Risk management in military mobile communications

L. Lukas

***Abstract*—**Military Communication Systems (MCS) are a key element of Command and Control. MCS provide data transmission for Combat Information Systems. Situation awareness would be impossible without its proper functioning. The battle usage of MCS requires new planning and control approaches. Risk Management is a new approach which improves the timeliness and resilience of MCS. Risk Management is aimed at new ways of planning and managing business continuity during a combat deployment. Risk Mapping tools improve the planning process. Risk Management ensures business continuity management during a combat deployment. Risk Analysis and Risk Assessment are the most important points of this approach. A number of methods are suitable for Risk Analysis purposes. The FMEA method is a suitable method for Risk Management in MCS battle-usage. This article analyzes the Risk Management options to improve the resilience and timeliness of Military Mobile Communications.

***Keywords*—**military mobile communications, resilience, risk analysis, risk management, risk mapping.

I. Introduction

The mobile communication system ensures the transmission of information in battle areas where communication infrastructures are not available. It is used primarily by military forces at a time of emergency or military actions. The basis of mobile communication systems is a network of base stations and transit nodes. When we plan the deployment of a mobile communication system, it is important to quickly evaluate a series of parameters.

In the military area, planning involves studying and clarifying the mission task, evaluating the battle situation, creating variants of the task and option choices, and elaborating subordinate task forces and resources in a military environment. It is important to respect the difficulties and threats that can endanger the solution of this mission task. Risk Management is one of the ways to eliminate the impact of negative effects. The essence of this process is to identify risks that may jeopardize the task; then, design and prepare measures to eliminate the impacts of negative effects. In the past, this process was fulfilled pragmatically, based on previous experience. Nowadays, Risk Management and Risk Mapping uses more sophisticated approaches.

This work was with the financial support of Research Project: NPU I No. MSMT-7778/2014, from the Ministry of Education of the Czech Republic and also by the European Regional Development Fund under the Project: CEBIA-Tech No. CZ.1.05/2.1.00/03.0089 and the TBU project: *The Correlation of Critical Infrastructure and Functional Continuity of Territorial Units.*

L. Lukas. Author was with University of Defence in Brno, Czech Republic. He is now associate professor with Faculty of applied informatics, Tomas Bata University in Zlin, Czech Republic. (corresponding author to provide phone: +420-576 035 248, e-mail: lukas@fai.utb.cz).

II. Mobile Communication System

Mobile Communication Systems are used by military forces in time of emergency or military actions. Military Mobile Communication Systems are designed according to the Tacoms post 2000 standards. Current military MCS - developed according to the Tacoms post 2000 standards, have a fixed architecture. The MCS architecture consists of four subsystems. Each subsystem has specific features and quantities. These quantities depend on the manner of battle-usage, user-requirements - and the tactical scenario. The architecture of military MCS typically consists of [8]:

- A Wide Area Subsystem (WAS)
- A Local Area Subsystem (LAS)
- A Mobile Subsystem (MS)
- A System Management and Control System (SMCS).

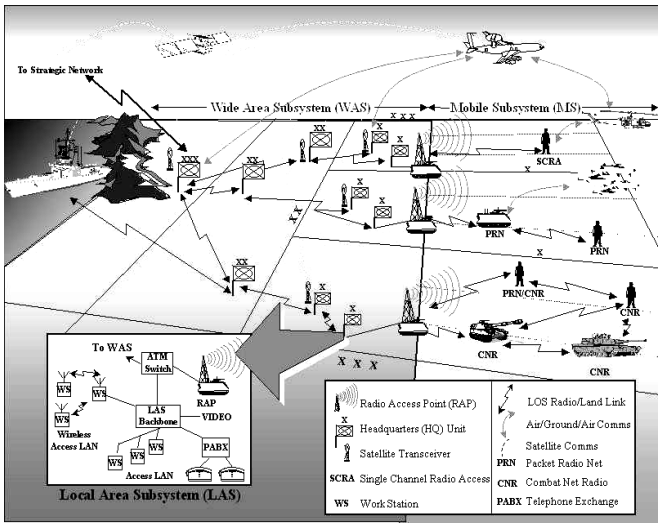

Fig.1 TACOMS post 2000 architecture [8]

A Wide Area Subsystem forms the backbone of area communications based on transit nodes. These nodes create the transit network. The transit network has a mesh topology. The transit nodes are connected by microwave radio relay stations. Each transit node covers a designated part of the

territory by using radio relay signals. Headquarters are connected to nearby transit nodes by microwave access links.

A Local Area Subsystem provides information distribution at the headquarters. This is typically created by a wireless LAN. A Mobile Subsystem connects the distributed mobile users into the MCS structure. Mobile users are connected to the transit network by connection through the nearest base station. A System Management Control System controls all these subsystems. It is used for the remote control of switches, radio-relay stations, links and radios.

III. MCS Deployment Problems

A Mobile Communication System is deployed on territory (i.e. battle areas) where normal communication infrastructures do not work [15]. An MCS is used in situations that require the synchronization of military activities. A communications infrastructure is usually disrupted by emergencies, enemy battle actions or where it does not exist in the deployment area. An MCS is deployed in this area as a temporary comsys to ensure information transmission. Deploying an MCS is an important prerequisite for commanding and controlling the operation of forces. The MCS provides voice and data services, including video signal transmission.

MCS deployment requires precise and correct planning. This process is mainly a capacitive and locale character. The cornerstone of good planning is the precise specification of the location of MCS elements. Base stations and transit nodes should be located so as to be able to provide connections between mobile terminals and access nodes. A transit node is typically established at a location that provides the requisite territorial coverage by radio signal. This key requirement is the basis for the selection the location of their deployment. However, at the same time, other dominant criteria should also be met. These criteria include ease-of-arrival and deployment, and ease-of- supply of energy and fuel.

An MCS may also be disrupted by an enemy jamming system. Artillery can be kept firing on transit nodes too. One´s own planning process is the combination of analytic and synthetic processes. An important role is played by the evaluation of the situation, the assessment of the requisite forces and the creation of an MCS model. The evaluation and design of the locations for the deployment of base stations and transit nodes is the basis of the assessment of the situation.

Risk assessment of locations in the deployment area allows the establishment of the explicit level of risk. The use of intuitive of risk level assessment earlier has now been replaced by Risk Mapping. Risk Mapping allows risk evaluation directly on the map, the assessment of all locations of interest, and the selection of those locations that meet other requirements.

The Risk Mapping process represents the risk calculation for all of a location entity in the area of interest. Location entities are usually considered as separate elements of the Spatial Grid. An element is usually a 100 x 100 m square. The assessed risk generally reflects all the static attributes of the territory, i.e. elevation, hydrography, road networks, settlements, forests, etc. The dynamic attributes of the situation are another great advantage of risk mapping too. These attributes can create a special layer of GIS for the evaluation of situations and for risk calculation.

For example, if we take into account the possibility of intentional enemy jamming and the shielding properties of the terrain; the impact of jamming on individual grid elements can be calculated. Direct Line of Sight between jammer and transit node is the basis for this calculation. The newly created GIS layer, expressing the possibility of enemy jamming, allows one to assess selected dominants and to offer various selections of locations for base stations and transit nodes, and allows the use of the shading properties of the terrain. Similarly, it can also assess the possibility of rapid leaving dominants in different ways and roads, taking into account the masking properties of terrain for HQ, etc.

IV. MCS Deployment Problems

Command and Control (C2) is an information process which depends purely on the transmission and processing of information. Every military organization has its own Communication and Information System. Communication and Information Systems (CIS) are dynamic systems which provide the communication and information support required for the command and control of troops. CIS provides this support for the Command and Control Process [12], i.e.:

- continuous command of subordinate units
- transmission of information between cooperating units
- transmission of warning signals
- logistical support management

A CIS must be able to fulfill all functions related to the control process. The structure of the command and control system is based on the organization of command and control. This must comply with the rules and principles of the organization and the building of the system to cover the communication and information section by its powers. The individual functions of the management process can mutually overlap. The process is divided into these steps:

- receiving, studying and clarifying tasks with the necessary conclusions for the control members
- the collection and analysis of information with a mission and signal character
- the creation of a communication system structure model based on the expected variants of the planned battle operations
- the processing of command documents (e.g., contribution to the battle orders of the commander)
- the organization of building-up and operating mobile communications networks

Risk Mapping can be used as a new approach to planning steps and managing risk in operation steps.

V. Risk Mapping

Planning is an important part of management. It is an information-based process, where mapping can be used. Risk Mapping is the representation of risks on a map. Risk Mapping is a process that identifies areas with different levels of risks of injury or potential emergencies. This is the point-of-view of the risk assessment results for special map (i.e. a risk map), showing the level of expected losses of communication equipment that can be expected in a given territory. A Risk Map allows one to identify the composition and risk-level of each part of the analyzed territory.

The basis of Risk Mapping is the classification and quantification of risks in relation to the territory. It is an expression of the level of risk for all elements on the map. The risk is interpreted as a sum of complex risks for different types of emergencies. The basic premise is that, by mapping risks, one can include only those types of emergencies whose impact can be expressed in some way on the map.

The use of simple numerical and statistical analyses in risk mapping is to obtain more accurate and realistic results. The development of risk mapping is unthinkable without the support of a GIS. Only GIS technologies allow the application of all of the principles of the risk mapping method to get useful results. Risk Mapping includes only those types of emergencies whose impact can be expressed on the map by a special GIS layer (such as list of objects of a given type, a list of dominants, or a list of coordinates).

This layer can be static or dynamic. The static layer is a long-term view based on static geographic data. The dynamic layer represents the interaction of static geographic data and about elements that are temporarily placed in the terrain and can have an effect on the deployed MCS. Risk Mapping uses Risk Analysis results for different types of emergencies.

Mapping uses the results of the analysis of possible emergencies in the terrain (i.e. battle area). These sub-analyses can be made on the basis of Numerical Model Calculations (e.g. hazardous substance leakage, enemy radio jamming), long-term meteorological and hydrological monitoring statistics (e.g., floodplains during natural floods, snow and wind fields), monitoring natural phenomena and other methods - expert estimates included.

Risk Maps are cartographic layers of a defined area (e.g., a municipality, county, area of deployment), on which risk levels are marked with different colors. The map displays risk level depicted in the color scale. This visualization highlights areas with higher levels of risk, and is then subject to further investigation of why there is such a risk, and its composition (i.e. what is due), etc. Risk is the product of Threat Probability and Damage level:

$$P = D \times F \quad (1)$$

R – Risk level
P – Probability - (likelihood) of a threat
D – Damage

Risk (R) is thus the expected adverse effects due to activation of the threat in the territory. Any important aspect shall be taken into account in the risk mapping process. This aspect is about the distribution of the threat impact. Nearly all of the defined types of threat – i.e. the probability of threat exposure to the entire surface area, are not constant. A typical example is the kind of threat that comes from a particular source. In areas adjacent to the threat source, the damage caused by the activation of the hazard is usually more intense than in remote areas.

VI. Cumulative Risk Map

The next phase of Risk Mapping is to create Cumulative Risk Maps (CRM). A CRM is created by individual risk interactions. The maximum value of the cumulative risk expressed in an index can be assumed to be 1. For cartographic visualization, it is appropriate to divide the set of values into classes that are in the interval (0, 1), each of which represents a range of values. Each class is assigned a suitable color. The distribution of values in classes can be linear or nonlinear.

Table 1 Range of values

Range of Values	Color
> 0.6	Red
0.6 – 0.5	Orange
0.4 – 0.3	Yellow
0.2 – 0.1	Light-green
< 0.1	Dark-green

The whole range of cumulative risk index values, representing risk level, can be as expressed verbally in this way. The color scale allows the visualization of the risk level. The importance of visualization is primarily to highlight and draw attention to areas with higher levels of risk. If one would like to work with a risk map, and to obtain accurate information about the location of risks, it is necessary to use GIS software or to create a special application.

Table 2 Verbal representation of cumulative risk

I_r	Verbal Expression of Risk	Content of Representation
> 0.6	Very high	Risk is obviously high - unacceptable. Preventive measures are necessary.
0.6 – 0.5	High	Risk is obvious. Preventive measures are recommended.
0.4 – 0.3	Medium	Risk is significant - acceptable. It does not require preventive measures.
0.2 – 0.1	Low	Risk is barely noticeable.
< 0.1	Very low	Risk is acceptable.

The development of a risk map enables one to obtain a comprehensive overview of the risks in the MCS deployment area.

Using GIS software enables us to get accurate information about a particular place – e.g. the structure of vulnerability for an analysis of preparedness, etc. Using risk mapping results, one can evaluate and optimize the deployment of MCS resources.

The Risk Map enables one to perform complex analyses - like finding the maximum risk on the risk map, etc. The Risk Map will be an important tool in planning the deployment of a mobile communication system.

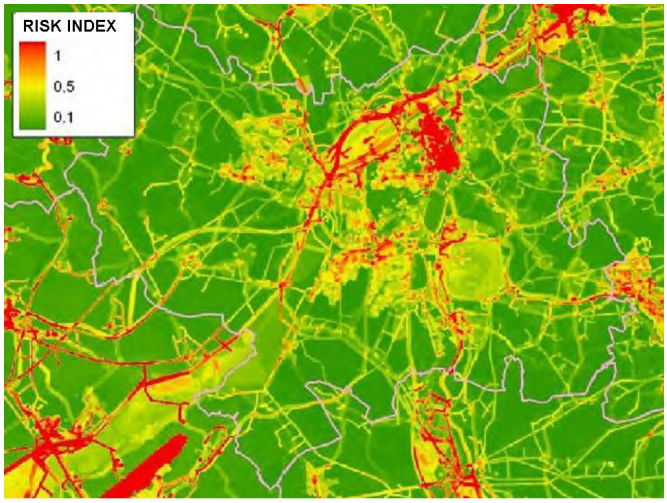

Fig. 2 I_r Risk Map [11]

VII. Risk Mapping in Mobile Communications

Based on an analysis of the mobile communication system deployment process, the basic layers of Risk Mapping include:

- Radio Coverage risk layer
- Enemy Jamming risk layer
- Deployment risk layer
- Logistics risk layer

A. Radio Coverage risk layer

One of the roles of transit nodes is to ensure connections between the access nodes and network. The second role is to create a transit network. The deployment location is usually chosen with regard to the Command Posts (CPs) position. There must be a direct line-of-sight between the transit and access nodes. Risk exists when the location of an access node is unknown. Therefore, the transit node location is selected where the radio signal covers the maximum possible of the battle area. If the greater proportion of the area is covered by the radio signal there is a lower risk that the new position of an access node will not link to the transit node. The level of risk is determined as a supplement to the ratio of the surface area covered by the radio signal to the total surface of the battle area.

B. Enemy Jamming risk layer

An MCS represents a very important target for an enemy. All communication nodes are First Order Targets. These are typically canceled by jamming radio signals. The effect of radio jamming depends on the profile of the terrain between the jammers and the transit node. If there is no direct visibility between both nodes, the jamming signal is attenuated by the terrain – and the transit node is not jammed. It is important to know the expected locations of enemy jammers so as to determine the coverage of the battle area by jamming signals. The risk of jamming is determined by the identification of the level of the jamming signal at different battle area locations.

C. Deployment risk layer

The objective of a Deployment Risk Assessment is to evaluate the possibility of deploying to a designated dominant by sheltered vehicles. The basic deployment criteria include the existence, type and quality of roads. The steepness of the slope is another criterion. The Risk Level is proportional to the steepness of the gradient and inversely proportional to the density of roads in the location. If the road density is greater, then the risk of the unavailability of dominant positions is less. Forest roads have a greater risk of unavailability than hard-surfaced roads. The roads´ density also reduces the risk in the time needed to rapid leave a location.

D. Logistics risk layer

The operability of the transit node depends on electricity supply possibilities. Electricity is usually generated by mobile power generators. It is advantageous for transit nodes when a telecommunications facility, hotel or building is on a dominant point. This facility can supply a transit node with electricity. The risk of the failure of the transit node due to electricity supply failure is much lower than when power is provided by a mobile power station. Its operation is threatened by technical failures or fuel supply problems.

Each of the layers above must be set for the battle area and created on the basis of a specific calculation. The calculation is done for the entire area, and selectively for chosen dominants or locations. Taking into account the risks improves the overall planning process and allows Signals officers to select a deployment area that represents less risk for the mobile communication system operation.

VIII. Risk Management

The aim of Risk Management is to focus on the quality of individual processes [14]. In a dynamic environment where many factors negatively affect operations, it is appropriate to expand the problem´s solution by an assessment of threats and their elimination. This part of the management process allows one to proactively prepare for negative factors. Provision of C2 communications and information support belongs to areas whose outcome is influenced by a number of negative factors – especially, enemy action. The use of Risk Management improves the signal unit´s task performance quality.

Risk Assessment provides a mechanism for identifying which risks represent potential pitfalls for an organization. For risk assessments to yield meaningful results, certain key

principles must be considered. Risk Assessment is a systematic process for identifying and evaluating events that could affect the achievement of an aim. Such events can be identified in both the external and internal environments too. Risk is difficult to qualify or quantify because the basic assumptions for calculating mathematical probability cannot be met. Risk Assessment consists of several key steps. These include:

- Threat Identification
- Probability/Likelihood Assessment
- Risk Assessment, and …
- Risk Management

A. Threat Identification

This is the identification, description and understanding of what a threat´s impact on organizations´ assets or processes will be, and the selection of the appropriate threat level. Threat is an active actor with capabilities and the intent to do harm to an asset. Threats are characterized by their level of impact on an asset. Some threats have a high impact, others low. Basic MCS threats include enemy jamming, truck failure, the wrong location of a transit node, etc.

B. Probability Assessment

This is the likelihood that a target has been, or will be selected by a threat actor; how threat actors view organization´s assets; and which assets threats find the most attractive to exploit. This can be accomplished by using statistical values or estimates.

C. Risk Assessment

Expresses risk in the form of a calculation. This should be scalable so that the risk can be calculated for any single key asset or for the entire organization. Risk Prioritization is an important part of Risk Assessment. One needs to prioritize risk such that the most important risk can be mitigated first, and the least important risk will be mitigated last.

D. Risk Management

This provides recommendations for countermeasures to mitigate risks. Basic strategies can be used for Risk Management - like avoiding, sharing, reducing or accepting risk.

In order to protect the organization´s assets, we must determine what those assets are. All organizations have three type of asset: People, Property (i.e. Signal Equipment) and Information. A Risk Analyst must determine what those assets are, and how critical those assets are, to an organization´s mission and what consequences could occur if vulnerabilities are exploited.

Evaluation can be performed quantitatively and qualitatively. The method used depends on the data available. The most accurate assessment is Quantitative – the available data is expressed numerically and the results are easily expressible and understandable. Qualitative assessment is used to express the probability (likelihood) of an event by using words such as Low, Middle and High- the likelihood (probability) and its effects are estimated. Qualitative methods can be used for Risk Analysis and Assessment for Mobile Communications. The reasons are:

- It is not an economic system where it is possible to quantify impact by financial loss
- We need to identify the level of the impact and the priorities to be measured
- We need to measure priorities, especially for events caused by external effects
- Probability/likelihood is usually only verbally estimated

The key stage of the Risk Management process is the Risk Analysis and Assessment. Based on an assessment of the appropriateness of Risk Analysis methods for Military Communications Management, the following methods can be recommended:

- Scenario Analysis (SA)
- Business Impact Analysis (BIA)
- Cause and Effect Analysis CEA)
- Failure Modes and Effect Analysis (FMEA)

Each method has its own advantages and disadvantages. All these methods are scenario-based. The FMEA method can be used for Mobile Communication Risk Analysis and Assessment.

IX. The Failure Modes and Effects Analysis Method

The FMEA method is a technique used to identify the failure modes of systems and processes. Using FMEA, one can identify:

- Possible failure modes
- The consequences that these disorders can have on the system
- Ways of preventing or mitigating the consequences of failure

The FMEA method can be used both during the design of the system as well as for its operation [10]. The method helps in terms of safety when choosing design alternatives and their assessment. The method also provides consideration of all kinds of system failures and their consequences. The method identifies the forms and consequences of human errors. It improves the proposal of processes too. The FMEA method can be combined with other analysis techniques, such as Event Tree Analysis, for instance.

Information about elements and their failures are the input information for the FMEA method - more detailed information provides a deeper analysis. This information may include flowcharts, functional descriptions of elements, evaluation of the environment, the consequences of failure descriptions and historical information about failures.

The FMEA process involves the following steps:

- Setting objectives and the scope of the mission (Study)
- The formation of the assessment team (Signal Officers)
- The definition of the system being evaluated and its elements
- The determination of the function of each element (Phase or Step)
- And for each element of the set:
  - What faults may occur?
  - What mechanisms can cause faults?
  - What (consequences) failure could cause?
  - How harmful is failure?
  - How failure is detected
- To identify measures to eliminate disturbances.

The Degree of Criticality is assessed when evaluating failure or disorders. The basic assessment methods of Failure Criticality include a Criticality Index, the level of risk, or the risk priority number. The Risk Level is obtained by combining the consequences of an impact and its´ Failure Probability. The FMEA analysis output is a list of failures, their causes, the consequences for each component and elimination measures. It is also important to determine a threat´s priority and criticality. The final assessment provides a comprehensive overview of possible negative effects occurring and ways to eliminate them. In the next part of the article, an example of the use of the Risk Management method in the Military Communications field is discussed.

X. Risk Management in the Redeployment of a Mobile Communication System

The most important stage of Mobile Communication Systems Management is to fulfill the signal mission. Signal units provide C2 Communications and Information Support tasks in a mission area. The use of Risk Management in the management of mobile communications is depicted in the mission fulfillment example. For Risk Management, it is important what time-frame is available to perform the risk assessment.

Available data also affects the range of the assessment process. Many data items are only estimated based on previous experience. The Risk Value and Risk Assessment are carried out qualitatively in our example. The FMEA method was chosen based on an assessment of the adequacy of several risk analysis methods and because it allows both Risk Analysis and Risk Assessment. The Risk Management process includes the following phases:

- Determining the mission stages
- Threat identification in the mission stages
- Risk Analysis
- Risk Assessment
- The definition of a strategy to eliminate risk (e.g. avoid, reduce/share, accept)
- Identification of measures to eliminate the risk

A fulfilled mission typically involves the following stages:

- Redeployment of signal units
- Placement in deployment location
- Network traffic in the mission area
- Redeployment to finish the mission

Fulfilling a task is menaced by many threats. These threats include: Signal truck crashes, Signal truck failures, the wrong radio-relay profile, reductions in fuel, etc. The Risk Analysis, Risk Assessment and Risk Management processes results are depicted in Table 3. The strategy adopted to eliminate risk is based on its size. If the risk is high – we usually avoid it. At medium risk levels, there is a need to reduce the causes, or to share the consequences. Low risk is usually accepted – or this can be reduced too.

The main measures to eliminate risks include the strict preparation of orders, the checking of railway underpasses, a mobile repair car, reconnaissance, an anti-jamming regime, convoy protection, etc. The example shows how to use Risk Management techniques in Tactical Communications Management. Many data items have only an approximate value and must be clarified. The data will also depend on the mission´s range, signal units´ capabilities, enemy capabilities, etc. Because Risk Management is elaborated, it allows the use of more accurate Risk Analysis and Identification methods and measures. The Risk Management method allows signal officers to systematically prepare for situations that may affect the fulfillment of the Signal Unit´s mission.

XI. Conclusion

Risk Management is one of the most important management areas. It allows the resolution and management of problems (crises) by using Risk Identification and Prioritization and the preparation of Risk Elimination Measures. Risk Management is a separate area, which has found its application in many fields. Risk Management tools are used in Crisis Management, Technological Systems, Property Protection, Investments and Military Mobile Communication systems too. Risk Analysis is the basis of Risk Management. Correct identification of risks enables the development of measures to overcome them. The basic strategies for managing risk include avoiding, sharing, reducing and accepting risk. Risk Management methods can be used in the Mobile Communications field. Planning of the Mobile Communication system model and the establishment and operation of mobile communications are the most important phases of ensuring Command and Control Communication and Information Support. The FMEA method is suitable for risk analysis in tactical communications. Its use is demonstrated in the last part of the article. The use of Risk Management methods has wide implementation uses in Tactical Communications. Risk Management enables a higher level of signal task fulfillment.

Risk Mapping is a new way of using GIS in Communication Planning. Today, the Risk Management concept can be used in choosing the sites or location of transit nodes. Special GIS layers are devised that express the Risk Assessment for individual points of a battle area.

Table 3. Risk Management in Mobile Communication Missions

Phase	Threat	No.	Consequence	Risk			Strategy	Measure(s):
				Probability	Impact	Risk		
Redeployment of Signal Resource	Wrong order: redeployment	R1	Longer time to redeploy	L	M	M	R	Strict preparation of orders
	Collapse of convoy	R2	Longer time to redeploy	M	L	M	R	Redeployment Tactics
	Wrong route: (bridge, tunnel)	R3	Longer time to redeploy	M	L	M	R	Checking railway underpasses
	Truck crash	R4	Signal Capacity Outage	L	M	M	S	Reserve signal truck
	Truck failure	R5	Signal Capacity Outage	L	L	L	R	Mobile repair car
Place-ment	Wrong location of node	P1	Communication Outage	M	H	H	R/S	GPS, maps, reserve node
	Unsuitable place for node	P2	Communication delays	L	M	M	R	Reconnaissance
	Wrong profile for radio-relay	P3	Troops without communication	M	H	H	R	High-quality planning
	Wrong radio frequency data (i.e. Jamming)	P4	Troops without communication	L	M	M	R	Reserve radio frequency data, signal radio net
Network traffic	Station failure	N1	Communication reduction	M	L	M	R/S	Repair, reserve
	Transmission jamming	N2	Communication reduction	M	M	M	R	Anti-jamming regime
	Station destruction	N3	Communication reduction	L	L	L	S	Reserve
	Net infection with a virus	N4	Communication outage	L	H	H	R	Anti-virus measures
	Network Management Failure	N5	Communication reduction	L	M	M	R/S	Reserve Management Shelter
	Fuel reduction (or electricity outage)	N6	Communication outage	M	H	H	R/S	Own fuel supplies, HQ Logistics
Redeployment to finish operation	Fuel reduction	F1	Longer time to redeploy	M	L	M	R/S	Own fuel supplies HQ Logistics
	Truck failure	F2	Longer time to redeploy	L	L	L	R	Mobile repair vehicle
	Truck crush	F3	Longer time to redeploy	L	M	M	R	Vehicle extrication
	Destroyed car	F4	Signal Capability Reduction	L	M	M	A/R	Convoy protection

L – Low, M – Middle, H – High, R – Reduce, S –Share, A – Avoid, Ac – Accept

These layers include the Radio Coverage risk layer, Enemy Jamming risk layer, Deployment risk layer and the Logistics risk layer. Its integration can more accurately select locations for transit network nodes and for MCS planning. An MCS planned in this manner has greater resilience. Risk Management is one of the most important management areas of an MCS. It allows the management of deployments through Risk Identification, Prioritization and Risks Elimination Measures preparation.

REFERENCES

[1] Baker, J. C. ,. Lachman B. E., and Frelinger D. R. "Mapping the Risks: Assessing the Homeland Security Implications of Publicly Available Geospatial Information." RAND Corporation, 2004.

[2] Bojkovic, Z., Bakmaz, B. "*A Survey on Wireless Sensor Networks Deployment.*" WSEAS Tran on Comm. 12, 2008. pp 1172 – 1181

[3] Brace, I. M., "Mobile Tactical Data Networks." System Design Group Pty Ltd., 2014.

[4] Campbell G. K. "Measures and Metrics in Corporate Security." Elsvier, 2014.

[5] Diaz J., Petit J. and Serna M. "*A random graph model for optical networks of sensors,"* IEEE Trans. on Mob Comp, 2003, vol. 2, 143-154.

[6] Elmasry, G. F., "Tactical Wireless Communications and Networks: Design Concepts and Challenges." John Willey&Sons, 2014.

[7] Fuka J et al., "Game Theory as a Tool of Research and Fight against Terrorism." Proceedings of the 2nd International Conference on Risk Management, Assessment and Mitigation (RIMA '13), 2013. pp. 182 - 187

[8] Gajdosik, J., and Lukas, L. *"The Flexible Architecture of Tactical Communication Systems,"* IEEE MILCOM 2000. pp. 105 – 109.

[9] Hromada, M., *"Resilience of CR Critical Infrastructure."* Sdruzeni pozarniho inzenyrstvi, 2014.

[10] IEC/ISO 31010:2009, "Risk management – Risk assessment method." Praha : UNMZ, 2011.

[11] Kromer, A., Musial, P., and Folwarczny, L., "Risk Mapping." Sdruzeni pozarniho inzenyrstvi, 2010.

[12] Lukas, L., Hlavica, J., and Tkacik, J., "Management of C2 Communication and Information Support." University of Defense, 2005.

[13] Rozsypal, L., "Communication and Information Support of Command and Control Systems." University of Defense, 2007.

[14] Penrose, M. D., "Random Geometric Graphs." Oxford University Press, 2003.

[15] Piyapong, J., Watanabe, T., *"Analysis of Citizen Quantitative Risk Assessment for the Development of Environmental Risk Communication in Contaminated Sites."* WSEAS Trans on Env and Dev. 10, 2014. pp. 274 - 287

[16] Poisel, R., "Introduction to Communication Electronic Warfare Systems." Artech House, 2008.

[17] Tont, M. D., Tont, G., and Tont, D. G., *"Integrated Framework for Risk Assessment in Socio-Technical Systems."* In: Risk Management, Assessment and Mitigation (RIMA), 2014. pp 252 – 257

[18] Tont, G, *"The Operating Risk Assessment for Dependable Systems."* WSEAS International Conference on Mathematical and Computational Techniques in Electrical Engineering (MMACTEE '09), 2009. pp 737 – 742

L. Lukas - (LTC ret.) was born in 1958. He graduated university studies in 1981 at Military Technical University in Liptovsky Mikulas (Slovakia) and doctoral studies in 1993 at Military Academy in Brno (Czech Republic).

During his working at the Military Academy in Brno (1991 - 2005) he held the function of lecturer, group leader, head of department and vice rector for study affairs. He currently works at the Tomas Bata University in Zlín as associate professor. His scientific research, publishing and educational activities are focused into area of C2 communication and information support, information management, physical security and critical infrastructure protection.