upsidedown
PROTECT

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

UPSIDE DOWN

2/2014

Novembre - Dicembre 2014 - Anno VII - Numero 2 - Editore - Regione Lombardia, D. G. Ambiente, Energia e Sviluppo Sostenibile - Registrazione del Tribunale di Milano n.404 del 14/06/2006

upsidedown
because security matters

Utility Database, Urban Asset Management and Cyber-Attacks

EDITORIAL

Be ever alert!
Chiara Dell'Orto

"Cyber Attack is any type of offensive maneuver employed by individuals or whole organizations that targets computer information systems, infrastructures, computer networks, and/or personal computer devices by various means of malicious acts usually originating from an anonymous source that either steals, alters, or destroys a specified target by hacking into a susceptible system" (source Wikipedia)

Cyber attacks have become today's threat and not only scenarios seen movies or in videogames. Sabotage of critical infrastructure, stopping the delivery of public services, in this case the water supply, are only one of the new forms of intimidation implemented by those who aim to hit a wide audience, sparking panic and alarmism .
We have to say that a way of threat, just as impactful as others is represented by cyber attacks. If a cyber attack on a planetary scale is rather unlikely, different is the case of many local and targeted attacks designed to strike strategic sectors of certain states or nations.
There are many recent cases, such as the simulated 'White Hut' attack type, carried out by taking control of the SCADA system of a county in Ireland by a foreign government, the attack to the pumping system of Springfield Illinois (USA) by cyber Russian hackers through stolen credentials managed by the SCADA software provider and, not least, the series of destructive attacks against information systems of the Gulf that destroyed 30,000 hard drivers of Saudi Aramko and the one in Qatar, that has put in severe crisis the the operating system of Ras Gas.
The cyber threat is growing because the space of conflict tends to extend from the physical realm (land, sea, air) to new virtual dimensions, where the exercise of control marks competitive advantages for those who want to violate the sovereignty of other players.

Therefore cyber attacks are the invisible weapon used to hit the economic interests and political sovereignty of a nation. In this sense, in fact, National States lie exactly at the top of the list of possible attackers, followed by:
- disgruntled / former employees with inside knowledge,
- Criminals: Their aim is extortion
- Terrorists / Political Activists to trigger disruption, publicity, killing and ransom
- 'Vandal Hackers' who created "Disruption for 'fun'
- 'Fun Hackers' with desire for challenge

Once the subject is defined, there are many different ways to implement a cyber attack:
- Spyware: Monitors user activity
- Trojan Horse: Malicious file / program That disguises itself as legitimate file / program
- Virus: Attaches to existing file / program
- Worm: Malicious file / program That disguises itself as legitimate file / program
- Sniffer: Monitors information traveling over networks
- Key Loggers: Records and Transmits keystrokes to the originator
- Phishing: False websites / email messages looking genuine user asking for some confidential information

The impact of a cyber attack can be much more resonant than you might imagine, trespassing beyond the cyber space itself. A cyber attack can impact at the same time different aspects: Social (Health, Community fear, Physical move of community), Economic (legal claims against authority, service disruption in the wider economy) Environmental (Pollution, Physical), and Digital (Changing of parameters / settings or Altering date: such as alerting facilities).

So, according to these considerations, the key message is to take potential cyber attacks seriously, building cyber security into routine workflows utility and having a "ready remediation plan" because *the question is not 'if' but 'when' you will be attacked!*

Anno VII – Numero 2
Novembre-Dicembre 2014
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:
Sergio BIANCHI, Rosella BOLIS, Chiara DELL'ORTO, Björn GUSTAVSON, Alessandra LAFRANCONI, Emilio Attilio LANFRANCHI, Andrea ZACCONE

UTILITY DATABASE, URBAN ASSET MANAGEMENT AND CYBER-ATTACKS

Risk analysis must consider two models that are apparently operating in a similar way but are actually quite different in their *modus operandi* and in the skills they require:

1- **Attacks on a large scale:** it is a type of attacks that do not require great expertise and knowledge of the network, but the impact can be very strong as they impact on the population of big cities, and very few victims creates panic. This article will not focus on these attacks.

2- **Targeted attacks:** these kind of attacks are designed to strike the symbols of power. Target of these kind of attacks are water networks of some institutions, prisons, courts and centers of power in the broadest sense (parliaments, political assemblies, etc.). They also require simple logistics, as in all cases of homegrown terrorism, but a greater knowledge of the water system, needing access to the data management system, in order to understand how to address the pollutants in the desired direction and how to measure out the amount and timing.Therefore the knowledge of the system is more and more a crucial point. Moreover, the ICT skills, as we shall highlight in the article, is highly needed to carry out the attacks, but can itself become a lethal weapon in the hands of terrorists.Therefore, the article will deal just with this dimension, trying to 'shoot' the state of technology and the level of vulnerability to which it is exposed.

1. UTILITY DATA-BASE, URBAN ASSET MANAGEMENT AND CYBER-ATTACKS

ENRICO BOI AND MARCUS EDWARDS

In this chapter we will analyze the role that a cyber-attack could have on a water network and how the attack could be carried out.

To better define the role that could play a cyber-attack, we have segmented it in different categories that can be classified as "passive" or "active" uses of IT information or networks to support or play an attack.

The "passive" use of the IT infrastructure is related to the acquisition of informations related to a specific network, and all the activities related to their processing and data elaboration that would provide valid data to support a terroristic attack on the network. This activities are normally related to the acquisition of the geospatial data of the utility network (its layout), as well as the functionality of every part of the network itself.

The "active" use of the IT infrastructure is, on the other hand, related to a real attack carried out through hacking activities from remote connections to the mainframe management systems of an utility network, or through a the direct connection to an hardline used to control and manage a network part.

In the following paragraphs we will analyze the criticality of the existing system and we will also evaluate possible solutions to mitigate these potential threats.

To better understand the real world scenarios, we have carried out an extensive study on a defined test area located on a residential neighborhood of Milan, this area will also be used to perform the project's simulated exercise of "exploiting" the water distribution network.

1.1 IT Passive cyber attack

IT Passive threats are, as already described, related to the acquisition of data related to utility networks, their processing an elaboration, and its use to support a terroristic attack.
More specifically we can define two areas that have to be considered important for this particular type of threats:

- Geospatial data quality. More precise is a dataset, more precise and fatal can be an attack;
- Data accessibility. More easy is the access to the data, more easy id to plan an attack.

1.1.1 Geospatial data quality importance

With the increase of precision on utility mapping technology, we have now the possibility to structure reliable geo-databases with a sufficient grade of accuracy allowing the utilization of this data infrastructure for a wide band of applications, from urban planning to landscaping, from the design of a new telecom network based on the use of old infrastructure to the support on excavation activities on high density urban environment scenarios. The analysis of the positive fallouts related to the availability of high quality data on underground infrastructures can be long and various, but unfortunately this list can also be populated with some negative aspects that can cause some concerns with regards to the security of underground utility networks and for the population potentially exposed.
Every network have his vulnerability, this are normally buried under the ground with the network itself, so they cannot be really exploited if hidden. The accessibility of this information through a detailed geospatial database by anyone with bad objectives can pose threats proportional to the detail of the network database.
An extensive knowledge of the water distribution network layout can make the difference for the planning of an attack. The injection of a poisoning substance on the network on a precise location, chosen on the results of a computer simulation of the network dynamics (EPANET algorithm), could cause the highest impact on the network, with the highest spread of the substance on the network along with the longest life time.
An attack designed and engineered in this way can be very effective and hard to detect in real time, and depending on the life time of the substance on the network, it could also take long to be mitigated.
Besides the strength of the poisoning substance, we also have to consider the psychological impact on the population that relays on the water for a large number of activities, as drinking, cooking, cleaning, etc.. Water is life.

Fig 2.1 – Example of an injection high pressure hose connected to a hydrant

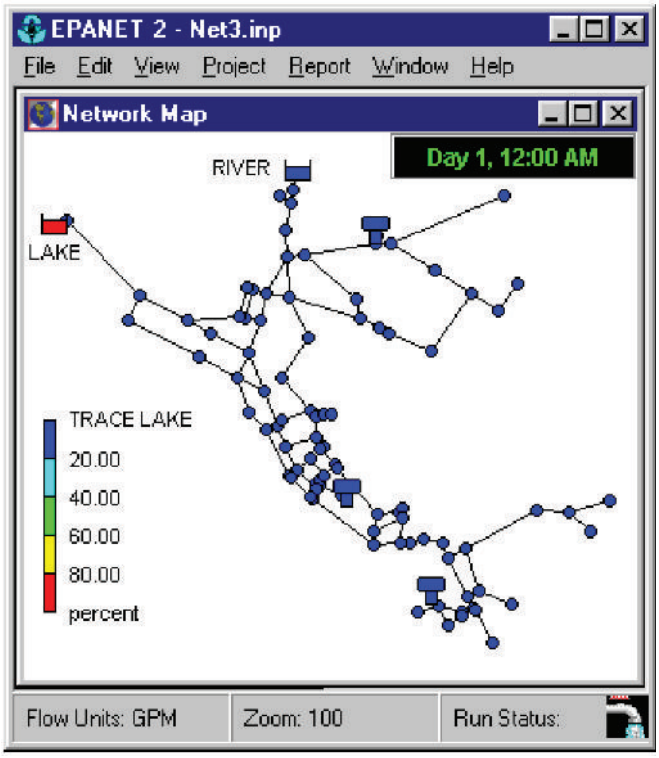


Fig 2.2 – Epanet network simulation graph

These scenarios are achievable only with a good knowledge of the network layouts complete with all the network information.

1.1.2 Historical Records Availability and Source

With regards to underground infrastructures, historical archives have always been the data source more readily available. Until a few years ago, utility infrastructures belonged to a small number of public bodies or private companies who owned the network and managed their asset directly. The maps were paper based with local reference systems. To have access to this information was sufficient to apply, with a reason, at a dedicated office of the operators, to obtain permission to "copy" only specific parts of the maps. The process was simple and most of the information were kept and maintained by a small group of people that physically kept the information into a locked drawer. Security was simple and it was also very simple to keep track of the people who accessed this information.

Over the past 20 years, but mostly during the last 10, the digitization of paper maps into cartographic databases or GIS infrastructures, changed completely the way to manage and handle this important geographic information, opening to a wider number of people the accessibility of data for project collaboration, but also opening to a potential wrong use of the information itself, and in a way breaching the security of the network.
On the following paragraph it is described the result of the analysis carried out on the test site, with the aim to understand the quality of the available data and also its accessibility.

1.1.3 available GEOGRAPHICAL information - Milan test site

The test site area has been selected in the northwest of Milan, with a surface of about 1.014.295 square meters, this particular area contains all the most common urban models that can be found on an high density populated environment. Within this large test area a more defined space has been localized on a residential and old industrial area, with an extension of about 68,400.00 square meters. This particular area was selected on the base of the following parameters:

- urban models;
- site conditions, with regards to vehicular and pedestrian traffic, parked cars, presence of trees, etc.;
- site utility congestion, high, medium, or low;
- ratio sidewalk/road;
- population percentage.

The selected area has been divided in 3 different sub areas to better implement the various step of the research.
In the following picture the 3 areas are visible in green, yellow, and red color.
Purpose of this first activity was to understand the relation between the quality of the geospatial data, with its origin. To track this information, a reference table has been implement-

Fig 2.3. Milan test site - 68,400 square meters

ed to benchmark the acquired and processed data.

The classification of the data has been divided into 4 different classes, related to data origin and data processing activities. One of these classes is also divided into sub-classes to better define quality levels.

The Quality Levels starts from level 4 with the lowest quality; it is related to all the data acquired with utility record or oral recollection. Quality Level 3 is related to all information acquired with QL 4 incremented and verified with topographical surveys of all the infrastructures connected with the underground. Quality Level 2 is related to all information acquired with QL 3 incremented and verified with a manhole opening campaign. Quality Level 1, the highest quality, is related to all information acquired with QL 2 incremented with survey activities carried out with survey equipment like georadars or EM locators.

The following table shows in details the Quality Level classification along with sub classes for QL1.

Data origin	Quality Level	Subclasses
Utility Records Oral recollection	**4**	none
All of the above Topographic survey	**3**	none
All of the above Manhole opening and survey	**2**	none
All of the above Instrumental mapping and survey (GPR, EM Locators, etc.)	**1**	**1A:** Use of GPR and EML with high density grid **1B:** Use of GPR and EML with low density grid **1C:** Use of EML with high density grid

Tab 2.4. Quality Level reference chart

Using the above table as the main reference chart for the comparison of the acquired data and the post processing data, the following activities have been implemented:

- Historical record data acquisition and processing;
- Instrumental survey data acquisition and processing;
- Comparison of the above data;
- Representation of the produced layouts with GIS or WebGIS infrastuctures.

1.1.4 Historical Record Data Acquisition and Processing

The use of record drawings have been the most common practice to acquire information about underground infrastructures, but in time this practice has shown its limitation.
This approach relies too heavily on limited information, in particular:

- record drawings usually do not depict connections and abandoned lines, describing only main and operating services in a schematic way;
- the data is available on different formats, paper, raster images, pdf, vector drawings, database;
- data accuracy is different from record to record and for this reason it is very hard to mesh into a usable map;
- different geographical coordinate systems.

The collection of record drawings has been a very important activity, on which the technicians involved dedicated a great effort. One of the goals was to understand how much the data acquired through historical records is considered reliable against the data acquired with survey equipment.
The collection process has been divided in three main activities:

- data preparation, by the company or Authority that stored the data;
- data collection, by a team able to sort all the potential differences between maps;
- data fusion, interoperability activity carried out to produce the best possible meshed map from all the different formats.

The resulting dataset would be classified on the reference table as a Quality Level 4.
It is important to highlight the criticality of the historical data acquisition process, from the different stakeholders. While searching for all the historical records available from utility companies, we have experienced a quite complex scenario with regards to data source and data versioning.
A single set of data, of a specific network, could be located in different databases, with often different data versioning. These data-

bases had all different level of access, from open public, to private with non-disclosure agreements prior the access to the information.

This scenario highlights different policies within different organizations and most of all an absence of a shared approach with regards to data security. Every internal policy has been driven by different needs, for example Regione Lombardia gives public access to WebGIS resources because it is within their mandate to support planning and design, as well as sharing knowledge between the various stakeholders.

The following chart represent the data source for the selected test area in Milan, it is interesting to note how certain information were shared within the territory.

Milan Test Site				
Utility	Digital format	Infrastructure ownership	Network manager	Data Source
Gas	DWG SHP	na	A2A	Comune di Milano Regione Lombardia A2A
Water	DWG SHP PDF	Comune di Milano	A2A	Comune di Milano Regione Lombardia A2A
Waste Water	DWG SHP PDF	Comune di Milano	Metropolitana Milanese	Comune di Milano Regione Lombardia Metropolitana Milanese
Public Light		na	A2A	Comune di Milano Regione Lombardia A2A
Telecom Italia (telecom)		Telecom Italia	Telecom Italia	Comune di Milano Telecom Italia
Metroweb (telecom)		Metroweb	Metroweb	Comune di Milano Metroweb
Colt (telecom)		Colt	Colt	Comune di Milano
Fastweb (telecom)		Metroweb	Metroweb	Comune di Milano Metroweb
Worldcom (telecom)		Worldcom	Worldcom	Comune di Milano
Wind (telecom)		Wind	Wind	Comune di Pero
Power		na	A2A	Comune di Milano Regione Lombardia A2A
Central heating		na	A2A	Comune di Milano Regione Lombardia A2A

Tab 2.5 – Milan Test Site – Data source

1.1.5 Survey equipment data acquisition and processing

The survey activities carried out using survey equipment, mostly commonly known as No-Dig Technologies, and more specifically with survey equipment like GPR (ground probing radar), or EM locators, are intended to produce good and accurate results with a minimum impact on the environment and without any damage to road infrastructure. Moreover, through this No-Dig approach, surveys on site where performed without interruption of business activities or traffic flows.
The survey activities have been organized in 2 different stages, the first one has been used to cut off all the technical approaches that didn't provide results above a certain standard, based on a set of parameters, as for example the availability of enough information to populate a database formatted following the specification of the Italian Dataset Standard for State Agencies (Catalogo dei dati Territoriali – DigitPA) or the Regione Lombardia regulation RR6/2010, all the above based on the Inspire European Directive.

1.1.5.1 Survey Equipment

Important factor for the quality of the acquired information has been the selection of the right survey equipment, chosen from the high-end of market available equipment and with a proven, recent, history of good usage.

1.1.5.1.1 GPR or Georadar System Composition

The georadar system for utility underground detection on the test study was composed of:
- A data collection device:
  - Antenna array
  - Data acquisition apparatus
- Dedicated software for processing the radar data.

Considering the data collection device, the Antenna Array is the most critical part of the apparatus, where the specification and the antennas central frequencies are the key factor on the detection capabilities of the GPR. We will here describe the specification of the Antenna Array used on our test; we will not describe the data acquisition apparatus, because the technical characteristics are commonly shared between most of the apparatus of different makers.
The use of an array of antennas, against the use of a single antenna, maximizes the capacity of acquiring underground information; in particular it is proven an increase of performance on the following characteristics:
- increased detection capacity
- reduction of false targets
- capability of solving complex geometries

The working frequencies of the used array of antennas were in the range 200-600MHz in consideration of the type of application and penetration depth required on the project.
As a general rule, frequency selection normally follows the guidelines below:
- medium frequency sensors (400-600 MHz) are used in the depth range 0.5-1.5 metres
- medium-low frequency sensors (200-400 MHz) are used in the depth range 1.5-2 metres

The used array worked with 8 channels divided into 3 antennas (boxes) to optimise investigation effectiveness and the overall size occupied by the system. The possibility to adjust the clearance of the system is really useful in urban environment with parked cars and confined spaces.
Another important factor is the positioning system in use with the array of antennas. The GPR needs to reference its movement to a local reference system. On the market are available many different systems with either GPS real time positioning or mechanical linear encoders that record the movements of the apparatus on the ground.
The system used on the acquisition on the Milan test site used a mechanical encoder referred to a local reference system, a more efficient system in urban environments.

Frequency range	200-600 MHz
N° of antennas	1 to 8 antenna configurations
N° channels	From 1 to 8
Types of channel	Monostatic, bistatic and crosspolar
Metric wheel resolution	≤ 2.5 cm

Tab 2.6 – Milan Test Site – Used GPR Specification

The acquired radar data has been processed by experienced engineers with specific software capable of displaying and process the radar data, with the scope of extracting the information of interest.

In particular, the following functions have been used for the production of high quality results:

- automation of operations such as:
  - gain equalization
  - propagation velocity estimate
  - determination of the zero value of sections
  - alignment over various channels
- automation of the supply of technical information such as:
  - identification and layout of radar profiles performed
  - penetration depth
- use of radar processing and data visualization techniques such as :
  - 2D radar sections
  - 3D tomographic views
- use of a data base for the management of radar data

1.1.5.1.2 Electromagnetic Locators specifications

A very important contributes for the identification of particular services, id the use of the Electromagnetic Locators usually called EM Locators. During the Milan test site acquisition the following detectors have been used:

- Hum Detectors (A cable-locating device set on power mode). These are receiving instruments that detect the magnetic field radiated by live electricity cables, which have current flowing through them. However, these instruments will not detect service connection cables to unoccupied premises or street lighting cables during the daytime, as little or no current will be flowing through the cables at that time. They may also fail to detect some well-balanced high voltage cables, where these cables generate little magnetic field.

- Radio Frequency Detectors (a cable locating device set on radio mode). These are receiving instruments that respond to low frequency radio signals, which may be picked up and re-emitted by cables and long metallic pipes. If radio frequency detection is used, other metallic objects may re-radiate the signal and results may vary appreciably according to locality, length of buried pipe, distance from the termination and geographical orientation.

- Transmitter-Receiver Instruments. These instruments involve connecting a small transmitter or signal generator to a metallic pipe so that the signal is induced into it. The receiver then detects that signal. Usually, some part of the cable or pipe will need to be located in advance of the operation in order to ensure that the transmitter is positioned correctly.

1.1.5.2 Method for Performing Investigations

A critical aspect of the use of any equipment, survey or not, are the operating procedures. The best survey equipment used on the wrong way will deliver wrong results. Medium level survey equipment used in the proper way can deliver very good results.

All survey activities performed on the Milan test study have been proven as guarantee of quality on the utility mapping industry.

Frequency	50 or 60 Hz 15-30 kHz 512 or 640 Hz 8 kHz 33 kHz 65 kHz 131 kHz 200 kHz
Current Reading	+/- 5% Active signal bw limited
Locate Quality	Dynamic range 140dB @ 10Hz bandwidth
Selectivity	120dB/Hz to 200kHz
Sensitivity	5E – 15 Telsa (32,768Hz ; 1Hz b/w)
Locate Accuracy	+/- 5% of depth, good condition

Tab 2.6 – Milan Test Site – Used EML Specification

The following activities have been performed during the Milan test study:

a) EML detection activity:
- Definition of the reference system
- Search for longitudinal utilities
- Search for transversal utilities

b) Radar detection activity:
- Definition of the reference system
- Search for longitudinal utilities
- Search for transversal utilities

c) Processing activities and detection of ground characteristics,
- Radar data processing radar
- CAD processing
- Data storage

1.1.5.2.1 Georadar surveying activity

The operational sequence used on the project consists of the following steps:
- definition of the reference system
- geological mapping and calibration using manholes
- performance of longitudinal scans (parallel to the direction of the road) and transversal (perpendicular to the road direction) to search for utilities
- verification of the penetration depth reached

1.1.5.2.1.1 Definition of the reference system

The local reference system can be used for both the GPR mapping and the EML investigation.
As illustrated in 3.6, the reference system consists of the following features:
- **a *zero point***, (starting point reference for the successive transversal and longitudinal scans); this must be a clearly visible and signalled architectural element (e.g. the corner of a building, the corner of the pavement etc.);
- **a *reference line***, which must correspond to clearly visible and reproducible topographical elements (for example the edge of a building, a fence, a pavement kerb, road edge, road centreline when marked etc.), and which, together with the zero point constitutes the starting point for measuring all the site coordinates; normally, the reference line follows the road direction.

  and also:
- the **T axis**, passing from through the zero point and coinciding with the reference line;
- the **L axis**, passing through the zero point and orthogonal to the T axis;
- ***transversal step:*** this is the coordinate along the T axis measured starting from the zero point

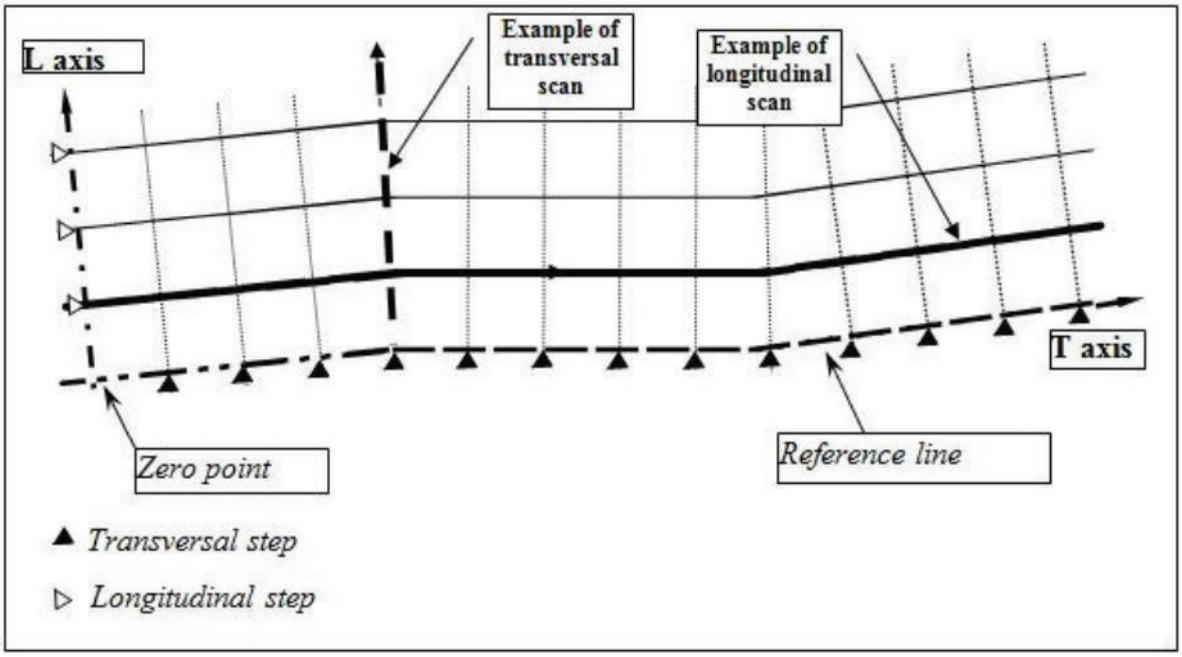


Fig. 2.7 – Implementation of the local reference system

- ***longitudinal step:*** this is the coordinate along the L axis measured starting from the starting from the reference line.

Once the reference system has been defined, the transversal steps have been marked on the site; normally at intervals of 10 meters, and in any case with a distance below or equal to that of the position markers. As a general rule, greater distances are permitted for linear paths on smooth surfaces (e.g. good quality asphalt); the distance has to be reduced in the presence of sharp curves or irregular road surface.
The measurement and signalling of transversal steps must be performed very carefully to avoid degrading the localization accuracy of the investigation.

1.1.5.2.1.2 Performing Radar Scans

The way in which the radar scan is performed depends on the investigation objectives. For the Milan test study project, two different level of scanning have been defined prior the commencing of the project.

- The first one, has the objective of reaching the highest possible results, and therefore requires as a high density scanning grid;
- The second one, has the objective on reaching a lowest data quality with a lowest budget, requiring in this case a low density scanning grid.

The following paragraphs illustrate the methods of performing both complete coverage and reduced coverage for both an antenna array and for a single antenna.

Investigations high density scanning grid: complete coverage
Complete coverage is intended literally in that a series of radar scans (both longitudinal and transversal) are performed to cover the entire investigated surface.
To obtain a complete coverage, two adjacent scans (both longitudinal and transversal) must be separated by a distance equal to the transversal width of the array or the single antenna (see Tab 3.7). Transversal width of the array is intended as that orthogonal to the surveying direction.
It is a good practice, used also in the Milan test project, to minimize the risk of human error; by setting up the distance between two scans

Transversal array width	*Distance between two adjacent scans*
Less or equal to 50 cm	50 cm
Between 50 and 100 cm	100 cm
Between 100 and 150 cm	150 cm
Between 150 and 200 cm	200 cm

Tab 2.8 – Distance between two adjacent scans

to a multiple of 50cm. Therefore, by rule, the scans (both longitudinal and transversal) will be spaced by a quantity equal to the transversal bulk of the array rounded up to the nearest 50cm.

Tab 3.7 shows an example of how to define the distance between two adjacent scans.

The table illustrates the choice of scan distance for complete coverage.

The following figure shows on a plain view the position of the array performing a high density scanning of transversal scans with an array of antennas, to locate longitudinal pipes.

The following figure shows on a plain view the position of the array performing a high density scanning of longitudinal scans with an array of antennas, to locate transversal pipes.

In certain cases it is also possible to use single

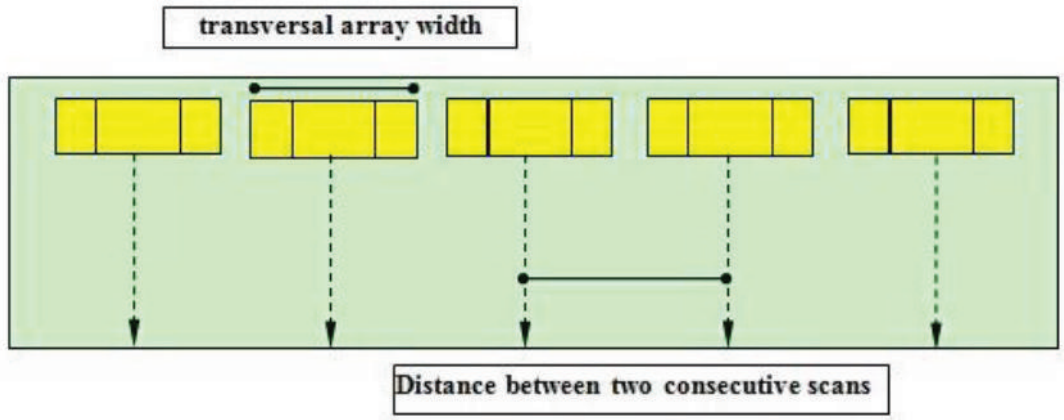


Fig 2.9 High density transversal scans with an array of antennas

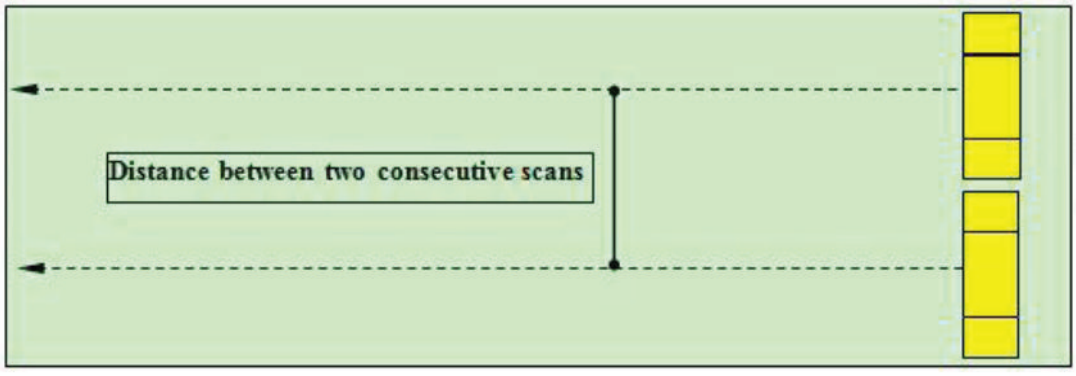


Fig 2.10 High density longitudinal scans with an array of antennas

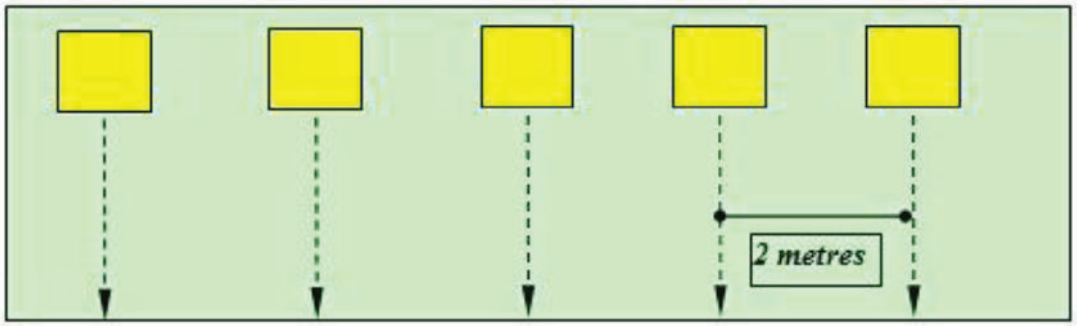


Fig 2.11 Medium density transversal scans with a single antenna

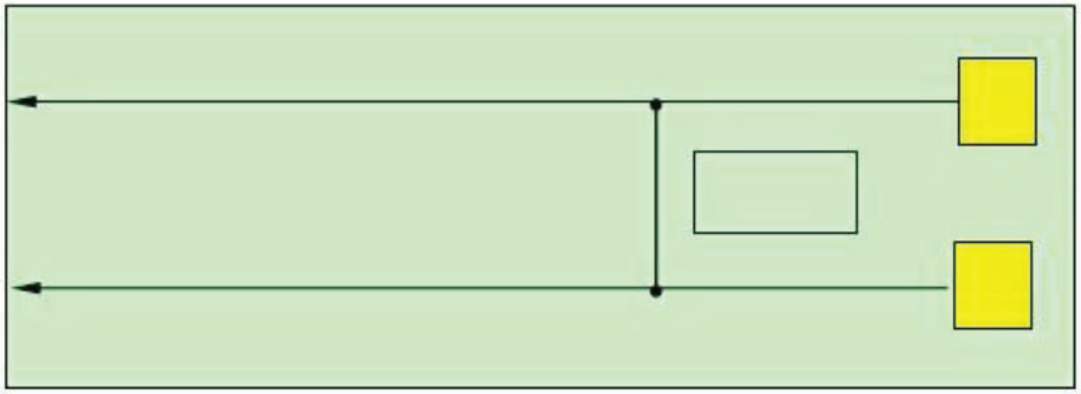


Fig 2.12 Medium density longitudinal scans with a single antenna

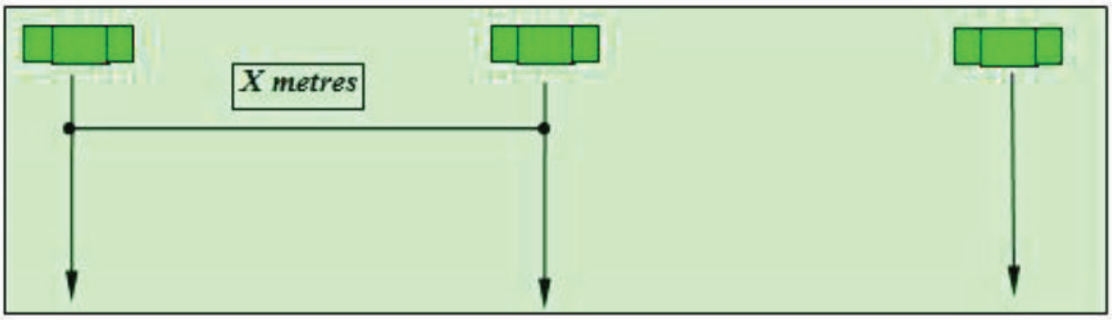


Fig 2.13 Low density transversal scans with an array of antennas

antennas with scanning distances of two meters or, more generally, a minimum width related to site conditions (for example the presence on site of trees or parked cars, where only a single antenna can perform the scans). In this case we can consider a "medium" density scanning grid that supply not as many information of the high density scanning grid, nor the reduced level of information as the low density scanning grid. During the acquisition phase of the Milan test project, this site conditions have been encountered several times.

The following figure shows on a plain view the position of the array performing a medium density scanning of transversal scans with a single antenna, to locate longitudinal pipes.

Fig 2.14 Low density longitudinal scans with an array of antennas

The following figure shows on a plain view the position of the array performing a medium density scanning of longitudinal scans with a single antenna, to locate transversal pipes.

Investigations low density scanning grid: reduced coverage

Reduced coverage is intended as the performance of a series of scans with the radar array (both in longitudinal and transversal directions) that permits the coverage of a part of the investigated surface.

The reduced coverage of the investigated surface is performed using a regular grid; the position of the utilities is detected on the grid, and is extrapolated in the intermediate points.

The following figure shows on a plain view the position of the array performing a low density scanning of transversal scans with an array of antennas, to locate longitudinal pipes.

The following figure shows on a plain view the position of the array performing a low density scanning of longitudinal scans with an array of antennas, to locate transversal pipes.

1.1.5.3 Survey Data Processing

Survey data processing has been the most complex part of the entire test study. Beside the GPR data processing activities and related CAD design with 2D and 3D delivery layouts, the most challenging aspect has been the need of compiling together a large number of information to be INSPIRE Directive consistent, in our case to be consistent with to the Italian Dataset Standard for State Agencies (Catalogo dei dati Territoriali – DigitPA) or the Regione Lombardia regulation RR6/2010, all the above based on the INSPIRE European Directive.

The required data has been acquired not only from the available cartographic information, but in certain cases, analyzing administrative documents.

The following figure shows an example of the details of an attribute table structure of the Regione Lombardia regulation RR6/2010, in this case related to the linear elements of the water distribution network, class coded 070101:

1.1.6 DATA REPRESENTATION

After acquiring and processing all the data used for this test, an important third phase has been implemented: the verification of the possible different layout that could be implemented within the processed data. This aspects is of a critical importance because, as we have seen in relation to the data source of historical records, data can be available in many different formats, from 2D to 3D representations, both in CAD or GIS format. Two different types of representation have been tested in the test. A classical 2D WebGIS representation, with a solution based completely on open source components and on Open Geospa-

Nome classe	Nome campo	Formato	Lunghezza	Decimali	Codice attributo	Descrizione	DOB	DEF
070101	COD_CLASSE	testo	2	0	-	Codice della classe	✓	
	FILE_ID	numerico	n	0	-	Identificativo univoco progressivo per la classe di oggetti	✓	
	RILIEVO	data	-	-	-	Data rilievo/inserimento nel SIT [gg/mm/aaaa]	✓	
	COM_ISTAT	stringa	8	0	09010101	Codice ISTAT del Comune nel formato rrpppccc, con rr (regione), ppp (provincia), ccc (comune)	✓	
	TP_STR_COD	stringa	?	0	03010101	Codice ISTAT della strada	✓	
	TP_STR_NOM	testo	100	0	03010102	Nome della strada		✓
	ES_AMM_CF	enumerato	2	0	03020107	Classifica funzionale della strada		✓
	L_EG_COD	enumerato	2	0	07010101	Codice Fiscale/Partita IVA del Gestore	✓	
	L_EG_NOM	testo	50	0	07010102	Denominazione del Gestore		✓
	L_BORN	data	-	-	07010103	Data posa/installazione [gg/mm/aaaa]	✓	
	L_DIA	numerico	8	2	07010104	Diametro [mm]	✓	
	L_LUNG	numerico	8	2	07010105	Lunghezza [m]	✓	
	L_MAT	enumerato	2	0	07010106	Tipologia di materiale	✓	
	L_STA	enumerato	2	0	07010107	Stato della condotta	✓	
	L_PRO	enumerato	2	0	07010108	Range di profondità cui è posato l'oggetto	✓	
	L_POS	enumerato	2	0	07010109	Posizione dell'elemento rispetto alla strada		✓
	L_POS_SUP	enumerato	2	0	07010110	Posizione dell'elemento rispetto alla superficie	✓	
	L_INFR_TY	enumerato	2	0	07010111	Eventuale tipologia di infrastruttura di alloggiamento		✓
	NODO_INI	numerico	n	0	07010112	Identificativo del nodo iniziale	✓	
	NODO_FIN	numerico	n	0	07010113	Identificativo del nodo finale	✓	
	L_A_TY	enumerato	2	0	07010114	Tipologia di tratta	✓	
	L_A_PROCAT	Booleano	Si/No	0	07010115	Esistenza protezione catodica		✓

Fig 2.15 Example of RR6/2010 attributes table structure

tial Consortium (OGC) standards, and an experimental 3D WebGIS representation.

With regards to the security of the published information, we have faced the problem of restricting the access with personal credentials to provide a minimum of security from external access but we haven't tested more secure means of protecting the stored information.

1.1.6.1 WEBGIS PORTAL

Since 2008 Regione Lombardia has developed a webgis portal to allow and facilitate all stakeholders to consult, query, download all available information on the utility networks of all 1544 municipalities as water and sewage, electricity, telecommunications, natural gas grid, district

heating, etc. The portal groups all information available, from legal aspects, to documentation, videos and presentations and a WebGIS interface to facilitate the display and query of utility network data: http://www.ors.regione.lombardia.it.
All utility data has been standardized in terms of database structure and attributes, following the regional law n. 26/2003 "Norms of local services of general economic interest. Rules on waste and energy management, use of underground water resources" and following regulations, and has been published with a unified and standardized legend. A recent regional law (l.r. 7/2012 Measures for growth, development and employment) forces Municipalities and Utility Companies to update their utility data continuously and provide the Region with regular updates.
The WebGIS solution is based on an open source stack of components, communicating with each other through standard protocols. The data can be consulted through a WebGIS client, can be downloaded in Shape (a widely used proprietary data format) or KML (Key Markup Language, an OGC data standard) Format or can be accessed through standardized services. This allows for a true interoperability between the stakeholders and the centralized standardized database.

1.1.6.2 EXPERIMENTAL 3D REPRESENTATION

For local governments it is common practice to prefer a two-dimensional representation of geographic information. This approach is typically requested for the practical need of everyday simple working needs, but inevitably collides with the real nature of the three-dimensional reality. The design of underground infrastructure must now inevitably face the congested reality of existing utility networks: every new design and installation cannot occur regardless of the evaluation of the elevation data component (altitude below ground level). An accurate 3D survey of the existing infrastructure is, as mentioned previously, the requirement for any accurate and timely new design. Often, during new installations of underground infrastructures, it

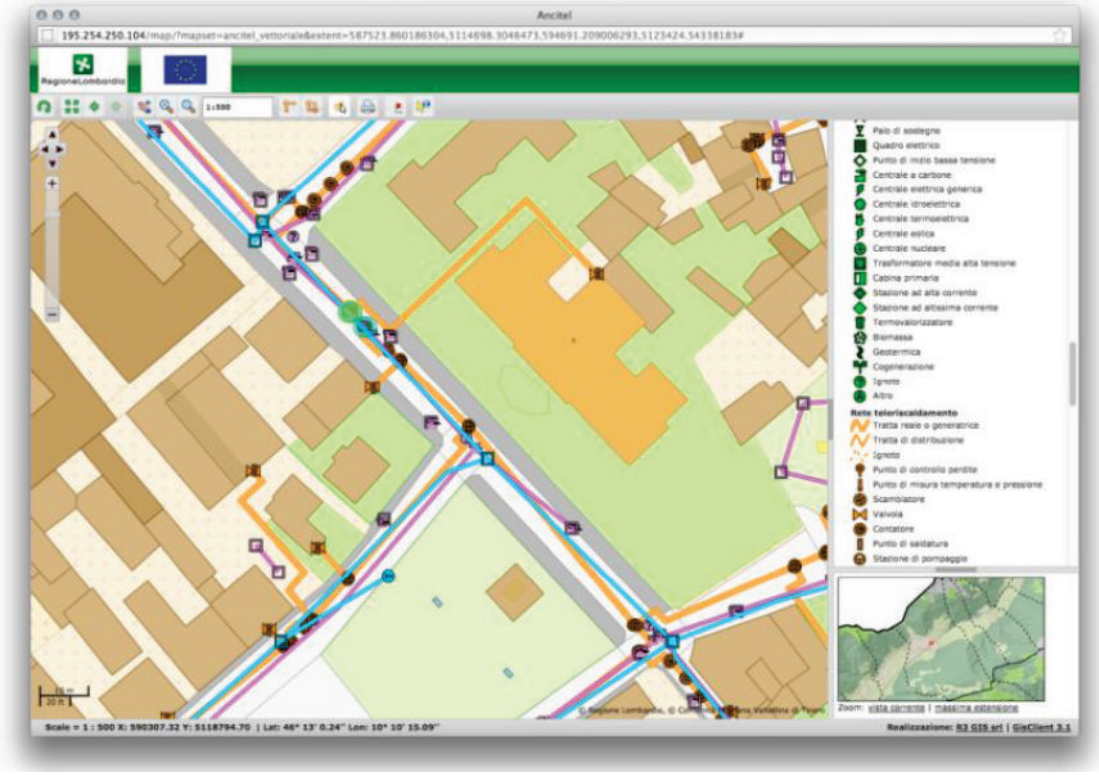


Fig 2.16 - WebGIS interface of the Regione Lombardia ORS Portal

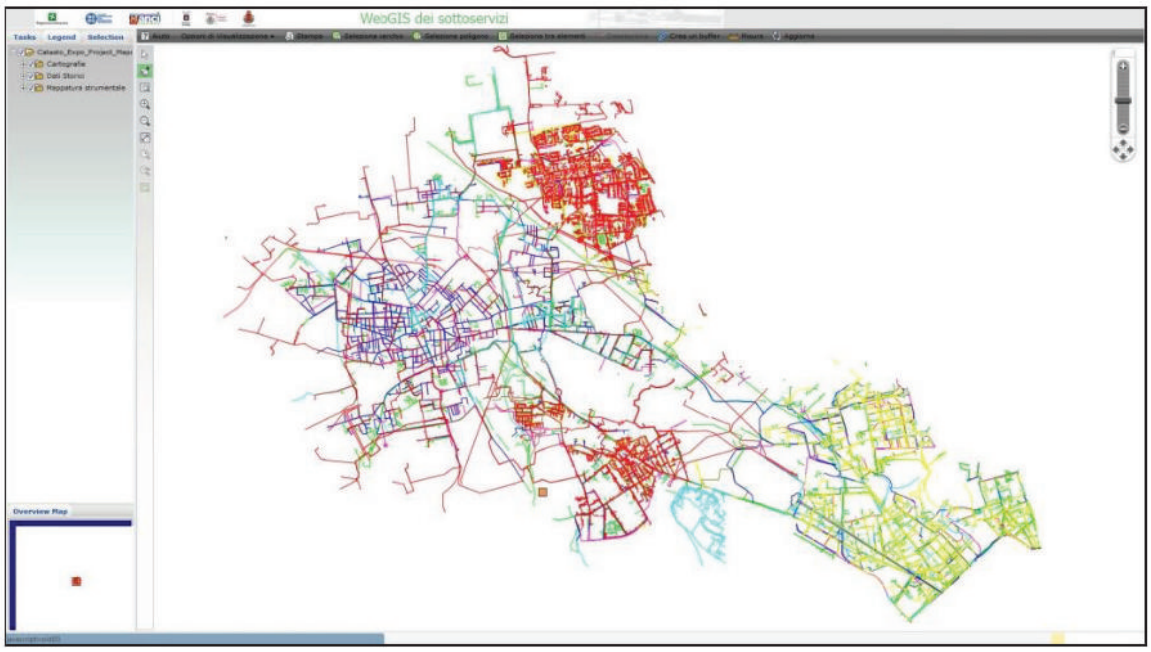


Fig 2.17 - Snapshot of a MapGuide view of the project area

is necessary to divert the designed route because of the presence, detected live on site, of other unrecorded networks or infrastructures. The knowledge of the precise position of existing networks along with all 3dimensions allows obviating these drawbacks with a considerable savings on time and resources.
The need to represent the positioning of the underground-network infrastructures in a clear and fully understandable way has been one of the aims of this test study. For this purpose the following web based software has been tested on the project:

- AutocadWS web based portal for sharing and collaboration on DWG files;
- MapGuide on proprietary server, 2D WebGIS;
- SkylineGlobe Enterprise, 3D WebGIS solution;

All the utility mapping data, both from historical records and from GPR survey, have been also produced in WGS84 coordinate system, and in both DWG and SHP format. This guarantees the maximum interoperability with all potential users.
The GPR survey data has been produced, on the base of the different mapping typology, with 2D and 3D layouts.

With this last activity we have been able to verify the level of details that can be reached with data representation, along with its related usability factor, that we have to remember it could be a good or a bad use.

1.1.7 DATA COMPARISON and related vulnerability

In order to fully understand the difference in precision and quality of all the acquired and processed data, and relate it to the increase of vulnerability of a specific network, a comparison of the produced dataset has been carried out.
A precise analysis of the produced layouts were carried out in order to verify and cross check the different acquired dataset and to evaluate the different parameters usable to extract comparison indexes. This complex process used several analytical dimension parameters to perform the data comparison, in order to obtain indicators that could be used on decision making activities. The following briefly describes the results of this process.
Some discrepancies were found between the results of the surveys on site and the informa-

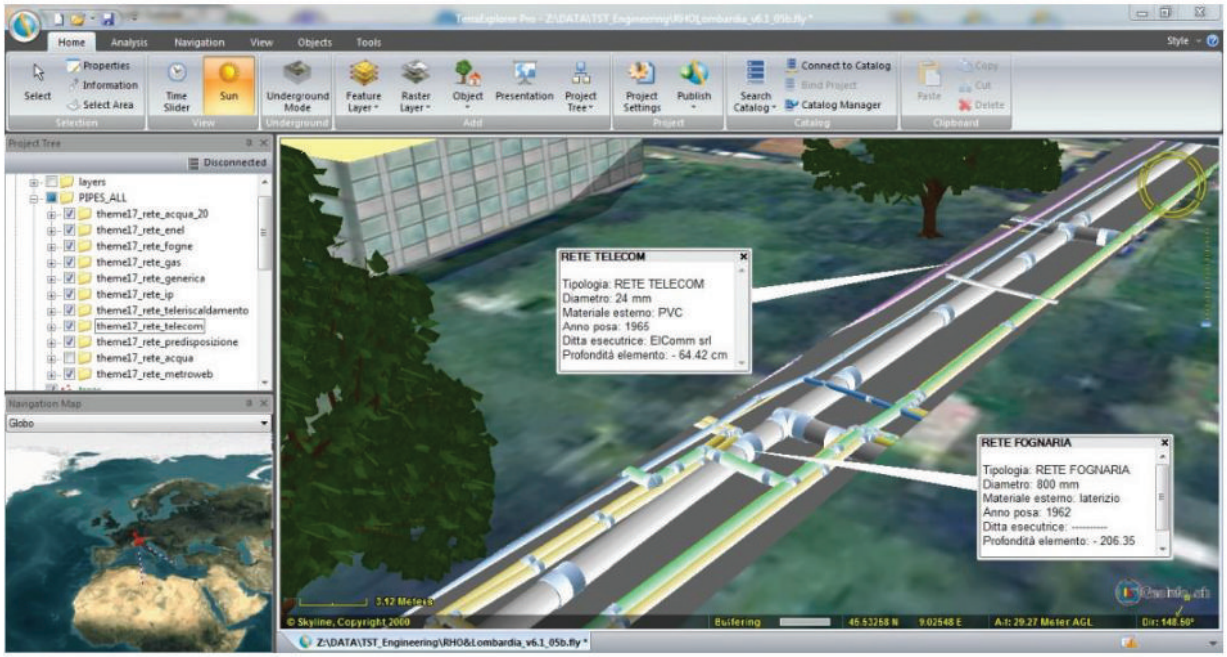


Fig 2.18 - Snapshot of a Skyline 3D layout of street detail

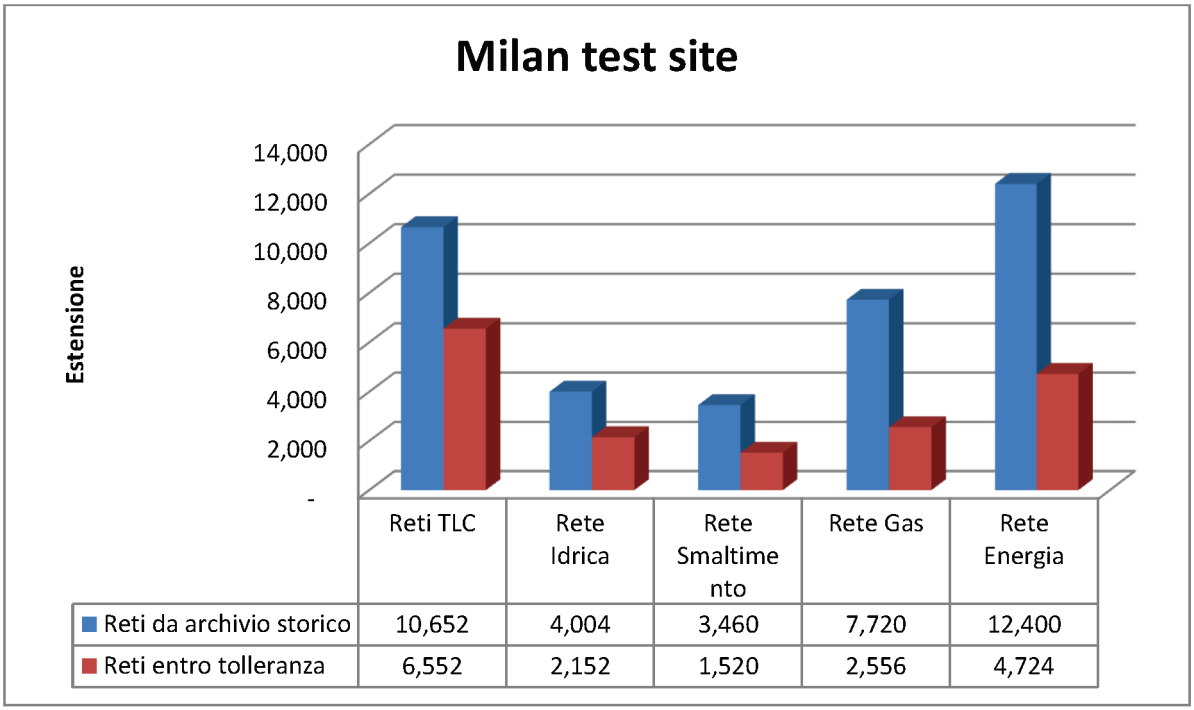
tion from record drawings. The 'first level' of discrepancy was related to the position of the items within the survey area. Historical records information was only schematic, while the 2D or 3D model provided by the GPR survey represented the elements with their real position and dimension within the adopted coordinate system. Considering a boundary of one meter on the axes of the mapped lines, we have calculated how many record drawing lines would fall into this boundary (Tab 2.19 and Graph 2.20)

A 'second level' of discrepancy between record drawings and surveys has been recorded in relation to the existence of several services that were not depicted in records information. Justification of this is seen throughout numerous abandoned and redundant utilities left underground with no record.

Non-invasive surveys were also able to locate and depict distribution and feeding lines which were not usually found in records information. In some cases, feedings from main lines were undetectable with the instruments and technology adopted due to their small dimensions. Nonetheless, engineers were still able to identify the existence and approximate

Milan test site			
Utility	Record drawings extension of lines (linear meters)	Extension of lines within one meter (linear meters)	Percentage of lines within one meters
Telecoms	10.652	6.552	62%
Water	4.004	2.152	54%
Sewage and storm	3.460	1.520	44%
Gas	7.720	2.556	33%
Energy	12.400	4.724	38%
Total	**38.236**	**17.504**	**46%**

Tab 2.19 Milan test site – accuracy of the two dataset within one meter



Graph 2.20 – Milan test site – accuracy of the two dataset within one meter

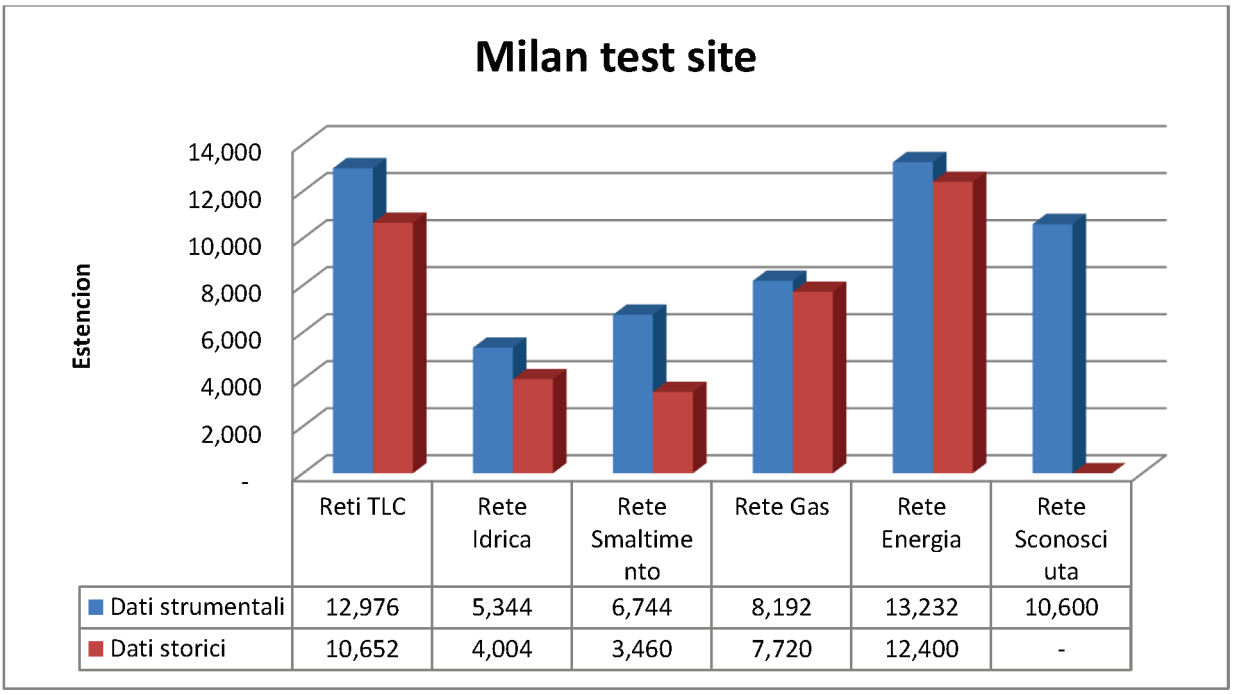
location of these lines through a careful analysis of surface elements located within the site (e.g. valves, meters etc); therefore, depicting this information in the final drawing. (Tab 3.20 and Graph 3.21)

A 'third level' of discrepancy between information provided on records and its authenticity against site surveys, has been identified. The position of services in existing record drawings did not match the number and position of the surface items (e.g. manhole covers, chambers, and valves) found within the surveys. Only through a thorough analysis of site data was it possible to assign the right typology to each item.

In general, records information depicted the position of each determined utility with no specific geographical reference; this lacked

Milan test site				
Utility	Instrumental mapping extension of lines (linear meters)	Record drawings extension of lines (linear meters)	Difference in extension of lines (linear meters)	Difference in percentage
Telecoms	12.976	10.652	2.324	22%
Water	5.344	4.004	1.340	33%
Sewage and storm	6.744	3.460	3.284	95%
Gas	8.192	7.720	472	6%
Energy	13.232	12.400	832	7%
Unknown	10.600	-	10.600	100%
Total	**57.088**	**38.236**	18.852	**49%**

Tab 2.21 – Milan test site – comparison of different data sources



Graph 2.22 – Milan test site – comparison of different data sources

useful information in designating the utilities on site.

1.1.8 Security point of concern

The activities carried out on the Milan test area, provided us all the needed information to better understand the different possible security threats related to the access of a utility network geospatial data, more specifically of the water network.
We have defined the different level of precision that are related to every different mapping methodology and we have also verified the different procedure to retrieve the data from the owners.
We can summarize the "security point of concern" as follow:

- More precise is the data we obtain, more harmful could be the threat;
- 3D geospatial data have enough precision to allow the use of dynamic network simulations with specific software (Epanet algorithm for water networks);
- GIS data usually contains important information with regards to the management of the network;
- Data can be accessible in different ways: when not available on webgis portals, the simplest way to obtain the data is to fake a planning of a project on a specific urban area and make formal request to the utility network companies.

1.2 IT active cyber attack

The "active" use of IT infrastructure when related to a real attack can be carried out through the following methods:

- hacking activities from remote connections to the mainframe management systems of a utility network
- through the direct connection to a hardline used to control and manage a network part

With reference to the appendix 1. "Water and terrorism chronology" shows that the use of "Active" IT Cyber-attacks on water infrastructure or supply is not a common means of attacking water infrastructure. In fact only 3 of the reported and documented 50 could be recorded as Cyber-attacks on water supplies. These 3 attacks are:

Date	Parties Involved	Description
1998	United States	The Washington Post reports a 12-year old computer hacker broke into the SCADA computer system that runs Arizona's Roosevelt Dam, giving him complete control of the dam's massive floodgates. The cities of Mesa, Tempe and Phoenix, Arizona are downstream of 50 this dam. No damage was done. This report turns out to be incorrect. A hacker did break into the computers of an Arizona water facility, the Salt River Project in the Phoenix area. But he was 27, not 12, and the incident occurred in 1994, not 1998. And while clearly trespassing in critical areas, investigators concluded that the hacker never could have had control of any dams and that no lives or property were ever threatened.
2000	Australia	In Queensland, Australia, on 23 April, 2000, police arrested a man for using a computer and radio transmitter to take control of the Maroochy Shire wastewater system and release sewage into parks, rivers and property.
2002	United States	Papers seized during the arrest of a Lebanese national in Seattle included "instructions on poisoning water sources" from a London-based Al-Qaida recruiter. The FBI issued a bulletin to computer security experts around the country indicating that Al-Qaida terrorists may have been studying American dams and water-supply systems in preparation for new attacks. "US law enforcement and intelligence agencies have received indications that Al-Qaida members have sought information on supervisory control and data acquisition (SCADA) systems available on multiple SCADA-related websites" reads the bulletin, according to SecurityFocus. "They specifically sought information on water supply and wastewater management practices in the US and abroad."

Tab 3.01 – An example Monitoring device

It seems that the Cyber threat to utility infrastructure networks really comes down to two key threats:

1. Taking control of hardware used to control assets
2. Obtaining data for terrorism planning activities

These two areas will be documented below:

1.2.1 Taking control of hardware used to control assets

If it was possible to take control of hardware used to control assets then it would theoretically be possible to either disable them from accurately monitoring contaminants in the water, or to cause damage by opening flood gates for water or sewerage (as per case 34 in Appendix 1).

1.2.1.1 Disabling Monitoring devices

To date two main approaches have been utilized to detect contaminants used to affect the quality of water supply.

Toxicity Monitoring:
Toxicity is the ability of a substance to cause a living organism to undergo adverse effects upon

exposure. These effects can include negative impacts on survival, growth, behavior and reproduction among others. Toxicity tests are an attempt to measure toxicity in a sample by analyzing the results that exposure produces on standard test organisms. (1)
Toxicity testing in the realm of security monitoring holds promise due to its ability to detect a wide variety of potential threats. This ability has lead to the development of a number of online toxicity monitoring devices as well as field verification kits that utilize a number of diverse organisms and methods to detect problems in the water supply.

Multi-parameter Monitoring:
Multi-parameter monitoring entails monitoring common water quality parameters and then looking for anomalies that may be indicative of a water contamination event. Sensors can include parameters such as chlorine residual, total organic carbon, pH, conductivity, turbidity, UV absorbance/fluorescence and others. One advantage of this approach is that it utilizes common, widely used instrumentation to make the measurements. Immediately after 9/11 the concept of deploying common sensors to act in just such a manner was investigated for water security monitoring. A number of government, academic and private industry studies evaluated a variety of sensors to see if they would respond to the contaminants most likely to be used by a terrorist in an attack. A number of instrument manufacturers have developed multi-parameter water quality monitors for both source water and distribution system water. These systems encompass a diverse selection of different sensors and can be tailored to meet monitoring needs.
The possible intention for disabling any monitoring devices would be to disable alarms for when an actual terrorism attack took place. This would mean that the pollutant could disperse further before being detected.

Fig 3.02 – An example Monitoring device

1.2.1.2 Controlling Floodgates

Controlling Floodgates could cause catastrophic effects on the community as mentioned in Case 26 (See Appendix 1) where a man attempted to hack into the SCADA computer system that runs Arizona's Roosevelt Dam, giving him complete control of the dam's massive floodgates. The cities of Mesa, Tempe and Phoenix, Arizona are downstream of this dam. No damage was done.
While this report turns out to be incorrect the effects of such a hack would be catastrophic to multiple cities in this case.
Referring again to Case 34 (See Appendix 1) where in Queensland, Australia a man took control using a computer and transmitter the Maroochy Shire wastewater system and was actually able to release sewerage into parks, rivers and property.
This case may not seem overly dangerous although it definitely illustrates the fact that remote control of a facility is possible and could cause a significant incident.

1.2.2 Hacking a webgis portal

Firstly the question needs to be asked as to why someone would want to hack a GIS Web Portal?

Fig 3.03 – Roiseavelt Dam

Two reasons can be considered 1. Disrupt the Web GIS Portal with the possible intention to disrupt the operation of critical infrastructure. And 2. Simply to obtain the actual asset data, this could then theoretically be used to plan a terrorist attack using the data for example; understanding the flow of water through a water network as per the Epanet network simulation.

See Appendix 3 – Al-Qa'eda plans cyber attacks on dams News article

1.2.2.1 Disrupt the Web Portal

Disruption can be caused by many ways, some of these include:

1.2.2.2 Obtain asset data

Stealing data as mentioned above in the previous point is an obvious way to obtain data, however analysis already shows that in the Milan test area how accessible the asset related data actually is. Anybody can request the data and if they are refused for any reason they can go to the next data provider and ask again. This points to a key issue in that the data should be accessed only via a central secure requesting service.
The below table shows the data providers and how you can request the same data from many different data providers, this is not good for security reasons.

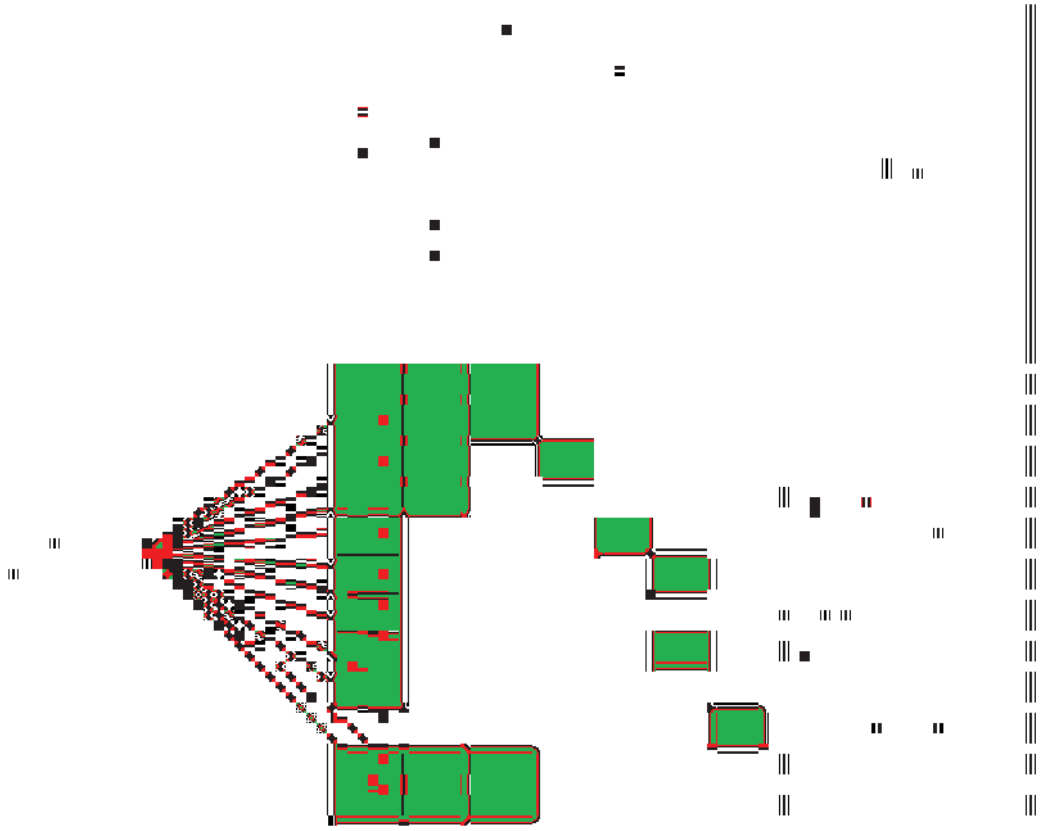
Evidence found on al-Qa'eda laptop computers in Afghanistan indicates that cyber terrorism could be a realistic possibility. Logs showed that al-Qa'eda members visited websites that offer software and programming instructions for the digital switches that run water, power and communications facilities.

One computer contained models of a dam, including software that could simulate a catastrophic failure. According to the FBI, the computer had also been running Microstran, a tool for analysing steel

Fig 3.04 – Quote from Appendix 3 News Article

Type	Comments
Viruses	A computer virus is a type of malware that, when executed, replicates by inserting copies of itself into other computer programs, data files, or the boot sector of the hard drive; when this replication succeeds, the affected areas are then said to be "infected". Viruses often perform some type of harmful activity on infected hosts, such as stealing hard disk space or CPU time, accessing private information, corrupting data, displaying political or humorous messages on the user's screen, spamming their contacts, or logging their keystrokes.
DDOS Attack	In computing, a denial-of-service (DoS) or distributed denial-of-service (DDoS) attack is an attempt to make a machine or network resource unavailable to its intended users. Although the means to carry out, motives for, and targets of a DoS attack may vary, it generally consists of efforts to temporarily or indefinitely interrupt or suspend services of a host connected to the Internet. As clarification, DDoS (Distributed Denial of Service) attacks are sent by two or more persons, or bots. Perpetrators of DoS attacks typically target sites or services hosted on high-profile web servers such as banks, credit card payment gateways, and even root nameservers. DoS threats are also common in business, and are sometimes responsible for website attacks.
Page Hijacking	Page hijacking is a form of search engine index spamming. It is achieved by creating a rogue copy of a popular website which shows contents similar to the original to a web crawler, but redirects web surfers to separate, unrelated or malicious websites. Spammers can use this technique to achieve high rankings in result pages for certain key words. Page hijacking is a form of cloaking, made possible because some web crawlers detect duplicates while indexing web pages. If two pages have the same content, only one of the URLs will be kept. A spammer will try to ensure that the rogue website is the one shown on the result pages. In some cases, legitimate web pages can be edited by external advertisers via XSS and redirected to promoting web site. In extreme cases entire web sites can be redirected to display for example extremists messages instead of the original web site content.
Corrupt database	Data corruption is the deterioration of computer data as a result of some external agent. The intention can be to render the system that accesses the database unusable. A common method of corrupting a database is to insert records into the database that can cause scripts to be run on the database, for example to delete all records and record could be inserted in a common executable string "del *.*".
Steal data	The action of stealing data via the internet, this mainly involves gaining access to a system and being able to download content.

Tab 3.03 – An example Monitoring device



Tab 3.04 – Data Providers

This table clearly illustrates the fact that a single person has many options for requesting utility information so apart from the fact that it is confusing for the legitimate users, the data has many failure points because if a security check was to take place for someone requesting information regarding the water network and the user was refused access, the user would then still have two other data providers to go to try again.

1.2.3 How to protect the data

Protecting GIS and utility data is a key responsibility for those who wish to stop unwanted access to their data sets. Some key questions to consider when putting forward a model to keep data secure;

- Who is responsible for the data?
- How should people gain access to the data?
- Who can gain access to the data?
- How is the data kept secure?

1.2.3.1 Who is responsible for the data?

Each individual asset owner should always be responsible for their own data, this means that they must control who can access their asset information and approve each person to have access. This removes the blame game and also means that data can only come from the owner themselves.

1.2.3.2 How should people gain access to the data?

Centralised access can be argued as a benefit because a single approval process could then be granted to a user who could then access and download GIS or asset plan information, the issue that comes up here is who will take on the responsibility of issuing access to other companies (private and government) data? Experience has shown (Australia, New Zealand, Singapore, United Kingdom, United States) that no-one is prepared

to take on this role on behalf of other asset owners. The model that has worked in many countries around the world is known as a OneCall model, this is simply a model that allows a single enquiry to be made by the person who needs the information. This request is then passed to the relevant utilities who can then vette the user as required and provide the information. The key is that the asset owner decides the action, if they are unsure of the user they can refuse them access or even arrange to meet them onsite to discuss their construction requirements.

1.2.3.3 Who can gain access to the data?

Only people who have been approved and possibly security checked should be allowed to access the data from utilities, this responsibility should still remain with the asset owners themselves.

1.2.3.4 How is the data kept secure?

The asset data is kept secure because the only way to gain access to the information is via a central portal where access is granted when an enquiry is passed across to them for approval. This means that data is not distributed through an uncontrolled network which often means that the data is never kept up to date.

1.2.4 Analysis of the system used by Regione Lombardia (Security)

The existing service that has been made available to users in the Lombardia Regione has some significant issues, these include:

- Security
- Who and Where data is accessed
- Data currency
- Disclaimers and Terms of use

1.2.4.1 Security

1.2.4.1.1 Ping - is currently enabled on the URL

This should be disabled because Ping flood is a simple denial-of-service attack where the attacker can overwhelm the victim with ICMP Echo Request (ping) packets. It is most successful if the attacker has more bandwidth than the victim (for instance an attacker with a DSL line and the victim on a dial-up modem).
The attacker hopes that the victim will respond with ICMP Echo Reply packets, thus consuming both outgoing bandwidth as well as incoming bandwidth. If the target system is slow enough, it is possible to consume enough of its CPU cycles for a user to notice a significant slowdown..
Unvalidated inputs is where you do not check whether text a user types into a field on a website is appropriate for that field.
Problem: Hackers use these fields to type commands that allow them to scan for vulnerabilities and gain access.
What you can do: Validate that each field accepts only those characters that are common for that field (such as numbers for a post code field) and are an appropriate length. Run the inputs against a small library of post codes and addresses to confirm that the information is valid.

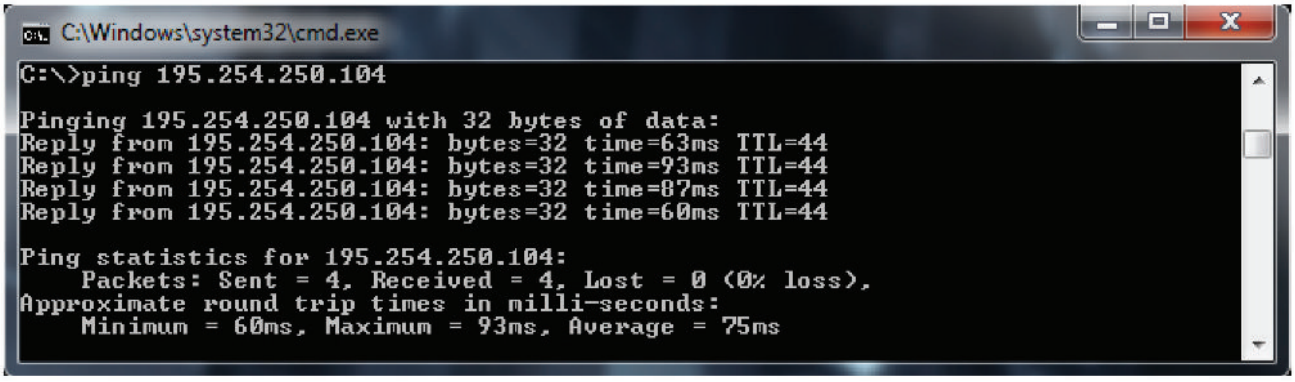


Fig 3.07 – Ping example for server

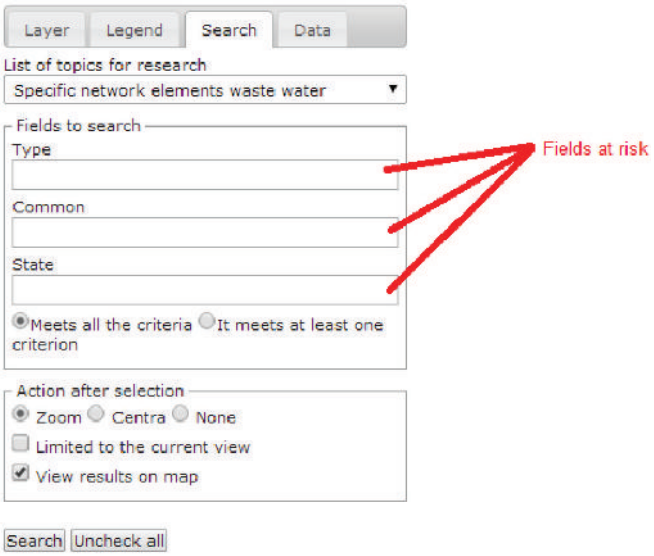


Fig 3.08 – Data entry fields at risk

1.2.4.1.3 Cross-site scripting

Cross site scripting is when a hacker sends commands embedded in queries to a website.
Problem: A hacker types JavaScript into any text field, such as a change-of-address field. When a legitimate user types information into that field, the JavaScript is activated, which allows the hacker to take control of the session and grants him all the user's session rights, enabling him to move money or steal credit card numbers. Javascript hacks could be typed into the fields shown in **Fig 3.08 – Data entry fields at risk.**

1.2.4.1.4 Buffer overflow

Definition: Allows an attacker to input more information than the buffer can manage.
Problem: Attacker can take control of the application server, gaining access to all the data that the server manages.
What you can do: Move away from C++ programming language, which is most vulnerable, to Java or .Net languages. If you must use C++, use static analysis tools to find overflow vulnerabilities.
What you can do: Make sure every text field will accept only those characters and length of characters that are suitable for that field--for example, five numbers in a ZIP code field and five numbers only.

1.2.4.1.5 Unsecured storage

Definition: Not protecting stored data using encryption, not properly securing the keys for accessing encrypted data, and not using effective randomness for passwords.
Problem: Once a hacker gains access to a system, non-encrypted data is easily accessed or hacker

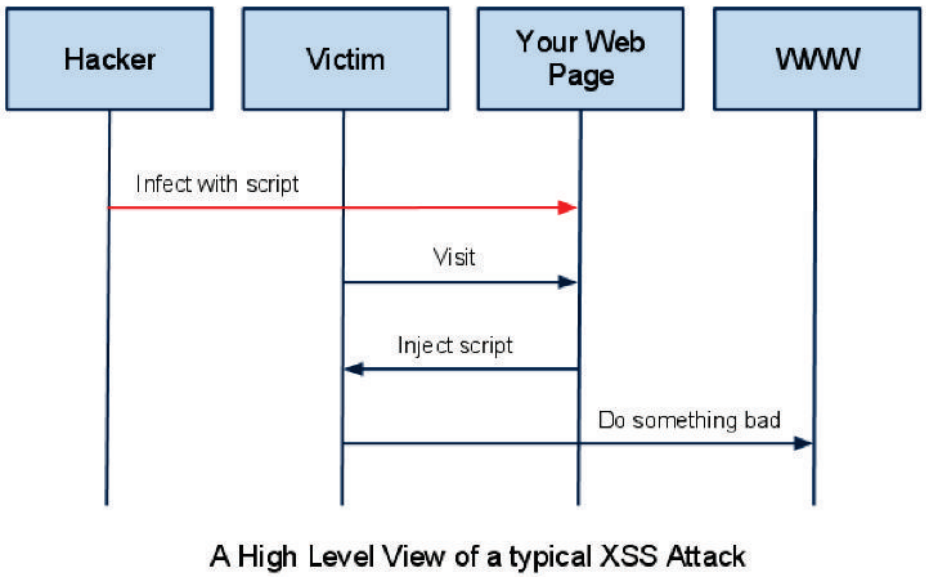


Fig 3.09 – XSS Example Diagram

can find unsecured encryption keys to gain access to encrypted data.
What you can do: Do not store data that is not absolutely necessary for the operation of the business, and minimize use of encryption. If encryption is used, store the master secret to open the encryption in two locations (say, a configuration file and an external sever) and assemble it at runtime.

1.2.4.1.6 Denial of Service

Definition: Sending thousands of queries to a Web server to overload the system, slowing it down or causing it to crash.
Problem: While not an attack meant to steal personal information, the attack is meant to be purely malicious by slowing down a business's online services and commerce.
What you can do: Require users to log on to your site so that you process queries only from legitimate users. Limit the number of queries within a certain time frame per user. After three log-in failures, lock out the user for a certain amount of time to thwart a DNS attack on the log-in app.

1.2.4.1.7 Insecure configuration management

Definition: Unpatched security flaws on server, use of default passwords or improperly secured passwords, improper file and directory permissions, and others.
Problem: A hacker scans for these vulnerabilities, and if found, gains access to administrative and other sensitive accounts.
What you can do: Create configuration security guidelines that lay out the specific steps that developers and Web operations staff must check off. Removes the debate between staff on how to set up proper configuration.

1.2.4.1.8 Broken access control

Definition: Access controls determine what a user can access after logging in to his personal account and blocks access to other accounts.

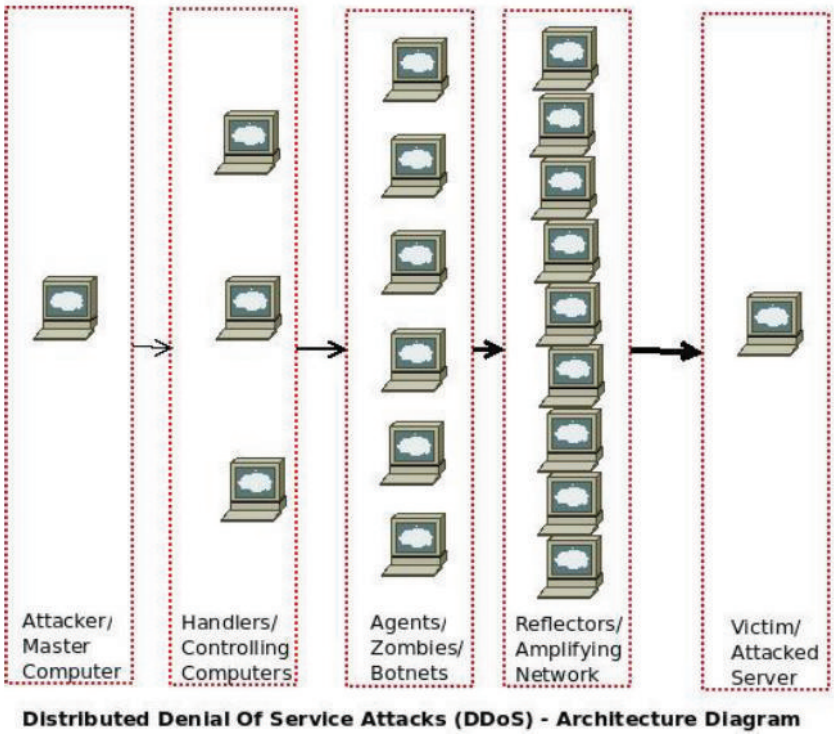


Fig 3.10 – DDOS Arhictecture Diagram

Problem: About half of all websites have serious access problems because of poor testing during development.
What you can do: Test all possible permutations of what a user may do to try to access information that is not his own.

1.2.4.1.9 Secure Login

A significant concern for this site is that it has no security in terms of restricting access to information for unauthorized users. As a minimum the site should have a registration page where users must register before being allowed access to anything. This will then allow each user to be pre-approved before they gain access. Without restricting users to this website you are allowing terrorists and the like to download this information about critical infrastructure which we know could be used to plan a terrorist attack.
If all users where made to register the owners of this service would know exactly who has made the download of data and for which area the data has been downloaded. Without doing this the data can be downloaded by anyone at any time and used for anything, this is very alarming!
Data currency is always an issue with critical infrastructure; this online service allows anyone to download the data and does not keep track of who or when they download the data. This means that no records of currency of data is kept, basically the data is immediately out of date as soon as it is downloaded.

1.2.4.1.10 Broken authentication and session management

Definition: After logging into a website with a user name and password, you receive a cookie that works like a hand stamp at a night club, authenticating your identity as you go through the site.
Problem: Sometimes companies will customize authentication, inadvertently allowing hackers to infiltrate sessions and use the ID cookie to access the legitimate user's account.
What you can do: Rely on the built-in authentication schemes in the application; use secured sockets layer (SSL) to encrypt the session.
Registration of Users also means you can enforce them to agree to Terms and conditions for how they will use the data, they can also agree to the currency of the data.

1.2.4.1.11 Sensitive Data Exposure

Sensitive data exposure is a significant risk for this web site, basically all data can be downloaded by any person who comes across the site. Even different option sare presented so the user can do this easily:
Many methods can be used to breach the security of data or a web site; the more common methods are shown in the table below:
The two methods highlighted in red (Sensitive Data Exposure & Cross Site Request Forgery) are both very relevant when looking at the Regione Lombardia webGIS Service.

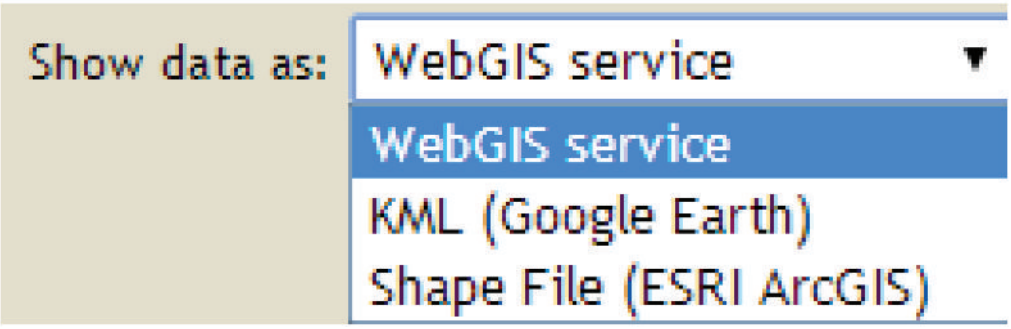


Fig 3.11 – Data Exposure

Method	Description
Injection	Injection flaws, such as SQL, OS, and LDAP injection occur when untrusted data is sent to an interpreter as part of a command or query. The attacker's hostile data can trick the interpreter into executing unintended commands or accessing data without proper authorization.
Broken Authentication and Session Management	Application functions related to authentication and session management are often not implemented correctly, allowing attackers to compromise passwords, keys, or session tokens, or to exploit other implementation flaws to assume other users' identities.
Cross Site Scripting	XSS flaws occur whenever an application takes untrusted data and sends it to a web browser without proper validation or escaping. XSS allows attackers to execute scripts in the victim's browser which can hijack user sessions, deface web sites, or redirect the user to malicious sites.
Insecure Direct Object References	A direct object reference occurs when a developer exposes a reference to an internal implementation object, such as a file, directory, or database key. Without an access control check or other protection, attackers can manipulate these references to access unauthorized data.
Security Misconfiguration	Good security requires having a secure configuration defined and deployed for the application, frameworks, application server, web server, database server, and platform. Secure settings should be defined, implemented, and maintained, as defaults are often insecure. Additionally, software should be kept up to date.
Sensitive Data exposure	Many web applications do not properly protect sensitive data, such as credit cards, tax IDs, and authentication credentials. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes. Sensitive data deserves extra protection such as encryption at rest or in transit, as well as special precautions when exchanged with the browser.
Missing Function Level Access Control	Most web applications verify function level access rights before making that functionality visible in the UI. However, applications need to perform the same access control checks on the server when each function is accessed. If requests are not verified, attackers will be able to forge requests in order to access functionality without proper authorization.
Cross Site Request Forgery	A CSRF attack forces a logged-on victim's browser to send a forged HTTP request, including the victim's session cookie and any other automatically included authentication information, to a vulnerable web application. This allows the attacker to force the victim's browser to generate requests the vulnerable application thinks are legitimate requests from the victim.
Using Components with Known Vulnerabilities	Components, such as libraries, frameworks, and other software modules, almost always run with full privileges. If a vulnerable component is exploited, such an attack can facilitate serious data loss or server takeover. Applications using components with known vulnerabilities may undermine application defenses and enable a range of possible attacks and impacts.

Invalidated Redirects and Forwards	Web applications frequently redirect and forward users to other pages and websites, and use untrusted data to determine the destination pages. Without proper validation, attackers can redirect victims to phishing or malware sites, or use forwards to access unauthorized pages.

Tab 3.12 – Data Security

1.2.4.2 Analysis of the system used by Regione Lombardia (Attack)

Stealing data is a significant issue with this site, in fact with no security today it means that no-one knows how many times data has been download nor is it known who has downloaded the data. Also the fact that the many types of data is stored on a single server means that it is ever less secure.
A OneCall Service will never host any asset data, this is the core to offering a secure service. The way that the OneCall service works is to register Areas of Interest for each asset owner and when an enquiry is made and falls within one of these areas then the asset owner is passed an enquiry. All users must register to use the OneCall service, these contact details are then passed to the asset owners when an enquiry is relevant to their network base. The asset owner then critically makes the decision as to who can have access to their
information and asset data. This means that each asset owners has complete control over who accesses their asset data.
When a User makes an enquiry they only see a street map (no assets are shown), the reason is that the user is required to define the area that they are interested in, this allows the OneCall Service to keep a historical record of all enquiries by all users.

1.2.5 A Proposed data model

A OneCall Service is a "Plan Request" service designed to assist anyone who requires underground or above ground asset plans for their proposed dig site. The OneCall service enables people to request plans from utilities in a very simple step-by-step process. Once the request has been made each relevant utility is sent a request for asset plans for the nominated site.
This model means that the user does not see any assets until the individual asset owners send the information to them.
The steps to commence making enquiries is to first register user details with the OneCall service, the registration process should make the user confirm their email address via a simple user validation email.
The second step is to log in and draw on a map (a blank street map – not showing any utilities) where plans are needed, these areas should be restricted so that a user cannot request plans for an entire suburb/city with a single enquiry.

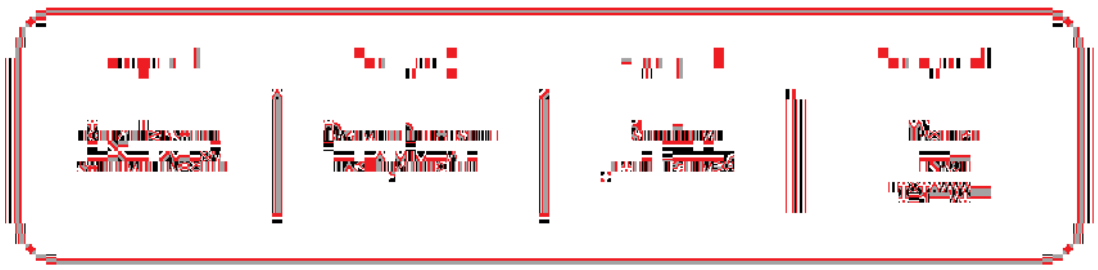


Fig 3.05 – OneCall steps

Step 3 is confirming the actual enquiry process, once this is done a list of the affected utilities is listed but again no asset data is shown to the end user. It is at this point that a formal request (enquiry) is passed via email to the utilities.
When the utilities receive the enquiry from the OneCall service it is then up to the utility to decide if the person requesting should actually be allowed to gain access to the data.
This is then followed by the Step 4 for the user which is about receiving their responses from the relevant utilities.

1.2.5.1 The OneCall process

The below process flow helps to explain the flow of data from firstly the request form the user to the enquiry being passed to the relevant utility and then finally the data or plans being passed back to the person making the initial enquiry.
As Table 3.23 shown earlier illustrated the lack of a coordinated approach the above model means that the entire process is now completely clear and that all enquiries must be processed via this model, if they are not then no information will be provided.
Step 1 is a User making an On-line Plan Request before commencing any excavation work. Information collected from the User includes, contact details, and site location information including a map.
Step 2 is where the OneCall Service searches its Utility(1) database to determine which Members should be sent a Notification. The Notification will provide text and geographical information to describe the Dig Site to the Utility.
Step 3 involves the OneCall Service sending the User an Enquiry Confirmation email, this email details three key areas about the users request, 1. Contact details used for this request, 2. Information about the proposed works, 3. A List of the Utilities who have been requested information on the Users behalf (2).
Step 4 of the OneCall process is where the Utilities provide feedback to the User regarding their assets at the location detailed by the User.

(1) The Utility database is not a database of all assets for the utilities; instead it is just network areas for where the utilities have responsibilities. The way the system works is that if an enquiry falls within one of these "Areas" then that utility is sent a request for information.
(2) This list does not provide any details or maps of the actual assets.

1.2.5.2 Utility Responses

Utilities become members of the OneCall Service, Membership means you will be notified when someone is planning works near your assets and you then have the opportunity to respond to these enquiries with clear instructions on how you believe the user should proceed. Common responses by members include:

1. Assets Affected – This will often include a Letter, Plans, and guidance notes.
2. Assets Affected – Halt Notice, this normally means that the Member will send a representative out for a site visit.
3. No Asset Affected – This normally includes an email response informing the user that their dig site will not affect the particular members' assets.

1.2.5.3 Utility Benefits

The OneCall Model serves the common needs of all asset owners in providing tools to protect underground assets and communities and allows them to adhere to regulatory requirements in preventing workplace injuries. By being a member of a OneCall Service asset owners can reduce the cost of asset repairs from accidental damage, reduce the environmental impact by managing the works around assets through better planning and coordination.
A major benefit of OneCall membership is information. Members receive valuable information about what is happening around their underground assets. This enables them to know:

- Who is working close to their assets;

- What type of work will be done;
- When the work will be done; and
- How to demonstrate their duty of care.

1.2.5.4 Security of Data

Members have complete control over who can gain access to their data, in fact each new enquirer that makes an enquiry needs to be approved by each of the members of the OneCall Service. This adds a security layer which helps stop unlawful access to the relevant data from the utilities.
The User Approval Model can be seen below; this shows the full request process and then the enquiry being passed across to the Utility.

1.2.5.5 Historical information

All searches are archived so investigations can be undertaken after any attack or breach to any network. This is a key component of a OneCall Service in that all enquiries and users are always archived. Each of the Utilities will also have an archive of all responses that have been sent to users from their own systems.
Historical information which is stored for all enquiries is extremely valuable when needing to look back at who has made enquiries and to possibly understand who has made an enquiry for a particular location, this has been used in many cases where damamges to networks have occurred and the network owner is looking to find out who caused the actual damages. The data has also been used to understand wether or not a person has actually made an enquiry, if not and they have damaged an asset then their legal stand poitn is significanlty weakened.

1.2.5.6 How should the data be provided?

Data can be provided in a number of formats, this can vary on the readiness of data in many cases. Examples of different data formats includes:
If data is provided in GIS format then it is much easier for people to run simulations and understand for example how the water may flow through a network.

1.2.6 Examples of data protection

Singapore – When a person wishes to obtain asset data in Singapore show ID in person to collect your asset plans
United States – Markups only, people cannot obtain asset data from utilities as the standard process for providing knowledge of where an asset is located is by sending out a "Locator" who will markup the path of the asset. Commonly this is either spray painted on the ground or marked

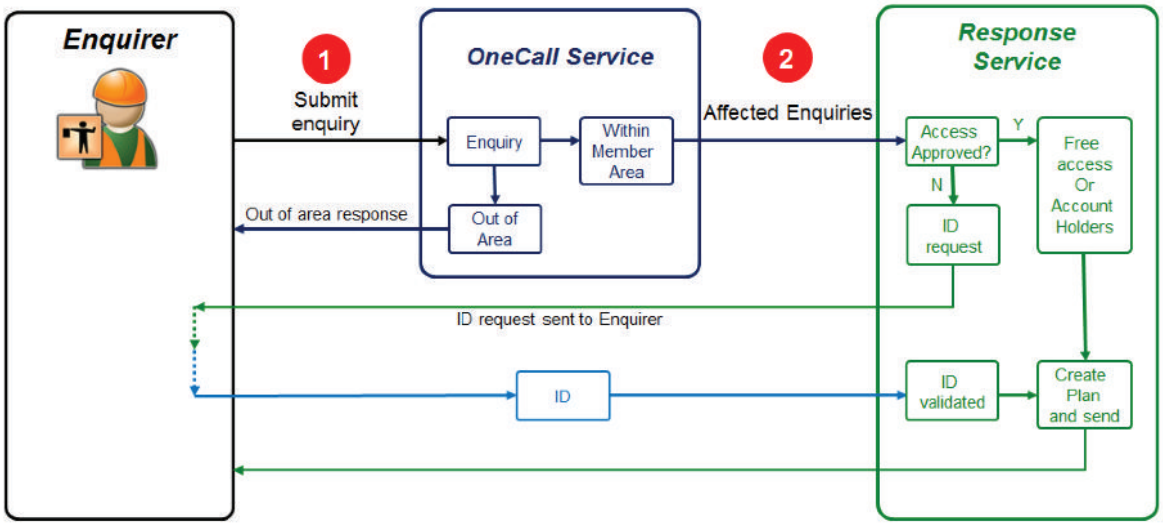


Fig 3.08 – The User Approval Screen

Data Format	Comments
Paper	Often companies who are yet to adopt a GIS system still have their data in Paper format, the easiest way to work with this is to scan the plans (assuming they are not too large) and then send them in PDF format.
PDF	A common and relatively safe format to send plans in, means that the user cannot easily extract the data from the PDF format but they can still see relevant details of network locations.
GIS (SHP/DXF/DWG/etc)	This is actually an uncommon format for asset owners to send information to users in, naturally it allows the users to overlay other asset layers at the same time which is good for planning. The downside is the security of the data and the fact that approved users will often hold onto old data for long periods of time instead of making new enquiries.
Image (JPG/GIF/etc)	A Raster file showing a map and the relevant asset layers, this is often seen as a primitive format because of the raster format in that it will pixelate if the user zooms in.
Live	This is when an online viewing portal is made available where utilities can make their data accessible, the data is only made available to those who have made an enquiry and it is only available for the particular site that they have expressed interest in.

Tab 3.09 – An example Monitoring device

with flags, different colours are used to illustrate different asset types (gas, water, electricity, etc).
Countries where Onecall service operate
Many countries already operate OneCall services, these countries include:

- Australia
- New Zealand
- Singapore
- United States
- United Kingdom
- Ireland
- Japan
- Canada
- Denmark
- Scotland
- France

1.2.6.1 Quotes about OneCall Services

Some quotes from these countries about the virtues of having a OneCall service:

"The use of 'OneCall' systems is recommended where available. This allows those who wish to excavate to obtain plans from a range of owners and operators through one contact"
(Avoiding Danger from Underground Services HSG47 HSE Books ISBN 0 7176 1744 0 - UK)

"…register(ing) a proposed project with the one-call centre's database offers the opportunity to identify, without guesswork, a succinct list of underground facility owners/operators"
(Damage Prevention Best Practices Report Version 7.0 Common Ground Alliance - US)

"The (OneCall) service was established as a means of simplifying contact between a customer and the many underground asset owners within a given excavation site."
(Service Guidelines for Vic/Tas 2009 Dial Before You Dig Vic/Tas Incorporated ABN 69 900 619 916 - AU)

1.2.6.2 Examples of Legislation

IRELAND

"Up-to-date plans of all potentially hazardous underground services in the area should be obtained before excavation work begins. Where possible, providers of all relevant underground services should be consulted."
(Code of Practice for Avoiding Danger from Underground Services Health & Safety Authority ISBN 978-1-84496-118-4 - IE)

UNITED KINGDOM

"The use of 'OneCall' systems is recommended where available. This allows those who wish to excavate to obtain plans from a range of owners and operators through one contact"
(Avoiding Danger from Underground Services HSG47 HSE Books ISBN 0 7176 1744 0 - UK)

SINGAPORE

Duty to enquire before excavation. Any person who digs, bores, trenches, grades, excavates or breaks any ground with any mechanical equipment or explosive or allows his employee or agent to do so without first ascertaining the location of any main or pipe belonging to or under the management or control of the Board that may be interfered with shall be guilty of an offence and shall be liable on conviction to a fine not exceeding $50,000 or to imprisonment for a term not exceeding 3 years or to both.
(PUBLIC UTILITIES ACT Chapter 261 www.agc.gov.sg - SG)

INTERVIEW WITH ENRICO BOI

Vice President Georadar Division for IDS North America

USING GPR

For the creation of a register of underground infrastructure, you need that geographical data representing the reality. The source of data is a matter of crucial importance in relation to the quality, usability and cost of the project. The use of different technologies brings to different results, related both to quality and cost. There explains it in this short interview Enrico Boi, who is now Vice President Georadar Division for IDS North America, managing geosystem and slope monitoring applications.

1) Are there advantages using GPR in comparison to topographic methodologies?

…..If only I had a dollar for every time I was asked this question, I probably would not be rich by now, but ……. This question has been asked many times by engineers, technicians, planners, designers, and sometimes by politicians, only the good ones I would say !

The curiosity has no national boundaries and it is horizontal within all the civilized countries, considering in our case, civilized, the ones that have underground utility networks.

The answer is not so simple how it may look at a first thought, because the potential advantages are multiple, spanning on different fields, most important of all: engineering; planning; health and safety, environmental and quality of life (of the citizens), and last but not least financials aspects.

It is also interesting to see how the majority of the research to properly answer this question, has been carried out by engineers. Consequently you may find answers that are mainly related to pipe position accuracy or pipe location.

But let's look at the different fields a little more in detail to see what answers we can now give to this crucial question:

Engineering approach

As mention before, the engineers are the ones that researched most, for this answer, and surely, engineers are the ones that have asked this question to themselves earlier. The result of this research is available through several Standards on underground utility mapping that have been relished in the last 15 years. The American ASCE issued the first Standards that, classifies, using 4 different quality level of mapping, the different methodologies normally used for utility mapping, or as the Americans call it, the Subsurface Utility Engineering. This standard considered the use of topographical surveys, as integration of the data from utility records, one of the possible way to design a utility mapping campaign. The same standard classifies the use of GPRs for utility mapping as a different quality level, and from a hierarchic point of view a more precise and defined one. The Americans were then followed by Canadians, Australians, Malaysians, the British, and now by the Italians, all of this Standards follows the same basic structure at 4 main quality levels, and all of them classify the topographical survey at a low level, while the use of GPR at an higher level.

Therefore, to answer your question, the main advantages of the use of GPRs in comparison to topographic surveys are (engineering approach):

- Mapping of the buried lines in their real position, instead of point to point mapping achievable with topographic surveys of the position of manholes or surface related infrastructures;
- Location and mapping of all the buried utilities, even if they don't have any reference with surface infrastructures;
- Ability to define the occupied areas in the underground, and the real extension of a buried infrastructure;
- Ability to identify the Z (depth) coordinate of the mapped infrastructures;
- Ability to locate and map the service pipes or house connections.

Planning approach

All planning initiatives needs reliable data for the positive outcome of the planning exercise. Higher is the data quality, better will be the evacuation of the parameters for the planning.

Whatever planning we may talk about: urban; asset management; renovation, etc.; the equation of better data equals better planning does not change, defining in this way the main advantage of the use of GPR instead of topographic survey.

Health and safety

This aspect is becoming day after day, more and more important for decision makers and

lawmakers. Health and Safety regulations are getting more complex and efficient, and most of all, are expanding in every sector, with particular emphasis in construction.
Excavation activities have always be considered high risk, mostly because of the lack of knowledge on the position and existence of buried utilities. Even in this modern years, we register an incredible high number of casualties and injuries, all caused by lack of information.
Having access to more reliable and accurate data on buried infrastructure is indeed a great advantage that can help mitigate site accidents and increase health and safety on construction sites.

Environmental and quality of life

How many times I have witnessed utility construction projects where excavation were carried out in different locations than where they were supposed to, all causing delays, extra hours of excavators and trucks usage, large quantities of earth to be excavated and moved.
All activities with heavy impact on atmospheric and noise pollution, and with a very high social cost.
Approaching site activities that includes excavation, without the proper knowledge of the existence and position of buried infrastructures can extremely affect the environment. Having access to high quality data with regards the existence and the 3D position of the buried infrastructures, can make the difference. GPR data is more complete and precise of topographical surveys data, and this makes the advantage for the use of one against the other.

Financials aspects

Analyzing the financial aspects related to the "convenience" of using topographical surveys or GPR survey mapping, is indeed a complex matter. To be able to evaluate the economic benefits of one method against the other, we need to insert them in a contest with defined parameters.
This activity has actually been carried out, to my knowledge, by several universities in the US, and a research project in Italy sponsored by Regione Lombardia, with the participation of IATT the Italian Association for Trenchless Technologies, and ANCI Lombardia. This project, where I was involved as the responsible of all the surface and subsurface mapping and cartographic layout, provided us with unexpected results with regards of the economic feedbacks in relation to the direct benefits of the use of high quality data against simple data. The project showed that, even if with a higher cost, the GPR mapping is, because of all the benefits, more convenient of a topographic survey that is cheaper but less reliable.

2) What are the peculiarities of a GPR relief?

Leaving on one side the possible different choices, with regards to cartographic layout, that are normally dictated by project specifications, the main characteristic of a map created with GPR processed data, is the survey database where all the 3D information of the mapped underground infrastructures are stored. GPR data, if collected in a proper way, can provide very detailed information about underground mapping infrastructures.
An high density GPR acquisition campaign, delivers an amazing high volume of information, that are made available to the engineer in charge of the data analysis. This engineer will choose how many information will be translated into CAD, and how many will remain available inside the dataset for further evaluations, if needed.
Furthermore, to answer the question, the following characteristics are probably the most important:

- The located underground infrastructures are, or can be, identified by a large number of points extracted from the radargrams;

- The located underground infrastructures are highly reliable with regards to the Z coordinate, the depth. This is calculated normally from the surface;
- The extracted cartographic layout can be verified accessing the available radar data.

3) How many types of GPR exist?

We can classify the georadars in two main families, the Pulsed ones and the Stepping Frequencies Continuous Wave, commonly known as SFCW.

The Pulsed one are the most common one and are largely produced and used worldwide.

The SFCW are, right now, only used in specific applications, but they are not commonly used for utility mapping applications. This technology is under development right now and it is believed it will be more commonly used in the coming years.

Within the Pulsed Georadars we can define 3 main groups of configurations:

Georadar Single Frequency – Single Antenna:

Generally quite simple systems and easy to transport, composed of an antenna, an analog-digital decoder, a laptop for recording and displaying data. On average, in the case of systems designed for the mapping of the underground, these systems have a lateral dimensions of about 40 cm. These GPRs usually have the transmitter antenna and receiver arranged so as to ensure the detection of linear target (such as tubes) perpendicular to the scan direction (a single polarization antenna); in this case the scans must be conducted along perpendicular directions (grid measurement) to ensure detection of all the existing pipes, regardless of their arrangement with respect to the grid.

The position of the GPR on the scanning plane is normally recorded through an odometer.

Usually the radar sections can be viewed in real time, during capture, or in post processing using special software.

Because of their relative simplicity and low cost, are widely used systems.

Multifrequency Georadar, multiple antennas with single polarization:

Antenna's array systems, generally modular. These systems are able to simultaneously acquire a large number of channels, usually up to 8, increasing the efficiency of both data acquisition and data processing. The lateral dimensions of this type of antenna array can reach 200 cm.

These radar systems typically use antennas arranged in the same way, ie with the same polarization; Therefore, these systems are to be used by performing scans along directions perpendicular to each other, as mentioned in the previous paragraph. Some systems may have one or more antennas arranged with a different polarization and used, for example, to perform data acquisitions defined cross-polar.

Normally, these systems capture the position data through an odometer, in some cases can be also used a cartographic GPS.

Usually radargrams can be displayed in real time during the acquisition, but, in complex cases, it is required data post-processing.

These systems are moderately popular and used by companies specialized in utility mapping.

Multi antenna and multi polarization georadar, mono or multi frequency – high dense array

Antenna's array systems, generally modular, often referred as complex array. These systems are able to simultaneously acquire a large number of channels, increasing the efficiency of both data acquisition and data processing.

The lateral dimensions of this type of antenna array can reach 200 cm.

These radar systems uses antennas arranged to perform the data acquisition using only the forward direction of the radar, longitudinal to the road direction. Some antennas, in fact, are arranged so to collect data in the

direction perpendicular to the direction of scan and then to allow the creation of sections defined radar "synthetic" (representing the cross-sections with respect to the direction of the scan).
These systems, developed recently, allow the optimization of the site acquisition activities by reducing the number of sections to be acquired.

Normally these systems acquires ther position through an odometer together with a GPS positioning system, or robotic total stations.
In the market there are different radar systems with these features, some of these have the possibility to display the data acquired and processed in real time.
These systems are not widespread and commonly used by companies specialized in utility mapping.