1 Managing Risk and Safety

The human safety and the surrounding his environment as well as the work sustainability and stability of technogenic and information objects are one of basic and strategic human problems on a way to a world sustainable development. In the present time, the quantity of technogenic dangers and the emergent situations on the globe menacing to a society and environment has considerably increased.

According opinion of a number of scientists, such events as natural disasters, technogenic and information accidents are characterized by growth of their number on 57%, damage growth — on 5,1%, the quantity of victims growth — on 6,1% annually. As is mentioned in the State strategy of sustainable development of the Russian Federation, the same tendency will preserve and increase until 2030.

For the decision of this problem it is necessary to carry out studying and evaluation of the ecological situation, forecasting of the dangerous situation development, to discover and classify the kind of dangers as well as to estimate of risk' level and to define operating effect for prevention of negative consequences from realization of ecological danger.

Every year many collapses happen in the world, which can be divided into three groups: natural, technogenic, and information collapses.

Natural collapses are hurricanes, floods, earthquakes and other acts of nature, which destroy the whole cities and lead to mass deaths of people.

Technogenic collapses are big accidents on industrial and transport objects which have been caused by failure in work of technical systems. Technogenic collapses are accompanied by victims among people and ecological disasters.

Information collapses are collapses, which occur in information computer systems. Mainly they occur because of viruses and other harmful programs.

1.1 The natural collapses

1.1.1 The earthquake on Haiti, January 2010

On 13 January 2010 near the Haiti coast happened an earthquake. Earth tremors were fixed on depth of 10 km in 15 km from capital of Haiti Port-au-Prince. The first and the most powerful tremor was equal to 7 magnitudes according to the Richter scale. After this, within several hours followed eight more earth tremors with magnitude from 5 to 5, 9 [Haritonov, 2010]. After the earthquake in the city the electricity and telecommunication was disconnected and pillages began.

The earthquake destroyed many buildings in Port-au-Prince. It is known that because of disaster at least 72 thousand people were killed. Local authorities do not exclude that during the life-saving works the number of killed people can reach 200 thousand [Haiti, 2010a].

Experts in seismology for many years have been warning the society about the possibility of destructive earthquake on Haiti, and present events did not surprise them. In 2008 five scientists at 18th Caribbean geological conference called the southern half of island Espanola (where Port-au-Prince is located) a zone of "large seismic threat". At that time one of the authors of the report, the senior scientific employee of Institute of geophysics in Texas Paul Mann took notice of the dangerous closeness of Port-au-Prince with the million citizens to a joint of two tectonic plates – North American and Caribbean [Haiti, 2010b].

According to the scientists, earthquake could set free the seismic pressure, which had been saved for 250 years. "This super cataclysm was simply time business", Roger Musson from the British geological service has told [Alekseev, 2010]. Plates moved and huge pressure grew.

It is rather difficult to predict the exact date of similar earth tremors: plates can lie motionlessly for hundreds of years and then unexpectedly start moving.

1.1.2 The snowfall in Saint-Petersburg, December 2009

The snowfall, which occurred in December 2009 (the night from 24th to 25th) in Saint Petersburg, was the strongest of snowfalls that had happened in December for last 130 years. According to hydro meteorological center, the snowfall became the strongest in December since 1881. The thickness of a snow cover exceeded 35 mm [Saint Petersburg, 2009a].

As a result of the snowfall, the traffic in the city streets was very complicated. The average speed of cars practically in all the streets of Petersburg was less than 40 km/h. In many places, the carriageway was narrowed to one line, because roadsides have turned to one continuous snow-drift, and between road-lines of different directions, the dividing line was formed by snow. Many drivers could not park their cars and left them directly on the carriageway, others tried to clear roadsides themselves. It was also difficult to walk on pavements: in many places, they simply had not been cleaned, and people had to go by carriageway [Saint Petersburg, 2009b].

Nevertheless, many scholars of authority claimed, that the snowfall in Saint Petersburg was not an anomaly. The formed in the city streets snow blockages were due to the inability of the city authorities to react operatively to the situation.

Anatoly Grabovsky, the head of the Northwest inter-regional territorial administration of federal service of Russia on hydrometeorology and environment monitoring, has noticed that in "anomalous" days only 15% of the monthly norm dropped out. For comparison: in Vladivostok only in one day the two-month norm dropped out [Grabovsky, 2009].

1.1.3 The earthquake in Italy, April 2009

On April 6th, 2009 in 3:32 a.m. in Italy occurred an earthquake, which power was equal to 6,3 according to the Richter scale. According to National institute of geophysics and volcanology of Italy the earthquake hypocenter was on the depth of 8,8 km and in 5 km from the centre of L'Aquila, that is located in 95 km to the north-east of Rome. Earthquake was both notable in Rome and at the coast of Adriatic Sea in the east of the country.

This earthquake became the most destructive one in Italy for the last 30 years. As a result of it, 300 people were killed, more than 1000 got wounds of different severity level, 29 000 lost their houses [Starzev, 2009].

Besides, because of the earthquake architectural monuments were damaged. In L'Aquile at least 4 temples were partly destroyed: Romance temples (XI-XII centuries) and the Renaissance temples. The castle, constructed in XVI century, in which there is a branch of the Italian National museum, was also damaged. The bell tower of the basilica of Sacred Bernarda fell down; the temple's apse was seriously damaged. In Italian capital, the terms of Karakally suffered from the earthquake [Italy, 2009a].

Joakino Juliani, a famous scientist of seismology in Italy, had predicted a strong earthquake in the central mountain region Abrutso some months before the tragedy. However, nobody had paid attention to his warnings, and even had obliged not to spread the information, which could cause a panic among local population.

The anxiety about the elements started to grow in a small town L'aquila from the middle of January, when the first weak underground tremor had been fixed. Then these tremors continued, but with variable intervals. Then Juliani, using the information about the raised concentration of radon gas around seismically unstable areas, made a conclusion on the future powerful earthquake.

In March, cars with loudspeakers drove around the town and urged the local population to begin evacuation. In police began to arrive many complaints about seismologist's panic distribution, and they caused the anger of mayor. As a result, the scientist had to remove from the Internet all information concerning the forthcoming earthquake. Moreover, on the 31 of March the Service of civil protection and the Committee on prevention of scale risks held special session to calm down the inhabitants of mountain areas. In the statement of its participants, it was said that underground tremors were normal for seismically active areas, such as L'Aquila. In addition, it was told that there were no occasions for anxiety, and that the supervision in these areas would be continued "just in case" [Italy, 2009b].

1.1.4 Tornado Katrina, August 2005

The tornado Katrina is the most destructive tornado in the history of the USA. The tornado reached the southeast coast of the USA on August 29, 2005. In the zone of its action were the following areas: Louisiana, the south and the centre of Mississippi, the south of Alabama, the West of Georgia, the West and the south of Florida. The speed of the wind reached 280 km/h.

The city of New Orleans suffered the most in those days. It was destroyed for 80%. The tornado Katrina killed almost 2000 human lives and brought an economic damage at a rate of 125 billion dollars.

The tornado had a very bad influence on the oil business. On September 2, the representative of the American Institute of Oil, Tim Sampson, established that Katrina destroyed 58 oil platforms and boring installations in the Gulf of Mexico, 30 of them were lost. Since the first days of tornado, the oil extraction in the Gulf of Mexico was reduced for 95%, and its price began to grow [Forex, 2005].

Tornado is a rotating warm air stream. Te speed of rotation can reach 1000 meters per second. Rarefied rain clouds and a powerful vertical stream of air between a cloud and an earth surface are necessary for its formation. Experts of meteorology consider that the most destructive tornados, which have become very frequent for last decades, are connected with global warming of a climate.

As the temperature in atmosphere is constantly growing, we should expect very strong tornados in the near future.

Experts in tornados have been repeating for many years that consequences of a blow of a strong tornado on New Orleans can be catastrophic. Two experts warned about serious danger to a city 6 weeks before an arrival of Katrina, but nobody trusted in their predictions in July 2005.

The atmospheric system, which turned into the tornado Katrina, arose on August 23 in the form of area of the lowered pressure at the coast of the Bahamas. This natural phenomenon not necessarily leads to tornado formation – for this purpose is necessary a much bigger quantity of energy. Within 6 days in 1 500 km from the coast the tropical zone of the lowered pressure slowly, but steadily gained its strength. At last, on August 29 it turned to a mature tornado in width more than 800 km. The speed of the wind was 280 km/h [Katrina, 2005].

The killing force of tornado is influenced by 4 basic elements.

The first element is the speed of the wind. During the tornado Katrina the speed of the wind reached 225 km/h, therefore it was given the fourth category on a scale of Saffira-Simpsona. For comparison: tornados of the first category have speed 120 km/h, the fifth category – 320 km/h.

The next element is the size of tornado. The more it is, the more its destructive force is. The zone of the destructions, caused by Katrina, was stretched on 160 km along the coast of the Gulf of Mexico and on 160 km deep into the continent. It is a territory with the population of 10 million inhabitants.

The third element is torrential rains. Hurricanes accumulate billion liters of water over the sea and bring it down on the earth in the form of downpours.

Besides, the tornado Katrina, as well as the majority of other tornados, had one more terrible weapon – the sea level abruptly rose and fell down upon the earth, sweeping away everything on its way. This phenomenon is called "stormy water tide". During the tornado Katrina in a resort town Biloxi the absolute record of stormy waters was set: more than 9 meters [Katrina, 2005].

These 4 elements are peculiar to the majority of tornados. They become the reason of the basic destructions and deaths of people in the zone of natural calamity. However, the tornado Katrina was not the champion in each of these categories, the destructions, caused by it, were apocalyptical.

1.1.5 The volcano Eyjafjallajokull eruption, April 2010

Starting on April 14, 2010, the volcano Eyjafjallajokull (Iceland) eruption rose in the air huge clubs of ash and steam. The last time the volcano woke up in 1821, and its eruption lasted for two years.

According to the head of the Meteorological Office of Iceland, Robert Matthew, on April 14 there were two ejections of volcanic lava, the second one was particularly big (Figure 1). As the magma immediately met with the ice the dirty jets of boiling water with stones and ash were ejected out of the crater [Newsru, 2010].

The airspace in Western Europe was blocked; flights to dozen countries were cancelled, because volcanic ash can damage plane engines.

"Firstly it is highly abrasive and can scour and damage moving parts. Secondly, if it enters a jet engine the intense heat of the engine can fuse it to the interior of the engine with a caking of hot glass, which ultimately can cause the engine to cut out completely", explained Dr. Mike Branney, senior lecturer in volcanology, University of Leicester [BBC, 2010].

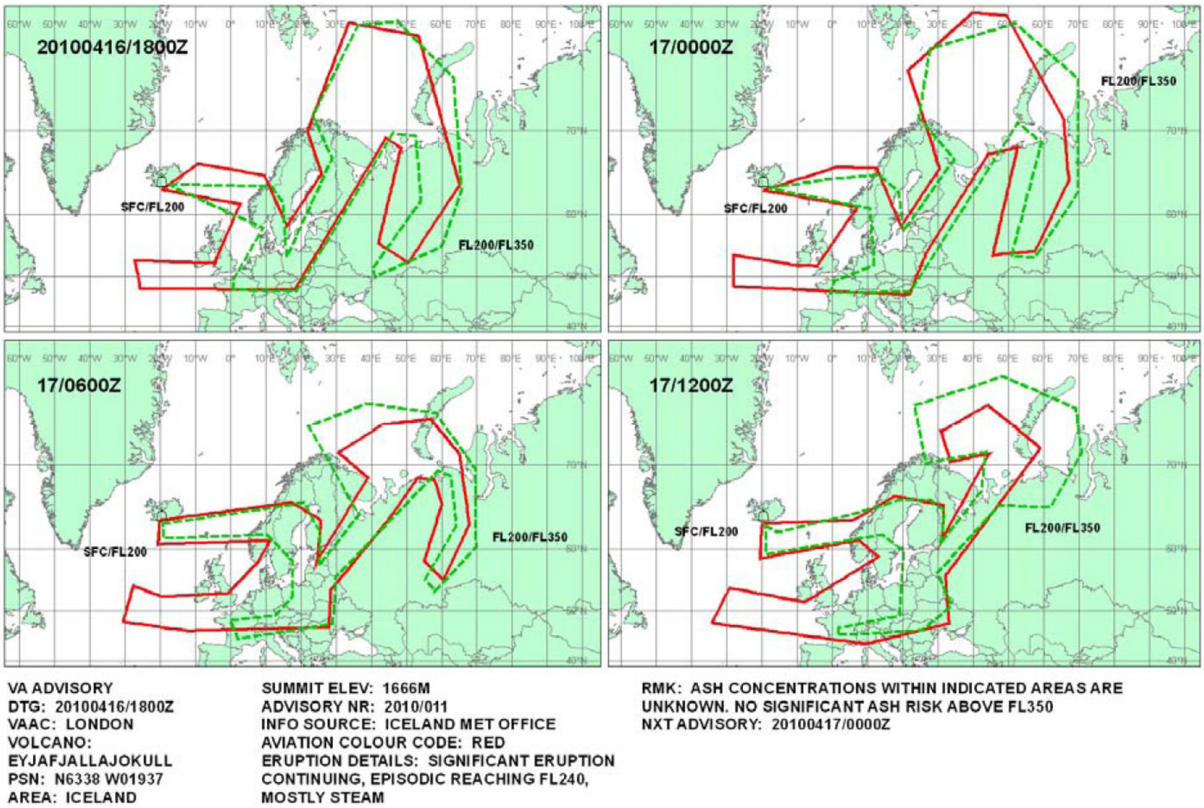


Figure 1. Ash concentration on April 17, 2010 [Metoffice, 2010]

The economic losses were extremely high. Airlines were losing about $200 million every day because of the shutdown of many European airports. In addition, trade goods transported by air were unable to reach their markets, so their prices grew, too [Kaufman, 2010].

According to the European flight control agency, about 500 flights in Europe were cancelled and about 20,000 delayed because of the ash cloud produced by the volcano in Island. The worst situation was in the airports in Great Britain, Spain, Portugal, and Austria [Ruvr, 2010].

Traffic jams once again raised the issue of high fragmentation of the European airspace. Because of this in Europe call for the adoption of the program "open sky", that will establish a common aviation area of the continent. The project should enter into force on January 1, 2012.

1.2 The technogenic collapses

1.2.1 Train collision in Belgium, February 2010

On February 15, 2010, two passenger trains collided near Brussels. Collision occurred in 8:30 a.m. local time.

The force of the stroke was so powerful, that the first carriages of trains reared and damaged the electric lines located at three-meter height over the railways. Some carriages were derailed, one of them turned over [Belgium, 2010a].

The incident picture looks as follows. The six-carriage train, going from Leuven in Braine-le-Comte, changed the track at station Buizingen and passed to the track number 96 of Belgian railways. Because of a strong snowfall, the engine driver did not notice the red signal of a semaphore. The track in that zone is equipped with the system of emergency braking, which does not allow a train to pass on a red light, but this train was not equipped properly, so it could not activate the system.

At the same time overcrowded with passengers 12-carriages express Kevren-Liege, going to Brussels, on full speed went on the same 96th track. The engine driver got the permission from the controller, who did not suspect that there was another train on this track.

Therefore, the human factor and technical insufficiency of security systems became the main version of the investigation at a preliminary stage.

Because of the accident, 18 people were killed, nearby 125 got wounds of various severity levels]. The railway traffic on the two main lines of the western Belgium was stopped: Brussels-Mons and Brussels-Turne, and the railway traffic of the international high-speed trains "Talis" and "Evrostar" was also stopped [Belgium, 2010b].

1.2.2 The accident at the Sayan-Shushenskaya hydro electrical station

Industrial technological disaster at the Sayan-Shushenskaya power plant occurred Aug. 17, 2009. 75 people died because of the accident. Equipment and premises of the station was severely damaged. Workstation electricity production has been suspended.

Consequences of the accident affected the ecological environment of water area, adjacent to the HPP. The accident has had a negative impact on the environment: oil bath lubrication of thrust bearings of hydraulic units from the destroyed management systems guide vanes and transformers fell into the river and formed a spot spread over 130 km. The total volume of oil leakages from the equipment of the station was 436.5 m^3, of which approximately 45 m^3 predominantly turbine oil has fell into a river.

Figure 2. Engine room Sayano-Shushenskaya power plant before (left) and after (right) the accident (www.lhp.rushydro.ru)

Because of the accident, the main hydropower number 2 and main hydraulic were destroyed. There are broken generators in hydro number 7 and number 9. Other hydraulic units were received substantial damage.

The walls and roof of the machine hall in the area of hydro-number 2, 3, 4 were destroyed too. Other equipment of the station – transformers, cranes, elevators, and electrical equipment was received varying degrees of damage. It was located in the engine room and near him. Total losses associated with damage to the equipment valued at 7 billion rubles.

This accident is the largest catastrophe in the history of hydropower projects in Russia and one of the most significant in the history of world hydropower. Nevertheless, the assessment of the consequences of the expert and political community is ambiguous. The accident caused a major impact on society, becoming one of the most talked about in the media events of 2009.

As a result of the investigation the direct cause of the accident was called fatigue failure studs cover attachment hydraulic turbines, which led to its disruption and flooding the engine room station (Figure 2).

It was found that it was not properly organized permanent control of technical condition of equipment operational and maintenance personnel (which should provide instruction on operation of Sayan-Shushenskaya HES approved by the chief engineer of HES 18.05.2009 g.). The main cause of the accident was the failure of taking prompt measures to stop the second hydraulic unit and determine the causes of vibration [GES, 2009].

1.2.3 The explosion at the chemical plant in Toulouse, France

At a chemical plant in Toulouse (France) on 21 September 2001 have occurred explosions, whose consequences are still considered like the largest industrial disaster in recent years.

The cause of the explosion was the violation of safety at the facility.

Thousands of homes and many institutions were destroyed, including 79 schools, 11 secondary schools, 26 colleges, 2 university, 184 kindergartens, 27 thousand apartments, 40 thousand people have become homeless, and 134 companies have stopped their work.

Government and insurance companies received 100 thousand claims for damages. The total damage amounted to 3 billion Euros. 30 people have died in the city, the total number of wounded has exceeded more than 3,5 thousand.

1.3 The information collapses

1.3.1 Sberbank, December 2009

On the 26th and 27th of December, 2009 the clients of Sberbank, who were paying for the goods and services with credit cards, were in an unpleasant situation: the money was removed from their accounts two times.

The representatives of Sberbank declared that the reason of the failure were technical defects at counterparts. The bank Press-service has confirmed "the doubling of some transactions, made on the 26th and 27th of December on purchases of clients of the bank in the networks, acquiring in which was carried out not by Sberbank". According to the bank, the failure influenced on less than 0,5% of the transactions served in the system of Sberbank every day [Gerashenko, 2009].

"Within several hours all doubled transactions will be searched, and the rests on the accounts of clients will be restored", was told in the Sberbank's communiqué.

But there is an opinion that these problems were not at the counterparts, but in the bank. For example, there could be a hardware failure. "The Sberbank has its own processing of cards, it means that the problems are somewhere in its structure", — tells a source in the sphere of bankcards service [Gerashenko, 2009].

1.3.2 Citibank, Summer 2009

On December 22, 2009 The Wall Street Journal, citing unnamed officials in the U.S. government announced the kidnapping of tens of millions of dollars from the accounts of depositors of the Citibank [Churumova, 2009]. The attack was noticed by the U.S. secret services in the summer of 2009, when it was discovered a suspicious traffic coming from Internet addresses previously used by the hacker group, Russian Business Network. It is quite possible that the kidnapping of money took place long before when he was tracked down by the suspect traffic. Moreover, as evidence of the involvement of Russian hackers for the crimes of U.S. investigators, allege that the hacking program Black Energy was used.

According to Secure Works expert Joe Stewart, Black Energy has written in Russia by hacker Crash.

This program infects the computer network and allows an attacker to perform actions using the resources of the infected computer. With its help, Georgian government portals and Estonian websites have blocked in 2007-2008 [RBS, 2009].

However, Black Energy sells online for $ 40, says Jose Nahariya, manager of Arbor Networks. According to director of Digital Stakeout Adam Mikruta, a software package YES Exploit System was selling for 700$ in April 2009 in the Internet. It allows you to steal the parameters of access to the bank accounts. It includes Black Energy also.

According to Joe Stewart, in summer Cr4sh has released a new version of the program, through which you can steal usernames and passwords for access to the bank servers [Churumova, 2009].

Citigroup denies any knowledge of the attack and the theft of a substantial amount of the bank. "We have not had any leaks in the system and no losses, both by consumers and by banks. Any suggestion that the FBI is working on a matter of Citigroup, associated with the theft of tens of millions of dollars, are not true", said Joe Petro, Managing Director of the Department of Security, Citigroup [Truhanov, 2009].

Russian experts also confirmed that Citibank was not hacking. "The incident is connected with the attack on the trade network 7-eleven, which occurred in the summer of 2008, Alexander commented to the guests, a global center of research from Kaspersky Lab. This trading network uses ATM Citibank.

Bank was providing their work from a technical point of view, although they were the property of 7-eleven. Hackers managed to access the payment system 7-eleven through vulnerability. They did not use malicious programs.

Then they worked with the so-called "loot" – people who received either ready-made counterfeit cards or instructions how to make them. After that drops, using these credit cards, withdraw money from ATMs" [Truhanov, 2009].

Robert Blanchard had trouble accessing account. It is an indirect proof that the hacking took place. He is co-owner of Bridge Metal Industries. At night, July 6, 2009, he tried over the Internet to gain access to the bank account of the company, but was unable to do so. Then he phoned to the bank, and there he was told that he would get a new password by e-mail. But even with the new password Blanchard was unable to gain access. By that time, hackers have been transferred from his account $ 1 million in banks in Latvia and Ukraine. As a result, Citibank returned most of the stolen Blanchard amount [Churumova, 2009].

It is worth mentioning that on December 22, the day with a message The Wall Street Journal, the White House decided to declare the name of "CyberKing" – the official, who will be responsible for cyber security departments. It became Howard Schmidt, who was cyber-advisor in the previous administration [Dubinskaya, 2009].

1.3.3 RBS WorldPay, November 2009

RBS WorldPay is organization that provides support payment transactions for the Royal Bank of Scotland (RBS) in the United States.

Hacking was detected in server of RBS In November 2009, located in Atlanta.

According to investigators, intruders broke into the bank's security system and have access to data of cards that receives the salary of bank customers. This information was passed by crackers accomplices, who cashed more than $ 9 million money with the help of charts around the world. Money was withdrawn in the U.S., Russia, Estonia, Ukraine, Italy, Japan [RBS, 2009].

The report of the Ministry of Justice of the United States called the names of criminals, these are Sergei Tsurikov from Tallinn, Victor Pleschuk from St. Petersburg, Oleg Kovelin from Chisinau, as well as people called in investigative materials "hacker 3". Living in Tallinn, Igor Grudizhev, Ronald Tsoi, Evelyn Choi, and Michael Yevgenov also accused of fraud with bankcards. 3 hackers could face up to 20 years in prison. In addition, they will have to pay compensation in the amount of $ 9.4 million. Other members of the group could receive up to 15 years in prison and a fine of $ 250000 [RH, 2009].

1.3.4 Spain, Summer 2009

In autumn 2009, the holders of cards of many banks have found their cards blocked. In most cases, operators of banks explained that the cards should be released again, as they have been compromised. Some customers have been informed that there were attempts of unauthorized transactions on their cards.

Most owners of blocked cards were in Spain in the summer or in September, where they used the cards [Spain, 2010].

Experts suggest that there was a hacking of servers, where information was stored on the cards. The Central Commission of credit cards in Germany called cards review like preventive measure, assuring cardholders that all potential victims will receive appropriate notice and in any case would not lose their money [Germany, 2009]. "Banks have been notified of the payment systems Visa and MasterCard (the latest reported first), the mass compromise of plastic cards (namely, their requisites: № cards, validity, etc.) used in Spain during the period January-September 2009 year" told the head of the interaction of "Alfa-Bank" Alexei Golenishchev [Jogova, 2010].

1.3.5 The service of state incomes of Latvia, February 2010

In 2000, the Service of state incomes of Latvia introduced the electronic declaring system (EDS) to simplify procedures of the report on the paid taxes by physical and juridical persons. Tax department counted on this IT-project, allocating for its realization the essential sums of money, and widely advertised it. It was especially underlined that all operations made in the system were safe: each document had its own password and SSL protocol was used during the transmission of the document [Kazakov, 2010].

But in February 2010 in the security system of the EDS was found a vulnerability through which for three months unknown persons have stolen 7,4 million documents (120 Gb) [Latvia, 2010a]. The information not only about finance of the state officials, but also about private persons and enterprises was stolen from system.

The group, called "National army of the 4th Atmody" (4ATA), has informed about the leak. As members of 4ATA said, last spring they found out about the existence of defects in the security safety with which help it was possible to get access to the EDS. This information one of the developers of the EDS told the members of 4ATA. He said that they had left the "hole" in the system, because a person of the high rank from the tax service had ordered them to do so. The "hole" was very simple and everyone could use it for all this time. Vulnerability allowed download documents by user without authorization, only the address and the number of document were needed [Latvia, 2010a].

It is necessary to underline that this vulnerability has existed for 10 years, as 4ATA claims.

From the point of view of potential harm, it is the greatest leak, which has ever happened in Latvia.

"Present or former leading persons of the Service of state incomes, guilty of the scale leak, will be punished", the minister of Finance Ejnars Repshe declared on February 15 [Latvia, 2010b].

1.4 Prediction of natural collapses

Earthquake early warning can provide a few seconds to tens of seconds warning prior to ground shaking during an earthquake. Earthquake early warning systems are currently operational in Mexico, Taiwan and Japan but not in the United States.

EalarmS, short for Earthquake Alarms Systems, is a methodology designed to provide warnings in California and other earthquake prone regions around the world. The warning messages provided by EalarmS can be used to reduce the damage, costs, and casualties in an earthquake [EalarmS, 2010].

EalarmS takes the form of a suite of algorithms designed to rapidly detect the initiation of an earthquake, determine the size (magnitude) and location of the event, predict the peak ground motion expected in the region around the event, and issue a warning to people in locations that may expect significant ground motion. The algorithms use data from regional broadband seismic networks (Figure 3).

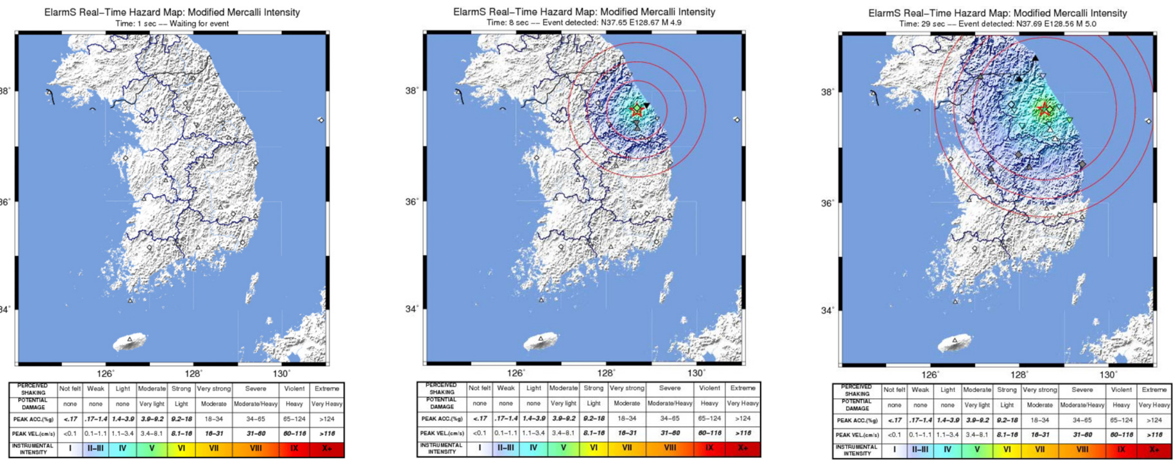
ElarmS is currently being tested by the CISN as part of the real time seismic system in California. This pre-prototype test will allow assessment of the likely timeliness and accuracy of warnings if early warning is implemented for general use in California. ElarmS has also been tested offline using data from Japan, Taiwan, Italy, Alaska, the Pacific Northwest, and California.

Earthquake early warning systems have been expanding rapidly around the world. There are currently warning systems in Japan, Taiwan, Mexico, Turkey and Romania

We need earthquake early warning because:

- current earthquake mitigation strategies focus on long-term ground shaking forecasts that can be used in building design and rapid post-event notification used for emergency response;
- early warning systems allow for short-term mitigation including slowing and stopping of transportation systems, switching industrial and utility systems to a safe mode, and taking personal protective measures;
- early warning would reduce the number of casualties and the cost of earthquakes in California.

Feasibility studies of the ElarmS methodology show that the amount of warning time would range from a few seconds to a few tens of seconds depending on your distance from the epicenter of the earthquake. This is enough time to slow and stop transportation such as trains, taxiing planes and cars entering bridges and tunnels; to move away from dangerous machines or chemicals at work, and take cover under a desk; to automatically shut down and isolate industrial systems. Taking these actions before shaking starts can reduce damage and casualties during an earthquake. It can also prevent cascading failures in the aftermath of an event. For example, isolating utilities before shaking can reduce the number of fire initiations.



(a) *(b)* *(c)*

Figure 3. Earthquake (a) not observed; (b) discovered; (c) 30th second after the first jolt (the red lines show the region of wave propagation)

Seismologists across California are currently planning real-time testing of earthquake early warning across the state. We want to hear from companies, institutions, government agencies, and individuals about how a few seconds to a few tens of seconds warning could be used to reduce the casualties and damage caused by an earthquake in the state.

AlertMaps are ElarmS 'prediction of the coming ground shaking. AlertMaps are updated every second as more information is incorporated into the ElarmS predictions. As time progresses and the ground, shaking spreads across a region the initially predictive AlertMaps evolve into a ShakeMap, which is a map of the observed peak ground shaking. You can view the AlertMaps as an animation or look at individual frames.

1.5 Rapid multi-sensor system for effective risk analyses

An international consortium of specialists from the Netherlands, Russia, Bulgaria, United States, and Australia has developed and demonstrated a new airborne multi-sensor system that is ready for implementation in two major areas of application, related to the Common Agriculture Policy (CAP): control of the Good Agriculture Environment Conditions (GAEC) and the update of the Land Parcel Identification System (LPIS) [Haarbrink et al, 2007]. The airborne multi-sensor system consists of several cameras including a soil moisture scanner for (underground) water and drought mapping, a thermal infrared camera for ground temperature data, a lidar scanner for elevation models, vegetation mapping, and deformation detection, and a digital photo camera for visual and near infrared imagery of the project area. All sensors are mounted on board one single light aircraft and are operated simultaneously to produce a wide range of critical information that is then processed into an Information Monitoring System (IMS). The international team has demonstrated the benefits of the system in a show case project in Bulgaria in the summer of 2007.

The project was successfully performed by MIRAMAP, a private company from the Netherlands that was founded at the European Space Incubator (ESI) initiative of the ESA Technology Transfer & Promotion (TTP) office. The TTP office is contributing to the capitalization of space-based technology and knowledge for the benefit of Europe's economy and science.

The MIRAMAP sensor suite simultaneously collects high accuracy soil moisture data, ground temperature data, digital elevation data, and ortho-photos. It consists of three microwave sensors in X-band, C-band, and L-band that are all GNSS integrated, a thermal infrared camera, a lidar scanner, and a digital photo camera. Table 1 lists the specifications of each different sensor and specific use.

Table 1. MIRAMAP Multi-Sensor Specifications

Sensor	Wavelength	Specs	Use
Passive Microwave Scanner	Microwave 2, 5, 21 cm	5-m GSD, 0.15 K precision	(Sub)surface detection of wet and dry areas
Thermal Camera	LW Infrared 7.5-13 micron	3-m GSD, 0.1° C precision	Surface Temperature
Lidar Scanner (Laserscanner)	SW Infrared 1064 nm	2-m GSD, 0.10 m precision	Elevation Model, Hydrological Model, Deformations
Digital Photo Camera	Visible 0.4-0.7 micron	10-cm GSD, Subpixel precision	Detailed Visible Interpretation, Cartography

The platform on which these instruments are flown is a reliable and safe twin Aero Commander (Figure 4). The aircraft is specially modified to carry simultaneously this range of instruments. The capability to measure such a comprehensive range of remotely sensed parameters from a single low-cost airborne platform is unique worldwide.

As for the soil moisture products, the X-band and C-band sensor makes a conical scan at constant incidence angle over a wide swath, while the L-band sensor for underground soil moisture mapping makes a twin-beam oscillating scan (Figure 5). The small instrument sizes and weights enable use of a low-cost light aircraft as the observing platform, providing decision makers with a new affordable tool.

Through both laboratory and field experiments it has been documented that the passive microwave radiometers with internal calibration, and the processing/retrieval algorithms from the Institute of Radio-engineering and Electronics (IRE) of the Russian Academy of Sciences (RAS) and Radio Corporation VEGA, are feasible to determine several soil, water and vegetation related environmental parameters and conditions. These are soil moisture content, depth to shallow water table, buried metal objects under shallow dry ground, contours of water seepage through hydro technical constructions (levees and dams), sliding zones, plant biomass above wet soil or water surfaces, temperature changes, oil slicks, salt and pollutant concentration in water areas, on-ground snow melting and ice on roads and runways.

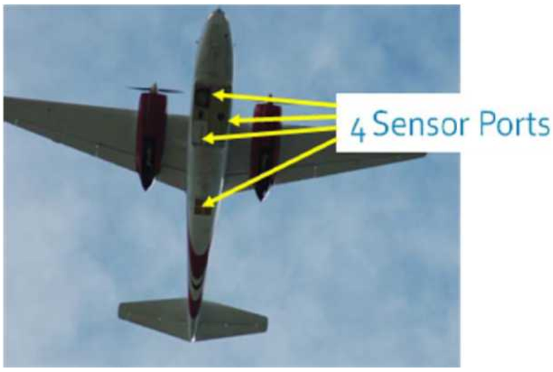


Figure 4. MIRAMAP multi-sensor aircraft

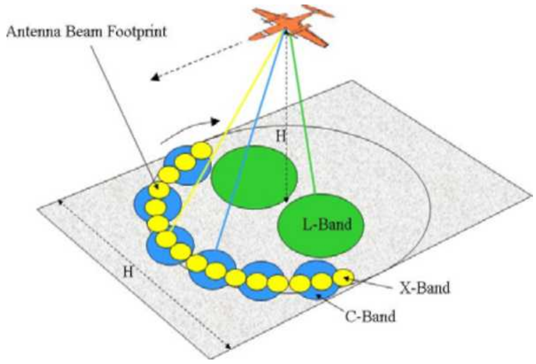


Figure 5. MIRAMAP soil moisture scanner

Simultaneously collected multi-sensor data from the air offer a high social-economic relevance. The approach brings government managers and decision makers the following benefits:

– *rapid*: Large areas can be monitored in a short time frame. The quick availability of information can also be of advantage to minimize the impact of disasters, or to prevent disasters. Adequate and rapid response in the first hours of an (pending) emergency situation is of great importance. Many data can also be collected at night;
– *effective*: Simultaneous acquisition of remote sensing data is a very effective tool to monitor water barriers and coastal zones. Detailed data and flexible deployment on a single platform enables water managers and decision makers to take adequate action, and therefore spend their financial resources effectively;
– *accurate*: A complete and detailed view of possible failure locations is given. The main failure indicators of water barriers and coastal zones are water seepage, dry areas, deformations, and vegetation quality. The results can be easily imported and combined with existing geo-information;
– *safe*: The measurements are collected from the air, so field inspection specialists are not faced with potentially dangerous situations, such as rising water.

Airborne multi-sensor data was collected over two selected areas in Bulgaria – river Rusenski Lom and dams at village Nikolovo – near town Ruse, and additional areas over river Danube, river Yantra, and a forest fire between July 30 and August 2, 2007. The project locations are shown in Figure 6. Unique information was received related to:

– land surface cover, including true ortho-photo at 10-cm ground sample distance, ground temperature data at 0.1 degrees precision, and relief features at 2-m grid and 15-cm vertical precision of terrain impacting moisture parameters;
– surface soil moisture, dry conditions 0.05 to 0.10 m^3/m^3 and saturation up to 0.35 m^3/m^3;
– underground soil moisture reached 0.35 m^3/m^3 in the condition of saturation;
– revealing over-moistened zones near water barriers.

Microwave surface moisture related data revealed over moistening in the areas near the Yantra River outflow zone, which is indicated with red arrows in Figure 7. Water seepage of Danube River through the dike or in land surface depression located in these spots could be reason of this phenomenon.

All different datasets (soil moisture maps, ground temperature data, digital elevation data, and ortho-photos) were processed and delivered to the product specs listed in Table 1 in UTM35 coordinates, so that all data can be quickly combined with existing datasets such as digital topographic maps and satellite imagery.

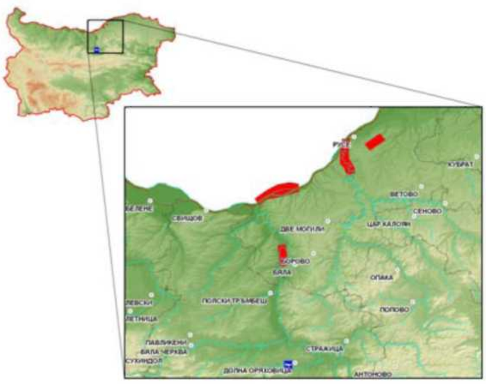


Figure 6. Project locations in Bulgaria

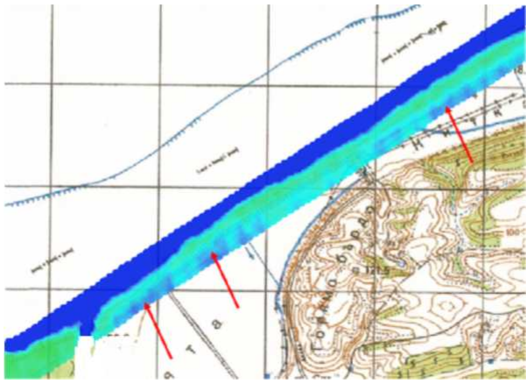


Figure 7. Water seepage at Danube river

During the project weather changed rapidly from dry to very wet condition, so that unique information was received related to soil moisture changes. Figure 8 illustrates surface moisture related data of July 31 under dry condition. Figure 9 illustrates surface moisture related data of August 2 under wet condition of the same area.

The colors in Figure 8 and Figure 9 correspond to the soil moisture gradations in the upper 0-5 cm thick layer. Dark green ranges between 0 and 0.05 m^3/m^3, light green ranges between 0.05 and 0.10 m^3/m^3, light blue ranges between 0.10 and 0.20 m^3/m^3, and dark blue ranges between 0.20 and 0.35 m^3/m^3, and represents open water.

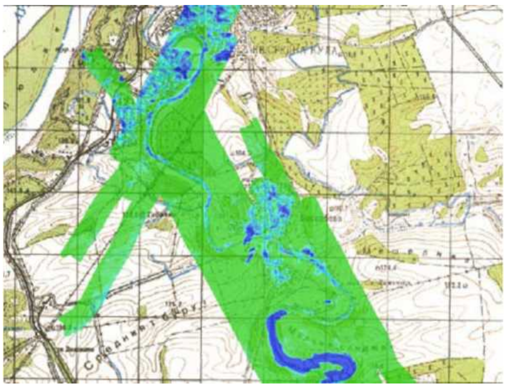


Figure 8. Soil moisture under dry condition

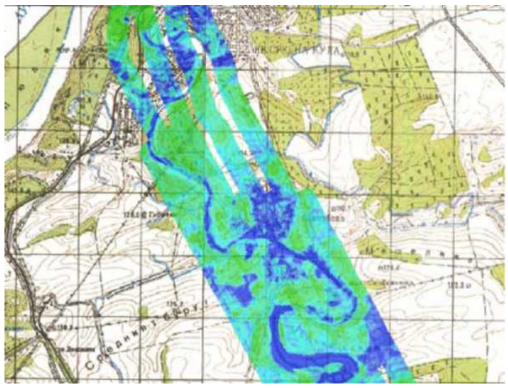


Figure 9. Soil moisture under wet condition

The land surface cover from 10-cm true ortho-photo (Figure 10) was combined with the lidar relief features (Figure 11) in a three-dimensional (3-D) fly-through by ReSAC. A snapshot of this product is shown in Figure 12.

The simultaneously collected multi-sensor data was finally combined in an Information Management System (IMS) for effective risk analyses. The block diagram of Figure 11 illustrates the various elements of the IMS: the airborne data that is geo-referenced using positioning and inertial data, a backup and retrieval database system that includes existing a-priori geodata, and an integral processing part using various mathematical procedures, such as normalization, weighting, and distribution.

Figure 10. 10-cm Orthophoto for LPIS

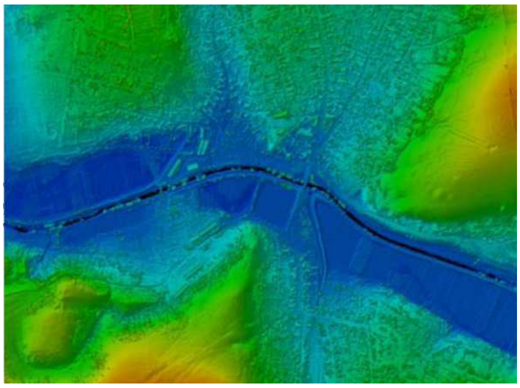


Figure 11. Lidar elevation model for GAEC

Figure 12. 3-D Fly-through of orthophoto and Lidar elevation

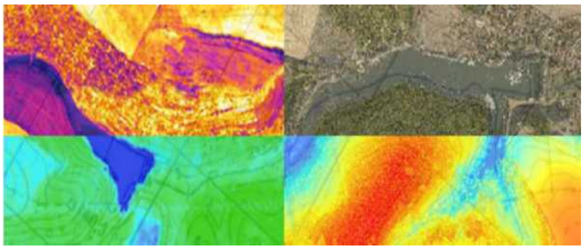


Figure 13. Multi-sensor composite

Figure 13 illustrates a composite of all datasets at Dams at Nikolovo. The surface temperatures (top left) range between 25°C (dark blue, open water) and 50°C (white, dry and open fields), and correlate with the soil moisture data (bottom left) and lidar elevation data (bottom right).

The main conclusions and recommendations of the show case project in Bulgaria are:

- the project has successfully proven the effectiveness of the used MIRAMAP multi-sensor technology and approach for preventive risk management of natural hazards, part of which is flood preventive measures and preventive control of flood protection facilities;
- the MIRAMAP system is ready for implementation in two major areas of application, related to the Common Agriculture Policy (CAP): control of the Good Agriculture Environment Conditions (GAEC) and the update of the Land Parcel Identification System (LPIS). As for the GAEC, the system has especially proven successful for standards; temporary channeling of surface water on sloping terrain, and defense of ground structure through maintenance of surface water drainage.

The conditions of over-moistening revealed on the August 2nd data were the important indicator of expected flooding.

1.6 Network protection – policy and technology reinforcements

Critical monitoring infrastructures that serve emergency management require strong network protection means. Security is not a finite state and is a permanent process. Basic technical means of network security include firewalls, secure protocols, PKI and electronic signature systems, virus and spam filtering. The final network protection level still depends on correct integration of mentioned components. It is sensitive the use of proper knowledge on known software bugs and intrusions. In general it is important to know about the existence of alternative means for security above the PKI [Aslanyan et al, 2002; 2003].

The issues mentioned above are treated in terms of several EC funded research project results. These projects were developing pattern recognition and data mining algorithms, estimating complexities of discrete optimization problems, they dealt with software agent structures, which are mostly implemented, in Java algorithmic language. Here we apply these results to the Network Protection schedule. First, in this section we discuss and conclude that the complications/combinations of basic means for security provide the same or comparable level of protection. Then, we show that the distributed software agent systems may provide additional means for security, being able to monitor wide network areas and analyze the monitored information – mining useful knowledge on intrusions, on malfunctioning, etc.

1.6.1 INTAS 04-77-7173 "Data flow systems: algorithms and complexity"

The project research objectives in global terms can be characterized as:

1. Comparative study and systematization of the achievements in combinatorial and computational algorithms and their complexities – intractability, approximation, lower bounds, and heuristics
2. Elaboration of new algorithmic approaches in cases, when the known algorithms are proven non-data flow optimal
3. Study of complex systems: asynchronous computational models (such as hybrid agent societies, WEB search engines), their computational and knowledge extraction power, the complexity counterpart of the overall behavior and functionality of cellular autonomous systems

One of the specific research objectives studies the encryption related algorithms. From one side – it is the well known the one way functions are valuable instrument in this area, from other side – it is directly unknown and important to know if a mixture and complication/combination of several one-way function will bring additional hardness in reversing these functions. It appears that combining combinatorial – computational means for security composes the mixture, which is the same level protection structure. Such postulation is one of the valuable inputs of INTAS 04-77-7173 project.

The formal framework is as follows [Grigoriev et al, 2006].

Let (G,E,D) be probabilistic worst-case polynomial time algorithms for key generation, encryption and decryption respectively of a PKI system S. The PKI scheme defined is δ(n)-correct iff for large n $Pr\{Dsk(Epk(m))=m\} \geq \delta(n)$ for $(pk,sk) \leftarrow G(1^n)$ /key pair generation by given security parameter/. Here sk, pk are secret and public keys and m is a plaintext message.

Probabilistic black-box A ε(n)-breaks PKI scheme if for infinitely many parameters n $Pr\{Apk(1^n,Epk(m))=m\} \geq \varepsilon(n)$ for $(pk,sk) \leftarrow G(1^n)$.

An encryption scheme (G_1,E_1,D_1) is reducible to an encryption scheme (G_2,E_2,D_2) if there exists a probabilistic polynomial time oracle machine R, such that for any probabilistic black-box A that breaks (G_2,E_2,D_2), R^A breaks (G_1,E_1,D_1).

We denote the class of all 2/3-correct public key encryption schemes by PKCS.

Theorem: There exists a complete PKCS /complete, as an analogy from the NP complexity theory means that all schemes are reducible to the considered one/.

Polynomial reduction of problems and complectness concepts appeared earlier in algorithmic intractability studies. Any NP complete problem is the hardest representative of class of nondeterministic polynomial recognition problems. The given result on encryption proves a similar property of being the hardest representative for encryption algorithms when an error is allowed. Our interest is not in details but is in PKI systems being reducible to each other. This means that they have the same protection power and then we conclude that alternative algorithmic forces are necessary for security out of combinatorial and computational counterparts, and then we try to strengthen the level of securities through the intelligent network monitoring and data analysis means.

A similar notion is placed in ESFORS (European security forum for WEB services, Software and Systems), FP6-027599 project documentation. Prof. Lioy (Politecnico di Torino) mentioned limitations and conflicts between business objectives and effectiveness of security services insisting to incorporate the ability of prediction of systems behavior. Prof. Malek from University of Berlin also mentioned the role of prediction with some specific details and suggestions. In the same line, the prediction through Data Mining and intelligent software agents is innovated by European Framework Program SPARTA project.

1.6.2 SPARTA "Security policy adaptation reinforced through agents" project

Security Policy consists of:

1. Detailed description of any information, which might be monitored operationally and which might be of some interest for data security reasons
2. Archiving of existing knowledge – systems, structures, technologies, viruses, hacking
3. The data analysis algorithms – to be designed and realized, by the above data descriptions according to the basic tasks and requirements
4. The set of laws, rules, and practice that regulate how an organization implements, manages, protects, and distributes its information and computing resources to achieve security objectives

SPARTA system started by the mentioned European Framework Program Project http://cordis.europa.eu and was further developed after the project. This framework considers the mobile agent server system, which monitors the implementation of security policies, identifies security problems, and performs intrusion detection tasks. Security checks are flexible, at run-time and without interrupting the system's activity. The two main use cases are Surveillance (of a given security policy) and Intrusion Detection (ID).

✓ System design, architecture, main components

SPARTA architecture supports both distributed and centralized use cases (Figure 14).

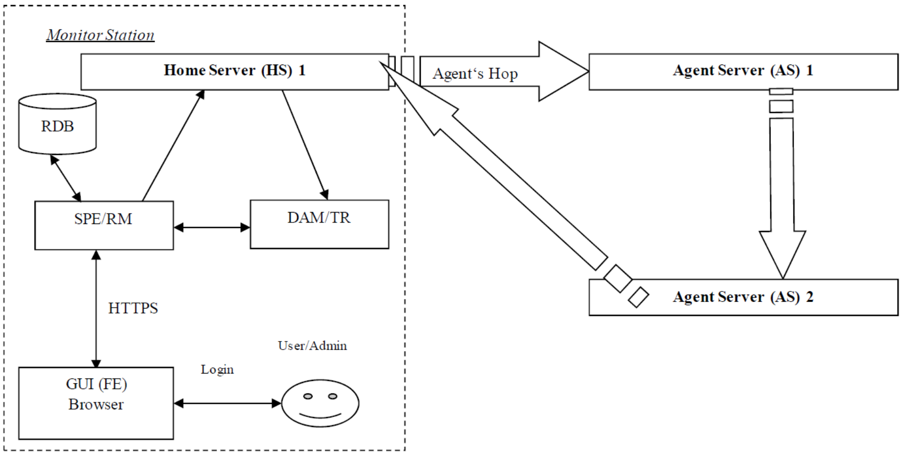


Figure 14. SPARTA architecture

Main components in SPARTA architecture are: Agents (A); Agent Server (AS); Home Server (HS); Secure Infrastructure with Secure Information Space (SIS); Data Analyzer Module (DAM); Security Policy Editor (SPE); and User Front End (FE).

✓ Architecture, Agents (A)

Agent is the centerpiece of SPARTA design. It bears mobile software code and serves automating application tasks. Main types of SPARTA agents are: One-hop, Multi-hop, and Embedded. Each agent consists of two parts:

1. Agent State: agent's operational data together with management information (e.g. user ID)
2. Agent Code: its source code as Java class file, which is separately downloaded from a Code Base Server

✓ Architecture, Agent Server (AS)

Each agent is initiated by an agent server (AS), running on an AS in a certain place. A place provides a run-time environment for an agent by allowing it to call certain functions. A communicator is an AS module, which is responsible for sending and receiving agents among the servers. An Agent Security Manager (ASM) prevents attacks from agents, which are directed against the AS or the underlying host.

✓ Architecture, Home Server (HS)

The home server (HS) has two main duties:

1. It allows agents that finished their work to return to a special place (User Place), where they are stored and wait for user login.
2. It provides an interface for components like FE, SPE, or DAM to access returned agents or to launch the new ones.

Home server supports detached computing, i.e. users might be disconnected from the network, while the agents are performing their work. User can optionally be notified by email or SMS when the agent has returned.

1.6.3 SPARTA implementation

In Figure 15 some aspects of SPARTA implementation are shown.

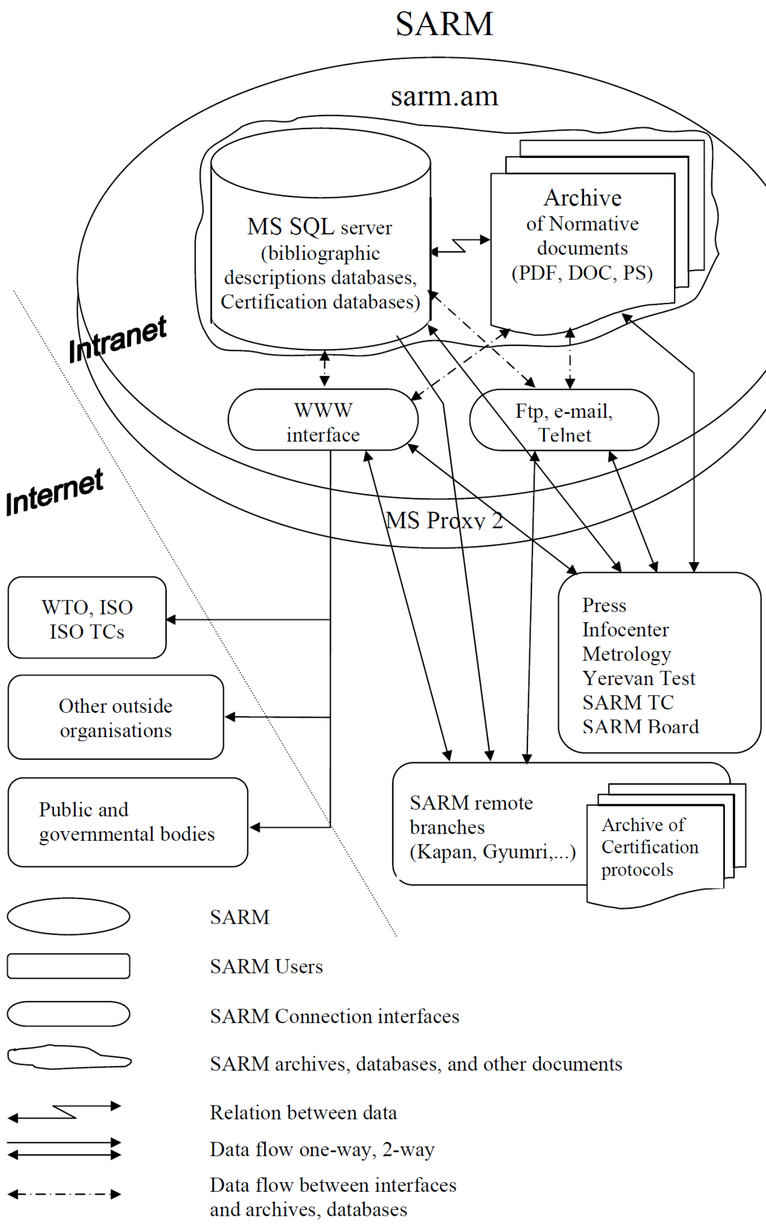


Figure 15. SPARTA implementation

✓ Case studies

SARM (State Department for Standardization, certification and Metrology), and its branch organization in Kapan (Armenia) (Figure 16):

SARM's Branch organization in Kapan manages provision of certification and accreditation process and documents, in relation to the product, services, quality system, etc. The certification body works with standardization documentation to make a conclusion regarding the kinds and services under the consideration:

– production certification (based on use of Technical Conditions);
– certification of delivered product (based on laboratory analysis);
– services certification;
– quality correspondence certification (ISO 9000).

After making conclusion, certification body sends the concluding certification document to the SARM server. Communication uses network of Infoservice Company.

Figure 17 is the scheme of the technical environment for Independent Verification and Validation tasks after the SPARTA Design and Implementation. The system specific part is validation, which is divided into subtasks:

– security policy validation, monitoring and enforcing;
– monitoring of systems integrity;
– vulnerability assessment;
– general purpose intrusion detection.

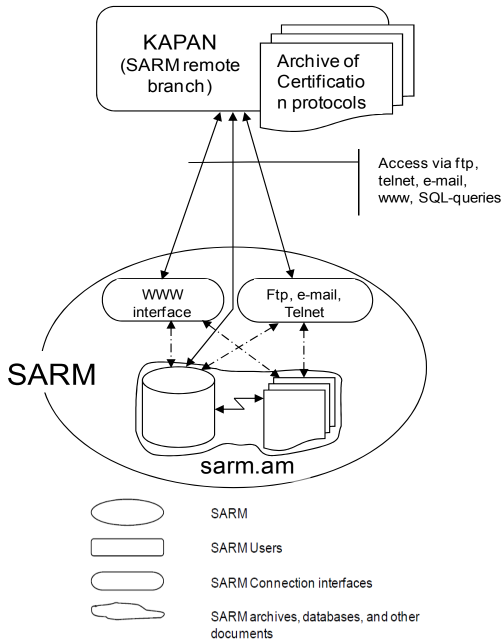


Figure 16. SARM's branch organization in Kapan

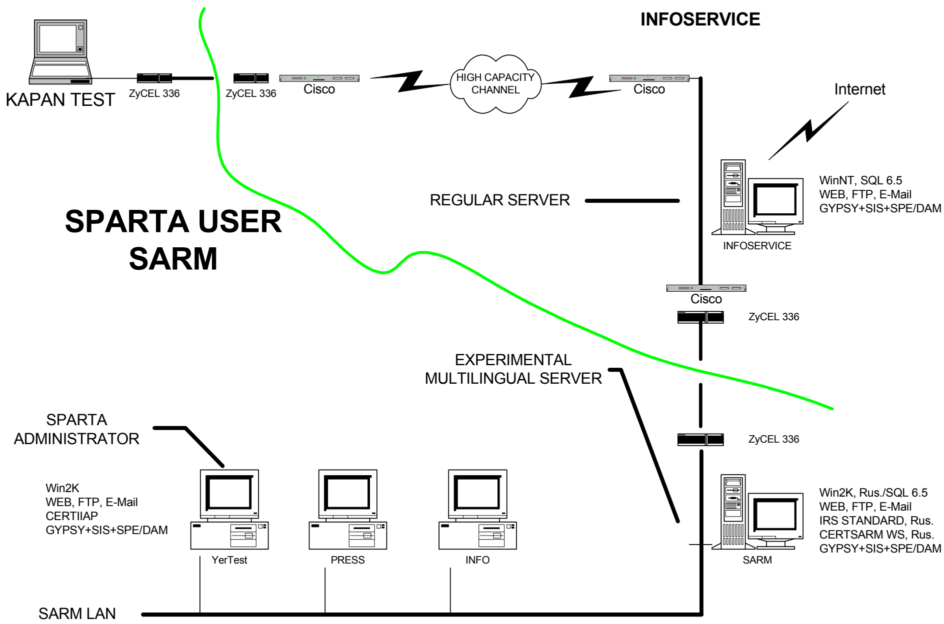


Figure 17. Scheme of the SPARTA technical environment for independent verification and validation tasks

✓ Data analysis module architecture

Next, the most intellectual component of system is the data analysis algorithmic tool. Here the main technology used is Data Mining where the practical algorithms were selected during the studies of Data Mining technologies through the INTAS research project described below (Figure 18).

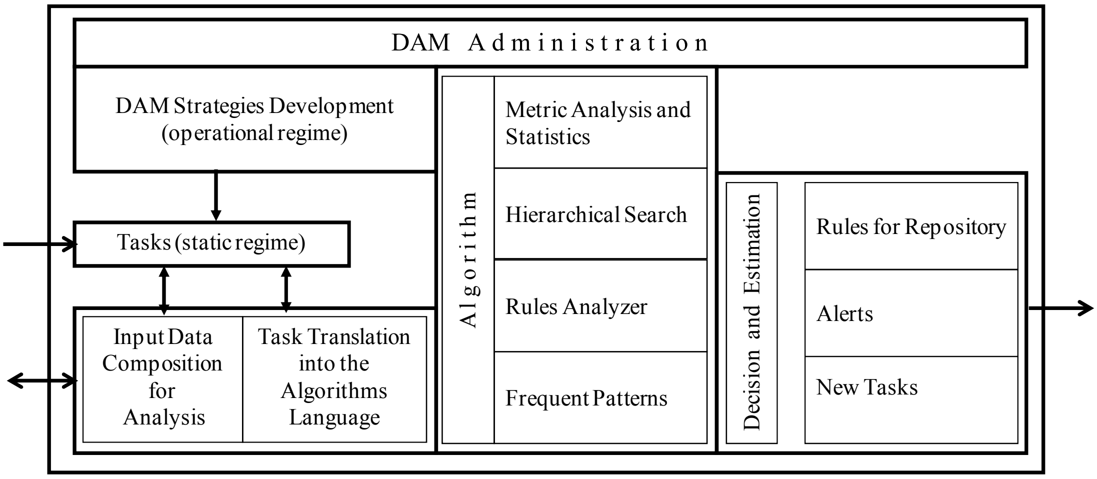


Figure 18. SPARTA data analysis module architecture

Each task of DAM has been formed by determining the input data, the data analysis method and – the output actions and forms (alerts, e-mail, SMS, special files, etc.). Three classes of task scenarios are assumed:

1. Fixed task scenario
2. Formal task scenarios by selection and composition (for experimentation by administrator)
3. Background (long term or permanent) search for regularities

✓ Fixed task scenario

In this scenario the input data types, sources, data analysis methods and output forms are determined and fixed during the design time on base of study of user's typical requirements. The individual tasks might be selected and activated by a user from the task list (it is the responsibility of system administrator to specify the data types for data collection, data analysis methods, by the ordered data and the type of interpretation of data analysis results and decision).

✓ Formal task scenarios by selection and composition

This class assumes the following cases:

- input data format is fixed/selected and user selects the data analysis methods for/by this format;
- data analysis method is fixed/selected and user selects data format for the input data;
- user selects any combination of input data formats and data analysis methods and the system checks the validity of the formed combination before the implementation.
- background search for regularities: in this case, the regular user similarly to the previous cases has formed new (experimental) DAM tasks. The functionality mode is automatic.

1.6.4 INTAS 00-652 "Data mining algorithm incubator"

- **Hybrid recognition schemes**

Monitoring systems collect huge information amounts, which require novel algorithmic approaches to be able to provide an online analysis. In recognition and classification where learning set is known as very limited in size, the first priority is the detailed information analysis. The shift of input from learning set to monitoring information requires restructuring of recognition algorithms. Hybrid recognition works in two stages. First is a quick tree based procedure. Then works a metric recognition procedure, but these work is with "error classes" after the first stage, which are much small in sizes [Aslanyan et al, 2007].

- **Frequent patterns mining**

Association rule mining is one of the basic data mining tools. The known realizations use "growing" of frequent subsets as the way of finding association rules. An alternative approach is developed, which uses the n-cube geometry elements. Monotone Boolean functions given by an oracle are recognized optimally through the special n-cube partitioning into the monotone growing chains. A modification of this structure is supported by chain computations, proven productive for frequent subsets finding [Aslanyan and Sahakyan, 2009].

- **Logic separation recognition**

Logic based Pattern Recognition extends the well-known similarity models, where the distance measure is the base instrument for recognition. Initial idea is under consideration since 70s and it reduces the logic based recognition models to the reduced disjunctive normal form of partially defined Boolean functions. An alternative pattern recognition approach combines the metric and logic hypotheses and features, and leads to studies of logic forms, hypotheses, hierarchies of hypotheses and effective algorithmic solutions. Current results provide probabilistic conclusions on effective recognition by logic means in a model environment of binary attributes and of data flows [Aslanyan and Castellanos, 2007], [Aslanyan and Ryazanov, 2008].

1.7 Intrusion detection systems

All information systems are vulnerable to computer attacks, in which they can completely fail. Computer viruses can also distort the functions of information system and add the undeclared capabilities. To prevent such situations it is required a robust information security systems. One element of such systems is intrusion detection systems. Initially, system administrators detect intrusions, sitting in front of the console and analyzing users' actions. Then began to be used logs user actions, the volume of these journals has increased with increasing number of users of information systems, so examine all records at once, administrators could not.

In the early 1990-s, there was developed intrusion detection system in operational mode, which looked through logs as soon as they are generated. Intrusion detection systems (Intrusion Detection System, IDS) is a software or hardware, designed to detect unauthorized access to the facts of a computer system or network or unauthorized management (mainly through the internet). Intrusion detection systems are used to detect malicious activity that may compromise the security of computer systems. Such activity includes network attacks against vulnerable services, an attack aimed at increasing the privileges of unauthorized access to sensitive files, as well as the actions of malicious software (Viruses, Trojans, and Worms).

An important characteristic of intrusion detection systems is the method of data analysis. There are two methods:

1. ***Detection of anomalies:*** In this case, the models of expected behavior of users and applications, the deviation from "normal" behavior of the system is interpreted as a violation of the protection [Denning, 1997]. The main advantage of such systems is that they can identify previously unknown attacks, but this is a high probability of false alarm due to significant variability in the information system.
2. ***Detection of abuse:*** Such systems contain descriptions of attacks (signatures) and looking for compliance with the descriptions in a controlled flow of data to detect manifestations of known attacks [Ilgum and Kemmerer, 1995]. The number of false positives in this case, very little, but these systems can only identify known attacks; therefore, the base of signatures must be constantly updated.

Typical architecture of an intrusion detection system is shown in Figure 19.

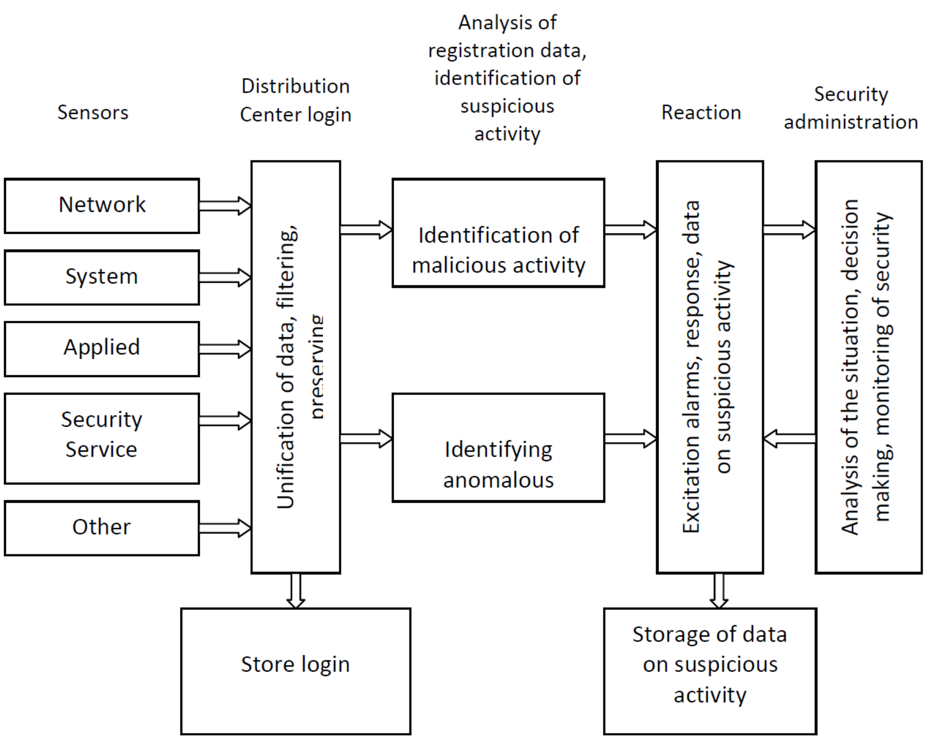


Figure 19. Architecture of an intrusion detection system [Galatenko, 1999]

Primary information gathering carried out by various sensors. To facilitate the work of all components of the system, the sensors can perform filtering of recorded data, but it is significantly complicate the structure of sensors. The sensors transmit the information received in the distribution center, which leads her to a single format, if necessary, was further filter and store in a database and send for the analysis of statistical and expert component. If the process of statistical or expert analysis identified suspicious activity, a message will send to the center response, which identifies whether the alarm to be justified, and chosen method of response.

1.7.1 System SNORT

Snort is a network intrusion detection system (IDS) with open source, which can perform real-time analysis of IP-packets transmitted on the monitored interfaces. Snort detects attack by combining two methods: the signature and protocol analysis [Yaremchuk, 2007].

All the information collected by the detector Snort could be saved to the log files that may have a different format. In addition, for ease of analysis, information can be entered in the database (Postgresql, MySQL, unixODBC).

The system, built on Snort, has the ability to collect and process information from multiple spaced sensors. All of the cases are in performance of computers that are used as sensors. In order to improve performance, sharing the quick work of IDS to capture packets and relatively slow in entering the information, you must use Barnyard, which is available on the upload page draft Snort. In this case, Snort creates a special binary output "unified" format, which working Barnyard.

Snort not directly able to work with 802.11 wireless networks, but connected to such a device will be able to interpret the information received. Today Snort in principle does not distinguish whether what type of network he has to do, no specific options to install and no need to configure.

There is a special branch of Snort – Snort-Wireless (snort-wireless.org), just designed for the detection of attacks aimed at the network 802.11. Snort-Wireless is backwards compatible with Snort 2.0, when it contains some specific rules for processing packets that are configured on the vulnerability and the typical attack wireless networks.

1.7.2 System OUTPOST

Intrusion Detection System "Outpost" version 1.3 is designed to identify and block network attacks in information systems (IS) [Outpost, 2010].

System of "Outpost" reveals an attack on user workstations, servers and communications equipment IP. It allows equally effectively identify and block attacks from both external and internal perpetrators.

The system of "Outpost" reveals an attack based on information collection and analysis of IP data packets on the network, transport, and application level stack TCP / IP.

"Outpost" uses signature-based method of detecting network attacks. It provides detection of attacks based on special patterns (signatures), each of which corresponds to a specific attack.

Getting network traffic, the system analyzes it to ensure compliance with these patterns of attacks available in the database system, which is constantly updated by the developer. In case of detection signatures in the original data, the system fixes the detection of network attack. The administrator has the ability to add to the system the new attack signature.

1.8 User-oriented policy for managing risk and safety

The growing frequency of natural disasters, their serious impacts, and huge damage have become to be considered one of the modern challenges of the countries in Europe and all over the World. The issue of having a preliminary assessment of the likely damage and ways to mitigate or even avoid it has attained an ever-bigger significance.

The experience gained in recent years from various national and international projects aimed at finding solutions to minimize damage from natural disasters and creating workable models of forecasting and assessing potential future damage reveals two components as being major factors for achieving good results: a good methodology and access to the necessary spatial data and information systems. Given that there have already been developed methodologies and simulation models of the respective disaster, what remains an open issue is ensuring the necessary data, in an appropriate format, with the relevant compatibility so that they can be combined with other data and processed as a package so as to obtain the required synergy effect and results as close as possible to the real ones. Thus good methods, simulation models, and software are reduced to zero when data sources are not available or they are not accurate, updated, and easy for use. The problem is related to the adoption of common rules for data exchange, data storage and formatting, etc., which are the subject matter of European Directive 2007/02/EC setting the legal framework for the establishment and operation of an Infrastructure for Spatial Information in the European Community (INSPIRE), but which also call for the introduction of rules vis-a-vis interoperability of the information systems.

Therefore the presented article is combining research & development topic – as modeling preliminary losses from natural disasters (earthquake in this case), and conceptual topic – as the development of a quality assurance reference data base and regional networking for data storage & processing and for risk and security management. One possible approach on the last item is creating an infrastructure to ensure such exchange of spatial data and their processing, and to set up a network of application servers for spatial information in different parts of Europe, which work in harmony and constitute parts of a unified system. Such an approach is considered in many respects be better, more effective, and yielding faster and better quality results than the creation of a central server, where primary data are fed by various municipalities, regions and countries.

1.8.1 General overview

In the course of several millennia, the human evolution turned the human being from someone who inhabited forests and various natural earth cavities into a geological factor who built first small, and then ever bigger and bigger artificial complexes – buildings grouped in even greater zones: population and industrial agglomerations. The matter moved to be input in these urban agglomerations is commensurate with the quantity expelled by major geological disasters – volcanic eruptions, or moved by tectonic processes – earthquakes.

Irrespective of his incessant effort, man cannot yet boast that he has tamed the natural force and the cyclic occurrence of hurricanes, earthquakes, fires that wreak havoc and claim many lives. No one has yet "won a battle" against a natural disaster, one can rather speak of avoiding the worst and mitigating the damage. This is why a "winning war" with the dark side of the nature would need a careful preparation of "the next battle" – an appropriate system for forecasting of possible disaster-induced damage and the strategic planning and preventive measures that go together with it.

1.8.2 Local and global approach

It is common knowledge that proper measures taken beforehand reduce many times over the damage from a possible natural disaster as well as the resources and money necessary to overcome the consequences. Given that a natural disaster may strike at a particular place but can affect a large geographical area sometimes covering several countries, the work should be aimed at achieving coordinated estimates and measures simultaneously, on the local, as well as on the inter-regional, community or even global, level.

This is why the respective methodologies, spatial databases, simulation models and outputs need to be compatible, aimed to achieve a synergy effect and create a platform of interoperability.
Five levels of management are identified:

- municipality;
- country;
- region;
- European Union;
- global level.

Halfway levels are possible too, such as unification of policies for risk management in a given area of impact, for example the catchments areas of big rivers. A good example of this would be the creation of an integrated system for prevention against flooding and water pollution along the Danube within the future European Danube Strategy.

In respect of earthquakes, an intermediate form of unification could be sought of policies for risk management in areas affected by known seismic foci or geological areas, e.g. significant faults in contact areas of tectonic plates.

Set out below is an opinion about the necessary exchange, and in certain cases, integration of spatial databases and information systems regarding seismic risk.

1.8.3 Methodological basis

The methodology for forecasting damage caused by natural disasters, particularly earthquakes, mainly targets the residential urban environment and the public utility and industrial infrastructure related to it, which make up the modern city. The methodology complies with the requirements to yield results that are useful for the end users (local and central powers, business entities, civil protection), as well as to tackle the existing problems with the available spatial data, unreliable information and absence of information.

Why is such a methodology an indispensable element of the effective policy for managing risk and safety? This is so for a number of reasons, namely:

- buildings differ in type, mode of construction and age, and thus have different vulnerability to catastrophic seismic impacts, so that the damage they will sustain will be different;
- the modern urban society has never had such surplus of energy, resources and temporal capacity so as to allow the construction of buildings able to withstand the possible maximum seismic impacts;
- rigorous construction supervision is missing (especially in the time passed); many violations are made on town-planning indicators and the requirements for free spaces and distances between buildings, laid down for safety reasons;
- the policy for sustainable development calls for judicious spending of resources for prevention against seismic impacts, allowing such expenditure only where the alternative to building a new earthquake-proof building or the reinforcing of an old one would yield an immediate positive effect for the public, either in terms of safety and quality of the living space, or as industrial

economic infrastructure, or also as protection of an intangible value of historical or emotional essence;

- recently we have witnessed (in Bulgaria) a dangerous scheme used by developers who opt for fulfilling their interests by contravening the law and even creating a threat to people's lives and health. In the scheme certain buildings which have public significance, constitute monuments of culture, or are banned from demolition by law, are left in disrepair or else their process of degradation is accelerated artificially, so that they reach the stage of self-destruction and can thus be freely removed and replaced by a new development project which usually exceeds considerably the permitted town-panning parameters. The scheme in question poses a double threat – on the one hand the disintegrating building poses a threat to the members of the public and to the buildings and infrastructure next to it (a fatal accident of this type occurred in Sofia only two years ago), and on the other, the new construction usually fails to comply with the safety criteria and standards and becomes a potential threat during a future earthquake.

Driven by various reasons the modern society (and particularly United Europe) has developed adequate methods for observing a given disaster and for managing economic flows during recovery; however, a single methodology is yet missing for forecasting disaster-induced damage, including in terms of individual risks and topics. This is especially true of places where the data necessary for making the estimates are rarely available in the necessary volume, accuracy, and credibility.

In such a case, the option is to look for a methodology that is "sustainable" and resilient to data incompleteness, a methodology that is nevertheless applicable, albeit with a reduced accuracy of results. The most important thing in this case is for the methodology to provide a good idea about the areas with increased risk and a reliable general assessment of the likely damage. The methodology needs to be able to be applied both at the local level – a neighborhood or a town, as well as at a greater one – a region or a country. At the next stage partnership is to be sought with experts and structures from neighboring countries to ensure interaction between such methodologies of two countries or more, as well as the exchange of data, models and results.

Such a methodology will prove very useful for risk assessments vis-a-vis urban centers with limited data about housing and public utility infrastructure.

The methodology takes into account the state of the spatial databases and information systems in Bulgaria and the actual difficulties in providing full, detailed and objective information. In this respect the situation in Bulgaria is similar to that in many other EU member states, meaning that the methodology can be successfully applied in the EU, as well as in other geographical regions.

The methodology, developed by a team of experts in different areas: geophysics, economy, town planning, informatics, has three successive layers:

1. risk assessment of housing
2. risk assessment of public utility and economic infrastructure
3. assessment of economic damage

Assessment of the so-called "intangible damage" has not been envisaged, as at this stage it proved impossible to validate in the respective software the connection between intangible or information values and current tangible values and assets of the modern city.

Several versions of the methodology have been set out, for example – for assessment of earthquake-induced damage of residential buildings; for an overall assessment of the seismic risk; for estimation of the economic losses from natural disasters.

1.8.4 Methodology for assessment of earthquake-induced damage of residential buildings at the level of municipality, district, country, region

The methodology has been used on test cases for the Bulgarian cities of Sofia, Ruse, Vratza, and for the whole country. First priority was given to results, which can be of use for the local and state administration for planning their economic, and resources actions as well as for urban planning, building rehabilitation, and civil protection.

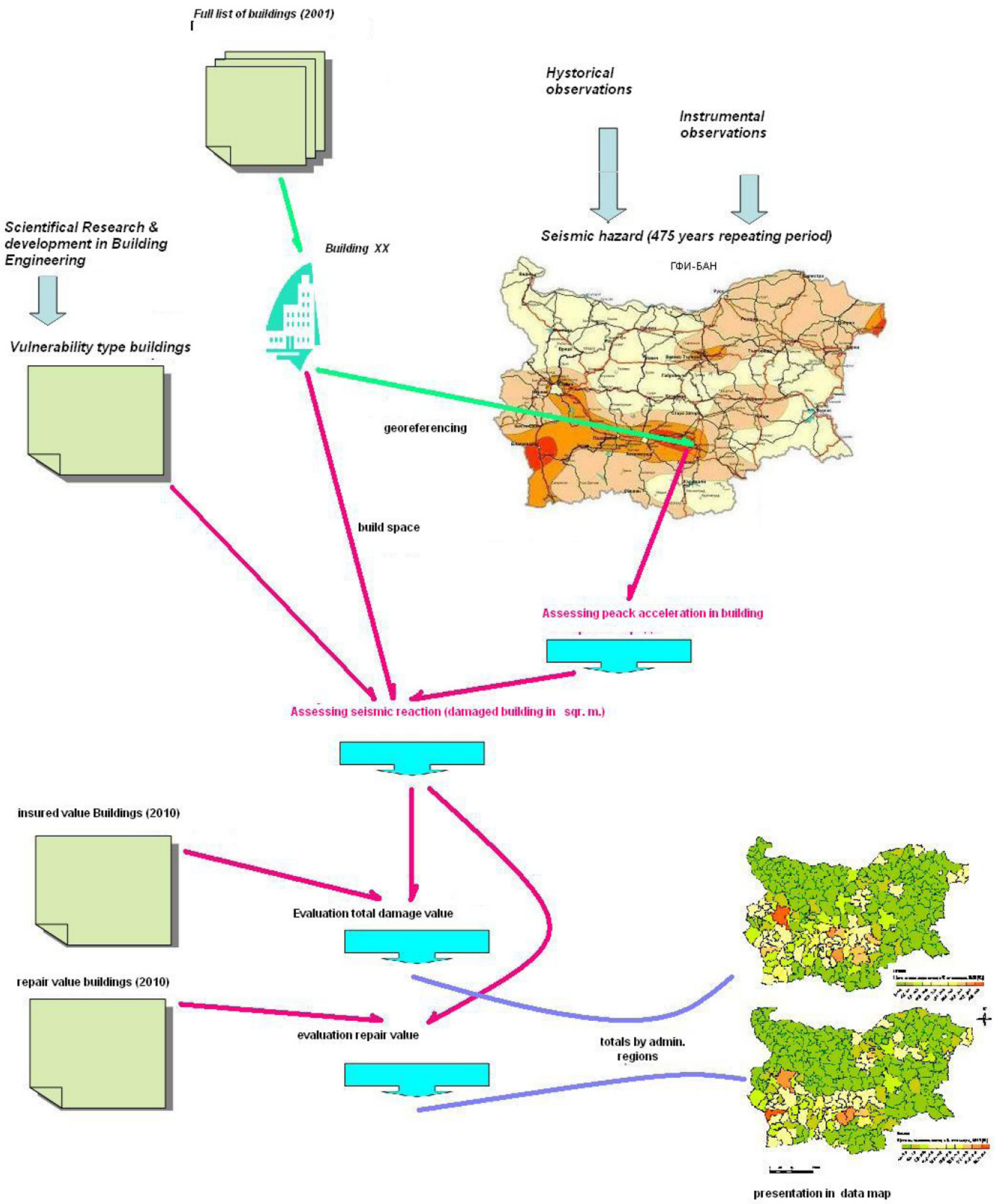


Figure 20. Simplified technology for seismic damage assessment of dwellings

The methodology is based on experience gained from work under the RISK-UE project in Europe and HAZUS in the United States in the late 1990s and the beginning of the new millennium. It starts from:

- availability of data about catastrophic impact (in the region);
- availability of data about housing (in the region);
- availability of a vulnerability function (vis-a-vis the respective housing related to catastrophic impact by type of buildings and type of impact).

To obtain an assessment of the expected damage, systematic modeling is made of the catastrophic impact for each registered housing object, depending on the planned maximum catastrophic impact.

The methodology concerns assessment of the likely damage on residential buildings caused by an expected earthquake with a given magnitude. It is applied on information about housing and the occupants thereof available in the respective National Statistical Service. The methodology is apt to be applied in assessing the value of small to medium damage (for example, up to 20-25% of the area), whereby the recovery value increases non-linearly when the percentage of damage is higher, as costs will be provided for clearance.

A brief scheme of the methodology is shown in Figure 20.

1.8.5 Methodology for overall assessment of earthquake damage

The methodology is in the process of being developed; the authors have set themselves the task of extending it (for housing infrastructure) to include the public infrastructure (the urban infrastructure in particular) in the actual situation of missing workable databases about buildings and other urban infrastructure. To this end, partial use is made of the methodology for structuring of the urban infrastructure in the European project RISK-UE (WP3) (Figure 21).

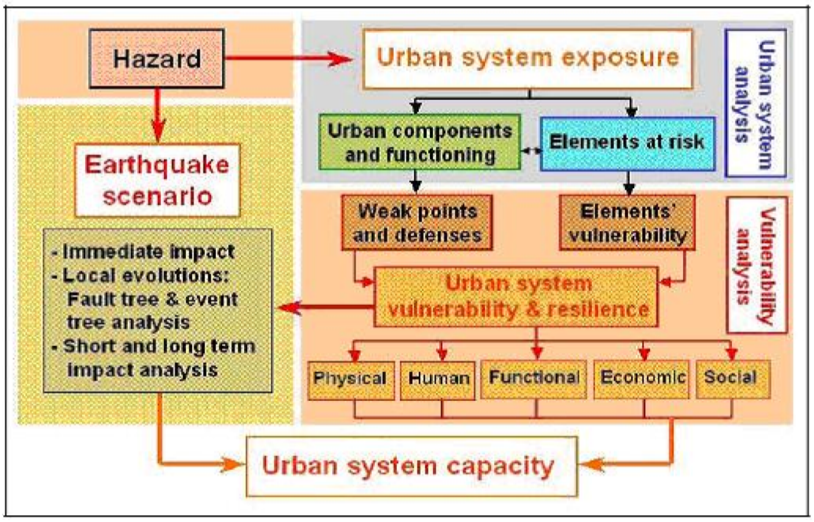


Figure 21. GEMITIS' seismic risk analysis

From the overall approach, the part covering the elements at risk complementing housing is being extracted.

The simplest option would be to apply the basic methodology on sets of infrastructure descriptions. Nevertheless, here lies the main obstacle, in this case – for Bulgaria – the absence of a detailed and comprehensive description of this infrastructure.

1.8.6 Extrapolation of the housing damages to damages in the public infrastructure

A more complex option would be to arrive at a system for extrapolation of the public housing data to a mechanism for assessment of infrastructure data as a main task in risk assessment.

Solving such a problem is not possible using simple linear extrapolation of housing damage (a purely physical assessment).

In the first place, the purely housing damage – provided that it does not exceed a minimum percentage (e.g., 5%), can be serviced in fully functioning infrastructure (i.e., without, or with only negligible losses in the public infrastructure). Then recovery is seen as part of the normal functioning of society, rather than an emergency activity. This is why losses in the public infrastructure should be considered from a certain threshold and above.

After the initial version, mechanisms can be applied as well for taking into account the impact of losses in the public infrastructure in the sub-scheme of their structuring according to the above-mentioned model of WP3-RISK-UE:

- vis-a-vis physical damage (collapsed buildings) of the public infrastructure;
- vis-a-vis functional damage of the public infrastructure (impossibility to function fully);
- vis-a-vis economic damage (from own collapsed facilities and from a diminishing workforce busy with recovery of primary needs);
- vis-a-vis functional and economic damage from newly emerging urgent social & material needs;
- vis-a-vis "social" (non-material historical, marketing and similar) damage as a result of the disaster which diminishes the economic value of the respective area.

Further, mechanisms are applied for transformation of housing damage to damage on the public and economic infrastructure. Some preliminary conditions are accepted as:

- going beyond a certain percentage of damage (e.g., over 10%) suggests additional costs for rescue, evacuation of population without shelter, setting up of medical aid, security and safety, provision of food for the population remaining in place;
- hurricane Katrina, and even more so, the earthquake disaster in Haiti, revealed the considerable shortage of capacity of the security services in the event of a large-scale disaster;
- in the case of more than 10% affected (destroyed) housing, emergency costs are to be provided for temporary housing to shelter the surviving population until recovery of at least 60% of the volume of housing from before the disaster;
- going beyond a certain percentage of damage (e.g., over 5-10%) suggests non-linear increasing of costs for site clearing. If more than 35-50% of the housing has been affected (has collapsed), from 10% to 40% costs (of the building value) should be provided for site clearing and environmental-friendly processing of waste;
- as a rule, the normal construction activity for a given region is determined as being designed to build/recover no more than 5% of the available housing (i.e., a term of restoration of housing of no less than 20 years). Above this percentage all activities for clearing and restoration constitute ADDITIONAL capacity for construction and repair works which is not available in situ;
- more than 35-50% affected (destroyed) housing suggests total destruction and a need to build anew the houses affected by the disaster;
- when the affected (destroyed) housing exceeds 10%, a relevant percentage of destruction of public utility infrastructure should be assumed – schools, hospitals, which could vary from 5% to

15-20% of the value of the housing (depending on the characteristics of the social environment at the place of the disaster). This should be taken into account, irrespective of the application of specially heightened seismic requirements vis-a-vis such public buildings in certain areas (e.g., in the United States). When more than 40-50% of the housing has been affected, total destruction of the subsurface public utility infrastructure servicing the given housing should be assumed. Respectively, rebuilding of the public utility infrastructure should be provided;

- in recovery actions in a region heavily hit by a seismic disaster, costs for the transport infrastructure should also be provided for, which need to be higher than the prices of such infrastructure during normal times of construction;
- when more than 15% of the public utility infrastructure has been affected (destroyed), urgent building of temporary replacement public utility infrastructure should be provided;
- in the event of a seismic disaster (affecting more than 5% of the housing), shortage of construction capacity should be assumed at the place of recovery and a subsequent increase (sometimes multiple) of the economic value of the restoration in relation to the own value of the destroyed infrastructure (both housing and public infrastructure).

1.8.7 Extrapolation of the housing damages to the economy

Together with the social and public utility infrastructure, a seismic disaster will also damage the economic infrastructure of the given region.

In the modern societies the economy constitutes up to 70% services (commerce, public utilities, energy supply and supply of staples, education, medicine, administrative services), which are proportionate to the available housing infrastructure and which are affected/destroyed in the same degree as the housing infrastructure.

For example, in the observation of the restoration works after the 2008 earthquake in China, destruction of a considerable part of the existing economic sector was observed on the one hand, and on the other hand the replacement thereof by a newly-emerged construction sector for restoration funded by the Chinese budget.

The industrial economic infrastructure will reduce its capacity by a given percentage of the overall damage to the housing but only within certain limits of the total disaster (for example, up to 20-30% of the housing). Individual sectors may witness less reduction when they are related to restoration of the infrastructure (construction, etc.). Above this percentage anticipatory increase of the damage of the industrial infrastructure can be expected, in parallel with the reduction of the workforce being used on the one hand (which has been redirected to salvage and restore housing), and on the other, on account of the destroyed transport infrastructure, and still other, on account of a change in the local consumption caused by the restoration boom.

Depending on the geographical location of the industrial facilities, they too sustain damage, proportionate to that of the housing infrastructure. In the majority of industrial productions, the damage caused by a seismic disaster can cause an additional disaster: fire, pollution with chemicals, bio-agents, radioactive substances, etc., gazing, flooding, etc., which (depending on the concrete industry) can increase the damage to more than 500% from the initial value of the industrial facility.

In large-scale disasters, there inevitably occur economic losses due to a need for restructuring the economic infrastructure.

An example for a non-linear, non-proportionate (as set against that of housing) increase of damage is shown in Figure 22.

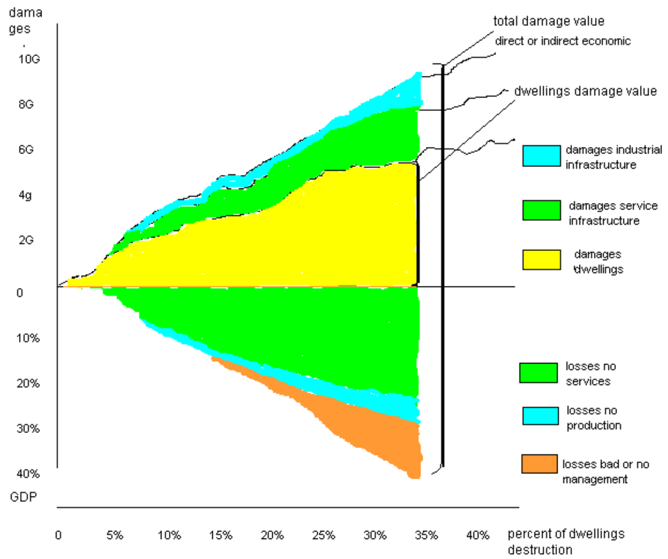


Figure 22. Non-linear, non-proportionate (as set against that of housing) increase of damage

1.8.8 Methodology for assessment of economic damage from natural disasters

This methodology constitutes an extension of the methodology for determining the total damage from a seismic disaster. In the presence of a baseline system for assessing housing damage caused by a catastrophic natural disaster (with taking into account of the "national" peculiarities), it is possible to make a multiplication scale which identifies parallel and subsequent damage on public utility and industrial infrastructure, and thus, an assessment of the relevant economic losses. A next step should analyze the cumulative effect from non-direct impacts, intangible assets, stress and psychological breakdown of big masses of the population.

A percentage of loss/destruction of public utility and industrial infrastructure commensurate to the housing infrastructure should be accepted as a basic criterion for economic loss, whereby the said infrastructures generate:

- public utility services (including transport, energy, communications, water and sewerage);
- material flows from industrial infrastructure;
- as a consequence of a reduced GDP – reduced tax revenue, restrictions/cuts in the government budget intended for restoration;
- additional reduction of the capacity for restoration and, respectively, the rates of GDP recovery.

Undoubtedly, a more precise assessment would be yielded by precise modeling of a "facility at risk" from a detailed map of the locations of public utility and industrial infrastructure compared to the map of the magnitude of the catastrophic impact via the vulnerability function, when such a map appears. Now information about the presence of such an integrated map is not available for any country in Europe.

As we said earlier, the public utility services are closely linked with the housing and the destruction of the former ties in very well with the damage on the latter. It is logical to recalculate the total volume of affected public utility services, via the square meters of housing area and the total lost/damaged square meters of area.

By way of an example, we offer below the preliminary assessments about Sofia, without claiming that they will not be adjusted when additional information and up-to-date data are provided.

Output data about Sofia, 2007:

- Gross Domestic Product 20,576,000,000 leva
- Gross Surplus Product 16,900,000,000 leva
- Redistributed via budget – 40% of the GDP, or 6,800 M
- Breakdown: Services 78.5%
- Industry 21.2%
- Forestry and farming 0.3%
- In services – 8.5% (increased, prior to that about 5%) construction, which will not decrease in the case of disaster.

With a total GDP per annum (2007) of 20,576 M for the territory of Sofia City, and projected maximum damage of 32% of the housing area, the total planned economic loss from services will be 5,530 million Bulgarian levas, or about the size of the direct damage of the housing lot.

The impact on the industrial sector (extracting and processing industry) of a seismic disaster as an assessment from a correlation with damage on housing is weaker than that of the service sector. Here we first have an impact threshold (above 5-10% affected homes from a separate industrial area). Secondly, the industrial activity is concentrated in separate industrial zones, mostly outside population centers, so that heavy damage of high-rise housing would not have a significant impact on the industrial capacity. In this context, it can be safely assumed that the percentage of damage of the industrial infrastructure will be no more than half of that of the housing infrastructure.

If we again take as an example Sofia City, the estimated projected economic losses would be to the tune of 411 million BG leva, or nearly a ten-time lower impact than a disaster in the service sector.

The occurrence of additional damage due to events caused by the primary disaster, such as fires, people/equipment buried under ruins, floods, pollution, etc., has relevance only for specific industrial infrastructure. In conducting a preventive analysis, a study should be made of available major industrial or energy facilities where a fire, pollution, flooding could occur in the case of disaster.

An additional damage from a disaster in the area of Sofia could be expected in the form of above-proportionate shrinkage of wholesale trade (up to 20-30%) and mostly, above-proportionate reduction of administrative and governance services since the administration is concentrated in the area of Sofia. Then the ensuing economic effect could reach up to 20-50% of the economic losses from services, or in the case of Sofia, this would mean another 2,000 million levas in damage.

The damage from necessary restructuring of the economy following a disaster is difficult to estimate precisely enough.

1.9 Discussion

Every year many collapses happen in the world, which can be divided into three groups:

- natural disasters
- technogenic disasters
- information disasters

Natural disasters are hurricanes, floods, earthquakes and other acts of nature which destroy the whole cities and lead to mass deaths of people.

Technogenic disasters are big accidents on industrial and transport objects which have been caused by failure in work of technical systems. Technogenic disasters are accompanied by victims among people and ecological disasters.

Information disasters are collapses, which occur in information computer systems. Mainly they occur because of viruses and other harmful programs.

Several examples of these types of collapses and opinions of scientists concerning their reasons were outlined. Examples of different intelligent systems for prediction, risk analysis, and intrusion detection systems were given.

It is clear for most experts that there is little likelihood for a comprehensive methodology yielding as truthful results as possible to be devised in the next couples of years in the European Union. Examples for such failures are found in risk prevention in the United States in cases such as Hurricane Katrina, in Europe in the recent floods in Central and Eastern Europe, the earthquake in China, etc.

Thus, above all we want to promote the pragmatic systematic approach in the creation and application of methodologies and models for risk management first on regional level, with a possibility for parallel verification in situ.

Developing of regional focal units, engaged in a large network of intelligent systems, covering the EU and later larger regions is a probably the best sustainable solution.

The absence of sufficient information in terms of diversity, up-to-date relevance, and correctness makes it necessary to look for effective use of the available data, whereby in most cases these constitute statistical information.

Two mainstays need to be used in order to achieve good results:

- European directives and regulations;
- strengthening the cooperation within the broad European area, which includes both EU member states and neighboring countries, based on the user-oriented approach which is better achieved if the regional and intelligent networking concept is accepted.

We need elaboration of national methodologies, simulation models, and analytical models for damage assessment, based on local data, which are subject to constant coordination and harmonization and in direct connection with the user – national governments, civil protection units, local authorities. In this sense a main partner of the regional and national teams could be some structures of the European Commission as the Directorate General Enterprise and Industry (more particularly, the department for Competitiveness, internal market for goods and sector policies), Directorate General Humanitarian Aid, Directorate General Joint Research Centre (more particularly, the Institute for the Protection and Security of the Citizen).

Meanwhile, a number of countries, as well as European structures, have set up relevant websites with up-to-date information for expected or past disasters. It would be a good thing if, on the basis of peer initiatives, and in addition to the information they upload, these sites adopt a unified intelligent system for presentation of information, including:

- automatically uploaded up-to-date information about actual events, including by regions and topics, e.g. fires, floods, etc.; the information should be stored, analyzed, and accessible by time periods, e.g. weekly, monthly, yearly;

- the system should be open for inclusion of other sources of information, as well as for making comparative analyses;
- the system should also include addresses of local, national, and European structures responsible for making of forecasts or for actions in the case of natural disasters.

In this presented above sense good opportunities are presented by:

- the European Directive 2007/02/EC setting the legal framework for the establishment and operation of an Infrastructure for Spatial Information in the European Community (INSPIRE), Directive 2003/98/EC on the re-use of public sector information and others;
- the creation of regional, and subsequently, European network of application servers for analyses and risk monitoring, which exchange data and information based on common standards and rules for exchange and processing and which can work as a super-computer when fed with particularly large amounts of data (Figure 23).

This can be developed jointly with several DG,s as DG ECHO, DG ENTR, DG JRC, under the Global Monitoring for Environment and Security (GMES) Program and the future realization of Global Earth Observation System of Systems (GEOSS).

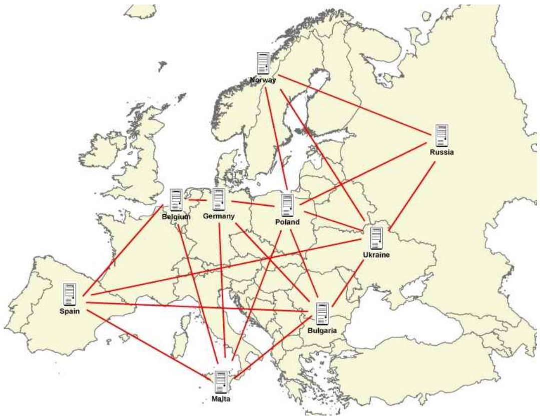


Figure 23. European network of application servers for analyses and risk monitoring

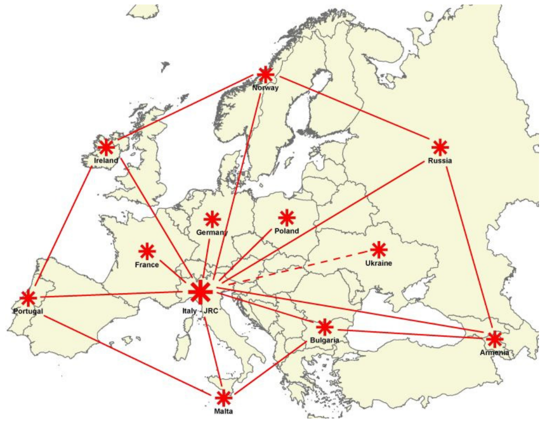


Figure 24. European network of regional units for risk and security management, land cover changes monitoring and data quality assurance

In close cooperation with the previous servers network, another regional network is needed to be developed – a network of regional cores (or units) for risk and security management as well as monitoring land cover changes and spatial data quality assurance, and subsequently, a European (or European-Mediterranean) network, also within the framework of the operational application of the GMES and the future GEOSS (Figure 24). The latest concept is very much open to the new tendencies and priorities in the EU 2020 strategy, as well as quality assurance (QA). It will take into account as well, the risk for the citizens, created by the ICT approaches and relevant technologies.