Human Factors: feeling safe

Alfredo M. RONCHI
JRC S2D2 – Politecnico di Milano, Milano, Italy
Tel: +39 393 0629373, Email: alfredo.ronchi@polimi.it

Abstract: *ICTs can considerably improve both safety and security. Off course if on one side technological solution can increase physically both safety and security on the other side, equally important, is the "human factor", this time partially due to the usual ergonomic aspects more significantly due to the humans' behaviour and the feeling of safety and security. This side of "mitigation measures" or "counter measures" is even more relevant than the technological side. Let's consider the case of eBiz, without the feeling of "security" it could be very difficult to convince citizens to buy and sell items on line or even to use credit cards. If we refer to the actual risks due to terroristic attacks again the ability to generate a feeling of safety and security in citizens is even more relevant than the real safety and security measures. Moreover, in case of disasters this positive feeling, in recent times often due to digital devices, is crucial to successfully manage the problem.*

Keywords: Human Factors, Safety, Security, Wellness, Feeling Safe/Secure

Foreword

Nowadays the demand for "safety & security" in all its forms has increased, especially quantitatively and qualitatively, making clear the need for new approaches to enable the entire sector to ensure better results. Safety and security are integral part of human rights; we must provide all the efforts in order to guarantee such rights (as stated in art 3, 22, 25 - The Universal Declaration of Human Rights). In addition, a number of SDGs are tightly connected or rely on safety and security. Some of the specific fields are: food & water security, human security, safety, critical infrastructure resilience, drugs security and more.

Looking from a different perspective considering the specific cyber domain: we outline the role of ICTs in risks assessment and management. ICTs are playing key roles in a number of "risky" scenarios from health and child-abuse to homeland security and law enforcement, crimes, trafficking (humans, drugs, weapons, artefacts, etc.) and even at safety working places and mobility [7]. The richness of applications and services provided by ICTs in the field of safety, security and disaster recovery and management is every day more than evident. Of course, technology it is not enough to solve problems, it is well known and demonstrated that a holistic, interdisciplinary approach and a culture of "safety & security" taking adequately into account human factors are the basis in order to obtain good results in this area.

Human Factors

This is a scientific discipline concerned with the understanding of the interactions among humans and other elements of a system, data and methods to design in order to optimize well-being and overall system performance. Human factors are many times hidden by technologies and the idea that cyber tools and artificial intelligence will be the unique actors and solve all the problems is widely diffused but in reality, if humans are part of the scenario, we may say "humans in the loop", human factors can play a relevant role. This may positively or negatively affect the outcomes. Many times, in case of dangerous circumstances we know that a timely intervention of humans avoided a catastrophe or on the contrary human factors were part or the main cause of an accident. Simply refer to aircraft crashes, an environment highly controlled by safety measures and computer systems, many times an accident final report includes human factors among the potential causes like: organisational failures, conditions of the operators (physical and mental state), physical and technological failures and finally human errors. Other times the intervention of humans forcing the system procedures may avoid a catastrophe.

The role of ICT

ICTs can considerably improve both safety and security. Of course, if on one side technological solution can improve on the "physical" side both safety and security, on the other side, equally important, is again the "human factor", partially due to the usual ergonomic aspects and more significantly due to the feeling of safety and security that is generated by the solutions.
This aspect of the "mitigation or counter measures" is even more relevant than the technological side; a video camera overlooking an almost empty car of the metro during a night run may elicit a feeling of safety as well as a satellite phone may generate a similar effect on the occasion of trekking in remote areas. To stress the role of cyber technologies in providing on the occasion of WSIS Forum 2015 H.E. Mr Yasuo Sakamoto, Vice-Minister for Policy Coordination, Ministry of Internal Affairs and Communications (Japan), yesterday said - on the occasion of natural disasters ICT is the lifeblood to ensure citizen's safety. Internet of Things [8], grids, network of sensors, remote sensing as well as Near Field Communication glued by networking are some of the building blocks of safety and security apps. Let's consider the case of e-Business; without the "feeling of security" it could be very difficult to convince citizens to buy and sell items on line.

This specific requirement was many times the key element in interaction design; time ago when the first public phones started to accept credit cards France Telecom released a public phone with a special slot to put in the credit card, in doing this the card was 100% inside the phone disappearing to the eyes of the card holder. This type of public phone didn't succeed because citizens were concerned to lose the card inside the phone in case of malfunction. In order to solve the "human" lack of trust in the machinery designers decided to modify the credit card slot leaving more than 50% of the card outside the phone thus providing the feeling of "trust". Moreover, when the first generation of automatic tellers started their activity it took some time to establish a trust relation with citizens

often concerned about the risk of losing the control of the specific transaction or losing their banknotes or credit cards inside the machine in case of a malfunction. In order to solve the "human" lack of trust in the machinery designers decided to reshape the design of both hardware and introduce much more interaction, thus providing the feeling of "trust".

The same happened more than thirty years ago with the early experiences of unmanned metro trains, the windscreen and windows of the conductor cabin were shielded with dark films to avoid that passengers waiting in the station could understand that there was no subway conductor.

If we pose the focus on elderly people, they are for sure citizen requiring a feeling of safety and security. Software interfaces represent for sure one of the key aspects in HCI for seniors but there is an additional component in the interaction design process that is equally relevant, hardware interface, the choice of the appropriate device. We have to consider which typology of devices we do consider much more appropriate for elderly people; according to the results of a survey, until now devices that do not "appear" as computers from the user perception standpoint used to be more welcome. In the early phase of the Internet revolution France Telecom, probably following the stream of the incredible success story of Minitel, chose to design ad hoc "telephones" having a big touch screen using an object-oriented interface. They were basically "computers" hidden enough, by an appealing "envelope", to be considered not as "computers". This approach was demonstrated to be appropriate in order to clear the user resistance to computers.

Human Factors: Feeling safe and secure

More in general, the lack of "feeling safe and secure" may influence a number of fields from transportation to real estate values, behaviours and wellness. If we refer to the actual risks due to terrorist attacks again the ability to induce a feeling of safety and security in citizens is even more relevant than the tangible effects of safety and security measures, so law enforcement agents patrolling streets and crowded places elicit in general positive feelings.

Human Factors: Security

The present document will limit the analysis of human factors to few fields starting from security and more specifically from cyber security as a key example of the relevance of this aspect. The extension of the security breaches due to human factors can be easily extended to other security scenarios. One of the typical domains of reference regarding human factors in cyber security is termed "social engineering".

The ability is to deeply understand human behaviour and offer a story that might be true is a typical ability of cheaters and other criminals; sometimes in order to establish a kind of complicity getting closer to legality borders. It is a "cyber" version of the old "risky" environment created by cheaters selling fake "Rolex" wristwatches on the road or illegal currency exchange; the level of stress caused by a risky environment and possible law enforcement intervention lowers the ability to identify frauds. Another security breach due to human factors is profited by hackers is termed "social engineering". Hackers may contact the system administrator and pose as a user who cannot get access to his or her system. This technique is portrayed in the 1995 film "Hackers", when protagonist Dade

"Zero Cool" Murphy calls a somewhat clueless employee in charge of security at a television network. Posing as an accountant working for the same company, Dade tricks the employee into giving him the phone number of a modem so he can gain access to the company's computer system.
Hackers who use this technique must have cool personalities, and be familiar with their target's security practices, in order to trick the system administrator into giving them information. In some cases, a help-desk employee with limited security experience will answer the phone and be relatively easy to trick. Another approach is for the hacker to pose as an angry supervisor, and when his/her authority is questioned, threaten to fire the help-desk worker. Social engineering is very effective, because users are the most vulnerable part of an organization. No security devices or programs can keep an organization safe if an employee reveals a password to an unauthorized person.

Social engineering can be broken down into four sub-groups:
Intimidation: As in the "angry supervisor" technique above, the hacker convinces the person who answers the phone that their job is in danger unless they help him. At this point, many people accept that the hacker is a supervisor and give him the information he seeks.
Helpfulness: The opposite of intimidation, helpfulness exploits many people's natural instinct to help others solve problems. Rather than acting angry, the hacker acts distressed and concerned. The help desk is the most vulnerable to this type of social engineering, as (a.) its general purpose is to help people; and (b.) it usually has the authority to change or reset passwords, which is exactly what the hacker wants.
Name-dropping: The hacker uses names of authorized users to convince the person who answers the phone that the hacker is a legitimate user himself or herself. Some of these names, such as those of webpage owners or company officers, can easily be obtained online. Hackers have also been known to obtain names by examining discarded documents (so-called "dumpster diving").
Technical: Using technology is also a way to get information. A hacker can send a fax or email to a legitimate user, seeking a response that contains vital information. The hacker may claim that he or she is involved in law enforcement and needs certain data for an investigation, or for record-keeping purposes.

Human Factors: Safety

Human factors of course impact even the safety sector as it happens when we deal with crowds of people in mass gathering event. A correct evaluation of human behaviour when we design locations populated by crowds is one of the key aspects both in case daily use and more important in case of emergency. The design of emergency paths and exits in big shopping malls or airports is of paramount importance in order to minimize risks and damages. How will crowd behave in case of fire during a show in a big theatre? Do they need a specific briefing as it happens on ships, public offices or even theme parks? Simulation of the behaviour of crowds was a typical application in the field of computer graphics in the 1990s, the outcomes of simulation algorithms were represented graphically to improve the readability of the results.
Interaction design may provide a significant contribution to avoid or mitigate dangerous behaviours due to human factors. A proper design and positioning of signals, an appropriate design of paths and key elements along the paths or a safe by design approach may significantly contribute to the goal, a basic example is due to the different mechanical shape of electronic or gas connectors. This is the

design approach of doors and handles facilitating the output flux of people in case of emergency, the inter-blocks of potentially dangerous machineries, the rich set of hard and soft solutions to minimize human errors while driving a car or controlling a chemical plant. Sometimes it may happen that such devices will elicit a feeling of safety even exceeding the real capability of the device, it was the case of the early use of ABS on cars or auto-pilot on motor boats. Anyway, positive feelings are of key importance especially in the field of safety and security.

Some concrete examples of digital devices improving safety are Cricket (Mexico), Virgo (Italy) and the well-known radio beacon enabling the geo-localisation of people in danger.

Grillo (Cricket) ; it was developed by Mexican students in 2014 [1]; thanks to a network of ad hoc sensors it provides a visual and acoustic alarm up to 90 seconds before an earthquake, enabling people to escape. Further exploring the field of human safety, we find Virgo (Italy 2015) [2], a safety device for the protection of operators working in a risky environment, such as fire fighters. The warning system for personnel safety is designed to alert the team when an "operator" is in danger; it is studied to be worn in three positions: shoulder, belt, chest; it incorporates accelerometers and other specific wearable sensors. Through the use of audible and visible alarms, in case of need, the "operator" can be easily and quickly found.

Lastly a typical device improving safety and in doing this enhancing the feeling of safety while enjoying boat cruises, flying on ultra-light aircrafts or simply skiing and an emergency happens we rely on an Emergency Locator Transmitter (also known as PLB, or EPIRB Beacon). An ELT is a device whose purpose is to instantly report, and in any part of the planet, the location of ships, planes and people in major emergencies. It consists principally of a beacon that interfaces with the satellite system COSPAS-SARSAT for search and rescue operations. The transmitter, once manually or automatically activated (by immersion or by shocks), emits signals on emergency frequencies that are picked up by the network of orbiting satellites and retransmitted to the ground at the rescue coordination centres.

At the WSIS Forum 2015 [6], held as usual in Geneva, Mr. Sunil Bahadur Malla, Secretary, Ministry of Information and Communications in Nepal, said that ICTs were crucial in recovering territory during and after the April 2015 earthquake. It was one of the first-time drones that provided a relevant contribution to in both identifying groups of citizens needing help and providing real-time evidence of the effects of the earthquake.

Position-aware devices running APPs, the Internet of Things, grids, networks of sensors, remote sensing as well as near-field communication glued by networking are some of the building blocks of safety and security in different fields. Of course, if we consider the prefix "cyber" as key actor in safety, security and disasters we must take care of one of the most critical infrastructures today: the telecommunication system. This means landlines but many more times wireless/satellite connections. In case of emergency both geo-localisation and communications are crucial. In addition, with specific reference to communications, interoperability of different communication systems is important, so a direct connection between tetra systems and mobile phone/landline or helicopter radio frequencies can make the difference in case of emergency. All these aspects suggest endorsing a holistic approach to the "Safety, Security, Disaster Recovery" sectors.

Human Factor: Ergonomics

It is a common understanding to group under the umbrella term "human factor" a number of different aspects that may deeply influence outcomes. Human factors may influence a sport match, an artistic performance, collegial decisions, critical errors in case of danger, behaviour of crowds and more. Decision makers, designers, coaches and leaders in general must carefully consider human factors, the aim may be to elicit a sense of unity and endorsement of a specific goal, to better the overall performances of teamwork, to train to act in the proper way in emergency and more.

As already recalled a typical field tightly connected with human factors is interaction design. What is interaction design? Some authors define it as "the design of interactive products that are able to support humans in their own working activities and in everyday life". Interaction design comprises a far wider "territory" than human computer interface (HCI); it may include physical devices design, their physical arrangement in the living environment.
As it happens in other domains such as Computer Graphics and Virtual Reality, cognitive psychology plays a relevant role even in interaction design. Certain basic principles of ergonomics provide the grounding for "interaction design", these include anthropometry, biomechanics, kinesiology, physiology and psychology as they relate to human behaviour in the built environment [4]. These include mental models, mapping, interface metaphors, and affordances. Many of these are laid out in Donald Norman's influential book "The Design of Everyday Things" [5]. This approach to interaction is usually termed "human factors and ergonomics". The present paper focus on human factors in the field of safety, security and disaster recovery even if interaction design plays a key role in such fields.

Human Factors: Wellness and positive feelings

"Wellbeing: A being that lives in close proximity to a well in the ancient of days, having a source of potable water. King Darius had sense of wellbeing because he had a well[1]*."*

Dealing with human factor issues it seems reasonable to introduce the concept of "well-being". Furthermore, nowadays we cannot avoid considering the relation between well-being and information communication technologies. The concept of well-being is attracting increasing attention in the context of development policies. However, the notion of well-being using digital media is still vague. It often tends to be confused with the concept of "interaction design" or "smart cities". Information and Communication Technologies (ICTs) as enablers of e-services have the capacity to allow processes of urban transformation, by helping cities become "smarter" and more "sustainable". To what degree do smart cities contribute to the well-being of citizens? By reviewing current trends in well-being policies, the paragraph questions the concept of quality of life as limited to improved infrastructure and public equipment. It refers to well-being also as intangible collective capital, such as the preservation and transmission of cultural heritage, collective memory, political participation, social equity, and inclusion for minorities and vulnerable social groups, which in the long run contribute to increasing the well-being of urban inhabitants. Finally, it proposes the use of ICTs to enable institutions to provide and offer innovative citizen services to enhance quality of life.

[1] Urban Dictionary, http://www.urbandictionary.com/define.php?term=wellbeing

The definitions of well-being are wide-ranging, and generally concomitant to concepts such as quality of life, health, wellness, and living environment: "quality of life is the factual material and immaterial equipment of life and its perception characterised by health, living environment and legal and equity, work, family, etc.". In most of the current bibliography, the concept of well-being is strongly linked to health, which in turn is defined as "A state of complete physical, mental and social well-being and not merely the absence of disease or infirmity".

Marcus Tullius Cicero (106 B.C., Arpino - 43 B.C., Formia) in the treaty "De finibus bonorum et malorum" [3] provides a range of definitions of well-being. The work is structured on the basis of the Aristotelian structure two orators, one sponsoring a thesis the other one refutes. In the first "book" Cicero let the orator Torquatus (Titus Manlius Torquatus – Consul in 165 B.C.) sponsor the Epicurean approach to good and evil. In the second "book" Cicero himself refutes this thesis. Epicurus use to consider the greatest good as the absence of pain, and the greatest evil as vice. In the third "book" Cicero let the orator Marcus Porcius Cato Uticensis (Cato the Younger 95 B.C., Rome – April 46 B.C., Utica) sponsors the Stoics' approach to good and evil. In the fourth "book" Cicero considers that this approach is not to be refuted but must be partially amended because it is too abstract and far from everyday reality. Stoics both do not consider pain as evil and assert that all the sins are equal. Stoics' ethics identify bliss in virtue, and this encompasses duties and sacrifice. Bliss is undoubtedness, the waiver of the passions, not believing in needs, contempt of adversity, suffering and disease. The fifth "book" doesn't face a sixth "book" that refutes the thesis; this means the Cicero approves and shares the Aristotelian approach. The "book" is located in the Academia of Athens and the thesis about greatest good and greatest evil is the one due to the philosopher Aristotle (Aristotélēs; 384–322 BC); well-being is achieved only when moral and spiritual wellness is associated with physical health, and success, even if not of primary relevance, is positively considered.

Conclusions

Experts in safety, security and disaster recovery must adequately consider human factors as a key aspect in influencing the behaviour of citizens in dangerous situations. Human factors may influence "decision makers", in a broad sense, in case of critical choices; within this domain the feeling of safety and/or security may impact a number of activities, services and even wellness. These positive feelings are many times elicited by a real context other times are more similar to a placebo effect but they are essential to ensure the enjoyment of some services or the idea of feeling well. Sometimes this feeling is due to technologies, sometimes to insurances, sometimes is provided "by design".

Bibliography

[1.] Grillo (Cricket) - Grillo's alerts will tell you when the earthquake will arrive and how strong it will feel where you are. http://grillo.io

[2.] Virgo - Safety device for the protection of operators working in risky environment, http://www.intellitronika.com/virgo/

[3.] Cicero Marcus Tullius, "De finibus bonorum et malorum", LOEB Classical Library - https://archive.org/details/definibusbonoru02cice goog

[4.] Nielsen Jakob (1995-2005) 10 Usability Heuristics for User Interface Design, ISSN 1548-5552, Nielsen Norman Group

[5.] Norman Donald A. (1988) The Design of Everyday Things, ISBN 978-0-465-06710-7, Basic Books
[6.] Ronchi Alfredo M., WSIS Forum 2015, High Policy Statements. https://www.itu.int/net4/wsis/forum/2015/Content/doc/outcomes/Policy_Statements_Booklet_WSIS2015.pdf
[7.] Ronchi Alfredo M., Duggal Pavan, et al., WSIS Forum 2016 Outcomes, https://www.itu.int/net4/wsis/forum/2016/Outcomes/
[8.] SAS report on The Internet of Things - http://www.sas.com/it_it/offers/ebook/iot-visualise-the-impact/index.html