this analysis is thus focused on the negative impact on the fulfillment of business tasks resulting from the predicted incidents;
- collecting detailed information about the organization's assets which need protection and are related to the fulfillment of business processes; these functions are conducted by the assets inventory; in the basic version IT assets are taken into account, while in dedicated versions – other assets that have to be protected, e.g. human life and health;
- conducting LLRA (Low Level Risk Analysis); this analysis enables to determine the risk value for each triple asset-threat-vulnerability (risk scenario); the existing security measures are taken into account, their technical advancement (automatic, procedural) and implementation level (planned, implemented, functioning); this analysis is focused on the causes of predicted incidents;
- selecting security measures which reduce the risk volume (risk management); for each risk scenario it is possible to define up to five security variants which differ in terms of their ability to reduce risk and their implementation costs (depreciation and maintenance); the most beneficial variant is considered for implementation.

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.). For each event a preliminary assessment of its consequences is done. Events identified as having significantly negative impact are qualified as incidents and, depending on their kind and weight, adequate actions are undertaken – even up to initializing a business continuity plan. After the incident is finished, it is closed. Then its causes and consequences are assessed and a short summary report is prepared. A simplified (anonymized) version of this report is sent to the OSCAD-STAT system. There are always lessons learnt from incidents. This helps to avoid them in the future.

Audit and review functions manage information about conducted compliance audits or reviews, generate reports and support the process of the reports acceptance. OSCAD has some audit lists allowing to achieve compliance with basic standards and laws. The lists facilitate the auditing process and half-automatic generation of reports. The audits and reviews are planned with the use of timetabling functions. The plan of the audit includes the opening and closing dates of the audit, names of auditors, detailed audit tasks (starting and finishing times of tasks, the checked section of the standard or technical/legal requirements, organizational department and people who undergo the audit). Based on the plans, the tasks for responsible persons are generated.

BCP (Business Continuity Plan) management functions help the user prepare, maintain and test business continuity plans. The plans are developed for business processes which are critical for the organization's operations. The plan indicates which assets are necessary to fulfill it, the environment of the fulfillment, list of contact persons involved in the process, and operations to be conducted. The plans have to be periodically tested by the organization's employees. The tests are planned with the help of timetabling functions.

Measures and indicators servicing functions allow to define and manage measures and performance indicators; a measure is a mechanism for measuring the value of the selected variable, carried out automatically or manually, comprising defined threshold values. If these values are exceeded, a task is generated for the person responsible for the measure; in general, measures are used to improve the efficiency of conducted tasks (process improvement).

3. ASSETS SECURITY AND BUSINESS CONTINUITY OF A MINE

The diagram of a system for the management of business continuity, information security and security of other assets in a mine is presented in Fig. 2. The diagram features the current organizational structure of a mining company.

To make things simpler, the organizational structure of the mining company has two levels:

- a supervising organization (group, holding) which manages several mines/mining companies,
- mines/mining companies which conduct mining processes.

Supervising organizations coordinate the operations of the mines and are typical business-oriented com-

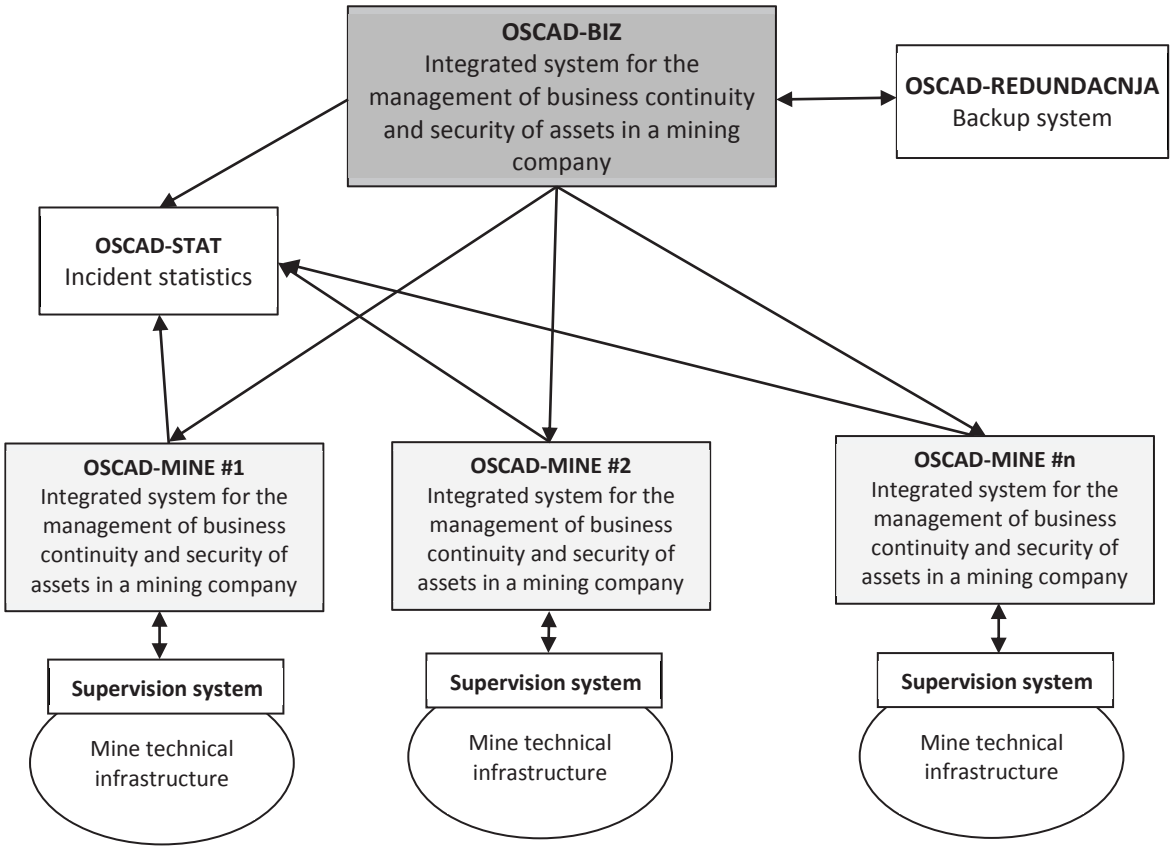

Fig. 2. Diagram of a system for the management of business continuity, information security and security of other assets in a mine
Source: EMAG Institute

panies. They are responsible for financial dealings, carry out common tasks and planning operations. Such organizations can make use of the basic OSCAD version (in Fig. 2 – OSCAD-BIZ) with two major protection objectives:

- to ensure the continuity of business processes of the supervising organization according to BS 25999 (ISO 22301),
- to protect information assets of this organization according to ISO/IEC 27001.

Optionally, it is possible to connect other management system to the integrated OSCAD system: quality, environment, or occupational safety management systems – provided that there are such systems in the given organization. Then OSCAD can be used to conduct a vocational risk analysis or an analysis of environmental aspects risk. OSCAD-BIZ can get from ERP basic information about the possibility of incidents (e.g. about materials and spare parts in stock).

The range of adaptation works for OSCAD-BIZ is typical, similar to implementations in other domains. Thus it includes the preparation of dictionaries, risk measures, indicators, procedures, and other documents.

Mining companies (mines) are technologically and organizationally separated units which have at their disposal certain means directly used for coal extraction. These means are, for example: mining excavations, building facilities or processing machines. The mining companies can make use of dedicated OSCAD versions (in Fig. 2 – OSCAD-MINE #i). These versions get information from supervision systems and other management systems (e.g. ERP, occupational safety systems).

Then it is possible to identify three major security objectives:

- to provide business continuity of the organization's processes according to BS 25999 (ISO 22301), particularly the continuity of the mining process,
- to protect the integrity and availability of human and material resources involved in the mining process; here the following disturbing factors are identified: factors that cause damages to machines and devices, loss of health or lives of miners, breakdowns, downtimes, shortages in supplies, etc,
- to protect the integrity, availability and confidentiality of information related to the fulfillment of the organization's business processes, as understood by ISO/IEC 27001.

The adaptation range of OSCAD-MINE to work in the conditions of a mine is much wider than that of OSCAD-BIZ and comprises the following operations:

- preparing the vocabulary of the system, comprising extra assets and roles related to the processes conducted in the mine, specific threats, vulnerabilities and security measures,
- predefining the organizational structure and roles – as patterns to be specified during the implementation,
- predefining the patterns of typical processes occurring in the mine – to be specified during the implementation,
- identifying assets and processes of the mine,
- configuration of risk analysis tools (business loss matrix and other measures),
- preparing a taxonomy of threats and incidents that reflect the real conditions of the mine; adapting OSCAD-STAT to work on the basis of this taxonomy,
- integrating OSCAD with the SD 2000 system (or with a similar one) which monitors production and security parameters; elaborating an integrated system for incident monitoring (OSCAD/SD 2000) and connecting it to OSCAD-STAT.

OSCAD-MINE should be connected to supervision systems functioning in mines. EMAG prepared such a connection – with the SD 2000 system. The details about co-operation between OSCAD and SD 2000 were presented in [15]. More information about OSCAD solutions is available in [16], [17].

It is recommended to equip OSCAD-BIZ with a backup system. An extremely important issue is to collect statistical data about incidents as it allows to improve the systems which function within the organization. Even apparently trivial, unnoticed incidents may bring significant losses if their number is huge. OSCAD-STAT may become a very useful tool in solving such issues. It is suggested to install one statistical data server in one organization.

4. SELECTED ASPECTS OF USING OSCAD IN A MINE

The OSCAD structure recommended for a mining company has two layers corresponding to the structure of the organization and its cooperation links. The higher level concerns the supervising organization which is a typical profit-oriented company. The standards BS 25999 (ISO 22301) and ISO/IEC 27001 have been developed for such a company with the participation of representatives of big international businesses, mainly British.

Figure 3 features one of OSCAD's windows where sample business processes of the mine are listed. Modelling of these processes allows to determine relations between them and to decompose a process into subprocesses. Inputs and outputs of the processes are considered; critical, supplying and consuming processes are identified, along with process parameters related to business continuity (e.g. maximal tolerable time of the process shutdown). The process model of the organization is the basis for the BIA analysis (process-oriented). During this analysis the impact of losing the continuity and integrity attributes on the organization's functioning is examined. During asset-oriented BIA it is possible to take into account all information assets related to the fulfillment of the given process and analyze the impact of losing the integrity, availability and confidentiality attributes of this information on the organization's functioning.

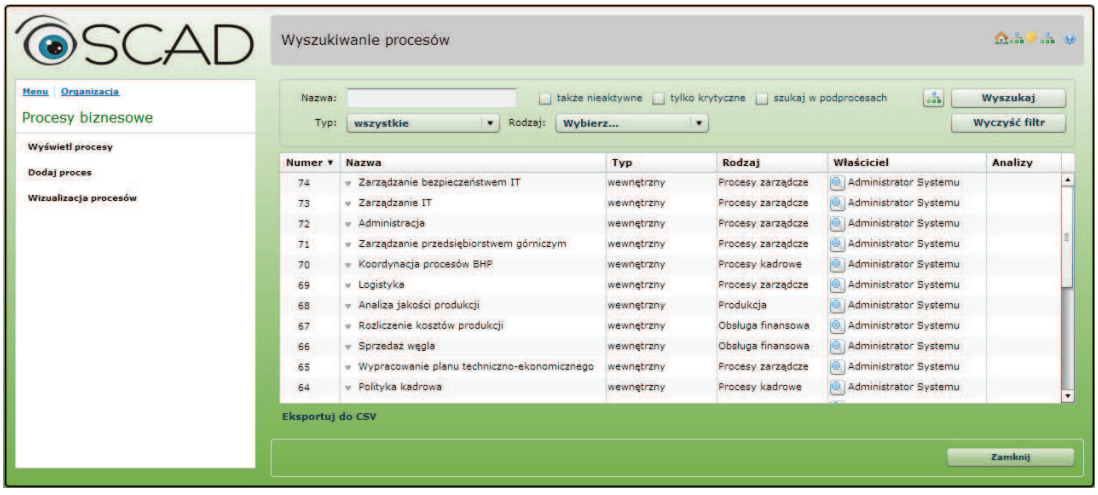

Fig. 3. Business processes of a mine in OSCAD-BIZ
Source: EMAG Institute

Implementing a full-functionality OSCAD in an organization is said to be a routine operation. Many consulting companies offer such services, yet they do not have as complex tools as OSCAD.

Further in the article the focus will be on untypical and innovative solutions related to OSCAD's adaptation to the needs of a mine. This will be illustrated by sample solutions to selected problems.

4.1. Risk management

A mining company is a place where the coal mining process is conducted along with other supporting processes. It is vital to provide the continuity of the process. This is directly related to business efficiency. In this environment there are many factors which disturb the mining process.

OSCAD supports the identification of disturbing factors and keeps them under control. For this purpose one can use the functions embedded in the system and related to risk analysis and risk management. It is possible to conduct three risk analysis variants:

- BIA (Business Impact Analysis); the result of this analysis is information what kind of business impact is related to the loss of the business continuity attribute in the mine – the loss is considered for certain periods of time; the so called critical processes are identified; in the case of the mine a critical process is the mining process;
- detailed BCM analysis (process-oriented) is conducted to examine the causes of phenomena which are unfavourable for the process; for each critical process the following are considered: threats and exploited vulnerabilities which have negative impact on the process; assets are treated here as a whole; this degree of detail is enough to assess the factors which disturb business continuity;
- detailed ISM analysis (based on the mechanisms of the ISMS system analysis, asset-oriented); in this case assets are divided into categories (this is defined by one of the system dictionaries), while the analysis of threats and vulnerabilities is carried out for each asset separately (the software uses the term "group of protected assets"); this way for each risk scenario ("how the threat that exploits a vulnerability negatively impacts the asset") the risk volume is determined, including the volume of loss and probability of its occurrence.

Figure 4 features a window of OSCAD (tab: "Information about analysis"). The window allows to determine the context of the initiated BCM risk analysis for the coal mining process. Each analysis has its descriptive parameters as well as all assets involved in the fulfillment of the process. BCM does not consider threats separately for each asset but focuses on those threats that breach the continuity of the process as a whole. Thus the continuity of the process becomes an asset here. More details can be obtained from the ISM analysis which looks at the groups of process-related protected assets from the point of view of threats and vulnerabilities.

The risk analyzer has a number of tabs. The "Documents" tab is for the management of documents attached to the system, while the "Authorization" tab – for the management for extra authorizations related to the given analysis. Figure 5 presents the "Risk calculation" tab with sample results of the analysis. For each pair threatvulnerability the weight of the

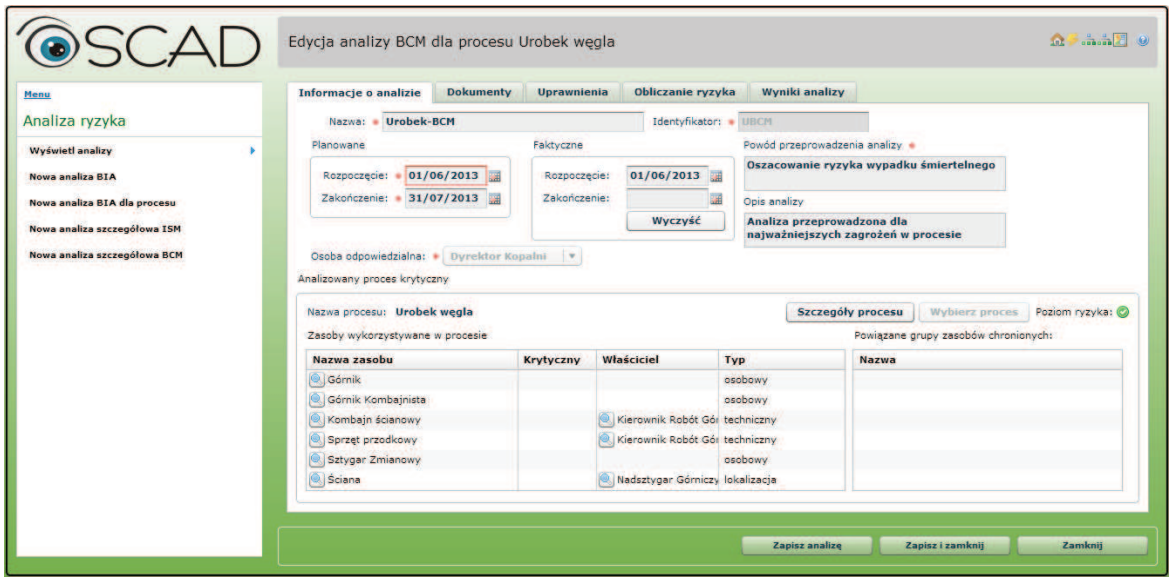

Fig. 4. Beginning of BCM analysis for the coal mining process (OSCAD-MINE)
Source: EMAG Institute

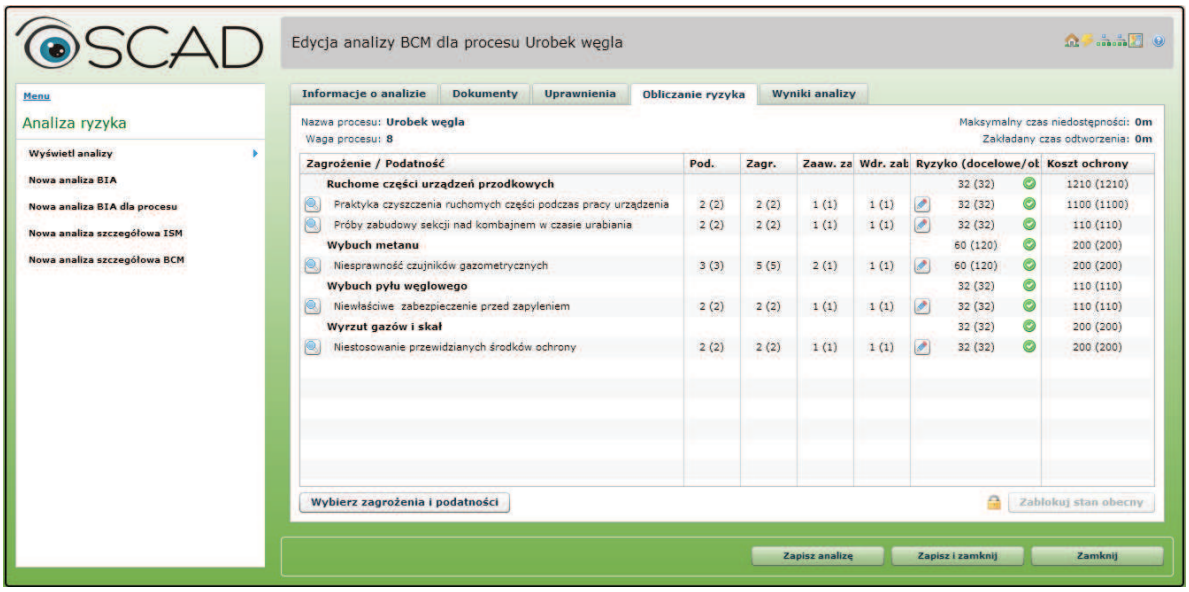

Fig. 5. Results of BCM risk analysis for the coal mining process (OSCAD-MINE)
Source: EMAG Institute

vulnerability was estimated (probability of occurrence), weight of threats (volume of resulting losses), degree of technical advancement of existing security measures (automatic - 3, under implementation - 2, organizational and procedural - 1), degree of progress in the implementation of security measures (implemented - 3, half-automatic - 2, planned - 1). Based on proper mathematic formulas [17] the volume of risk is determined in points of the used measuring scale. Numbers in brackets signify inherent risk (calculated for the first time) or risk estimated during the previous analysis. The existing security measures are taken into account: self-contained or implemented on the basis of the previous analysis. The costs of these security measures are registered, comprising two components: purchase/depreciation costs and maintenance costs. Additionally, during the BCM analysis the relation between two basic business continuity parameters is considered:

assumed recovery time <= max. time of unavailability.

The analysis results in a ranking list of risk cases organized according to the risk volume. For the cases which exceed the acceptability limit determined for the company, it is necessary to apply some risk reducing security measures.

Figure 6 features the selection of security measures for a concrete risk case, i.e. the pair threat ("Rocks and gas outburst") – vulnerability ("Planned security

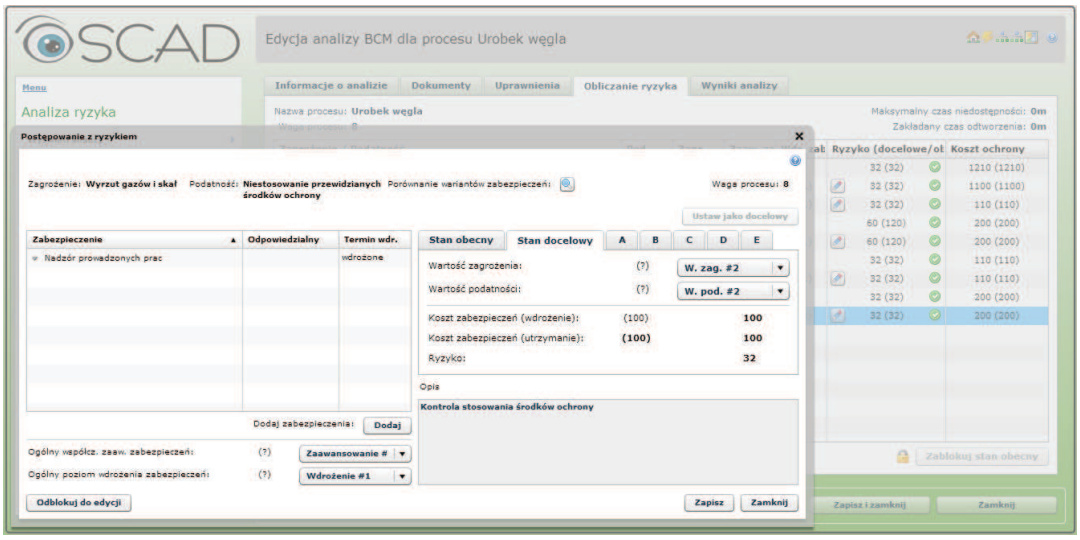

Fig. 6. Risk management – security measures selection (OSCAD-MINE)
Source: EMAG Institute

measures are not applied"). For such a pair a suitable security measure is selected (here: "Supervision of conducted works"), having in mind that each security measure has its ability to reduce the risk and its cost. For the given risk case it is possible to analyze 5 security measure variants (A-E) and select the most appropriate one, i.e. the one which will reduce the risk below its acceptability threshold and whose costs will not be higher than those assumed. The security measures are placed in security plans which indicate the time, place and cost of their implementation as well as responsible persons.

It is important to note that the results of the risk analysis are prognoses of unfavourable events. There is always an issue how real these prognoses are. Therefore they have to be confronted with the real number of occurring incidents and the losses resulting from them in comparable periods of time. This is one of the reasons why the incidents should be monitored and analyzed to obtain such data.

4.2. Incident management and central monitoring of incidents

The OSCAD system has an extended functionality for incident management, including automatic acquisition of data about incidents. This issue was described in detail in [15].

Incident management in the OSCAD system begins from reporting and classifying the event which is entered into the system:

- manually by an authorized person, with the use of a simple e-form or
- automatically through an interface with external monitoring or management systems, such as, for example, SD 2000.

Another authorized person assesses the events and classifies them according to their weight. More serious events are classified as incidents, less harmful remain events. The incidents undergo further processing while events are simply recorded in the data base.

SD 2000 is an example of a system which, from the outside and automatically, supplies events to OSCAD as its superior system.

Not every event registered in SD 2000 can be classified as an event in terms of incident management processes. Therefore SD 2000 is equipped with a special filter (Fig. 7) which allows to set boundary conditions.

Figure 8 features a window with reported events already classified as incidents, as the incurred losses were assessed as serious.

Each incident, no matter how it was reported, undergoes the incident management process which is implemented in the OSCAD system. The process encompasses the following operations:

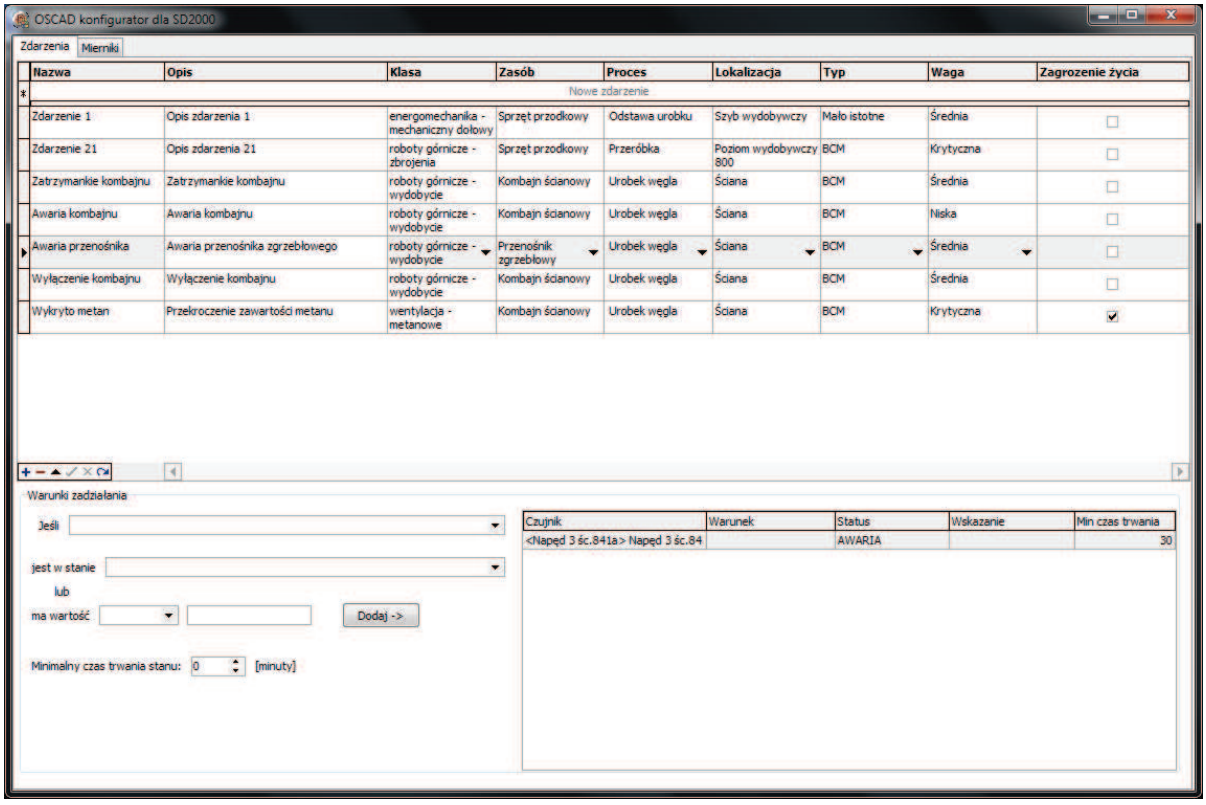

Fig. 7. Filtering events in SD 2000 before they are reported to OSCAD

Source: EMAG Institute

Fig. 8. Review of reported events (OSCAD-MINE)
Source: EMAG Institute

1. Analysis of the incident; in the course of this process the following are determined:
   - type of the incident,
   - threat that caused the incident,
   - identified vulnerabilities exploited by the threat,
   - real loss incurred as a result of the incident;
2. Appointing people responsible for handling the incident (appointing sub-tasks to these people);
3. Conducting a communication action by means of communication channels available in OSCAD;
4. Starting a previously prepared Business Continuity Plan (for serious incidents only; tasks predicted for crisis situations are launched);
5. Re-directing the tasks to a different responsible person (if needed);
6. Closing the incident (the incident gets the "handled" status and one can add a corrective action to it resulting from conclusions drawn from the incident; this is commonly called "lessons learnt");
7. Sending information about the incident to the OSCAD-STAT statistical information system.

It is important to note that OSCAD is a homogenous, central incident management system for the mine, supported by the OSCAD-STAT statistical data server. The collected information about incidents are an added value provided by OSCAD to the client. This information can be used to revise management processes in the organization – in corrective actions and as input information for risk analysis. Figure 9 features an example of statistics offered by OSCAD-STAT (fictitious data). The figure shows a diagram of accidents for the selected industrial branch (here: the mining industry). OSCAD-STAT allows to make statistics for the needs of the organization.

It is possible to register incidents which are not apparently significant and tend to be skipped in the everyday routine. However, their number is huge and they cause significant losses for the organization. It is necessary to draw conclusions from such events too.

The incident management system can be used to register accidents by the occupational safety department. Reports generated about that give a diagnosis how to improve the situation in this respect. It is possible to include in the OSCAD system other elements of the occupational safety management system.

4.3. Measures and indicators

The OSCAD system, as a system supporting management processes, has an embedded mechanism of measures and indicators. They are used to collect information which are then used to improve business processes and their management. The measures allow periodic sampling of physical variables (e.g. pressure, methane concentration) or process variables (e.g. current production output, number of breakdowns of machine X, total downtime caused by Y, etc). The measurement is performed automatically or manually. The measures have threshold values defined. Once these values are exceeded, there are tasks generated for a person responsible for maintaining a proper value of the variable.

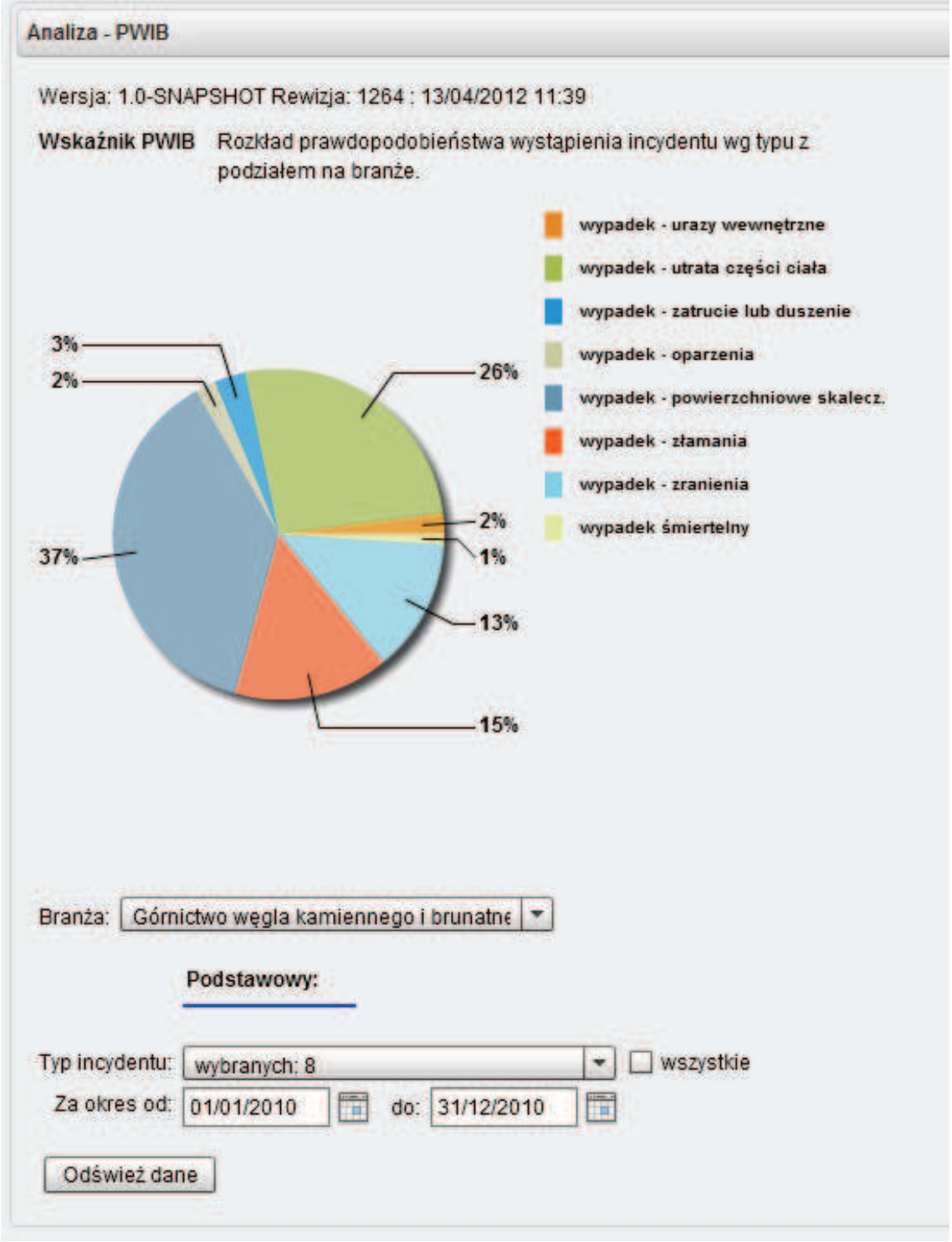

Fig. 9. Example of incident statistics prepared in the OSCAD-STAT application
Source: EMAG Institute

Apart from manually defined measures, in the OSCAD-MINE version there are measures which take automatically selected data from the SD 2000 system. The measures of the OSCAD-MINE system are all single sensors which were defined in SD 2000. The information they provide is updated in the database of OSCAD-MINE. These are, for example, an analogue methane level sensor, a bi-stable sensor monitoring the operations of a cutter loader, or a counter of skips of the extracted coal.

To carry out the integration of the two systems, there were some mechanisms developed for SD 2000. They allow to define the situation in the mine, reflected by sensor readouts or by previously described events and incidents.

Figure 10 features a window with a list of active measures in the OSCAD system. They measure security parameters (atmosphere in the production environment – anemometer, barometer and methane meters) and production parameters (skips counter). If certain thresholds or ranges are exceeded, a task is generated for a person responsible for a proper reaction.

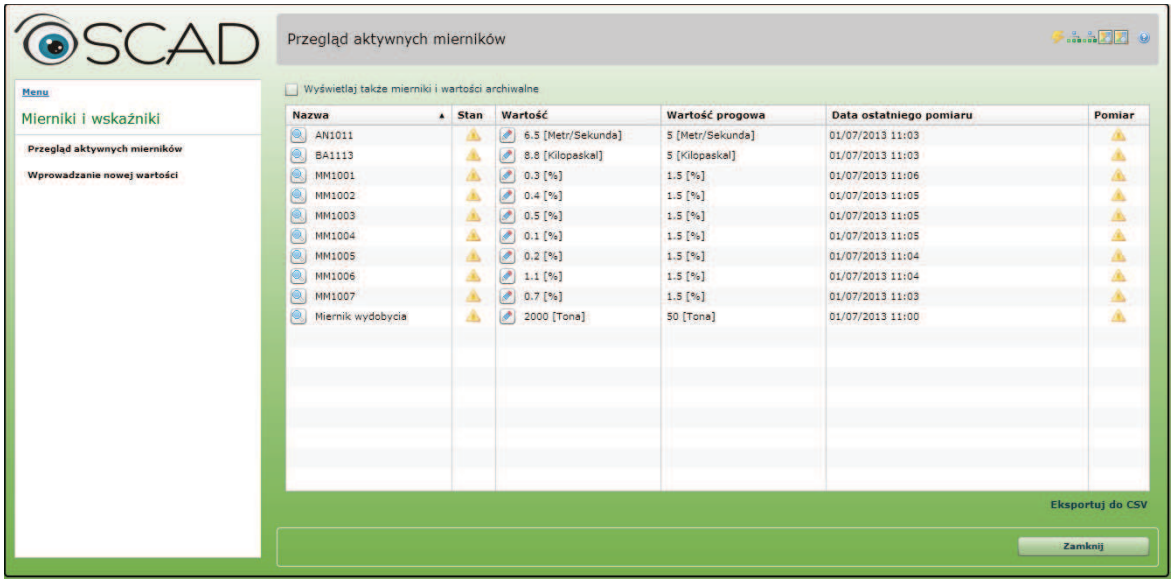

Fig. 10. Review of active measures (OSCAD-MINE)
Source: EMAG Institute

Figure 11 presents the details of a sample measure (coal extraction) for which measuring data are provided by SD 2000. It is important to note three ranges: alarm, warning and proper state. It was assumed in this example that the extraction volume is in the range 0-5,000 t. The current value is 3,500 t and is within the normal range. The drop below 2,000 t generates a warning signal, while below 1,000 t – an alarm signal. The measures can also be defined as "values from the range from x to y".

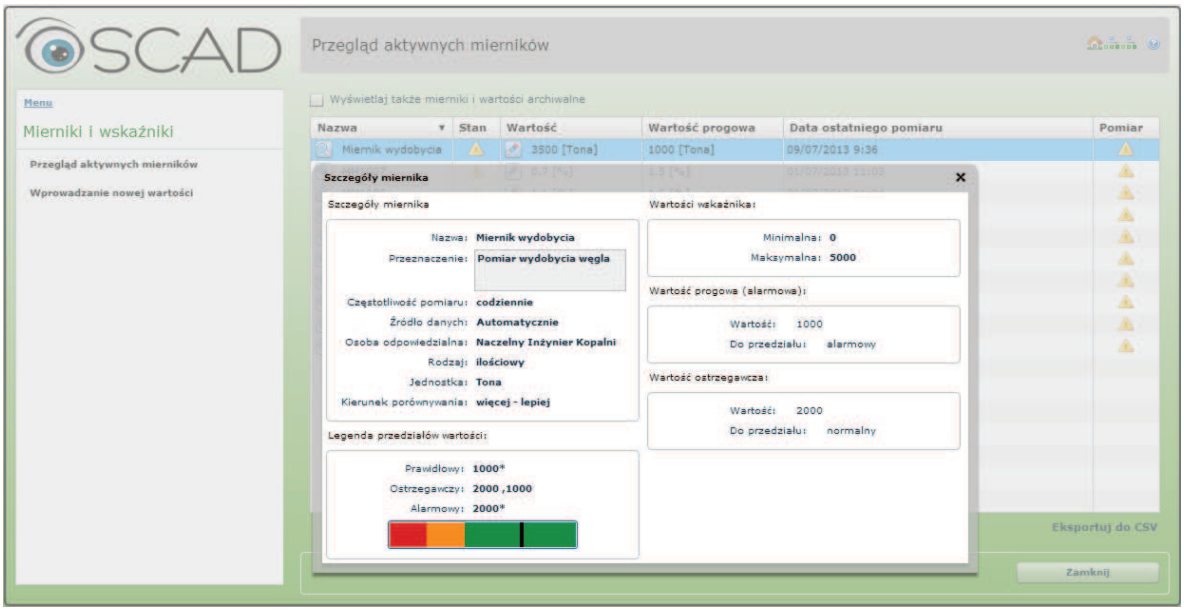

Fig. 11. Sample measure-indicator (OSCAD-MINE)
Source: EMAG Institute

Such a set of measures allows to register the most important variables which describe the efficiency of business processes and processes which are part of their management systems.

5. CONCLUSIONS

OSCAD is a system that supports the operations of managers in a mining company, on different levels of management. It comprises a procedural and organizational layer as well as software supporting management processes. OSCAD was developed according to world-known standards, such as BS 25999 (ISO 22301) for business continuity and ISO/IEC 27001 for information security management. It is an open system to be used in organizations of different sizes and profiles, yet each time it has to be adapted to the needs of the given organization.

The article presents, in general, the functionality of the OSCAD system, and then, with more details, its possibilities in terms of supporting business continuity and information security in a mining company and its departments. Mining companies which are business-oriented are typical organizations where the BS 2599 (ISO 22301) / ISO/IEC 27001 standards are used, along with the OSCAD system which was developed based on these standards.

The article is focused on three basic applications of OSCAD in the mine:

- risk analysis allowing to identify factors which can disturb the coal mining process and breach material and human resources engaged in this process, to select suitable security measures, to control the cost of these measures against their risk reduction abilities; risk prognoses allow to define corrective actions and proper reactions to incidents; management process based on risk analysis improves the organization's efficiency and its competitive position on the market;
- incident management system which provides synthetic information about real events and incidents, their causes and consequences – this allows to draw conclusions how to improve the personnel safety and efficiency of the mine;
- measures/indicators of efficiency and security which provide current, synthetic information about the state of processes and the organization's security, including the ability to react to potentially critical situations.

All these operations are performed to improve the efficiency of mining companies and the security of their personnel. The collected information is transferred to managers on different levels and helps them make decisions based on current data about the organization's state.

Apart from the above listed three basic application domains, the article features other functions of the OSCAD system, for example: information security management in the organization, audits management, planning of reviews and training, planning of security measures, emergency plans management, testing procedures management, task flow management, management of standards and documents, including those stipulated by valid laws.

OSCAD can be integrated with quality, environment and occupational safety management systems.

References

1. OSCAD, http://www.oscad.eu
2. BS 25999-1:2006 Business Continuity Management – Code of Practice.
3. BS 25999-2:2007 Business Continuity Management – Specification for Business Continuity Management.
4. ISO 22301:2012 Societal security – Business continuity management systems – Requirements.
5. PN-ISO/IEC 27001 – Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji – Wymagania (ISO/IEC 27001:2005 Information technology – Security techniques – Information security management systems – Requirements).
6. ISO/IEC 27002 Information security – Security techniques – Information security management systems – Code of practice.
7. ISO 31000:2009 – Principles and Guidelines on Implementation.
8. ISO/IEC 27005:2008 Information technology – Security techniques – Information security risk management.
9. Białas A.: Bezpieczeństwo informacji i usług w nowoczesnej instytucji i firmie, Wydawnictwa Naukowo-Techniczne, Warszawa 2006, 2007.
10. Białas A.: Some aspects of information security and business continuity in public administration. In: Pikiewicz P., Rostański M.: Internet in the information Society – Computer Systems Architecture and Security, Academy of Business in Dabrowa Gornicza, 2013, pp. 125-140.
11. FP7 ValueSec: http://valuesec.eu
12. http://pl.wikipedia.org/wiki/Cykl_Deminga
13. BS PAS 99:2006, Specification of common management system requirements as a framework for integration.
14. 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.
15. Białas A., Cała D., Napierała J.: Wspomaganie zarządzania ciągłością działania zakładu górniczego za pomocą systemu OSCAD, Conference EMTECH'2012 – Power supply, information technology and automation in the mining industry – Innovation and security. Szczyrk, 16-18 May 2012.
16. Bialas, A. Computer support in business continuity and information security management. In: Kapczyński A., Tkacz E., Rostański M. (Eds.): Internet – Technical Developments and Applications 2; Advances in Intelligent and Soft Computing, Vol. 118, 2011, Springer-Verlag: Berlin Heidelberg, ISBN 978-3-642-25354-6, pp. 129-144.
17. Bagiński J., Rostański M.: Modeling of Business Impact Analysis for the Loss of Business Processes and Data Integrity, Confidentiality and Availability, In: Theoretical and Applied Informatics, Instytut Informatyki Teoretycznej i Stosowanej PAN, Vol.23 (2011), no. 1, pp. 73-82.
18. Reports from the OSCAD project, Instytut Technik Innowacyjnych EMAG, 2013.