TECHNICAL SCIENCES
Abbrev.: Techn. Sc., No 15(1), Y 2012

USER REQUIREMENTS FOR MISSION-CRITICAL APPLICATION – THE SECRICOM CASE

***Shaun O'Neill*[1], *Jim Strother*[1], *Jan Zych*[2], *Wojciech Wojciechowicz*[2,3]**

[1] British Association of Public Salety Communications Officials
[2] ITTI sp. z o.o., Poznań
[3] Institute of Computing Science, Poznań University of Technology

K e y w o r d s: SECRICOM, Interoperability, Crisis Management, Requirements Engineering, Critical system

A b s t r a c t

The SECRICOM Project as a communication system for operational crisis management, requires paying significant attention to the requirements engineering phase. Any mistakes made during the requirements gathering phase may affect the subsequent software development phases, which creates excessive operational risks for the users of the system. These types of risks – as in any other critical systems – could have serious consequences, such as inefficiency of rescue actions and loss of lives.

This article presents the requirements engineering process, which was defined and carried out for the needs of the SECRICOM project. It describes the system's environment (the crisis management reference structure and the main organizational rules) and its impact on the developed. As a result, a requirements engineering process for SECRICOM is proposed. Finally, main points of gathered requirements are presented.

WYMAGANIA UŻYTKOWNIKA DOTYCZĄCE SYSTEMU KRYTYCZNEGO – PRZYPADEK SECRICOM

***Shaun O'Neill*[1], *Jim Strother*[1], *Jan Zych*[2], *Wojciech Wojciechowicz*[2,3]**

[1] British Association of Public Salety Communications Officials
[2] ITTI sp. z o.o., Poznań
[3] Insytut Informatyki, Politechnika Poznańska

S ł o w a k l u c z o w e: SECRICOM, interoperacyjność, zarządzanie kryzysowe, inżynieria wymagań, system krytyczny.

Abstrakt

W systemie SECRICOM, ze względu na tworzenie systemu komunikacji do operacyjnego zarządzania kryzysowego, szczególnie ważne było położenie szczególnego nacisku na etap gromadzenia wymagań. Błędy popełnione na etapie specyfikacji wymagań mogą rzutować na kolejne etapy wytwarzania systemu, co w rezultacie generuje nadmiarowe ryzyka dla użytkowników systemu. Ryzyka te – jak w przypadku innych systemów krytycznych – mogą spowodować poważne konsekwencje, w tym obniżenie skuteczności akcji ratunkowych, a nawet straty po stronie ludności.

W artykule przedstawiono proces inżynierii wymagań, który zdefiniowano oraz przeprowadzono na potrzeby projektu SECRICOM. Przedstawiono środowisko systemu (zarówno referencyjną strukturę zarządzania kryzysowego, jak i główne zasady organizacji) oraz określono wpływ na budowany system. Na zakończenie przedstawiono główne wnioski z zebranych wymagań.

Introduction

This paper describes an approach to manage user requirements for the mission critical application, which was developed within the SECRICOM project. The main aim of the SECRICOM project is to propose a seamless and secure reference communication platform for EU crisis management operations. For that purpose, the first step within the SECRICOM project was to specify the requirements to be fulfilled by such a platform. As a result, not only user requirements were specified, but also a methodology for managing user needs for mission-critical application was created.

This article consists of four chapters. In the first chapter, the crisis management structure used by SECRICOM to gather the requirements is described. The second chapter explains the principles of crisis management and its impact on the capability gap analysis. The third chapter presents selected user requirements gathered in the SECRICOM project. The conclusions are provided in the fourth chapter.

Reference crisis management structure

In order to better address the user requirements, a reference crisis management structure has been proposed within the SECRICOM project and it is going to be described in this section. Typically, operational emergency services use a 3-tier command structure. For that reason the same command chain was proposed for the aim of collecting user requirements' in SECRICOM. Members of senior civil protection, and emergency service personnel in the UK, Luxembourg, Slovakia, Spain, Sweden and Poland, validated the structure. All the aforementioned parties agreed that the basic operational structure for the emergency services is similar, and it is based on three tiers:

strategic command, tactical command and operational (called also ground command). In the UK these tiers are represented by three types of metals – Gold, Silver and Bronze – hence the colours in Figure 1.

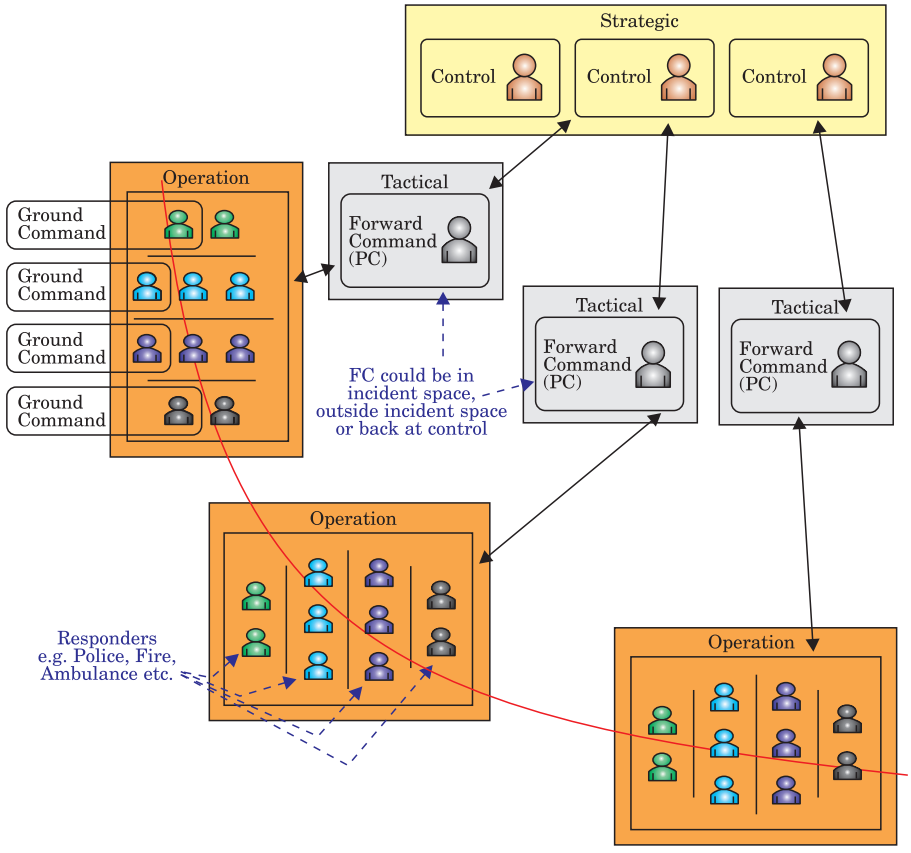


Fig. 1. Emergency Service Command Structure
Source: SECRICOM project.

The command structure has significant impact on gathering the user requirements; not only in terms of functional requirements (e.g. circuit-switched voice communication, Push To Talk, data transfer) but also non-functional requirements (e.g. security requirements) – as confirmed during the project.

Principle of crisis management

Crisis management is a process carried out by public authorities in co-operation with organisations, institutions and society in general, to cope with the crisis and ensure broadly defined public safety. Assuming that crisis management includes the whole sphere of the crisis situations, prevention issues occurring before, during and after an event, it is taken that its process should comprise of four permeating and highly connected fields of action that all constitute four phases of the crisis management. In each phase, challenges related to communication are identified. What's more, each of them expects different functionalities from communication. It seems that synthetic characterisation of each phase is necessary. Decision making process within the crisis management is greatly determined by the quality of system communication.

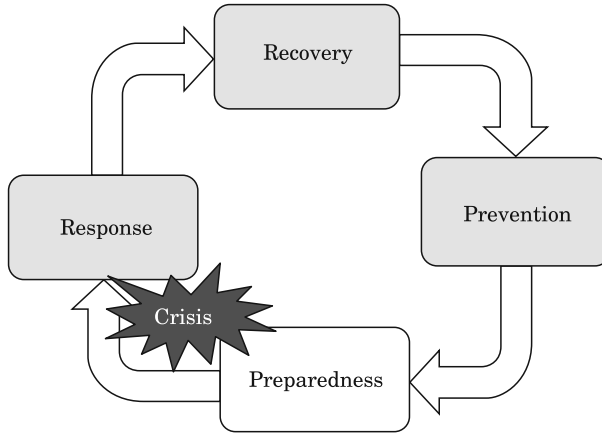


Fig. 2. Crisis management phases
Source: own elaboration based on http://oki.krakow.rzgw.gov.pl.

Prevention phase – the priority in this phase is to take actions, which will eliminate or significantly decrease the probability of a crisis situation occurrence and reduce its consequences. The main objective of undertaken actions is to foil the occurrence of a threat. Should it happen, the prevention phase will focus on minimizing potential effects. Preventive actions mainly deal with the risk analysis, predicting, spatial planning, strategic planning, realisation of investments increasing safety, planning and developing preventive actions, monitoring possible threatening events, systematic classification and identification of a threat sources and evaluation of mental and technical state of the society to the crisis management. However, there are threats which cannot be

prevented, for example natural disasters. The only thing that can be done in such situation is to minimise the effects. All actions in this phase are constant, which plays an important role in the whole process of the crisis management. It seems obvious that without properly organised communication the realisation of prevention phase related tasks are impossible or at least very problematic. In this phase, requirements concerning communication revolve around gathering information from multiple sensors, its processing and developing preventive measures.

Preparedness phase – deals with identification of a potential threats, analysis of their character and probability of occurrence. In this phase, it is crucial to formulate roadmaps and operation plans that would be executed during the crisis situations, organise communication as well as warning and alarm systems, establish crisis management centres and provide various services and citizens with proper training of how to behave during the crisis situation. Furthermore, in this phase, actions aiming at increasing manpower and resources necessary for effective reactions are taken. One should remember that communication plans (usually formulated in several versions – for instance in the event of damage of a part of communication infrastructure, among others) shall be developed in this phase.

Response phase – is about taking actions initiating rescue services work, directly responsible for eliminating or limiting the scope of arising crisis situations, which should provide victims with necessary help and neutralize sources of a threat. It's a phase of practical actions that are taken in the event of the crisis situation. Without compelling and well-organised communication those actions cannot be taken efficiently. Properly organised communication is a key to rescue actions. Constantly informing citizens about current situation state is a vital element in the crisis management. Yet, it could not be generated until efficient information flow is established. Taken actions are determined by the character and the size of an event. At this stage all neglected elements from previous phases can be noticed. Any faults or deficiencies in organisation communication may cause great loses. Reacting relies on scrupulous event analyses, designing set of possible solutions, taking right decisions and coordinating works using means of communication.

Recovery phase – it covers actions, of which main objective is to reconstruct infrastructure and strengthen its former state taking into consideration gained experience so as not to let similar situation happen in the future. Such actions rely on damage assessment, helping citizens, replenishing resources and formulating conclusions. It is important to isolate those elements that have been damaged or destroyed. Taken actions should focus not only on eliminating the effects but also on removing causes determining the occurrence of a given crisis situation. There is a visible interdependence between the

crisis management phases as mistakes made in the initial phases generate negative consequences during decision making process. The borders between certain crisis management phases are disappearing, which formulate decision making to a continuous process.

From the communication system point of view, the most challenging is the response phase. The response phase is characterized by a variety of emergency plans that are put into action in order to rescue lives and minimize the damage in a disaster or emergency situation. Response is the phase where actual rescue actions are undertaken; these actions include search and rescue, risk assessment, first responders' actions (Ambulances, Fire brigade, Police, etc). Given the unpredictability of natural disasters, this phase requires that first responders conduct rescue actions in real-time in order to stabilize the situation and avoid further damage. Under these circumstances, the need for exchanging information between participants of the rescue actions is undeniable. Another important principle – from communication system perspective -is the decision making process, as presented in Figure 3.

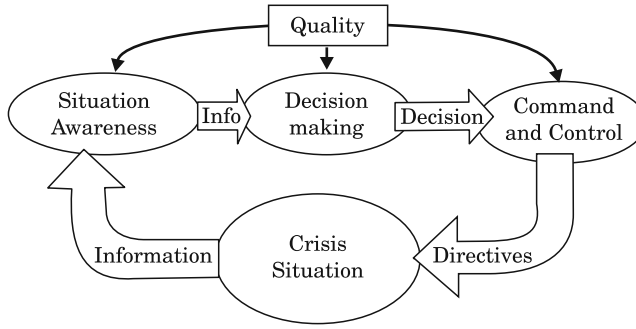


Fig. 3. Crisis management decision making process

The crisis management structure was used in conjunction with the decision-making procedures to show how operational decisions are made. Starting at the Situation Awareness, we can notice that the quality of information available about the situation affects the quality of decision-making, which in turn influences the quality of Command and Control orders and directions. These should have a positive impact on the situation on the ground. New information feeds the tactical and strategic commanders' situational awareness and the circular motion continues. This principle was used as a basis to analyse the capability gap SECRICOM was intended to address.

User requirements in SECRICOM

SECRICOM approach

After reviewing some of the most popular approaches to the requirements engineering, it was decided that none of them fully meets SECRICOM project's needs. As a result, a dedicated approach to the requirement engineering process has been developed within the project. The high-level overview of this approach is presented in the Figure 4.

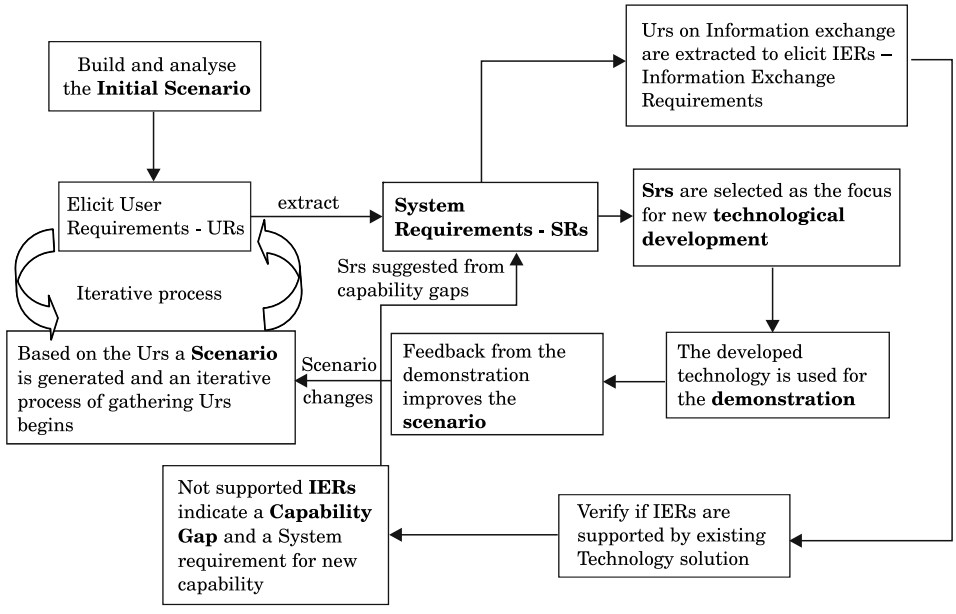


Fig. 4. SECRICOM Requirements Gathering
Source: own elaboration.

The approach used in SECIRCOM is summarized as follows:

– At the beginning, user requirements are collected from an initial scenario (report or debriefing of an incident). From these URs a new scenario is generated. Afterwards, an iterative process of extracting user requirements that improve the given scenario begins.

– System requirements are selected form the URs, which defines the technology development required.

– Information Exchange Requirements (IERs) are considered the URs that concern exchange of information; IERs are used in gap analysis.

– When an IER is not supported by the existing technology, it is considered a technology capability gap and a new requirement for technology improvements is elicited.

User Focus

Since the SECRICOM project from the very beginning was user-oriented, a User Team had been established for collecting requirements. The team had representatives from various countries as well as agencies to ensure that a complete spectrum of issues is addressed within the project. The B-APCO was responsible for leading this group.

The User Team comprised representatives from Spain, Sweden and UK. These individuals reflected a variety of roles and responsibilities in terms of national, regional and local first responders' agencies. Furthermore, between the members of the user group, they held a range of senior, middle and junior management roles within Fire, Police and Local Authority agencies.

Users constitute the most important source of information in SECRICOM, because it was possible to obtain from them experience based statements, remarks and suggestions from individuals well versed in crisis management and in terms not only of functional requirements, but also non-functional, incl. security requirements for communications assets needed during a major crisis.

IER

In this section Information Exchange Requirements are presented and their use and benefit for defining the requirements for crisis management communication technologies is described.

Information Exchange Requirements (IER) are defined as "the description, in terms of characteristics of the requirement to transfer information between two or more end users. The characteristics described include source, recipients, contents, size, timeliness, security and trigger. IERs are defined to be independent of the communications medium. An IER can express both current and future requirements" (http://ceur-ws.org/Vol-340/paper03.pdf).

Therefore, the purpose of the IERs is to provide structured means for establishing the capability gap and thus defining new requirements. An IER is the *Unconstrained User Requirement for Information Exchange*, thus IERs shall be technology, system and solution independent. IERs are used in capability gap analysis to model URs, which may (or not) be supported by current technology solutions. In order to capture the IERs about an activity or

actor, it is necessary to have a well-defined set of URs, and most importantly, these URs should be independent of the technology or system.

To capture the IERs in SECRICOM, the following approach has been applied:

– Define a set of **User Requirements** – describe what users want to achieve.
– A representative **Scenario** brings URs to life.
– The Scenario is broken down into **Activities**.
– Activities are recorded as **IERs**.
– Each activity has one or more IERs associated with it.
– IERs fall into Situational Awareness or Command and Control.

Every operational need for a piece of information to be transferred from one place or person to another has been captured. Then IERs were used in a realistic scenario to ensure that all relevant activities were represented – and in particular to allocate them into Situation Awareness or Command and Control.

IER capture was done in an in-depth exercise during the User Team Exercise in September 2009. In total, over 700 IERs were captured, providing information across a range of criteria including:

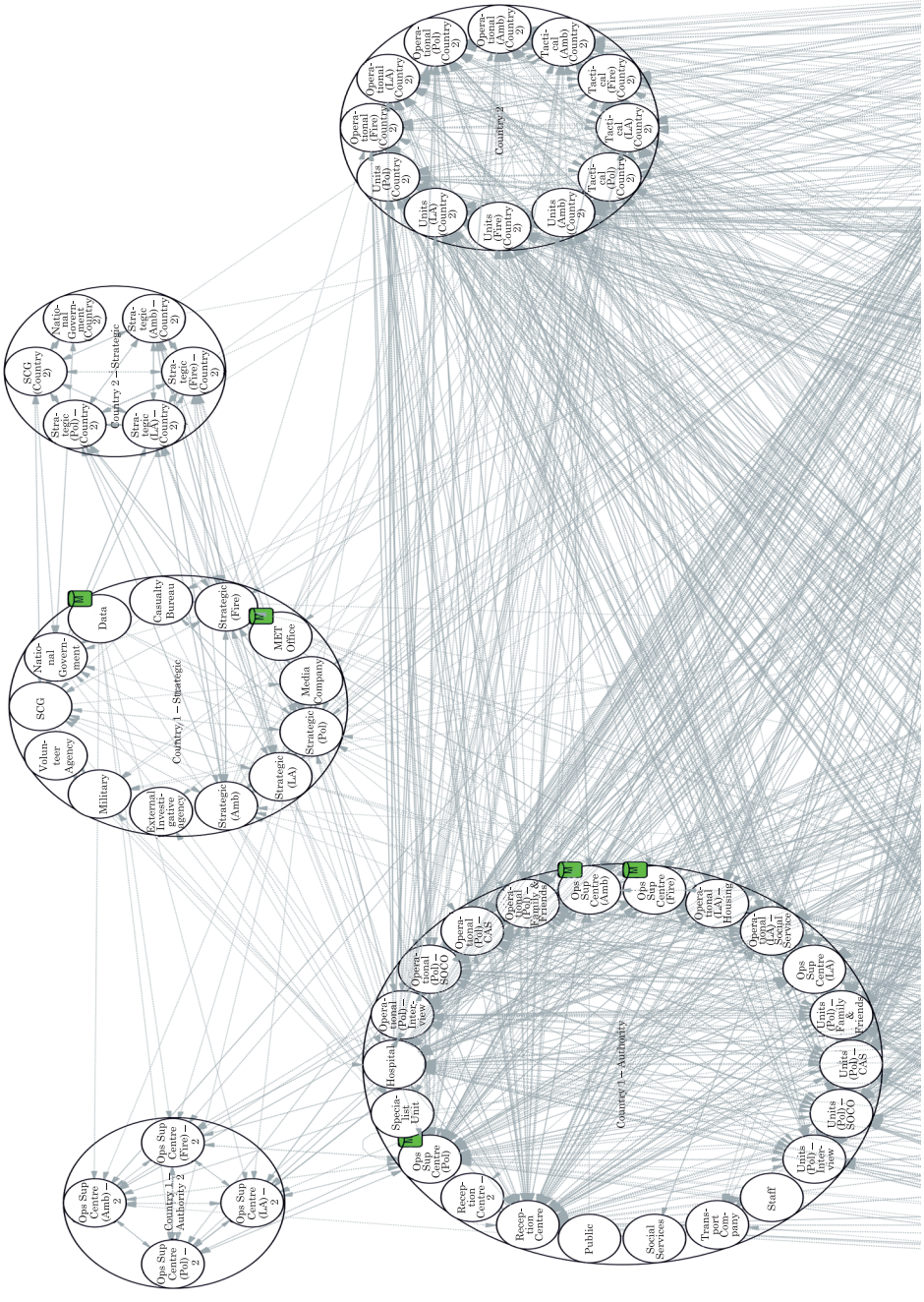
– **Source** & **Destination** (of a piece of information).
– **Information Type** (e.g. voice, message, image).
– **Size** (associated with the Information Type).
– **Timeliness** expressed in the worst case as delivery time.

These criteria were complemented with qualitative data on:

– Criticality.
– Confidentiality.
– Other analysis attributes (e.g. business function).

The complexity of the information exchange is illustrated in Fig. 5, which shows the mapping of IERs to the scenario node location mappings. These location nodes represent a town, a chemical plant, school area, authority areas of different countries, etc. The Fig. 6 presents information flow associated with the scenario and demonstrates co-ordination and liaison with neighbouring country's units and information flows from operational to strategic and fixed infrastructure nodes.

On the other hand, the demand for services – with respect to the agency and command level – have been captured and aggregated. As foreseen, the voice was predominant (for each command level and agency) while the access to the internet was less valuable; those results have confirmed the expectations from interviews. Detailed results are presented in Figure 6.


Country 1 – Authority
Ops Sup Centre (Pol)
Specialist Unit
Hospital
Operational (Pol) – Interview
Operational (Pol) – SOCO
Operational (Pol) – CAS
Operational (Pol) – Family & Friends
Ops Sup Centre (Ambo)
Ops Sup Centre (Fire)
Operational (Fire) – Housing
Operational (LA) – Social Services
Ops Sup Centre (LA)
Units (Pol) – Family & Friends
Units (Pol) – CAS
Units (Pol) – SOCO
Units (Pol) – Interview
Staff
Transport Company
Social Services
Public
Reception Centre
Reception Centre – 2
Country 1 – Strategic
Strategic (Pol)
Strategic (LA)
Strategic (Amb)
Strategic (Fire)
MET Office
Media Company
Casualty Bureau
Data
National Government
SCG
Volunteer Agency
Military
External Investigative agency
Country 2 – Strategic
Strategic (Pol) (Country 2)
Strategic (LA) (Country 2)
Strategic (Fire) (Country 2)
Strategic (Amb) (Country 2)
National Government (Country 2)
SCG (Country 2)
Country 2
Operational (Pol) Country 2
Operational (LA) Country 2
Operational (Fire) Country 2
Operational (Amb) Country 2
Tactical (Pol) Country 2
Tactical (LA) Country 2
Tactical (Fire) Country 2
Tactical (Amb) Country 2
Units (Pol) Country 2
Units (LA) Country 2
Units (Fire) Country 2
Units (Amb) Country 2
Country 1 – Authority 2
Ops Sup Centre (Pol) – 2
Ops Sup Centre (Fire) – 2
Ops Sup Centre (LA) – 2
Ops Sup Centre (Amb) – 2

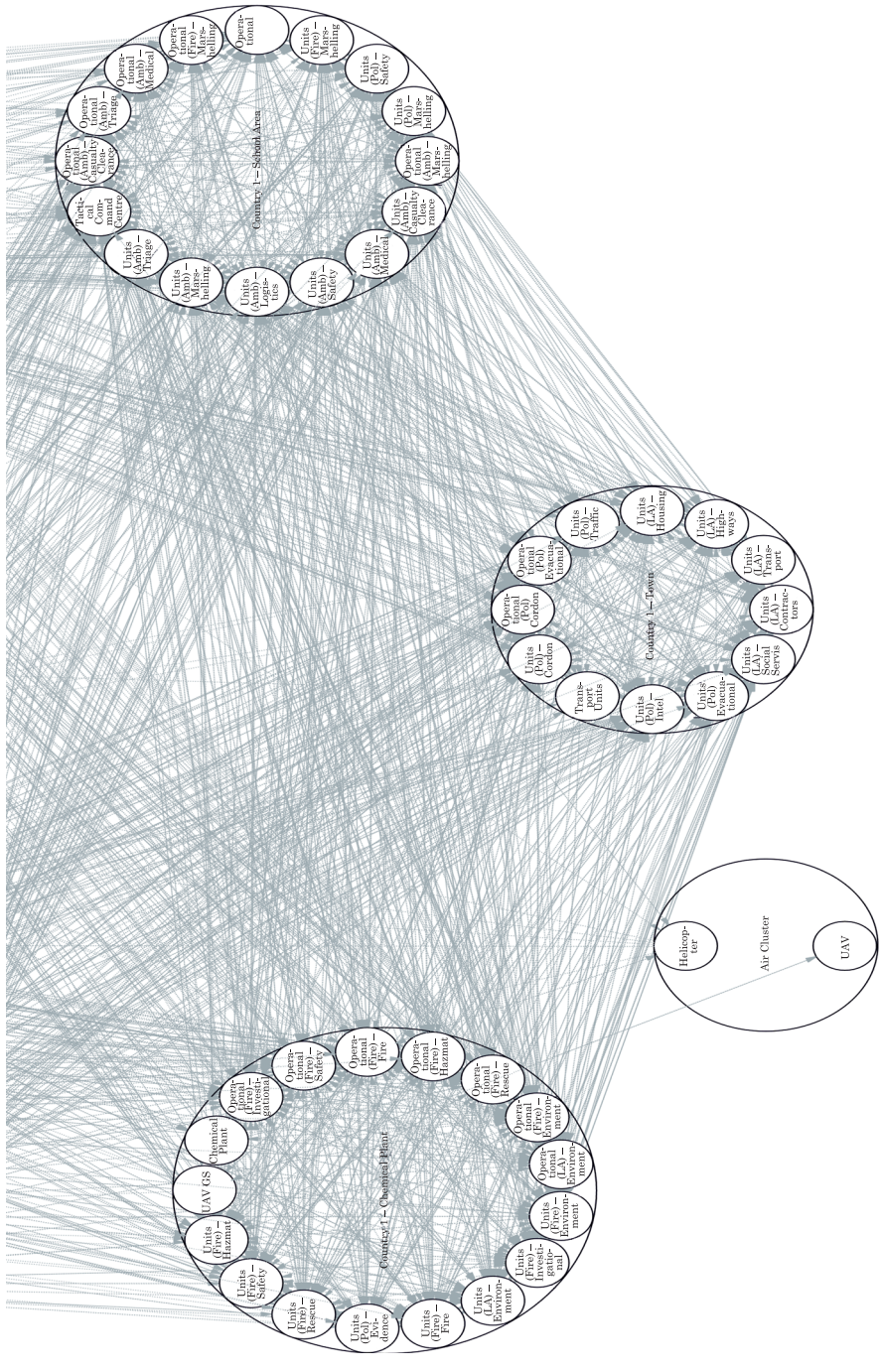


Fig. 5. Information flow between agencies

Source: SECRICOM Information Exchange Requirements 1.0.

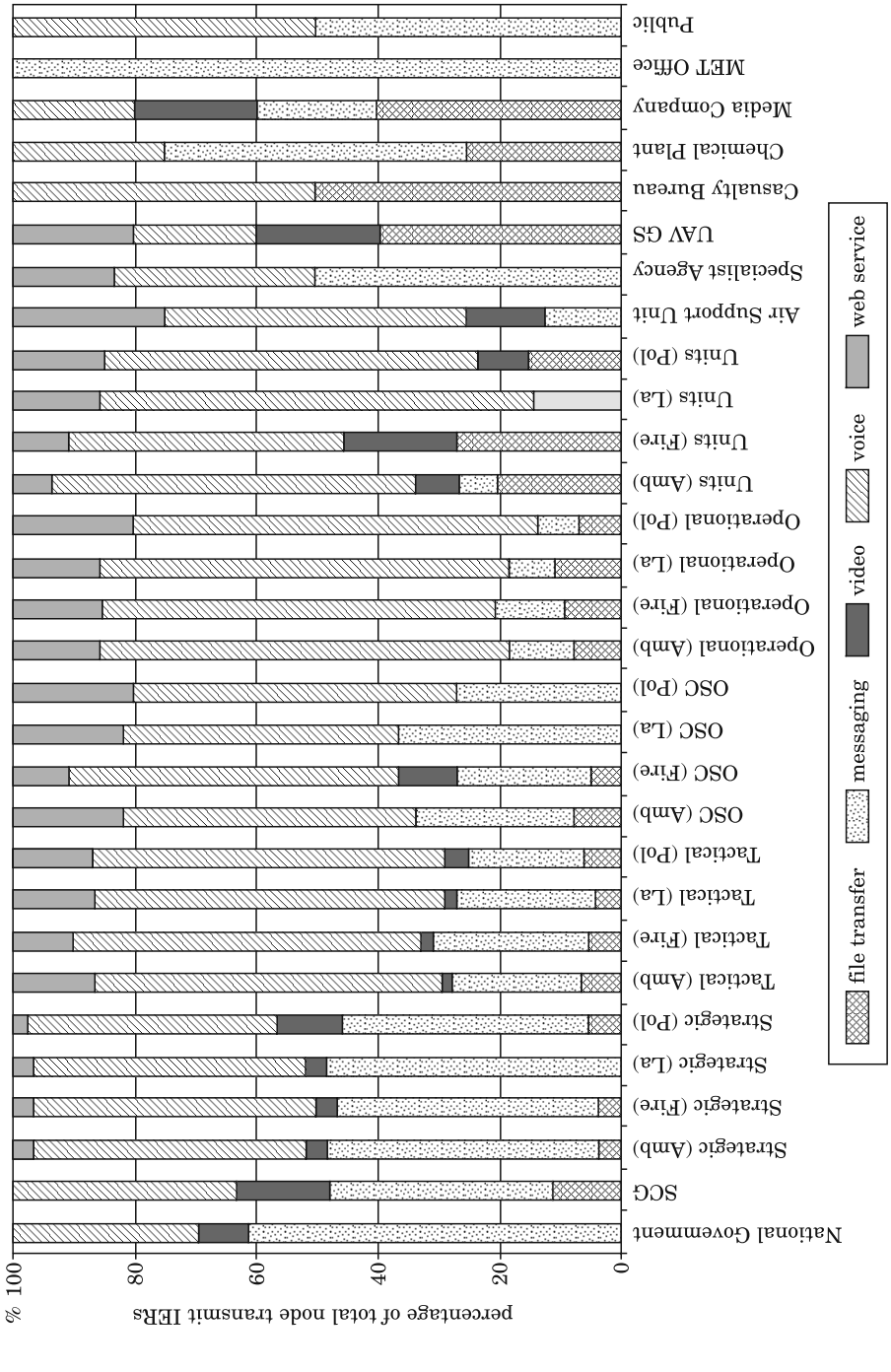


Fig. 6. Total Node transmitting IERs

Source: SECRICOM Information Exchange Requirements 1.0.

During the next step, the IERs were **developed** from the URs **analysed** in the context of a scenario, and used to **model** existing communications architecture and to **identify** which IERs would be supported by the current architecture. Any **unsupported IERs** would tend to indicate a Capability – and therefore an Interoperability – shortfall (see Fig. 7 below).

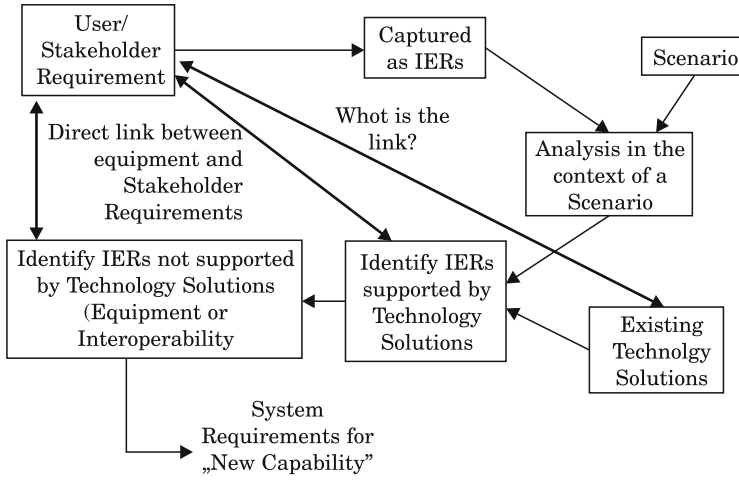


Fig. 7. Capability gap analysis process
Source: SECRICOM Information Exchange Requirements 1.0.

Gap analysis

The purpose of the gap analysis in the SECRICOM project was to find the problems of existing communication technologies when used in crisis situations, and mitigate key capability gaps faced by users of existing systems. The SECRICOM project addressed not only existing capabilities but also new ones. SECRICOM provides value added through finding new requirements for future technology developments. This is achieved at the overlap between existing and future infrastructure and systems, as illustrated in Figure 8.

To perform gap analysis a realistic operational scenario was used, user requirements were formulated and then IERs were extracted from URs.

User requirements were extracted from the following sources:

– Interviews with end-users.

– Scenario-based demonstrations.

IERs provided the communications requirements upon which the technical development would be based – and which would also direct the final demonstration.

The idea was to identify URs that are not met by existing communication systems and mark it as a capability gap. In this way, the capability gaps provide the value added by SECRICOM as they are interpreted as system requirements for technological development.

Additionally, in the SECRICOM the capability gap approach was used as a basis to develop URs and was verified in a demonstration test.

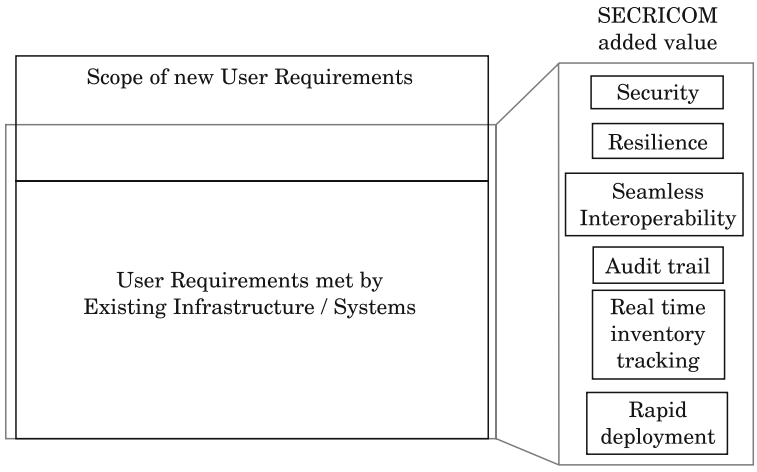


Fig. 8. SECRICOM added value

Source: SECRICOM project.

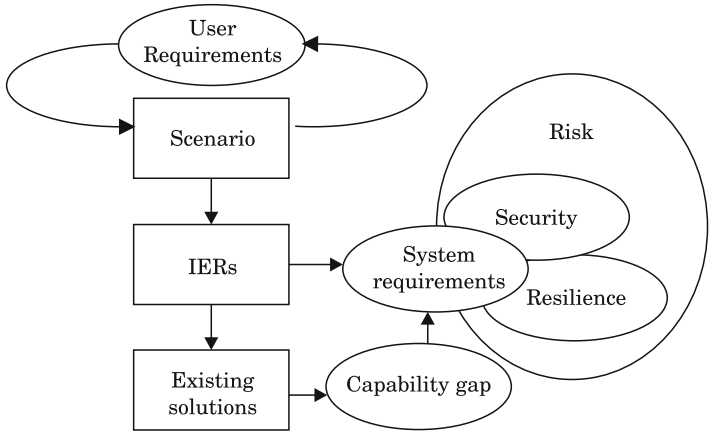


Fig. 9. Requirements within the SECRICOM project

Source: Security requirements user workshop – Report.

In order to demonstrate the significance of the capability gap outcome. A comparison between the SECRICOM User Requirements and current communications systems (e.g.: TETRA, TETRAPOL, WiMAX, CB, GSM/UMTS) capabilities needed to be made. This comparison established the difference / delta between where the capability shortfall exists and where SECRICOM could add value. As it was explained previously, in the SECRICOM project user requirements were created from the scenario through an iterative process. Those URs, on the other hand, were feeding the system requirements. Selection of the appropriated system requirements defined the technology development required. A vignette or mini-scenario, together with the new technology capability, formed the final demonstration. Figure 9 presents the methodology used for acquiring system requirements.

Security requirements

Another aspect that has been discussed through the analysis is security. Security was always an integral part of the project. To correctly address the security requirements, a workshop – dedicated just to security issues – with the user team was conducted. The requirements that emerged are framed around a crisis management structure; the security requirements vary on each of the three levels of command chain. Furthermore, the impact analysis was performed; hence the operational capabilities related with each asset have been established, referring to:

– Saving lives.
– Ability to conduct emergency services.
– Provision of local contingency services.
– Impact on judicial proceedings.
– Impact on foreign relations.

Additionally the security requirements in terms of confidentiality, integrity and availability have been established for the most important services, namely:

– File transfer (documents).
– Messaging (Email, Data/Image).
– Video.
– Voice.
– Access to the Internet.

The outcome of the security assessment was understanding of how important the identified factors are to the users. Bellow the main results achieved by the security assessment are summarised:

– Voice communications at all 3 levels of command, and between agencies, are seen as critical. It requires the **highest level of security** in terms of Confidentiality, Integrity and Availability.

– Messages and file transfer are seen as the **second important**.

– Access to the Internet is the **least valued**.

– Integrity, across all 3 command levels, is seen as a **key requirement** (voice in particular) for all communications assets.

In comparison to Integrity and Availability, Confidentiality is considered a **less important requirement**.

– Availability.

– Voice viewed as **essential**.

– Messaging and file transfer more important than video and web.

The following charts (Fig. 10, Fig. 11, Fig. 12) illustrate the results at strategic, tactical and operational level considering the impact perspective on confidentiality, integrity and availability, for the most dominant services.

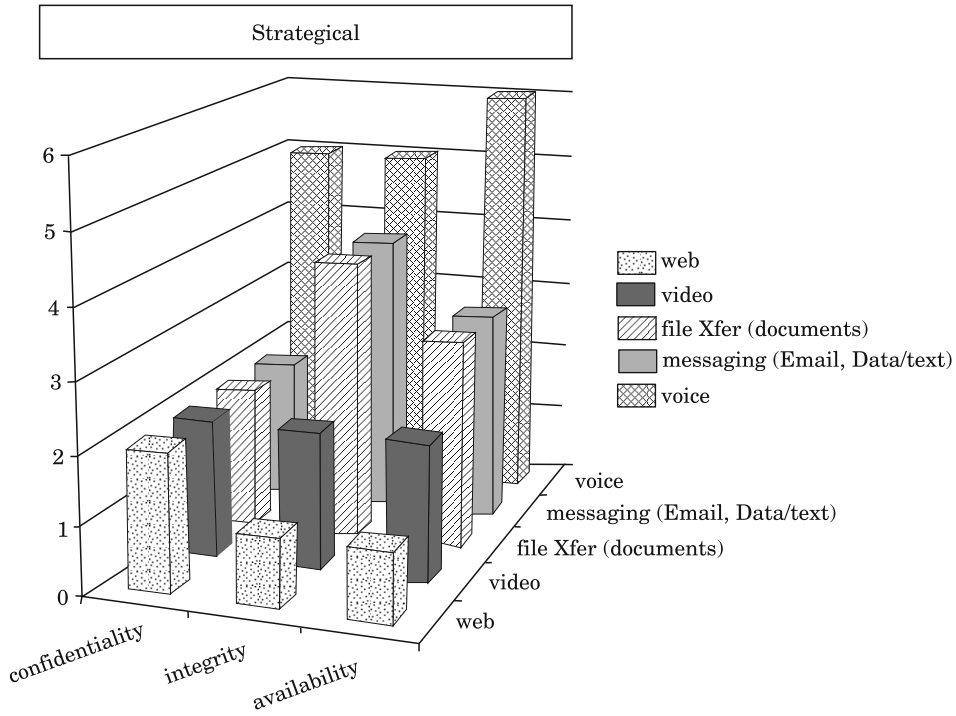


Fig. 10. Security requirements at strategic level
Source: Security requirements user workshop – Report.

The key findings of the IER exercised as a whole are:

– Overall voice is predominant (~ 50%), messaging is next (~ 25%).

– Voice more concentrated at operational level – decreases higher up the command chain.

– Data more concentrated at strategic level – decreases lower down the command chain.

– Specific increased need was identified for image and video capabilities at operational level.

– **Intra**-Agency communications are key at all levels of command.

– **Inter**-Agency communications account for nearly a quarter of all IERs.

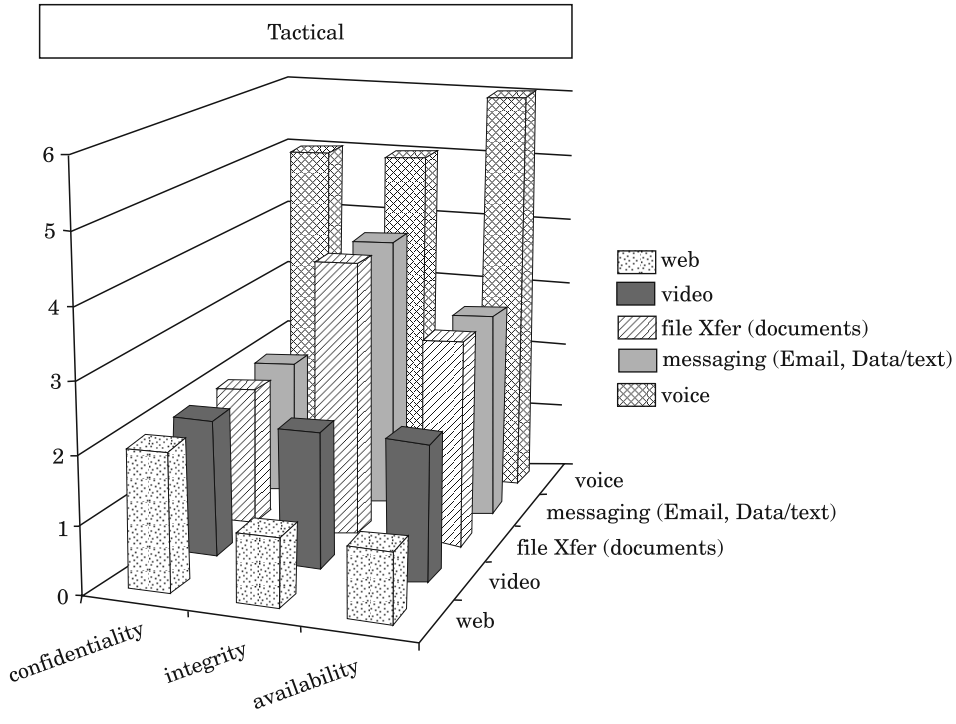


Fig. 11. Security requirements at tactical level
Source: Security requirements user workshop – Report.

– Situational Awareness provides the greatest proportion of IERs (~ 59%).

– Ratio of Command & Control to Situational Awareness distorted due to voice.

– Data versions of the same IER (driven by the need of audit trail).

– Voice remains the most significant IER data type for both Command & Control and Situational Awareness (Situational Awareness demands a greater use of non-voice data types).

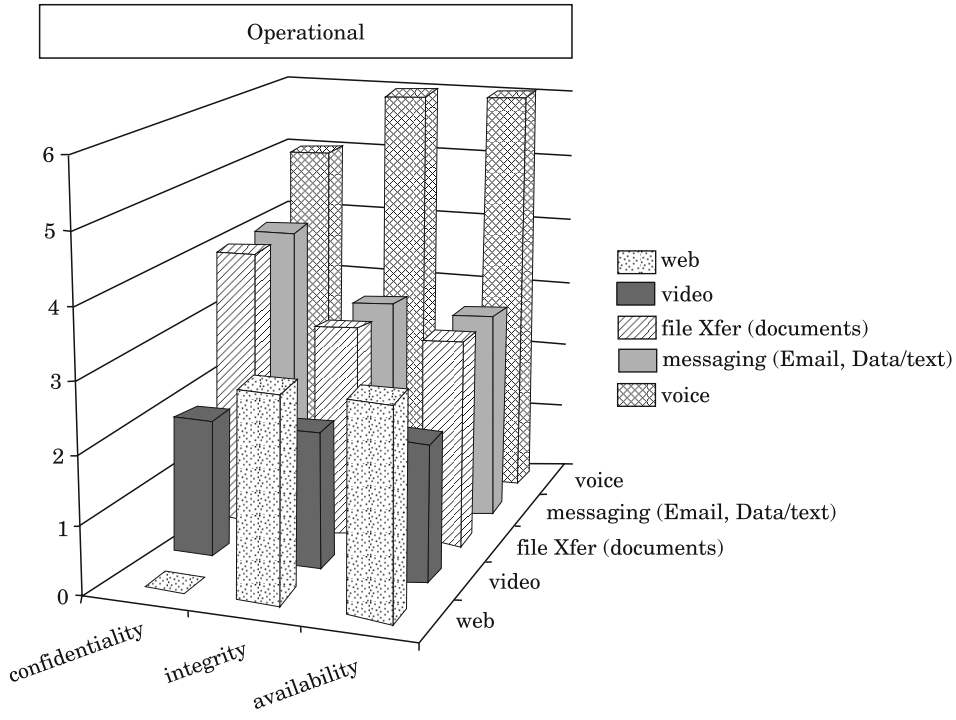


Fig. 12. Security requirements at operational level
Source: Security requirements user workshop – Report.

Conclusions

In this article an approach to elicitation, analysis and validation of user requirements for critical system has been presented. A brief review through most popular approaches to the user requirements have been given, taking into account its use in the SECRICOM project. The system environment (incl. structure, principles and decision making process in crisis management) was analysed and results were reflected in the proposed process.

Afterwards a detailed description of SECRICOM requirements gathering process has been provided. This process is based on three complementary approaches:

- Permanent monitoring of the technical innovations in terms of their adaptation in the area of crisis management, with the particular focus on the communication area.
- Use of scenarios – historical knowledge to develop two types of scenarios that verify the effectiveness of particular features:
  - Generic scenarios,

– Anticipation scenarios (which assume a range of possible outcomes).
– Gap analysis.

This approach combines both retrospective and prediction elements. On top of that, it allows to monitor and proper address important changes in communication domain.

The most important change in crisis management communication is a growing use of ICT systems. Although symptoms of these changes were evident for many years, the current state of telecommunications infrastructure allows to offer a wide range of new services, such as analysis of connections in real-time, video telephony, use of new source of information (e.g. social networks) or dynamic group management.

Finally, the requirements obtained were presented. The results were presented for each command chain level. There was a particular focus on security issues, since they were found critical in crisis management field.

Acknowledgments

This work was funded by the SECRICOM project (EC FP7-SEC-2007 grant 218123).

Translated by AUTHORS

Accepted for print 30.06.2012

References

ABRAN A. 2004. *Guide to the Software Engineering Body of Knowledge*. IEEE Computer Society.
Advertising materials http://www.itti.com.pl/pl/projekty-ue/projekty-trwajace2.html.
SECRICOM D2.2 Crisis management requirements assessment report.
SECRICOM D9.1.1 requirements of the security model.
GOBAN-KLAS T., SIENKIEWICZ P. 1999. *Społeczeństwo informacyjne: Szanse, zagrożenia, wyzwania*. Wydawnictwo Postępu Telekomunikacji, Kraków.
http://ceur-ws.org/Vol-340/paper03.pdf
http://int3.de/res/RUP/RUP_Paper_JohannesPassing.pdf
http://spot.pcc.edu/~lmiddlet/CIS122/coursematerial/Requirements.html
http://www.comp.lancs.ac.uk/computing/resources/IanS/SE7/index.html
HULICKI Z. 1998. *Systemy komunikacji multimedialnej*. Wydawnictwo Postępu Telekomunikacji, Kraków.
Information from the website http://www.secricom.eu/
KOTONYA G., SOMMERVILLE I. 1998. *Requirements Engineering: Processes and Techniques Chichester*. UK: John Wiley and Sons.
Risk management Guide for Information Technology Systems.
SECRICOM Information Exchange Requirements 1.0. R. Edwards, J. Dexter, S. O'Neill – Report, internal SECRICOM deliverable.
Security requirements user workshop – Report, internal SECRICOM deliverable.
WOJCIECHOWICZ W., ZYCH J. 2010. *Kierownicze gry decyzyjne w zarządzaniu kryzysowym*. MAIUS-CULA, Poznań.
WOJCIECHOWICZ W., ZYCH J. 2011. *Koncepcja infrastruktury telekomunikacyjnej o podwyższonej niezawodności*. In: *Bezpieczeństwo współczesnego świata – Informatyka, technika i gospodarka*, Ed. Z. Dziemianko, WSHiU, Poznań.