ESRC Social Contexts and Responses to Risk Network

Cambridge, 29-31 March 2007

Technology in risk communication: opportunities and limits

David Domingo (Universitat Rovira i Virgili)

Enric Castelló (Universitat Rovira i Virgili)

Digital information and communication technologies (ICTs) are usually portrayed as enabling better industrial risk and crisis management. Databases, surveillance cameras, online messaging, virtual simulators and wireless communications allow emergency teams to offer a quicker and more efficient response, and preventive information can reach easier more citizens. But the use of digital technologies also has limitations and can add risks: systems may crash, design might be inefficient, users may misuse software and hardware. This paper draws a conceptual framework that allows a critical approach to technology and risk communication, an approach that is sensitive to the opportunities and shortcomings of this uneven relationship. This framework counters technological determinism (found both in euphoric and catastrophist discourses on technology and risk) and helps in assessing the communicational weaknesses and strengths related to technology of industrial risk prevention and emergency systems. A case study in a leading European industrial cluster is used to illustrate the conceptual proposals.[1]

[1] This research has been developed in the project 'The process of risk communication in Tarragona: analysis of social perception and reception of petrochemical risk. Social participation, social communication and proximity communication', directed by Dr. Jordi Farré Coma and financed by the Spanish Culture and Science Ministry with the number **SEJ2004-00892**.

1. Theoretical framework and objectives

As Donald MacKenzie and Judy Wajcman point out (1999: 3-4), technological determinism is partly right: technology matters. Not only from the material point of view or because it facilitates daily human activities, but also because it affects how we relate to one another, how we create social links and how we communicate. The emergence of new technologies may also lead to changes in social structures. However, these authors stress the fact that technology is part of a much more complex system and it is only one of the reasons why society changes: politics, economy and culture are also elements that cause changes, speed them up or slow them down. Thus, new technologies that facilitate communication do not necessarily make our daily activities more effective. What is more, the use of technology *per se* does not lead to better management if there is not an appropriate political, economic and cultural environment to facilitate and guide use.

The implications of technology in risk management cannot be analyzed in abstract terms. Technology can only be understood in the social context in which it is used (Bijker & Law, 2000): different contexts can mean different definitions of what a technological tool has to solve, how it will be used, who it will be used by, how valuable it will be in comparison to other elements of risk management, etc. Technology is not only the equipment (software, hardware, surveillance and measurement tools), but also the rules governing how it is used and the meanings it is assigned. In this article, we attempt to explore this "technological system" (Bijker et al. 2001) through a relevant case study: the emergency centres of the Catalan Government, which manage the surveillance and response to petrochemical risks of one of the biggest European industrial area, Tarragona, in the North-east of Spain. The in-depth analysis of a case lets us drive conclusions on the organization and dynamics of the uses of technology in risk communication. Even though the conclusions cannot be directly generalized, we believe that this Catalan case may be representative of other organizations and institutions.

Public institutions in the Western world have attempted to predict, prevent, manage and respond to such situations of risk as natural disasters, extreme climatological phenomena, nuclear or chemical accidents, terrorism or so-called low-intensity daily

risks (exposure to waves, noise, radiation, etc.). The development and use of technology may be able to mitigate disaster situations, as long as access to this technology is universal. Thus, a more democratic distribution of the ICT could mitigate the devastating effects of natural disasters, such as the terrible results of the tsunami in 2004 in Indonesia (Samarajiva, 2005).

The so-called information and communication technologies (ICTs) have often been identified with Internet. However, ICTs are not only Internet: they are all those technologies used to process, store and transmit the information used by computer and telecommunications systems. Besides the emergence of the Internet, the implementation of high-capacity communication networks, the development of computer systems and programs that enable simulation scenarios to be created, the advances in telecommunications with GPS (Global Positioning Systems) or the interconnection of powerful databases have all led to improvements in risk management.

Nevertheless, the use of ICTs in the field of risk communication and emergency management also involves new risks. Claudio Ciborra (2004) approaches the issue of technology from the economic perspective and considers that technology involves a duality because ICTs tend to have a life of their own and little attention is paid to the technical interdependencies between the old technologies and the new technological platforms. Ciborra (2004: 12) believes that change and innovation in risk management can generate new risks.

He argues that merely technological or emergency management points of view are not completely valid if the complexity of risk communication is to be measured. In our case, although some applications of technology may fail, petrochemical risk may lead to fatal consequences that are difficult to assess in economic terms. Traditional risk analysis, often based on technical schemes that use the formula "consequences multiplied by probability" for purposes of measurement, is now almost obsolete if all the factors of a petrochemical disaster, for example, have to be taken into account (harmful effects on the population, the environment, future perspectives, infrastructures, etc.). Ciborra also argues that basic risk management models make several assumptions: a linear logic prevails in which organizations are seen as structures in which bosses

make plans, and objectives dictate decision taking; control and planning are key activities for designing strategies; evolution and change are seen as improvement processes based on response, which can be managed and measured; or it is assumed that the trial-and-error learning system is used. But the reality is that organizations that use ICTs are at once more controlled and more difficult to predict (Ciborra 2004: 14). Ciborra's basic idea, which we have used here, is taken from Beck, Giddens and Lash (1994), and is based on the duality or "reflexivity" of ICTs in relation to risk:

> Reflexivity refers to the fact that every new technology or regulative measure aimed at controlling risks, such as the grid technologies, inevitably creates new risks originating from regions beyond the control of the new powerful platforms. In other words, the more we are able to extend the frontier of (formalised) knowledge thanks to technology, the more dangerous could be the events emerging out of the regions of our ignorance (Ciborra: 2004:14).

Therefore, we consider that the use of ICTs, the availability of advanced management equipment connected to information networks and databases, means both greater control and greater risk. Control is often implemented by applying the technique of prevention, which involves simulating emergency situations and carrying out tests or drills. Technology has been an ally in this task of "simulating reality", which centres for civil responsibility have spent so much time on. Even so, we have to understand other drawbacks of using ICTs.

"Simulation" often attempts to emulate reality. Therefore, "simulations" are "approximations of possible scenarios" that technology allows us to create to assist in making decisions or taking action. Emergency management centres use various technological mechanisms to carry out these simulations. In the first place, they use computer applications that make it possible to "represent real scenarios". For example, a program can reproduce the direction in which a toxic cloud or a chemical slick on the sea will travel if it is configured correctly and the appropriate parameters are entered. Likewise, cameras are often used to give emergency centres an instant view of the accident that is causing the risk, a representation of what is happening.

Technological "simulation" systems and cameras undoubtedly help to reproduce the reality and make decisions during emergencies. Some authors have also pointed out the usefulness of mapping systems and the need to integrate information for risk

communication management (Drew et al. 2004). However, systems for reproducing reality also have their drawbacks: they are not reality but, like everything that surrounds communication, only a version of it. So the most reliable vision of a risk situation is often assessment in the field, which has to be carried out by land or air.

As Lundgren and MacMackin have pointed out (2004: 352-252), ICTs can help to reproduce risk situations so that the population can learn what to do in an emergency situation. Detailed emergency plans can also be drafted that require intensive use of ICTs or the population to use technology. Nevertheless, as these authors remark, the more we trust in technology in emergency situations, the more exposed we are to a technological error or disaster causing a risk:

> In recent years, various crises in the United States have crashed the Internet, overloaded phone lines, rendered cell phone towers inoperative, and triggered multi-state electrical blackouts extending into Canada (Lundgren and McMackin, 2004:367).

Although ICTs can give us a feeling of security in advanced societies, they cannot predict, control and respond to everything. As welfare based on technological mastery increases, the possibilities that the system will break down also increase. As Dwayne Winseck has pointed out (2002), the availability of technology and information can create an *illusion* of perfect information or a *fantasy* that society is under control. The society of risk and uncertainty also involves more ICT development, which attenuates how we perceive them. The logic is circular: the greater the risk, the more technological developments are required, which in turn lead to new unforeseen risks coupled with a naive sense of control. So how should we manage risk communication and how can we use ICTs in emergency situations? There is no single, easy answer; not even a correct one. Perhaps the study of specific situations, analysis, prevention, information and education, transparency and rationality can help us to make effective use of ITCs, provide us with suitable risk communication strategies, and respond efficiently in emergency situations.

In this respect, our study focuses on the use of ITC in the centres involved in petrochemical risk management in Tarragona: the National Emergency Centre of Catalonia in Tarragona (CENCAT) and the Emergency Coordination Centre of

Catalonia in Bellaterra (CECAT). The aim of the study is to describe the strengths of using ICTs to manage petrochemical risk, but also to point out what are or what may be their weaknesses and drawbacks. The essential idea on which we base our analysis is that the mere availability of technology does not necessarily improve emergency management; rather, other elements are required if the technological experience is to be optimum.

2. Methodology and object of study

To carry out our research, we made several in-depth interviews with head technicians or ICT users in the emergency centres studied. We also observed a chemical emergency drill in Tarragona (Plaseqta) and finally analyzed documents provided by the administrations about the technological structures and uses of the centres, as well as information that the Catalan Government published on the Internet.

In Tarragona, petrochemical risk is managed by the CENCAT, which depends on the General Directorate of Emergencies and Civil Safety of the Department of Justice and the Interior of the Catalan Government. This centre, however, functions as a subcentre or branch of the central emergency management office located at the Emergency Coordination Centre in Bellaterra. So the CENCAT in Tarragona is not an isolated or autonomous management unit; rather, it functions in coordination with the Bellaterra centre, where activity is centralized and the political decisions are taken. Understanding this structure was important for the research design, because this bipolarity and branch relationship needed to be taken into account.

The CENCAT is responsible for activating and managing the Plaseqta, the petrochemical emergency plan in Tarragona, while it also acts as a sort of backup of the centre in Bellaterra, where the final technical and political decisions are taken. Although this duplication of centres may involve some redundancy and create some management confusion, it can also be a safety mechanism, because all emergency centres should have another physical space to assist and provide backup. From the technological point of view, redundancy functions as a safety mechanism, which minimizes risk and can improve how emergency situations are managed.

Thus, we designed and carried out in-depth interviews with people involved in petrochemical risk management both at the Tarragona centre and in Bellaterra. These face-to-face meetings attempted to understand the activities and situations of the informants (Taylor & Bogdan, 1987). The method was particularly suitable because the information sought was not accessible in any other way. In the interviews, questions were asked about the daily use of ICT by staff or the technological design of the centre, its functionalities and shortcomings. We paid particular attention to the vision of the workers and section heads as users. The informants were selected bearing in mind their position in the organization and their relation with the use of technology.

The interviews took into account the function of the informants and asked them about their personal vision of the use of ICTs. The professional experience of the informants was also an important factor. The material obtained was duly transcribed and the text analyzed. Issues were separated, information on each specific issue was checked and the responses were systemized so that conclusions could be drawn about the object of study.

As far as the observation analysis was concerned, the research group organized a study session that consisted of attending a petrochemical emergency drill. The fieldwork consisted of collecting information about the uses of ICT during a drill in which sirens were set off in the districts of Tarragona closest to the sea. According to Taylor and Bogdan (1987), participatory observation is a good way of witnessing what is being studied at first hand. In our case, we positioned three researchers at three different points in the emergency room during the exercise. Although some of the actors knew why they were there —otherwise they would not have been allowed to enter—, researchers kept a reasonable distance, and only asked some very specific questions and noted down all the events and conversations possible during the exercise.

Finally, the research was complemented with the documental analysis of a variety of statistics provided by emergency centres about the nature of the calls to the emergency number (112) and the technological structure of the centre, and the information available on Internet, which is published and managed by the Department of the Interior of the Catalan Government, about chemical risk in Catalonia.

3. Internal and external communication

The emergency coordination centres in Catalonia are equipped with advanced technology for managing and transmitting information. This article is not the place to give a detailed description of all the technical mechanisms that are used daily in Bellaterra and Tarragona to prevent, control, and manage different sorts of emergency. Even so, after studying the documentation provided and made several visits to the centres, we believe that it is useful to make a basic distinction between the technologies that are used to manage and control risk from the point of view of **internal communication** (within the organization) and those that are activated when it is necessary to contact other organizations, the population, institutions or businesses (that is to say, **external communication**).

In this respect, the first remark that has to be made is that there is a considerable imbalance between the ICTs used for internal and external communication. The emergency centres studied have a wide variety of ICTs at their disposal, which they use daily in their internal communications, but when they have to communicate with other organizations and with the population, they have clear technological limitations.

Table 1. Scheme of the use of the ICT in the emergency centres

Internal communication		**External communication**	
Intra and inter centres	Conventional telephony	Institutions, council, companies	Conventional telephony
	Mobile telephony		Mobile telephony
	Internet		Internet
	Intranet		E-mail
	E-mail	*Population*	Internet
	Optical fiber		Sirens
	Dedicated radio network		Conventional telephony (being tested)
	Internal and external		

	cameras		
	Internal public-address system		
	Interconnected databases		
	Interconnected simulation applications		
Mobile units	GPS		
	Mapping and databases		
	Radio		
	Mobile telephony		

Source: authors

Table 1 shows the variety of ICTs commonly used for internal communication. Among other mechanisms, the centres have systems of internal telephony which make it possible for any department to be contacted by means of extensions, so communication is immediate and direct. On an internal level, mobile telephones are also widely used, both for voice and for data. An automatic system for sending SMS (Short Message Service) keeps the people in charge and the politicians up to date with news about the most important incidents. The centres also have an Intranet and are in constant contact via e-mail.

As far as transmission supports and transmission systems are concerned, it should be pointed out that the centres are connected not only by phone but also by a high-speed optical fiber network. Likewise, they can communicate with each other and also with mobile units through a dedicated broadband radio network. These connections lead to immediate, high-quality internal communication, which facilitates information management.

The centres in Tarragona and Bellaterra have a videowall system —a large television platform where multiple images and computer applications can be projected— which keeps them connected to a complex mechanism of cameras distributed throughout Catalonia. In this way, the petrochemical complex in Tarragona is under visual surveillance 24 hours a day. The cameras can be controlled from the Tarragona

emergency centre: they can be guided, the perspective can be changed, items can be zoomed in on, etc. What is more, the centres have access to several databases that may physically be in the centre or in other centres. These databases provide information about water flows, environment, weather, etc.

When the centres have to communicate with the mobile units that are operating throughout the region, they can monitor them via GPS and use a map reproduction system to inform the vehicles of the existence of water dams or irrigation systems, aquifers, access roads or natural obstacles, built-up areas or woods, etc. In this way, the system of mapping and monitoring units provides information in real time about their location, the characteristics of the terrain, the equipment on board the unit and even the speed of the vehicle. Mapping systems have facilitated quite considerably the remote management of mobile equipment and both centres have this capacity.

All these advanced technological mechanisms make it possible to control petrochemical risk to some considerable extent. The centres are connected to detection systems of the Department of the Environment that can perceive the presence of hazardous gases in the air or substances in water through detectors in towers or sea buoys. Thus, the indicators, the surveillance mechanisms and the instant transmission of information provide what could be called a sense of control over a scene where an emergency may be declared unexpectedly at any moment.

However, as we have said above, there is a clear technological step backwards when emergency centres have to communicate with the exterior. In the event of a petrochemical crisis, the Bellaterra and Tarragona emergency centres have to use fax, phone and e-mail to warn town councils, politicians, media and other institutions. Finally, the general population is warned directly by sirens, a technology that has the same function that was historically carried out by church bells.

The emergency centres can receive calls from the general population on the emergency phone number 112. In Catalonia, they receive an average of 15,999 calls every day on this number, 14,127 of which are dealt with by Bellaterra and 1,873 of which are dealt with by Tarragona (theoretically the number of calls made from the area, even though

Bellaterra can divert calls to Tarragona and vice versa in the event of saturation). A total of 64.08% of the calls are made from mobiles, and only 15.21% from fixed phones.

In our opinion, these data about the emergency telephone service 112 are not the most significant. What is really surprising is to see that, of all these calls, only 9.88% are "operational": the rest, 90.12%, have no message (26.19% are calls with no response, technical errors or wrong numbers, and 63.93% are pranks or callers who have no intention of requesting a service). Most of the valid calls are diverted to health assistance services or the police. Those that affect the petrochemical industry are not classified as such, but figure both as "technical accidents" and "fires" (for example in an industry). Only 2.66% of the calls are for "technical accidents" and 9.1% for fires, but it is clear that these figures include many events that have nothing to do with the petrochemical industry.[2]

The 112 service and emergency management are two different activities that come together at the Bellaterra and Tarragona centres (in this latter centre, the 112 service is part of the same command room and it is managed by the room coordinator). The 112 service provides the centres with a window on those emergencies that the control mechanisms cannot detect and with data from witnesses that supplement and define those emergencies that have been detected. Through the 112 service, citizens can become informers. The data tell us, firstly, that the calls are largely made from mobiles phones but, as we have said, what stands out most is the considerable noise made by the "false" calls, which leads us to reflect on civil responsibility.

Continuing with our separation between internal and external communication, we can ratify the technological limitations in external communication: the centres receive vast numbers of incoming calls and they generate phone and fax messages that inform institutions, the media, companies and organizations. Finally, large-scale warnings are given to the population via a system of sirens. The emergency number 112 is largely conceived as an input channel, not as a channel for communicating information, and the operators can only give callers the information that has been authorized. Tests have begun on other mechanisms for warning the population, such as large-scale calls to

[2] All the data have been provided by the 112 Emergency Centre of Catalonia. CENCAT. Department of the Interior. Government of Catalonia. Data obtained between 02/01/2006 and 08/01/2006.

population groups. The Tarragona centre carried out a test in the town of Flix. The system consisted of recording and sending a telephone message that urged the population to lock themselves in, close all windows and turn on the radio. The test was not very successful because a high percentage of calls were not answered. At present, other systems are being studied: for example, large-scale calls to mobile phones or large scale delivery of SMS, but these systems have yet to be fully developed. Therefore, like other European Union countries, the most widespread large-scale warning mechanism that is being tested is the activation of sirens. To evaluate this technology, which in fact carries out a basic function through an ancestral, though modernised, mechanism, we carried out an observational analysis.

4. The challenges of using ICTs

During the in-depth interviews we dealt with several aspects of how ICTs were used in risk communication management. In the first place, it should be pointed out that the emergency centres studied have the great advantage that they integrate several units in the same physical space. Thus, in both Tarragona and Bellaterra, the centres were designed for a variety of technologies, equipment and human resources: for example, firemen, environmental or health personnel, policemen or technicians from the Catalan Water Board. The aim was to make it possible for the teams to work in a coordinated fashion at any moment during the management of the emergency. For this reason, the emergency centres are designed to house technical staff who do not usually work there. These positions are operational, the computers are on, the applications are ready and theoretically everything is prepared in case the mechanisms have to be activated. The reality, however, is that the presence of operatives other than the firemen themselves is limited or non-existent in the centres' daily activity.

The **integration of technology** has the advantage that it concentrates in one area all the operatives involved in responding to an emergency situation. This makes it possible to centralize the information, which is assumed to make decision taking more efficient. The informants state that on the purely technological level the integration of ICT is positive, but that things will only run smoothly if the organization is good, and the main requirement in this respect is **overall coordination**. Experience in emergency

management also shows that centralizing the management of information and technology does not always give the best results. According to these opinions, which are based on the emergency situation generated by Neucat in January 2006, having a decentralized, small, highly operative presence in the field, is a more effective way of managing situations.

Centralizing ICTs also gives rise to two other situations that must be taken into account: in the first place, accumulating information management in a single area involves a risk of technical and human overload, which is particularly probable and problematic during emergencies; also, maintaining everything on standby but without actually operating, waiting to be used if needed, leads to a lack of routine.

The **lack of routine** is one of the most obvious dangers that the research team detected in the use of ICTs in emergency situations. These situations are characterized precisely by the fact that they are exceptional, which means that neither the human resources or the machines are used to carrying out particular functions or putting into practice particular processes with the efficiency that an emergency requires. For one of the informants, this is a major issue, and he mentioned some of the preventive measures that he could take:

> *"Because there is no routine, we find that the people from the Mossos d'Esquadra (Catalan police force) are not always the same and are not used to working in the place, they don't have half of the information and we have to give it to them at that moment. So, the room coordinator, who's in charge of the emergency, can't be around to see to them (…) What we do, though, is to check all the systems and make sure everything works twice a week."*

According to the teams, the best weapon for fighting the lack of routine is to make sure that the equipment is well maintained, but they suggest that there are shortcomings in the human aspect of the system: each group (police, health, environment, industry, etc.) should put into practice the routines for using the equipment by ensuring that the team members are physically present in the emergency room on a daily basis. In this way they can minimize incidents during real emergencies.

Information overload, however, is a problem that is more difficult to solve. The informants admitted that emergency situations generate so much information which needs to be processed that systems are often brought to a standstill. The emergency phone lines become saturated, which means that phoning 112 can create long queues. When this happens, the centres at Bellaterra and Tarragona divert calls from one to the other when one of them cannot cope, but there is no guarantee that the calls will be dealt with correctly. Mobile telephone lines can also become saturated if the emergency occurs in a particular place, so radio frequency devices are used for internal communication. On the other hand, sending information from the centres to companies and institutions tends to saturate the fax systems because the centres send large-scale emergency warnings to local councils, institutions, schools, media, etc. Thousands of warnings have to be sent in just a few minutes.

In the drill observed by the research team, both lack of routine and information overload where problems that raised at the emergency centre. By chance, the same day of the petrochemical alert siren system test, the centre had to activate the emergency plan for snow and freezing temperatures. According to CENCAT sources, there was some controversy over whether the drill should be cancelled, but the centre decided to go ahead, arguing that a real emergency can occur in all sorts of conditions. In any case, the centre was extremely busy responding to emergencies caused by the snow and ice and therefore the response of the population to the drill overwhelmed the 112 telephone operators. They just were able to answer 36 calls in the 45 minutes that followed the starting of the drill (which lasted 20 minutes). Even though there had been information meetings in the neighbourhoods where the sirens were to be activated, and the media had warned about the drill, most of the calls were of people that did not know that it was just a test and wanted to know that to do.

The Internet eases the information load because it enables a considerable number of warnings to be sent by e-mail, which is much faster than the fax. Even so, most institutions do not receive warnings by e-mail, not because they do not have the technology, but because they are not used to it and they still require the fax, the paper with the official stamp on it. The availability of the technology *per se* is not enough if the cultural and social context is not favourable, as we have indicated. Although many

institutions are now using e-mail, there are still many that require a faxed warning or both, which only increases the amount of information to be sent.

The considerable information load is mainly related to the **scale** of the emergency centres. A very ambitious scale can mean that peaks in ICT use can be well managed, but it also means high costs throughout the year. According to the informants, the smaller scale of Tarragona made integration more effective. This logic suggests that the smaller the scale, the better the technological integration. For one of the technicians, this is the main problem of all emergency centres: if expense is no object, the human team can be increased to cope with high ICT pressure, but budgetary limitations usually mean that scale must be balanced with costs, a criterion that often does not respond to real management needs. To some extent, the informants recognize that the criteria for the technological design of the centres depend on extra-technological factors: real management needs often do not coincide with the budget available and political imperatives. Economic and political criteria are not governed by the same logic as technological criteria. Finally, however, it is society that can suffer the most damage if economy, politics and technology cannot reach an understanding.

During the observed drill, there was a clear shortage of human resources due to the overlapping of a real emergency situation and the test. Actually, the fireman in charge of activating the sirens of the drill did not receive the order in the expected moment, because the general chief of operations was busy managing the rescue of a family trapped by the snow and himself was using the cell phone to contact his colleagues distributed on the ground to check if they were on their positions (they were supposed to check if the sirens produced the alarm sound properly). Thus, the order arrived through a 112 operator, who received a call of the head of the fire brigade and *viva vocce* ordered the siren technician to activate the test.

The Catalan emergency centres have taken considerable effort to **visualize risk** for decision making. The ICTs that help to materialize risk, visualize it and make it tangible are extremely useful according to the managers. In this line, three basic technologies should be highlighted: cameras, simulation applications and mapping systems. The petrochemical industries in Tarragona are constantly under visual surveillance by the nearest emergency centre and the one at Bellaterra. As a technical head points out,

cameras have been one of the most valuable tools for detecting problems, and on one occasion even detected a fire in a plant before the company itself did.

The emergency centres have access to about five hundred cameras spread throughout Catalonia and belonging to several owners: companies, motorway concession holders, Catalan Television, various government departments (Environment, Interior, etc.). According to one of the informants, an agreement has been reached whereby the camera owners inform the emergency centres if they detect an incident. The centre can immediately link up to the camera and use the videowall system to visualize what is happening. The cameras belonging to the Catalan Government and focusing on the Tarragona industrial estate can be controlled from the centre by means of a joystick system. The system of cameras has made it possible to detect accidents the moment they occur. In places where there are no surveillance cameras, visualization has been made possible by MMS technology (Multimedia Message System), which enables images to be sent by a mobile phone. These images can be enlarged and examined in real time, which makes it easier to decide what action has to be taken.

Simulation systems also help to prevent risk in all areas but can be particularly useful in the area of petrochemicals. The emergency centre in Bellaterra is helping to develop applications that make it possible to simulate forest fires, and also predict the evolution of toxic clouds and spillages at sea. The parameterization of the systems makes it possible to draw up a scenario of possibilities, speed up response time and improve decision making. The technicians all agree that they are not going to get everything right, but these simulations and predictions are extremely useful when faced with a fire or a spillage at sea.

According to the informants, the simulators can be parameterized relatively quickly. It is clear, though, that these tools are not fully reliable in representing reality and that situations can arise that change the predictions made. The **limited nature of the reproduction of reality** is a fact in both simulation technology and video cameras. Of course some gases cannot be seen and others are not easily detectable. The distribution of the cameras and their positioning are also factors that should be taken into account. And as far as simulation is concerned, we must accept that not everything can be predicted and some things are, even today, uncontrollable.

Another aspect that should be taken into account about the use of the ICT in emergency centres is the **management and interconnection of databases**. Information technology is based on the logic of the links and nodes in which the information resides. Clearly the maintenance and interconnection of these deposits of information is essential, but this is often a weakness of the organizations that manage risk. The emergency centres in Catalonia can access several databases, although they are not always interconnected and sometimes even incompatible. Therefore, according to the informants, one of the most important tasks of the centre is to integrate all the micro-databases into more powerful centralized systems; that is to say, there is a migration of small databases and information tables to more powerful systems.

The unification and maintenance of information, however, is a cumbersome task to which the centres still do not devote sufficient resources, as the actors themselves point out. It involves changing a local council's telephone number in several databases, and is often not done properly. At the time we were carrying out our research, there was a project to unify the databases and a demand, from the centres, for more administrative support so that information updating could be optimum.

New developments, **technical maintenance** and the response of the companies subcontracted for **ICT management** are other points that can be crucial for emergency centres. According to the informants, one of the most complex issues for centres such as Bellaterra or Tarragona is to find a technological company that can provide *ad hoc* solutions for risk management. Large companies tend to produce standard products that are quick to make a profit because of the economy of scale. These products, however, are not suited to such organizations as emergency centres. This means that the centres have to have a technical staff that can adapt the software and hardware, or carry out *ad hoc* maintenance. What is more, emergency centres are not like other companies where a ten-minute wait merely supposes an economic cost that can be calculated and assumed. Technical response must be immediate, and this involves extremely high maintenance costs or the presence of their own technician during emergency episodes. This latter option is the one favoured by the emergency centres.

This demonstrates something that may be common to any risk management centre that uses ICT: there are often lots of technical resources but few humans to manage them. And on top of this, some of the humans may not be sufficiently or optimally trained to use them. In this respect, **training and life-long learning** are considered to be a key, strategic element if technical resources, and therefore ICT, are to be properly used in any organization, but particularly in those that deal with the communication of risk. We no longer speak only of the technical knowledge of the human staff but also of their organizational training, their ability to understand what their function is, how their job is defined and how they should respond in any particular situation. According to the informants, it is essential that competencies be delimited, and jobs and responsibilities defined: they all accept that these aspects can be improved at present.

5. Using the Internet to communicate chemical risk

While this research was being made, the Department of the Interior was working on a new website for information about chemical risk.[3] According to CENCAT, this website aims to be understandable to anybody who requires further information about Plaseqta, the chemical products used in industry, what has to be in the event of risk, etc. One of the features of the website is that it has a sound file so that people can find out what a siren sounds like. The rest of the material consists of maps, pictograms, photographs and text.

ICTs can be extremely useful tools for informing about petrochemical risk if they are used properly by institutions and the people who require the information. The new website contains a space for a forum where the Department of the Interior hopes to receive queries, which will subsequently be used to draw up a FAQ page (Frequently Asked Questions). This space, however, does not initially provide direct access to a mailbox or forum but simply announces: "The questions that are sent to the Department of the Interior and other participatory mechanisms will be used to complete this section".

[3] <http://www.gencat.net/interior/emergencies/plaseqta>

The administration admits that the information available on the Internet may be insufficient, that it must be structured better and that it must also be presented so that it is more readable and didactic. According to our informants, few people consult this website and its visibility is low. The administration is aware that providing a website with the standard information is only one step in the difficult task of maintaining a proactive informative and educational policy that raises awareness of petrochemical risk and shows the population how to behave and what habits to adopt.

The new website is one more step that makes the information about Plaseqta more intuitive, usable and understandable. Although it is a good means for promoting a policy of transparency, it is not the only one. It should not be forgotten that ICTs can help to mitigate the consequences of accidents, but only if there is universal access and if they are supplemented with other elements that also raise awareness.

The information that has been published on the Internet about industrial risks seems to be more aimed at fulfilling a duty rather than being a training or didactic tool. It is important to see how the information about petrochemical risk is evaluated, how it is used, what the demand for it is and, finally, whether ICTs can be a more convenient or effective means for providing this information.

6. Conclusions

ICTs can be a great ally to organization if they are used rationally and planned carefully. They can help to prevent situations of petrochemical risk and improve emergency management. So they are a fundamental tool for risk communication and they may become a useful means for attenuating the hazards that the activities of the petrochemical industry give rise to. The analyses carried out lead us to the conclusion that the optimization of ICT management in the risk communication environment is a complex task that does not depend on individual elements but on a combination of elements. In the first place, it is not the technological, institutional, political or economic decisions that are exclusively responsible for the effective use of ICTs. Responsibilities should be sought on a wider scale, among all the actors involved. Companies, institutions, official organizations and citizens all have to accept their respective roles in this field. The availability of or access to ICTs per se does not

necessarily mean that they will be optimally used. What is more, inefficient organization, an inoperative political environment, a largely untrained social base and other economic, political and cultural factors can have a negative effect on how these technologies are used. The technological system, then, does not function independently of its environment and, what is more, can give rise to distortion and risk. Some of the risks and shortcomings of the ICT are the following:

ICT failure

Technology fails more often than is desirable at critical moments in emergency management. Technical failure puts the team that is managing communication under stress and gives rise to dysfunctions which prevent communication from taking place or the message from arriving correctly. Technical failures are related to the size of the centres, the operativity and capacity of the equipment, and the capacity of the human resources and the stress to which they are subjected.

ICT overload

Overload comes about at moments of technical and human stress, which is the defining feature of an emergency situation. In the case analyzed, we detected several instances of overload: the mechanism for receiving emergency calls cannot cope with crises because ICTs are designed for a particular volume of activity. Nevertheless, overload does not depend exclusively on this: it also depends on whether the population is trained to act in risk situations and on educational and cultural issues—which can be seen by the considerable number of irrelevant calls received.

Incompatibility with the protocol

The use of technology can cause unpredictable situations —because of overload, misuse or failures— which means that it is difficult to apply effective response protocols. This situation may also come about in reality. Likewise, it is by no means unreasonable to think that one emergency situation will lead to another: extreme temperatures can be the cause of technical problems, for example. In emergencies, characterized by human stress, the intensive use of ICTs can lead to situations in which the actions taken are incompatible with predesigned protocols.

Saturation of the human team

The use of ICT requires human effort. So the logic that machines involve less human presence should be reviewed. The feeling that the researchers had during the analysis was that the human team in the emergency rooms during daily activity is quite limited in comparison to the amount of technology there.

Inefficacy of technology per se

Although technology usually works properly, it may be unable to fulfill the organization's objective. For example, its ability to represent reality or to predict is limited. It also requires information and training before it can be used and this is not always provided in the best conditions. Not only is it necessary to train the emergency management team but also the general public, which means that both state and society in general have to make an effort.

Unpredictability of the use of technology

As we have seen, the use of sirens but also of any other type of technology can have unpredictable consequences because numerous variables are involved, the effects of which are difficult to calculate: for example, weather conditions. Therefore, a "margin of unpredictability" is to be expected, the unexpected must be foreseen. The context in which the ICT are used is changing and emergency situations are subject to stress and the lack of routine, which also provoke technical and human error.

Organization and use of ICT

Technology requires clear, well-structured organization, and sufficient resources to respond appropriately. It does not function in isolation from the rest of the organization. Thus, attempts must be made to combine economic, political, organizational and technological criteria if ICTs are to be used in an optimal fashion. We are aware that this is by no means an innovative conclusion, but it is clear that, although obvious, these attempts are not always made.

During our research, we observed that there are differences between how ICTs are used internally and externally to the emergency and risk communication centres. We have also shown how failures, overload and misuse of ICTs can arise at any time and change the direction of the emergency management. We have detected key aspects such as technological concentration and integration, the size of the centres, stress and the lack of

routine of the technical equipment and the human teams, the “visualization” of risk, the management and maintenance of databases and equipment, staff training and information to the general public. All these factors must be taken into account if the opportunities and the limitations of the ICT in the management of emergencies and risk communication are to be understood. As far as the case studied is concerned, the emergency centres in Catalonia that guard against petrochemical risk are technically very well equipped, but this technology can be put to even better use if efforts are made in the right direction. Greater organizational definition, integral management that does not impose unique criteria (economic, political or technical) but which is based on general objectives, additional technical and human support in several areas (ranging from administrative staff to technicians) and a more suitable social and cultural fit with informative, learning and didactic activities could further improve the processes of technology use and draw management closer to the required level of excellence. These are just some of the actions that, as we have said, are not the exclusive responsibility of the state administration but require a broad vision of the role that the social actors have in the current environment.

References

BECK, U.; GIDDENS, A. & LASH, S. (1994) *Reflexive Modernization: Politics, Tradition and Aesthetics in the Moderns social Order*. Cambridge: Polity Press.

BIJKER, W. & LAW, J. (1992) *Shaping Technology/Building Society*. Cambridge, MA: MIT Press.

BIJKER, W. *et al.* (eds.) (1987) *The Social Construction of Technological Systems*. Cambridge, EUA: MIT Press.

CIBORRA, C. (2004) 'Digital Technologies and the Duality of Risk'. Centre for Analysis of Risk and Regulation. London: London School of Economics.

DREW, CH. H. ET AL. (2004) 'Promoting Transparency of Long-Term Environmental Decisions: The Hanford Decision Mapping System Pilot Project'. *Risk Analysis*, 24 (5): 1641-1664).

LUNDGREN, R. & MCMACKIN, A. H. (2004) *Risk Communication. A Handbook for Communication Environmental Safety and Health Risk*. Columbus, OH: Battelle Press.

MACKENZIE, D. & WAJCMAN, J. (1999) 'Introductory essay: the social shaping of technology', pp. 3-27 in MACKENZIE, D. I WAJCMAN, J. (eds.) *The Social Shaping of Technology*. Maidenhead, PH: Open University Press.

SAMARAJIVA, R. (2005) 'Mobilizing information and communications technologies for effective disaster warning: lessons from the 2004 tsunami'. *New Media & Society*, 7 (6): 731-747.

TAYLOR, S.J. & BOGDAN, R. (1987) *Introducción a los métodos cualitativos de investigación.* Barcelona: Paidós.

WINSECK, D. (2002) 'Illusions of perfect information and fantasies of control in the information society'. *New Media & Society*, 4 (1): 93-122.

David Domingo and Enric Castelló
Communication Unit, Universitat Rovira i Virgili
Tarragona, Catalonia (Spain)
Contact e-mail: enric.castello@urv.cat