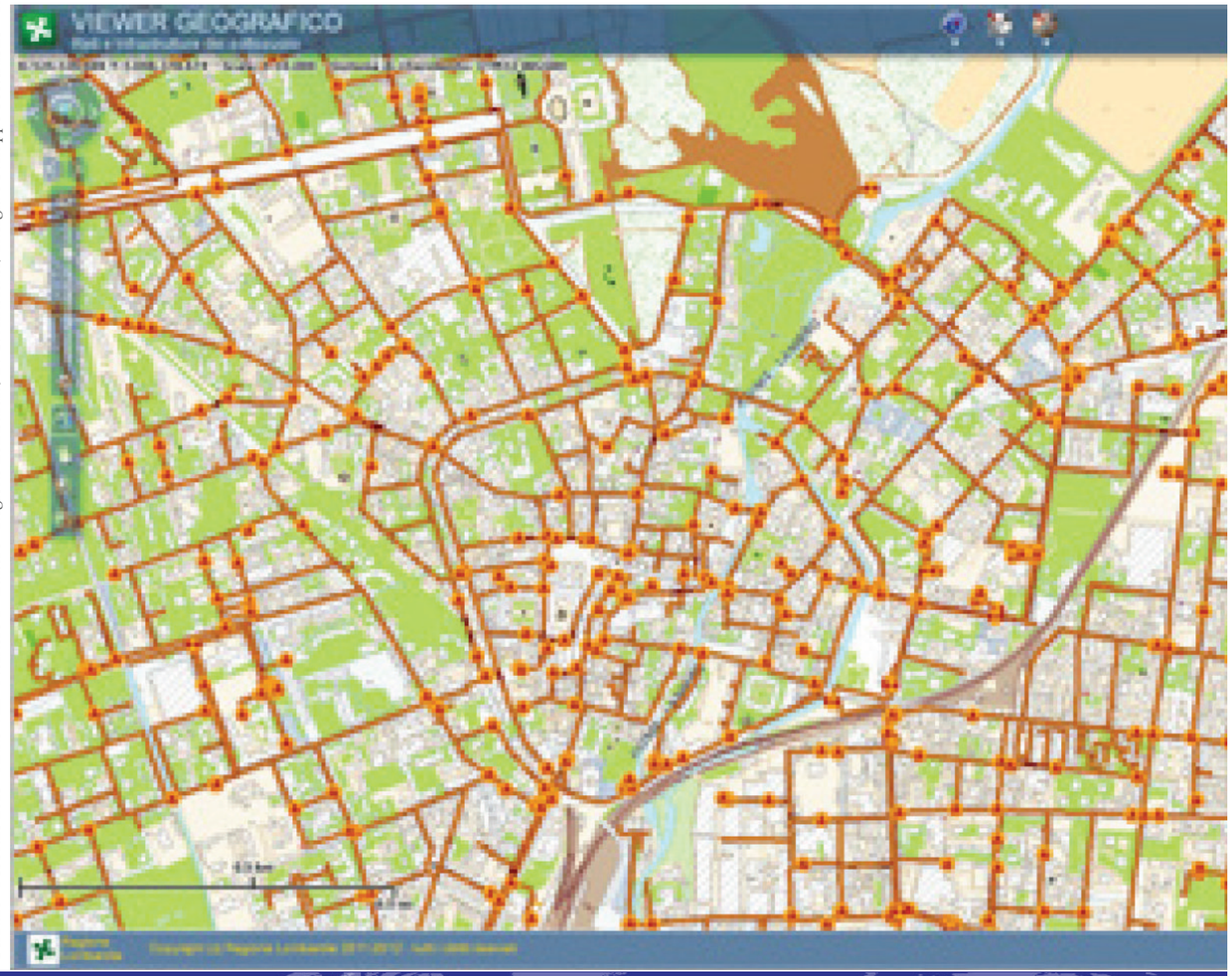
upsidedown
PROTECT

website: www.upsidedownprotect.eu
for contact info: info@upsidedownprotect.eu

Gennaio - Febbraio 2015 - Anno VIII - Numero 1 - Editore - Regione Lombardia, D. G. Ambiente, Energia e Sviluppo Sostenibile - Registrazione del Tribunale di Milano n.404 del 14/06/2006

UPSIDE DOWN

1/2015



upsidedown
because security matters

EDITORIAL

Editoriale

Rosella Bolis

The European project "Upsidedown protect" has shown that the infrastructure of water distribution is a fundamental asset for the development, safety and quality of life in industrialized countries, that have to worry about terrorist attacks.
We have to say that, because of its strategic nature, water has always been a target, even if the EU has formally excluded the water supply infrastructure with the Directive 114 of 2008 from the critical ones.
The comparison between the safety measures adopted by different member states and the results obtained from the simulation of a hypothetical terrorist attack to the water supply, have shown that systemic complexity of the infrastructure of water supply multiplies the threat's types.
The project has also made it clear that the protection of this strategic resource is also very complex, since the points of vulnerability of the system are numerous and widely spread over the territory.
Last but not least, there is also a growing IT component in the production and management of data that needs to be considered, both by water service operators and decision makers, as an additional aspect regarding hypothetical threat to cyber attacks.
In summary, the final "Upsidedown protect" conference brought to light the following final policy recommendations on four main topics:

1. **Awareness raising and knowledge sharing in the field of underground CI security:**
   - Identify and acknowledge the specificity of underground CI issues;
   - Raise awareness on underground CI issues;
   - Promote existing Best Practices and enhance knowledge sharing among stakeholders;
   - Increase knowledge and reinforce capacities of stakeholders in the field of secure underground CI.
2. **Incentives**
   - Propose new legislation/regulation in the field of underground CI;
   - Provide opportunities for funding;
   - Develop new certification standards
3. **Support the decision making for underground CI security**
   - Promote Public-Private stakeholders' collaboration;
   - Develop new tools to support the decision making process of stakeholders;
   - Provide Guidelines on all phases of the security implementation process
4. **Data sharing to address underground CI protection**
   - Promote the systematic collection of data related to underground systems;
   - Ensure and improve data security

From the topics outlined above it is clear that the EU needs to urgently revise the classification of critical infrastructure and add water systems into CIPS previsions.

Anno VII – Numero 3
Gennaio Febbraio 2015
Registrazione del Tribunale di Milano n. 404 del 14/06/2006

Publisher
Regione Lombardia
Direzione Generale Ambiente Energia e Sviluppo Sostenibile
Piazza Città di Lombardia, 1 – 20125 Milano

Direttore Editoriale
Andrea ZACCONE, Regione Lombardia

Direttore Responsabile
Roberto FIORENTINI, Regione Lombardia

Comitato di Redazione:
Sergio BIANCHI, Rosella BOLIS, Chiara DELL'ORTO, Maria LADU, Andrea ZACCONE

Design, layout and printing
Ledizioni
Via Alamanni 11
20141 Milano
Italia

On-line version available at:
http://www.upsidedownprotect.eu/

A questo numero hanno collaborato:
Rosella BOLIS, Sara BOUCHON, Sergio DE VITA, Chiara DELL'ORTO, Carmelo DI MAURO, Mateusz GRYGORUK, Calogero RAVENNA, Maciej STACHOWICZ, Franco VICO

THE INTEGRATED CYCLE OF WATER SUPPLY: AN EUROPEAN OVERVIEW

Calogero Ravenna*, Franco Vico** AMFM GIS Italia[1]

* C.Ravenna@asa.livorno.it
** franco.vico@polito.it

INTRODUCTION

The full title of Upsidedown project is "Spatial Data Protection for the Underground Critical Infrastructures". The emphasis on spatial data with respect to the security of underground infrastructures makes sense. In fact, to manage security effectively is essential to have good data on underground networks: reliable, up to date, but also interoperable and consistent. The last two attributes refer to the fact that there are several people who manage underground infrastructure networks (and in given contexts they are quite a huge number). Therefore spatial data are normally produced and managed by various subjects, but it is essential to effectively use together these data : they must be managed and delivered in formats that allow such joint use, i.e. spatial data must be interoperable. The inherent complexity of spatial data implies that the goal of interoperability is not trivial.

1 AMFM is a non profit association founded in 1990 whose purpose is to spread the culture of geographic information. Its members are national institutions, local authorities, geoICT SME, geo-technology providers, professionals, researchers.... Among its members there are some utility companies.

Consistency means that the geometric quality of data must be adequate and they shall be topologically correct: eg. if the water pipe (ignoring connections) runs underground, its cartographic representation must not intersect private spaces or buildings.
For the ordinary management of the networks but also for security management, data have to be shared between different operators and they have to be accessed quickly when needed: therefore data access is a matter to be managed very carefully; there are potential contradictions between the easy access and the protection of critical data.
As known, the focus of Upsidedown Protect project is the integrated water supply's cycle (which includes the water uptake and extraction, purification, treatment and distribution and the waste water collection, treatment and disposal.

THE SURVEY ON COMPANIES OF WATER SUPPLY'S CYCLE

In order to map how the issues of spatial data (data quality, details, accessibility, technical solutions and standards adopted…) and of security are handled in each companies, we developed four questionnaires : on the company, the water production and distribution, the waste water network, the laws and more relevant regulations.
These questionnaires were filled by "expert users" identified in different countries by the Project's National Contact Partners: they attended Expert User Groups held in different locations. Altogether the indicators identified were 87, that can be grouped into 4 groups:

- indicators on company's overall ICT technological level;
- indicators on geoICT technological level (production and management of spatial data);
- indicators on overall security;
- indicators on security of data.

A fifth group of indicators deals with company's and networks' size (extension and inhabitants of served area, company's employees, extension of networks, number of customers…)
Information collected by these questionnaires has been organized in a database: however this detailed information (at company level) has a character of confidentiality and in our opinion it should not be made public in an uncontrolled manner (any interested party may contact the authors of this paper).

THE COUNTRIES' REPORTS

The companies included in the survey, because of the method with which they were identified, are not a statistical sample: it is reasobnable to state that they are at least "good practices" even if not all of them may be labeled "best practice".

It should be noted that the sector of water supply's cycle is very complex: some companies are entirely public (sometimes of small size); the sector includes companies with highly differentiated size, technological level etc. and also legal status. The largest companies are very large and often publicly traded.

On the other side, the number of companies included in the survey is limited.

So, at some point, the need to complement this survey at company level with summaries at country level has become clear. In order to address this need experts for each country were identified and were asked to prepare a "Country Report". A common pattern for preparing these reports was defined: it includes seven sections (presented after).

We have to take into account that each report is a summary of very articulated processes, often uneven in the different parts of the same country. Therefore each of these country reports is a simplification, largely influenced by the experience of its author.

All "Country Reports" are available here [URL xxx.xxxxxx.xx].

However, the attempt to make comparisons at European level is unavoidable in a European project. Accordingly, for this purpose, the following table was produced.

In the following paragraphs the "titles" of the Country Reports' sections and some comments relating to the table are given.

The overall organization of water supply (columns 1-4 in the table)

The issues are: are companies mainly public, private public-owned or private? Are companies growing in size and in served area? There are processes of merger or establishment of holding companies? The situations and the trends are homogeneous across the country?

The table shows that in all countries (apart from Estonia) there is a presence of public providers, at national or city level.

The third column indicates the presence of private providers, public private partnership, or situations where the legal status of the provider is "private" (for example a limited company) but the property is in fact public since the shares are held by public bodies. For example in Italy the property of the companies must be public for at least 60% by law

Regarding the trends, we can highlight the following (column 4):

- A: companies are growing in size and in served area, merger of companies…;
- B: separation between ownership and service provider, a type of externalization;
- C: there is an ongoing process of centralization at state level. This is happening in one country only, Ireland. We know the situation of Ireland is very peculiar (see Ireland Country Report).

Laws and regulations (columns 5-7 in the table)

The question is: what are the most relevant existing laws and regulations at national and/or sub-national level and the main topics covered?

Laws and regulations are mainly at national level, only in one case they are only local, in 4 cases at both levels.

Laws and regulation concern (column 5):

- A: prices;
- B: quality and safety of water supply;

- C: sewage services;
- D: spatial data standards;

All countries have rules on quality and safety of water supply. The number of countries that have rule on prices is perhaps higher than you might suppose. Only a few countries have rule on spatial data standards.

Governance of the water supply cycle (columns 8-9)
The question is: are there agencies, institutions and other bodies at national and/or sub-national level in charge of managing or controlling the overall process or some its parts?
Obviously the governance issue arises only in the countries where a variety of subjects are operating. An authority at the local level is given only when there is a national authority as well.

Management of spatial data on water supply cycle's infrastructures (column 10)
The questions are: what kind of technologies and what formats are most used by companies for the collection and management of related spatial data? Different companies are likely to be using different technologies and manage data in different ways (CAD, GIS, paper maps…), what are the typical solutions in place? Are specific standards in place? Is the INSPIRE directive considered? Are there differences among various areas in the country?
Given options are (colums 10):
- A: geoDB whith structured DBMS:
- B: GIS data without structured DBMS (shape files…);
- C: CAD;
- D: no IT instruments are used.

Options are listed in a descending scale in relation of the technological development. Obviously in most countries various technologies at different level are simultaneously in use.

Spatial data on underground utilities integration (column 11-12)
The questions are: is there any body (public or private) in charge of the collection, integration and management of spatial data about the integrated water supply cycle on a specific area (sub-regional, regional, national)? With reference to the overlay and the integration of spatial data concerning all kind of underground infrastructure. i.e, is there any body (public or private) in charge of managing and maintaining what is sometimes called "cadastre" of all underground utilities?
The request makes a distinction between integration of the water network data and integration among data related to various underground infrastructures (likely managed by various bodies): the second issue is crucial for the management of significant interference between different networks. In several Country Reports this distinction has been little focused.
In most cases, the integration of the data is at the national level, in a few cases at the local level (regional or municipal), in one case at both levels.

Spatial data on underground utilities access (columns 13-14)
The first question is: who is allowed to access the spatial data on the integrated water supply cycle? Is there a security procedure in place to access these data?

Given options are (column 13):
- A: network data are basically secret information;
- B: for digging to assessed persons only;
- C: free access (apart explicitly classified data);
- D: clear definition of several permissions' level.

The second question is: taking into account the different existing parties and bodies that, at various levels, have to deal with underground infrastructure, is there a procedure for the secure exchange of information between private companies and public bodies?
Given options are (column 14):
- A: there are specific procedures defined in general;
- B: procedures are defined case by case.

1.2.7 Acts of vandalism and terrorism (column 15)
The questions are: are there records of serious act of vandalism or terrorist attack to the water supply underground infrastructure in your

COUNTRY	OVERALL ORGANIZATION				LAWS/REGULATIONS		
	Providers						
	Public at national level (1)	Public at municipal level (2)	PPP or private company (3)	Present trends (4)	Laws and regulation (5)	At national level (6)	At sub-national level (7)
Austria		x		B	B	x	-
Bulgaria	x	x		A	A-B-C	-	-
Cyprus	x			-	B-C	-	-
Czech Republic	x		x	B	A-B-C	x	x
Estonia			x	-	A-B-C	x	-
Francia		x	x	A-B	B	x	x
Finlandia		x		A	B	-	x
Greece	x	x		-	B	x	-
Ireland	x			C	B-D	x	-
Italy		x	x	A	B-C-D	x	x
Lithuania	x			A	A-B	x	-
Netherlands	x			-	B-C	x	x
Poland		x		-	B-D	x	-
Slovakia		x	x	-	B-C-D	x	-
Slovenia	x	x		-	B	x	-
Spain		x		-	A-B	x	-
Sweden		x	x	B	B-C	x	-
UK		x	x	B	A-B-C	x	-

COUNTRY	GOVERNANCE		MANAGEMENT OF SPATIAL DATA ON WATER SUPPLY CICLE'S INFRASTRUCTURES	SPATIAL DATA ON UNDERGROUND UTILITIES INTEGRATION ("CADASTRE")		SPATIAL DATA ON UNDERGROUND UTILITIES ACCESS		ACTS OF VANDALISM AND TERRORISM
	At national level (8)	At sub-national level (9)	(10)	At national level (11)	At sub-national level (12)	Who is allowed (13)	Secure data exchange procedures (14)	(15)
Austria	x	x	A-B-C-D	-	-	-	B	-
Bulgaria	x	x	-	-	x	-	-	-
Cyprus	x	-	-	x	-	-	-	-
Czech Republic	-	-	B-C-D	x	-	-	-	-
Estonia	-	-	B-C	-	-	-	-	-
Francia	x	x	B-C	x	-	B	B	C
Finlandia	-	-	B-C	-	-	-	-	-
Greece	x	x	B	x	-	-	-	-
Ireland	-	-	B	x	-	D	-	-
Italy	x	x	A-B-C-D	-	x	D-B	A	-
Lithuania	-	-	B-C	-	-	A	B	-
Netherlands	-	-	A-B-C	x	-	D	A	-
Poland	-	-	B-C	x	x	C	B	-
Slovakia	x	-	B-C	x	-	-	B	-
Slovenia	x	x	B	x	-	C	B	-
Spain	-	-	B-C	x	-	B	B	-
Sweden	-	-	A-B-C	-	x	A- B	A	-
UK	-	-	B	x	-	-	B	-

(with the contribution of Rosella Bolis , [Regione Lombardia] and Chiara Dell'Orto [Fondazione Lombardia per l'Ambiente])

country? If yes, what happened, when, what pollutant was involved, consequences?
Given options are (column 15):

- A: serious acts of terrorism were reported;
- B: serious acts of vandalism were reported (thefts of materials are not included);
- C: security regulations prevent communicating this information.

This information comes from the memory of the report's author, or was collected by consulting newspapers and by Internet searches. No real acts of terrorism or vandalism with serious consequences are reported. Some minor vandalism are reported and, often and widely, theft (of manholes and other materials).
Where the acts of vandalism and theft are registered with more accuracy (e.g. in Sweden) you obviously could have a perception of less security.
Significant recent actions to increase security are mentioned in some countries.

SOME FINAL REMARKS

It has been extremely difficult to outline, in the Overview Table, overall operating procedures of various companies and bodies, and trends in the various countries. A wide variety of behaviors, even within the same country, has emerged, to the point that it was difficult to summarize all in few options. Perhaps the options considered in the table, that have been identified through the comparative reading of Country Reports, are the most interesting part of the table itself, which seeks to provide an overall picture, to grasp what are the prevailing trends, to stimulate reflection.

We can see that a common tendency is the aggregation in groups of companies and the establishment of holdings companies that are conscious that they can not define their optimal management models without information systems that enables them to communicate with the various actors in their territory.
Connections between different operators and public authorities and other bodies, are more and more important and need to become easier and more robust to increase efficiency and effectiveness of the overall system, in view of the proper use and preservation of water resources.
If these are the trends (identification of shared data models, linked or federated databases, common procedures among various public and private bodies operating in the same territory), we must think about the nature of the security of data and information concerning the provision of water services, correctlyidentified as a common vital asset.

THE CADASTRE OF UNDERGROUND INFRASTRUCTURE NETWORKS: THE MODEL OF LOMBARDY REGION

Rosella Bolis*, Chiara Dell'Orto**

*Regione Lombardia, **Lombardy Foundation for the Environment

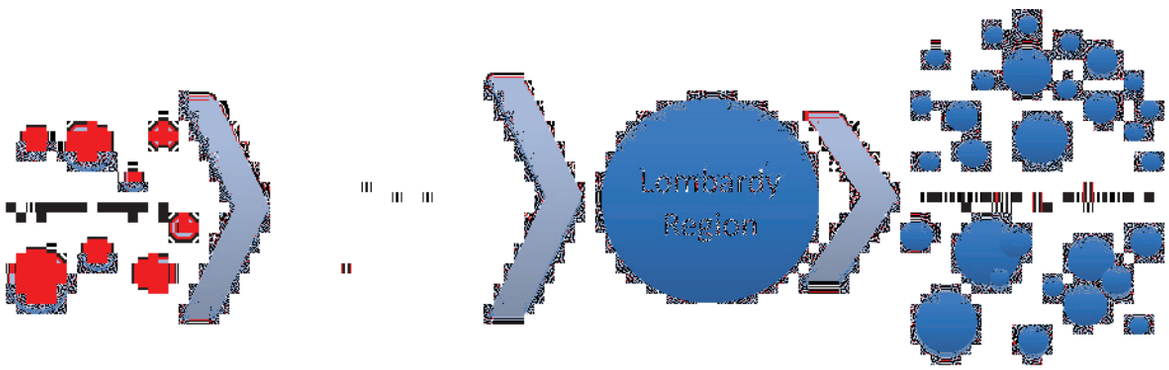
In a very heterogeneous situation as the Italian one regarding underground management, Lombardy Region stands out with the Law of 12 December 2003 n. 26 *Management of local services of public interest. Rules on waste management, energy, use of underground and water resources* that governs the use of the subsoil, planning the creation of a geographical database related to all the networks and infrastructure in its territory.

At the European level, in 2007, the INSPIRE directive, with its principles of accessibility, sharing and interoperability of geographic information at different levels, gives a new focus on the importance of structuring homogeneous territorial databases to govern the development and the planning of the territory in all its forms (environmental, infrastructure, urban planning, etc.)

But it is only with the regional law n. 7 dated 18 April 2012, " *Procedures for economic*

development and occupation "that for the first time, in Lombardy, is established the legal framework for the creation of the underground Cadastre.

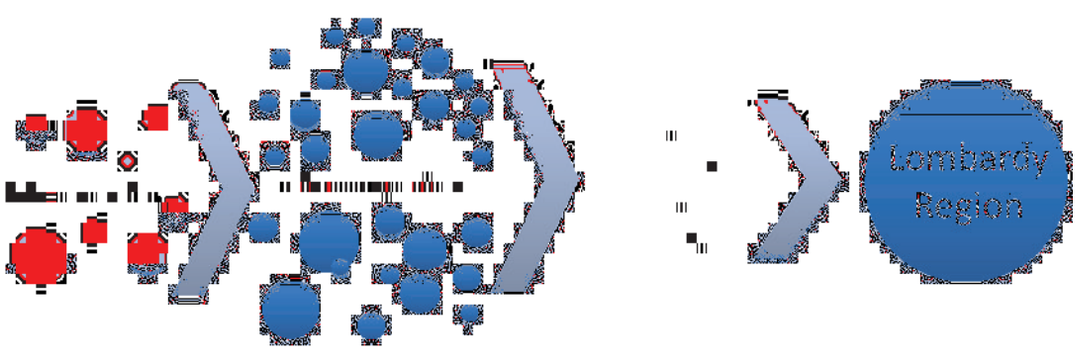
is also to consider the significant impact that might derive from a more punctual and reliable underground interventions programming and planning. Last but not least, is the opportunity



The Underground Cadastre, as defined by the Act, is configured not only as a tool to catalogue the underground infrastructures but also as the set of tables, maps, planimetry and related documents, (in electronic format and with geographical references), suitable to represent:

to know the exact value of each network in terms of ownership, management and service delivery.

While creating the Cadastre of underground infrastructure networks, the Lombardy Region has provided the enactment technical standards



- the stratigraphy of the soil and subsoil;
- location and dimension of infrastructures for the distribution of public services
- attributes related to the property, the management of the the underground infrastructure and the service delivery.

In view of the benefits that a knowledge instrument of this type may be for policy-makers, both in terms of the investments to be made and for a better use of resources, there

and mapping specifications. With the aim of facilitating; the exchange of geographical information between the involved parties. As early as the year 2005, technical specifications for surveying and mapping underground service networks have been enacted. The last upgrade of the technical specifications (April 2014), took into account the experiences made by municipalities and the stakeholders involved in the first step of the implementation of the Underground Cadastre.

The Cadastre of underground infrastructure networks should in fact be managed at a local level (municipality), and implemented, step by step, by the entities that own or operate infrastructures in the subsoil. In particular, these are the possible information flows:

Actual Governance Model

1. The stakeholders transmit to the city governments the underground geographical data they are responsible for. Data are organized according to regional standards;

and legal, related to its implementation. Lombardy Region has addressed this issue since a long time making use of the case analysis, both through direct experiences and pilot projects. From the close observation and listening of the territory has emerged that the data retrieval by municipalities is the passage that hinders further planning.
Taking this into account, in 2014, an alternative to the current information flow was planned. Before, were the municipalities that had the task to speak with the operators for finding

2. City governments organize a local GIS (Geographic Information System) of the underground networks, integrating all the information located in the municipal area;
3. City governments share their local GIS with Lombardy Region that integrates them into a single Geographical webgis portal.

The legislation therefore assigns a central role to the city goverments, providing that the local underground Cadastres will contribute to the creation of a single regional underground cadastre in the pursuit of a wide territorial scope.
However, there are many issues, both technical

data; now, it's Lombardy Region that is in charge of receiving data by the operators making them available on the Geographical webgis portal, for the interchange of cartographic information.

Future Governance Model

An important consideration in the making of and Underground Cadastre, and of a geographic database in general, is related to its updating process. The Underground Cadastre, according to the meanings mentioned above, is useful only if constant and continuous updating procedures are defined upfront. In this regard, the Lombardy

Region planned annual updates, from the main operators, in order to implement in the database the "as built" arising from their new infrastructure construction.
In compliance to the principles of INSPIRE and the logic of OPEN DATA, Lombardy Region has implemented the Underground Cadastre in the Geographical webgis portal, allowing anyone free access to the database according to different permission levels. The operator is thus enabled, before making an excavation, to get the information with a level of detail needed to assess any interference in the intervention. The freelancer will instead see the networks and assess the presence of certain services in the "design phase" located in the urban area.

has prepared a dedicated application for the transmission of PUGSS (General Urban plan of underground services) and related databases. By registering to the "*Multiplan application*", each city government can send documents about their management plan for the underground services simply by uploading documents. Lombardy Region then takes charge of the uploaded material and, after verification, will make it publicly available.

Screenshot of Multiplan Application

As already mentioned, also the cartographic component relative to the positioning of the underground networks, better defined as "Cadastre", has been implemented in a special section of the *Multiplan application*. In this

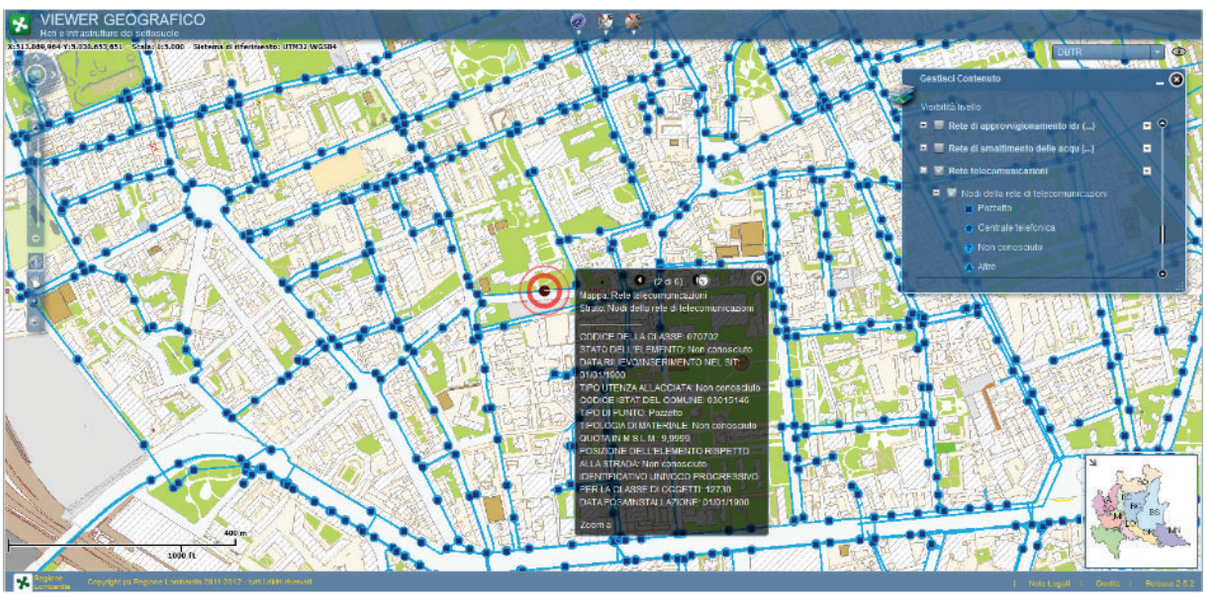
Stored data covers all types of underground utility assets: different layers for water supply, waste water, power supply, gas network, district heating and telecommunications. Each network has a different mode of representation both in colour and symbology

Free access to information, the creation of Web Map Service (WMS) or Web Feature Service (WFS) are the first step towards the development of a cloud-based system that makes interoperability between different databases his real strength.
Lombardy Region, operating according to a logic of subsidiarity for public entities and operators

section local authorities, managers and citizens can access with different permissions. Citizens for example, will have the sole privilege of viewing maps for specific geographic scale ranges.
The managers instead will have the permission to view the information relating to their own databases in its entirety and with a minimum

level of detail those of other operators. In this way, the tool provides the chance to view and manage as best as possible the problem of the connections between interfering networks. Local authorities are finally able to view all the geographic information and databases associated with networks present in its territory. All cartographic databases that service providers transfer to the Lombardy Region are homogeneous in format (shapefile) and content.

As mentioned before, the Lombardy Region has prepared detailed technical specifications for mapping and surveying technological networks in order to ensure uniformity and standardization of content associated with that type of information. The set of all these instrument testifies that the Lombardy Region operates in line principles of interoperability, accessibility and sharing of information typical of the INSPIRE directive.



Informations contained in the database are related to: location, size, date of installation or survey, infrastructure material, pressure, state of use of each individual networks. Data are geo-referenced and uniquely coded to standard specifications

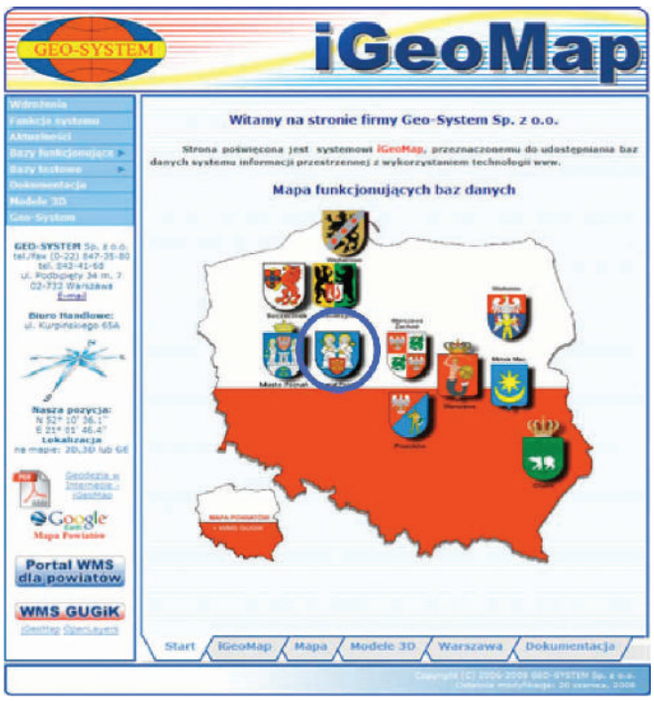
MANAGEMENT OF GEOGRAPHICS INFORMATION RELATING TO SUBSOIL NETWORKS: THE CASE OF POLAND

Maciej Stachowicz, M.Sc., Eng.; Mateusz Grygoruk, Ph.D.

INTRODUCTION

The system of spatial Administration in Poland is divided into *Regions-Voivodeships*; *Sub-regions-Poviats*; and *Local authorities-Comunes*.

In Poland, systems used for collection and management of spatial data related to water, and in general to all types of underground infrastructure,



are generally homogenous in the country scale and stored in well described and indexed formats. Institutions responsible for the storage and management of the spatial data are ***Poviat Centres of Geodetic and Cartographic Information (PODGIK)***.

PODGIKs store and prepare the data. This is a result from harmonized geodetic, cartographic and construction laws and regulations operating invariably for many years. Requirement of this laws is the mapping of all built building and infrastructure before put to use. Many years of this practice caused that Polish infrastructure is known in 98-99%.

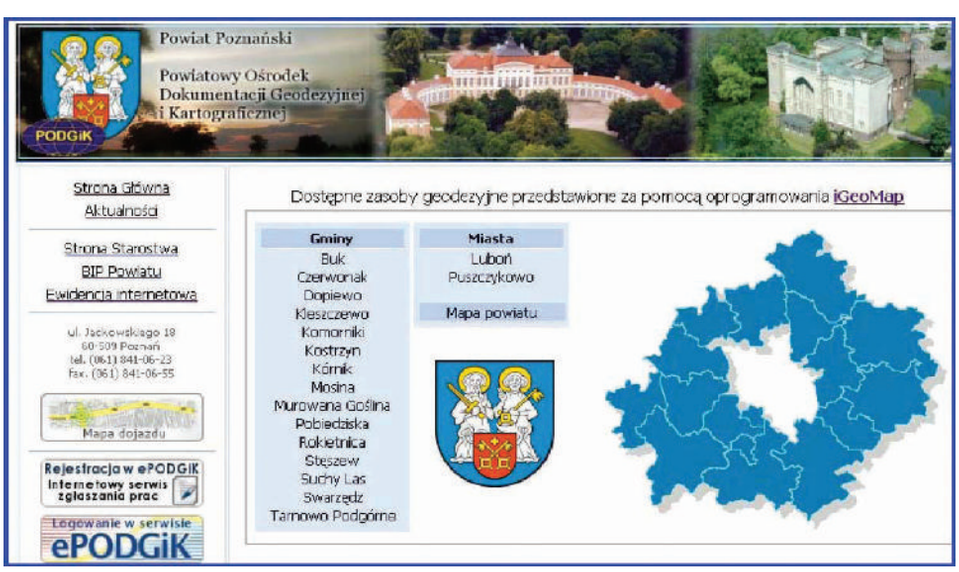
Although not all the maps are available in a vector format, for nearly all of the underground installations in Poland one can obtain information on:

- spatial geometry,
- types of installations,
- features of installations with differentiation of the type of measurement (estimation) which was the base for the classification of particular installation (e.g. if there is a given information about the diameter and elevation of the pipe); additional information about this object allows to identify, whether the measurements of these parameters were done with the detector of pipes, georadar, total station, GPS, levelling or if the data was obtained directly from the company/subcontractor responsible for the design and maintenance of particular installation (pipe, set of pipes).
- diameter,
- depth,
- slope of the pipe.

METHODOLOGY OF MANAGING AND ARCHIVE SPATIAL DATA

1. *Paper maps* – Many years of practice caused that archives of paper maps, on this moment, are biggest and most accurate source of geodetic knowledge about underground infrastructure.
2. *CAD* – at the present time, most of paper maps was moved or are moved to their electronic equivalent. Dominant in this case is CAD software, which allows for easier changing and archive of geodetic and cartographical data of underground infrastructure.
3. *Geo-database* – generally in Poland there aren't centralized geo-databases holding global (in Country aspect) knowledge of underground infrastructure. In Poland there is a diversified system based on district local institutions PODGIKs (called District Centers Geodetic and Cartographic Documentation). They are gathering all information and data about underground infrastructure (it is one of the tasks of this institution) from whole district. In theirs archives are stored all paper maps and electronic data (CAD) of all infrastructure

Approximately 95-99% of spatial data regarding underground infrastructure including water supply and wastewater is stored in the public units under the national jurisdiction: the so called PODGIKs. The data are spatially integrated (refer to standardized cartographic reference systems) and topologically correct. Majority of installations, before they are constructed, require "permissions for construction". Every issue, which construction is legally covered by the "permissions of construction",



requires detailed geodetic measurements once the construction process is finished, before the issues are passed to be used. Every measurement of the building, installation or any issue subjected to "permissions for construction" must be reported to the local relevant PODGIK. Therefore, PODGIKs store all the spatial data. Moreover, the data stored in PODGIKs are of acceptable accuracy, as they can only be measured and verified by skilled and nationally approved geodesists.

In Poland units responsible for gathering, managing and archive of spatial data about integrated water supply system are:

1. Local

a) Water supply and sewage companies – particular companies manage spatial data regarding the networks and devices they manage and maintain.
b) PODGIKs – complete information for all underground infrastructure for whole district area and in some cases multiregional.

2. National/country

a) Government institutions for the Crisis Management – only necessary information for crisis managing
b) Higher instance geodetic units - mostly multiregional infrastructure data

The data is in public domain and can be accessed by anyone. The procedure is the following:

– to report to PODGIK the need to obtain the data from particular region (city, district, commune)
– the data are prepared in the form of a "base map" in the scales 1:500; 1:1000, 1:2000, as required and requested.
– if the applicant is wishing to use the map in purposes of construction of the issue, for which the "permission for construction" is required, once the construction is finished the applicant is ought to hire a geodesist, who has to measure the newly constructed issues.
– newly constructed issues, once measured, are put on the maps in PODGIK. Therefore, the situation presented at these maps is continuously renewed.

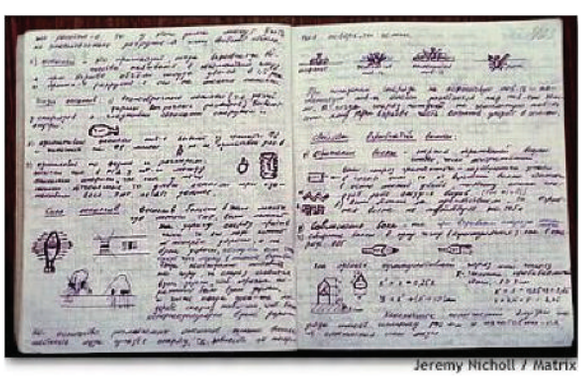
There is no particular security procedure assuring the safety of data. Anybody can access the data. Although the clear track of data users is known (people wishing to get the data from public cadaster in PODGIKs are registered and it is generally known who is using the data) the further exchange of data obtained from PODGIKs is not a subject to any data security procedures and data exchange limitations. There is no specific procedure of data exchange between the private companies and public institutions storing the data. The only regulation is that every issue constructed in the procedure of "permission for construction" requires to be measured and the measurement data (e.g. pipe elevations, diameters, depths, slopes) are obligatory transferred to PODGIKs. If the data was not transferred to PODGIK then it is not possible to obtain the permission to use the newly constructed buildings and installations.

A NEW PROFESSIONAL PROFILE: EXPERT IN SECURITY MANAGEMENT FOR WATER UTILITIES

Sergio De Vita*

*President of Agenfor Italia

INTRODUCTION



The so called Manual of Manchester

The "Islamic" terror threat to attack American's water supply is almost as old as 9/11 and may be used as a means to start the bio-terror pandemic a night mare of the International security community. Information that Al Qaeda plans to attack the U.S. water supply and kill millions evidently started around July 30, 2002, when it was reported that U.S. authorities arrested an Al Qaeda suspect who had planned to poison U.S. water supplies[1]. A year later on May 28, 2003, it was reported that Al Qaeda again threatened to poison the U.S. water supply[2].

Four years later on April 27, 2007, it was reported that an Al-Qaeda chief planned to poison Britain's water supply[3]. A couple years later on February 11, 2009, a report stated that the FBI had released bulletin warning that Al Qaeda might try to poison water supplies by use two naturally occurring toxins: nicotine and solanine. Roughly two years later on August 20, 2011, it was reported that an Al Qaeda suspect had "plotted to poison water"[4]. On May 9, 2013, it was reported that an alleged Tunisian Muslim in Canada had plotted to poison the water supply of a large Canadian city with bacteria in order to kill up to 100,000 people. Two weeks later on May 25, 2013, it was reported that an Israeli official stated that Syria hackers tried to access Haifa's water system[5] in failed cyberattack. Yitzhak Ben Yisrael, Israel's former cyber security adviser, said that a group calling itself "The Syrian Electronic Army" had launched the failed attack.

The black year was certainly 2013, when between April and June in the US alone there have been 27 accidents to well water systems, although mostly minor. Europe lacks a systemic and accurate reporting as the American, that can work as the basis of risk analysis on technical grounds. So it is very difficult to propose statistics.

What is certain though is that 2015 did not begin under a good moon. In fact, on 11 January 2015 Al Adnani, the official spokesman of ISIS, the organization that is leading guerilla actions in the Middle East and North Africa, has asked dormant jihadists in Europe to carry out attacks in response to the actions of the Coalition in Syria and Iraq. With the video posted on Youtube, Al Adnani goes for the first time into detail on how to attack the West. Among others, we've to worry about Al Adnani tips to attack the water systems with poisons

TRAINING AS A RESPONSE TO SECURITY NEEDS

The UPSIDEDOWN project found that these types of attacks are possible, contrary to what is often supported by the water cycle experts. Indeed, they are likely to happen, considering the ease with which in some cases they can be performed because of the vulnerability of networks.

Hence the urgency, alongside that of raising the barriers of access to water systems, to raise the level of awareness and knowledge about the problem at the level of utility, security agencies and public bodies, as well as private individuals. To this end, the research team of Agenfor, an

1 http://www.foxnews.com/story/2002/07/30/feds-arrest-al-qaeda-suspects-with-plans-to-poison-water-supplies/
2 http://www.washingtontimes.com/news/2003/may/28/20030528-102548-4938r/?page=all
3 http://www.thesundaytimes.co.uk/sto/news/uk_news/article63891.ece
4 http://www.cbsnews.com/news/fbi-al-qaeda-might-use-poison/
5 http://www.foxnews.com/world/2013/05/25/israeli-official-says-syria-hackers-tried-to-access-haifa-water-system-in/

2013, THE BLACK YEAR FOR WATER ACCIDENTS

accredited institution in the Region of Lombardy, Emilia-Romagna, Veneto and Sardinia for the design of specialized training processes, has designed a new profession of "Expert Security Services in Water Utility".
This professional figure was then tested through two international training events in Ljubljana and in Milan, with the participation of international faculty and students The objective was to validate, through field experience, the elements of research emerged from the experimentation of UPSIDEDOWN, building a coherent framework of skills, knowledge and abilities now missing in the training market.
Through a comparative analysis conducted by the European Research Group UPSIDEDOWN, Agenfor detected as in most European utilities figures of technical safety are present in many contexts, but dedicated figure of managerial level able to develope a comprehensive and integrated threats are absent. The professionals in existence today, in large part coming from the police, are for unskilled personnel involved in the case of buildings, plant and equipment. The model of good practice identified, however, is that of a managerial figure capable of integrating the various systems, both internal and external to the company. In short, a Swedish model transported on the shores of the Mediterranean and transferable across Europe.
The result is the design of a new professional of managerial level, contributing to design, implement and protect the security of water infrastructure in their integrated cycle, in terms of business continuity, safeguarding production and guarantee social services provided, in infrastructure protection and the reputation of the companies that manage the service and welfare of the citizens who use the water for domestic, industrial, agricultural uses or other.
In this context, the Expert Security Services in Utility designs the plan for Security Operators (PSO) of the critical infrastructure, plans maintenance and coordination of safety initiatives in agreement with police business and community services to it MPs and civil protection, manages the prevention indicators and models of intervening in situations of alarm and verifies management PSO through appropriate measures to monitor, control and exercise.

CONTEXTUAL ELEMENTS AND TRAINING PLAN

The Expert Security Services in the Water Utility may operate or as an employee / consultant of SAs external or as a direct employee of the Utility itself. In the first case, these innovative professionals work as supervisors by private security, for which case in order to operate they must have a license issued annually by the Prefecture of the province in which they operate. For employees, however, the contractual framework and framing is given by the national labor contract and the job description of individual utilities. For the purposes of proper activity, however, it is necessary for both contexts to satisfy the requirements of Article. 134 of the Consolidated Laws of Public Safety and demonstrate, with each document considered appropriate (eg curriculum vitae, previous work experience),

to possess the technical capacity to services that wishes.

BASIC SKILLS

Basic knowledge

- Elements of law and applied criminology
- Elements of computer security
- Legislation on private security
- Statement of protecting the health and safety of workers in all sectors of private or public activity
- International Standards: ISO 31000: 2009, HB167: 2006 Security and Risk Management, AS 3745-2002 / 1-2004 Amdt and other reference standard
- be able to design and transmit procedures and standards of corporate security: Armament and equipment, Fundamentals of shooting, Notions behavior in the presence of suspicious elements, techniques of passive defense, techniques of personnel profiling consistent with the privacy policy, terms of annual training
- Regulations relating to the regulatory framework and management utilities
- Regulatory basic techniques relating to the management of the water cycle, its equipment for the collection, distribution and disposal
- Knowledge of the technological base of the integrated water system, with particular attention to the interrelationships between the cybernetic parties and the hardware ones.

Ability

- Knowing how to interpret their role as part of the company structure
- Apply and be able to communicate and trans-

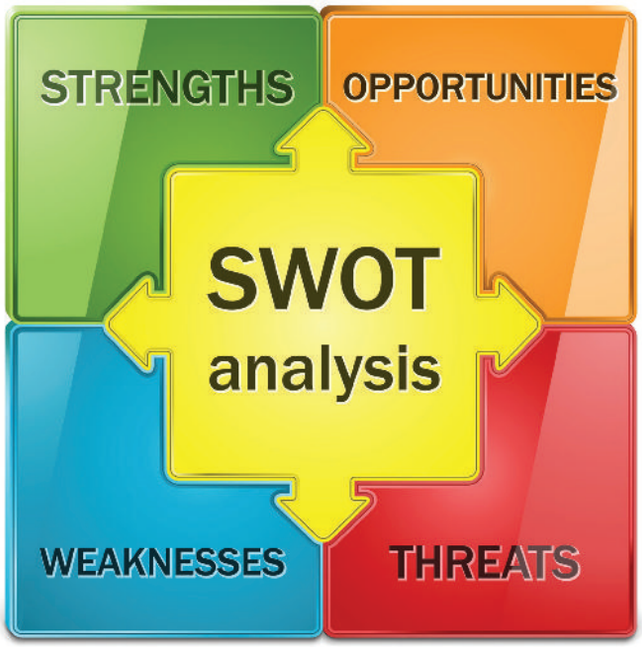
mit properly to security guards the protocols for the oversight personnel
- Apply and be able to communicate and transmit properly to security guards the pattern of use of Armaments and Equipment allowed
- Apply and be able to communicate and transmit properly to employees (of) the utility protocols for emergency management
- To Apply and be able to communicate and transmit properly to security guards the defense techniques
- Apply and be able to communicate and transmit properly to security guards the techniques of disarmament
- Apply and be able to communicate and transmit properly to security guards the safe driving techniques
- Apply and be able to communicate and transmit properly to employees of the utility techniques emergency surgery and broke
- Apply and be able to communicate and transmit properly to employees of utility intervention techniques in security
- Apply and be able to communicate and transmit properly security officers surveillance techniques
- Apply and be able to communicate and transmit properly security officers transfer techniques motorized
- Apply and be able to communicate and transmit properly security officers techniques for passive defense of property and facilities
- Apply and be able to communicate and transmit properly security officers practical techniques of close protection
- Apply and be able to communicate and transmit properly security officers techniques and regulations regarding the use of firearms
- Apply and be able to communicate and transmit properly to the security personnel

management software for the management of alarm procedures
- Use and know how to apply the relevant legislation relating to their professional profile within the company
- Use and to interpret for safety technical diagrams, cartography and maps plant related to integrated water cycle

SKILLS: Designing and Planning the PSO knowledge
- Know the principles of risk analysis (RVA Risk and Vulnerability Analysis) applied to the water cycle and be able to classify threats against indicators and scalar analysis of the damage
- Know the principles and techniques for the allocation of risk objectives, individual and collective, based on scales of damage defined by the company management, according to the general principles of corporate governance, private and public (regulations, budget, requirements, etc .)
- To know and to apply the principles, techniques and technologies of physical surveillance, remote and cybersecurity applied to the water cycle in its complexity
- Knowing how to find and manage the information needed to build risk indicators and forward them to the staff as managerial, technical and operational company.
- Know how to manage plans for classification of information
- Know the principles and methods governing the definition of security plans to protect persons (IRPA, LTIF, PLL, FAR, IR), networks and collective goods in critical infrastructures water
- Know and be able to choose the matrices of risk assessment processes integrated water cycle, building indicators (EWS) shared with the rest of the company
- Knowing how to design the Safety Plan for Operators (PSO)
- Know how to test the level of application of the PSO and the emergence of more and new risks also through the provision of security drills and tests of resistance / resilience of systems and services
- Knowing how to communicate the specific objectives of the PSO to each segment of the company
- Know and know coordinate the regional system of security and civil protection

Ability
- Apply principles and techniques of analysis of the need for security, even with the help of all segments of the company, each at their own level
- Assign tasks to individual and collective functions of the company involved in the security plan, monitoring the level of adjustment over time with respect to performance indicators defined
- Apply appropriate measures to Identify, Prevent and Counteract risks, on the basis of specific analyzes and decisions taken by bodies competent under the scales of risk.
- Apply and enforce the PSO, checking the indicators of effectiveness, strength and resilience of the systems compared to the various types of emerging threats
- Ability to Design, Implementation and Managing techniques predisposition PSO also respect the general safety at the local level, knowing how to coordinate with security forces and SAs external companies.
- Apply security measures best suited for the prevention and response to emergencies through the mobilization of internal resources: identification of vital resources and time to reboot the system, identification of replacement systems, emergency management and management of redundant processes.
- Apply the most appropriate technologies compared to PSO in the various segments of infrastructure protection
- Apply the operating procedures provided in the PSO according to the terms of the threat, knowing mobilize tangible and intangible resources provided by the plan and knowing

relate to the services of security and protection on the territory outside the utility
- Manage information according to standards of security classification
- Make exercise tests to check the levels of application of PSO, resistance and resilience of the systems as well as emergence of new potential vulnerabilities unknown in the phase of preliminary safety assessment
- Plan and manage, through the offices dedicated to it, the internal and external communications company with regard to security issues. The training project, at a later stage, will be brought to the attention of the competent bodies of vocational training at regional level, in order to obtain the inclusion of this new managerial figure in the professional standards of the various regions. The eventual accreditation of the professional favor, among other things, the integration of water services utility and the results of monitoring, as well as greater coordination of internal services of companies and prevention activities carried out by the forces of the risk security in the territory. The model is that of Sweden, that the project UPSIDEDOWN identified as a good practice. But you know, make Rome a new Stockholm is not the easiest thing in the world.



POLICY RECOMMENDATIONS

di Sara Bouchon e Carmelo Di Mauro

Risk Governance Solutions S.r.l.

METHODOLOGICAL APPROACH

(a) SWOT Analysis

The SWOT Analysis is a useful technique for understanding Strengths and Weaknesses, and for identifying both the Opportunities open and the Threats that need to be faced. Strengths and weaknesses are often internal to an organization, while opportunities and threats generally relate to external factors. Strengths and oppor-

tunities are related to positive aspect that can contribute to reach the final objective. Instead, weaknesses and threats can encumber it. The SWOT analysis can help to describe common opportunities to be exploited or constraints that have be taken into account. By understanding the weaknesses identified by each category

(b) Stakeholders' workshop

Question 1-What type of protection strategy for underground infrastructures (UI) can be developed at Local and Regional level?

Question 2-How to decrease or mitigate the impacts and cascading consequences of potential UI disruption?

stakeholder, it could be possible to define policy recommendations that eliminate threats that would otherwise impact the future application and exploitation. The purpose of performing a SWOT is to reveal positive forces that work together and potential problems that need to be addressed or at least recognized.

Question 3-How to promote the **harmonization of data management** related to UI and the data security?

Question 4-How to steer the **data sharing process** and the **collaboration** between stakeholders in particular the collaboration between public and private actors?

STAKEHOLDERS' INPUTS

The inputs provided by the stakeholders in answer to the four questions are summarized in the following figures.

Figure 1 - Stakeholders' inputs to question 1

FINAL POLICY RECOMMENDATIONS

Based on stakeholders' inputs gathered during the final UPSIDE DOWN workshop, following policy recommendations and actions to be taken can be proposed.

(a) Awareness raising and knowledge sharing in the field of underground CI security

The main outputs of the UPSIDE DOWN Project, as well as the inputs from the stakeholders

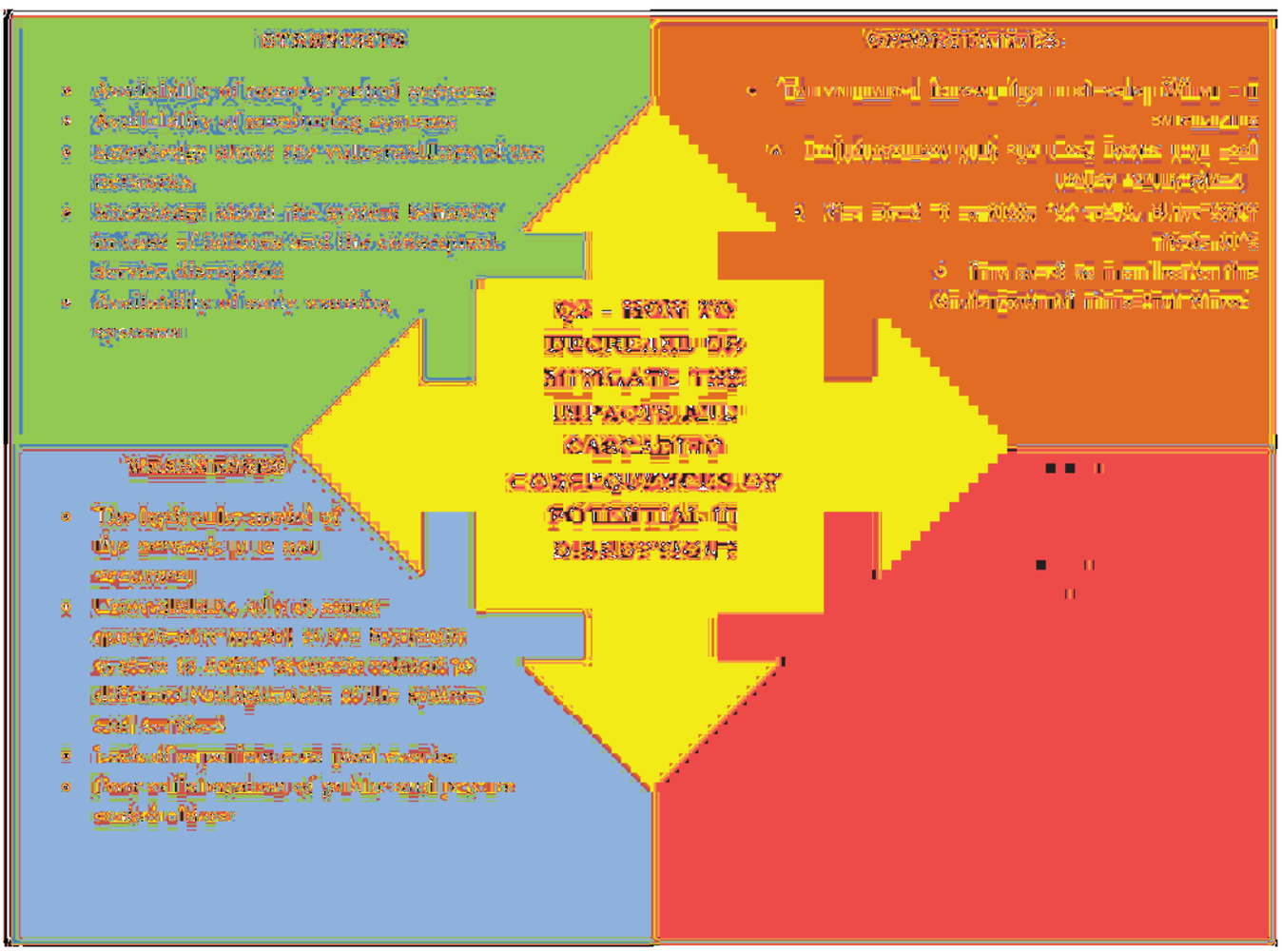


Figure 2 - Stakeholders' inputs to question 2

Figure 3 - Stakeholders' inputs to question 3

show that there is still a need to increase the awareness and knowledge on the protection, security and resilience of underground infrastructure systems. The objective of awareness raising is to develop the sense of urgency related to the need to address underground CI issues in relation to their security, protection and resilience. This includes the following actions

➢ *Identify and acknowledge the specificity of underground CI issues*

The issue of critical infrastructures protection and resilience is now acknowledged in Europe. Stakeholders responsible for the security of underground CI feel that the specificities of CI should also be emphasized. Although the protection aspects of underground CI are very similar to those for on the ground infrastructures, some issues are specific, e.g. the colocation of several infrastructure systems, the difficulty to access the systems, etc. With regards to security, this raises issues that cannot be addressed in a similar way. It would be thus necessary that at EU level, these specificities are recognised. For instance specific criteria to identify underground CI assets could be developed.

➢ *Raise awareness on underground CI issues*

Focusing policy on awareness raising activities will trigger a better understanding among stakeholders at all levels (EU, national, regional, local) of the issues to be addressed and of the potential added-value of getting involved in risk management activities with respect to the potential disruption of underground CI.

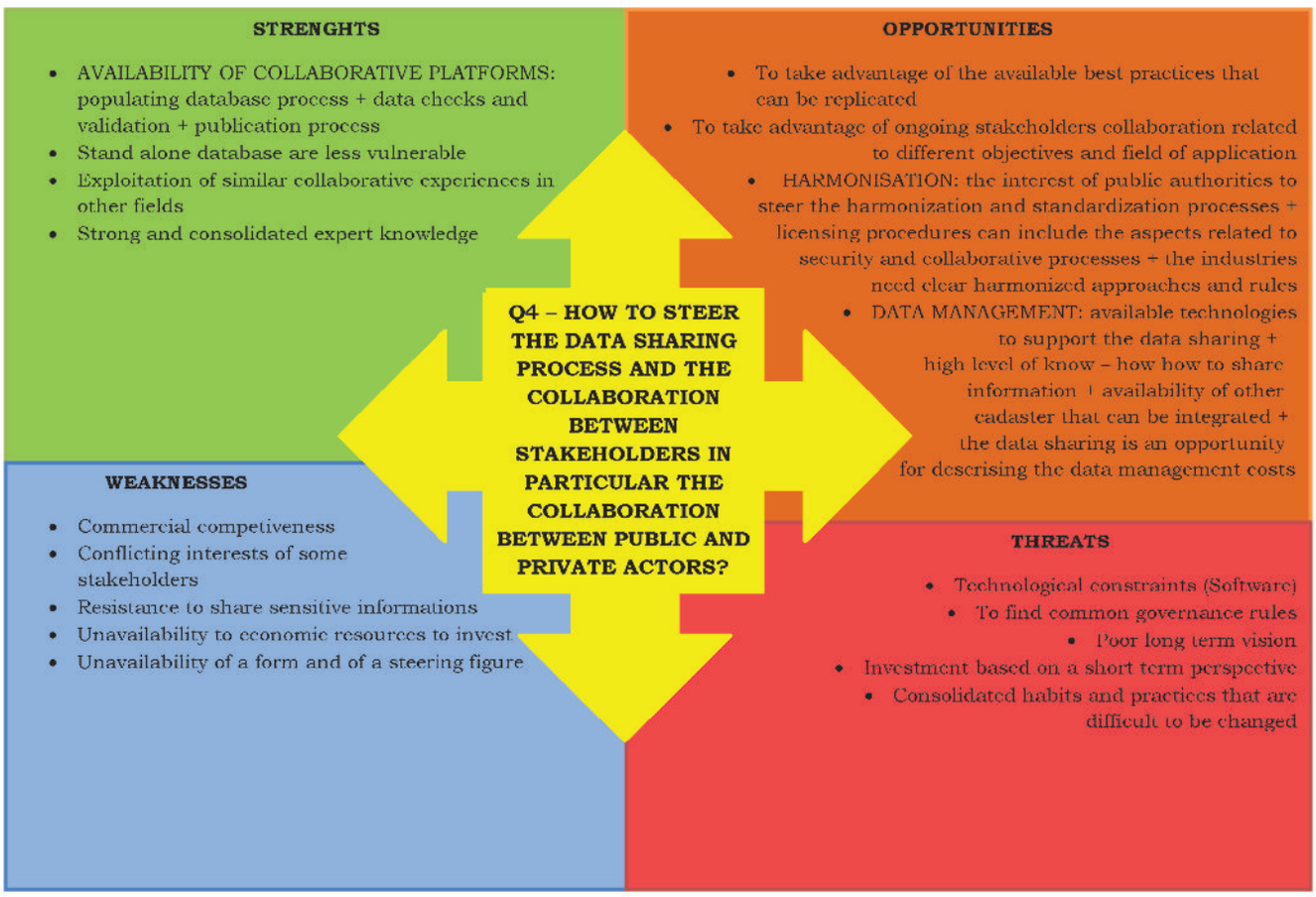


Figure 4 - Stakeholders' inputs to question 4

Targeted stakeholders for awareness raising are the authorities responsible for critical infrastructure protection/resilience or risk /disaster management activities, the operators of the different CI sectors concerned by underground sections of their systems. Other stakeholders such as the insurance companies, consumers' protection association who could be key actors in awareness-raising activities should also be taken into account. One action to be taken to increase awareness is for instance to set-up a systemic lessons learned mechanism after each event.

➢ *Promote existing Best Practices and enhance knowledge-sharing among stakeholders*

Stakeholders have reported the difficulty to concretely put into practice their objectives to increase the security level of their infrastructure. They are keen in learning, from others, similar cases. It is thus necessary to identify and promote best practices, to ensure the dissemination of this knowledge, to create contacts and create networks opportunities among stakeholders involved in addressing underground CI issues.

➢ *Increase knowledge and reinforce capacities of stakeholders in the field of secure underground CI*

Besides knowledge sharing opportunities, stakeholders have also emphasized the importance of improving their skills and capacities in the field of protecting underground CI. In particular training activities are seen as one of the most efficient way to achieve it. Training can focus on

testing the own emergency plans. It is also an excellent way to improve the cooperation and coordination with other stakeholders. Systemic feedbacks on lessons learned from training should also be reported.

(b) Incentives

Stakeholders have identified the need for more incentives to trigger a better involvement of all relevant actors in protection and security activities.

➢ *Propose new legislation/regulation in the field of underground CI*

Stakeholders' input was very much clear on the role legislation plays to trigger action in the field of security. Compliance with the legislation is seen as a very incentive way to invest in security and protection. Following stakeholders, it is important that the entire risk management/ protection or resilience aspects cycles could be taken into account in order to support a comprehensive approach to secure underground CI. One of the suggestions coming from stakeholders is that the EU could provide a more comprehensive framework of CI protection (including aspects related to risk or resilience management), while member States would adopt new policies.

➢ *Provide opportunities for funding*

Funding in research and innovation are an excellent way to support the development of new tools and strategies to increase the security level of underground CI. The visibility of underground CI issues could be enhanced if some topics or calls would focus specifically on them. For instance more accurate scientific methods are needed to assess the vulnerabilities and propagation of cascading failures within networks, such as hydraulic models.

➢ *Develop new certification standards*

Certification is commercially relevant for operators and can be seen as a trigger factor to improve existing protection and resilience practices. The definition of a certification based on standards related to underground CI security could be an efficient way to develop enhanced risk management practices. One example given by stakeholders was to associate licensing with compliance with standards.

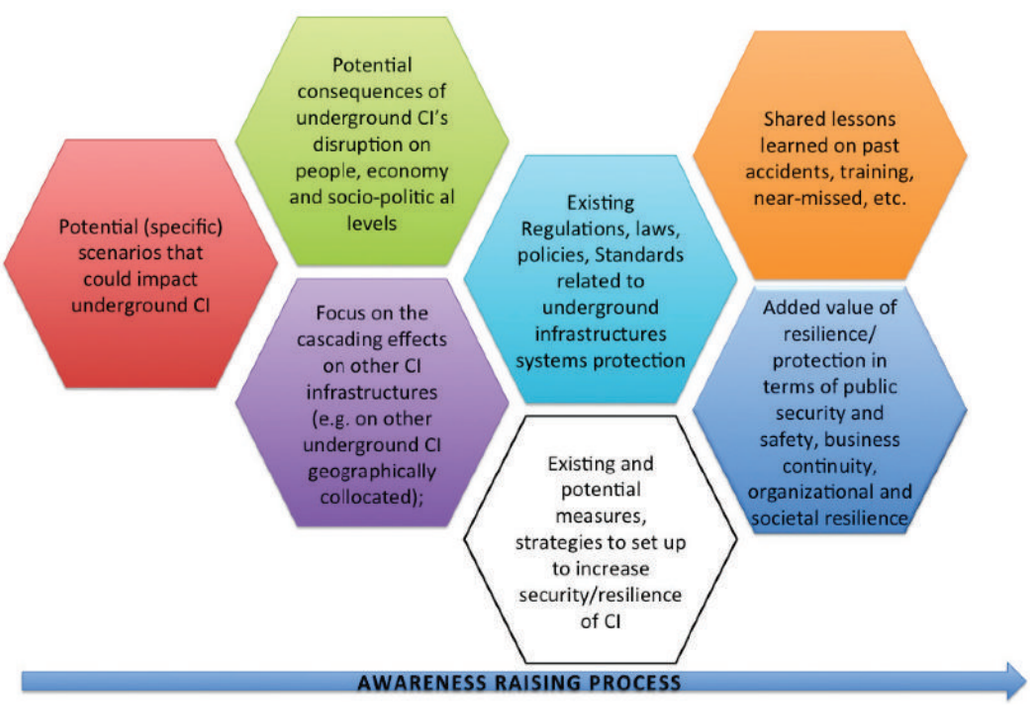


Figure 5 - Possible focus of awareness raising actions

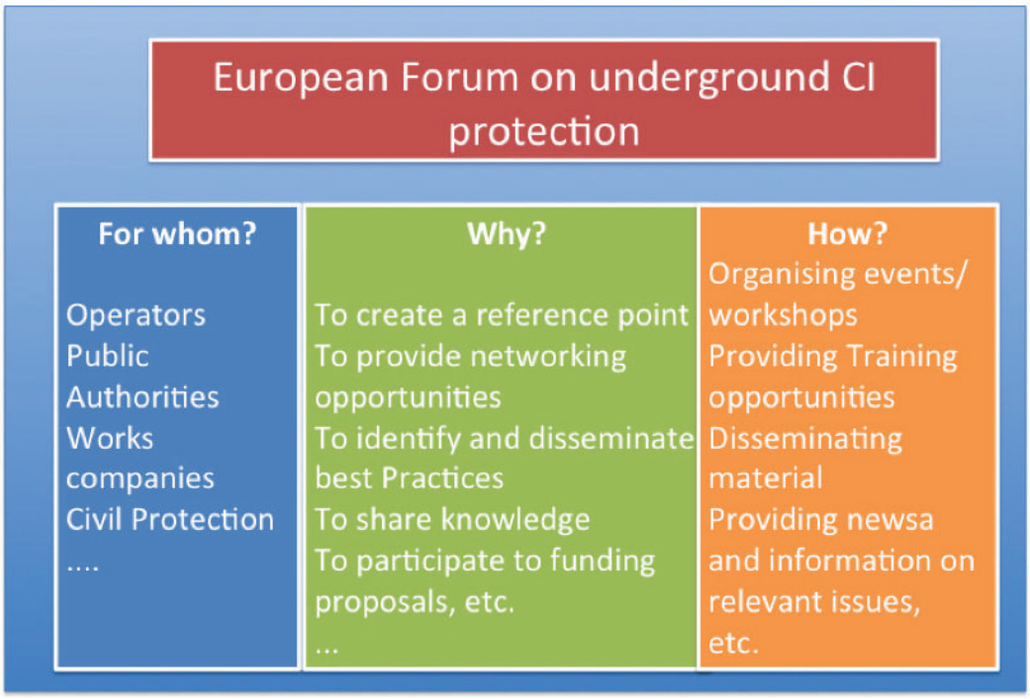


Figure 6 - the set up of a European Forum on underground CI protection is a priority recommendation from stakeholders

(c) Support the decision-making for underground CI security

Policy recommendations aim also at targeting the need to support the decision-making process of stakeholders involved in underground CI securities. The lack of public-private collaboration was identified as a weakness in current practices. Policies should then focus on promoting and facilitating stakeholders' collaboration to address underground CI issues.

➢ *Promote Public-Private stakeholders' collaboration:*

There is a need to promote Public-Private stakeholders' collaboration to address security issues in underground CI. The added value of stakeholders' collaboration is related to the possibility to provide all stakeholders with a common basis on strategy, objectives and governance rules. It facilitates the exchange of information, as well as the collaboration and coordination. It allows having a better picture of each stakeholder's role and responsibilities. This added value has to be emphasized in order to convince private and public stakeholders to participate. Trust building, shared responsibilities are also a result of collaboration. It is important that the collaboration starts as early as possible, for instance already during the infrastructure planning and construction.

➢ *Develop new tools to support the decision-making process of stakeholders*

In order to promote Public-Private stakeholders' collaboration, innovation and new tools are required. This issue is relevant for all actions related to risk management, in order to facilitate the exchange of information and provide a comprehensive picture of the issues to address. For instance, information-sharing platforms are an efficient way to support the exchange of information among relevant stakeholders during emergencies.

➢ *Provide Guidelines on all phases of the security implementation process*

Guidelines have been mentioned by stakeholders as an efficient way to support the decision-making process. It is a way to promote a common and harmonised vision of the risk management among underground CI stakeholders and to provide a common reference basis to address underground CI security issues. For instance guidelines could provide a list of the relevant scenarios and risks that are relevant for underground CI systems, a list of potential measures to be taken or the steps to set up a stakeholder collaboration process. They could also answer the need to take into account some aspects that are now currently underestimated, for instance the cyber threats. The set up of a European Forum on Underground CI protection could support the common elaboration of these guidelines, together with other objectives.

(d) Data sharing to address underground CI protection

The topics of data sharing and data security should be specifically addressed by the policy-making process, as they are particularly relevant for underground CI infrastructures

➢ *Promote the systematic collection of data related to underground systems*

Stakeholders highlighted the importance to have maps or geographic information systems based on data related to existing underground CI. It appears necessary to promote the systematic collection of this data, based on common format and meta data specifications. Data could be collected at local/regional/national levels. Regarding the format of data, the INSPIRE Directive is seen as an excellent opportunity to collect harmonised data, although some specific data relevant for underground CI are not mentionned. In addition more efforts should be dedicated to the effective implementation of the Directive.

➢ *Ensure and improve data security*

The issue of data collection is in conflict with the issue of data security. Information on underground CI can be sensitive from a security or commercial point of view and the issue of data collection cannot be addressed without ensuring a proper level of data security. It is thus necessary to tackle this issue by providing models of secure data management, or providing new technologies ensuring that data are not accessible to all, by identifying possible strategies making some data accessible and others not, etc.