DOI: 10.15439/2014F371
ACSIS, Vol. 2

A Framework for Dynamic Analytical Risk Management at the Emergency Scene
From Tribal to Top Down in the Risk Management Maturity Model

Adam Krasuski*
*Section of Computer Science,
The Main School of Fire Service
ul. Słowackiego 52/54, 01-629 Warsaw, Poland
krasuski@inf.sgsp.edu.pl

***Abstract*—We present a framework designed for the risk management at the emergency scene. The system that implements the framework is focused on supporting an Incident Commander during the fire and rescue actions. The system is able to assess and manage the risks with the use of sensory data, ontology modelling and reasoning techniques from AI domain. Within the framework we propose the novel approaches for perceiving and modelling the emergency scene, for reasoning, for assessing the state and the relations among the objects at the scene, for assessing the risk mitigation and for communicating the risks to the Incident Commander.**

***Keywords*-Fire Service, Decision Support, Risk Management, Sensory Data, Domain Ontology**

I. Introduction

EMERGENCY scene is considered one of the most challenging decision making environments [1]. The safety and the success of the fire & rescue (F&R) action depends strongly on the evaluation of the risks at the emergency scene. The *Incident Risk Management* is the principal consideration of an Incident Commander (IC) in order to ensure the safety of the rescuers. Therefore, prior to deciding upon the tactics, risks must be assessed. The IC must identify the threats and the vulnerabilities (subjects to threats) as well as assess the risks and implement all reasonable control measures. The risks must be recognized and controlled before committing rescuers into the danger zone.

In the State Fire Service of Poland there are no regulations that impose an obligation of risk assessment. There are no procedures or habits that introduce the methods of risk assessment or management. The management of F&R actions is regulated according to the general procedures. The procedures in the scope of the evaluation of the emergency scene distinguish reconnaissances: initial, complete and continuous. However, even the experienced ICs are not able to distinguish how these reconnaissances differ from each other, and what exactly should be done within the instance of each of these reconnaissances.

Having the incident – in the scope of the risks – poorly evaluated there is also a problem with proper controlling (by leading) the processes emerging during the F&R action. Therefore, the safety of rescuers and success of the F&R action depends strongly on the experience, knowledge and skills of individuals. The risk management maturity model [2] defines such a process management as *tribal and hectic*. The management of the emergency scene is ad-hoc and chaotic. The success depends primarily on individuals heroics, capabilities and verbal wisdom. The emerging processes are unpredictable, poorly controlled and reactive.

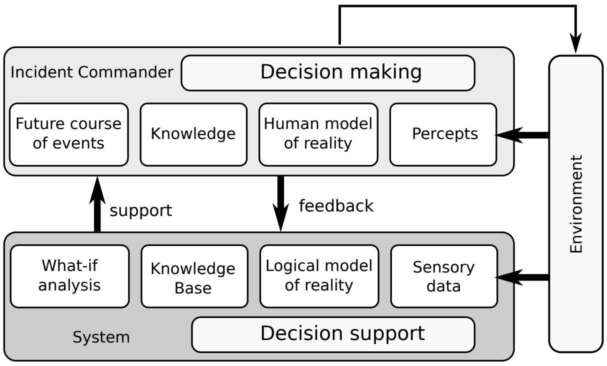


Fig. 1. Cooperation between the IC and the system.

So far there are no standalone computer systems that are able to support the IC at the emergency scene in the risk management activities. This is mainly caused by a) specificity of the decision making environment, b) problems of communicating the risk assessment to the IC. The issue of a) is caused by significant uncertainty and dynamically changing conditions of the objects and phenomena at the emergency scene. There is a problem with obtaining the information which satisfies the IC's *information triangle* rule [3]. It means that the information reported to the IC should be *relevant, accurate* and *timely*. The b) issue originates from the problem that the IC operates under time and mental pressure and has no time for longer analyses and more complex reports. The IC is very sensitive to information overload, simply not important from the intervention objectives point of view [4]. Moreover,

978-83-60810-58-3/$25.00 © 2014, IEEE

during the F&R action the IC reasons using the very abstract and vague concepts, such us safety, danger, threats, potential losses and others. Therefore, the system that supports and cooperates with the IC during the F&R actions should use the same concept's namespace as the IC. The system should gather information through the sensory layer and translate the concepts to be "compatible" with the model residing in the IC's mind. The accuracy of such an approximation is crucial in order to follow the IC's strategy and to provide help whenever any new risks arise. Figure 1 illustrates the correspondence of the IC and the software with respect to different aspects [5].

Creating the system which satisfies these constrains is a real challenge. There were a few attempts [6], [7] to build such systems. However, they depended strongly on a dense sensors networks which are not currently operating in the real world. Also, there was an issue with translating all these sensory data into whatever the IC could comprehend.

There are practical implementations that introduce the risk assessment in other countries' Fire Services. However, they are either complex and demand comprehending of large amount of information [3] by the IC or the are based on the IC experience [8]. Therefore, the safety of rescuers and the success of F&R actions depend again on the individuals. Implementing such approaches in the State Fire Service of Poland can only result in the advancement to the *specialist silos* [2] level in the risk maturity model (see Figure 2).

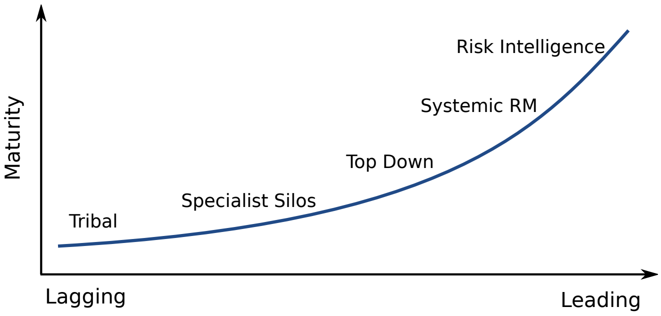


Fig. 2. Risk management maturity model chart.

In this article we present an approach which is able to transform the current *tribal* risk management model into *top down* (see Table I). The top down model is characterized by a) common framework, program statement and policy, b) routine risk assessment c) proper communication of strategic risks to the IC, d) knowledge sharing across risk functions e) awareness activities.

The rest of the article is structured as follows: in section II we present the context for risk management at the emergency scene, giving examples of applied risk assessment methodologies. Section III contains our proposition for the risk assessment. Section IV describes our methods for risk management at the emergency scene. The article is concluded with the evaluation of the approach and a discussion on the perspectives for the future work.

II. The Context

There are two leading approaches implemented for the risk assessment at the emergency scene. One of them is used by German Fire Service and is called *Threat Matrix* (in German – Gefahrenmatrix) [10], [8]. After arriving at the emergency scene German commanders have to recognise and evaluate the appearing risks. In order to do this systematically and not to miss any of the threats they have to fill the Threat Matrix. The Threat Matrix helps to identify both the threats emerging at the scene and the threatened objects (vulnerabilities). Having this information, the commanders can recognize the primary danger to deal with. The approach structures the problem of risk assessment, defining and limiting the set of threats and vulnerabilities to be recognized. However, the method strongly depends on individual experience and intuition. The definition of the consecutive threats are vague and there is no method of risks evaluation – the risks either exist or not. There is no evaluation of the likelihood of risk materialization and the consequences.

The more advanced approach — much more complicated as well — is one used by British Fire Brigade. The approach is composed from three risk assessment methods *Generic Risk Assessment (GRA) Dynamic Risk Assessment (DRA)* and *Analytical Risk Assessment (ARA)* [3].

GRA is a general framework for risk assessment in the Fire Service, regardless of the scope and nature of an incident. The approach takes under account the risks at every stage of duties – from the activities in the fire station via travel to the emergency scene up to the incident commanding. The approach links the risk with the conditions at the emergency scene and the tasks performed by the rescuers. "Generic" means that the values of the risks come from statistics based on the similar actions from the past. The results of the approach consist of a set of rules matching the given situation [11]. During the F&R action GRA allows the IC to operate under the standard procedures. GRA forms the foundations for DRA, operating procedures and training schemes. It also assists in the completion for ARA at incidents.

The second one, DRA, is used to describe the continuing assessment of the risks that is carried out in a rapidly changing environment at the emergency scene. DRA is defined in the initial phase and then reviewed continuously and updated. The outcome of DRA is a declaration of a tactical scheme for the IC, i.e. *offensive* or *defensive*. DRA is a continuous process and takes into account the continually and sometimes rapidly evolving nature of an incident. During DRA phase the IC refines the general rules defined by GRA [11] and fits them according to the state of the phenomenon, objects involved, equipment available and others. DRA must be reviewed continuously and updated as required. Having carried out the DRA and the tactical scheme established, the IC is aware of the immediate threats, vulnerabilities at risk and the control measures necessary to protect those vulnerabilities. This initial assessment of DRA further forms the basis of a more detailed risk assessment – ARA. ARA is introduced to analyse situation

TABLE I
THE RISK MANAGEMENT MATURITY MODEL [9]

Tribal and Hectic	Specialist Silos	Top Down	Systemic	Risk Intelligence
Ad-hoc/chaotic.	Independent risk management activities.	Common framework, program statement, policy.	Coordinated risk management activities.	Embedded in strategic planning, capital allocation, product development etc. across silos.
Depends primarily on individual heroics, capabilities, and verbal wisdom.	Limited focus on the linkage between risks.	Routine risk assessments.	Risk appetite is fully defined.	Early warning risk indicators.
	Limited alignment of risk to strategies.	Communication of too strategic risks to the Board.	Enterprise-wide risk monitoring, measuring and reporting.	Linkage to performance measurement/incentives.
	Disproportionate monitoring and reporting functions.	Executive /Steering committee.	Technology implementation.	Risk modelling/scenarios.
		Knowledge sharing across risk functions.	Consistency plans and escalation procedures.	Industry benchmarking.
		Awareness activities.	Risk Management training.	

in more detail on the basis of information obtained from the reconnaissance and from the rescuers. The special forms are defined and provided to the IC in order to help calculating and recording ARA [12]. The outcome of the review of ARA either confirms that the DRA and chosen tactical scheme was correct, or it results in a change of the scheme. This also provides the basis for the current and future DRA.

The discussed approaches enhance the risk assessment at the emergency scene and improve the safety of the rescuers. However, they have a major shortcoming: it is not easy to implement the risk assessment as a stand-alone, unsupervised computer process since they require a) a rich sensory infrastructure and b) a clever AI processing.

The issue with a) is continuously improving: the technology can deliver more precise, more modern and cheaper sensors each year which can produce lots of streams of data about various phenomena. The b) issue improves as well: there is a significant improvement in the fire and evacuation modelling [13], [14], the ontology modelling methodologies are being invented and evaluated, AI-based algorithms can support big data analytics and so on. We can therefore support the claim that the computer-driven Dynamic Analytical Risk Assessment, independent from IC is becoming more and more feasible.

III. DYNAMIC ANALYTICAL RISK ASSESSMENT

We propose an approach which allows for supporting the IC at the emergency scene in the managing of the risks. We called our approach Dynamic Analytical Risk Assessment due to the fact that the method reacts dynamically to the changing at the emergency scene and is detailed enough to be considered an analytical risk assessment. Our approach derives the foundations from the risk approaches presented in section II and uses the methods from AI to implement the ideas.

A. Scene Modelling

We start our process of creating the scene model from the review of the domain. We used a Use Case diagram for this purpose. The elaboration of the diagrams results also in a better mutual understanding between architect of the system, analytics and domain experts. The Use Case diagrams allow to extract the main objects, concepts and relation within the domain. Then, we used a set of documents called *incident analysis* in order to obtain the more detailed description of the domain. The documents study in detail the selected incidents and contain a comprehensive description of them, including the context, previous trainings at the objects involved, their recognition, the course of action minute after minute, decisions made and their background. It allows us for extracting (with support of domain experts) the complex objects, their hierarchy and spatio-temporal relation among them. The description was too complex to model it using Use Case diagrams. Therefore, we use the taxonomic hierarchies of classes defined by [15] in order to better represent the hierarchy and relationships between complex, plain objects at the emergency scene and their attributes.

In our approach we consider an emergency incident as a set of frames [16] from time t_s when the incident begins to the time t_e when the last crew come back to the fire station. A single frame F_n from the set represents the emergency scene at time t_n. The frame can be considered as a complex object which is composed by other complex objects such as buildings, equipments, rescuers, occupants and others. Figure 3 depicts the idea of the perception of the scene.

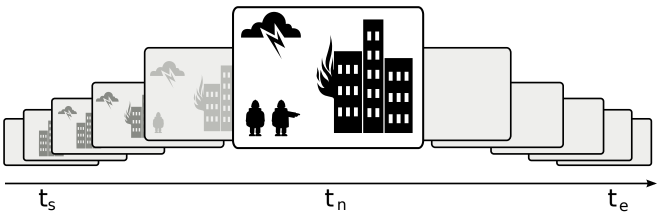


Fig. 3. The idea of frame-based scene modelling.

The complex objects within the frame may be composed from other complex objects or just by plain objects. Plain objects are represented only using vectors of attributes values. We can create for each of the complex objects at the scene the hierarchy of sub-objects, attributes or both.

The attributes describing the objects can be static i.e. *nominal pressure* of the firefighting nozzle or dynamic when they reflect the current state of the object i.e. *a firefighter is exhausted*. The static attributes can be quite easily defined when the object is created. The values of dynamic attributes change continuously and are much more difficult to define. They depend on the situation at the scene and need communication with the sensory layer. For example, the level of the fatigue of the firefighter can be defined at the basis of breathing ratio and exhausted carbon dioxide concentration.

Modelling such aspects is challenging as it require to apply sophisticated methods. In order to face this problem we extend our ontology by the spatio-temporal perceptual concepts modelling defined by [17], [18]. The approach needs a domain ontology which is a core for reasoning processes. The creation of the domain ontology needs tight cooperation with domain experts. A cooperation with domain experts towards definitions of ontology is poorly studied. There are also no measures evaluating the correctness and completeness of the created ontology. Therefore a high attention should be paid in order to perform this correctly. First we created a draft of the ontology on the basis of domain literature [8], [19], [3]. Then we extended this draft with support of domain experts and contextual visualization [20] of the situation. In this process we involved not only the experts but also the software architects and psychologists. Figure 4 depicts the simplified snapshot of the created ontology.

B. Risk Assessing

The created ontology is only a carrier in our reasoning processes. It allows for structuring the problem and applying the method of *divide and conquer*. The evaluation of the value of the selected risk needs applying the hierarchical classification. This means that at the basis of lower layer concepts from our ontology we *approximate* a higher level concepts. We consider this process as an approximation because the concepts, objects or attributes from lower levels are not in such relation with higher level, which allows for its crisp definition.

The approximation of the higher level concepts by the lower level is a problem which in our case can be reduced to the classification problem. The standard classification uses the information system [21] for training the classifiers. The classifiers have to extract the features and their impact on decision class. However, in the hierarchical classification, where the decisions classes of lower level classifiers become the attributes for higher classes, the approach is insufficient due to the computing complexity. For example, in our case we have a sub-system for recognition of activities performed by rescuers [22]. The sub-system consists of a set of accelerometers and magnetometers placed in different body parts of the rescuers. In the purpose of the recognition of the activity of single rescuer the standard classification approach is good enough. However, if the recognition of some activity needs observing the group of rescuers (i.e. a tactic used to access the room on fire) the standard approach fails. This is caused by the necessity of consideration of a Cartesian product of each of the attributes values from the sensors.

In our approach, domain experts assist not only in the creation of ontology and categorization of objects/situations but also in learning the phase of classifiers. This recalls the human learning process when the tutor filters the information indicating features which plays the key role in the classification problem. In our case it is important that the higher level concepts (objects) are created as relational structures in which the points are represented by the vectors of attributes values from the lower hierarchical level and relations between them represent constrains. Over such objects the new attributes are defined with domain experts support. On the basis of this idea, the methods for ontology approximation were developed [23], [24].

We use the classifiers in order to induce the rules [25], [26]. Rules learnt from data can be used to support approximate reasoning about the concepts. Approximations can be considered both with respect to degrees of satisfaction of particular patterns in the observed data and the degrees of correspondence of previously unseen situations to already established ontology areas. It allows us for building the dynamic and spatio-temporal model of the emergency scene.

The presence, the state and the relations among complex objects at the scene define the concepts used by IC during the reasoning process. As was mentioned in the Introduction the concepts originate from the risk assessment field. Those are such concepts as: threats, vulnerabilities, risk, safety, danger and others. In order to approximate these concepts the across-hierarchy reasoning about objects within the frame is used, as well as spatio-temporal across-frames relations reasoning. For example, in order to evaluate, whether in a given moment the risk of explosion for rescuers exists, we have to consider the chances of *backdraft*[1] occurrence and recognition whether rescuers are currently entering the compartment on fire. Figure 4 depicts a simplified snapshot of the ontology created for recognition of the risk of an explosion for rescuers.

We present the methodology of risk assessment performed by the system, on the following example. The sub-systems for recognition of the activity of the rescuers and their position [22], [27] generate the stream of data. The set of classifiers uses these data to approximate the lower level concepts from our ontology (see Figure 4). These concepts are related to the navigation in the building, fire location as well as usage of rescue equipment. The decision classes from those classifiers constitute the attributes for higher level classifiers which recognize for example the usage of forcible entry tools. The usage of forcible entry tools simultaneous with the kneeling position of other rescuer approximate the concept of starting position of rescuers to enter the compartment on fire. The starting position of rescuers preceded by "gaining access to the fire" indicates that rescuers are already entering

[1] http://en.wikipedia.org/wiki/Backdraft

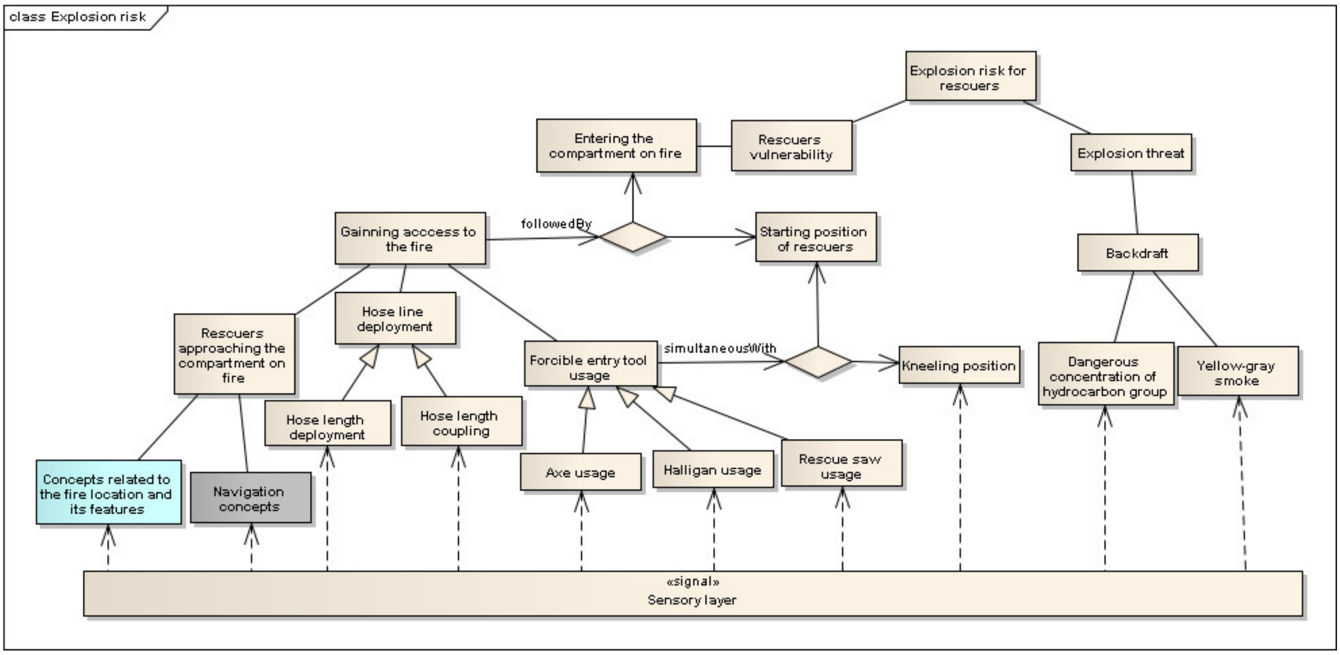
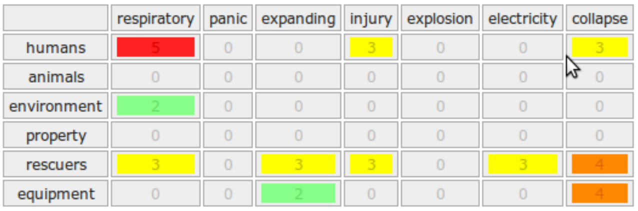

class Explosion risk
Explosion risk for rescuers
Entering the compartment on fire
Rescuers vulnerability
Explosion threat
Gainning acccess to the fire
followedBy
Starting position of rescuers
Backdraft
Hose line deployment
Rescuers approaching the compartment on fire
Forcible entry tool usage
simultaneousWith
Kneeling position
Dangerous concentration of hydrocarbon group
Yellow-gray smoke
Hose length deployment
Hose length coupling
Axe usage
Halligan usage
Rescue saw usage
Concepts related to the fire location and its features
Navigation concepts
«signal»
Sensory layer

Fig. 4. The ontology for hierarchical spatio-temporal reasoning.

the compartment on fire creating vulnerability on the explosion threat caused by the backdraft phenomenon. The sensors from fire detector aspiration system and smoke observation provide the data for the classifiers which recognize the likelihood of explosion threat. All the concepts defined are introduced to evaluate the root concepts of *explosion risk for rescuers* (see Figure 4). The presented methods of feature extraction and filtering from lower level to upper level is supported by domain experts.



	respiratory	panic	expanding	injury	explosion	electricity	collapse
humans	5	0	0	3	0	0	3
animals	0	0	0	0	0	0	0
environment	2	0	0	0	0	0	0
property	0	0	0	0	0	0	0
rescuers	3	0	3	3	0	3	4
equipment	0	0	2	0	0	0	4

Fig. 5. An example Threat Matrix

C. Risk Communicating

As we mentioned in the Introduction, the IC is a very demanding subject to efficient risk reporting. Therefore, we introduce a hierarchical level of risk communication. We use the general indicator about the actual risk level at the top level of the hierarchy. Due to the fact that we use augmented reality glasses (characterized by low resolution) to communicate with intervention level commander, the highest level risk indicators are just two squares with colors: green, yellow or red indicating risk for human and rescuers. If the IC needs a more detailed information about the actual risks, the second level of risk communication is Threat Matrix. The Threat Matrix presents the threats at the emergency scene and the vulnerabilities which can be subjects to the threats. The example Threat Matrix is presented in Figure 5.

In most cases the matrix contains enough information for the IC to evaluate the emergency scene [8]. However, the less experienced ICs may need a more detailed explanation concerning the origins of the risks presented in the Threat Matrix. Therefore, we created the next level of information provided to the IC. We present the rules which were launched and served to calculate the given risks. Table II depicts the presentation of the rules.

TABLE II
THE PRESENTATION OF THE RULES THAT WERE USED TO CALCULATE RISKS IN THE THREAT MATRIX

Id	Situation description	L	S	Control
A1.1	farm site fires: presence of dust	2	1	use Personal Protection Equipment (PPE)
A1.3	hazardous atmospheres	1	4	Use PPE, Resuscitation equipment immediately available / monitoring of atmosphere
A1.7	asbestos on the roof (the hazard comes from breathing)	1	2	Use PPE, decontamination after intervention

The rules presented in the table contain also the control measures aimed at decreasing the severity if the risks do materialise. This is additional guide for less experienced ICs to help them in risk mitigation.

IV. Risk Management

The presented approach allows for the complete risk assessment at the emergency scene and for its presentation to the IC. However the risk assessment is only part of the process of risk management. The other important parts of this process are methods of risk mitigation and measurements of the effectiveness of the controls applied.

A. Risk Mitigating

The presented approach for risk assessment allows for reasoning under uncertainty about vague concepts at the emergency scene. This allows the IC for better assessing of the situation and keeping the operation safe. However, the better situational awareness is only part of the success of the incident risk management. Equally important is planning and operating. The good incident action plan (IAP) plays a key role in the successful incident management [19]. According to the [28] the IAP should contain the strategy of risk mitigation. A good mitigation plan predicts future course of events and proposes the adequate controls to mitigate the risks. Therefore, the risk management could be perceived as a game between the nature and the IC. In order to win the game IC has to recognize the ”strategy of the nature”. The recognition of the strategy and creating own strategy is a challenging task. We are not able to address the problem yet. Therefore we are going to face the problem in our future work aimed at transition of the system into *Risk Intelligence* (see Figure 2). At the current state of the research we are only able to hint the general recommendation and propose the control measures matching the rules from risk assessment (see example in Table II).

The system determines, on the basis of the risk assessment expressed by the Threat Matrix, whether the potential benefits (saved live or property) outweighs the undertaken risks. If this is the case, the system proposes the general recommendation – the tactics scheme – (*offensive* or *defensive*). The proposition of the scheme is based on the rules, taking mostly into account the chances that people are present inside the building and the building construction type. If this scheme is accepted by the IC, the system is trying to endeavour to reduce the risks to an acceptable level.

The second level in our *hierarchy of control measures* are the general strategies of applying the control measures. At every moment in the F&R action the system is trying to recognize whether any of the following strategies should be applied. *Eliminate* the risk or substitute it with something less dangerous. For example changing the scheme to defensive thus preventing rescuers access the danger zone. *Reduce* the risk by preventing or reducing the number of vulnerabilities that come into contact with the risk or reducing the time of the exposure to the risk. The strategy is calculated according the evaluation of the parameters of the fire [29] and the amount of resources needed to extinguish the fire or to rescue people. Ensuring that *discipline* is maintained throughout the exposure to the risk. This is performed by monitoring and visualization of activities performed by the rescuers [22].

The third level in hierarchy of control measures constitute the rules used for risk assessment. As it was mentioned in section III-B there were rules induced from ontology which approximate the concepts related to the risks. We asked the domain experts to define the controls which should be used if the given risks materialize. The number of rules, even limited to active at the moment, is significant. Moreover, the controls proposed are very detailed and need some attention while reading. Therefore, leaving the navigation across the rules to the IC would result in information overload. We tried to partially address the problem by introducing a tool called what-if analysis. The approach allows for keyword search, faced search or fast navigation across the rules. The IC or her/his assistant at the control room can quite quickly find, using the keywords, the rules matching the actual situation. This allows for fast review and implementation of proper control measures. The IC has access to the appropriate risk related information to assist with the identification of suitable control measures. This, in conjunction with other specific facts regarding the premises, for example information gained on risk visits, will assist the IC to formulate an effective plan.

B. Performance Indicators

The approach presented so far is designated to deal with the risk defined as a likelihood of threatening the vulnerabilities and the potential consequences [28]. However, during the rescue action there is also a risk related to the definition provided by ISO 31000 defined as an effect of uncertainty on intervention objectives [30]. This type of the risk is related to the tactics applied by the IC. Each of the activities of the rescuers committed by IC are characterized by uncertainty about the obtained outcome. This type of the risk should be measured by the defined performance indicator of applied strategy.

The performance should be measured against agreed standards to reveal when and where improvement is needed. Active self-monitoring of the system reveals how effectively the management system is functioning, looking at the equipment, processes and individual behaviour/performance.

Every incident has an objective that reflects the mission’s objective – protect life, property and the environment from harm. An IC develops a strategy for accomplishing this mission, depending on the conditions that exist at the time. The rescuers execute the full mechanics of the tasks to complete each phase of the operation at the emergency scene. These tasks are based on fundamentals – ventilation; nozzle operation; water flow rates; secondary egress and emergency bailout by ladder.

Although each of the incidents is different there are common tactical phases of the incident management. There can be distinguished: arriving, reconnaissance, resource deployment, gaining access to the fire, search and rescue activities and extinguishing. Each of the phases has a set of activities and the outcome. The activities should be performed with accordance to the tactic and training processes, executing the rule "play as you train". Therefore, we can define in each tactical phase the checklist which should be completed if the IC obeys to the procedures. There also should be observable, measurable effects for each of the tasks that is performed, which can be observed by the system, and the effects of completion of each step as the outcome.

If the set of activities at each phase is performed according to the checklist and the outcome is consistent with the expectations (trained) then we can state that the risk of the intervention objectives is low. If the IC is not well-trained, insubordinated and does not obey the defined checklist, then the risk related to the uncertainty on the intervention objectives rises. The analogous situation is when the conditions of the incident are changing in an unexpected way – then the risk also rises.

For example, the rescuers are in the phase of entering the compartment on fire. The checklist consists of: rescuers in full gear kneeling before the door, breathing apparatus in use, hose line wet, forcible entry tools ready to use, second squad ready for assistance, etc. The outcome of the phase are the jets cooling the ceiling and opened windows. Every task and tactical procedure completed is also reported as a "benchmark".

C. Call for Action

Apart from the organization of the scene where the risks are assessed, the main idea of this process is the *call for action*. Having the risks assessed we have to communicate them in such a way that forces the stockholders to the action of the risk mitigation. In our system the call for action is implemented by risk exposure and control activity level matrix. Figure 6 depicts the idea of the matrix.

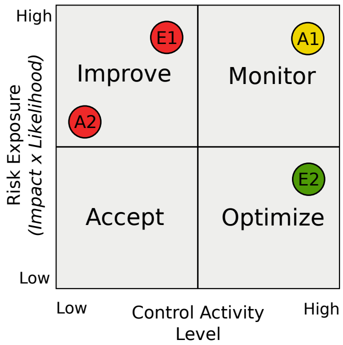


Fig. 6. Risk maps for presenting risk/control relationships.

There are four areas distinguished in the matrix. *Improve* is the area of high risk exposure with a low level of control. This area must be key priority for improvements in management and control activities. *Monitor* is the area of high risk exposure where controls are deemed adequate. This area should be monitored to provide the ongoing assurance of control effectiveness. *Accept* is the area of low risk exposure that also have a lower level of control. This area may be consciously accepted by the IC. *Optimize* is the area of low risk exposure with a high level of control. This area may generate opportunities for the IC to optimize the management and control activities.

Such a visualization of the risks and the controls illustrates clearly the areas where the current controls are not sufficient to operate in safe condition. This forces the IC to mitigate the risk in such areas or to lower the risks by it avoidance. The location of different risks within the given areas of risk maps is calculated according to the rules presented in Table II. The rules beside the calculation of the risks have also defined the control measures which help to mitigate the risks. If the selected rule is active and there is no adequate control applied then balance between the risk and the control is biased. The location of a given risk within the risk maps depends also on the risk level. Figure 6 illustrates that the risk caused by threats A2 and E1 should be handled by implementing the additional control measures; threat A1 creates a high risk, however it is properly controlled and some controls from E2 may be relaxed.

V. Conclusions

We present an approach allowing for the management of the risks at the emergency scene. The approach defines the framework for scene modelling, introduces the reasoning algorithms, risks mitigation methods, performance measuring and risk reporting and communicating. We implemented all the presented ideas into a standalone computer system. However, so far the system is not deployed in the State Fire Service of Poland. Our system is currently at the 4 level of Technology Readiness Level[2] It means that the main technological components of the system are integrated to establish that they will work together. This is relatively “low fidelity” compared with the eventual system. The system was tested in the laboratory with controlled parameter of the fire and many assumed simplifications. However, on the basis of the performed experiments we can support our claim that Dynamic Analytical Risk Assessment, independent from IC is becoming feasible.

We argue that it is possible to improve the quality of interventions and minimize the corresponding risks by providing IC with the support in the following areas: a) grouping and interpreting incoming information by means of higher level concepts and linking them with intervention objectives; b) filtering and ranking information; c) indicating which information is missing in order to make reliable decision; d) indicating where and how to acquire important information; e) monitoring situation and decisions made so far. We claim that such functionalities can be achieved through a combination of modern methods from the domain of Information System Security Risk Management, data organization with compliance to ontological approaches and interactive algorithms processing recommendations for IC. We pointed out that there is still a gap between analytical models and human abilities to benefit from them.

[2] http://en.wikipedia.org/wiki/Technology_readiness_level

Acknowledgment

Supported by Polish National Centre for Research and Development (NCBiR) – Grant No. O ROB/0010/03/001 in the frame of Defence and Security Programmes and Projects: “Modern engineering tools for decision support for commanders of the State Fire Service of Poland during Fire&Rescue operations in the buildings”.

References

[1] B. Brehmer, “Strategies in Real-Time, Dynamic Decision Making,” *Insights in decision making*, pp. 262–279, 1990.

[2] P. X. Zou, Y. Chen, and T.-Y. Chan, “Understanding and improving your risk management capability: Assessment model for construction organizations,” *Journal of Construction Engineering and Management*, vol. 136, no. 8, pp. 854–863, 2009. [Online]. Available: http://dx.doi.org/10.1061/(ASCE)CO.1943-7862.0000175

[3] Department of Communities and Local Goverment, *Fire Service Operations, Incident Command*, 3rd ed., ser. Fire Service Manual. London TSO, 2008.

[4] A. Cowlard, W. Jahn, C. Abecassis-Empis, G. Rein, and J. L. Torero, “Sensor Assisted Fire Fighting,” *Fire Technology*, vol. 46, no. 3, pp. 719–741, 2010. [Online]. Available: http://dx.doi.org/10.1007/s10694-008-0069-1

[5] A. Krasuski, A. Jankowski, A. Skowron, and D. Slezak, “From sensory data to decision making: A perspective on supporting a fire commander,” in *Web Intelligence (WI) and Intelligent Agent Technologies (IAT), 2013 IEEE/WIC/ACM International Joint Conferences on*, vol. 3. IEEE, 2013, pp. 229–236. [Online]. Available: http://dx.doi.org/10.1109/WI-IAT.2013.188

[6] H. Liangxiu *et al.*, “FireGrid: An e-infrastructure for next-generation emergency response support ,” *Journal of Parallel and Distributed Computing*, vol. 70, no. 11, pp. 1128 – 1141, 2010. [Online]. Available: http://dx.doi.org/10.1016/j.jpdc.2010.06.005

[7] N. Ashish, J. Lickfett, S. Mehrotra, and N. Venkatasubramanian, “The software ebox: Integrated information for situational awareness,” in *Intelligence and Security Informatics, 2009. ISI’09. IEEE International Conference on*. IEEE, 2009, pp. 77–82. [Online]. Available: http://dx.doi.org/10.1109/ISI.2009.5137275

[8] A. Graeger, U. Cimolino, H. de Vries, and J. Sümersen, *Einsatz- und Abschnittsleitung: Das Einsatz-Führungs-System (EFS)*. Ecomed Sicherheit, 2009.

[9] B. Endicott-Popovsky, “End-to-End Risk Assessment Approach,” in *Building an Information Risk Management Toolkit*. Coursera.org, 2014, p. 23.

[10] Bundesamt für Bevölkerungsschutz und Katastrophenhilfe, “Feuerwehr-Dienstvorschrift 100 Führung und Leitung im Einsatz : Führungssystem,” FwDV 100 Stand: 10. März 1999.

[11] Department of Communities and Local Goverment, *Generic Risk Assessments, GRA 3.1 Fighting fires in buildings*, ser. Fire and Rescue Authorities Operational Guidance. London TSO, 2011.

[12] Department of Cummunities and Local Government, “Fire and Rescue Service Operational guidance. Operational Risk Information,” 2012.

[13] W. Jahn, G. Rein, and J. Torero, “Forecasting fire growth using an inverse zone modelling approach,” *Fire Safety Journal*, vol. 46, no. 3, pp. 81–88, 2011. [Online]. Available: http://dx.doi.org/10.1016/j.firesaf.2010.10.001

[14] ——, “Forecasting fire dynamics using inverse computational fluid dynamics and tangent linearisation,” *Advances in Engineering Software*, vol. 47, no. 1, pp. 114–126, 2012. [Online]. Available: http://dx.doi.org/10.1016/j.advengsoft.2011.12.005

[15] T. R. Gruber, “A translation approach to portable ontology specifications,” *Knowledge acquisition*, vol. 5, no. 2, pp. 199–220, 1993. [Online]. Available: http://dx.doi.org/10.1006/knac.1993.1008

[16] I. Düntsch and E. Orlowska, “A discrete duality between apartness algebras and apartness frames,” *Journal of Applied Non-classical Logics*, vol. 18, no. 2-3, pp. 213–227, 2008. [Online]. Available: http://dx.doi.org/10.3166/JANCL.18.213-227

[17] A. Mallik, H. Ghosh, S. Chaudhury, and G. Harit, “Mowl: An ontology representation language for web-based multimedia applications,” *ACM Transactions on Multimedia Computing, Communications, and Applications (TOMCCAP)*, vol. 10, no. 1, p. 8, 2013. [Online]. Available: http://dx.doi.org/10.1145/2069276.2069280

[18] A. Mallik, S. Chaudhury, and H. Ghosh, “Nrityakosha: Preserving the intangible heritage of indian classical dance,” *Journal on Computing and Cultural Heritage (JOCCH)*, vol. 4, no. 3, p. 11, 2011. [Online]. Available: http://dx.doi.org/10.1145/2542205.2542210

[19] Emergency Management Institute, “Introduction to Incident Command System, ICS-100,” http://training.fema.gov/EMIWeb/IS/courseOverview.aspx?code=IS-100.b, 2013, access: 22.02.201.

[20] P. Teicholz, R. Sacks, and K. Liston, *BIM handbook: a guide to building information modeling for owners, managers, designers, engineers, and contractors*. Wiley, 2011.

[21] Z. Pawlak, “Information systems theoretical foundations,” *Information systems*, vol. 6, no. 3, pp. 205–218, 1981. [Online]. Available: http://dx.doi.org/10.1016/0306-4379(81)90023-5

[22] M. Meina, K. Rykaczewski, and B. Celmer, “Towards robust framework for on-line human activity reporting using accelerometer readings,” *Lecture Notes in Computer Science*, vol. 8610, pp. 350–361, 2014.

[23] J. Bazan, “Hierarchical classifiers for complex spatio-temporal concepts,” in *Transactions on Rough Sets IX: Journal Subline*, ser. Lecture Notes in Computer Science, J. F. Peters, A. Skowron, and H. Rybiński, Eds. Heidelberg: Springer, 2008, vol. 5390, pp. 474–750.

[24] J. G. Bazan and A. Skowron, “Classifiers based on approximate reasoning schemes,” in *Monitoring, Security, and Rescue Tasks in Multiagent Systems (MSRAS’2004)*, ser. Advances in Soft Computing, B. Dunin-Kęplicz, A. Jankowski, A. Skowron, and M. Szczuka, Eds. Heidelberg: Springer, 2005, pp. 191–202. [Online]. Available: http://dx.doi.org/10.1007/3-540-32370-8_13

[25] S. H. Nguyen, J. Bazan, A. Skowron, and H. S. Nguyen, “Layered learning for concept synthesis,” in *Transactions on Rough Sets I: Journal Subline*, ser. Lecture Notes in Computer Science, J. F. Peters and A. Skowron, Eds. Heidelberg: Springer, 2004, vol. 3100, pp. 187–208. [Online]. Available: http://dx.doi.org/10.1007/978-3-540-27794-1_9

[26] S. H. Nguyen, T. T. Nguyen, M. Szczuka, and H. S. Nguyen, “An Approach to Pattern Recognition based on Hierarchical Granular Computing,” *Fundamenta Informaticae*, vol. 127, no. 1-4, pp. 369–384, 2013.

[27] M. Meina, K. Rykaczewski, and B. Celmer, “Certain Aspects of Foot-Mounted Inertial-based Indoor Navigation Systems,” in *Type II Proceedings of WIC 2014 Conference.Warsaw, August 11-14*, 2014.

[28] G. Stoneburner, A. Goguen, and A. Feringa, “Risk management guide for information technology systems,” *Nist special publication*, vol. 800, no. 30, pp. 800–30, 2002.

[29] M. Fliszkiewicz, A. Krasuski, and K. Kreński, “ Evaluation of a Heat Release Rate based on Massively Generated Simulations and Machine Learning Approach,” in *Proceeding of FedCSIS 2014 Conference, Warsaw, September 9-11*, 2014.

[30] “ISO 31000 - Risk management,” 2009.