From Safety to Security: Organizational challenges in Industrial Cyber Security (ICS)

A. Zanutto
Security Lancaster Institute
Lancaster University

ABSTRACT: Cyber security is a growing challenge for all organizations. In the past two decades, organizations have developed a huge amount of infrastructures based on important industrial control systems (ICS) for their businesses. A specific domain of these challenges comprises the industrial organizations that manage railway infrastructures, public utilities, nuclear plants, communication infrastructures and utilities.

The aim of the paper is developing a conceptual bridge between organizational research on safety and new research program on cyber security in industrial setting. Working on data provided by an ongoing project on cyber risk in ICS, the paper suggest a preliminary framework to face with relevant questions and reflections on how the organizational social construction of safety can be in some way a good proxy to understand the sociotechnical side of cyber risk in industrial sites.

1 INTRODUCTION

Cyber security is a growing challenge for all organizations. In the past two decades, companies have developed a huge amount of ICT infrastructures based on important information for their businesses, and many practices have been developed through these innovation processes. A specific domain of these innovation processes is represented by industries that manage railway infrastructures, public utilities, nuclear plants, communication infrastructures, and so on. These companies' businesses are not just managing private businesses, but they deal with public interests and strategic resources like power, water, transports and so on.

From the past, these businesses were intended as developed through local practices and knowledge and shared initially through the market at local or national level. Today, everything seems to be driven globally. On this new scenario, organizations must be aware that their industrial plants are even more connected through the internet based protocols. It means that potentially every industry is permanently under 'observation' from 'outside', and that their data and industrial processes must be guaranteed not only by technological physical artefacts and surveilled boundaries from potential "attackers". Their security depends also by the protections thoroughly the virtual world. Through Internet, industries have to devote their attention against information theft, dangerous tentative to destroy part or all of their infrastructure for many different, not ever competitive, reasons (Macaulay & Singer 2012).

Otherwise, many events, often malicious, impose new constraints on the organization if they want to survive. Security policies, protocols, detecting practices and incidents/alerts management, are just some organizational practices with which to manage knowledge about security in the organization and to counter external cyber-attacks.

Historically organizational studies and management studies has been able to explore in many direction the safety's issues and through them has been

able to suggest many relevant aspects on how organizations become dangerous for people inside and outside the organizations.
On the basis of an interdisciplinary cooperative analysis conducted on data emerging from the MUMBA project (Multi-Faceted Metrics for ICS Business Risk Analysis) active at the Institute for Security at the Lancaster University, we would present some preliminary findings of a special relationship between practices of security and practices of safety in industrial environment.

2 RELATED WORK

Risk is one of the main growing fields in industrial management. In the recent past IT literature has started providing many works related to how protect brands, data, IT infrastructures, local sites, local technologies for productive sites and so on. Many events and critical incidents are emerged to show how relevant and dangerous could be any attack provided to industrial plants or public utilities around the world. It is well represented by different international databases and by many works (Bayuk *et al.* 2012; Knapp & Langill 2011; Radvanovsky & Brodsky 2013). These works suggest that almost all economic sectors (Fig.1) are interested and, because is difficult to know exactly how many attacks are addressed to the companies, it clear that the industrial risk is a persistent and widely explored field present in the agenda of any country.

The industrial risk is strictly connected to the knowledge of what the company are producing and to the physical and technological environment present in a plant. Historically it was a myth that industrial processes were immune by attacks because the environment outside the plant were separated from technological instruments adopted to manage it. Furthermore, as point out by many reports, until fifteen years ago ICS were based on proprietary code and standards, ICS operated in a benign environment and protocols and protocol implementations were therefore simple and not hardened against attacks. In this scenario hackers were not interested in ICS. But what it is important for us is that the knowledge was relevant at local level, regarding specific workplaces and a small set of experts. Nobody else was interested.
This was a scenario developed also for managing knowledge on companies, about safety. Safety has been studied by scholar considering mainly management issues, but after it had become clear that it depends from organizational cultures and the way people do their job in the organizations (Taylor 2012). In other words, as pointed out by Taylor, safety needs to take in account that different levels in an organisation have different influences on the safety-culture. These levels need to be understand through their workplaces. Executive and senior management, middle managers, supervisors and workforce teams are differently involved in this process. All the employees are requested to comprehend what safety means in a specific organizational environment. The researches have to consider these workplaces to move forward until the top management strategies, including discursive practices in different community of practices (Gherardi & Nicolini 2000).

In these works, "safety" still represented as something constructed along relationship present in the workplaces. Understanding what happen at a local level in every specific practice acted along the day work in the workplaces when people are in permanent interaction with other actors and technologies too, open a new way to look at safety in a sociotechnical environment (Bruni & Gherardi 2007; Luff *et al.* 2000; Latour 2005). In this way safety is best managed and understood if we put in light local practices and every performance that people arrange around them (Suchman 1995; Luff e*t al.* 2000).

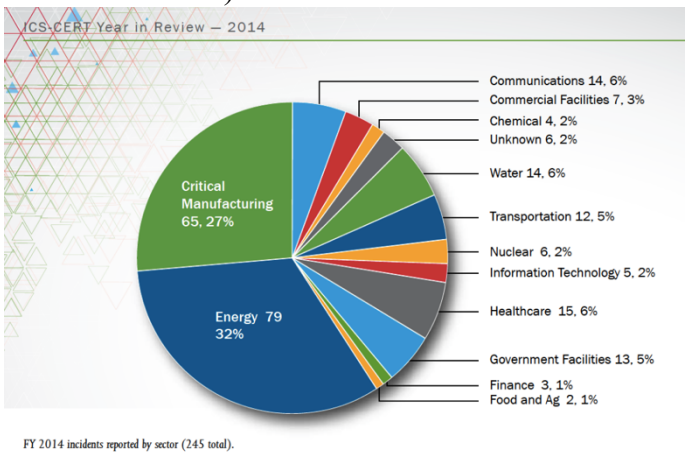

Fig.1 US ICS-CERT agency incident reporting 2014

Risk is a relational topic as well. As shown by Boholm & Corvellec (2011), risk is something culturally constructed and his relevance is built through by organizational practice. They point out the theme that a risky situation at least requires a "risk object" a "relation" and an "object of risk". "The relationship encapsulates the proprieties the observer considers prominent, rather than reflecting the properties of the objects as such. One could therefore say that relationships of risk are expressions of cultural preferences" (Boholm & Corvellec 2011: 180). Risk is a cultural

based issue and its relevance in an industrial site depends on the representation of its relevance, causal implications and strategic priority.
From these issues, we can assess some general assumptions that put safety and security in touch. Both are knowledge based organizational activities, driven locally and dependent on the sociotechnical environment and organizational culture available at workplace level. Many contributors studying safety have provided relevant theoretical assumptions. Among many we can refer to the work of Turner (1997), Rasmussen (1983), Reason (2000) and Leveson (2004). Combining their work and Schein's theory on organizational culture (2010) helps moving to more recent related work on what culture does in organizations.
Complex organizations like those that manage power grids, water systems, or nuclear plants have to consider this multiplicity. We can assume that there are many practices addressed to future risks following different orders and organizational strategic constraints. However, adopting the organizational studies approach, we can assume that risk and safety are both collective, situated and constructed by enacting practices around it (Gherardi 2009). Through these practices we have "to understand how unintentional and intentional actions can result in systemic faults and failures that could impact safe and reliable operation in today modern industrial processes" (Macaulay & Singer, 2012: 16). Again, these authors point out that through practices we often find opportunities for failure modes and processes on a day-to-day basis that go largely unnoticed. Giving attention to these event helps when something anomalous occurs. The analysis of the relation between risk and safety have to start from everyday practices and from the knowledge they represent. This work aims at exploring the challenges that this "new" field represents for organizational studies.

3 FIELDWORK

Analysis data is provided by a qualitative case studies research design intended to build a set of metrics. It is developed in collaboration with the cyber security management in the industrial sites of two big national UK companies. These companies are active in different domains and their activity is relevant to national infrastructures and to many public utilities. Furthermore these companies are important players for large public clients in many countries over the world and in many sectors. They offer tailored solution to tackle with cybercrime and cyber-attacks in the industrial sector. They also develop many other products as well. For example they develop specific technologies for communications and imaging analysis through CCTV protected environments. They have important competences in safety and in risk management, and are well known for this at the national and international levels.
During a period of eight months, meetings and dialogues at different level were organised with these companies, in different contexts. Progressively they have started to share their experiences with different customers and in different case studies. We have made ethnographic observations of these meetings and many interviews with managers involved in industrial security. In addition, we have carried a few interviews that were theoretically sampled, with an engineer in the water sector, a couple of hackers expert in ICS, and a couple of consultants on security in industry plants. Finally, two days at a national conference in ICS were included in the observation sessions. Settling some public rhetorical assumptions on risks in industry was an important first step.

Table 1. Organizational knowledge spread by different roles.

N	Role	ICS Sector	Organisation
10	Engineers in IT	Development of software for ICS: detecting, penetration test, mitigation, networks	Various companies
3	Engineer	Maintenance	Utility companies
3	Security manager	Security policy and team in organizations	Utility companies
3	Vendor	Appliances for ICS	Industry
2	Security expert (ex-hacker)	Hidden market malware, post-event analysis, fixing	CEOs of their own companies
1	Technical Engineer	Network reliability, penetration test in industry	CEO of own company
1	Engineer	PLCs testing	Power company
1	Scholar	Risk & safety analysis	University
1	Scholar	ICS analysis	University

Data analysis of transcribed interviews and fieldwork notes were carried following an ethnographic, reflexive, grounded-theory approach focused on connecting concepts, emerging issues, labelling and commenting. According to this, data analysis has been developed assuming the framework of the social construction of qualitative research. Its openness fosters the researcher's responsibility on theoretical work (Holstein & Gubrium 2013).

4 FINDING AND DISCUSSION

A core issue, when seeking data on industrial security, is dealing with the scarcity of open doors for researchers to collect data from companies. Many contacts had to be woven for a long time between researchers and management to obtain cooperation. In fact, security, instead of safety, is an open issue, something strictly related to the companies' brand.

When researchers visit companies to explore ICS risk issues, many frameworks emerge from the field. Some frameworks come up through the manager's vision, although they are not easily involved in this topic. When working on safety there are protocols, guidelines, internal manuals, norms and so on that are a clear starting point to evaluate what companies are doing. Comparing companies' prescriptions and norms is a well-defined task.

Risk analysis, unfortunately, brings little guaranteed result. Even after developing the best security conditions, as prescribed by norms, one can still be missing many (potential) holes that technologies and protocols cannot cover at all. For these reasons companies are not happy to open their doors to researchers at any level, in particular at production sites. This is also the probable reason why organizational studies are not exploring this specific issue much.

However, organizations have several social constructed frameworks useful to explore risk management. For this preliminary paper we concentrate our attention on three main levels: management, local security engineers and security consultants.

4.1 *Manager's knowledge and official representations*

Managers' frameworks on risk is probably the more interesting element when observing the social construction of risk. Managers know what the risks are for their companies and they are aware of many the implications of this topic. Several surveys show that managers know how critical an industrial sector is under threats. At the same time a strong commitment on what should be done to deal with risk is not always part of their agenda. For instance, many companies have just one person dedicated to this activity as a security manager (Piggin 2015). Often, this task is provided by IT managers that have a point of view not comparable to the one of industrial engineers. As pointed out in an interview with a consultant:

"Often the security governance in not an issue for the management. They are worried to consider too much their consultants or their managers because of the 'probability of risk' in their industrial sites. As usual you have got many alerts from a sites in the field but usually they are rarely due to cyber-attacks. So this event can be used against strong investments on security. Fortunately because of the brand economy view, many managements are changing their strategic position on this." [C2: Foods].

The managers of the companies we have met agree with this situation and confirm that internal report on security rarely have great diffusion at the board. One reason are the costs of the investments, and another reason is the internal organization. Adopting a new competence or a new risk manager stresses the stability of the organization. Also, in industrial control systems, risk is intended as a convergence between automation issues (PLCs, SCADAs, etc.) and IT architecture (protocols, access and identity, local resilience…).

Organizations have not much time to deal with these issues, and yet they still tend to miss concrete representations of the damages that cyber-attacks can cause their businesses. A possible explanation is the differentiation of points of views at different organizational roles.

Another concern regards international standards and certifications. Companies' governance must deal with these, especially when they deal with public customers or become a global player. However, not all standards are the same. Some of them address governance, others deal with technical structures. Nonetheless, standards are an institutional and international discourse on security that companies use to certify their security performances.

"Some standards are addressed at a very high level, and this is important because if you want to write a norm for all players the standard have to be "high". Of course, it keeps you far from specific details. Further, there are technical standards that are absolutely different from each other. They are really specific and usually they are addressed directly to the engineers not to the management. Managers are used to work on the compliance with the international standards as the 27001 that require specific responsible roles in the companies. But, locally, there are many 'tailored" solutions that can reduce the effective technical impact of the standards" [C2: Public utilities IT manager].

Despite the low evidence of attacks in medium sized industries, managements – mainly the ones driving public utilities – have to deal with security at a growing rate. The past has shown only a few well-known events in big industries. However, the perception that all companies should be dealing with security issues and should intervene on the organizational knowledge management of risk has become concrete.

4.2 *Local security engineers: exploring the workplace level.*

While working with people involved at different organizational levels, we observed that many workplace practices are not represented as "dangerous" unless organizations change their representations of industrial cyber risks. In addition, knowledge available in organizations about ICS cyber risk is not available through all roles and operators. In local sites, division of labour is relevant to understand that knowledge on safety and security is not managed in the same way. Security is mainly a novel IT-related issue. Instead, safety is an almost acquired public knowledge, fixed by many rules and managed by automation engineers and safety devices. Usually, about cyber security, it

is very difficult to share perception and discourses between different workplaces. Control centres on security are built remotely since they manage data coming out from many different sites and from many devices (e.g. SCADA). Safety issues are, instead, managed locally according to numerous documents and protocols already provided by standards and safety policies, procedures and devices.

"These people here, at the remote centre, only see a restricted view. They have very little power over the operational process going on. So, if an alarm comes in, there is not much that they can do about it other than ring somebody to sort it out. There might be some limited functionality: if a very basic alarm came in from a device, they might reset that device remotely but it wouldn't go beyond that. [Instead] the people here at the local level have a very very detailed view of what is going on at the operational site. They know it at an engineering level [...]. [At the remote centre], if a high level of this alarm comes in, they only know that it is important, either [from experience] or because it is a number "5" on a criticality scale. Other than that, they do not have an engineering view of what is going on." [T1: Power engineer]

As reported by other works, a better convergence between safety and security still constitutes an opportunity for many companies. Many issues emerge from the separation of these two points of view that in big companies become two concrete and thoroughly different structures. Lack in communication between the two could offer more useful informed practices on security (Piggin 2013). Research data shows that sociotechnical environment dedicated to safety and specific practices learned around it are different and remain separated from security practices (Gherardi 2009). What is clear from our data is that people should be informed and trained continuously about how these two hierarchically separated worlds have in fact many links that oblige them to work in parallel. A typical situation is when automation devices are stressed by maintenance crew for safety reasons. Engineers think about this situation locally. They know the physical constraints in depth, they have experience with the most common critical events, how to safely restore the system and put it again in production. However, in their minds, as we will show later, there is a clear hierarchy in their professional cultural assumptions: saving money and maintaining the production effective stand above all goals.

Managers are evaluated mainly on the production of their sites. Managers' bonuses depend on production performance: they are rarely connected to safety or worse, security. At local level, engineers are not interested in communicating too much to their hierarchy about critical alerts registered on the field. Production has to be maintained: if alarms come in and they are able to "solve the problem", for example resetting a PLC, not much care is paid to other things as long as the system works. Concerns arise only after an event happens so often that it could be related to a cyber-attack. Production comes before anything else. Again, if an alarm comes in and it is known to be actually dangerous, safety procedures are applied as prescribed by protocols and all the personnel have to follow them.

"If a severe alarms comes in, there are specific procedures even for people like cleaners, receptionists and those people in roles completely separate. If the alarm was that severe on that site, there would be an alert, some kind of notifications for everybody on that site. Then all have to follow the procedure… Just like a fire alarm, if you think about a fire alarm you have to stand up in front of the building or things like that. […] It would be assumed in the first instance there is either a problem with the instrumentation itself that is monitoring that signal, or with the device responsible for generating the alarm, the RTU, the siren itself, the configuration of the SCADA workstations, the PLC, etc. It would be blamed on everything but an external threat actor. I think if it was something severe and you went and reboot something and the alarm went away and it fixes the problem, it depends from management to management, different types of facilities, but some managers would be very keen on exploring that further" [T2: Power engineer].

According to the experience of this engineer, knowledge about alarm situations is continuously lost. On the one hand, very few specific traces of these events are collected, and on the other hand, if an important alarm happens the official protocols must be followed. Although many maintenance activities are recorded in great details, their readability as security issues is quite limited. Engineers' tales are about getting things working safely, rarely securely. In fact, alarms at local sites are managed mostly as technical failures. It is only after multiple occurrences and multiple device replacements that an alarm could be interpreted as a security issue.

It must be also considered that people at lower levels are probably at the lower paid income of the company and their culture is neither strategic nor oriented to understand their workplace as a part of a big design. This consideration highlights the importance of organisational granularity at the local level.

Managers tends to reduce the impact of security policies because of their cost. Also, security managers tend to emphasize alert analysis because those critical and well documented are few.

4.3 *Security consultants*

Going through field data, a way to approach security practices and discursive practices as well is to understand the different orders that companies manage along their activities. In this perspective, security is an "imagined" order opposed to a disorder created by attackers. Both security teams and hackers could be represented in potential opposite scenarios happening in an organization. In fact, a starting point of hackers

is to cohabit with workers in the workplaces in a hidden fashion. Many attacks start with a research by the attackers team on people's habits, on their passions, their feelings, their competency, family, networks, relationships and so on. Attackers overlap with operators: they are not interested in taking an exclusive control of a system.

"Hackers are interested in controlling machines in a shared way. Their only focus is to hide any action on the machine when they act at a local level. They program their actions in a way that they can be taken when nobody is controlling the target. Consider that these control machines are always on and active because they are so complex that it is impossible to switch them off without any dangerous effect. If they turn them off, they pray, because nobody really knows what could happen when they will be restarted [H1: Security CEO].

Working on field sites requires learning the local operator knowledge, both at the physical and practical level, and this learning process is usually hidden and covered by normal operator practices. The machines have a great stability, they must always be active and any strange behaviour is a threat to the hackers' strategy.

"They have many procedures to stop and analyse any anomaly that are quite strong. If they launch these procedures they will be able to detect you. If they detect you, usually they would be well prepared and able to block you quickly. In these moments it is important to stop every action to avoid any alert. To avoid these risks, you schedule these activities when you are sure that nobody can see you directly. Moments that are less crowded. When the attacks take place it is after many many days and months. It is also typical of classical attacks devoted to data extortion. When an attack is aiming at extracting data from an industrial site, they stay on it for a long time. In a case I had worked on, we discovered that the attacker were able to extract data for almost one year and an half" [H1: Security CEO].

Learning from the field is also a goal for hacker teams. They need to understand which activities are connected with a specific machine, when operators come in and work on it, in which way and so on. Such activities happen every busy day, with a lot of production staff to manage, maintenance, upgrade of systems, tuning to get the machines active for the production.

"Many times, I had the feeling that in a design phase, when a designer starts to think about a possible attack or possible intrusions, for instance a worm, and investigate possible scenarios, often people say "Yes, well, it could be, but it is too much paranoid of an approach", or, sometimes people around say "It works, why are you guessing again on it, it works!" It comes more often from an automation engineer. In my experience, there aren't specific experts of cyber security working exclusively on industrial systems. They are represented just as systems designed by someone to produce something. And then come the operator and the IT manager. That's all." [C1: Security manager].

Considering the knowledge that must be managed in the workplace to fix such complex machines in a production line, the problem is that sufficient useful knowledge is not always available. Many machines are legacy, other might be very complex, others have been recently substituted and so on. So, if an IT/security manager comes to suggest a penetration test, that would not be welcome.

"Note that in many industrial systems offensive experiments are forbidden. And many offensive security practices, such as simple port scanning, in an industrial context, could be potentially dangerous. A PLC could go down under a simple procedure like a port scan. The reason could be, on one hand, because the system is a legacy system, and on the other hand, because the machine's interactions are not completely understood. Sometimes operators do not know their system at all. […] So, you are often embarrassed. You don't know how the industrial system works exactly, how it could react under your tests, you are not allowed to make penetrations test, nor to apply specific procedures that were not documented in the site… What can you do? Often an error in these tests could cause trouble to the production, or worst it could hurt people as well. It is too dangerous, so you can't do any test" [C2: Security manager].

Knowledge in industrial systems is something distributed in workplaces and following different practical competencies. The fieldwork shows that many knowledge holes persist that people cannot explore deeply, but that hackers are searching into. Hence, when a hacker finds a vulnerability they have a bit of knowledge that probably nobody has in the industrial site. Again, their knowledge starts putting together security issues (how can I use a hole in the system?) and safety issues (how can I damage the system through this hole?).

In the fieldwork we point out the theme of knowledge repeatedly. From an organizational point of view, attacks to industrial systems are a knowledge and relational fight. From the inside, it is quite clear that knowledge is something connected with places and time, answering the internal organizational question: "where and when something should happen"? Many studies have pointed out that the analysis unit should be the local practices. This organizational 'brick' can be defined through the practical knowledge available in organizations, historically represented within closed boundaries (Suchman 1995). What is important to recall here is the sociotechnical dimension of reality: design is a matter of socio-materiality strictly depending on knowledge and its distribution around organizations (Bjorg and Carsten 2014). A practice is a hybrid, a basic unit, that shows us that when we act it happens not "under the full control of consciousness; action should rather be felt as a node, a knot, and a conglomerate of many surprising sets of agencies that have to be slowly disentangled" (Latour 2005: 44). Following this path we can assume that one of the most important practices undertaken by organizational actors is narrating accounts of everyday work life. These tales show the core of the job connected to that practice; the process of the practice as social action, and eventually practices allow people to enhance the social construction of the reality. These accounts on workplace practices reveal what "doing

do" in organizational life (Bruni Gherardi 2007; Czarniawska).

One can argue that organizations are the field where discursive practices may give an account of what people experiment in the workplace, and a strategic way to produce new insights on it.

5 CONCLUSION

A simple model could be adopt to represent an organizational scenario to give a linear view of different layers where risk management matters. But, considering tales and workplaces, we need to represent how knowledge is distributed in the relational texture of organizations starting from the division of labour at workplace (Gherardi 2006; Carugati & Rossignoli 2011).

As suggested by Hilgartner "risk is not something that gets attached to technology after the engineers go home, when the press and public arrive. Risks are constructed constantly as technological networks evolve. Social scientists must abandon their post hoc approach to risk, and move analysis upstream to the arenas where specialized professionals are working most intensively to extend sociotechnical networks" (1992: 52).

Again, this requires understanding that knowing is a situated activity and that knowing-in-practice is always a practical accomplishment. In organizations knowing is something that people do together in a workplace context. It is done in every mundane activity, when people work "together". "It describes a web of relationships among people, material artefacts and activities and regard the question on how to connect them successfully with the field" (Gherardi, 2009: 118).

In the field, the professionals that we have identified as the main net of the knowledge-in-practice texture, working on the accounts about the local knowledge are: managers, engineers, IT security managers, hackers and vendors. These roles represent different knowledge domains relevant to understanding, at the workplace level, what is relevant in term of risk for them (Green et al. 2014).

On one hand, knowledge domains represented by managers, safety engineers, vendors are represented as fixed, durable, rational. Instead, on the other hand, the knowledge of hackers and security personnel are represented as vague and strategy dependent. In fact, these domains feature a lack of norms, protocols and shared knowledge on how security matter on company sites. This recalls the organizational concepts on boundaries developed by Lucy Suchman through which she showed that boundaries are a social matter (1995). Every working group survives on a relation between owned social location and view of others social groups. These relationships sustain boundaries among organizational actors, "including boundaries between professional designers of technology and technology users. The distance of professional designers from the sites and activities that are the subjects/objects of their work has given rise to a range of techniques aimed at representing relevant others in ways responsive to design concerns" 1995: 59).

Following this path, accounts are oriented to construct and maintain such boundaries and preserve organizations from ungovernable confusion. At the same time, these accounts push organizations to apply standards and bureaucratic norms that institutionalize boundaries and practices useful to build an order in the organization. But, again, standard and norms are a waiver of any possible constructive communication.

The main visible cleavage about risk accounts is between production and safety managements. Safety management is oriented towards protocols and procedures and towards the quality of life in the workplaces. On the other hand, production wants things to work. Looking to our field, we can add that a new domain is driven by knowledge of security managers. They, more or less remotely, have to provide instructions and knowledge about risk in production sites. The matter here is that they are quite "new" in the industrial environment and they haven't the legitimacy to act in a production site that belongs to another domain since the boundaries of their domain are still under construction (Lave & Wenger 1991; Wenger-Trayner *et al.* 2014).

The security teams have many warnings to forward to business management that require money to fix up, and often they have to manage a knowledge that could potentially hurt production. The problem here is that they are not allowed to assess their knowledge domain because of the need to analyse the production and safety domain. But managers from production and from safety are scared by everything that could block the productions or damage any machineries. As collected accounts show, production requires specific and local settings that any experiment in security could disrupt. Just a port scanning in a PLC could be a dangerous activity, especially if the PLC is in a delicate production segment.

In this way we have to consider the security managers as a third pole of knowledge that must be investigated.

The more visible answer of security managers is to pass through bureaucratic practices. They suggest to monitor specific aspects such as access procedures, firmware updates, external devices protocols and so on, by tracing every step provided by users. But,

again, in a productive process this is not enough. Practices there are more complex and still need day-by-day learning and adjustments.

Eventually in some accounts it emerges that organizations are growing in visibility and their brands could be increasingly affected by security issues. People inside and outside the organizations are starting to deal day-by-day security issues in a global perception. When something has happened in a foreign country, it is broadcast in the media as a risk that could touch everyone directly. This is, again, socially constructed, and help to open the mind of business managers and employees about sometimes that can affect their industrial life.

6 REFERENCES

Bayuk, J. L., Healey, J., Rohmeyer, P., Sachs, M. H., Schmidt, J., & Weiss, J. 2012. *Cyber Security Policy Guidebook*. John Wiley & Sons.

Bjorn, P., & Osterlund, C. 2014. *Sociomaterial-Design: Bounding Technologies in Practice*. Springer.

Boholm, \AAsa, & Corvellec, H. 2011. A relational theory of risk. *Journal of Risk Research*, *14*(2), 175–190.

Bruni, A., & Gherardi, S. 2007. *Studiare le pratiche lavorative*. Il Mulino.

Carugati, A., & Rossignoli, C. 2011. *Emerging Themes in Information Systems and Organization Studies*. Springer Science & Business Media.

Gherardi, S., & Nicolini, D. 2000. The organizational learning of safety in communities of practice. *Journal of management Inquiry*, *9*(1), 7–18.

Gherardi, S. (2009). Introduction: The critical power of thepractice lens'. *Management learning*, *40*(2), 115–128.

Green, B., Prince, D., Roedig, U., Busby, J., & Hutchison, D. 2014. Socio-Technical security analysis of industrial control systems (ICS). In *Proceedings of the 2nd International Symposium on ICS & SCADA Cyber Security Research 2014*: 10–14.

Holstein, J. A., & Gubrium, J. F. 2013. *Handbook of Constructionist Research*. Guilford Publications.

Knapp, E. D., & Langill, J. T. 2011. *Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems* (1 edition.). Waltham, MA: Syngress.

Latour, B. 2005. *Reassembling the Social: An Introduction to Actor-Network-Theory*. OUP Oxford.

Lave, J. & Wenger, E. 1991. Situated Learning: Legitimate Peripheral Participation. Cambridge University Press.

Leveson, N. 2004. A New Accident Model for Engineering Safer Systems. *Safety Science*, 42, no. 4: 237–270.

Luff, P., Hindmarsh, J. & Heath, C. 2000. Workplace Studies: Recovering Work Practice and Informing System Design. Cambridge University Press.

Macaulay, T., & Singer, B. L. 2012. *Cybersecurity for Industrial Control Systems: SCADA, DCS, PLC, HMI, and SIS*. CRC Press.

Piggin, R. 2015. Are Industrial Control Systems Ready for the Cloud? *International Journal of Critical Infrastructure Protection* 9: 38–40.

Piggin, R. 2013. Process Safety and Cyber Security Convergence: Lessons Identified, But Not Learnt? In IET (Transport Sector) (Ed.), *Resilience, Security & Risk in Transport*: 14–20. Institution of Engineering and Technology. Retrieved from http://digital-library.theiet.org/content/books/10.1049/perrsr3e_ch3

Radvanovsky, R., & Brodsky, J. (eds) 2013. *Handbook of SCADA/Control Systems Security*. Boca Raton: CRC Press.

Rasmussen, J. 1983. Skills, Rules, and Knowledge; Signals, Signs, and Symbols, and Other Distinctions in Human Performance Models. IEEE *Transactions on Systems, Man, and Cybernetics SMC-13*, no. 3: 257–266.

Reason, J. 2000. Human error: models and management. *BMJ : British Medical Journal*, *320*(7237): 768–770.

Taylor, J. B. 2012. *Safety Culture: Assessing and Changing the Behaviour of Organisations*. Gower Publishing.

Turner, B. A, & Pidgeon, N.F. 1997. Man-made disasters. 2nd ed. Boston: Butterworth-Heinemann.

Schein, E. H. 2010. *Organizational Culture and Leadership* (4th Edition edition.). San Francisco, Calif: John Wiley & Sons.

Suchman, L. 1995. Making Work Visible. *Commun. ACM*, *38*(9), 56–64.

Wenger-Trayner, E., Fenton-O'Creevy, M., Hutchinson, S., Kubiak, C., & Wenger-Trayner, B. 2014. *Learning in Landscapes of Practice: Boundaries, Identity, and Knowledgeability in Practice-based Learning*. Routledge.