Master’s degree in engineering management

Politecnico di Torino

Master's degree Thesis

The Impact of social media on safety culture

February 2026

Relatore:

Prof. Micaela DEMICHELA

Candidato:

Matteo CABUT

s342075

Abstract

The problematic of my thesis work is: “impact of social media on safety culture”. This research is situated within a dual context. On the one hand, social networks are increasingly popular, with intensive use across all age groups. They vary in their features and objectives. The evolution of social networks has profoundly influenced how they are defined, both functionally and in terms of their aims. Some platforms are well-known, such as Facebook, LinkedIn, and X, while others are less obvious or older. On the other hand, safety culture is a major concern for companies. Indeed, following industrial accidents, standards to protect people and the environment have emerged and grown increasingly stringent. Beyond compliance, organizations are increasingly focused on building a strong safety culture. Therefore, examining the impact of social networks on safety culture is highly relevant, an aspect not yet addressed in the literature.

Given the exploratory nature of my research, I adopted a qualitative methodology. Thematic analysis was used, which allow an in-depth examination of interviews conducted previously. These interviews were carried out with various voluntary participants from different industrial sectors.

My research identified six key themes regarding the impact of social networks on safety culture: benefits, risks, prerequisites for implementation, practical applications and limits of social media use. I was also able to highlight connections and tensions between these themes that allow me to qualify the benefits regarding the risks, limits…. Consequently, this study provides a comprehensive overview of how social networks influence safety culture. Based on these findings, I formulated recommendations for future research, suggesting more targeted, quantitative approaches to further investigate and refine the preliminary insights generated by this work.

Keywords: social media, safety culture, thematic analysis, qualitative research, organizational communication, risk management.

Glossary

SM: Social Media

SN: Social Network

OHS: Occupational and health safety

CSSN: Computer-Supported Social Network

KPI: Key Performance Indicator

DSA: Digital Service Act

DMA: Digital Markets Act

HSE: Health, Security and Environment

VLOPS: Very Large Online Platforms

BBS: Bulletin Board System

IRC: Internet Relay Chat

IAEA: International Atomic Energy Agency

ILO: International Labour Organization

ICAO: International Civil Aviation Organization

WHO: World Health Organization

ARPANET: Advanced Research Projects Agency Network

HSE: Health, Security & Environment

CEO: Chief Executive Officer

RSPQ: Road Safety Perception Questionnaire

ExCom: Executive Committee

CSR: Corporate Social Responsibility

EDM: Electronic Document Management

Contents

Ringraziamenti

Desidero esprimere la mia sincera gratitudine al Politecnico di Torino per l'opportunità di conseguire un doppio titolo di laurea magistrale con l'INSA de Lyon. Gli anni trascorsi a Torino sono stati eccezionalmente ricchi, sia dal punto di vista accademico che umano. Ringrazio tutto il personale amministrativo del Polito, i professori che ho avuto il privilegio di incontrare e tutti i miei colleghi studenti, in particolare coloro con i quali ho collaborato nei lavori di gruppo.

Sono molto orgoglioso di presentare questa tesi di laurea magistrale, che conclude il mio percorso accademico. Per questo lavoro, desidero ringraziare tutte le persone che hanno contribuito attraverso le interviste.

Tengo a ringraziare profondamente Hasnae BAKHOUCH per il suo prezioso aiuto durante tutto il mio percorso academico, ma anche per il suo aiuto nella formattazione di questa tesi.

Tengo a ringraziare i miei genitori, Paola e Christophe e mia sorella Giulia per il sostegno durante questi anni di studio.

Ringrazio in particolare la Professoressa Micaela DEMICHELA, relatrice della mia tesi, per la sua preziosa guida e il sostegno fornito durante l'intero svolgimento della ricerca.

Matteo

List of figures

List of tables

I / Introduction

General context of the research

This master's thesis work is part of my academic path at Politecnico di Torino as a student. Its aim is to acquire skills in the development of a research approach, while being a source of proposals.

This work falls within the disciplinary field of social and technological sciences. On the one hand, social sciences, particularly sociology, for the study of the behaviour of social network users, and communication sciences. On the other hand, also technological sciences, since in order to understand how social networks work, it is necessary to grasp algorithms and other technical issues of this nature.

Social networks have deeply penetrated society, becoming a widely used technology around the world. The social network Instagram has experienced very strong growth over the last three years, going from more than 2 billion monthly users in 2022 to more than 3 billion in 2025 (Meta CEO Zuckerberg says Instagram has grown to 3 billion monthly active users 2025) which shows an increase in usage. This phenomenon is not specific to Facebook, but rather a real trend. In 2024, more than 5 billion people use social networks, representing a large part of the world's population (Meltwater 2024). Moreover, this trend shows no signs of slowing down, as social networks gain an average of 8.4 new users every second.

Many features attract users and make social networks tools that are used daily. Indeed, the rapid dissemination of information and the ability to connect in real time to news and updates are aspects that appeal to users Beyond the increasing number of users, engagement is also intensive. In fact, the average time spent on social media in 2025 is 2 hours and 23 minutes per day (2025 Social Media Facts & Stats: Usage, Platforms, and Growth s. d.).

The multiplication of connected digital devices could only accelerate this phenomenon, making these platforms accessible to a wide audience. About 98% of users access the platforms via mobile devices (2025 Social Media Facts & Stats: Usage, Platforms, and Growth s. d.).

The objective of this research work is to analyse the impacts of social networks on security culture within organizations. To this end, an analysis of perceptions, behavioural influences, and practices regarding risk perception and security culture will be conducted. Thus, knowing the population that uses social media is a relevant factor. The following figures address this need:

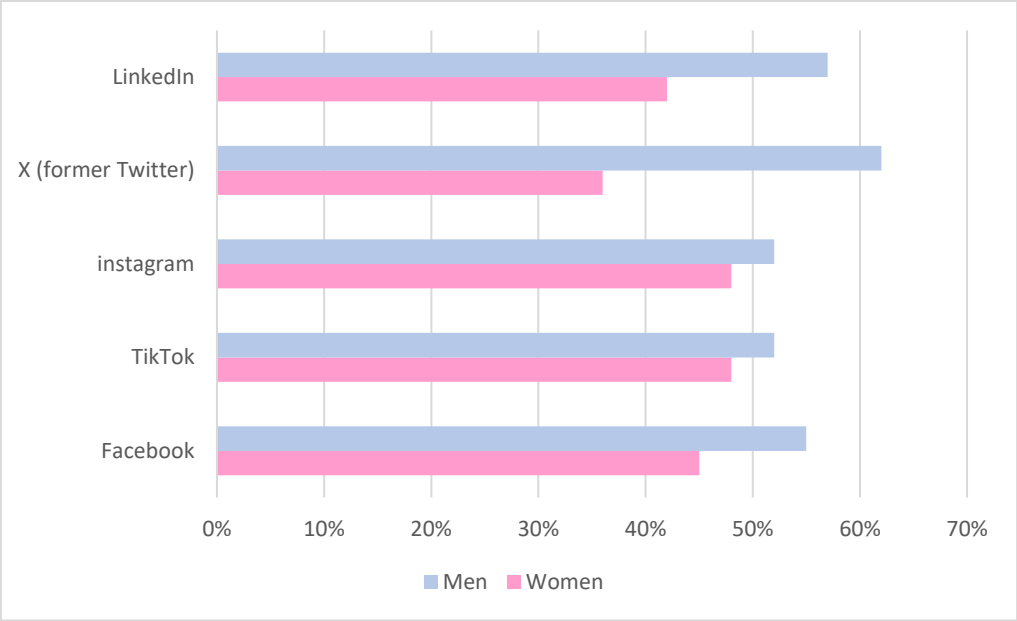

Figure 1: Gender distribution (source: 2025 Social Media Facts & Stats: Usage, Platforms, and Growth s. d.))

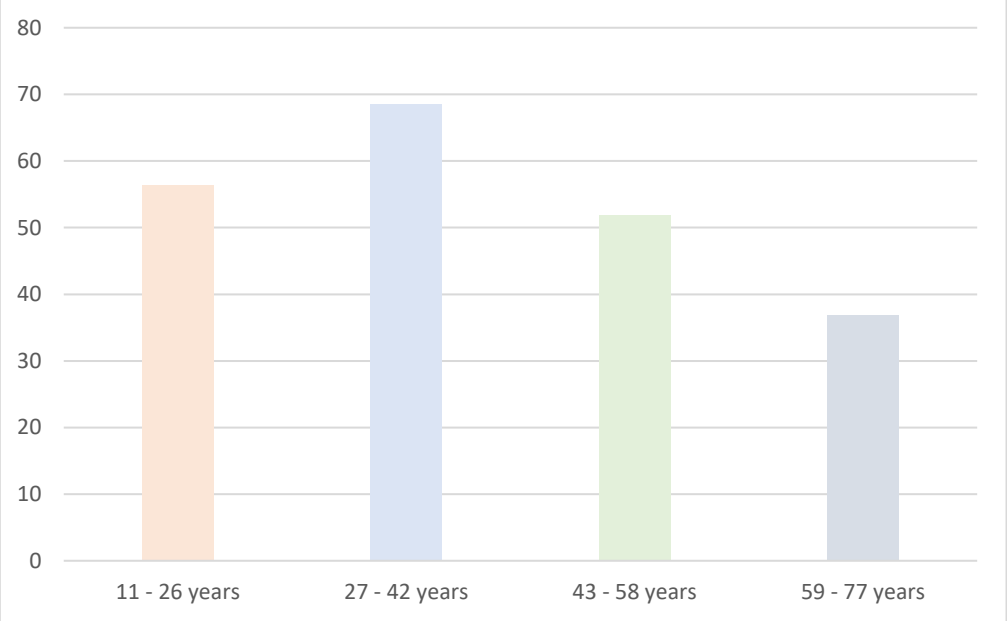

Figure 2: Demographics of social media users in the US (source: 2025 Social Media Facts & Stats: Usage, Platforms, and Growth s. d.)

The culture of safety is an increasingly strong concern for organizations, which are subject to more and more regulations to ensure quality at work. This quality of workplace safety is a real issue, as shown by the some 2.83 million non-fatal accidents and the 3,298 work-related deaths in European companies (Accidents at work claimed 3 298 lives in the EU in 2023 2025). This context shows the importance of safety policies, and the implementation of new methods to improve the culture of safety. Companies and organisations were initially very reluctant to implement safety policies. Indeed, these policies were seen as major investments, even though it has now been demonstrated that these investments are ultimately positive for a company's economy. The implementation of these policies helps prevent work stoppages for employees. In this way, a company can expect to earn up to 4 dollars for every dollar invested in safety policies (Naji et al. 2022).

Problematic

This explosion in the use of social networks consequently raises the question of their potential dangers or positive impacts, and in particular the impacts on safety culture. Indeed, due to the democratization of social networks, they have provided the possibility to post a large amount of content on a wide range of topics. Some subjects can thus be poorly treated, both in terms of content and form. In terms of content, social networks allow an almost total freedom of speech without safeguards or contradiction (modulo platform moderation), which can serve as a powerful tool of influence. In terms of form, social networks promote fast and very concise content, which often favours positions that are caricatural, unnuanced, and lacking depth. In this sense, social networks, with their vast amount of data and users, provide an additional space to both measure and promote safety culture. On one hand, these platforms make information highly accessible to a large audience in real time. On the other hand, they can also be used to spread, intentionally or unintentionally, bad practices, rumours, or normalize behaviours that weaken safety culture.

In this sense, in July 2025, the European Commission published guidelines on the protection of minors within the framework of the Digital Services Act (DSA). The broader objective is to regulate social networks in order to ensure the protection of citizens and users. In France, for example, a parliamentary commission of inquiry into the psychological effects of TikTok on minors has been established, proof that the issue of regulating social networks is an increasingly serious matter for the authorities. These concerns highlight the need to understand the security culture surrounding social networks, particularly users' perception of security.

Research's targets

The topics of social networks and security culture have been widely studied in the literature, as it is covered by a large number of articles or papers, but the link between safety culture and social media is under-researched. Indeed, it is essential to understand the mechanisms and issues of the security culture of social networks, in order to make a contribution that has been little explored by research.

Despite these concerns, it can be noted that this topic is not sufficiently addressed in research. (Zhou et al. 2024) note that there is a lack of empirical research on the real impact of engagement on social networks on the perception of security. This work therefore aims to try to enrich knowledge on this subject. Indeed, a literature review (Laroche, L'Espérance, et Mosconi 2020) shows that only seven studies are focus on the benefits provided by social media for promoting an healthy lifestyle for employees. This study also suggests that may be useful to promote OHS (Occupational and health safety) programs, but it is difficult to draw conclusions due to the lack of evidence and studies on this topic.

Social media use has increased in the last few years, thanks to the globalization of the digitalisation. Thus, the lack of scientific evidence and literature on the possible applications and impacts of social media on safety culture is poor due to the emergence of social media. This study aims to explore this topic and to try to address this lack of literature.

Research objectives and questions

As mentioned earlier, the objective of this work is to highlight the links between social networks and security culture by analysing their impacts. Indeed, security culture has traditionally been promoted using conventional methods (emails, posters, etc.), but social networks may represent an opportunity to transform these classic communication channels (cf. literature review). This analysis focuses on identifying the perceptions and practices of organizational security conveyed through social networks, whether positive or negative. The social networks targeted are all those currently used within organizations to promote security culture in companies (Workplace, LinkedIn, WhatsApp, etc.). More formally, this work seeks to answer the following research questions:

RQ 1: What are the positive and negative impacts of social media on security culture within industrial organizations and companies?

RQ 2: What are the possible applications of social media in order to enhance safety culture within industrial organizations and companies?

The first research question aims to analyse the concrete effects and links between social networks and security culture, while the second seeks to put future trends into perspective.

Methodology overview

This research work is structured beginning with a literature review, in order to understand the concepts of social networks and security culture through the definitions, concepts, scopes, and developments established by the academic literature. This section aims to provide a clear conceptual and theoretical foundation.

Next, the methodology used in this research is presented. It is based on a mixed-methods approach (qualitative and quantitative). Indeed, the first part allows for an understanding of the major trends and themes related to the issues, opportunities, and potential perceptions regarding the use of social networks as a tool to strengthen organizational security, through semi-structured interviews conducted with security experts (researchers and practitioners). This section is intended to feed into a second, more quantitative part, which aims to test possible correlations, hypotheses, and trends on the themes discussed during the semi-structured interviews. The second part will be developed through questionnaires and statistical analysis.

II / Literature review

The objective of this section is to provide an overview of the progress of academic research on the topics of social networks, safety culture, and the link between the two. These two topics will first be addressed separately.

Social networks are tools with a broad and dynamic definition depending on the era and technological advances, according to research. Due to the massive adoption of social networks by a large public, regulations have begun to emerge to monitor the content published on these platforms. These regulations can be issued by countries, supranational entities, or by the platforms themselves, through content moderation techniques. These latter techniques have proven very effective and relevant according to the literature, resulting in decreases in racist content or the spread of misinformation.

The notion of safety culture has also evolved over time, through scientific advances proving the danger of certain practices and the norms established to protect people at work. There are two aspects in this notion: a first qualitative aspect that focuses on the implementation of safety policies, and a second more quantitative aspect that focuses on how safety is measured and monitored (KPIs…). These two aspects complementarily contribute to the safety culture within organizations.

Finally, the link between these two notions is not currently covered in the literature, which justifies my research work. This link has been addressed through non-academic sources, analysed using the issues highlighted in the synthesis of research on social networks and safety.

Definitions of social media: historical overview

To understand today's social networks, it is relevant to look at their evolution, and in particular the definitions provided over time. Indeed, using a systematic literature review, (Aichner et al. 2021) identified 21 definitions of social networks from 1996 to 2019. This result derives from a search in the EBSCOhost database, using the keywords 'social media' or 'social networking site' in the title. This search yielded 88 relevant papers, from which the authors extracted 21 definitions by publication year. This wide variety of definitions highlights (i) the difficulty of defining a concept that is nevertheless widely understood, and (ii) the dynamism of the definition, which has evolved over time and with technological advances that have enriched the features and uses of social networks. The term social network was used for the first time in 1994 to describe a Japanese online environmental media: Matisse (Berry n.d.). To illustrate the evolution of definitions over the years, let us take the definitions given in 1996, 2010, and 2019 (Aichner et al. 2021), classifying them into 3 periods :

(i) The first period: virtual communities (1996 – 2002)

"When computer networks link people as well as machines, they become social networks, which we call computer-supported social network (CSSNs)" – Wellman (1996)

In this period, social networks are perceived as virtual communities. The technical dimension is central in the definitions of this era, yet the social and communal aspects are already acknowledged. A socio-technical approach is thus favoured at this time for defining social networks: technology acts as a communication tool serving the communities. Operating within a community inherently restricts communication spaces, which tends to limit the possible interactions.

The definitions from this period are primarily descriptive and functional. Technology is perceived as a mediating infrastructure, but the users' creative space is constrained by the very structure of the community.

(ii) The second period: Social Networking Site (2002 - 2009)

"Social network sites are web-based services that allow individuals to (a) construct a public or semi-public profile within a bounded system, (b) articulate a list of other users with whom they share a connection, and (c) view and traverse their list of connections and those made by others within the system" – Boyd and Ellison (2007)

In this period, the community gradually recedes, giving way to an increasingly prominent focus on the individual. Social interactions become more explorable through digital interfaces that open up virtual communities. Profile management thus becomes central, highlighting the growing importance of individuals. At the same time, network mapping emerges: connections between people are made explicit, often using a format based on mutual acceptance.

(iii) The third period: social media and user-generated content (2010 – 2019)

"Social media is a group of internet-based applications that builds on the ideological and technological foundations of Web 2.0, and that allows the creation and exchanges of user-generated content" – Kaplan and Haenlein (2010)

Here, it is observed that content generation takes on an important role, giving users an important creative function. The role of the platforms is still present, but become marginal in the different definitions used in this period. They thus become both producers and consumers, participating in a collaborative social dynamic. Indeed, interaction was previously limited to mere connection, but it now becomes more substantial. Content and user engagement are therefore central in the definitions, even though the role of technology remains supportive.

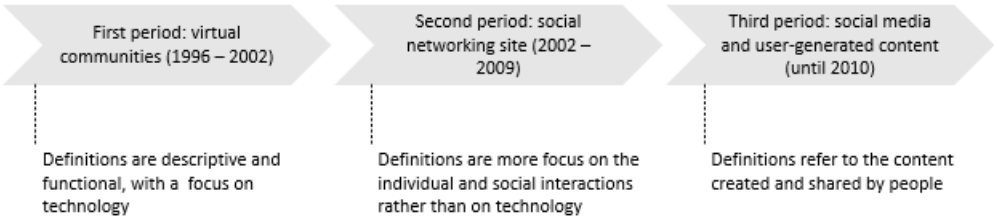

Figure 3: Evolution of social media definition

In summary, the definition of social networks shows a significant evolution: it was initially centred on describing the tool's functional aspects, but progressively, its social dimension has been recognised. This evolution reflects a deeper conceptual awareness, since the social dimension is less immediately perceptible than the technical one. This shift highlights that social networks have become ecosystems where social norms are created and broadcasted.

The term social network is often described in the literature as an "umbrella term" (Aichner et al. 2021) encompassing a very broad variety of online platforms. The difficulty in reaching a clear and universally accepted definition of social networks can be explained by several factors, such as the blurred boundaries between related concepts (platforms, online communities, etc.) as well as the disciplinary perspective adopted by researchers. For instance, a researcher in computer science is likely to provide a more technical definition, whereas a sociologist would focus more on the relational uses of social networks.

Evolution of social media: historical overview

This evolution of definitions goes hand in hand with technological advances and the changing uses of social networks. In another literature review, (Dhingra et Mudgal 2019) synthesized the dates of public release of major innovations and developments in social networks. For this synthesis, a social network is described as a group of Internet-based applications that enable the creation and exchange of user-generated content. According to the historical overview of social media (Dhingra et Mudgal 2019), one can classified the different periods according to the characteristics of social network :

(i) Emergence communication channel (1792 – 1895)

During this period, the term *social network* was not yet defined or used. The technologies developed during this time were not social networks, but rather important innovations in means of communication. Thus, long-distance communication greatly developed during this period (Telegraph 1792, Morse code 1836, Telephone 1876, Radio 1895). This period marks a major paradigm shift in communication methods, replacing traditional and slow methods (mail, written messages, etc.) with fast and efficient systems. These new and innovative methods of information transmission were based on electromagnetism, as they used electric currents (Telegraph, Morse code) as well as electromagnetic waves (Radio).

(ii) The emergence of digital communication (1970 – 1990)

This period marks the advent of digital communication technologies. Indeed, in 1971, Ray Tomlinson sent the first electronic message using ARPANET, which was a revolution in information transmission. Some sources (Sajithra K 2013) even note that the creation of email (1971) represents a significant development in the history of social networks. Although there is debate over whether emails can be categorized as a social network, this is consistent with the earliest definition (1996) of social networks—as computer networks connecting people as if they were machines. Thus, email marks an important and revolutionary starting point in long-distance communication between individuals. Usenet, created in 1979, marks the beginning of real-time messaging, representing a significant evolution from the email systems used until then. Following the early stages of electronic communication, more spontaneous, conversation-based systems were implemented. IRC (Internet Relay Chat, 1988) aimed to improve existing messaging systems by enabling one-to-one communication via private messages, more spontaneous and closer to the flow of real conversation.

At the end of the 1970s, a network connecting computers and allowing users to exchange messages appeared: the Bulletin Board System (BBS). It is one of the precursors to social networks according to the definitions mentioned (cf. definitions of social media: historical overview). However, it was in 1990 that information sharing experienced a major turning point, following the deployment of the World Wide Web. Indeed, this interconnected information system enabled the sharing of resources through hyperlink. Some definitions of social networks even use the Web as the reference interface, which is still the case today. It is the Web that made modern social networks accessible, as it serves as a platform for blogs, personal pages, and message forums—all considered social networks, as mentioned earlier.

(iii) The first interactive virtual communities (1970 -2000s)

Thanks to the introduction of the Web, the first social sharing platforms such as blogs appeared (link.net 1994, Classmates 1995, Six Degree 1997, Blogger 1999, Ryze 2001, Friendster 2002…). This was the beginning of social networks, in the form of communities of people interacting together.

However, interactions were quite limited, as they were structured according to community-based logics.

(iv) Mainstream social networks (2000 – present)

The social networks known and used today appeared in the 2000s and 2010s (LinkedIn 2003, Facebook 2004, YouTube 2005, Twitter 2006, Instagram 2010…). Beyond the technical evolution of social networks, the target audiences of these platforms have also evolved over the years. Some social networks, such as Facebook, were first built as niche platforms before becoming widely used. Indeed, this platform first emerged in universities, since it was necessary to use a university email address to create an account. Later, Facebook gradually opened up to the general public (Boyd et Ellison 2007). The strategy of restricting access to a site according to certain criteria was not only used by Facebook. Other platforms, such as MyChurch or aSmallWorld, deliberately limited their target audience in order to appear exclusive. Furthermore, these platforms were structured in communities - as mentioned previously - bringing people together around common themes and subjects. Current social networks, however, aim to bring people together who do not necessarily share the same interests, by opening up to all audiences.

A number of early social network users complained about the lack of available actions once friend requests were sent. Indeed, some were not ready to meet strangers, while others simply did not have enough friends active on these social platforms (Boyd et Ellison 2007). This shows a significant evolution over the years, as people are now more open to talking to or meeting strangers, evidenced by various thematic groups on social networks such as Discord, which bring together people with a shared passion who do not know each other beforehand.

Moreover, the functionalities offered by social networks have developed significantly, shifting from a community-based system to a more individual-centered vision (Cf. Figure 4). Social platforms are no longer limited to a specific function such as sending textual information; they have evolved to offer innovative features such as sharing photos, videos, voice messages, and other content, making social networks more engaging and less monotonous.

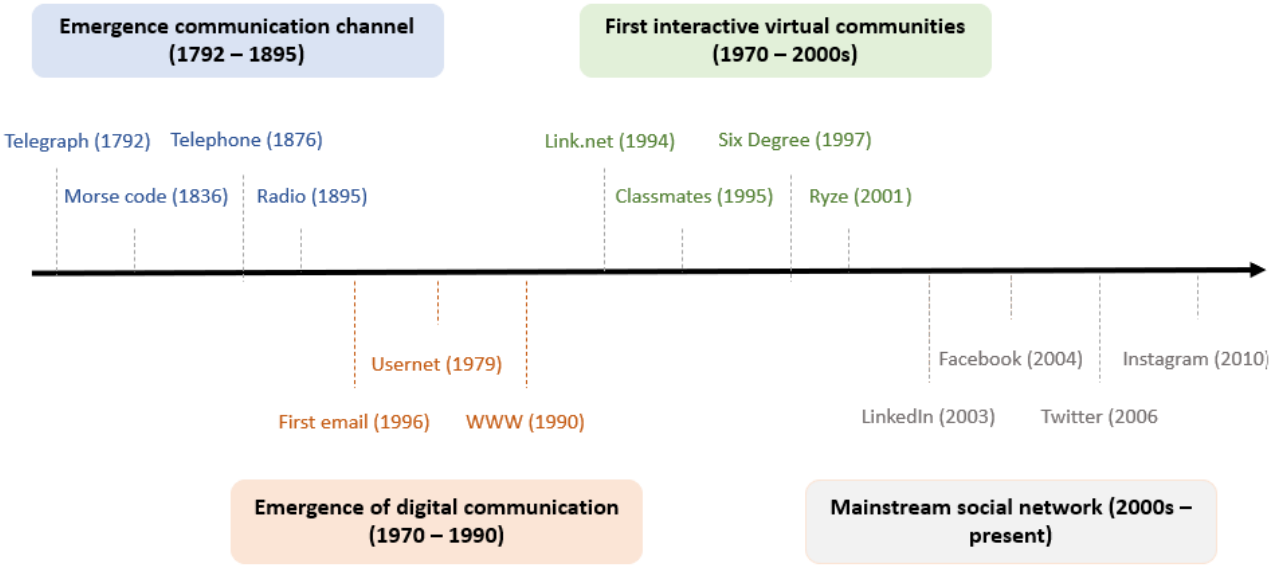

Figure 4 : Evolution of digital communication and social media

Regulations of social media by authorities

Thus, this openness to all audiences raises questions, particularly regarding the content shared on social media. Given their large potential for influence, social networks have become extremely powerful vectors of influence. One can therefore legitimately ask about the regulation in order to prevent potential issues for users.

This issue of platform regulation has been politically debated. The U.S. Congress has discussed stronger control over these companies on several occasions, but without reaching a comprehensive coercive policy (Nieminen, Padovani, et Sousa 2023). The European Union, however, has been the most committed actor on this matter. Indeed, in 2018, the European Commission introduced the General Data Protection Regulation (GDPR), with the aim of protecting personal data. Article 5 of this directive highlights the principle of lawfulness, which is closely linked to the user's consent. The data subject must therefore freely and knowingly accept or refuse the processing of their personal data (Battista et Uva 2023). Although social media platforms were not its primary target, this reform marked a symbolic turning point in the regulation of a space that had previously escaped almost any form of legal framework. Moreover, Directive 95/46/EC preceding the GDPR – rendered obsolete by the adoption of the latter – states in its Article 2: "Data processing systems are at the service of mankind; they must, whatever the nationality or residence of natural persons, respect their fundamental rights and freedoms, notably their privacy, and contribute to economic and social progress, the development of trade, and the well-being of individuals" (Battista et Uva 2023).

Between 2021 and 2022, the EU launched a series of regulatory initiatives aimed at better controlling digital platforms, including the Digital Services Act (DSA) and the Digital Markets Act (DMA) (Nieminen et al. 2023). The objectives of this regulatory framework are to:

- Improve the monitoring and control of the dissemination of disinformation and misinformation;
- Strengthen the regulation of targeted advertising and the prevention of its misuse;
- Increase the transparency of algorithms that collect and exploit user data;
- Impose specific obligations on the largest platforms that act as "gatekeepers" in their markets.

Although a pioneer in regulation, the EU waited until the 2020s to regulate platforms that had emerged decades earlier. Several reasons have been put forward to explain this slow reaction on the part of the EU: the influence of major economic powers acting in favour of the deployment of the Internet and platforms, the complexities of coordinating the EU's digital policies, or the implementation of neoliberal policies in Europe (Nieminen et al. 2023). This late reaction by the EU can also be explained by a desire not to hinder tools perceived as forms of individual freedom, but also as sources of economic competitiveness. The issue of the legal framework also makes regulation complicated, since digital companies and platforms refuse to pay taxes or duties in the countries where they do business. Indeed, they engage in tax optimization by relocating their headquarters in order to avoid certain standards, regulations, or taxes. Many platforms have established their headquarters in Ireland, where the tax rate is around 1–2% (Battista et Uva 2023). This is why a supranational body such as the European Union is relevant for regulating large platforms, in order to harmonize the rules between the countries.

The content of the Digital Services Act (DSA) is studied in this article (Muhammad Muslim Rusli et al, 2025), which compare the DSA and Malaysia's regulations regarding social media:

- Application: applies to all intermediary services conduit/caching/hosting services. Extra obligations to VLOPS (Very Large Online Platforms) with over 45 million users;

- Harm Mitigation: VLOPS must mitigate risks delated to illegal content and systematic risks. Smal and micro-enterprises are exempt from this duty;

- Content risk definition: What is defined as illegal content depends on the laws of the country hosting that content;

- User empowerment: It is mandatory to implement a system that allows users to report illegal content. Platforms must also properly inform users about these reporting systems;

- Minor protection: Special obligations exist for VLOPs to protect minors, including protection from illegal content and targeted advertising;

- Transparency obligation: Requires clear, transparent terms and conditions;

- Legal Authority: Enforcement by national authorities and European Commission;

- Intermediary liability: EU members and the EU Commission may impose 6% fines of annual turnover for non-compliance.

These different regulations aim to govern the content on social media and on the internet more broadly, while also drawing users' attention to the associated dangers. These regulations help connect the impact of digital platforms on user practices to the need for a stronger culture of security.

Self-regulation by the social platform

The regulations by the countries or EU Commission are not the only way to regulate social media content. In fact, the enterprises themselves have tied to regulate the content published on their platforms. For instance, several famous platforms regulate their contents during Covid-19 pandemia (Marina Rizzi, 2024):

- Facebook deleted more than 3,000 accounts and removed more than 20 million posts because of vaccine misinformation;
- Youtube removed more than 130,00 videos due to misinformation content;
- Twitter removed posts that spread information and narratives that were against vaccines.

On December 2020, Twitter declared that it was going to ban and remove any tweet that contained racist content (Marina Rizzi, 2024). Twitters' policy aims to fight against racism by banning or suspending the account or removing the racist post.

This article (Marina Rizzi, 2024) studies the difference between two social media: Twitter and Parler. The first one had implemented rules in order to decrease the number of racist posts. The second one is better known for its poor moderation. The author selected a group of users active on both social media in order to compare them and measure of Twitter's policy id effective or not. In that respect, 8 million tweets from almost 7,000 users who mentioned race or minority-related keywords were analysed in the study. The estimation of the effects of the Twitter's policy against racism is studied using a linear panel model. The results of this study are unequivocal: the policy implemented by Twitter is effective. In fact, after the policy, the number of racists publication decrease by 19% and the number

of posts with hate speech decrease by 21%. However, it's important to implement global regulations to all platforms, because the article evoke a possible substitution of abusive behaviours from Twitter to Parler after Twitter's policy, because Parler's policy is less binding than the first one.

When policies are implemented by the platforms to regulate the content, they are effective. Every single action taken to fight against harmful content on social media is useful and has a positive effect in practice. These mechanisms of self-regulation allow my research to connect platform governance with development of safer practices among users, highlighting the behavioural impact of social regulation.

Self-regulation by the users of social media

Beyond the companies themselves, users are also capable of self-regulating the content they publish and disclose on social networks. Indeed, a number of psychological causes can explain these self-regulation behaviours. (Rebello et al. 2024) conducted a study to identify correlations between psychological factors and social network usage. This study was carried out following a consultation with social media users, using advertisements on Facebook and Reddit pages, as these are spaces where people share personal stories. The participants of the study responded to a questionnaire using a Likert scale. The aim of the study was to adopt a holistic approach. Certain correlations are interesting to highlight and analyse (Rebello et al. 2024):

- An insecure sense of self was strongly correlated with a need for external stimulation which translates into significant use of social networks to be stimulated;

- A positive correlation was found between an anxious need for external validation and an insecure sense of self. Anxious users, who tend to spend more time online, experience a need for external validation, which may manifest through the publication of content on platforms;

- A secure sense of self was negatively correlated with naïve posting. Even insecure individuals practice a form of self-regulation to avoid facing negative emotions;

- An insecure sense of self was correlated with the tendency toward self-regulated posting. Anxious individuals experience negative emotions such as social fear, which leads to better control over what they share on social networks.

From these few correlations extracted from the study (Rebello et al. 2024), it can be observed that self-regulation on social networks is influenced by the user's personal psychology, particularly their level of anxiety. Moreover, although people may disclose personal information online and on social networks, they can at the same time be concerned about their privacy and the protection of their data — this is known as the Privacy Paradox. Indeed, the literature shows that this paradox does not exist when a person is genuinely concerned about the potential consequences of revealing personal information (Rebello et al. 2024). By being aware of their privacy, users can therefore adopt individual behaviours to limit their publications and the information they reveal online.

Before posting online, users assess the advantages and disadvantages of disclosing themselves on social networks, a process known as Privacy Calculus, which reflects the users' consideration regarding whether or not to engage in content publication.

Another way to understand the phenomenon of user self-regulation comes from the Theory of Deviance Regulation. This theory predicts that actions translate into meaningful identities, insofar as they push individuals to deviate from the norms of their reference group (Hart Blanton and Charlene Christie, 2003 – folder). In other words, this theory states that people wish to maintain or strengthen a positive social identity. To do so, they regulate their deviance in relation to group norms, they decide for themselves when it is good or bad to distinguish themselves from others. This theory can be applied to social networks. Indeed, users may wish to maintain a valued identity, being perceived as engaged, interesting, and authentic, while at the same time conforming to certain group norms (friends, family, social norms, etc.). For example, people who post content to show support for a cause will be perceived as having a committed and therefore positive identity. Thus, the user self-regulates by anticipating group reactions, modifying their behaviour to remain within the zone where their deviance is perceived as positive rather than negative.

Safety culture: definitions and origins

The notion of safety culture was initially used mainly in industrial settings. It was often neglected in favour of increasing profitability, as companies saw it as a costly and unnecessary expenditure (Cole, Stevens-Adams, et Wenner 2013). Several major industrial accidents, such as the Triangle Shirtwaist factory fire (1911), Chernobyl (1986), or the series of dam collapses in Banqiao, China (1975), prompted strong regulations requiring industries to implement important safety standards. The term "safety culture" was in fact first cited in reference to the Chernobyl nuclear accident. The International Atomic Energy Agency (IAEA) even described the safety culture there as poor or weak.

As with the definition of social networks, there is no single universal definition of safety culture. As social media, the definition tends to vary over the years, depending on the researchers' fields of expertise. Between 1991 and 2011, 16 different definitions were identified (Cole et al. 2013). Some examples are listed below:

Definition	Author	Date
"Safety culture reflects the attitudes, beliefs, perceptions, and values that employees share in relation to safety"	Cox and Cox	1991
"The collective mental programming towards safety of a group of organization members"	Berends	1996
"Culture is the product of multiple goal-directed interactions between people (psychological), jobs (behavioural), and the organizational (situational); while safety culture is that observable degree of effort by which all organizational members direct their attention and actions toward improving safety on a daily basis"	Cooper	2000
"A set of prevailing indicators, beliefs, and values that the organization owns in safety"	Fang et al.	2006

Table 1: Evolution of the definitions of social media (source: (Cole et al. 2013))

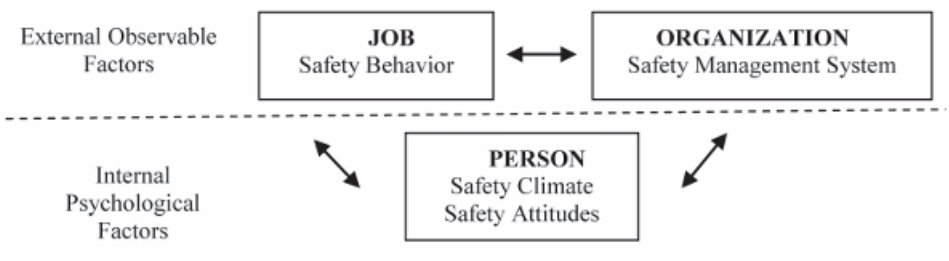

Figure 5: The safety culture model by Copper (1998) - (Odrakiewicz s. d.)

An analysis of the evolution of these definitions highlights a paradigm shift in the scope of the concept. Initially, safety culture was focused on the individual (1991). When approached individually, safety culture tends to place responsibility and actions solely on individuals. This can lead to the perception that accidents are caused only by individual factors, such as failing to follow safety rules. Over the years, the notions of groups and organizations gradually appeared. In contrast to the previous individual approach, a collective one emphasizes shared responsibility, where individuals are links within a system. This shift also reflects the growing importance companies place on safety, as the entire organization mobilizes to prevent risks.

While safety culture is focus on collective behaviours and long-term organisations, safety climate is rather a snapshot of the current state of the organisation. Thus, most of the KPI measured the real performance of the organisation, so rather link to safety culture as they represent persistent behaviours and organisation practices. Some indicators or results extracted from survey reflect the underlying of safety climate. Between 1980 et 1997 (Cole et al. 2013) a collection of 9 definitions extracted from the literature is presented. Some of them are quoted below:

- *"A summary of molar **perceptions** that employees share about their work environment"* – Zohar (1980)
- *"A set of **perception** of beliefs held by an individual and / or group about a particular entity" – Brown and Holmes"* (1986)
- *"The shared **perceptions** of organizational members about their work environment and, more precisely, about their organisational safety policies"* – Cabrera et al (1997)

Despite the years and the various researchers who have worked on these definitions, the notion of perception remains predominant. While safety culture is focus on collective behaviours and long-term organisations, safety climate is rather a snapshot of the current state of the organisation. Thus, most of the KPI measured the real performance of the organisation, so rather link to safety culture as they represent persistent behaviours and organisation practices. Some indicators or results extracted from survey reflect the underlying of safety climate. This notion is not only limited to rules, procedures that guaranty safety, but rather on the perception of them by people.

Safety culture is not limited to the protection of operators and workers, but also extends to the protection of clients, the general public, and the environment. It is therefore a very broad concept, which also takes into account material damage, even though physical harm is generally considered more serious. Safety culture aims to prevent and/or minimize the impact of accidents, which can be defined as undesirable and uncontrollable events (Shamsuddin et al. s. d.).

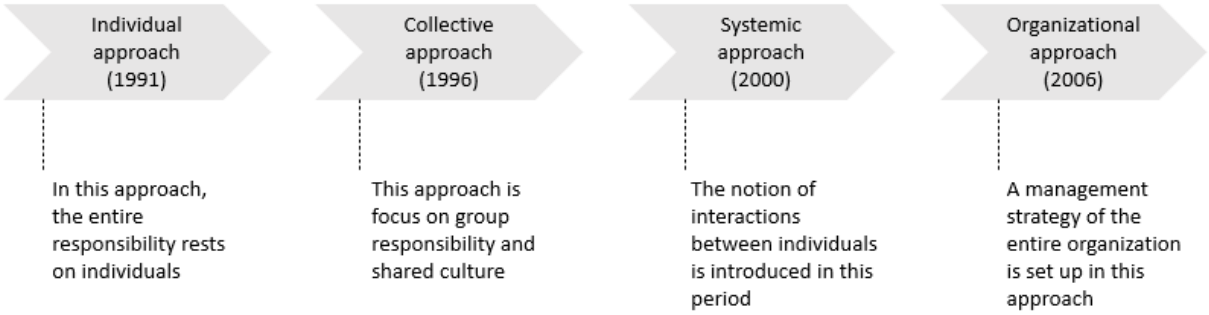

Figure 6 : Evolution of the safety culture approach

Evolution of regulations to enhance safety culture

In order to improve workplace safety, regulations and standards have emerged over the years. This is notably the case with HSE (Health, Safety & Environment) standards, which began to be introduced with the rise of mass industry around 1850 during the Industrial Revolution (Anaba, Kess-Momoh, et Ayodeji 2024). The purpose of this standard is to include all stakeholders within a company, workers, employees, and managers, in order to organize the collective as a whole.

Three main components are identified within the HSE framework (Anaba et al. 2024):

- Health: management of physical injuries, long-term illnesses, and employees' mental well-being;
- Safety: prevention of accidents through rigorous risk analysis processes;
- Environment: management and recovery of waste, air and water quality, and companies' environmental performance.

At the time of their introduction, these regulations focused mainly on a limited range of industrial accidents, such as fire prevention and ventilation. The goal was more to minimize consequences than to actually prevent accidents. Industrialists were primarily focused on profitability and viewed HSE investments as significant costs that would ultimately reduce their profits. Over time, as accidents multiplied and public pressure increased, HSE regulations became increasingly stringent. Advances in technological and scientific knowledge, particularly in medicine, also made it possible to adopt stricter standards, justified by increasingly precise scientific understanding.

HSE standards differ from one country to another, which can be problematic in a globalized economy. Generally, the most industrialized countries tend to have stronger HSE regulations than developing nations, which prioritize rapid economic growth. However, several international organizations aim to harmonize HSE standards across countries, such as the ILO (International Labour Organization) and the WHO (World Health Organization). These differences in standards can encourage companies to relocate their operations to less demanding countries in order to increase profits. This is precisely why international organizations, although lacking executive power, strive to promote common standards. It is also essential to ensure the protection of imported goods and services that do not comply with the same standards as local companies, which may be subject to stricter regulations.

The literature thoroughly documents the relationship between regulations, safety standards, and the outcomes achieved (Nævestad et al. 2019). Public authorities have therefore been established to legislate and enforce safety regulations in companies, particularly in strategic industrial sectors such as

energy and transport. As a result, regulatory and supervisory bodies such as nuclear safety authorities, petroleum, railway, or maritime agencies have been created in many countries. These sectors are considered sensitive given their history of major disasters, which justifies increased vigilance to standardize and monitor safety rules.

Globalization has fostered the growth of international trade, raising the issue of harmonizing standards to ensure a minimum level of safety. Although most international bodies do not have direct regulatory power like a state, they establish standards, recommendations, and best practices that member countries are expected to implement in their national laws. Examples include:

1) International Civil Aviation Organization (ICAO): defines international air safety standards, including pilot training and equipment maintenance;
2) International Atomic Energy Agency (IAEA): develops nuclear safety standards and conducts audits, training programs, and site inspections;
3) International Union of Railways (UIC): promotes railway safety standards.

According to (Nævestad et al. 2019), the traditional approach to regulatory safety policy (the so-called "hard" approach) is based on strict compliance with specific rules. More recent approaches favour self-regulation and a more democratic and consultative function.

Quantitative approach of safety culture: KPIs and metrics

A quantitative approach exists for assessing safety culture. In this approach, the term security metrics is often used, which tends to refer to quantitative data, although there is no widely accepted definition (Pendleton, Garcia-Lebron, et Xu 2016). This numerical approach makes it possible to measure phenomena objectively.

There are international guidelines such as ISO/IEC 27004, which deals with information systems security (Andrzej Pacana & Karolina Czerwińska, 2025). Although this standard is specific to information systems, the KPI construction approach can be applied to other sectors of activity.

For the implementation of effective KPIs, the standard recommends a structured approach (Andrzej Pacana & Karolina Czerwińska, 2025):

- 1) **Definition of the resources to be measured**: identification of what must be monitored and measured, referred to as an asset. This can be a process, a plan, or an information system, in order to measure defined, documented, and repetitive activities, actions, or processes;
- 2) **Specification of reference points for each measurement domain**: these points may represent system performance limits, such as critical thresholds or defined and approved targets;
- 3) **Data collection**: gathering the necessary data over a given period to create relevant safety indicators;
- 4) **Definition of measurement methods**: obtaining a reference value for an indicator that serves as a source of information for improving or confirming the effectiveness of the applied solution;

- 5) **Interpretation of measurements**: based on the differences between the measured value and the reference value for a given indicator, the interpretation should identify areas for improvement. This step can be facilitated by defining value ranges and implementing actions adapted to the magnitude of the deviation;

- 6) **Communication of results**: communicating the assessment to relevant stakeholders, for example in the form of reports. Ensuring the comparability of measurement results provides the basis for deciding whether to conduct a detailed review (audit) or take actions aimed at improving safety.

Figure 7: Construct relevant KPIs

Qualitative approach of safety culture

The other side of security is the qualitative approach. The indicators we previously discussed are important data for managing an organization. However, these measures describe the consequences but rarely the mechanisms, rules, and practices put in place to improve security.

There are two ways to ensure workplace safety within companies and organizations: prophylaxis (V S Serdyuk et al, 2020):

- Prevention: aims to adopt preventive measures to avoid accidents before they occur;
- Minimization: aims to adopt measures a posteriori, once the accident has occurred. The objective here is to minimize its consequences.

The Bradley Curve method is effective in addressing the first point. This curve makes it possible to assess the safety culture in order to measure the level of maturity of a company. It can be applied to many fields to evaluate safety culture and, in all cases, provides a model for interpreting the evolution of behaviours and attitudes toward risks.

Four levels of maturity are presented in this curve (V S Serdyuk et al, 2020):

- 1) **Reactive**: no safety management, no process is implemented, no action is taken. The accident rate is high, and the overall performance of the organization is low. Individuals decide on their own conduct based on personal experience or feelings;

- 2) **Dependent**: risk management is carried out under supervision. The accident rate decreases compared to the first level;

- 3) **Independent**: individuals' safe behaviour is determined by their awareness and personal learning;

- 4) **Interdependent**: work is organized in a structured and team-based manner. It is founded on shared goals and values, with attention given to other team members.

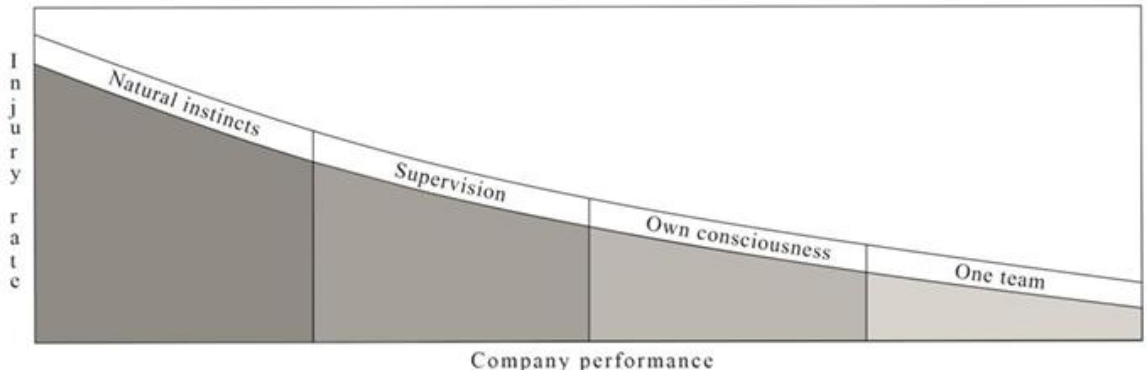

Figure 8 : Diagram "Curve Bradley" (V S Serdyuk et al, 2020):

This evaluation curve can be applied to many fields and, in all cases, provides a model for interpreting the evolution of behaviours and attitudes toward risk.

However, despite all the rules an organization may establish, accidents remain inevitable, a reality consistent with the Bradley curve presented earlier. Sociologist Charles Perrow explains that there are technical systems so complex and tightly coupled that accidents are a normal occurrence (Le Coze, 2011). Thus, even with the implementation of strict safety policies and their effective operational application, complex systems will inevitably produce accident situations.

This concept introduces the notion of the "normal accident", understood as a natural consequence of the way a system or organization is designed. Perrow introduces two key ideas to characterize "high-risk systems" (Le Coze, 2011):

- **Interactions (linear / complex):** represent the unpredictable relationships between subsystems, including dependencies that are difficult to anticipate;
- **Coupling (tight / loose):** refers to the degree of interdependence among components within a system or organization, with varying degrees of flexibility (tight coupling / loose coupling). A disturbance in one part of the system can therefore propagate and impact other components or the entire organization.

Charles Perrow thus defines a matrix composed of four quadrants (Le Coze, 2011):

- **Tight coupling and linear interactions (Zone 1):** the interactions between system components are simple and understandable. This corresponds to a zone with a high risk of error propagation, even though the system itself is relatively simple;
- **Tight coupling and complex interactions (Zone 2):** this corresponds to the zone of normal and systemic accidents, which are unavoidable due to the system's high level of complexity (e.g., nuclear power plants, space shuttles);
- **Loose coupling and linear interactions (Zone 3):** represents sequential processes with significant flexibility and opportunities for correction. Because of their sequential nature, these systems are predictable and manageable;

- **Loose coupling and complex interactions (Zone 4):** the interactions are numerous, but a degree of flexibility remains. This zone represents systems that still carry a non-negligible risk of accidents, though the propagation and consequences of these accidents are limited and contained.

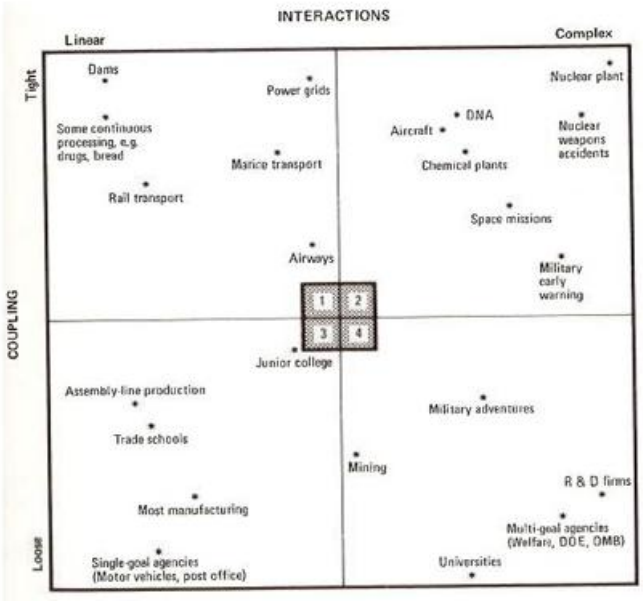

Figure 9: Perrow's matrix (Le Coze, 2011)

By interpreting Perrow's matrix (Cf. Figure 9) as well as the concepts introduced by the same author, several important elements emerge:

- **Perrow distinguishes between two types of risks: structural and avoidable:**
  - **Structural risk** does not depend solely on individual performance, overall safety strategy, or process quality, but rather on the very structure of the system itself. Thus, complex systems inherently generate accidents due to their structural nature. The challenge, therefore, is to minimize the frequency and consequences of accidents, acknowledging that in such systems, accidents are to be expected.
  - **Avoidable risk** refers to accidents that can be prevented through a strong safety culture by defining and adhering to safety processes. This type of risk falls under organizational and human responsibility, rather than technical aspects as in structural risk.

- **With Perrow's classification of system risks, it becomes possible to anticipate certain outcomes:**
  - In **systems with linear interactions**, it is entirely possible to implement a proactive safety policy based on a preventive approach. Indeed, such systems are relatively simple to understand and transparent, which facilitates the drafting and implementation of procedures, controls, and so forth.
  - In **systems with complex interactions**, the system's functioning is highly opaque, making the implementation of processes very complex or even impossible. Consequently, it is impossible to anticipate all risks. A corrective policy must therefore be implemented. However, this corrective approach must also include a structural dimension, meaning that it is necessary to act on the technical system itself, not solely on human behaviour or organizational structures.

Thus, based on Perrow's observation that some systems can address their safety issues through a preventive logic, it is relevant to identify the tools and methods used in preventive safety management. One of the best-known tools for risk prevention is the Failure Mode and Effect Analysis (FMEA). This method was introduced and developed in the late 1940s by the U.S. Army (Sharma et Srivastava 2018) and aims to prioritize risks by applying the methodology presented in Figure 10.

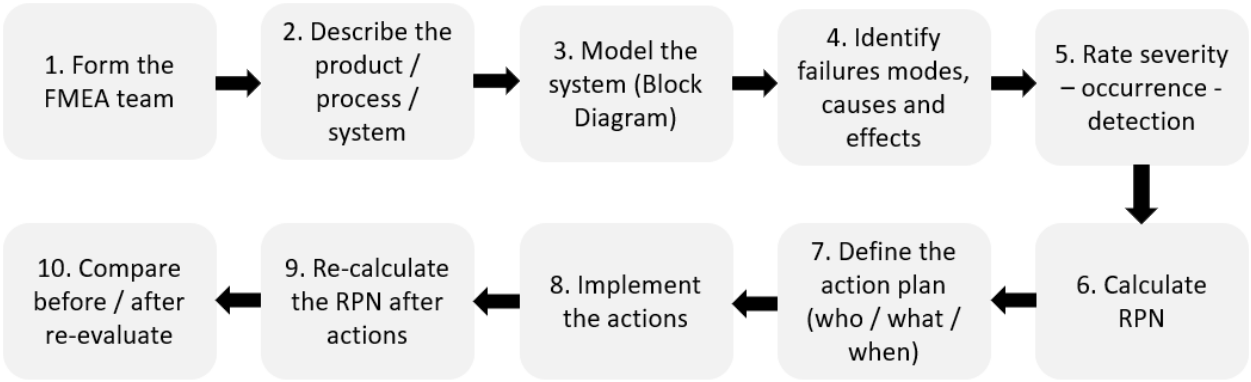

Figure 10: FMEA methodology (source: Sharma et Srivastava 2018)

The formula to calculate the RPN (Cf. Figure 10) is defined below (Sharma et Srivastava 2018) :

$$RPN = O\ x\ S\ x\ D$$

- RPN: Risk Priority Number
- O: Occurrence
- S: Severity
- D: Detection

Safety communication: traditional tools and methods

The implementation of safety policies must be accompanied by clear communication in order to involve all stakeholders within the organization. Communicating the safety culture allows (Naji et al. 2022):

- To convey the rules, procedures, standards, and guidelines in place;
- To demonstrate management's commitment to safety issues;
- To encourage communication between employees and management, which can help adjust policies based on feedback;
- To correct behaviours before they lead to serious accidents.

Before the advent of digital technology, traditional tools were implemented within companies and organizations. The most documented over the past 45 years are summarized below (Hafezad Abdullah 2022):

Tools / method	Description	Importance (according to literature)
Meetings	Periodic formal meetings that aim to discuss about hazards, incidents, new rules…	Routine safety meetings are one of the best ways to decrease risks, especially in specific sectors such as

		construction and oil & gas. Those meetings aim to align expectations and facilitate the communication
Toolbox talks / Toolbox meetings	A brief and short talk, before work starts. This tool is a task-specific one, it is the reason why it is brief	These tools are micro targeted ones so they have a direct and concrete effect on workers' situations, avoiding theoretical and general talks that can annoy workers
Posters / signage / safety boards	Refer to the visual communication deployed in the workplace, such as pictograms, reminders, poster…)	This tool is the earliest form of safety communication, reinforcing rules continuously and activate visual memory. They are simple tools, not deeply ones but they produce constant cognitive priming
Face-to-face training	A training session led by an instructor, usually in classroom not on the workplace	This method was the dominant one on the 1990s and 2000s. Studies highlight that this method has better results than self-reading
Bulletins / paper memos / newsletters	Refer to printed notes describing tasks or new rules. They can have a periodic format (monthly / weekly newsletter…)	This method was the dominant channel to share information about safety culture. The main strength of this tool is that it traces the communication

Table 2: most documented tools to communicate safety rules (source: (Hafezad Abdullah 2022))

Although still in use, these tools and methods have evolved with the emergence of digital technology, which includes social media. Digitalization has profoundly transformed the way communication takes place on social networks.

Measuring of people's perception

We saw previously the methodology to follow in order to establish relevant KPIs, rather focused on the process and rules established to measure the safety performance of the system. Nonetheless, those indicators don't take into account people's perception. It exists methodologies to set up questionnaires in order to obtain information on peoples' perception, such as road safety: (Fabricio Esteban Espinoza Molina et al., 2021) aims to design and validate a methodical approach of RSPQ (Road Safety Perception Questionnaire). **Although this study is focus on road safety, some elements of the method can be used in other contexts, such as people's perception of safety culture.** The study is structured in two main phases, comprising six sub-stages (Fabricio Esteban Espinoza Molina et al., 2021):

First step: design. Sum-up of this step: this development stage includes the identification and selection of variables according to available evidence and expert knowledges, validation of the selected variables by an expert group, and the construction of the instrument (questionnaire). In detail, those steps are composed of sub-stages presented below:

Stage I: identifying and selecting RSPQ variables

Sub-stage 1: identification and selection of road safety dimensions and items

- A literature review is carried using different data in a specific time slots. To identify the relevant literature, keywords such as “road safety” or “drivers’ behaviours” are used. The objective is to identify existing validated questionnaires that asses drivers’ perception;
- Researchers analysed nine National Road Safety Plans of South America countries in order to identify items (questions and indicators) used to assess road safety. The objective is to group common items employed in road safety.

Sub-stage 2: verification of compliance with RSPQ item criteria

- The items previously identified are validated against five criteria: relevance, measurability, clarity, non-redundancy and comparability;
- As a result, the number of items is reduced being submitted to evaluation by a panel of road safety experts.

Sub-stage II: Validation of the system of variables to make up the RSPQ

- A group of experts judge whether the variables are suitable or not, applying the Delphi method which consists to interview several experts, anonymously and iteratively. This method is considered the most appropriate to achieve convergence of the responses of the road safety experts. This methodology is also used in case of lack of information;
- The main point in this stage is to select relevant experts. In this respect, they used an “expert competence coefficient” based on the self-assessment of the experts, in order to rank them and select those that best fit the research objectives.

Sub-stage III: Construction of the RSPQ

This stage aims to establish criteria to construct the questionnaire. In the study, three criteria are used:

- Purpose of the instrument: aims to clarify the objective of the questionnaire;
- Instrumental conceptualization: this criterion aims to establish factors to structure and organise the measured variables;
- Structure and composition of questions, presentations and instructions: The structure chosen for the questionnaire is a five-points Likert scale, with a rating of: 1 = very low, 2 = low, 3 = medium, 4 = high and 5 = very high.

Second step: validation. This phase is focus on carrying a pilot test to determine possible corrections and adjustments to the questionnaire, after which a Confirmatory Factor Analysis is performed to determine its reliability and construct validity. To avoid bias as much as possible, filters are applied to delete incorrect questionnaires (for instance, a minimum completion time for the survey is required).

<u>Stage II: Questionnaire validity</u>

Sub-stage I: evaluation of RSPQ contents

- A pilot test is carried in order to address the possible concerns or doubts regarding the clarity and understanding of the questions. The survey is corrected in function of the feedback of this pilot test;
- Then, the corrected version of the questionnaire is presented to the group of experts. Their role is to judge the relevance and clarity of the questions asked.

Sub-stage II: Construct validity

- The questionnaire construct is validated using an Exploratory Factor Analysis (EFA) and Confirmation Factor Analysis (CFA). This validation aims to check the relevance of the items;
- The aforementioned statistical methods are used to remove outliers and to confirm the significant contribution of items and factors.

Sub-stage III: Reliability

- The RSPQ's internal consistency is evaluated using Cronbach's alpha on the Likert-scale items collected from the participants.

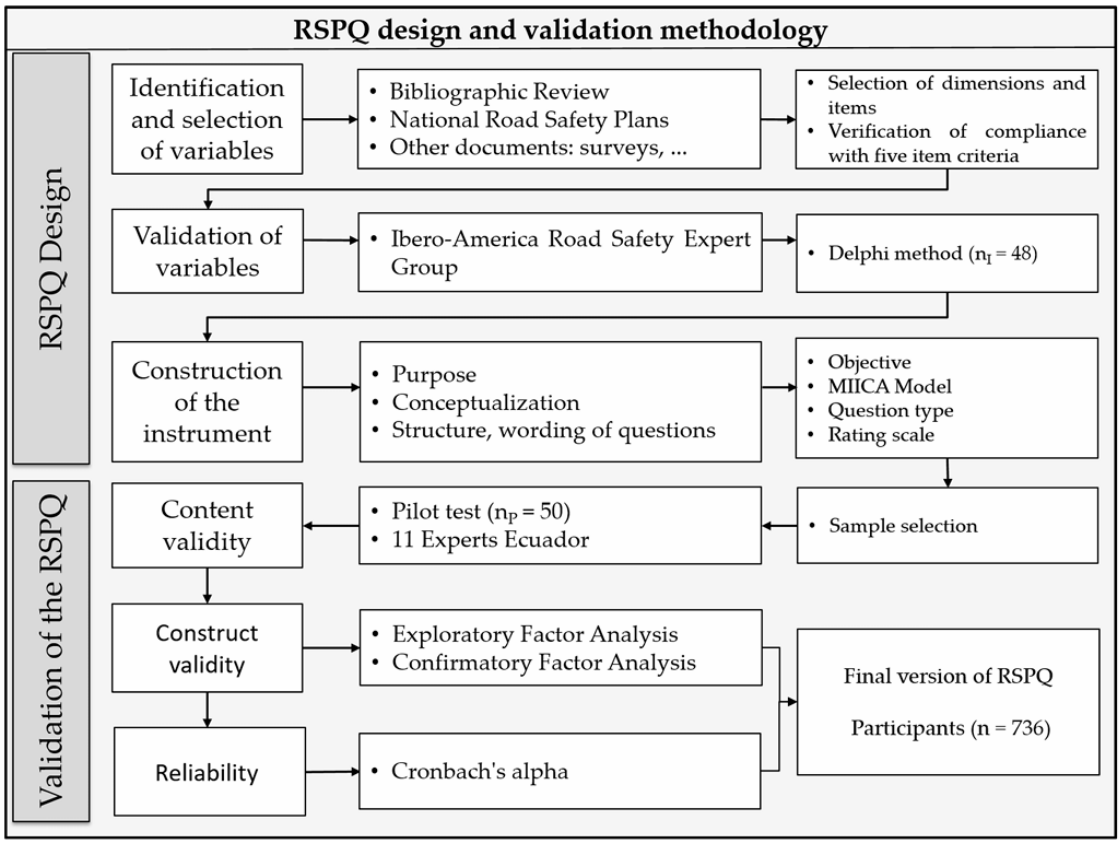

Figure 11: methodology process-flow for RSPQ design and validation ***(Fabricio Esteban Espinoza Molina et al., 2021)***

Although specific to the road transport sector, this article allows me to understand the steps to follow in order to build a relevant and qualitative questionnaire. The content of certain steps can therefore be fully adapted and reused within the framework of my research.

Social media and safety culture

Now that we have clearly defined the theoretical frameworks of social networks and safety culture separately, we can ask ourselves about the possible link between these two notions. These platforms are very effective means of dissemination and have a strong capacity for influence. For example, during the COVID-19 pandemic and the vaccination campaign, social media users were about three times more likely than non-users to follow health guidelines (Jafar et al. 2023). This aspect shows that social networks, through their rapid and massive dissemination of information, can be used to strengthen

prevention and support safety policies, with more effective results than traditional communication methods. Thus, despite positive impacts on preventive behaviours, these platforms have also exacerbated anti-vaccine debates by increasing misinformation due to sometimes deficient moderation (Jafar et al. 2023). More generally, social networks are tools that have both advantages and disadvantages for disseminating safety culture, for example in the health field (Jafar et al. 2023) :

- **Main advantages**: the platforms make current information and prevention messages accessible in impactful formats such as visual content (graphics, videos, images, maps, diagrams…). This type of content, more inclusive and dynamic, facilitates understanding and strengthens the impact of prevention policies. Beyond this aspect concerning the form taken by the information, social networks play a major role in the very rapid dissemination of information, in a logic of reactivity. Indeed, before the democratization of social networks, people read information in newspapers or watched it on television, which included a significant latency time between the emission and the dissemination of information. Social platforms precisely help to greatly reduce this latency time, making them an effective tool for crisis management;
- **Main disadvantages**: the speed of information dissemination on social networks is also its greatest drawback. Indeed, misinformation, fake news, and unsourced information spread as quickly as sourced ones. The content on these platforms is also shaped by influencers, who may be paid to produce advertisements and thus deceive and disappoint consumers, since moderation is less present on these platforms than on other traditional channels. The aggressive advertising of harmful products such as tobacco or alcohol is a practice used by companies on social networks, which contributes to the possible misinformation allowed by the format of these networks. Moreover, social networks use algorithms that tend to highlight content generating many reactions (likes, comments, views…), which encourages increasingly controversial content and can thus be problematic regarding safety. This type of algorithm also tends to polarize users by creating “bubbles” in which people are only in contact with others sharing the same opinions as themselves.

A literature review (Laroche et al. 2020) shows that social media could be use to enhance the lifestyle of employees, by promoting health practices. Despite the lack of scientific evidence on the literature concerning the topic of social media and safety culture, the conclusion of this study is summarizing bellow (Laroche et al. 2020):

- **Source of motivation**: social media can be a source of motivation for employees to adopt healthy lifestyle. For instance, the content explaining the physical evolution of people by adopting a healthy lifestyle can give motivation to the other users of social media;
- **Promoting healthy lifestyle efficiently**: the content promoting healthy lifestyle such as healthy food and exercise is also really efficient for the general population, based on the evaluation of young adults and adolescents. Nonetheless, these results need to be confirmed thanks to further studies, because this topic is not enough addressed for now;
- **Great communication channel:** social media can be a great communication channel to share information and good practices.

Social media and safety culture: case studies

We can now observe possible links between social media and the culture of safety, notably through case studies. The example of Carhartt, an American clothing company, is a good illustration of the connection between social media and the culture of safety. This company imposed vaccination or

weekly COVID-19 testing on its employees during the pandemic. However, the U.S. Supreme Court then blocked the federal mandate requiring companies with more than 100 employees to enforce internal vaccination (Yang 2022). Despite this decision, the CEO of Carhartt communicated to all employees that vaccination or weekly testing would remain mandatory for all company staff (Carhartt CEO says he's still mandating staff vaccinations. Now he's facing a boycott. - CBS News 2022).

This internal communication leaked on social media and provoked a wave of outrage among conservative circles, with many reactions on Twitter calling for a massive boycott of the brand. The CEO of Carhartt responded on Twitter that the safety of employees is a core value of the company and that it was an economic risk the company did not wish to take (Yang 2022). The *Guardian* article also shows that some employees disagreed with management's decision. However, it should be noted that some consumer reactions were much more positive, as this situation portrayed the company as one that genuinely cares about the safety of its workers.

This case study illustrates several important links between social media and the culture of safety:

- **Massive diffusion vector of social media:** social media gave great visibility to this story, which was relayed by major newspapers. Social networks clearly contributed to making this debate more visible, giving it national reach;

- **Polarization of the debate:** the trivialization of prevention within the culture of safety and the promotion of poor practices damage the perception of risk among both employees and citizens regarding vaccination, and more broadly, prevention and safety issues. By politicizing the debate, conservative and anti-vaccine groups polarized the issue of vaccination, which can also lead to decreased organizational trust and potential tensions regarding the future implementation of safety rules;

- **Internal mistrust:** this situation can compromise collaboration between employees and management, making it harder to implement safety policies. Indeed, as discussed previously, safety is built through coordination within an organization, where everyone has a role to play.

More broadly, this case study illustrates a new situation arising with the advent of social media. These platforms modify the space of debate, shifting it from the organizational (internal) sphere to the public (external) one, which can exacerbate tensions, harm constructive discussion, and undermine the safety and prevention policies pursued by companies. Thus, social media make the debate more emotional than rational, which can affect the values, behaviours, and perceptions related to people's safety.

A literature review (Laroche et al. 2020) highlights the transformation of the OHS system of a French enterprise (Selenis), using an information system combining intranet and OHS experts. The conclusions on the benefits of this system are presented below (Laroche et al. 2020):

- More sharing of information among employees;
- More collaboration between employees;
- Better onboarding for new employees;
- Creation of a new team identity.

Positive and negative impacts of social media on safety culture

Social media can also positively influence the safety culture. Indeed, Terry L. Mathis, founder of ProAct Safety, explains that an increasing number of companies are using social media as a means to

disseminate safety rules (Safety Culture and Social Media s. d.). They can be used to create discussion groups and accessible content that also promotes individual engagement. Some companies, such as Petzl, have implemented solutions like Workplace from Meta, a professional social network designed to improve internal communication and collaboration within companies (Clark 2022). Features such as sharing posts, photos, videos, or documents are available on this professional social network. This type of platform helps to streamline internal communication by transforming a “top-down” approach—where leaders communicate in a transversal and distant way, into an approach that is closer to workers, using a more accessible format.

III / Methodology

General introduction to the methodology used

This chapter aims to make explicit the macro-methodological choices and the approach adopted within the framework of this thesis work. The objective is to answer the issue of the study, by analysing the impacts of social networks on the culture of safety. Although both topics (social media and safety culture) are deeply addressed in the literature, the link between the two is not. This study is of exploratory – explanatory nature:

- **Exploratory**: the subject is very little documented, which leaves a lack at the level of the literature;
- **Explanatory**: the objective of the study is to identify potential relations between social networks and the culture of safety on various factors (communication, engagement, sharing of good practices, perception of rules).

To do this, a qualitative approach is used. As explained previously, the topic is poorly addressed in the literature, so I want to adopt an exploratory approach, using a qualitative method. Indeed, my thesis aims to identify the main themes, pros, cons and issues on the use of social media for safety culture.

Qualitative data collection instrument

The qualitative part aims to collect the opinions and impressions of people working in the field of security (cf. Population and sample). To do this, semi-structured interviews, that is to say composed of some key questions as a guide but being particularly flexible, are used. This choice is justified by the nature of the phenomenon under study, which involves complex perceptions, representations and social practices that are particularly difficult to quantify.

Preliminary question (PQ) to verify the profile of the participant: do you use social networks for subjects related to safety at work?

The participant is previously informed of the following definition of social networks: "For purposes of this chapter, we define social media as any online resource that is designed to facilitate engagement between individuals." – Bishop (2019) from (Aichner et al. 2021). Thus, email, newsletters or collaborative platforms are included in the category "social media" in this work, because the definition used is as broad as possible, and which fits perfectly with the exploratory aspect of my research.

The definition of safety culture is presented as all the practices, strategies and rules applied, that aim to reduce the number of accidents (physical or not). Thus, cybersecurity is also considered on the field of safety culture, because it concerns the security of the personal data of the worker, or the data of the enterprise.

Here are the questions that are going to be asked within the framework of these interviews, discriminated by major themes. The objective is not for all the questions to be explicitly asked during the interview, but rather for all the themes to be covered based on the participants' responses, and also to give a framework for the interview. The objective of these interviews is to address the two research questions (Cf. I/ Introduction): what are the possible applications of social media on the safety culture and the positive and negative impacts of this practise once it is used.

A) Concrete usage of social networks

- List the social networks that you use within the framework of your work?

- At what frequency do you use these social networks?
- What type of content do you publish on these networks?
- For what do you use these platforms: inform, ask for help, share experiences…?

B) Communication and diffusion of information

- Do these tools facilitate communication on subjects related to safety? Why?
- Can you give a concrete example in which a social network allowed to improve the diffusion of information in the case of a safety problem?
- Have you noticed differences between the traditional communication methods (e-mails, boards, meetings…) and social networks?)

C) Engagement and participation of people

- What type of content favours the most your participation / the participation of the people receiving the content?
- How do you perceive the engagement of your colleagues on this new way to communicate good practices related to safety? Does this practice favour engagement?
- How do these tools influence collaboration and solidarity between colleagues on safety?
- How do these tools influence the perception of personnel on the managers and people responsible for implementing rules and processes related to safety?

D) Obstacles and limits

- What difficulties do you meet in the use of these tools for safety?
- Do you have concerns regarding the confidentiality or the security of the information and data shared?
- How to improve the effectiveness of social networks at the service of the culture of safety?

Final questions

- Do you see any concrete applications of social networks in support of a safety culture?
- Do you wish to add something that has not been addressed in this interview?

Population and sampling: qualitative part

The targeted population, that is to say all of the people aimed at by this interview, is composed of:

- Researchers specialized in the culture of safety;
- Director, safety managers of companies;
- Managers who implement the processes and rules of the culture of safety with the employees;
- People in charge of communicating safety rules.

A sampling of around **9 – 17 persons**, representative of the various hierarchical levels of the population mentioned previously. Indeed, (Hennink et Kaiser 2022) show that the saturation -meaning the point at which additional interviews does not provide additional information – is between 9 and 17 participants. To do this, a reasoned sampling method (non-probabilistic) is used. This sampling technique aims to better target certain specific groups within the target population. The following

information is going to be indicated in order to be able to judge the representativeness of the sample in relation to the target population:

- **Position of the participant**: this criterion allows to discriminate three different categories:
  - Direction: the person decides the safety policies at the scale of the organization;
  - Executives / managers: their objective is to make apply the policies decided by the direction;
  - Employees / operators: execute the tasks and apply most of the instructions and safety rules.
- **Sexe of the participant:** to identify from a qualitative perspective whether there is a gender gap in the analyses of the impacts of social media on safety culture;
- **Field of work:** to explicit the possible differences of safety approach and perceptions depending on the activity sector of the participant;
- **Participant age:** only the range in order to protect the anonymity of the participant;
- **Interview duration:** this information aims to know the depth of the interview.

Moreover, information such as the duration of the interview, the framework in which the latter took place (at distance or in person), the gender of the person is going to be indicated. However, the anonymity of the person is respected, and a neutral naming is used (P1, P2…). All of the information allowing to possibly identify the person will be blurred.

Method used to address the problematic

In order to analyse the interviews conducted in this qualitative part, **a thematic analysis method** is employed. This method makes it possible to analyse interviews and qualitative data (Braun et Clarke 2006), which corresponds to the need of the study. This technique is not only descriptive and with the aim of organizing qualitative information but it is an analytical approach in its own right. The approach is divided into 6 phases (Braun et Clarke 2006), which have been adapted to correspond to the context of my study:

- **Familiarising with data**: the objective of this phase is to re-read several times the interviews carried out, while trying to identify common patterns between the interviews. The verbatim transcription of the interviews is essential in order to start to interpret the interviews. Although there is no precise guide for this transcription step, it is recommended to be rigorous, for example by paying attention to punctuation, since the latter can modify the meaning of a sentence;

- **Generating initial codes**: this step consists in attributing a code or a segment (word or short sentence) which summarizes the meaning of the passage studied in the interview. At this stage, there is not a lot of interpretation, since the objective is to summarize the raw elements of the interview in a broader element. For example, if during the interview a participant says: “I have the impression that the direction and the managers do not listen to the operational challenges in the implementation of safety policies”, this extract will be coded as “distance between direction & operation”. I also use sub codes in order to be more specific when necessary. I perform several iterations in order to ensure the coherence of the codes, and then group sub codes under their respective main codes;

- **Searching for themes**: when all of the interviews have been coded, a phase of more advanced analysis on the coding begins. Indeed, this phase aims to regroup codes between them, in order to make major themes emerge. For instance, 3 codes “distance between direction & operation”, “interactions between technicians & operators”, “tensions between managers and shareholders” can be group in a theme that catch the main idea: “interactions and dynamics between groups of people”;

- **Reviewing themes**: the objective of this step is to sort themes, by regrouping certain ones which are similar, or on the contrary by dividing themes in order to be more precise. Themes can thus be deleted or merged when some of them are too similar and catch the same ideas. I will use tables to carry out this grouping, which integrates the title of the theme and the codes in order to present from a very clear way my grouping;

- **Defining and naming themes**: after having well discriminated the themes between them in a global way, this step aims to describe them in a clear and precise way. For that, it is first necessary to specify the perimeter of each theme, that is to say what is included and excluded inside it. Then, it is necessary to write a description of each theme, by making explicit the interest of the latter in relation to the research problematic, and to name this theme by using a clear, precise and understandable title. The last step of this phase is to verify the global coherence between the descriptions, the titles and the content of each theme;

- **Producing the report**: this phase consists in the writing of the complete analysis of the themes previously worked on. This written part aims to link the themes between them, to interpret the latter by explaining their usefulness for the resolution of the research problematic. It is important to keep in mind that this report should use verbatims extracted from interviews in order to give consistency to the analysis, and justify the analysis I made.

In order to determine whether saturation has been reached, coding will be carried out at the end of each interview to check for the emergence of new codes. **Saturation is confirmed once no new code or theme appear after two consecutive interviews, as mentioned by (Dello, De Smet, et Sermeus 2025).** In this case, no further interviews will be conducted. Thus, the previously made explicit method (Cf. Figure 12) is going to be applied within the framework of my research work to analyse all of the interviews carried out (Cf. IV / Results).

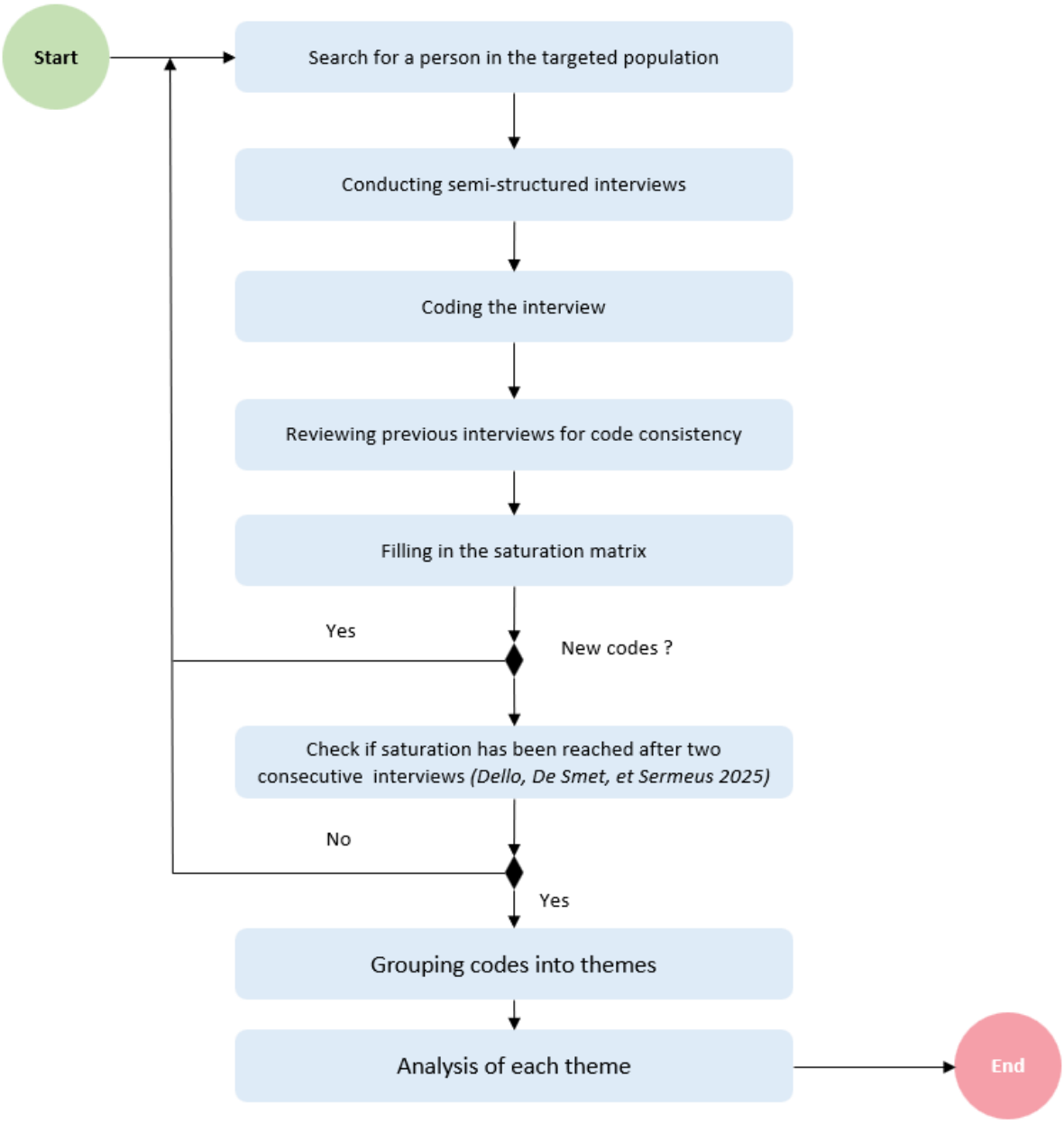

Figure 12: Overview of the methodology used

IV / Results

This chapter aims to present the different results of this thesis work, using the methodology previously seen (Cf. III / Methodology), using the so-called thematic analysis method. Indeed, the aim of this chapter is to address the researches questions presented in the introduction of this work:

RQ 1: What are the positive and negative impacts of social media on security culture within organizations and companies?

RQ 2: What are the possible applications of social media in order to enhance safety culture within organizations and companies?

Qualitative approach: actual sample

The table below (Cf. Table 3) summarizes the key information of the interview participants. As it was previously mentioned, all the interviews are anonymized (name of the company, name of the participant…). Only a few information is presented, in order to show the representativity of the sample of participants.

Participant number	Sexe	Position of the participant	Field of work	Participant age (years - range)	Interview date	Interview duration
P1	M	CEO	Plastics industry – large group	[45 – 54]	11/11/2025	33’
P2	M	HSE director	Plastics industry – large group	[45 – 54]	13/11/2025	45’
P3	W	Communication officer of safety researches	National Institute for security research	[54 – 63]	20/11/2025	26’
P4	W	Communication manager / professor	Plastics industry – large group / communication university	[54 – 63]	21/11/2025	47’
P5	M	Cybersecurity consultant	Consultancy firm	[23 - 29]	21/11/2025	38’
P6	W	Environmental security consultant / professor	University of environmental engineering	[54 – 63]	29/12/2025	53’
P7	W	Civil engineer: project owner assistance	Construction site work	[23 – 29]	12/01/2026	27’

Table 3: Summary of relevant information about the participants in the semi-structured interviews

Moreover, the saturation is confirmed after the seventh interview conducted (Cf. Methodology), as illustrated Figure 13 and Table 4 show us. Several codes (39) were identified in this thesis work.

Interview	Number of new codes	Comment
P1	21	Broad exploratory phase
P2	10	Broad exploratory phase
P3	3	Emergence of core themes
P4	3	Emergence of core themes
P5	2	Thematic consolidation
P6	0	Thematic consolidation
P7	0	Saturation is reached

Table 4: Saturation matrix

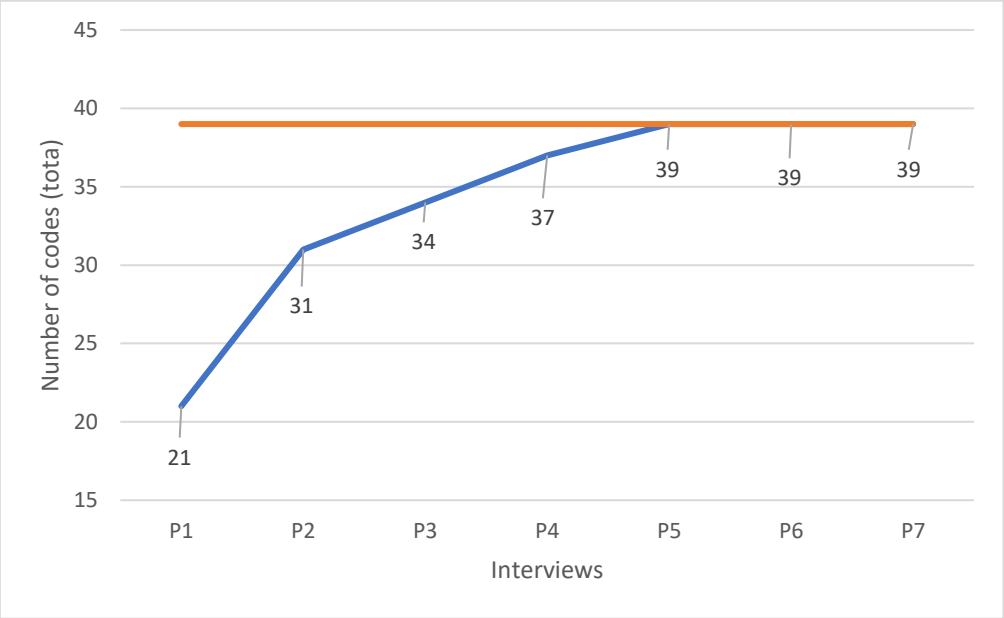

Figure 13: Saturation curve

Presentation of the codes

This section aims to present the different codes and sub codes of each interview. This in the application of the thematic analysis method to the interviews. The raw elements are available in appendix of the thesis; the written transcript is the very first step of the thematic analysis approach. As presented in the methodology of the thematic analysis, the step of coding includes no interpretation. In this respect, this section will only present the codes and sub codes used for all interviews, without commenting them. The goal of this section is to maintain the traceability of the thematic analysis, to demonstrate the thoroughness of the thesis. I previously made the step of initial coding, that aim to be verry broad in the quotes of verbatims and in the coding. The first iteration I made provide around 150 extracts coded for each interview. Some of the initial codes were really narrow, so I merged them.

Verbatim	Code	Platform (if applicable)

OK, so there's Teams. WhatsApp. OK. LinkedIn. SharePoint. Then we have a certain number of platforms. So, for safety, it's RedOnline. Actually, we subscribed to a service that lets us lock down the rules, the regulatory points. It's called RedOnline. [My safety director], he'll certainly tell you about it better. For monitoring laws. Obviously, email. That's it.	Multiple social media platforms	Teams; WhatsApp; LinkedIn; SharePoint; RedOnline; Email
So, already, email. Email allows us to launch safety weeks. It allows us to send out safety alerts when there's an accident or incident.	Social media to alert safety incidents	Email
Teams and SharePoint allow us to track — first to gather documents, gather action plans. And then they let us track everything we call transversal memos … have a common database … jointly track the progress on each transversal memo.	Social media as help to share information& Centralization of the information	Teams / SharePoint
We put our roadmaps there … So actually, it's more of a sharing exchange, a database exchange. It's a dynamic database.	Social media to help share information	Teams / SharePoint
During our safety weeks, through Teams, that's what allows exchanges between plants. So sharing photos, videos, and then making a best-of and then making a poster for the safety week, communicated afterwards to people.	Social media as help to share information	Teams
…have a common database … jointly track the progress on each transversal memo … We put our roadmaps there …	Centralization of the information	Teams / SharePoint
So sharing photos, videos … best-of … poster for the safety week … communicated afterwards to people.	Social media to help share information	Teams
And then it allows us … to have a common database … track the progress … roadmaps …	Centralization of the information & Data storage	Teams / SharePoint
…within 24 or 48 hours, there's an alert to everyone.	Fast information	Email / System alert
So actually, it's more of a sharing exchange, a database exchange. It's a dynamic database.	Centralization of the information	Teams / SharePoint
There are things that can't be replaced by social media; there are face-to-face meetings that can't be replaced.	Social media can't replace face to face	/

For example … onboarding … received by the safety manager … That cannot be replaced. That has to be face-to-face.	Social media can't replace face to face	/
I think face-to-face meetings are more an act of management … twice a month, we have a meeting about accidents …	Face to face communication from management	/
So it's a real complement, meaning the use of digital tools allows us to get certain messages across as if we were face-to-face in a room.	Social media as complement to face to face	Teams (for meetings)
We also put screens in our break rooms … So it's really a combination of both. In-person, or Teams.	Social media as complement to face to face	Screens / Teams
Teams is also all the institutional presentations, all the risk maps … monthly presentations of the status of safety actions … available to all plants.	Centralization of the information & Data storage	Teams
…there are activities carried out in the plant … very important to do in person with people to create engagement … trophies … in-person time with teams …	Face to face communication from management	/
Now … within 24 or 48 hours, there's an alert to everyone …	Fast information	Email / System alert
So it's really a combination of both. In-person, or Teams. It's a way to make safety part of everyday life, not just about following procedures and traditional methods	Social media as complement to face to face	Teams
There are things that can't be replaced by social media …	Social media can't replace certain actions / things	/
So the idea is to open people's minds and make everyone understand that we're in a risky environment … the first actor in safety is the person himself …	People engagement as safety actor	/
I want each executive committee member … to be present at a plant to make an impact …	Social media can't replace certain actions / things	/
I think the advantage of small groups is that … it's as close to the field as possible and they feel listened to … but that's more for our operators … so operators don't have access to WhatsApp … Teams … it's super important to do safety talks in person with them …	Access issues to social media for operators / People engagement as safety actor	/
Operators don't have access to WhatsApp. They don't have access to Teams.	Access issues to social media for operators / Top-down implementation of actions	/

Use media to reach managers. Use plant tours, in-person … to reach operators.	Using different communication methods for managers and operators	Media (email/Teams) vs in-person
Operators only have access to … the screen. And to the plant tour we can do … they don't have a mailbox to receive newsletters …	Access issues to social media for operators	Screens
Newsletters are displayed on screens … posters are put in the plants …	Social media as complement to face to face	Screens / Posters
In big groups, operators have access to computers … otherwise no.	Access issues to social media for operators	/
They can have notebooks … 'there's such and such dangerous situation' … suggestions for improvement.	Using notebooks to report hazards and suggest improvements	Written notebooks
Digitalization … I believe in it yes and no … the person must already understand …	Prerequisite for safety culture	/
But that mindset, you have to create it first. And it's not AI or social media that create it.	Prerequisite for social media use	/
Once he's mentally conditioned … then indeed it allows keeping traces, storing, sorting, tracking …	Prerequisite for social media use / Data storage	/
A staircase is swept from the top … initial pressure is on managers … objectives related to that …	Top-down implementation of actions	/
… it's a tool, all these media … allows conveying the information … putting guardrails …	Social media to help share information	/
… the meeting is complementary, because it's often done via Teams … but it's still face-to-face.	Social media as complement to face to face	Teams
Information circulates fast, it's like an open book, info circulates fast, there's information available to everyone …	Fast information	/
… when something happens at a plant … within 24 or 48 hours, there's an alert to everyone …	Fast information	Email / System alert
… the guy knows I'm going to ask him questions … he's mentally trained not to say anything random …	Motivation & engagement	/
So yes, somehow it allows structuring the system. Information circulates fast … we see the dynamic …	Fast information	/

The only somewhat sensitive data we have are data related to the group's risk mapping …	Sensitive data	/
… risk mapping … shareholders' view of the risks … not stuff we want to communicate …	Sensitive data	/
I'm more in favor of communicating them massively to all staff …	Mass communication to all staff	/
So WhatsApp, messages are encrypted if I understood correctly … once you have a phone, you have a spy in your pocket …	Sensitive data	WhatsApp
… more sensitivity on our financial accounts … budget …	Sensitive data	/
If the files disappeared completely, if they were encrypted, we'd lose much of our historical record …	Risk of data loss	/
… everything related to people's health could be considered sensitive data. I agree.	Sensitive data	/
It was on the network … on the server. Access to those data is limited, but you never know actually.	Sensitive data	Server / Network

Table 5: coding matrix for interview P1

Verbatim	*Code*	*Platform (if applicable)*
we use a lot of Teams, SharePoint in the broad sense. Because we have a lot of shared files on which everyone can be brought in to intervene.	Multiple social media platforms	Teams / SharePoint
So yeah, we're a lot on sharing information and communication.	Social media to help share information	Teams / SharePoint
But the thing is to make it accessible.	Access issues to social media for operators	/
So yes, we use it as a communication tool, via messaging, via what we're doing.	Social media to help share information	Teams
The tool is called HSE Compliance. HSE Compliance, which is provided by RedOnline.	Multiple social media platforms	RedOnline / HSE Compliance
And then, article by article, you come to state on conformity. Conform, non-conform, conform, non-conform. As soon as you have a notion of periodic control ... It also allows you to build a surveillance plan ... and when you have non-conformity, you can also pilot an action plan.	Social media as a tool for digital traceability	HSE Compliance
As a central HSE director, I have a bit of a big brother. I have access to all the sites. I see what they do and what they don't do ... I have access to the dashboard. We can do an extraction. We can do a quarterly, annual report.	Data storage	HSE Compliance
It costs a lot, but it's a great tool.	Economic impact of social media as safety tool	HSE Compliance
I have access to the dashboard. We see a lot of things.	Social media for enhancing visual presentation	HSE Compliance
Given the amount of text today, it's a great tool.	Centralization of the information	HSE Compliance
It's because we used to do that with Excel, but it's the age of stone.	Need for modern digital tools	HSE Compliance
we have a lot of shared files on which everyone can be brought in to intervene ... update, add a data or status on the progress of such or such item.	Centralization of the information / People engagement as safety actor	Teams / SharePoint
you have access to the register ... article by article ... state on conformity ...	Data storage	HSE Compliance
you subscribe to a subscription ... you're going to pay for an annual subscription that gives you access to your text list ...	Prerequisite for social media use	HSE Compliance
There's a dedicated platform ... I've created user profiles ... HSE, maintenance, site management ... and maybe the HR too ... They have their own profiles that have been created on the platform.	Acess issues to social media for operators	hsecompliance.com platform

No, because I go to the site hsecompliance.com. There's a dedicated platform.	Data storage	hsecompliance.com
we trained the managers who cascaded their N-1 ... until we trained 100% of the collaborators in the company ... all this was made completely accessible to everyone via Teams.	Top-down implementation of actions / social media to help share information	Teams
All these media ... the training follow-up file ... the training module ... hot evaluations ... all this was made completely accessible to everyone via Teams.	Use of social media for supporting the training	Teams
We created our own intranet ... which gives you access to ... the group's documentary base ... all these documents ... are accessible on our intranet ... specific HSE tab ... work docs accessible to everyone too.	Centralization of the information / Social media to help share information	SharePoint (intranet)
examples of instruction sheets on machine tools ... control sheet for ladders ... control sheet for lifting trucks ... sites use it ... these docs are available to them ... accessible to everyone.	Data storage / Centralization of the information	SharePoint (intranet)
all these media ... accessible to everyone ... anyone can go there.	Social media allow wide access	SharePoint (intranet) / Teams
I'm creating a Teams channel ... I put all the Comex ... RHs ... HSEs ... site managers ... production managers ... publish photos and videos on this communication channel.	Top-down implementation of actions / social media to help share information	Teams
every day ... you have photos, videos from everywhere ... it gives the impression that it's moving all over the place on all the sites for five days non-stop ... it gives a little depth to the subject.	Continuous flow of information via social media	Teams
I voluntarily put very wide ... all the Comex ... and ... they are more spectators ... but ... non-stop. All the sites balance.	Continuous flow of information via social media	Teams
it's a thing that gives you the impression ... it really gives the impression that it's moving ...	Continuous flow of information via social media	Teams
we went from, I don't know how much, from 1 million to 500,000 euros ... we have drastically reduced the costs related to employee absenteeism	Economic impacts of safty accidents	/
TF2 ... we went from 11.8 at the end of 2019 to 5.5 at the end of October ... the curve ... is just going down ... the indirect cost is three times the direct cost.	Economic impacts of safty accidents	/
the direct cost is concrete ... the indirect cost is three times the direct cost ...	Economic impacts of safty accidents	/
if you do your calculation ... direct cost, multiplied by three ... indirect cost ... more than a million euros ... you can still show that you can save money by doing prevention.	Economic impacts of safty accidents	/

we are on what we call security meetings ... behavioural security ... we inform managers and we ask them to go out and meet people ... benevolent approach ...	Top-down implementation of actions	/
we're dematerializing this support ... filling out this synthesis on the phone, you can immediately share with the head of service concerned, with the HSE or quality ... facilitate the follow-up work.	Fast information / social media to help share information	Smartphone app / digital forms
we're going to try to dematerialize it ... ensure a tracking, a traceability of the information ...	Need for modern digital tools	Smartphone app / audit forms
we're moving from the paper version to online versions on smartphones ...	Need for modern digital tools / Using notebooks to report hazards and suggest improvement	/
Training is the key ... you say, well, you have to do the lock-out, tag-out ... you do it concretely on the machine ... people retain a lot more.	Social media can't replace face to face	Dojo (hands-on training)
I would really like to integrate elements a little more virtual ... you put the headset on the head ... a 4.0 dojo ...	Social media as complement to face to face	VR / virtual elements + dojo
great examples of dojos at Renault ... a real lift truck ... anyone ... climbed on the truck to see all the dead angles ... super interesting.	Motivation & engagement	Dojo (hands-on training)
I do it a lot on LinkedIn ... I often go on YouTube, to look for very concrete videos.	Use of social media for supporting the training	LinkedIn / YouTube
he just showed a video of a truck falling out of a quay ... they signed right away ... social networks are great ... thousands of examples ... it makes it easier to convince.	Use of social media for supporting the training	YouTube
I'm not going to show them a video of a serious accident in the dining room ... It must be in a small circle, animated, discussed ...	Use of social media for supporting the training / Social media as complement to face to face	/
well-targeted during specific training with a time of exchange ... arouse debate ... make the link with our rules in force ...	Use of social media for supporting the training / Social media as complement to face to face	Training sessions + videos
That's it. I have another example in mind ... fire permit training module ... There are very good videos about fire departures ...	Use of social media for supporting the training	Training module + videos
they made a video that will be viewed by all the group's collaborators.	Social media to halp share information	Internal video (Teams/SharePoint)
they didn't have the authorization to put the rights to the image ... It's a mess ... internal viewing ...	People consent for social media use	/
We have nothing to hide in HSE ... if it can be used elsewhere, as much as it serves ...	Mass communication to all staff	/

I went to see him on LinkedIn ... Can we get in touch? ... most HSE have a rather open mind ... there is no competition in HSE.	Prerequisite for social media use	LinkedIn

Table 6: coding matrix for interview P2

Verbatim	Code	Platform (if applicable)
we use different communication mediums, either via the web, we do webinars, technical days, in person or remotely…	Multiple social media platforms	Web; webinars
the poster… remains a tool for communication within the company… through the visual message that they will convey.	Social media for enhancing visual presentation	
we use different communication mediums, either via the web, we do webinars… and… posters…	Multiple social media platforms	Web; webinars
Companies… in the tertiary… with a computer… Communications will be done a lot via the internal network… webinars… information campaigns… Newsletters…	Prerequisite for social media use	Intranet; webinars; newsletters
applications… with a photo of a job situation that may seem dangerous. The employee takes the photo, it is sent to the preventer, to the team leader…	Bottom-up information flow via social media	Internal mobile app (personal phone)
they use applications… to communicate… via the employee's personal phone.	Social media to help share information / social media allow wode access	Internal mobile app (personal phone)
Public networks, Insta, Facebook or others… are not used for companies to speak to their employees.	Work-life boundary erosion	Instagram; Facebook; public networks
it remains a social network, but internal… security talks… a group of employees to discuss a security issue.	Social media to help share information / Social media as internal communication channel	Internal network; safety talks

LinkedIn… groups… rather around an activity… nuclear… electricity… water treatment… groups for company preventers, for security managers… not open to others.	Using different communication methods for managers & operators / Social media as internal communication channel	LinkedIn groups
In terms of security… they are looking for… new ideas, new techniques… participate in salons…	Prerequisite for safety culture	Industry events / salons
Ministry of Labour… an internal collaborative work network… open only to members of the group… TV campaigns, radio campaigns… they communicate via X… Facebook…	Social media as internal communication channel	Internal collaborative network; TV; radio; X; Facebook
they communicate via X, for example… if they have X, they must have Facebook too.	Multiple social media platforms	X; Facebook
Teams… remains a meeting tool… possibly collaborative work… companies like to formalize… program… intervener… duration… training attestation.	Social media to help share information	Teams; webinars
with the application tools… take a photo… inform someone… treatment message… on a phone… on a tablet… management can send communication messages… statistics…	Continuous flow of information via social media	Mobile app; phone; tablet
whatever the tool, the important thing is the message and how it is adapted to the target… the more personalized it is, the more… employees… will feel concerned.	Prerequisite for social media use	

LinkedIn is still a personal account with a professional target. So, my company… communicate with me through LinkedIn, it would bother me… it is a personal account.	Work-life boundary erosion	LinkedIn
social networks… according to their nature, when they are personal, normally the company does not have to communicate through this personal tool… there is a limit to be found…	Work-life boundary erosion	Personal social networks
there are companies that have created accounts asking their employees to subscribe… at the time of COVID… keep in touch… but it remained a voluntary act… not mandatory.	Work-life boundary erosion / Motivation & engagement	Company social accounts (COVID)
social networks… when they are personal… company should not… communicate through this personal tool.	Work-life boundary erosion	Personal social networks
there is a limit to be found… according to the tools, there are things that lend themselves or that do not lend themselves.	Work-life boundary erosion	
we receive the newsletter… and once out of ten, nine out of ten, I don't read it… That's not what will allow me to be alert to prevention…	Prerequisite for social media use	Newsletter
small videos are becoming more and more popular… visual works well… short formats and a bit catchy work well…	Social media for enhancing visual presentation	Short videos (YouTube etc.)
the idea of waking up and prevention is… allow exchange… if it's just information coming down… it's useless.	Social media as complement to face to face	

Yes, it can. But it has to be well targeted… the more personalized it is… the more employees will feel concerned.	Prerequisite for social media use	
Training, or even a webinar with an active chat… we can also mobilize people…	Social media as complement to face to face	Webinar + chat
if it's on personal time… people won't necessarily come… it has to be on time… integrated into their activity.	Prerequisite for social media use	
It's an element to convince. It's part of the toolbox… exchanges, interactions… so that the message really takes hold.	Social media as complement to face to face	Videos (YouTube examples)

Table 7: coding matrix for interview P3

Verbatim	Code	Platform (if applicable)
traditional social networks, typically TikTok, Facebook , etc.	Multiple social media platforms	TikTok / Facebook
it's more difficult to set up for questions, in particular, of private life, etc. And	People consent for social media use / Work-life boundary erosion	/
So, if we go to social networks, you see YouTube is also considered a social network because we can exchange. Well, on the same title, then, we have Teams. Teams is a pure and internal social network. And we can also have our Intranet.	Multiple social media platforms	Youtube / Intranet
our Intranet allows you to just share information, communicate with collaborators.	Social media to help share information / Social media allow wide access / Social media as internal communication channel	Intranet
the problem we have today is that our collaborators in the workshop, who don't have a professional phone, don't have a professional computer, don't have access to information in the same way, at the same time.	Access issues to social media for operators	/
The staff at the workshop, well, you have to make a poster, you have to create it, you have to print it, you have to go and display it. So, it's much longer.	Access issues to social media for operators	/
And the idea was to develop an application.	Need for modern digital tools	/
So, in fact, it's only at the level of managers	Top-down implementation of actions / Using different communication methods for managers & operators	/
It's going to go down to the team leader. And then, you have special collaborators, who are going to be quality, things like that, or logistics, who have a pro phone or a pro computer.	Top-down implementation of actions	/
But a press operator, for example, will not have a pro computer or a pro phone. And they don't have it because there is no utility to what they have. And in addition, since he is focused on his machines, on the management of his production, it would even be... A distraction.	Access issues to social media for operators	/

We could put him in danger. Because if he is distracted, if he is not careful, there can be an accident. And also, in terms of profitability, we are not good.	Economic impact of social media as safety tool	/
Because, as a result, the collaborator is not allowed to use his phone during production hours, but he can take his personal phone during his break. And there, in these cases, he can connect and take some information. Or in the evening, he can always have access to his work application to know what is going to happen tomorrow.	Social media to help share information	/
... Since it's a personal phone use, in relation to security, in a way, when you're a pro, there can't be an exchange. That is to say, it's illegal to exchange information from your pro to other personal phones.	Work-life boundary erosion	/
And in fact, there's this whole notion that has to be taken into account. It's how we're going to manage the fact that, well, suddenly, we authorize... We authorize these applications on personal phones, but it's still pro.	Work-life boundary erosion / People consent for social media use	/
I mean, we don't have a pro email address for workshop collaborators. Because it's a cost, you know. There's a cost just for... But then again, it's a choice. I mean, if we get into this approach, we're going to have to buy these famous addresses,	Economic impact of social media as safety tool	/
And yes, so, precisely as the operators, they don't have access, let's say, to everything that is digital, it's rather the communication that's going to be done, it's rather in terms of posters, workshops, training, etc.	Access issues to social media for operators	/
you structure your newsletter. When you receive emails saying, enjoy this offer, well, in fact, it's often sent in bulk, it's created on a software, and that's a newsletter, in fact, sent in bulk. We don't have that software internally. We're going to do either an email, or we're going to create a little design, yeah, we're going to make a PDF, send it by email. It can be really... Okay. But there are small newsletters on really specific information.	Economic impact of social media as safety tool	/
E-mails are a means of communication, clearly the most used.	Mass communication to all staff	E-mails

, but we used a YouTube link that made ambient music, you see, because we had to make a game with headphones, noise, so we use that. I also use YouTube as a non-repertory link to sometimes post videos to be able to broadcast them afterwards in meetings or typically in workshops last year where I had created specific sounds, I had put them on YouTube as a non-repertory link and then I just had to share this link with people who needed it. We made a video about integration, so yes, we use YouTube but it's controlled, that is to say we give the link, we make sure, that's it, it's not… and on the other hand we have YouTube as an external link too, but overall that's it.	Data storage	Youtube
And you see, on the other hand, there's always, in relation to this security, we had an intervention from a client that during the week of quality, which was last week, yes, because we have a lot of weeks, we made a video, in fact, we made several videos. We made a video where **[the CEO]** was speaking, by the way, a specific video on quality, so we put it on the screens, it's broadcast, in fact, it's shared, there's a link that's on SharePoint and everyone shares it to broadcast it to their teams, that's it, everyone has it on their computer.	Social media allow wide access	/
to share the videos internally, without going through YouTube, to still ensure a maximum, because we never know a maximum of security on these subjects, everything that is client quality, when we go in the production processes, it's quite secret stuff, so there, we avoid everything that is a bit related to the external.	Social media as internal communication channel	Youtube
. So, it's more complicated to get them through because, you see, even with WeTransfer, you have to be careful because there can be a loss of data, you see, normally not, but it's still, you have to, that's it, you have to be very careful about what you share. With WeTransfer, it's a bit more secure, but hey, it's the same. It's never, we never know ,	Sensitive data / Risk of data loss	WeTransfer
to share them with you in all security, without using an external system that can put you a little at risk,	Social media as internal communication channel	
but you see, LinkedIn, we're going to encourage the internet to like, etc. But behind, you're never at risk, you have no control of your communication. You see, it's more that, but we're more in the image, so it doesn't really answer the security part. It	Difficulty to control communication via social media	LinkedIn

In fact, I think that's the real issue today. Everything is digitized and we want to be fast. How do we do to be fast? We go to the workshop, we have a machine problem, we take a picture, we send it, we say, look, I have this on my machine, your team leader, he may be at home because, you know, sometimes compared to the competent person who can answer you, she is elsewhere, you send her a message and then suddenly you have your personal phone, you take a picture, you send it, that's it. It's always this use of the personal tool that comes out, in fact, that comes out of context and, you see, it's often WhatsApp, the teams, but WhatsApp is not professional.	Difficulty to control communication via social media / Fast information / Bottom-up information flow via social media	Teams / WhatsApp
There is no control. We agree. But at the same time, WhatsApp is super practical and everyone has it. So that's a challenge.	Difficulty to control communication via social media	WhatsApp
To create links. To create links. Yes, clearly. To create links. In	Social media as a tool to create connections	/
information a bit instantaneously, on a daily basis, the feeling of belonging.	Fast information	/
Yes, overall, that's it. In the sense of engagement. If you want, engagement, to feel like you belong to the company, when you feel concerned, informed, quickly, not having had a drink in the bar on one side of the company and then, that is to say, learning at the table on the other side, the information, you see, it's still more pleasant. And in fact, often, you get it more quickly through social networks.	Fast information / People engagement as safety actor / Social media as a tool to create connections	/
You see, we were contacted supposedly on Teams precisely by a person who needs help when in fact it was not at all a fake thing. So, to have... or wait, it was an email.	Use of social media for supporting the training	E-mails
maybe social networks can also help in the sense that it's fun, everyone knows, everyone is addicted to that, unfortunately.	Use of social media for supporting the training	/
You see, we laugh, it's still a training where you learn things but it's rather relaxed and good children and suddenly, these trainings, well, behind you share the photo internally, well, it comments and that's where it creates links, that's where it creates memories, that's where you say ah, well, I'm good in this company, it's still nice.	Social media as a tool to create connections / Use of social media for supporting the training	/

And then, I would say a disadvantage is that it's time-consuming, social networks. You see, when you spend time on Teams answering tac, tac, tac, tac, there is no more another question and so on and then, you take time to answer, sometimes a call goes faster. Yes, that is to say that, well, it's more about usage but having a little step back on the use of social networks.	Fast information / Social media as time-consuming	Teams
You see, sometimes, is the request really urgent?	Social media to alert safety incidents	/
Mental health is the issue of this year. I don't know if you heard, but it's really the problem of this year. In any case, they put a lot on it.	Work-life boundary erosion	/
So finally, in the improvement of security, it's reactivity, already, on a social network, since you give the information right away.	Fast information	/
After that, it's true that on the internal, on the internal, we are often a little more limited. So it all depends on the means of the company and the strategy, too, of what we want to invest internally in the company. But there are companies like Airbus, all that, which must be on a level of internal security and different communication compared to us.	Economic impact of social media as safety tool	/
No, but that's it. And see how to re-apply the codes with IA. And you see, because I see IA now, and everywhere.	Need for modern digital tools	AI

Table 8: Coding matrix of P4

Verbatim	Code	Platform (if applicable)
We're going to give a little global information on Teams, but we're going to have the details, and the procedure itself, we're going to have it on the SharePoint dedicated to the dedicated document.	Social media to help share information / Centralization of the information	Teams
And in fact, by using social networks, we're going to better communicate good practices, etc.	Social media to help share information	/
because it's true that on Teams, we may not necessarily have the history of the whole conversation, we can lose track, and really have this community aspect, we can list, do it like a kind of forum,	Social media as a tool to create connections	Teams
Today, we are in a world of more and more connected, we have new collaborators, younger and younger, who will be directly more sensitive to this kind of procedure, so who are really all with a strong digitalization.	Social media for enhancing visual presentation / Need for modern digital tools	/
So social media can be really useful for transmitting brief messages.	Social media for transmitting brief messages	/
I think we will have to have this aspect, so social networks and, because of that, continue to have meetings. I think we have to do more meetings. For those who are a little more interested and who want to ask questions or who want to know more.	Social media as complement to face to face	/
We will show that the management of the company also wants to do that. And not just show that we will have to.	Prerequisite for social media use / Prerequisite for safety culture	/
The main obstacle – from a cybersecurity point of view- is that you want to use social networks that are hosted in another company.	Sensitive data	/
So for me, you have to try to internalize, you have to make a really internal social network.	Prerequisite for social media use	/
It can happen even on the most famous social networks. There are	Sensitive data	/

always leaks, there are even people who can find it. It would just be enough for a malicious person to get access via an internal employee		
And especially if we are talking about a large company, which is mainly a large company that is going to set up a social network, that an SME does not really have an interest in doing it because it can easily make a small internal communication, but for a large company or a large group, in this case, it is subject to attacks.	Prerequisite for social media use	/
I think it can still be a door. But if there is already little critical data that is released on the social network, it can happen, but there will always be a risk.	Sensitive data	/
So tomorrow, there is no more network, and an attack, you can't work. You use Teams, you have to talk to your client, you use SharePoint, etc. That's just an example. But it can be, for example, for the industrial sector, there could be an attack that cuts the power and there is a machine that may not work.	Dependence of social media	Teams
I think it can facilitate in the sense that we manage to set up a regular dissemination. Not necessarily consistent because I think the longer the message is, the more it will be zapped.	Social media to help share information	
Sometimes, even if we organize meetings, e-learning, they won't necessarily follow, we lose the thread. So doing this daily reminder, I think it will still help them.	Social media as complement to face to face / Continuous flow of information via social media	e-learning

Because often people, so professional teams, functional people, they will zap a little for them cyber and IT, when there is a cyber-attack, it affects just these two sectors. While not at all, it will affect everyone. And so, more the involved in it. Because the biggest risk in cyber, ok, there are cyber-attacks, ok, the economy of cybercriminal increases a lot. But the biggest problem is the human risk. That is to say that people are not very sensitive, so the most common attacks, by phishing, by a person who manages to usurp identity, by downloading malware, etc.	People engagement as safety actor	/
But if you can do 15 seconds, 30 seconds, people have to spend as little time as possible. You have to realize that today we are doing more and more training and we see that it doesn't change that much. We see that the human risk is still as high. There is a problem. The message does not pass. I think that doing, especially today, or people, whether they are older or younger, we see that people have more and more a problem with attention. I think you really have to involve them from the beginning and really try to do either a small explanatory video of 30 seconds,	Social media for transmitting brief messages	/
Do it by theme. I think it could be interesting. On this format, yes. But if you just send a video of 5-10 minutes where we explain to you, it's just a political speech, it's not going to interest people.	Social media for transmitting brief messages	/
That's it, that's it. They're going to say, what is CTO telling us again? They're going to say, but it doesn't concern us. Whereas if you take people, I don't know, I think try to make a video and talk about each job.	Social media as a tool to create connections	/

People want to have quick access to things to be able to share documents easily.	Fast information	/
Yes, social networks are a very good way, I think, to do that. To make everyone communicate and make them understand that if there are security rules,	Social media as a tool to create connections	/
The disadvantage is perhaps to have reluctant people to change. Yes, to change, to put in place social networks. There are people who say, I already have enough stuff, I'm bored to be on social networks.	People consent for social media use	/
But if you use it badly, it can just be one more problem and it can even, if you share confidential data, for example, you do it via a social network that is really public,	Sensitive data	/

Table 9: Coding matrix of P5

Verbatim	Code	Platform (if applicable)
So I have WhatsApp, like everyone else. But Instagram, Facebook, my only social network is LinkedIn.	Multiple social media platforms	WhatsApp, Facebook, Instagram, LinkedIn
People see a text. It's very badly written. I eat from it every day. It's very badly written. And again, the labor code, I think it's worse than the environmental code. It's badly written; it's badly explained. People are not trained at all.	Prerequisite for safety culture	
No, but that's the security. So yes, you have to know things. But you don't have to go out of Jupiter's kitchen to do the regulation.	Prerequisite for safety culture	
To do all this on the ground, you have to sensitize people. Okay. But I have a hard time sensitizing employees by telling them that it's good to protect the little birds if they are insecure in their job.	Prerequisite for safety culture	
Objectively, if the question is for me, personally, I save a man before saving the environment, before saving the birds and the environment, that's it.	Prerequisite for safety culture	
The social network, direct proximity, can save lives. Before, there was the bell that rang, people knew they had to flee. Today, we have the fireman's siren, but we also have social networks.	Need for modern digital tools	
At the university, it's not a social network, it's an alert network based on SMS in the event of a terrorist attack.	Social media to alert safety incidents	SM

Tomorrow, there is a factory in Feyzin. First, we'll talk on the radio. I think I have an alert. In the metropolitan area, I think I signed up for the alert via social media. Even if I don't hear the discontinued siren that says it blew up there and I shouldn't go there, I think I'll have it on my phone.	Social media to alert safety information	
having people in a network that can be warned quickly, in the case of Aleppo, it's not bad.	Fast information	
Yes, and especially now, you have to imagine a social network that can be pulsated on others to warn everyone at the same time because no one listens to the same radio anymore.	Social media allow wide access / Mass communication to all staff	
The social network allows you to pulse information very quickly. So that, I think, for a heat alert, it's good.	Fast information / Social media to alert safety incidents	
Indeed, it can shock people when you never know. Once I saw a video of a guy falling off his truck and dying, I think it was a mistake. Some people were really shocked. I had negative feedback.	Risk of shocking on social media	
On the other hand, the social network inside a company can bring up dangerous situations. We always have a problem in a company, because the security culture involves everyone's cooperation.	People consent for social media use / Motivation & engagement	
On the other hand, he has an internal social network.	Social media as internal communication channel	

He has an internal social network that allows him to take a picture. It geolocates, it takes his name. We know who he is. It's anonymous. Well, it's anonymous to others, but we know who set the alarm, when, why. In this case, he doesn't denounce anyone. He takes his picture. Watch out, pole fell, risk of electrocution. I say anything. It's done, it's rolling. There's one up there who gets the alert. He says, wow, he's right, Robert. Thank you, Robert. It allows you to be quick to respond. People will only report if we act on the fact that they reported and we make the modifications afterwards. To have feedback from the field, you always have to put more energy to thank and respond to the field. The field only makes efforts if it's useful and it has the results.	Bottom-up information flow via social media / Fast information / Social media to alert safety incidents	
The social network can be interesting because it generates a possibility of reporting and it also generates a reactivity of response and a possibility of acting that we noted what the person said. It's not so much the fact that it's a social network, it's that it's quick communication, that everything is tracked, that the social networks, the applications allow you to compile the data and process it.	Fast information / Data storage / Social media as a tool for digital traceability	
It allows for shorter processes without going through the hierarchy and without going through the guys who will forget	Bottom-up information flow via social media	

to pass the message. So it's good for reporting and it's good for good ideas.		
It was a different process, you had to make a file, there was a key price, we earned something for ourselves or for the association, for the association, I don't remember. But it could be slow. It could be slow and on paper. Whereas George comes along and says, no, it would be better if we had a piece of paper so that it's faster.	Using notebooks to report hazards and suggest improvement	
And when it has to be fast, the social network, the modern communication of our time is good .	Fast information	
it's made of picking up messages, but above all, listening to the ground. They realize that we're listening to them and so it makes them want to join in. It's just a thing that's quite improving. Very long to build, very quick to put together.	People engagement as safety actor / Motivation & engagement	
Of course, when you're at Hermès, it takes the girls 7 days to sew a bag, and the bag doesn't start at 4,000 euros, and so on. She's proud of her bag, and there's her name on it. A guy who makes a badge of 5,000 pieces per minute, what pride! So there's only security left. The environment can be a good thing. But the culture that is based on bringing money to the shareholder, it doesn't work at all since the 1980s. It's over.	Prerequisite for safety culture	

Yeah, it allows you to make a good link which is a little bit perverted because there is no more pride in being in the same team. So that's for inside the company.	Social media as a tool to create connections	
Precisely in some, you may know it, but in some industries where the operators are on machines, they forbid personal phones. So that they are not distracted. Which is normal.	Access issues to social media for operators	
And in fact, a guy who has his workplace, he doesn't move, he's not the most useful guy in the world. In terms of security, what is interesting, it's the security guard who moves, who sees a lot of things. And the maintenance guy, who moves and sees a lot of things. So no, but you have to cut this conflict between no social network, no disturbance, and social networks to report.	Prerequisite for safety culture / Prerequisite for social media use	
So the social network is a bit of a solitary thing. It allows you to do that, except to come across teams, but there it's collaborative, it's not even a social network, it's a network that allows... So what's good here is that it can cause people who are very far from each other and who have the same problems.	Social media as a tool to create connections	
They have a kind of application where the guys write in real time	Fast information	
for a team leader, when he has large construction sites, to know that these guys have entered on such a perimeter. So it allows him to know that you don't have to go	Social media to help share information / Bottom-up information flow via social media	

Everything goes through social networks. The most stupid messages, the most intelligent messages. I don't know if... I think that's it. It's pretty bad. When you don't know who's talking to you, I prefer to go see people.	Difficulty top control communication via social media	
It allows you to put them in contact even if we are far away, even if there is COVID. It's good.	Social media as a tool to create connections	
As soon as you have information circulating somewhere, there is a risk. I think it's easier to do it on the ground.	Sensitive data	
It's done. It's a social network. It's Power BI for numbers. It's Teams for ... It's their social network.	Using different communication methods for managers & operators	
It can be used for something; it becomes a tool. If it's just for everyone to exchange things on everything and anything, it's not for us, it's a product. It's useless, except to mess up people's heads.	Prerequisite for social media use	
Once again, you need neurons behind. It's not LinkedIn that makes your intelligence. It's you who have the intelligence to use it properly. We're still in this. You have to take control.	Prerequisite for social media use	
Imagine. Before, if **[name of an oil plant]** was doing an exhibition, there was a guy in the street with his drum saying alert, alert, alert. We made the bells ring because the wolves were coming to Paris or the Germans. Obviously, progress is undeniable.	Need for modern digital tools	

Table 10: Coding matrix of P6

Verbatim	Code	Platforms (if applicable)
Teams, Outlook, everything that is, I don't know if we call it the Microsoft suite, SharePoint, because it's a place to share docs, at work, and then sometimes there are what are called management jets [EDM], I don't know what, documents, electronic documents, which are platforms,	Multiple social media platforms	Teams, Sharepoint, Microsoft suite, EDM
There is a security controller called a CSPS, which is in charge of the physical security issues of the people who work on the site, and who establishes reports each time.	Prerequisite for safety culture	
Yes, they are transmitted by email and deposited on a [EDM] when it is available.	Centralization of the information	EDM
After the posters are always present, I can't say if they are mandatory or not. But on all the sites, I think they are mandatory. So you have a display panel at the entrance saying, wear mandatory safety equipment, so safety boots, helmet, vest	Prerequisite for safety culture	
the security of the sites is different depending on the site, even if the regulations are the same.	Prerequisite for safety culture	
I have the impression that it is rather the displays that have become a complement, in the sense that these displays, if they are removed, the impact is minimal, even non-existent, because no one pays attention to it.	Prerequisite for safety culture	
once a month or Monday morning, a security session with their workers. But it does not fall within the framework of the social network, since it is live.	Social media can't replace certain actions / things	

that it is more a question of communication to others, that sometimes there are publications on LinkedIn, saying point security with our workers this morning,	Mass communication to all staff	
We are sure to reach the target,	Social media to help share information	
There is the advantage of monitoring too. We know what information was transmitted at what time.	Fast information / Social media as a tool for digital traceability	
The only limit, which is not really one, is that this transmission is not done to all the people who intervene on the site, but to the managers of each company, and they then have the duty to pass it on to their workers.	Using different communication methods for managers and operators	
from the moment a person's life is in danger, or even their physical health, inevitably there is a certain commitment.	Prerequisite for safety culture	
So in a way, it promotes commitment, but it's not the thing that will make us commit.	Motivation & engagement	
Yes, this kind of video exists, but it's really the big companies that do it, that organize it, either to show them within their internal training, or in the case of communication on social networks to show that the question of security is an important issue for the company.	Use of social media for supporting trainings / Mass communication to all staff	
you know a little bit about the values or the directions, the objectives, etc. of a company. And the fact of having in mind that security is an important question, yes.	Motivation & engagement	

Yes, for example, when there is a team working on a competition, so there are between the different actors, there are documents related to the offer that will be proposed. And inevitably, when there are competitors who are working on the same competition, there is this risk there.	Sensitive data	
The risk is rather inside, in order to be careful that a person does not share them, because they have an interest in giving these documents to another company, or to give information on the offer that is being proposed to a competitor.	Social media allow wide access / Sensitive data	
it's sharing documents between different actors who are on an operation.	Social media to help share information	
Sharepoint, EDM…	Multiple social media platforms	Sharepoint, EDM
I want to say yes. It's a bit like the definition of... In the definition of the social network, there is this story of links.	Social media as a tool to create connections	
I would rather say that these social networks don't promote the link between a manager and an operator because there is nothing better than a direct contact to promote relationships.	Social media as complement to face to face	

In the sense that in a construction site, there are always electrical and heating installations, etc. It's very specific to the field of construction. There are fire regulations, the walls must be cut to a certain degree, etc. At that time, it's another person, what is called a control office, who comes to look at the technical equipment to be installed, and at the same time make reports to say that something is poorly installed.	Prerequisite for safety culture	
social networks are a tool for the transmission of information, in general	Social media to help share information	
And then it can be very short because it's rather something urgent in the sense that the firefighter's access road is blocked by someone who parked his car there.	Social media for transmitting brief messages	

Table 11: Coding matrix of P7

V / Discussion of the results

This section aims to analyse the results presented in the previous section. While the codes have been presented, it is necessary to group them into themes and analyse them, as mentioned in the methodology section (thematic analysis method). Firstly, the analyse of each theme will be presented. Then the methodological limitations that may have influenced these results will be discussed, in order to ensure transparency.

Following the coding of the data gleaned from the interviews (Cf. section IV, Results), six distinct themes emerged. The tab presenting an overview of the themes and codes includes in each of them is presented bellow (Cf. Table 12). As a reminder, my two research questions guiding my thesis work are as follow:

RQ 1: What are the positive and negative impacts of social media on security culture within industrial organizations and companies?

RQ 2: What are the possible applications of social media in order to enhance safety culture within industrial organizations and companies?

Theme	Codes	Research question coverage
1 – Social media a tool for rapid and wide dissemination of safety information	• Fast information • Continuous flow of information via social media • Mass communication to all staff • Social media allows wide access • Multiple social media platforms • Social media as internal communication channel • Social media for transmitting brief messages	• RQ1: positive impacts • RQ2: Applications
2 – Social media as operational support for safety management and prevention	• Social media to alert safety incidents • Social media to help share information • Social media for enhancing visual presentation • Use of social media for supporting safety trainings • Social media as a tool for digital traceability • Data storage • Centralization of the information	RQ2: social media as tool for safety culture
3 – Complementarity and limits of social media compared to traditional safety tools / methods	• Social media can't replace face to face • Face to face communication from management • Social media as complement to face to face • Social media can't replace certain actions / things	• RQ1: social media limitations • RQ2: social media as a complementarity tool to traditional safety methods

	• Using notebooks to report hazard and suggest improvement	
4 – Actor engagement and participatory dynamics in safety culture	• People engagement as safety actor • Motivation & engagement • Bottom-up information flow via social media • Top-down implementation of actions • Social media as a tool to create connections	RQ1: positive impact of social media on people engagement
5 – Organizational, cultural, ethical conditions and challenges for social media use in safety	• Prerequisite for safety culture • Prerequisite for social media use • Economic impact of social media as safety tool • People consent for social media use • Need for modern digital tools • Using different communication methods for managers & operators • Access issues to social media for operators • Economic impacts of safety accidents	• RQ1: conditional impacts • RQ2: necessary conditions
6 – Risks, limitations and negative impacts associated with social media	• Sensitive data • Risk of data loss • Difficulty to control communication via social media • Work-life boundary erosion • Social media as time-consuming • Dependence of social media • Risk of shocking in social media	RQ1: negative impacts

Table 12: Overview of the themes, codes and research question coverage

Analyse of the first theme: social media, a tool for rapid and wide dissemination of safety information

The first theme is titled: **Social media, a tool for rapid and wide dissemination of safety information**. This theme includes the codes presented below (Cf. Figure 14). It partially addresses both research questions in the following aspects:

- RQ1: The positive impacts of social media on safety culture (speed, broad dissemination, etc.)
- RQ2: The possible applications of social media as a communication tool in service of safety.

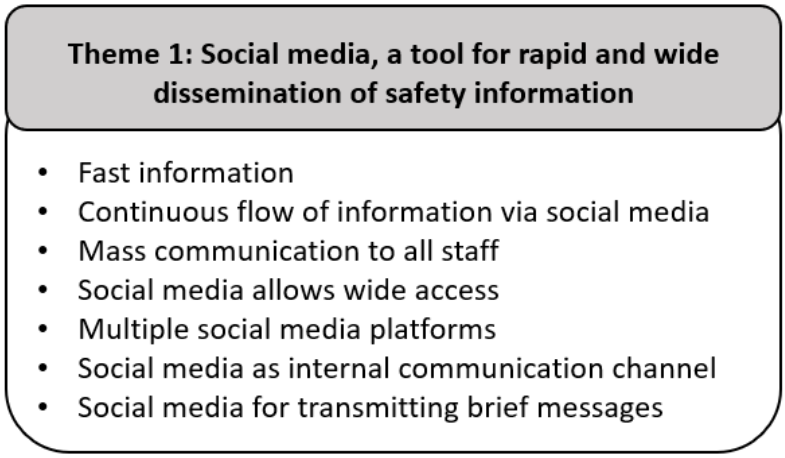

Figure 14: Presentation of theme 1

Definition of Theme 1: This theme highlights the relevance of social media applied as a communication tool for safety culture, through two fundamental dimensions: spatiality and temporality.

Analyse of the theme

This theme emphasizes two fundamental dimensions. On one hand, the temporal aspect, as social media are presented as tools to accelerate corporate communication regarding safety. On the other hand, the spatial aspect, as the capacity of social media to widely disseminate information was raised by participants.

On one hand, the interviewees unanimously recognized the ability of social media (Teams, WhatsApp, LinkedIn, etc.) to transmit information quickly, as the code "Fast information" appears in all the interviews conducted. Indeed, in the context of this work, social media are defined as internet-connected resources that facilitate collaboration among individuals, which is the broadest definition found in the literature (see methodology section). Being internet-connected, these tools are highly effective for almost instantaneous communication, which stands in stark contrast to the traditional tools and methods used in safety culture, as revealed by the interview analysis. As discussed in the literature review section, these methods and tools (in-person meetings, notice boards, handwritten notes and memos, etc.) also allow for the dissemination and communication of safety-related information, but at a slower pace than social media. For safety topics, the rapid transmission of information is an important element highlighted by the participants, as suggested by the following verbatim: ***"The social network allows you to pulse information very quickly. So that, I think, for a heat alert, it's good."*** – extracted from the P6 interview. Thus, it is suggested that the ability to circulate information quickly (such as an alert) is an important lever in improving safety culture, particularly in critical situations, as mentioned in the cited verbatim. These critical situations are especially likely to

occur in highly interactive systems (see literature review – Perrow's matrix), where implementing preventive policies is challenging, and curative policies must instead be established. As shown by the previous verbatim, social media have the capacity to be relevant in deploying curative solutions (post-accident) by sounding alerts rapidly. This aspect of speed is likely reinforced by the fact that social media generate significant information flows, which are well-suited to effectively transmitting brief messages, often safety instructions and rules, as indicated by the analysis of the interviews. However, this constant flow of rapid information may lead to the trivialization of safety alerts transmitted through these communication channels, which can be problematic for managing priorities and risks, as well as generating fatigue and burnout due to the omnipresence of information. Thus, this phenomenon can be interpreted as a side effect with strong counterproductive outcomes, creating new vulnerabilities. In this sense, (Fu et al. 2020) have shown that the influx of information can lead to user fatigue. It can be assumed that this fatigue may impact individuals' adherence to safety culture policies.

On the other hand, participants generally acknowledged the relevance of social media for widespread information dissemination, as shown in this verbatim from the interview with P6: ***"Yes, and especially now, you have to imagine a social network that can be pulsated on others to warn everyone at the same time because no one listens to the same radio anymore."*** Participants suggested that this broad dissemination of information helps better engage individuals by keeping them regularly informed and fostering accountability, which is a fundamental element of safety culture. Indeed, the highest level of maturity in an organization's safety culture, according to Bradley (see literature review, Bradley Curve), emphasizes interdependence and collaboration among individuals. This aspect of collaboration, with the goal of achieving unity, appears to be facilitated by social media based on the interviews I conducted. By broadcasting a message to all teams, social media seem to be a highly effective tool for involving individuals. The interview analysis highlights the spatial dimension of social media, which is one of the two dimensions of this theme. This mass dissemination of information prompts a revaluation of the spatial dynamics within professional organizations, especially for multi-site companies and organizations. Thus, it is suggested that social media are highly important and effective for safety culture, as they enable the alerting of managers, HSE directors, firefighters, and others, as emphasized in the interviews. Moreover, the code "continuous flow" shows that social media serve as a means to keep safety highly visible as a topic, thereby fostering engagement, participation, and the role of everyone as safety actors. However, as highlighted regarding the temporal aspect, concerns arise about fatigue and burnout related to this continuous flow of information and its mass dissemination. This potential downside could be mitigated through effective, relevant, and targeted communication. Indeed, overly broad and poorly targeted dissemination may prove counterproductive, inefficient, and lead to diminished adherence to the implemented safety policies due to weariness.

Moreover, participants particularly emphasized the dimension of speed, which is not explicitly named in the definition I used, nor in others proposed in the literature to define social media (see the literature review section). The same applies to the spatial aspect, as social media are capable of disseminating information very widely, reducing distances between individuals. These two dimensions are largely highlighted as predominant by participants for acting quickly on safety issues, which require high responsiveness and resource mobilization—aspects that social media can effectively address according to participants. It can be argued that this mass communication enables better implementation of the KPIs discussed in the literature review section. Indeed, KPIs require substantial inputs, which may come from various company sites or departments, thereby facilitating both phase 3, "data collection" (see literature review section), and phase 6, "communication of the results." Social media can thus help centralize this data, allowing for better communication of safety-related information. It is worth noting,

however, that social media are cited as tools in service of a broader safety policy and cannot, on their own, create a comprehensive safety culture.

In summary, this first theme shows that social media are perceived as relevant tools for safety culture, as they support rapid exchanges and reduce the distance between actors within the organization. However, counterproductive effects can arise, such as the trivialization of messages due to an overly abundant and poorly targeted flow of information, which may lead to reduced engagement among individuals.

Analyse of the second theme: social media as operational support for safety management and prevention

The second theme of my work is titled: **Social media as operational support for safety management and prevention**. This theme includes the codes presented in the figure below (Cf. Figure 15). It partially addresses research question RQ2 by demonstrating social media as a tool that facilitates the structuring of safety culture.

Figure 15: Presentation of theme 2

Definition of Theme 2: This theme discusses social media as an organizational tool that facilitates the structuring of safety culture. It addresses social media as an organizational instrument in service of safety culture.

Analyse of the theme

This section is divided into three axes: (i) social media as a tool for reacting to an accident, (ii) social media as an infrastructure for tracking safety information, and (iii) social media as a tool for preventing future risks. Thus, this division proposes a process-oriented view of safety through social media, derived from the analysis of the interviews.

First, the interviews suggest that social media serve as a tool for responding to an accident, particularly for structuring the accident response. In this regard, social media are perceived as coordination mechanisms that facilitate the coordination of the response following an incident. Initially, social media enable the reporting of the issue through an alert, which can take various forms depending on the situation and the company's organization (automated message, instant message, alert, etc.). This idea is perfectly summarized by a verbatim from the interview with P6***: " […] there is a factory in Feyzin. I have an alert. In the metropolitan area, I signed up for the alert via social media. Even if I don't hear***

the discontinued siren that says it blew up there and I shouldn't go there, I'll have it on my phone." This initial alert, facilitated by social media, is crucial as it initiates a chain of responsibility and response to the accident. Once this alert is activated, social media subsequently allow for real-time exchanges among different stakeholders. Thus, various roles within the company (managers, workers, HSE personnel, etc.) can effectively structure their response to an accident by receiving feedback from individuals affected by the incident and those within the previously mentioned responsibility chain. Through these exchanges, the different roles can coordinate, even via informal communication, as it still helps structure and coordinate the response. Indeed, individuals with a good level of information can act accordingly in a coordinated manner. In this logic, social media support curative actions (post-accident) by enabling alerts and subsequently structuring the response to the accident. However, it can be suggested that the effectiveness of social media in this aspect depends on two key elements and prerequisites. The first is the prior definition of a clear organization and process for accident response. Defining this strategy is essential to trigger the appropriate processes: Who triggers the alert? Through which channel? With what level of priority? The answers to these questions must be established in advance; otherwise, social media cannot initiate the chain of responsibility as previously discussed. The second essential prerequisite, in my view, lies in the quality of the information distributed. Incomplete, imprecise, or poorly contextualized information can directly impact the coordination of the response, for example, by influencing the decision-making of various actors in the responsibility chain. Thus, these prerequisites are essential conditions for enabling social media to become useful tools within a clear organizational process.

Secondly, social media enable the traceability of safety information. Indeed, several verbatims pointing in this direction were coded under "use of social media as a tool for digital traceability." The interviews highlight the utility of social media in this regard, as they are capable of storing data (messages, photos, etc.). Platforms such as Teams or WhatsApp are cited in the interviews as facilitators for circulating this information. Thus, safety is no longer merely experienced but also documented, transitioning from informal traceability (handwritten notes, oral exchanges via traditional methods, etc.) to a documented and tracked safety system facilitated by centralized data. Through this traceability, social media contribute to institutionalizing safety by enabling the tracking and formalization of safety events and incidents. It can be assumed that this traceability allows for the better construction of KPIs (see literature review section). Indeed, this centralization of data and events can be transformed into KPIs. For example, social media can track the time an alert was issued, the time of the first response, etc. Thus, in this scenario, it is plausible to develop an indicator measuring the operational responsiveness of teams. Furthermore, it can be assumed that this information traceability reinforces collective responsibility, which is crucial following the activation of the responsibility chain, as previously discussed. This idea is supported by several verbatims, one of which from the interview with P1 states: ***"Once he's mentally conditioned … then indeed it allows keeping traces, storing, sorting, tracking."*** Participant P1 explains that individuals with roles in the responsibility chain are, by nature, prepared to be questioned by their superiors about the circumstances of the incident, the response to it, etc. This information is tracked, documented, and centralized through social media, which allows for the verification of the authenticity of individuals' statements, as indicated by the interview analysis. Thus, social media help bring to life a process comprised of strict procedures by stimulating interactions among stakeholders and thereby facilitating the adoption of safety culture.

Finally, this theme encompasses a third aspect: risk prevention through social media. As previously discussed, social media enable the tracking of information, which can subsequently be leveraged for prevention purposes. The interviews revealed that videos, messages transmitted via social media during incidents can be repurposed for preventive measures in response to an accident. These messages, videos, and all tracked information serve two key functions: firstly, they facilitate the analysis

of operational implementation and prompt reflection on the effectiveness of organizational processes established for accident response. Secondly, the interview analysis indicates that this information enables the presentation of visual formats to capitalize on accident lessons learned. Indeed, participants highlighted the utility of social media in this context, as illustrated by the following verbatim from the interview with P3: ***"But short videos are becoming more and more popular because people are generally less readers. So the visual works well, and short formats and a bit catchy work well, even if it brings additional information."*** Thus, the interviews emphasize that such video content captured via social media can be effectively repurposed for prevention efforts, for instance by disseminating impactful visual formats on screens in common areas.

In summary, social media can facilitate and structure the response to an accident. Indeed, the three dimensions previously discussed follow a logical progression in accident response: (i) the reaction to an accident, (ii) the structuring of the response and the traceability of safety information, and (iii) preventing future risks by learning from this accident. Consequently, social media are approached as an organizational tool. It should be noted, however, that as a tool, social media aim to facilitate and animate an already established process and therefore cannot, on their own, address safety challenges. Social media thus serve as a support for an organizational process, making its implementation more efficient.

Analyse of the third theme: complementarity and limits of social media compared to traditional safety tools / methods

The third theme is titled: **Complementarity and Limits of Social Media Compared to Traditional Safety Tools / Methods**. This theme includes the codes presented below (Cf. Figure 16). It partially addresses both research questions in the following aspects:

- RQ1: The limited impacts of social media on safety culture.
- RQ2**:** An application of social media as a tool complementary to traditional methods and tools in safety culture.

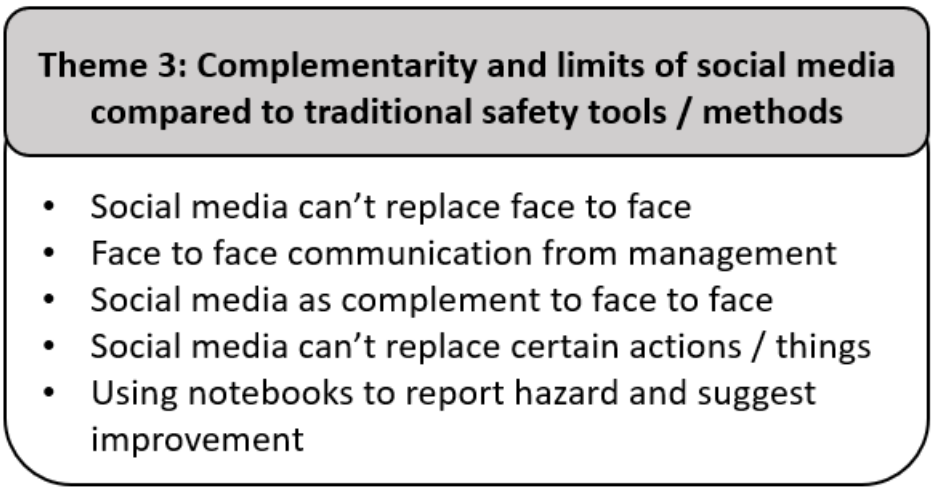

Figure 16: Presentation of theme 3

Definition of the theme 3: This theme explores the complementary roles of social media alongside traditional safety methods. Traditional safety tools and methods refer to those presented in the literature review (cf. Table 2): in-person meetings, posters, signage, in-person training, bulletins/memos or handwritten notes, as well as toolbox meetings.

Analyse of the theme

This section addresses two distinct areas: (i) "Physical" interactions are irreplaceable for ensuring a strong safety culture, and (ii) Social media as complementary (but not substitutable) tools to traditional safety methods

First, the analysis of the interviews shows that face-to-face physical interactions are highly valued, as demonstrated by verbatims coded under "social media can't replace face to face" and "face to face communication from management." On one hand, the interviews suggest that these in-person meetings (a traditional safety tool—see Theme 3 definition) are necessary for safety culture to conduct prevention, training, or inspection activities. Indeed, participants recognize that direct human exchanges foster greater engagement by enabling better detection of verbal cues among actors, thus promoting more effective safety communication. In this regard, existing literature indicates that individuals' satisfaction levels are higher with direct, in-person communication compared to digital tools. For instance, (Tkalac Verčič et Verčič 2025) also shows that in-person interactions make non-verbal signals more accessible and strengthen social presence, which enhances participant engagement. This study thus confirms the participants' perceptions. Participation among stakeholders is also higher in in-person meetings, as emphasized in the interviews. On the other hand, the digitalization of companies and organizations tends to reduce direct or real exchanges, as practices like video conferences have become widespread even in small to medium-sized organizations. Social media, in this sense, contribute to the digitalization of relationships and may increase the distance between individuals. The interview analysis indicates that these exchanges are crucial for building a strong team identity and spirit within safety culture. This notion of exchanges and the distance between managerial functions (who implement safety policies) and operational functions (who execute a large portion of safety rules and policies) is a key factor in fostering genuine trust. The following verbatim from the interview with P7 precisely aligns with this view***: "I would rather say that these social networks don't promote the link between a manager and an operator because there is nothing better than direct contact to promote relationships."*** The interview analysis further reveals that individuals feel more considered, heard, and respected when safety training and prevention rules are explained in person rather than through media like social media. These elements are prerequisites for a collective to function as a cohesive team. This concept of an organized collective is significant, as it corresponds to the fourth and final level of the Bradley Curve, which aims for every actor to operate interdependently as a single team (see literature review). Additionally, these traditional formats, tools, and methods help avoid excluding individuals who are uncomfortable with digital tools or social media, which could otherwise be counterproductive for safety culture. Similarly, safety policies already impose significant constraints on individuals, which can itself be a source of resistance to change. Thus, it can be assumed that implementing new safety policies alongside the rollout of new digital tools may amplify this resistance to change and ultimately challenge the organization's existing safety culture. Safety culture can only materialize if it remains accessible and understandable to all, which may not be the case for operational roles such as workers if social media are used as the primary communication channel. Moreover, it appears that social media do not enable managers to engage directly with the field, thus limiting their ability to confront and adjust safety policies based on on-the-ground constraints and needs. As previously discussed, in-person meetings or discussions foster exchanges and can facilitate the adaptation of safety policies to field realities. This direct engagement is more challenging through social media, which inherently limits managerial presence and interaction in the field.

Moreover, although social media cannot replace traditional safety methods, they can serve as complementary tools, in function more than in medium. Indeed, traditional safety methods (meetings,

in-person training, posters, signage, handwritten logbooks, etc.) are effective in structuring safety culture. The analysis of the interviews shows that these methods provide strong, scheduled, and periodic events that are effective for building a robust safety culture. Social media, in turn, serve as complementary tools to these methods, as illustrated by this verbatim from the interview with P1: ***"So it's really a combination of both. In person, or Teams. It's a way to make safety part of everyday life, not just about following procedures and traditional methods."*** In this sense, the interview analysis indicates that social media ensure the continuity of safety culture, complementing traditional methods that structure safety culture in a periodic manner. It was suggested that social media sustain these key moments through reminders and the ongoing dissemination of lessons learned outside of in-person meetings, thereby enabling real-time adjustments to safety policies. Thus, social media extend already established routines, which has a positive impact on safety, as explained in the interviews. To summarize, the Table 13 synthesizes the temporal and symbolic dimensions that justify the complementarity between traditional methods and social media, as derived from the interview analysis:

	Temporal Complementarity	**Symbolic Complementarity**
Traditional methods	Occasional and static actions (posters, signage, in-person meetings...)	Better embody safety policies and build trust among all stakeholders
Social media	Continuity of actions, real-time follow-up, reminders...	Relays messages through repetition

Table 13: Complementarity between traditional methods & social media

In summary, social media are tools that complement traditional methods. Indeed, the latter are effective and necessary for a strong safety culture, fostering trust-based relationships among stakeholders. These in-person methods carry strong symbolic value, serving as a time for exchange and connection between managers and operators. Social media extend these key moments by ensuring the continuity of exchanges and lessons learned. It should be noted, however, that implementing these social media tools can increase resistance to change among individuals who are not comfortable with them, which may be counterproductive for the operational application of safety policies within organizations.

Analyse of the fourth theme: Actor, engagement and participatory dynamics in safety culture

The fourth theme is titled: **Actor Engagement and Participatory Dynamics in Safety Culture**. This theme groups the codes presented below (Cf. Figure 17). It partially answers the first research question (RQ1) by analysing the impacts of social media on individuals' engagement in favour of safety culture.

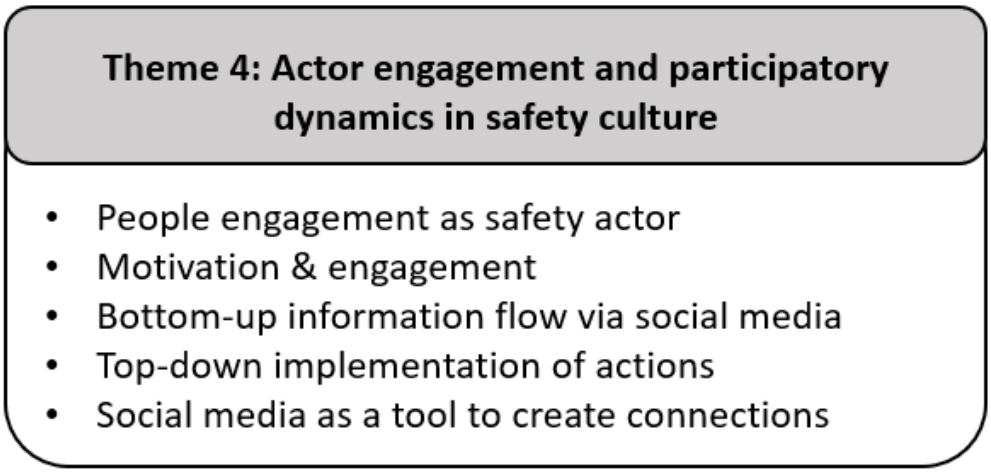

Figure 17: Presentation of theme 4

Definition of Theme 4: This theme discusses the various relational dynamics facilitated by the implementation of social media in the service of safety.

Analyse of the theme

This section addresses two distinct areas: (i) Social media as a driver of collective engagement, and (ii) An examination of the relational dynamics that social media enable within safety culture.

Firstly, social media help stimulate collective engagement among individuals in matters of safety. Indeed, the analysis of the interviews shows that social media are tools that provide a greater space for expression than traditional methods for operators, as anonymity is guaranteed, allowing anyone to report problems, accidents, hazardous situations, or poor practices. These reports enable managers to draft lessons learned and thus adjust safety policies more quickly than with traditional methods, as evidenced by the interview analysis. Traditional methods like handwritten logbooks are less effective than social media in stimulating stakeholder engagement. In fact, a social media platform (WhatsApp, Teams, internal platform, etc.) used within an organization is perceived as less restrictive than a handwritten logbook for operators to make suggestions. Suggestion boxes in factories are placed in specific locations, which can make access difficult for operators not nearby. Moreover, social media facilitate interactions between people, as they can respond to and enrich others' messages or follow up if the transmitted information is unclear, making interaction simpler than in logbooks. Consequently, social media help reduce isolation and improve information sharing, which is crucial for safety. Beyond hazardous and problematic situations, the analysis of the interviews indicates that social media enable the sharing of best practices among individuals. For instance, an operator can take a short video showing a specific situation and share it on the company's internal social media, thereby bringing safety culture to life. Thus, social media are tools that facilitate the collective ownership of safety, making it a shared, dynamic topic rather than merely institutional through rules, by engaging people. This notion of collectivity is explained by the verbatim from the interview with P6: ***"Yeah, it [social media] allows you to make a good link which is a little bit perverted because there is no more pride in being in the same team. So that's for inside the company."*** This highlights the key difference between formal safety (rules, policies, theory, etc.) and safety culture, which is intended to be dynamic, shaped by habits, implicit norms, and collective representations, as explained by (Guldenmund 2000). Through this engagement, individuals within the organization develop a stronger sense of belonging, as safety culture becomes a collective and shared value. However, this engagement in favour of safety culture may be diminished for individuals uncomfortable with using social media, raising once again the question of inclusivity.

Beyond interactional aspects, the interview analysis shows that social media facilitate the creation of dynamic relationships. Indeed, the formal and traditional view of safety is based on rules primarily coming from managers and directors, applied by operators and operational functions. These tools create an interface between managers and operators, thereby facilitating dynamics. Information is no longer solely top-down but also bottom-up, as operators can provide feedback. Although traditional safety methods like handwritten logbooks offer this capability, social media are perceived as facilitators between different functions. This analysis is confirmed by the following verbatim from the interview with P6: ***"It [social media] allows for shorter processes without going through the hierarchy and without going through the guys who will forget to pass the message. So it's good for reporting and it's good for good ideas."*** However, while social media promote participation and interaction dynamics between managerial and operational functions, this can have a side effect: frustration. It can be assumed that frustration may arise because individuals are facilitated in reporting information but rarely have control over decisions to resolve these issues, even though operational functions are best positioned to have rapid and accurate information since they are on the ground. However, this side effect is not intrinsically linked to social media but rather to the definition of the chain of responsibility during critical incidents, for example, where operational functions are often confined to alerting roles rather than mitigating problems.

In summary, social media are tools that facilitate interactional dynamics among individuals in the safety responsibility chain. As a result, safety culture is strengthened, as it becomes lived and reinforced by both bottom-up and top-down communication facilitated by social media. Indeed, traditional safety methods primarily emphasize top-down information flow: from the institution or manager to operational functions. Thus, social media facilitate upward flow, enabling more relevant adjustments to implemented safety policies, as well as governance and decision-making in safety processes, which are prerequisites for establishing a strong culture in this area.

Analyse of the fifth theme: Organizational, cultural, ethical conditions and challenges for social media use in safety

The fifth theme is called: **Organizational, cultural, ethical conditions and challenges for social media use in safety**. It groups the codes presented below (cf. Figure 18). This theme helps to partially answer both research questions (RQ1 and RQ2), by addressing the following aspects:

- RQ1: organizational impacts of social media as safety tool
- RQ2: necessary conditions to use social media as safety tool.

Figure 18: Presentation of theme 5

Definition of theme 5: This theme discusses the prerequisites and conditions necessary for implementing social media in the service of safety. These prerequisites can be organizational, economic, or related to user acceptance. It is intentionally transversal, as it analyses the conditions for deploying social media for safety within organizations.

Analyse of the theme

This section addresses two distinct areas: (i) Economic prerequisites for implementing social media as safety tools, and (ii) Organizational prerequisites. The theme highlights a dissonance between companies' strong desire to enhance safety culture through digital tools like social media and the economic and organizational constraints they face.

First, the interview analysis reveals various prerequisites for deploying social media as useful safety tools in organizations. One initial prerequisite concerns the economic investment required for social media, as emphasized in the interviews. Indeed, as discussed in the literature review, companies no longer view safety policies solely as expenses but also as a means to achieve savings (see literature review and introduction – (Naji et al. 2022)). It was not possible to quantify the exact costs of implementing social media through these interviews, as too many parameters influence implementation costs, making generalization difficult. However, social media are not exempt from the cost–benefit trade-off in economic terms. The following verbatim from the interview with P2 provides context on this cost consideration: ***"The direct cost is concrete, the indirect cost is three times the direct cost."*** The interview analysis highlights various direct and indirect costs associated with implementing social media as safety tools in organizations. Direct costs are predictable and include expenses such as software licenses (Teams, collaborative HSE platforms, etc.), purchase and deployment of dedicated hardware (phones, computers, etc.), initial training time on the tools, and IT security measures (cybersecurity, access management, etc.). Indirect costs are more difficult to predict and typically amount to three times the investment in direct costs (see previous verbatim). The analysis shows that these indirect costs are primarily organizational in nature. Thus, beyond economic prerequisites, another key factor is the organizational cost of implementing these tools.

Indeed, these organizational prerequisites also entail economic and human costs, classified as indirect costs. The analysis indicates that indirect costs may stem from additional workload for existing teams or from providing IT equipment to access social media. Participants explained that in production workshops, workers often lack access to computers or phones, as reflected in the code "Access issue to social media for operators." The analysis also suggests that this lack of access can be counterproductive, as workers should not be distracted by notifications or messages while operating production machinery that requires concentration. However, this observation should be nuanced, as access varies significantly depending on company size, as illustrated by the following verbatim from the interview with P1: ***"In big groups, operators have access to computers … otherwise no."*** The interview analysis also underscores the importance of differentiating communication methods based on an individual's role (e.g., managers vs. workers). For operators, social media can become an additional source of resistance to change, a significant factor when implementing safety policies. Moreover, the deployment of social media can be perceived as a means to monitor individuals' actions, particularly those of operators and operational staff. This perception can severely undermine safety culture. This raises the question of equality of access to safety culture, depending on the company's values—a potentially problematic issue for personnel.

In summary, while social media offer promising advantages for safety culture (see previous themes), certain prerequisites are essential for their implementation. These tools are subject to a cost–benefit trade-off, both economically and in human terms. The mobilization of these resources is heavily dependent on a company's size and resources, as shown by the interview analysis. These costs represent a significant barrier for smaller companies, which may lack the capacity to mobilize such resources.

Analyse of the sixth theme: Risks, limitations and negative impacts associated with social media

The sixth theme is titled: **Risks, Limitations, and Negative Impacts Associated with Social Media.** This theme analyses the vulnerabilities, negative effects, and tensions that can arise from the use of social media, which may consequently be counterproductive for safety culture. This analysis partially addresses the first research question, RQ1, by detailing the negative impacts of social media.

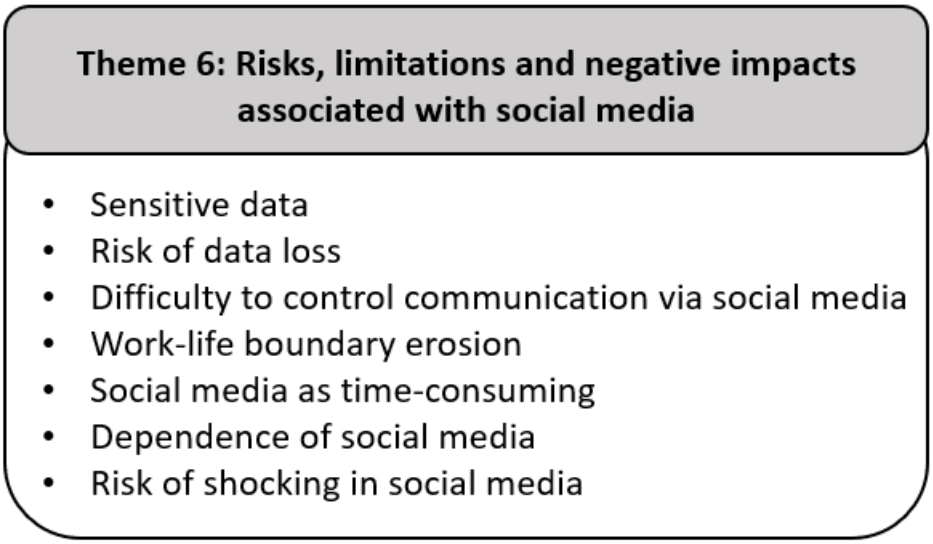

Figure 19: Presentation of theme 6

Definition of Theme 6**:** This theme addresses the risks and limitations associated with implementing social media to serve safety culture. To this end, it is divided into distinct dimensions: (i) informational risks (loss of control and sensitive data), (ii) workload overload, and (iii) emotional exposure and psychological risks.

First, issues intrinsically linked to social media were raised during the interviews. Indeed, the analysis shows that loss of control over published content is an inherent problem with social media. As discussed in depth in previous themes, social media enable broad and rapid dissemination, which can also be negative, as they can facilitate the spread of messages or videos showing poor safety practices. While participants stated this can be corrected with communication, very rapid dissemination can have significant safety consequences, requiring substantial attention. Thus, contradictory messages or the spread of bad practices can create interference with good practices, increasing the risk of poor behaviors or postures. Furthermore, participants perceive social media as facilitators of risks of confidential information leaks, as shown by the following quote from the interview with P1: ***"So WhatsApp, messages are encrypted if I understood correctly … once you have a phone, you have a spy in your pocket …"*** A genuine limitation of implementing social media for safety is therefore the lack of assurance regarding data confidentiality. Indeed, confidential safety-related data, such as vulnerabilities of industrial installations or cybersecurity risks, could be subject to leaks, as social media are opaque in their data handling. Thus, the use of social media appears contradictory, as these tools can facilitate the creation of a strong safety culture but also be counterproductive in this same regard, creating a real tension where the tool becomes a vector of vulnerability.

Moreover, workload overload related to social media for safety is an element that emerged from the interviews. Indeed, just as with the implementation of the internet in work organizations, social media pose new problems regarding the boundary between personal and professional life. People's safety is not limited to physical integrity but also includes the prevention and mitigation of employees' mental health. Participants expressed discomfort with receiving communications and messages outside of working hours, as this creates significant mental overload that can generate fatigue and burnout. Being digitized, social media facilitate interactions, as discussed in previous themes. Consequently, individuals can easily interact outside of working hours, leading to increased working time. This threat to work-life balance is summarized by the following quote from the interview with P4: ***"And in fact, there's this whole notion that has to be taken into account. It's how we're going to manage the fact that, well, suddenly, we authorize... We authorize these applications on personal phones, but it's still professional."*** The literature shows a link between workload overload and mental overload, such as (EEG power spectral measures of cognitive workload : Psychophysiology s. d.), which explains that workload overload causes a decrease in performance, leading to an increase in errors. Applied to the safety context, this overload can have significant and counterproductive consequences, conflicting with the very essence of implementing social media for safety. The tension in this sub-theme lies in the fact that social media are perceived as facilitators of safety communication, yet they paradoxically add an additional burden, potentially weakening the conditions necessary for a strong safety culture.

The third dimension of this theme lies in the psychological risks generated by social media, beyond the aforementioned aspect of mental overload. Indeed, the analysis of results shows that the omnipresence of messages, reminders, and communications via social media can generate a feeling of permanent pressure, comparison, or evaluation. For instance, disseminating a video of good practice gestures may be perceived by some individuals as a challenge to their actions, work, or involvement. Furthermore, the code "dependence on social media" illustrates that the addictive aspect of these tools is problematic for individuals performing tasks requiring high attention, such as operators working on dangerous production machinery. These negative reactions and behaviors clearly weaken individuals'

ability to adopt safe behavior, thereby harming safety culture. Thus, these reactions demonstrate that social media are not merely technical tools but can have significant impacts on the humans who use these technologies.

In summary, social media possess intrinsic limitations that nuance the positive effects discussed in previous themes. A careful weighing of the advantages and disadvantages of using social media for safety must be conducted to determine whether the negative effects outweigh the positive ones, or if one set of effects dominates the other. This question was not addressed in the interviews, as it is highly specific and dependent on the organization's unique situation.

Synthesis analysis of the six themes

The global analysis of the six themes - *explained in details in the previous sections* - is presented in the table below (Cf. Table 14):

Theme	Main idea / Summary	Contributions to safety culture	Contradictions / limits	Links to other themes
1 - Social media a tool for rapid and wide dissemination of safety information	Social media reconfigure the temporality and spatiality of safety communication. In practice, this theme explains how information circulates faster and further, which is particularly effective for safety policies, for example, by enabling rapid alerting in the event of an accident.	Rapid dissemination allows for alerting, initiating the chain of responsibility to address the accident. Broad dissemination homogenizes knowledge of safety rules among employees, especially in a growing globalized context with sites in multiple countries. Broad dissemination minimizes the time and effort required to communicate best practices and safety rules while increasing individual involvement. In these aspects, social media are more effective than traditional methods (handwritten logbooks, oral exchanges...).	A constant flow of information and the trivialization of alerts generate fatigue and weariness, which is counterproductive for safety. If dissemination is poorly calibrated, it can encourage individual actions not defined in accident mitigation processes. Social media are an effective tool, but they support an already established process. Without this prerequisite, their contribution to safety is null.	**Theme 2:** Social media help structure the post-accident responsibility chain. **Theme 6:** Cognitive overload, fatigue...
2 - Social media as operational support for safety management and prevention	This theme offers a process-based reading of safety culture, highlighting the contributions of social media in structuring the post-accident response. Indeed, social media help coordinate the chain of responsibility, the initiation of which was facilitated by them (as	Social media support the post-accident process in three stages (excluding the alert covered in Theme 1): 1) **Reaction:** Facilitated by social media, which help homogenize the level of information and coordinate personnel. 2) **Storage:** social media allow for storing data, messages, and information, enabling the creation of relevant KPIs to manage safety. 3) **Analysis:** After resolution, social media enable tracing of individual behaviors, which can	Social media facilitate person coordination. However, individuals must be able to communicate information correctly, in a brief and rapid format. Social media are an effective tool, but they support an already established process. Without this prerequisite, their contribution to safety is null.	**Theme 1:** Post-accident responsibility chain. **Theme 5:** Operational effectiveness depends on organizational prerequisites. **Theme 6:** Operational use of social media amplifies psychological risks.

	discussed in Theme 1).	challenge current organizational processes or detect deviant behaviors.		
3 - Complementarity and limits of social media compared to traditional safety tools / methods	This theme shows that traditional methods (toolbox meetings, memos, handwritten notes, in-person weekly training and meetings, posters, signage...) remain highly relevant for establishing a strong safety culture. Social media are thus complementary to these methods.	Physical interactions are perceived as more impactful and symbolic. Social media serve to reinforce messages. By reducing distances between managers and operators, social media make safety rules more acceptable, bringing people closer and fostering social bonds. Traditional methods better embody safety culture, structured around key moments, while social media ensure continuity of actions, keeping safety alive outside these key moments.	Deploying social media can increase resistance to change. Implementing new safety rules and policies is already difficult; adding the implementation of social media on top can create tensions and exclude individuals who are not comfortable with these tools.	**Theme 4:** Social media promote participation and the building of strong relationships between managers and operators. **Theme 6:** Strong participation without decision-making power can generate frustration.
4 - Actor engagement and participatory dynamics in safety culture	This theme analyzes social media as a driver of collective engagement, favorable to establishing a safety culture.	Social media provide a simpler space for expression than traditional methods, facilitating the reporting of issues. They reduce individual isolation by creating contacts between people. Traditionally, safety rules are implemented by higher hierarchical functions onto operational ones. Social media precisely offer a space that facilitates bottom-up communication (operator => manager), a previously underutilized flow.	Can create frustration, as operational functions are often limited to basic roles like reporting problems or giving alerts. Operational functions, however, do not really have control over problem mitigation, even though they are paradoxically the best informed about the situation. This can create tension and frustration.	**Theme 3:** Social media promote participation and the building of strong relationships between managers and operators.
5 - Organizational, cultural, ethical conditions and challenges for social media use in safety	This theme is descriptive, enumerating the prerequisites and necessary conditions for implementing social media in safety.	Requires a new organization of safety via social media.	Although companies have a strong desire to digitalize, including via social media, economic and organizational constraints can hinder large-scale deployment. Furthermore, social media are useful and implementable mainly for companies of a certain size, with significant human and economic resources. Social media can distract, for example, workers who must not be distracted while operating dangerous machinery. Thus, social media can be	**All themes**, as it is a cross-cutting theme.

			counterproductive for safety in certain situations.	
6 - Risks, limitations and negative impacts associated with social media	This theme is also descriptive, explaining the limits and risks associated with implementing social media for safety.	*(Note: This column is left blank in the original, as the theme focuses on negative aspects.)*	Social media generate mental fatigue, as personnel are continuously connected, which reduces attention and promotes mental fatigue-related illnesses. By reconfiguring the temporality and spatiality of safety communication, the boundary between personal and professional life erodes. Individuals are encouraged to remain constantly connected to work due to the constant influx of information from social media.	**Theme 1:** The flow of information generates fatigue, harming vigilance and safety. **Theme 4:** Strong participation without decision-making power can generate frustration.

Table 14: Synthesis analysis of the six themes

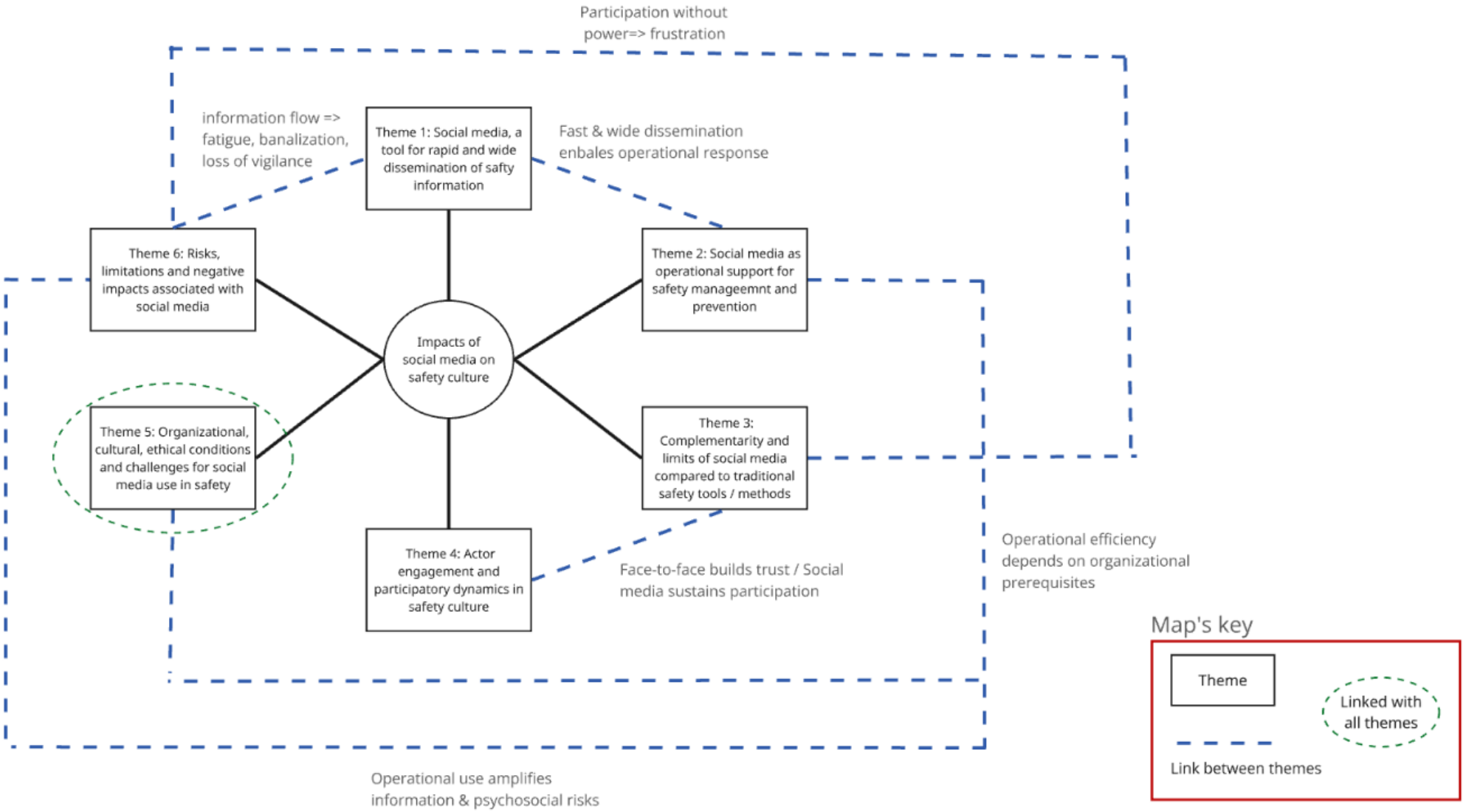

Figure 20: Links between the themes

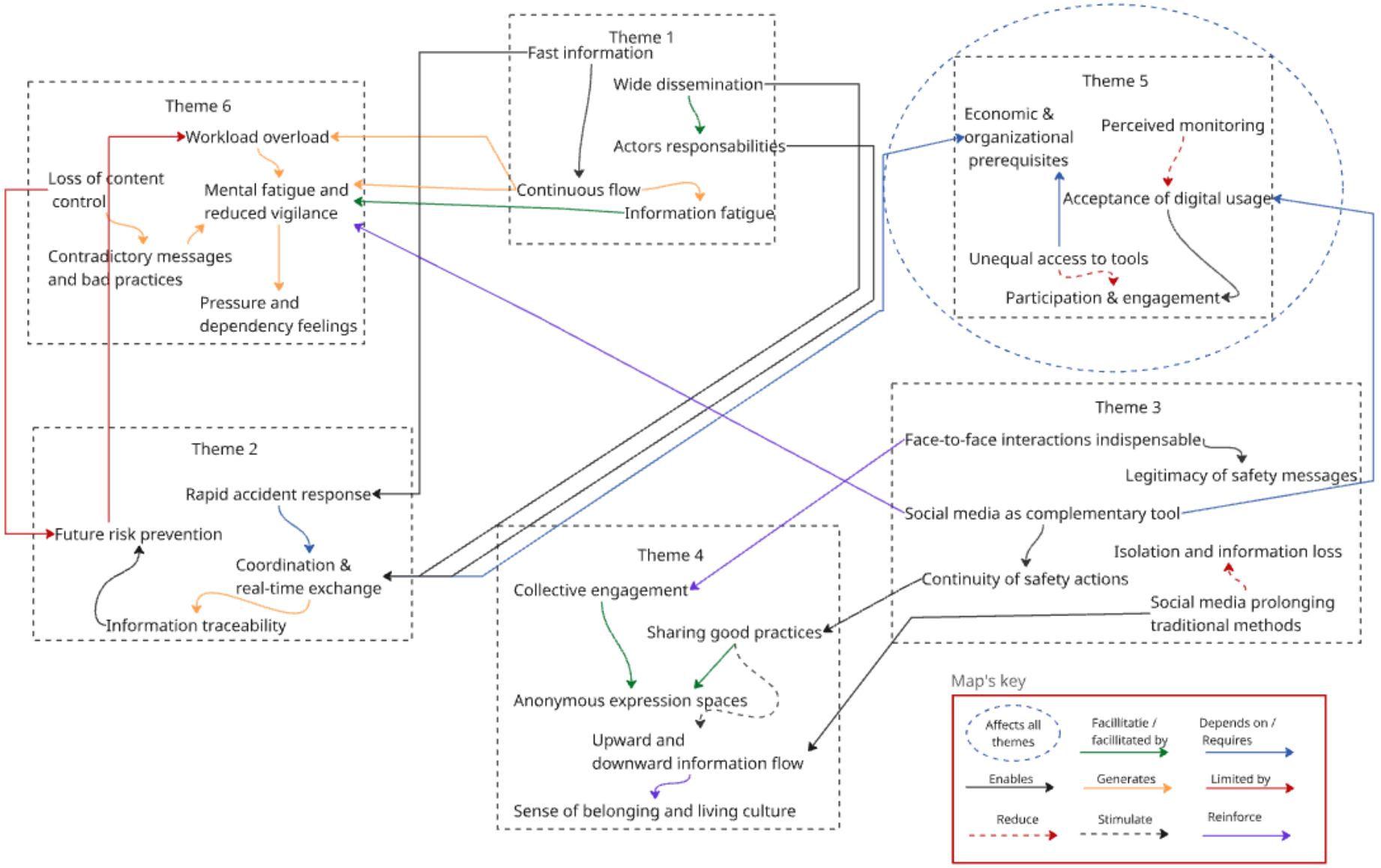

Figure 21: links between the main ideas of the themes

VI / Conclusion

Synthesis of the thesis

To conclude, my thesis work has addressed the research problem concerning the impacts of social media on safety culture by answering the following two research questions (RQ1 and RQ2). A summary of my thesis results is presented below:

RQ 1: What are the positive and negative impacts of social media on security culture within organizations and companies?

Positive impacts	Negative impacts
Rapid and broad circulation of information	Generates mental fatigue and leads to decreased attention (a safety risk)
Creates a continuous flow of data, keeping safety alive in daily operations	Risk of losing control over the information transmitted
Complements traditional safety methods (signage, posters, memos, in-person meetings, etc.)	Unequal access to social media generates frustration, reducing team cohesion and compromising safety culture
Structures real-time coordination of human resources	Requires significant organizational and economic prerequisites for implementing social media
Allows information to be tracked, shifting exchanges from informal to more formal	Creates a feeling of constant supervision and control for individuals
Improves engagement and accountability of all stakeholders	Endangers the boundary between personal and professional life, promoting decreased attention and psychological fatigue
Enables the creation of bottom-up communication (operators => managers), breaking from traditional top-down methods	
…	…

Table 15: Synthesis of the positive & negative impacts of social media on safety culture (RQ1)

As discussed earlier, the impacts listed in the table above should be nuanced, as positive impacts can generate side effects and ultimately have negative consequences for safety.

RQ 2: What are the possible applications of social media in order to enhance safety culture within organizations and companies?

We have discussed that social media are interesting tools for establishing a strong safety culture. Indeed, social media allow for the broad and rapid dissemination of safety rules, initiating the chain of responsibility by issuing alerts in case of accidents, extending and keeping safety active to create a genuine culture, among other applications discussed in more detail in the results section. Social media can also make safety training more educational and engaging, which helps facilitate prevention. However, numerous prerequisites are necessary, such as defining a clear organizational process that social media support, or gaining user acceptance for using social media (change management, etc.). Thus, social media are particularly relevant for companies with multiple sites due to globalization, as they reconfigure notions of space and time by quickly connecting people over short or long distances. The human and economic prerequisites required for companies to implement social media seem more accessible to large companies than to small ones. It is possible to create a strong safety culture without social media, these tools are interesting but do not automatically guarantee the creation of a strong culture. The sector in which the company operates (industry, services...) is also a differentiating factor

in the application of social networks to safety culture, as these sectors have different needs, as discussed in this work.

To conclude my thesis work, I wish to create a macro summary of my work while giving a concrete dimension to my results. Indeed, I propose to illustrate my findings in a concrete way, using the example of the social network WhatsApp, which came up frequently during the interviews:

- **WhatsApp as a tool facilitating safety culture.** Indeed, this instant messaging platform allows for the rapid circulation of information (photos, messages, etc.), particularly suited for situations requiring a quick reaction. Beyond this "emergency" aspect, WhatsApp also helps maintain the vigilance level of teams by keeping the safety culture alive. In fact, WhatsApp extends prevention messages and safety rules that are embodied during key moments (training, workshops, field visits, etc.)

- **WhatsApp as a complementary tool to traditional methods (in-person training, signage, posters, workshops, etc.).** By extending the key moments of safety, WhatsApp complements traditional methods without replacing in-person interactions, which are essential for trust, ownership, and legitimacy. These prerequisites are necessary for creating and fostering team cohesion, a fundamental condition for building a strong safety culture

- **WhatsApp promotes employee engagement.** By breaking down barriers between operational and managerial functions, WhatsApp encourages more horizontal communication. However, as a tool, WhatsApp depends on organizational processes as well as the company's level of maturity

- **The implementation of WhatsApp as a security tool is subject to prerequisites.** Indeed, organizational prerequisites are necessary, such as providing phones for everyone, particularly for operators. The latter often do not have access to their phones when working in production workshops, as it can be distracting. Other prerequisites, such as securing personal information, are also part of the necessary requirements for implementing WhatsApp.

- **Despite the advantages offered by WhatsApp, certain aspects can also compromise safety culture.** Indeed, WhatsApp contributes to the erosion of the boundary between private and professional life. By being hyper-connected, individuals can become overloaded with information, especially outside working hours, leading to reduced attention. WhatsApp also facilitates information overload, which negatively impacts employees' mental health, thereby affecting safety culture.

Methodological limits of my thesis

To conduct this work, I used a thematic analysis methodology (Braun et Clarke 2006). Indeed, my research is qualitative and exploratory, as this topic is not covered in the literature. The objective was therefore to provide an initial overview of the various impacts of social media on safety culture, paving the way for future research. My research has limitations, both in terms of the method used (thematic analysis) and the way I applied and conducted this method. These limitations are outlined below for the sake of transparency:

Limitations Related to Thematic Analysis

Some scientific articles have already addressed the limitations of thematic analysis. Indeed, the method itself is considered rigorous and reliable, but some authors question its misuse. For example, the very authors who popularized this method have written an article highlighting the limitations in its application as practiced in scientific publications (Braun et Clarke 2024). Several issues are discussed in this article:

- Articles using this method generally rely on too little theory. This lack of theory makes it difficult to contextualize and interpret the data (interviews, verbatims, etc.). Articles that do not sufficiently engage with theory are often described as descriptive rather than analytical, which goes against the spirit of the method.
- The concept of a "theme" is not well utilized. It is noted that many themes are descriptive, lacking strong interpretation and reflection. While some themes can be descriptive, the majority should not be.
- The lack of analytical transparency in research using this method is also highlighted in the article. Indeed, the methodology is rarely explained in detail, and interview transcripts are often not included in articles using thematic analysis.

Limitations Related to How I Conducted My Thematic Analysis

In my analysis, I deliberately adopted a very broad theoretical framework. I used the broadest definition of social media I found in the literature: **"For purposes of this chapter, we define social media as any online resource that is designed to facilitate engagement between individuals." – Bishop (2019) from (Aichner et al. 2021).** Since my research is exploratory, I wanted to avoid being overly restrictive, which means this definition includes, for example, emails and digital platforms. This definition may be too broad, and it would be interesting to refine it for future research in this field. I also used a broad concept of safety, encompassing physical, mental, and data/information security.

The interviews I conducted also have limitations. Indeed, three out of seven participants are from the same company and therefore the same industrial sector. This could bias the results by reinforcing certain viewpoints. Furthermore, it would have been relevant to conduct this work with multiple researchers to verify the reliability of the codes and enhance their analysis.

Advice for future researches

Since my work is exploratory, it is interesting to consider various relevant research directions on this topic in my view. I recommend conducting a concrete case study on the implementation of social media in a company. This study would make it possible to verify the positive and negative impacts, as well as the applications of social media for safety culture. I advise continuing, for the moment, with the broad theoretical framework I used for defining social media and safety. Indeed, these concepts can be narrowed down at a later stage to measure very specific effects, but since this is an emerging field of research, it is advisable to remain broad for now. Furthermore, it could be interesting to quantify the impacts I have identified to see if there are statistical correlations between certain qualitative variables I highlighted. It would be interesting to conduct further research on the trade-offs involved in implementing social networks in the workplace. It could be interesting to test if age is a factor in resistance to change, but it requires a restriction of the definition used by social networks for this, since email is used by everyone without age distinction.

Appendices

Interview of the first participant P1: CEO of a plastic industry group.

Matteo: The interview is about the link between social media and safety culture. The definition we give for social media is all the platforms that allow people to interact with each other using the Internet. That means it's quite broad, all that is considered social media, even if it's internal. And so, I'll have to ask a few questions about the links between social media, etc. So, could you list the social media that you use in a professional context, especially that you use professionally, social media, whether for safety or not?

P1: OK, so there's Teams. WhatsApp. OK. LinkedIn. SharePoint. Then we have a certain number of platforms. So, for safety, it's RedOnline. Actually, we subscribed to a service that lets us lock down the rules, the regulatory points. It's called RedOnline. **[My safety director],** he'll certainly tell you about it better. For monitoring laws. Obviously, email. That's it.

Matteo: And RedOnline, is it connected to the Internet?

P1: Yeah, it's connected to the Internet. I'll give you the contact of **[my safety director]** so you can ask him more questions. Actually, it's a platform where you have all the legal texts and you add your quotations and it gives you reminders, as well as all the updates of legal and regulatory texts. What I call legal is regulatory. Otherwise, what else is there? Yeah. I think that's good already.

Matteo: OK. And regarding everything related to safety, what do all the platforms you mentioned help you with?

P1: So, already, email. Email allows us to launch safety weeks **[this refers to a full week of workshops related to promoting safety].** It allows us to send out safety alerts when there's an accident or incident. So that's an important point. Teams and SharePoint allow us to track — first to gather documents, gather action plans. And then they let us track everything we call transversal memos. So, we put them in Teams and SharePoint. And then it allows us, afterwards, to have a common database, and to jointly track — because it's important, the emulation between plants — jointly track the progress on each transversal memo. So, the progress on a certain number of things. We have 100 or 150 transversal memos. We have all the plants and we want to know which plant has closed which transversal memos. So that's an important point. We put our roadmaps there [medium- and long-term strategic plans with target objectives regarding safety]. So, the target roadmap and each plant's progress on the roadmaps. So actually, it's more of a sharing exchange, a database exchange. It's a dynamic database. So, on the one hand we have best practices and on the other hand, tracking and progress on these best practices. There's one important point: during our safety weeks, through Teams, that's what allows exchanges between plants. So sharing photos, videos, and then making a best-of and then making a poster for the safety week, communicated afterwards to people. So that, I think, is an important point. LinkedIn, for me, when I surf on LinkedIn, when there are interesting points, I send them to **[my safety director]** or to people in the organization. For example, I saw that the **[name blurred**] site had a contractor rate of 2 at 0.42. So I retrieved that LinkedIn data. So that seems important. For the others… And WhatsApp allows us to be super reactive. Now, what many — almost all of our plants — do is that between

management committees and team leaders, they have a shared WhatsApp space, and so they send each other information. So for example, in Mexico [one of the group's plants is in Mexico], as soon as there's a dangerous situation, they take a photo, they kill the situation, and then they ask each other to forbid it. So it streamlines information and allows nearly real-time reaction. So that's pretty great. That's a big advantage of WhatsApp. So we covered mail, WhatsApp, Teams. So, Teams is also all the institutional presentations, all the risk maps. So actually all the data collection, all the best practices, and all the progress of our action plans. So, regarding the roadmap, regarding the risk maps. So that's an important point for me. And then all the monthly presentations of the status of safety actions and safety points. And that's important because all the plants have that presentation available and they use it within their management committee. That's my point.

Matteo: OK. Do you have, typically — because some companies do this — internal pro groups on LinkedIn, on specific topics?

P1: No, we have a group that is excellent, a group, there is a group, but it's not very… There isn't a specific topic on the company. OK.

Matteo: And so, you kind of answered, but you can broaden the question. It's in the sense: if there are differences or complementarities with more traditional methods on the dissemination of safety policy implementations, traditional methods like meetings, post-its, signage, are there…

P1: Actually, I think it's really a complementary approach, meaning there are all the things we just talked about, and then there are also screen communications. So whether it's for safety weeks, major incidents, major safety points that we implement, we communicate via screens. So we have screens in all the plants, and that's really important. There are things that can't be replaced by social media; there are face-to-face meetings that can't be replaced. So already, when we onboard new arrivals, they're received by the safety manager or by their boss directly, who explains all the safety standards in the company. For example, our last new hire, when she joined Rose [one of the company sites], in the second hour she was received by the safety manager of [a site in France]. So that cannot be replaced. That has to be face-to-face. I think face-to-face meetings are more an act of management at my level. So typically, next Friday, twice a month, we have a meeting about accidents that occurred, where the plant director, the manager of the department where the accident happened, come and present to all the other plant directors, to my **[safety director]** and to me, the actions they put in place. So there's transversal action and management action, because the guy needs to understand that it's also his responsibility. So nothing can replace that. I mean, social media— well, the meeting is complementary, because it's often done via Teams, since we have plants at the ends of the earth, but it's still face-to-face. So it's a real complement, meaning the use of digital tools allows us to get certain messages across as if we were face-to-face in a room. So that's important. The big complement is still on safety week, because there are activities carried out in the plant. So in the plant, either looking for risks in workshops with paper forms that we bought three years ago with my **[safety director].** We have workshops: it can be a car that rolls over, it can be blurred glasses. That's very important to do in person with people to create engagement and bring them along. That seems to me a major point. Then we also put in person — because I really believe in in-person — the awarding of safety trophies. So that's in-person time with teams. In person, there's also doing plant tours. So plant tours allow identification. That's also a management action. And above all, we developed safety talks **[small trainings on safety topics]**. **[My safety director]** will tell you about it. That's so that the M1 or management committee members go

and deliver tools as close as possible to the field. Meaning that for me, safety is truly the number one management point. Meaning basically, if you're not interested in safety, you're interested in nothing. No point being a director or manager. And there are a number of tools, of media, that allow — media broadly speaking: screens, Teams, SharePoint — that allow strengthening your message. We used, with **[my safety director]**, email four years ago when we started the safety point, to launch safety week together. We did the same with [my quality director] for quality week this year. That was the first time. So it allows us to rapidly reach everyone in the computer. This year, with [my quality director], we wrote to maybe 150 people [in our company]. We wrote to all of [the company], actually. All of [the company and the group]. We did the same in safety. So the advantage of these tools, like email, like communications also, newsletters, which are then sent by email and stored on SharePoint, is that they allow having traceability, to quickly reach a large number of people. And so, people know there is a newsletter on safety, they know where it's stored and can go check it in their spare time. We also put screens in our break rooms. So we display a number of messages about quality, safety, whatever we want. So it's really a combination of both. In-person, or Teams. But I still really like in-person for plant tours because there's a real managerial impact. The tools that allow even more impact, notably those we mentioned, are fundamental.

Matteo: OK. And during safety weeks, it's in-person workshops where you have trainers that come in on specific situations, right?

P1: That's right. So we had glasses that simulate being a bit drunk. Yeah. With **[the safety director],** we bought maps where there are dangerous situations, operators have to find them. We had firefighters who came with a car that rolls over. We had extrication exercises. We had — what did we have? — oh yes, we had sensors that measure ergonomic positions. So the idea is to open people's minds and make everyone understand that we're in a risky environment, that we try to reduce risks as much as possible, but that the first actor in safety is the person himself. Because me, from my office, I'm not going to monitor 2,500 people. So if nobody pays attention, it'll quickly be a mess. So that's mostly it. If you're interested, Matteo, safety weeks — I have schedules that we used. I can send them to you.

Matteo: Why not, yeah. That would give me an idea.

P1: So each year he **[the safety director]** prepares his schedule. And then I present it at the executive committee because I want each executive committee member — although the others don't want it every year — but I want each executive committee member to be present at a plant to make an impact. And me and **[the safety director]** go to the plant that we defined as the one that will receive the safety award.

Matteo: OK. And so what… what involves better participation from people? Is it the more traditional in-person methods? Or is it really the fact that they're in loops, like you said in Mexico, where they're in small groups, WhatsApp, etc.?

P1: So I think the advantage of small groups is that really, people — it's as close to the field as possible and they feel listened to. And there you go. But that's more for our operators. So operators don't have access to WhatsApp. They don't have access to Teams. So actually, for operators, it's super important to do safety talks in person with them, plant tours in person with them, because there are lots of tools

they don't have access to. Meaning that their manager, their supervisor, their production manager, they will have access to a computer with their account. So they will have access to Teams, SharePoint, email. So actually, operators only have access to their FF, to the screen. And to the plant tour we can do. And to the management committee when it comes to do safety talks. So you see that there's a whole part of the population, especially those who don't have access to computers — if we limit ourselves to media tools, we reach them only moderately. So my point is to say: use media to reach managers. Use plant tours, in-person, etc. to reach operators. And operators. That's why with **[the safety director],** we set up safety talks because it forces managers to see operators and talk with them. They don't have a mailbox to receive newsletters, etc.

Matteo: Operators don't have access to computers?

P1: No. No, no, newsletters are displayed on screens. Yeah, so in break rooms, common areas. They're displayed on screens. And then, when there are important things, you see, the poster is put in the plants. Safety week, when there are important things, it's on screens. When we secured stocks, etc. But in big groups, operators have access to computers when we want to do surveys, especially HR. But otherwise no. They can have notebooks where they can report — or rather, they can say "be careful, there's such and such dangerous situation" or make suggestions for improvement.
Matteo: Written notebooks then?

P1: At the moment, they're written notebooks. We're looking at, for [the company], [a site] in particular, how to digitalize this. But we don't know yet. OK. But digitalization, well, I believe in it yes and no. For me, it's the next step. Meaning the person must already understand. Because actually, everyone with AI — they all jumped on it like crazy. They say "that's crap". Actually, the guy must already understand the process, what we want to do. For example, the operator must be mentally conditioned to say: "there's a risk, I raise my hand, I go see my manager, I put the preventive measure, etc. And then I suggest how to improve it". And after, whether it's paper or digital, if he's in the right mindset, digitalization is just an improvement that comes afterward. But that mindset, you have to create it first. And it's not AI or social media that create it. So the idea is: once he's mentally conditioned, then indeed it allows keeping traces, storing, sorting, tracking. So it's powerful. But for me, you shouldn't skip steps.

Matteo: And so you were saying that social media was mostly used by managers? Do you think they are more involved because there's this whole traceability aspect, that they are more concerned about these topics?

P1: Actually, my thing is always to say: a staircase is swept from the top. So obviously, the initial pressure is on managers. So I put it on plant directors, and then it cascades. So they're concerned for many reasons. I don't know if it's directly linked to social media. They're concerned because they have positive pressure from their management. They're concerned because they have objectives related to that and because they're involved. And then indeed, it's a tool, all these media. So it allows conveying the information we want, putting guardrails in the system. But I'd say it remains a tool. And it's a good tool, because it allows us to control roughly everything that happens. We talked about emails earlier. Now, when something happens at a plant, an accident — of course before, it was me, now it's **[the site director]** — we get a call from the plant director, but immediately, within 24 or 48 hours, there's an alert to everyone. So that's important. And the guy who sends the alert — well, it goes to everyone,

including me. So he knows I'm going to ask him questions, the production manager. So he's careful about what he writes. So actually, the advantage is also that the guy says "careful, I'm putting an alert in the system, I need to have properly looked into it beforehand, because I know in three minutes I'll get a question about it". So the guy is mentally trained not to say anything random, to have informed himself beforehand. He knows I'm going to ask the same three questions, always. Have you seen the operator and is he OK? If he's OK, does he accept an adapted position? Was he wearing his PPE? Because he's not just a victim, he also has a duty to wear his equipment. So actually, the guys are already conditioned. And indeed, they know that when they issue an alert — and that's the guy who can do it in our system — yeah. And now we added with [the safety director] that twice a month they come and present the accident, what happened, what they put in place to resolve it.

Matteo: So at manager level?

P1: Manager and plant director, yeah. Well, in a month or two I won't say it anymore, I think it'll be **[the safety director and the plant director],** but for now… So yes, somehow it allows structuring the system. Information circulates fast, it's like an open book, info circulates fast, there's information available to everyone, and that's what I called a database. And we see the dynamic, because with [the safety director], with all the documents we now have, we're able to see the dynamic of the number of memos closed or not, evolution, etc. So it's really rich.

Matteo: OK. OK, clear. And in terms of obstacles, do you see any obstacles in promoting social media for safety, besides what we said — that you first need to understand the process in person, etc.?

P1: No.

Matteo: In terms of data, is that something that is already worrying, in terms of data, data safety?
P1: For pure safety, I'd say no. I'd say, well, I'd say no. The only somewhat sensitive data we have are data related to the group's risk mapping, which didn't exist before I arrived and which I wanted to implement with **[the safety director]** to give shareholders a view of the risks in our plants, which we can't necessarily communicate. But for us, we have this vision to have a longer-term plan to address them. So that's… That's not stuff we want to communicate. So it's somewhat sensitive data. Besides that, our indicators are what they are. I'm more in favor of communicating them massively to all staff. No, that's the only point that I'd consider sensitive. Safety investments are open. I don't think it's secret. That's it.

Matteo: Because you talked in terms of dissemination, but regarding the platforms themselves — for example, you use SharePoint, WhatsApp, Teams to communicate this. Do you have doubts about the content you share and the fact that you put these data, like the risk maps, etc., which can be sensitive, on these platforms? There could always be a risk.

P1: So WhatsApp, messages are encrypted if I understood correctly. But overall we know there's always a risk. … The former head of **[external security intelligence service]** said that anyway, once you have a phone, you have a spy in your pocket. He said that on air. So indeed, honestly, it's not safety data that is most sensitive. Because, well, for safety there's these risk maps but I don't see who would want

them, frankly. But there's more sensitivity on our financial accounts, on a number of things, our budget. So typically, we have an IT department that simulates attacks. Because they can take data, but there is also system paralysis that is a possible consequence of an attack. At a branch **[of the group]** called **[name blurred]** at the time, the game was — they used to encrypt your files. So it's not just data theft; it's also losing access to your data.

Matteo: Meaning that they deprive you of files that aren't typically shared, not local?

P1: Yes, that's it. For me, in safety, if we go back — if there are data that leak outside, I'm telling you there's this risk map that's sensitive. But I don't see who would want to use it honestly. But it's more: if the files disappeared completely, if they were encrypted, we'd lose much of our historical record and it would take time to get things straight again. If you lost that, you have all your transversal memos, the safety roadmaps per plant, and all the massive work **[the safety director]** did behind.

Matteo: And since you, by law, are not allowed to have health data of people when they have sick leave, etc. You don't have access to that. Because that could be sensitive data.

P1: Yes, that could be. I don't know whether we have access or not to be honest. But you're right, that could be sensitive. We're not subject to that because we don't have direct exposure. But in companies like **[name blurred]** or Plastic Omnium where there were manual paint booths, there were indeed regular hearing exams to ensure noise exposure levels were OK. So everything related to people's health could be considered sensitive data. I agree.

Matteo: And typically, how did you store that kind of data? Was it through SharePoint, etc.?

P1: It was on the network too. It was on the network… yeah, on the server. Access to those data is limited, but you never know actually.

Interview of the second participant P2: Safety director of a plastic industry group

Matteo: It works. Well, thank you very much for taking the time. In fact, I'm writing a thesis on everything that concerns security, especially industrial security, and see how social networks can possibly help, the challenges that may arise, etc., to really try to implement social networks in the service of industrial security. So, in the definition of social networks, it's something that's very broad. It's everything that allows people to exchange information by using the Internet. It's really super broad as a definition.

P2: Okay, so as much as YouTube as LinkedIn, Snapchat, Facebook, etc. It's really very, very broad.

Matteo: That's it, it's super broad. And so, in relation to that, I'd like to ask you a few questions. I did a part with **[P1],** but there are certain things that he didn't necessarily know everything about. I have a lot of questions about all the tools that are used, digital tools or social networks that are used for security purposes, to share information, etc. Do you have a list in mind?

P2: On the tools I use today?

Matteo: Yes, or even at the managers' level, which they implement.

P2: Which are used by managers on very specific tools. In fact, we use a lot of Teams, SharePoint in the broad sense. Because we have a lot of shared files on which everyone can be brought in to intervene. Whether it's to update, add a data or status on the progress of such or such item. So yeah, we're a lot on sharing information and communication. But the thing is to make it accessible. How can I tell you that? Yeah, it's file sharing. In fact, it's Teams. So yes, we use it as a communication tool, via messaging, via what we're doing. But there's also a lot of shared files where everyone can be brought in to intervene, to bounce, to update. Yeah, I use a lot of that. That's basically it. Then I have other tools that are very specific. For example, I have a regulatory monitoring tool. I'm not sure we're on social media. RedOnline.

Matteo: I'd like you to talk a little more about it please.

P2: The tool is called HSE Compliance. HSE Compliance, which is provided by RedOnline. RedOnline is the name of the company that developed this tool. In fact, it's a software for regulatory compliance. That is to say, you subscribe to a subscription. First, you pay for the implementation of the solution. Because they're going to create regulatory templates. And then, basically, you're going to pay for an annual subscription that gives you access to your text list. And at the same time, it's going to give you every week, the regulatory day. Such and such regulation has evolved. Such and such regulation become applicable or will be applicable from such and such date. And the software as such allows you

to do your regulatory compliance assessment. So beforehand, you have a list of questions. It's very diverse. What type of activity? There's the ISO regulation for French sites. Installation placed for the protection of the environment. So you're going to click on your rubrics. You're going to define what your thresholds are. And then it's going to ask you the question: Are you an owner? Are you a tenant? What is the surface of your building? Is there a floor? The number of employees? Do you have interim employees? Do you appeal to outside companies? Do you have this or that type of machine? Do you do three steps? In fact, there's a whole questionnaire. Very diverse and very varied, which is very, very long. In order to determine what your applicable regulatory obligations are. Do you have photovoltaic panels? And if you click on yes, all the applicable regulatory texts become applicable to you. The advantage of this tool is that it makes you sort out the texts that are applicable to you. Example, to give you a very concrete example. Do you have radioactive substances? Or are you concerned about non-ionizing radiation? Depending on what you answer, it gives you access to this or that text. And then you have access to the register. And then, article by article, you come to state on conformity. Conform, non-conform, conform, non-conform. As soon as you have a notion of periodic control. I don't know, your photovoltaic panel installations. You have to check them once a year by a competent body, etc. It also allows you to build a surveillance plan. Every year, it will remind you at what date you have to check your photovoltaic panels. And when you have non-conformity, you can also pilot an action plan. And this solution, as a central HSE director, I have a bit of a big brother. I have access to all the sites. I see what they do and what they don't do. And then each entity has access to its own software. And so it does its conformity assessment. And I have access to the dashboard. We see a lot of things. We can do an extraction. We can do a quarterly, annual report. The solution is really good. It's because we used to do that with Excel, but it's the age of stone. Imagine doing regulatory conformity with Excel. Given the amount of text today, it's a great tool. It costs a lot, but it's a great tool.

Matteo: And then you communicate it to everyone, right?

P2: No, because I go to the site hsecompliance.com. There's a dedicated platform. Typically, I've created user profiles. I have HSE profiles that will evaluate. I have profiles that are more responsible maintenance, site management. It's more for information. I could also put them as an evaluator. But today, it's more information. But basically, today, on each site, I have HSE, site management, so the director of the unit, the responsible maintenance, sometimes maybe a maintenance coordinator, and maybe the HR too, because there are elements related to labor medicine, labor accident management, pro-disease. So basically, HSE, maintenance, site management, and then RH They have their own profiles that have been created on the platform.

Matteo: Whether it's on this tool or even on everything you share on SharePoint or Teams, it's only managers who have access. It's not the jobs or the operational level that they don't have access to?

P2: Yes, mainly for this subject. We have a number of teams on Teams. When you practice Teams, you see that we have teams. We have, for example, the team operations, where you will find all the coders, the central operations services, the supply, HSE, quality, etc. The top management operations. I don't know, there must be a hundred people who have access to all this. But it's still a rather private channel. Conversely, we have public channels that are accessible to everyone. For example, I'll give you a very

concrete example. Four years ago, we wrote our golden rules, the HSE golden rules of the **[corporation name blurred]**, and we created a training module that we made accessible. We also created a certain number of supports, of hot evaluations or a whole system of communication support. You know, the golden rules in blue card version, a kakimono, the big panels, etc. And all these media, in fact, we made them accessible to everyone. And we started to cascade the training, we trained the managers who cascaded their N-1, who cascaded their N-1, who cascaded their N-1, until we trained 100% of the collaborators in the company. And so, all this media, all this, the training follow-up file, the training module, hot evaluations, etc., all this was made completely accessible to everyone via Teams. I have that, and then I have another example. We created our own intranet called **[name blurred]**, which is neither more or less than SharePoint, but a customized version, which gives you access to several things. There is in particular the group's documentary base. So it's not just HSE, you'll find all the **[CSR – Corporate Social Responsibility]** documentation, quality, supply, IT, responsible purchase, RH. And so all these documents, these official **[corporation name blurred]** documents, they are accessible on our intranet. But in fact, it's a SharePoint, our intranet, you see. And so I have a specific HSE tab, and I have a lot of work docs that are accessible to everyone too. You will find examples of instruction sheets on machine tools, a number of documents that I have not deliberately coded as being central documents, but which are actually accessible and which can be used by sites. So some sites have taken some docs. I don't know if it speaks to you, but the management of... What do I have? A number of documents, for example, on fire prevention plans, these are things that I have not coded centrally. I have not deliberately coded them, but the sites have taken these documents and coded them in their own system. So it's also a bit related to the history of **[the group],** because each site is successive purchases of companies. So in fact, each site still has its own documentary system. I come from a group called **[name blurred]**. Well, there was only one central system, all the documents were in it and all the sites used these docs. Well, we tried to find a compromise for... In fact, there are a lot of docs that are in my HSE tab, which are not coded, but which can be used by sites. And it's as much mode op as procedures, as annexes, or even instruction sheets depending on the themes, or a control sheet for ladders, a control sheet for lifting trucks. I didn't code it centrally, but sites use it because in parallel, I have a roadmap that requires them to implement a number of devices. So these docs are available to them. But it's finally accessible to everyone. Anyone can go there.

Matteo: Ok, it works, great. It also seems to me that one of the big actions at **[name of the company blurred]** on security is the Security Week.

P2: Yes.

Matteo: So that's where, if I understood correctly, you do a number of workshops with trainers who come, situations, etc. That's it. And in this week, there are specific tools that you use. Or is it really in person, very physical, let's say?

P2: Well, I don't use specific tools. On the other hand, there's something I do for the Security Week **[Cf. itw P1],** because there's a planning that's built in advance. Each site thinks about what they want to do during this week. In the central part, we're going to deliver an award. In general, with **[P1],** we go to the site to give the award to the site that performed the best, according to very specific criteria. We

always do an introduction letter at the beginning of the week to announce, you see, it's like an introduction to the Security Week. But each site organizes itself. And in fact, what I've been doing since the first edition is that I'm creating a Teams channel, a communication channel, a discussion, in fact, where I put... So, I voluntarily put very wide. I'm going to put all the Comex, all the executive committee of the group. I'm going to put all the RHs, all the HSEs, all the site managers, all the production managers, all the... I put a lot of people in this communication channel. Because in fact, what I'm asking the HSEs is... Well, the HSEs of each factory, is to take pictures, take videos of what they do, of their activities, and to publish them on this communication channel. And in fact, the advantage... So, it allows you to... Because we started like this the first year, and the following year, in fact, I hadn't done it. And in fact, you don't feel like... You feel like nothing's going on. Because in fact, each site does its thing in its corner. So, the second time I did it, I told them, well, you store the photos in such and such a place, so they were going to put two, three photos, etc. But in fact, there wasn't this feeling of grandeur that you have when you have a Teams conversation. Because when you do this Teams conversation, every day, every day, you have photos, videos from everywhere. And it gives a feeling of grandeur. It's a thing that gives you the impression of... It really gives the impression that it's moving all over the place on all the sites for five days non-stop. And so, it gives a little depth to the subject. Whereas if you don't do it, well, basically, each site does its thing in its corner. And we're waiting for the end, or the week after, to make a newsletter, or make a comm, with a few photos. You see, it's a little... It's not the same thing at all. So, the fact of creating a Teams channel where everyone comes to publish photos... So, some are more spectators, especially all the Comex. But I have Comex members, and especially **[P1],** or the group's CEO, who says to me, it's non-stop. All the sites balance. And then, it's diverse and varied. An extinguisher training on the right, a person-to-person rescue exercise on the left, a risk hunt, a tunnel vehicle simulation. You see, when we did a specific thing on road risk, a gesture and posture training, well-being at work, a game... You see, there are lots of photos, diverse and varied, and it gives depth to the subject. So, that's something that's really useful to me. But it's more of a communication tool to show the extent of the subject.

Matteo: Yeah, I see. I see. And just... So, it's a question that's related to the subject, but a little bit annexed. Do you, in terms of... Because all of this still represents investments on the week of the... Not only human, but also financial. Do you, in the end, if you were to make an economic assessment between all the investments that are made in terms of security, to protect people, to train them, etc., and the benefits, would you say that this assessment is positive for you? Specifically on less working hours, on...

P2: Yeah, it's... It's... Well... It's difficult because... In fact, all the energy you spend I mean, all the human resources, techniques, etc., in fact, you... You can figure it out. Yeah. But you... It's difficult to see what you're avoiding as an accident. Yeah, It's a bit like... You put your finger on the problem of all the HSEs in the world because, in fact, when there are accidents, we say to ourselves, but what is the HSE for? And when there aren't any, well, we also say to ourselves, what is it for? You see? In a way. And, in fact, you can't... I'm going to invest in training. You don't know, in the end, if you're going to save a life. But you don't know. Because you don't know what you've avoided. Or vice versa. Yes, you can. You can because, in fact, each site today has its... So, it's what we call the **[work-Related Accident and Occupational Disease]** pricing. So, in fact, it's what we call the employer account. So, all the work accidents, depending on the duration of the stop, there is a fee that is applied. Or not just work accidents. By the way, work accidents or pro-diseases, depending on the duration, you have a fee, so an amount that is planned. Also, there is a second device, everything that is permanent incapacity. A

serious accident and someone who ends up with 10% of permanent disability. Or a pro-disease, say, 20, 30, 40%. In fact, it can go up to several hundred thousand euros. And all this amount, plus a certain number of coefficients, I could send you, if you're interested. You just type on Google, you type **[work-Related Accident and Occupational Disease]** pricing, and it will explain to you precisely how it is calculated. But there are also coefficients depending on whether you are a small company, a medium or a large one, depending on the number of employees. It's either individual rate or collective rate. But basically, all your sinisterness over the last three years, in fact, is related to a salary mass. It calculates a rate for you, which, behind this rate, is multiplied by the salary mass of the year in progress. And in fact, this is what determines the direct cost of your **[work-Related Accident and Occupational Disease]** sinisterness. And in fact, this is something that each site follows closely. Because this is the direct result. When you have a good performance, you have fewer accidents over the last three years, you have fewer accidents and fewer pro-diseases, your rate improves and therefore you will lower your direct cost. And what is also said, the direct cost is concrete, it's factual, it's what you find on the payroll. So in fact, it's money that comes out directly from the employer because he had sinister. So when you invest in prevention, theoretically, if you do your job correctly, you lower your number of accidents and your number of pro-diseases. And so, you will eventually lower your **[work-Related Accident and Occupational Disease]** rate and therefore, you will save money. But the link between your investment at the moment and your impact on the rate, in fact, we are talking about several years.

Matteo: Yes, I understand.

P2: Or conversely, if you had a bad year because you had a lot of accidents, you did anything, and that, you will drag it for at least three years. At least three years, it will have an impact. But then, give you the direct impact between what we invested for the week of the insurance and the impact on the employer account. So, I can show you on **[the group, name blurred**], I have a graph that is very clear. Until 2019, it climbs. And from 2020, in fact, it starts to drop drastically. So, I arrived in 2019. So in fact, if you want, there was already a start of work brought on 2018, 2019 and in the continuity, after, we really had a drop, but very clear. And we went from, I don't know how much, from 1 million to 500,000 euros. So, we can say that, indeed, we have drastically reduced the costs related to employee absenteeism, compared to everything we have committed since the end of 2019. It also coincides with the arrival of **[the CEO – P1].** There was a big dynamic that was put in place. So, like that, I can make the link. But hey, it's…

Matteo: Yes, It's more in terms of trends than really in terms of numbers.

P2: Yes, that's it, that's it. When you make an improvement on a process, you invest time and you increase your cycle time. And so, you can make a very easy on energy savings. You invest time, you get out time on prevention. It's a little different. But what is certain is that everything that we put in place, and in particular, these weeks of security, the tools, the standardization of many things, actually, clearly allows to reduce the access to work and pro-diseases. Because there is really a health and safety culture that has begun to be created at **[name of the group blurred].** So, we are still very, very far from the best in class. Plastic, Ommium, Miforacea, etc. But we are there. And us, the impact, the metrics that we follow, in fact, it's the frequency rate of the vaccines of the work accidents.

Matteo: TF1, TF2, TF3.

P2: Yeah, that's it. So, we follow TF2, mainly, because we are not yet mature enough on the part of benign care. Because there are sites that have a lot of benign care and there are sites that don't have any at all. But because, in fact, it's the very definition of benign care. For example, in Poland, they never have benign care. It's weird, but it's the Poles. In Mexico, it's the same, there is never benign care. While in France, I have a site that can have up to 50. in fact, TF3, TF2, on the other hand, we have accidents with and non-stop. And we follow, for **[name of the group blurred]** people, the interim and also the contractors. You know, sometimes you're looking for a tech now, you can't find it. Well, the contractors that we're going to take for three months, he's going to take his accidents and his hours of work and it's going to weigh on the TF2. And the TF2, we went from 11.8 at the end of 2019 to 5.5 at the end of October. We're at 5.5. That's concrete, you see. And then the curve, it's just going down. So that's concrete. But in terms of costs, of economy, well, I gave you the direct cost, but you also have to know that the direct cost, in general, you have the indirect cost, it's three times the direct cost. The fact that the guy who is absent, you have to replace him, so in fact, you're going to take an interim. The brand image, the productivity loss, the motivation of the employees, in fact, the direct cost, that's when you follow your courses in risk prevention, we say that the indirect cost is three times the direct cost. That's it. But end to end, if you do your calculation, it gives you a direct cost, multiplied by three, it gives you the indirect cost, it gives you, in general, far more than a million euros, or even two. And well, if you follow it every year, you can still show that you can save money by doing prevention.

Matteo: OK, clear. Do you possibly have other projects in terms of security to further improve security, especially on, why not, social network deployment? As I said, it's really in the very broad sense of social networks, so even the tools that allow sharing information. Do you have any projects in progress or are you thinking about other projects? Or even IA, because it's fashionable at the moment.

P2: I'm not going to deliberately limit myself to a social network, I'm going to be very broad. In fact, I have something that we have committed since the end of 2024, but we are on what we call security meetings. So it's a tool, it's behavioural security, where we inform managers and we ask them to go out and meet people, to always start with something positive, a very benevolent approach, to be interested in what people are doing, to understand why people do it that way, do it that way, and sometimes we see a risky behaviour and try, if you want, to arouse the person's adhesion by saying, to make him recognize, well yes, I'm working in a risky situation and I'm looking for a solution with them. So in fact, that's what we call the security meeting. It's the next step, once you've deployed golden rules, you've put rules in place, etc., it's really how to make sure that people adhere to these rules. I'll give you an example, Secure Culture, when you're at the first stage, it's no one wearing a seat belt, second stage, it's you wearing a seat belt because you don't want to be attacked by the police. The next step, it's you wearing a seat belt because you're convinced that it's in your interest, because you don't want to have a serious accident, you want to be protected in case of an accident and not be ejected from the vehicle, so you're convinced that it's in your interest. The ultimate step, interdependence, is that not only do you protect yourself, but you also look after your peers, all those who are on board the vehicle, you're going to make sure that they are properly protected. And today, once you've defined the standards, the rules, to move towards interdependence, where everyone looks after everyone,

Secure Culture is a tool that is very, very functional. And why am I telling you about this? It's because we also have a support that allows you to make a synthesis and we're dematerializing this support. In fact, there are a lot of things that we're dematerializing because basically we're moving from the paper version to online versions on smartphones that would also you've done your security meeting, so in fact, the synthesis is what are the functions you met, which sector you were in, etc. But what are the positive points that you have addressed, what are the points of concern that you have also immediate action and long-term action. And in fact, basically, by filling out this synthesis on the phone, you can immediately share with the head of service concerned, with the HSE or quality so that they can compile all this behind, do a follow-up of the different actions. In fact, it will facilitate the follow-up work behind. And so, I think that's the project, it's more today in the dematerialization and so we also optimize it. But you see, there's more than that, there are a lot of tools that we are dematerializing. Typically, we make prevention plans when there are external companies who intervene. And there, from 2026, we're going to ask the order givers to do audits. That is, they do a risk analysis, define measures of prevention and protection respected by the subcontractor and by the people at home to make sure that the construction site is going well. Well, we're going to ask the order givers to go audit. And in fact, what was asked to me is, yes, but I want to do an audit plan with a dematerialized and the list of points to check, you see, with a thing directly on the phone. So there, we're going to try to dematerialize it, the same, to ensure a tracking, a traceability of the information. It's really going to make our lives easier. And another thing I have in mind, I believe a lot in what is called the dojo. the dojo, it's going to be... So, Toyota, you're going to spit, I'm going to be the car, I'm a little like **[P1].** But the dojo, so, I think it's going to be the next step to go even further, and especially from 2027. I believe a lot in... Training is the key. And we're not very good at **[name of the company blurred],** to be honest. We train because we have to train, but what is retained in the end of these trainings? And I believe a lot in a playful and interactive To take a very concrete example, when you're going to train people to designate a bike, designate a machine, you make them available the padlocks, the different cutting organs, you take a real machine and you say, well, you have to do the lock-out, tag-out, lock-in, tick-tag, you're going to do it in concrete, you're going to train them directly on a machine. You have the procedure, step by step, you do it concretely on the machine. And people actually retain a lot more. And so, this dojo, we're going to build it with different workshops, and I would really like to integrate elements a little more virtual, you see, you put the headset on the head to make it a little more playful, interesting, and it's a little bit a 4.0 dojo. So there, in 2026, I'm going to start working on it to be able to start deploying it on a pilot site in 2027. But there, for me, it's something that we're going to be able to make a little bit virtual, you see. I think it's the future, in a way. So, I've seen great examples of dojos at Renault, in particular. They had marked me a specific logistics dojo. So, they had a gym to train the guys, but they had a lot of space, but there was a real lift truck, and in fact, anyone, even non-logisticians, climbed on the truck to see all the dead angles. So, in fact, the guys positioned themselves in such a place, but it was super interesting.

Matteo: It was really your warehouse which was just to do the tests.

P2: Exactly. You had pedestrian alleys, you had barriers, you had the checklist on the machines, you had battery chargers, so the specific risks on charging, there was hydrogen coming out, there was a device that measured concretely to show you the hydrogen, what does hydrogen do, fire triangle, risk of explosion, you know. You say, well, it was heaven For me, who am HSE, the message, in fact, it was super easy to understand, you see. You don't have to be an HSE expert to understand all that. But it was very concrete. And it's not the ass on a chair that's a powerpoint, you see. And that's why I believe

a lot in that as the sequel. And it makes me think, I also give you another thing, we deployed some technologies. We deployed QR codes on the sites.

Matteo: Is it the firefighters?

P2: That's it, building security. I'm a volunteer firefighter, so it made things a little easier. But here, we're equipped with tablets in the pump machines. And the fire chief, when he arrives on a building, if there is a QR code, he scans it and it gives him access to plans, to risks on immediate measures. If there is a priority protected area, what are the water points? What are the specific risks? Fire stability of the building? Are the fire poles there? Are they good? What are the accesses? On all the HSE sites, we loaded a maximum of things, but even up to give the access code to unlock a portal. And the QR codes are accessible from the outside. At midnight, on a day of the year, it starts a fire, they have access to everything. And I think it's a top solution. It's called Batifire.

Matteo: Ok, super interesting. And yes, compared to what you were saying about the projects, to make it fun let's say, the training, I know that there are a number of companies that use social media, like now everyone uses social media, to make sure to share videos, etc., in an interactive way, a bit like what you were describing to me about the week of security, in the end. But typically, instead of scrolling on Instagram, TikTok, etc., it was really professional social networks, on which we had very concrete videos, where there were people from the trades, operatives, who explained certain situations, etc. So that's a bit of a bottle at the sea, I don't know if it's going to be a big project, but it can, in terms of playful interaction, not be interesting.

P2: Well, listen, I do it a lot on LinkedIn. I do it a lot on LinkedIn, because I like it, there's less bullshit on Facebook and all the rest. But it happens to me regularly, to have this or that video followed, or this or that publication, in fact, to my HSE network, from **[name of the company blurred]** and **[name of the group blurred],** to tell them, well, look. And conversely, I often go on YouTube, to look for very concrete videos. So I have an example in mind, but the Atex **[Explosive Atmosphere Directive]** problem, you know, the explosive atmosphere, when you have emanation of solvents, linked to electrostatic, to static electricity, you can have an explosion. And in fact, there are very, very good videos, where, for example, you have someone coming, there is a spill of solvents, or transfer from one cubic to another, it is charged in static electricity. The guy comes in with a rag, certainly a lambda rag, to clean, because there must be drops next to it, in fact, and the fact of rubbing, well, it blows your mind. So the video is very talkative. Or another example, we had the fall of an elevator truck from a quay on **[name of the company blurred].** We thought that normally, the driver arrives, he gives his keys, the keys are supposed to be put in safety, on the door, the door of the quay is open, or in a closed key box. So that's the standard we put in place. In reality, it was a small basket in the logistics office, the drivers put their keys, so accessible. The guy received his papers, because they were made in advance, it was not finished, he got his keys, he got in the truck, in the middle, in his truck, he left. In fact, there was still two pallets left. So the driver fell out of the quay. Well, more fear than harm, he gets by, but we almost had a death. And so, in fact, we looked for a technical solution to block the quay truck. We found it. I went to see the private sales site in the **[name blurred],** because they have warehouses, they have developed a solution, the GMR Safety, which is a good technical-economic compromise, because it blocks the truck, but at the same time, there is no civil engineering, so you see, it's pretty good, their solution. But we had to convince the group, because it's still 6,500 euros per quay. Well, we have, I don't remember how many, 38 quays, I think, from memory. So that's a big envelope. And in fact, it's **[The CEO]** who did it. He was on YouTube, he was looking for videos of trucks falling out of the quay. And in fact, he showed at the ExCom, so we had prepared the summary slide with the solution, the costs, the projection, the three-year plan, and in fact, he just showed a video of a truck falling out of a quay. Or two, I think there were two videos. Ah, well, they signed right away. There was no debate.

Because in addition, the video, he chose the right one. And that's where I think social networks are great, because you have access to thousands of examples of accidents or risky situations that end up more or less well. You have to choose the videos that you project, but it makes it easier to convince. Moreover, in the rules of gold, the training support of the rules of gold, when I talk about the lockout-tagout, the consignment of work equipment, in fact, I take a video of... I think it's in Quebec. They have a prevention organization in Quebec. They made this video. You see a guy getting crushed in a machine. But it's hard. It lasts 45 seconds. The guy gets crushed. He has a head of cross. There's blood everywhere. It's disgusting. Before showing this video, I always warn. But we left it in the training module because there is no better way to convince. Today, with everything we see on social networks, they share a lot of things. For HSE, to find example videos, it's super interesting.

Matteo: I see. I imagine you must have screens in common areas, typically in dining rooms, things like that. Could you show this type of video in common rooms?

P2: It's tricky because... I'm not going to show them a video of a serious accident in the dining room. The guy is eating, he breaks a nut, he pauses, he sees an elevator car that crushes a guy. It must be in a small circle, animated, discussed. We also warn people. I'm going to show you a video. There are videos that are... I think they see them in a certain way. I don't know what they scroll on.

Matteo: By themselves, you mean?

P2: Yes, by themselves. I don't know if it's because it's the AI that detects that I'm HSE. I see guys falling, I see... I see firefighter stuff. I think they detected my profile. I don't see putting this kind of content in dining rooms. However, well-targeted during specific training with a time of exchange. What could we have done differently to avoid this accident? What do you think? That way, you arouse the question, you arouse exchanges, you arouse debate, and it allows us to make the link with our rules in force. It's like any communication tool; you have to exploit it. That's it.

Matteo: Very clear. It's really a complement in your vision. Whether it's the digital tool, social networks, etc. It's a complement, a physical presence to a discussion.

P2: That's it. I have another example in mind. We deployed a fire permit training module. You know, when you have three hot spots, you have to do a risk analysis beforehand, deliver a fire permit. I allow you to disk, mill, weld up to a maximum of 16 hours, because I do surveillance for two hours. There are very good videos about fire departures, because the guy is disking, milling, he's doing nonsense. These are very concrete examples that we can share. There are good examples. Very good examples. I'm thinking about it, but my friend from the quality department made a video, because they did the safety week last week, and he made the clients intervene and they made a video that will be viewed by all the group's collaborators.

Matteo: If you have his contact, I'd like us to discuss it.

P2: His name is **[name blurred].** He's the quality director. The safety week, we've been doing it since 2022. 22, 23, 24, 25. We did the fourth this year. It's the first year they did the safety week. They made a pretty good video because there are clients who intervene, there's **[name of the client blurred]** in particular, there's **[The CEO]** who intervenes, there's him, **[quality director],** to remind the importance, the quality, etc., the good practices, to show the impact of the client, how our client perceives the quality of what is made by **[name of the group – blurred].** It's pretty good what they did.

Matteo: Is the video on LinkedIn by any chance?

P2: No, because they didn't have the authorization to put the rights to the image. It's a mess. They do internal viewing. But hey, they can show you a bit or talk about it, but behind the rights to the image, it's a mess. In health and safety, I don't ask myself too many questions. But it's still internal. Although we made a video once, we had published it on LinkedIn as a result of the safety week. We had to do a post. We do a post every year, but I think there was a time when we took pictures of videos from **[name of the company – blurred]** on LinkedIn. If you ever need us to go deeper on this or that subject or if you want examples, I'm at your disposal. You have my phone number too. Yes, don't hesitate to call me if you need elements to illustrate. I can give you whatever you want.

Matteo: It works. Anyway, I don't do anything. I don't publish it to anyone.

P2: Yes. We have nothing to hide. We have nothing to hide in HSE. If it can be used elsewhere, frankly, as much as it serves. I'm not at all in the protectionism of what we put in place. On the contrary, if it can help elsewhere. I contacted my counterpart on the Renault Trucks website in **[name of the site blurred].** I went to see him on LinkedIn. I sent him a little message. I said, hi, I see you're the security manager at Renault Trucks. I'm at **[name of the company – blurred]**. Can we get in touch? I have a lot of questions to ask you. I would like to know if he has set up a dojo and if he agrees that I bring the whole HSE team to show him a dojo. But you see, most HSE have a rather open mind. On the contrary, if it can be used to facilitate the work of the neighbours, in practice, to avoid the actions of work, there is no competition in HSE. So go ahead, do what you want, there is no problem.

Interview of the third participant P3: communication officer at the national institute for security research

Matteo: Thank you for taking the time. If you don't mind, I'll start by introducing myself.

P3: Yes, of course. I hope I'm the right person to answer your questions, so you'll tell me.

Matteo: I think so, with what I've understood from you, I think so. My name is Matteo Cabut, I'm a student at INSA Lyon and Polytechnique Turin. And in this context, I'm writing a research paper on company security, and in particular, how we can use social networks to improve company security, to send messages, etc. It really aims to make a panel of possible applications, advantages, disadvantages, etc. And by social networks, it's very, very broad, we mean all the applications that are connected to the Internet and that allow sharing content. And in this context, I'm doing a number of interviews to get feedback on security issues, see how we can apply social networks, the advantages that it can have, etc.

P3: Very good. So, for my part, I'm at **[name of the research institute blurred]** in charge of slightly transverse topics on risk assessment and everything related to work accidents. I'm based in **[name of the city blurred],** and we do, let's say, more of the communication, for the general public, of employees. And on the **[name of the city blurred]** site, we have colleagues who do more research. Okay. So, there could be colleagues, researchers, at the moment, who are working on everything related to messages and other things, but I've been thinking, and I haven't found any in their current research projects, but there were, at one time, topics, but since communication evolves very, very quickly, it's true that it's not obvious that research topics that were carried out 10 years ago are still relevant today. At **[name of the research institute blurred]**, to disseminate the messages and productions that we can do, we use different communication mediums, either via the web, we do webinars, technical days, in person or remotely, on dedicated topics, we also do written press, and in fact, within the companies, to talk about prevention, we provide one of the supports, which is perhaps a bit vain, but which I find quite effective, which is the poster. Okay. So, we have posters on different topics, different themes, and the goal is that they are hung up in the companies, but that they serve as a communication support, in fact, through the visual message that they will convey. So, we have a whole collection of posters, which can be abstract, which can be funny, which can be more serious, around a security topic, which can be individual protections, which can be protectors on machines, well, land licenses, there are a lot of different and varied topics. So, for us, it remains a tool for communication within the company, since the goal is to talk to the employees about a message, and for it to interrupt it. Okay.

Matteo: So, if I understand correctly, the role of **[name of the research institute blurred]** is really to facilitate the culture of security, let's say, in the companies, so it's the companies that come to you with a problem and you help them, is that it?

P3: So, yes and no, it's a little wider than that. We are a research institute, so we have about **[XXX]** employees, and on our site in **[name of the city blurred]**, there are really research laboratories, so on

very technical topics, noise, acoustics, vibrations, we have psycho labs, we have labs on musculoskeletal disorders, we have labs on lamia, we also have animals to do toxic tests, so there you go, very varied. On the site in **[name of the city blurred]**, we are going to be more on the part, let's say, communication, and our privileged partners are still the professional federations, since we are going to work to address as many as possible.

So, professional federations, ministries, professional associations, representatives possibly of unions, social partners in companies, and we also work with the CARES Act, which are the agents of control of companies on prevention issues. So, the CARES Act is an emanation of the National Health Insurance Case, so social security, there is a professional risk branch, this professional risk branch has regional agencies, and on the subject of work safety prevention, there are CARES Acts that are in contact with companies. So, a company has a need, a problem, it will normally address directly to the CARES Act, which will accompany it on the ground, and possibly use our productions to help the company to mature on a subject.

Matteo: Ok, so there is really a link between research and the operational that is done.

P3: Yes.

Matteo: Ok, and so, in relation to that, have you seen an evolution of companies on their way of communicating within the framework of the culture of security? Has there been, what has been the history, and what are the dominant methods that are used today?

P3: So, the question is within the companies.

Matteo: Yes, that's it.

P3: Ok, so within the companies, in fact, everything will depend on the nature of the company's activity. Companies that will be, let's say, in the tertiary, the service, but rather sedentary, with a computer. Communications will be done a lot via the internal network, possibly small webinars, information campaigns by internal social partners of the company. Newsletters, with a security subject. For example, when there has been a job accident, it is often the occasion that companies take to talk about a subject, or because there is a national campaign, and so they will broadcast the messages of the national campaign locally, but via their internal network. On the companies where, for example, there are people who are at a distance, I think people in the building sector, this is what is most often visualized, they are far from the headquarters, they intervene with clients on the roads, etc. Often they use applications that they have also been able to develop internally. For what I have been able to see, there are small applications, for example, that work with a photo of a job situation that may seem dangerous. The employee takes the photo, it is sent to the preventer, to the team leader, and then

there is a treatment that is done, and everything is communicated by this small application, via the employee's personal phone.

Matteo: So this is more at the internal level, right?

P3: Yes, internal. And then, it remains a social network, but internal. And then, they do a lot of security guards, so it also works quite well in everything that is going to be industry. It is a moment at the beginning of the week, every 15 days, where there is a group of employees to discuss a security issue. Okay. There too, in industry, they can, on large industrial sites, use these famous small applications to transfer messages Internal. Public networks, Insta, Facebook or others, to my knowledge, are not used for companies to speak to their employees. They would be more easily used for a branch security agency, a professional federation, to communicate to companies. Okay. But in internal business, to my knowledge, these external public networks are not used.

Matteo: And can there be, because it seems to me that on LinkedIn, there is a group creation function, can there be thematic groups dedicated to security within companies? Is that something you've already heard about?

P3: So, it will exist in large groups. Yes. For example, GDF or others. I know they have some, but in fact, they are rather groups that are not around a company, but rather around an activity. So, people who work in nuclear, people who work in the electricity sector, in water treatment or waste management, they can create this group, but suddenly, it will be groups for company preventers, for security managers. In my opinion, these groups are not open to others, and others do not join them. These are really thematic sectoral groups so that people in the sector do not talk to each other anymore.

Matteo: In terms of sharing good practices, whether it is the security managers, etc., it is still quite fluid, if I understand correctly. Even if we are in groups or competing companies, there is still sharing of information and good practices.

P3: In terms of security, in general, it is not something taboo. On the contrary, they are looking for collaborators to be aware of new ideas, new techniques. They can also participate in salons. You know, salons dedicated to security, on transport, it exists, on preventive measures, more focused on individual protections, where the equipment also exists. These are the groups that will meet.

Matteo: And precisely, in terms of the ministry, because you said you also work with ministries, have you seen an evolution in the usage of the way in which you communicate security issues with more traditional methods and perhaps a little more digitized today?

P3: So, digitized, yes and no. So, I know that at the level of the Ministry of Labour, there I am part of a group on the fall of heights, for example. There is an internal collaborative work network, but it is open only to members of the group. Then the project is to think about whether to evolve regulation or not and possibly to work on communication campaigns. So there, the Ministry of Labour has its place in the communication campaign part. So they are oriented, because they have already done it, on TV campaigns, radio campaigns. OK. But in my opinion, no campaigns via social networks, I am thinking. X or others, I don't remember. I admit I haven't looked. He must have a friend, he must have a friend, but do they use it as a means of communication? I don't know. And for once, it would be public. Yes, I am looking. Yes, they communicate via X, for example. So if they have X, they must have Facebook too. A priori,

Matteo: yes. A priori. And at the level of companies, do you see a utility or possible applications, precisely social networks, in a very broad sense, to help in the culture of security, for example, the fact that we can take videos, that we can make colleagues interact in very concrete situations, etc. Do you see a potential, in terms of development, or not necessarily?

P3: It could be no. It's very broad, as you said, Teams is one of your tools. Yes, companies use Teams to hold meetings, but it's not... It remains a meeting tool, in my opinion. Meeting, possibly collaborative work, but not tools used to raise awareness, information. Everything that is going to be a training tool, companies like to formalize what they are going to give as a descending element. So it has to be framed. There has to be a program, whatever the tool, but there has to be an intervener, a program, a theme, a duration, to have a training attestation. They can use Teams to do that, because they are large-scale communication tools. They are going to do webinars, that's possible. But to use the tools to make them interact. Yes, for example, with the application tools, I was telling you, there is a problematic situation, we are going to take a photo, it will allow someone to be informed and to have a treatment message of the information. It can be done on a phone, it can be done on a tablet. So on the tablet, the management can send communication messages on statistics, on a key message, etc. So that exists, it depends on the company's maturity and the will they want to put in the subject's animation. But when you say interactive, for example, I don't know, with quizzes or that kind of thing that could be proposed? You see, it already exists. So there are many things that exist and many things that are used. After, finally, whatever the tool, the important thing is the message and how it is adapted to the target. So employees, team leaders, such and such workshop, the more personalized it is, the more the employees, whoever they are, will feel concerned.

Matteo: And precisely, in this personalization of the message, the social networks that are now used by almost everyone can help in a certain way, can make the message accessible, very concrete, very...

P3: So, you were talking about LinkedIn earlier. LinkedIn is still a personal account with a professional target. So, my company would like to communicate with me through LinkedIn, it would bother me. Because it's a personal account. Like Facebook or like Instagram. After, there are companies that have created accounts asking their employees to subscribe, especially at the time of COVID. Because it was a way to keep in touch, sometimes outside the company's tools, which were not necessarily accessible, that's it. And to have a small collective at work, but to finally talk about a subject that is sometimes out

of work. You see? For example, we had set up a virtual coffee break, so every day we would meet on our mobile phones, because it was run by the boss, but outside the framework it was still a bit of work, and we talked about the rain, about our boredom, about our problems, so you see, it remained a voluntary act, it was not mandatory. So, social networks, according to their nature, when they are personal, normally the company does not have to communicate through this personal tool, since we enter the field of the private. So, there is a limit to be found, and indeed according to the tools, there are things that lend themselves or that do not lend themselves.

Matteo: Ok. Very clear. And there is also a tool that I heard about, that you may know, whose editor is RedOnline, which allows you to monitor European, national regulations, etc. Do you know the tool to tell me a little more about it?

P3: No. But it may be more very specific things, very professional, or even internal to companies, more than the classic networks, like Facebook, LinkedIn, Instagram, TikTok. Yes. We have watch tools, but they are proposed, in fact, we are users of a tool that has been bought or developed, possibly, by our documentary service. And in fact, either we can request live, or we can create a newsletter, or we ask them to do it for us. But for me, it is not a watch tool for culture, because it remains only the information coming down on criteria that are not always personal. We receive the newsletter of information in Europe, and once out of ten, nine out of ten, I don't read it, because I read the titles, and then I throw it away.That's not what will allow me to be alert to prevention, to safety at work.

Matteo: And precisely the fact of potentially broadcasting small videos in a social network format of accidents, work, etc., can it attract or arouse curiosity to be interested in a safety problem, for example?

P3: Yes, it can. But it has to be well targeted. If the company broadcasts an accident on a machine without accounting services where there are only computers, they will feel not at all concerned. That's why I say in a well-targeted way, who we address and what message we want to convey. But small videos are becoming more and more popular because people are generally less readers. So the visual works well, and short formats and a bit catchy work well, even if it brings additional information. But already as a topic of attachment, yes. Then, on YouTube there are a few that are also made by serious people. We have to see how the company can relay it. Because the idea of waking up and prevention is really to allow exchange. If it's just information coming down, it's like when we watch an ad, we put it away, we pause it, and then one day we may think about it. If we are not asked to come back on it, to bring elements of reaction, or as you said, to have an exchange, just information coming down, it's useless.

Matteo: So as part of a training, we can use in addition small videos to make people react?

P3: Yes. Training, or even a webinar with an active chat, even three quarters of an hour, we can also mobilize people. After seeing the registration conditions, it's mandatory, it's not mandatory, it's on time. Because if it's on personal time, people won't necessarily come, unless it's a matter of interest. Otherwise, it has to be on time, it has to be integrated into their activity. That's for sure.

Matteo: In the interviews I was able to lead, in the CODIR, they had to make decisions on security, and the security director had shown a YouTube video showing an accident, and that the CODIR was skeptical about making these investments. Once they saw the video, they signed right away. Because it's shocking, it wakes you up.

P3: Yes, yes, yes. It's an element to convince. It's part of the toolbox, of course. Because in pedagogy, you can see that each time there have to be exchanges, interactions, so that the message really takes hold. Okay.

Matteo: Very clear. I have no other questions.

Interview of the fourth participant P4: communication officer in the plastic industry

P4: I apologize. So, just tell me, explain your studies a little bit, quickly, and then we'll get to the heart of the matter.

Matteo: So, I'm an engineer at INSA Lyon and polytechnic in Turin. And so, precisely, in relation to this double degree in polytechnic in Turin, I have to do a research paper on the issues of industrial security. As I am an industrial engineer, I have to see the different methods of communication, and in particular the possible applications of social networks to communicate the security rules well. So, whether it's the advantages, the disadvantages that social networks can have to help in this communication.

P4: Ok, so, in relation to what you want to highlight, is it more on the inside, or is it more on the outside?

Matteo: So, in fact, either, in my basic scope, there are both, but the first interviews that I could see, in fact, we would rather focus on the inside.

P4: So, we would rather be on the inside, more than the use, because I think that's your question. For example, traditional social networks, typically TikTok, Facebook, etc. It can be a possibility, but from what I understand, it's more difficult to set up for questions, in particular, of private life, etc. And then there's this notion of cybersecurity. So, in the end, it can be interesting, in addition to the questions you just asked me. So, I hope I can answer your questions and give you all the answers you're waiting for. And then, I think that, in addition, it can be interesting for you to talk to **[IT manager – name blurred].** I don't know if you're going to talk to him or not at all. He's our IT manager, and he's very, very, very accessible to security. So, it can be an addition, it can be interesting for you, in relation to everything that is, precisely, means of communication, because he also manages... We're going to use the applications, but behind the tool, it's set up by IT. Typically, a Teams, a Microsoft Office, things like that, it's set up by IT. And then, it's a tool that we use to share documents. So, it can be interesting, I think.

Matteo: Well, thank you.

P4: You're welcome. I'll look at that.

Matteo: So, I had a few questions.

P4: Yes, of course, go ahead.

Matteo: So, in fact, already, the definition that we give to a social network, it's very broad. In the work that I put in, in any case, it's to say, in fact, it's an application that allows you to share content and information between people using the Internet. So, it's very broad. And so, precisely, I wanted to have a little list, even though I was able to have a first draft with **[security director – name blurred]** and **[the CEO – name blurred],** of social networks that are used in **[the group – name blurred]** for the communication of security.

P4: So, you see, we can even go a little bit like... So, if we go to social networks, you see YouTube is also considered a social network because we can exchange. Well, on the same title, then, we have Teams. Teams is a pure and internal social network. And we can also have our Intranet. So, it's called the **[name of the intranet blurred],** but it's with SharePoint. So, it's associated with Teams. And finally, the fact that we can comment, exchange, well, it fits, even if it's not really activated. People don't really comment on our articles. And so, it's not necessarily used. But it's still a social network too. So, basically, our Intranet allows you to just share information, communicate with collaborators. But it can be used as a social network, because we can actually comment below, write to each other, authenticate, make arrows, say this person. So, it fits in, yes. And then, I want to tell you, we are in the means of communication. We only have that. We had for a project to develop an application. But suddenly, it stopped for the moment. Because, in fact, if you want, the problem we have today is that our collaborators in the workshop, who don't have a professional phone, don't have a professional computer, don't have access to information in the same way, at the same time. You see, for example, we're going to make an article on tomorrow, Pink October, dress in pink. Well, on Intranet and on Teams, you can send a message, you can say to people, quickly, dress in pink. The staff at the workshop, well, you have to make a poster, you have to create it, you have to print it, you have to go and display it. So, it's much longer. And the idea was to develop an application. So, that exists. I'll give you, I think I have two or three names, I can find them for you on the Internet, in case you want to go into your file. And, in fact, if you want this application, you download it or not. So, that's up to the collaborators to choose. And then, you have access to information. You can also interact with colleagues. You can make work groups. For example, you can make project groups, but also personal groups. If there are people who love music, you can make a music group and meet up. So, in fact, that was the idea. And you have Loli. So, wait, I'm going to find the names.

Matteo: So, that's on the personal phone, because the operators don't have access to computers, phones.

P4: Exactly. So, in fact, it's only at the level of managers that there is... It's all the people. So, not necessarily managers, but all people. Yes, overall, it's going to be team leaders. It's going to stop. In fact, that's it. It's going to go down to the team leader. And then, you have special collaborators, who are going to be quality, things like that, or logistics, who have a pro phone or a pro computer. But a press operator, for example, will not have a pro computer or a pro phone. And they don't have it because there is no utility to what they have. And in addition, since he is focused on his machines, on the management of his production, it would even be... A distraction. We could put him in danger. Because if he is distracted, if he is not careful, there can be an accident. And also, in terms of profitability, we are not good. And on the other hand, that's why this application could have been interesting for them. Because, as a result, the collaborator is not allowed to use his phone during production hours, but he can take his personal phone during his break. And there, in these cases, he

can connect and take some information. Or in the evening, he can always have access to his work application to know what is going to happen tomorrow. Is there a football tournament? Things like that. Or go and propose an activity. Or exchange with a colleague if there is a problem. So, in application... So, I did some research. I had Stipple as a supplier. And so... Wait, there was another one. Well, you have a lot of them. You have a lot of them, but there was one that was interesting.

The... Yes, the... The... The... And that's it. So, these are two... Two that I had retained that were rather interesting. There are a lot of them.

Matteo: I'll dig into it, thank you. And why didn't you put them in place?

P4: It's because... Everything that is... Since it's a personal phone use, in relation to security, in a way, when you're a pro, there can't be an exchange. That is to say, it's illegal to exchange information from your pro to other personal phones. You see, it has to stay... For example, if I take pro photos, normally, it shouldn't end up in a friend's house. When I have a meal, I shouldn't show them. Normally, it's... You see, that's it. In this idea of security. And in fact, there's this whole notion that has to be taken into account. It's how we're going to manage the fact that, well, suddenly, we authorize... We authorize these applications on personal phones, but it's still pro. So, there are a lot of people who do it. You see, Sanofi... I have a friend who works at Sonofi. They have an application on their pro phone, Sanofi, internally. And it works very well, but because... They have limited, in terms of communication, to things that are very... Very... Let's say... Well-being at work, things like that, and not too much pro information.

Matteo: Yeah, I see. Well, me, since I'm an intern, I don't have a pro phone, and in my personal phone, I use... I use **[name of the app blurred],** which you may know, which allows you to have two different interfaces, between the pro and the personal. Because for interns, they don't give you a phone.

P4: Well, wait, I'm taking notes, because I don't know if **[the IT manager]** knows... Go ahead, say the name again. It's **[name blurred].** Because, suddenly, we don't have a domain name... I mean, we don't have a pro email address for workshop collaborators. Because it's a cost, you know. There's a cost just for... But then again, it's a choice. I mean, if we get into this approach, we're going to have to buy these famous addresses, we're going to have to... So, suddenly, it could go into this thing, it could work. That's it, that's very good. That's it. And yes, so, precisely as the operators, they don't have access, let's say, to everything that is digital, it's rather the communication that's going to be done, it's rather in terms of posters, workshops, training, etc. Basically, we have several communication platforms. We have, for everyone, we have TV screens in the breakout rooms, a little bit in the welcome hall, but the welcome hall, for me, it's more of an institutional communication. It's not yet in place, because it was just put in last year. So, there, already, we put information, we do it step by step. But in the breakout rooms, we communicate, well, you see, we did a communication campaign on Industry Week, so that people are aware. So, basically, we put all our campaign on the screens, but we also put posters, we print posters on hard communication spaces, that is to say, you have walls marked communication spaces, and there, HR put up posters that we made, that's it, all general communications, etc. So, that's our

communication support. Then we have a magazine that is published four times a year. It's an internal magazine, so we do it digitally, we send it by email, we put it on our intranet, and we print it only to collaborators who don't have a Mail Pro address. So, like that, at least they can also read it. So, there's that. So, wait, I'm going to go back to my supports, so I don't forget them. So**, [name of the internal magazine blurred],** the intranet, so...

Matteo: A newsletter, maybe?

P4: So, from time to time, we don't use, you know, the newsletter, I don't know if you know, but normally, you can use, they call it a main tip, distributors, basically, you send a big list of broadcasts, you structure your newsletter. When you receive emails saying, enjoy this offer, well, in fact, it's often sent in bulk, it's created on a software, and that's a newsletter, in fact, sent in bulk. We don't have that software internally. We're going to do either an email, or we're going to create a little design, yeah, we're going to make a PDF, send it by email. It can be really... Okay. But there are small newsletters on really specific information. You see, I don't know if **[the CEO]** told you about it, what, **[name of the group blurred]**? So, in fact, we've grouped up with another structure. So, in fact, following this reunification, basically, we made newsletters to follow up, because it was a little different there. It wasn't just about **[name of the group blurred]** it's brand new, it gives a new momentum, groups, etc. So, we really made newsletters for that, to follow the synergies, and that's it. but we call it “flash infos”, for the internal jargon.

Matteo: And because to set up a newsletter, you really need to have this software?

P4: Well, we really want to make things easier. Well, it's especially that we can do it in any format, in any case, it's sent by email, but it's true that it's better for a big shipment, yes. You see, for us, I think we are limited to a certain number, especially what is meetings, shipments. If the group grows to **[xxx]** collaborators, I think we are stuck for the moment. I couldn't send emails to **[xxx]** collaborators, you see, there are cases to go through, but hey, that's IT. We also have something that is very interesting, so we don't use it all the time so as not to overdo it, but it's super, super striking, computer screens. In fact, you should know that it is IT that manages our screen backgrounds. Initially, they can set you a screen background. So, for the week of security, for example, because we organize lots of events, you know, throughout the year, on the week of security, we had made a specific screen background and we had asked IT to put it on all computer screens. So, for those who did not turn off their computers, well, of course, it was not up to date, but when you come to turn off your computer because there is an update, well, you discover, you discover this little display and it's true that since it's your work tool and you inevitably come across your computer at the beginning on your screen background, you see it. So that's quite interesting. Then, we have e-mails. E-mails are a means of communication, clearly the most used. Then, internally, we have the info of the month. Here it's more, it's a meeting that is led by the management where we give the main information, everything that is business, everything that is finance, everything that is party, production, etc. The arrivals, the promotions, the big events that will happen in the month. So, this is a regular meeting once a month where we invite, not everyone, we invite the co-directors of the sites and all the people from **[name of the company blurred].** That's it, globally. And then, we will have, in communication, it will be the communication events we can use to

send messages. But that's it, it's separate. In support, in fact, it's really everything that is Intranet, Le Magazine, Teams, things like that. Is it clear for you or not?

Matteo: Yes, it's clear, thank you. And is it in the training or in the workshops that are done in relation to security, is there the use of YouTube or what to illustrate specific points or even social networks in general? Not necessarily YouTube, but do you know if there are these applications possible?

P4: So, what do you mean when there is a Lambda training?

Matteo: Yes, when there is a training, whether in class or in class context or typically in workshops, can we show for example YouTube videos to raise awareness, to shock maybe a little, even if the term is a bit strong, the operators on a specific subject?

P4: Ah, yes, we can. Typically, we did the week of the handicap there and suddenly we had built a whole workshop of one hour with several exercises of awareness including a moment we used, so I don't know if it really answers your question, but we used a YouTube link that made ambient music, you see, because we had to make a game with headphones, noise, so we use that. I also use YouTube as a non-repertory link to sometimes post videos to be able to broadcast them afterwards in meetings or typically in workshops last year where I had created specific sounds, I had put them on YouTube as a non-repertory link and then I just had to share this link with people who needed it. We made a video about integration, so yes, we use YouTube but it's controlled, that is to say we give the link, we make sure, that's it, it's not… and on the other hand we have YouTube as an external link too, but overall that's it. So does that answer your question completely or do you want something else?

Matteo: Yes, that's good.

P4: Don't hesitate if I'm next to the question.

Matteo: No, no, no problem, that's it. But what I understand well is that whether it's social networks or all the support, it's more of a support on a global message of a training, etc., where you have an intervener who can bounce, react to people, etc., it's more of a support that can't be replaced, what I mean.

P4: And you see, on the other hand, there's always, in relation to this security, we had an intervention from a client that during the week of quality, which was last week, yes, because we have a lot of weeks, we made a video, in fact, we made several videos. We made a video where **[the CEO]** was speaking, by the way, a specific video on quality, so we put it on the screens, it's broadcast, in fact, it's shared, there's a link that's on SharePoint and everyone shares it to broadcast it to their teams, that's it, everyone has it on their computer. And there's also, we had **[name of the client blurred]** who intervened, I edited it

to transcribe it to the night teams and in fact, all of this, each time, to share the videos internally, without going through YouTube, to still ensure a maximum, because we never know a maximum of security on these subjects, everything that is client quality, when we go in the production processes, it's quite secret stuff, so there, we avoid everything that is a bit related to the external. So, it's more complicated to get them through because, you see, even with WeTransfer, you have to be careful because there can be a loss of data, you see, normally not, but it's still, you have to, that's it, you have to be very careful about what you share. With WeTransfer, it's a bit more secure, but hey, it's the same. It's never, we never know, in fact, and suddenly, it's true that sometimes it's a bit, it's a bit the difficulty that we have because, as soon as you're on super heavy videos, to share them with you in all security, without using an external system that can put you a little at risk, well, it's quickly complicated, so, or after, you have to pay subscriptions for free for a video, that's it. But that's a problem.

Matteo: Are there other problems about using social networks?

P4: So, we talked about that, we talked about the pro-personal side, etc.

Matteo: Would you have other problems about using social networks to send messages, good security practices, etc.?

P4: So, it's not necessarily to send practical messages, but who says social networks on external internet? So, we're deriving a bit, but you see, LinkedIn, we're going to encourage the internet to like, etc. But behind, you're never at risk, you have no control of your communication. You see, it's more that, but we're more in the image, so it doesn't really answer the security part. It could be use. Yeah, no, after, no, let's say, the risk we can have is sometimes, you know, we're brought, today, everything is digitized. In fact, I think that's the real issue today. Everything is digitized and we want to be fast. How do we do to be fast? We go to the workshop, we have a machine problem, we take a picture, we send it, we say, look, I have this on my machine, your team leader, he may be at home because, you know, sometimes compared to the competent person who can answer you, she is elsewhere, you send her a message and then suddenly you have your personal phone, you take a picture, you send it, that's it. It's always this use of the personal tool that comes out, in fact, that comes out of context and, you see, it's often WhatsApp, the teams, but WhatsApp is not professional. So you can't see if there are new practices. There is no control. We agree. But at the same time, WhatsApp is super practical and everyone has it. So that's a challenge. I think that WhatsApp, I really think for all societies, there is no risk in itself, there is no risk right now, but for me, for societies, WhatsApp, it can be complicated, yes. More generally, everything that is not, I don't know the word, but that can't be monitored or moderated by the company. The best security is to apply everything, to use the tools put in place, to use all the tools and only the tools put in place by the company. Or afterwards, if you want to put an anti in place, to get closer to IT to always be in touch with cybersecurity and all that.

Matteo: Would you see other advantages in using social networks, etc., for security? So beyond the fact that it allows you to go fast, as we could say in the way we take the photo, etc. Would you see other advantages to that?

P4: To create links. To create links. Yes, clearly. To create links. In fact, the fact of having the information a bit instantaneously, on a daily basis, the feeling of belonging. In fact, overall, it still creates a feeling of group, things like that. I see that a bit in these advantages. Yes, overall, that's it. In the sense of engagement. If you want, engagement, to feel like you belong to the company, when you feel concerned, informed, quickly, not having had a drink in the bar on one side of the company and then, that is to say, learning at the table on the other side, the information, you see, it's still more pleasant. And in fact, often, you get it more quickly through social networks. So, in fact, that's it. That's for sure, yes. And to come back to security, you see, because you were telling me earlier about all the information about security. So, we are more about IT that will give you this information. And I really think you should contact them. It can be really interesting for you. They do awareness campaigns. They will send us fraudulent emails. They will send us all that to see if we have the right reflexes. Do we know well? Do we know well? You see, we were contacted supposedly on Teams precisely by a person who needs help when in fact it was not at all a fake thing. So, to have... or wait, it was an email. Because now Teams also sends you emails like what? Have you seen a Teams? There is a story like that. When we didn't see enough, when we didn't see everything right away, etc. And so, it seems to me that this was the campaign and suddenly it was necessary to point out that it was a fraudulent email not to be fooled. So, we are very sensitized about this. We made an escape game on cybersecurity. So, regularly, in fact, all the new ones now have systematically an escape game of sensitization on cybersecurity. So, that's it. And then afterwards, we try to do... You see, IT has made a game to make it a little more fun because always saying be careful, be careful sometimes it's a little harder to get in. Indeed, maybe social networks can also help in the sense that it's fun, everyone knows, everyone is addicted to that, unfortunately. That's it. Yes, but it's... So, afterwards... And you see, then, in the idea of the application, when you share a photo because you did a training, you often see the SST training, I don't know if you have the opportunity to do it or not, it's quite fun in the end. You see, we laugh, it's still a training where you learn things but it's rather relaxed and good children and suddenly, these trainings, well, behind you share the photo internally, well, it comments and that's where it creates links, that's where it creates memories, that's where you say ah, well, I'm good in this company, it's still nice. You see, it's all that. That's it. It's the advantage of social networks but also, that's it. And then, I would say a disadvantage is that it's time-consuming, social networks. You see, when you spend time on Teams answering tac, tac, tac, tac, there is no more another question and so on and then, you take time to answer, sometimes a call goes faster. Yes, that is to say that, well, it's more about usage but having a little step back on the use of social networks. That's it. That's it. So, in fact, what is interesting is to set up a framework of use, that's it, a framework of rules, a process. You see, sometimes, is the request really urgent? Well, suddenly, no, you send an email, rather than a Teams. That's it, it's things. And then, all that, it's going to go into, because if you don't do the right practices, behind, a person can be overloaded, under stress, not make the right choices, and suddenly, open a fraudulent email, because suddenly, under stress, that's it. It's things, in fact, it's not necessarily security, in fact, sometimes, it's on details, but there's a whole context to take.

Matteo: And even overload in terms of mental health at work, etc.

P4: Ah yes, yes. Mental health is the issue of this year. I don't know if you heard, but it's really the problem of this year. In any case, they put a lot on it. But it's super interesting, by the way. So wait, tell me your problem, because if I try to answer well, I want to answer well. Tell me again.

Matteo: It's actually seeing, so it's hyper-exploratory research, it's seeing how we can, possibly or not, use social networks to improve security, so in particular, to transmit messages well, etc. And make a list of advantages, disadvantages, etc.

P4: So finally, in the improvement of security, it's reactivity, already, on a social network, since you give the information right away. So tomorrow, you get hacked, you give the information on the network, on TMS, to everyone, you send a global message to everyone, everyone knows it very quickly. In fact, that's it. Reactivity means that when you have a message on TMS, it's usually urgent. So, in theory, you're supposed to look at a TMS, to see an email. So, often, you've seen, you've seen, I sent you an email, and you write it on TMS, that's it. So in fact, the reactivity of social networks will make that, and suddenly, the fact that you can share again very quickly, you see, too, it adds up. After that, it's true that on the internal, on the internal, we are often a little more limited. So it all depends on the means of the company and the strategy, too, of what we want to invest internally in the company. But there are companies like Airbus, all that, which must be on a level of internal security and different communication compared to us. But overall, if you have networks, more developed social networks than ours, I think you might even be able to put some kind of blockade, things like that, that make you, you might have training, what training? Some kind of, what do you call it? I lost the name. Through your social network, in fact, you can access a bit like Instagram, you know, you have ads sometimes. And there, you can access your cybersecurity training via an Instagramable intranet. I don't know how to explain it to you. But I don't know that. I imagine. I tell myself that if I had a lot of means, that's certainly what I would do. You see, apply the external marketing codes internally, typically. But yes, afterwards, to raise awareness of security, to strengthen security through social networks, if I only look at my spectrum, yes, intranet, it's going to be, it's going to be communicated, clearly. Informed, communicated, interpellated. I see it like that. I see it like that. And you see, then afterwards, I think there's a subject, so I don't know if you're going to go into it, but there's the IA part.

Matteo: Yes, I don't necessarily go into it a priori, but I don't forbid myself, let's say.

P4: Yes, I think afterwards, I don't know, but I imagine that it may be necessary.

Matteo: And we talked about it **with [P1 & P2].** And we were a little skeptical, in the sense that, basically, what he was saying was that the goal was for the person to understand the process, let's say, physically. And afterwards, in a second time, why not digitize IA? But the goal was really to understand the rules and then afterwards, why not, we can digitize IA.

P4: In fact, you can maybe do it openly. Because it will be the issue of tomorrow. No, but that's it. And see how to re-apply the codes with IA. And you see, because I see IA now, and everywhere. Especially, you know, I give courses next door. Yes, and there are master's degrees in project management and HR. So, I'm on the IA part. And when I ask them to make me an IA plan, it's Chat GPT who makes me IA plans. So, in fact, I apply it to the teacher process. That is to say, I come back to

having bought, I ordered paperboard rolls and I'm going to stick paperboards in my classroom and I'm going to put them in groups to work on definitions, to work on IA plans in groups, but to think, not to use Chat GPT. So, in the old way, cut the computers, cut the phones, cut all that, so that the first means of communication that is there, works again. And in fact, that's where we have to rethink our ways of working too and integrate IA intelligently. That is to say, it's a complement of tools, it saves us time, but in any case, it must not take the intelligence that we do not have and that suddenly, at some point, we will find ourselves in a situation where we will not have IA and how do you do in these cases?

Matteo: Thank you very much for your time. Have a good day

P4: Have a good weekend. Yes, you too. Thank you.

Interview of the fifth participant P5: cybersecurity consultant

Matteo: I'm doing a research paper on applications of social networks to improve the culture of company security. I'm just going to define what we mean by social network and company security. By social network, it's any web application that allows you to transmit information. It's really wide, it's not just traditional channels like Facebook, TikTok, etc. And culture of security is everything that is done to improve people's security. For example, in a production workshop, physically, or also security in terms of data protection, rather computer, which is not necessarily physical, but which is part of people's security. And so, in relation to that, I would have a few questions to ask you. First of all, in your work, are there social networks that are used in this context, to communicate about security, etc., about instructions, security rules?

P5: We communicate mainly by Teams, either by meeting, or by simply transmitting information directly in Teams conversations. It's only at this level, I think, from a social network point of view. Otherwise, when we talk about security procedures, it's directly by SharePoint. If we're talking directly about a device, we're going to implement a security process. Otherwise, we're going to explain our approach via a PowerPoint, like the rest of the consulting companies.

Matteo: And within **[name of the company blurred],** in your company, when there are security instructions, are there other channels used to transmit instructions? SharePoint. SharePoint, okay.

P5: SharePoint to transmit documents, and we can have procedures on it. It's mainly procedures that go through documents, not necessarily through a transmission channel. We're going to give a little global information on Teams, but we're going to have the details, and the procedure itself, we're going to have it on the SharePoint dedicated to the dedicated document.

Matteo: Okay. And are there WhatsApp groups, for example, on security, etc.?

P5: No.

Matteo: Is it possible for you to apply social networks to safety culture according to you?

P5: It can be useful to improve the security of companies, whether in terms of good practices, cybersecurity, etc. And if yes, it has advantages, could you give me a list of advantages that it can have?

Matteo: So, for example, a company has its dedicated page for collaborators, and it puts security devices there? Apart from good practices, right?

P5: It's more like, you're a company, you have security processes, whether, for example, at the computer level, on phishing, you see? And in fact, by using social networks, we're going to better communicate good practices, etc. For example, at **[name of the company blurred],** you have... What's it called? What's the name of the page? Intranet! Yeah, that's it, the Intranet of companies. You often find... You always have a security part, and there you can find both people to contact, the different poles, and you can have a bit of a context, and why it's important to have security. But it's true that, for example, when I was on stage at BPI France, I saw that there were a lot of things that were really put in place in a community aspect, and we saw that it was discussing security procedures a bit. So I think it's a good aspect, because at the beginning, I misunderstood your question. I really thought it was a wider audience, but if it's really internal, I think it's something to develop, because it's true that on Teams, we may not necessarily have the history of the whole conversation, we can lose track, and really have this community aspect, we can list, do it like a kind of forum, and in Rome, at the same time, we will find subjects and good practices, and at the same time, we can ask our questions, find key contacts. I think it can be a really interesting approach to put in place for all kinds of companies like **[name of the company blurred]** or others.

Matteo: So you're really talking about an intranet?

P5: Like an intranet, but a little more community-oriented. In the sense that we're going to have a panel of subjects, you go into the subject, and you have all the questions that have already been asked with the answers, the possibility to ask other questions, or even an aspect where, for example, there were not necessarily questions, but we talk about them, and it's like a little explanatory sheet of the subject. I think it could be pretty good. But then, in terms of social networks, using, for example, you talked to me earlier about WhatsApp, I don't know if it's really useful to use this kind of social network, maybe more. If it was for a wider audience, you can even talk about trusting your collaborators, maybe talk about good practices, for example, I don't know, on Twitter, or on LinkedIn, or other social networks a little more used, which will reach more people, because WhatsApp, it's still community-oriented, if we want to stay community-oriented, we have to stay on the intranet. It doesn't matter.

Matteo: Okay. And on all this aspect, social networks, etc., what do you think are the advantages compared to more traditional methods that were used in the culture of security? So it's typically, you know, to hold meetings, to write procedures by hand, etc.

P5: Today, we are in a world of more and more connected, we have new collaborators, younger and younger, who will be directly more sensitive to this kind of procedure, so who are really all with a strong digitalization. So we have to take that into account and go in that direction. But I think there will surely be a problem where there will be some procedures that are made a bit like the classic method and that will be complicated to transform and put directly into digitalization. But I think it will be totally better and more practical, because having meetings that can be redundant, people who may not necessarily listen or give information, especially if we have meetings of 2 hours, 3 hours, I think it's better to have a small explanatory file, it will always be more interesting. So social media can be really useful for transmitting brief messages. And if we want to go into detail, contact the key people and maybe add a section of details or propose, I think we will have to have this aspect, so social networks and, because

of that, continue to have meetings. I think we have to do more meetings. For those who are a little more interested and who want to ask questions or who want to know more.

Matteo: So it's something that complements, if I understand correctly, more traditional methods than the rest. What I could have observed is that sometimes when there are security instructions, whether it's computer security, etc., which are communicated, there is a bit of a reluctance from employees to apply them because it came from a direction that seemed disconnected. Do you think the fact that we can use social networks, or even, as you said, Intranet, etc., it can bring these two poles together? What would you say about that?

P5: I think it can be brought together if we say it explicitly, that yes, in collaboration with such and such an organization, we have chosen to tend to such and such a procedure or such and such a norm, etc. And not just say, well yes, contacted us to put such and such an ISO norm, etc. We will show that the management of the company also wants to do that. And not just show that we will have to. And then, in any case, we must also, I think, make a little more awareness for employees, to show them what the point is to have new norms. Why, especially when we are in a large company, a large company is obliged to be certified by ISO norms, for example, to protect itself, but also to obtain insurance from other providers and to be recognized by its customers. Obviously, you cannot be recognized by your customers and by your peers if you are not certified, if you do not adhere to certain norms, which are almost mandatory for some companies.

Matteo: OK. Do you see any obstacles or limits to developing social networks to improve corporate culture?

P5: The main obstacle – from a cybersecurity point of view- is that you want to use social networks that are hosted in another company. So tomorrow there is a problem with LinkedIn, Facebook, whatever the social network, tomorrow all the data is leaked, you are in trouble. So it's in that sense. Afterwards, if in this social network aspect, you try to anonymize yourself and you just talk about procedures, you don't go into detail, but it's a little more complicated. So for me, you have to try to internalize, you have to make a really internal social network. Otherwise, you risk having a loss of confidentiality and it will be problematic. You risk adding more problems than winning, you will have more losses than gains, I think.

Matteo: It's not a trap question, but does it happen often, the fact that you have data-based leaks on companies that use social networks and that there are leaks, etc.? Do you know if it happens often or not?

P5: It can happen often. It can happen even on the most famous social networks. There are always leaks, there are even people who can find it. It would just be enough for a malicious person to get access via an internal employee and maybe he can get through with a leak, do his business and get information back and spread it to competitors, or even more malicious people, to the biggest

cybercrime organizations. And especially if we are talking about a large company, which is mainly a large company that is going to set up a social network, that an SME does not really have an interest in doing it because it can easily make a small internal communication, but for a large company or a large group, in this case, it is subject to attacks. So tomorrow, there are the biggest attackers in the world, they see that your company is on your social network, they will try to get access. Because joining a social network is opening a door to an attack, a new door, knowing that there are already other doors. And the goal of security is to limit these doors and to reduce all this. For instance, just with the professional email address of the person, a malicious person can have the name and surname of the employee. Without being a cyber attacker, one person can have an important flow of information like the degree of the person, his place of birth… Indeed, an interesting fact is that ¾ of the passwords are easily findable in less than 15 seconds. Cyber attackers have algorithms that allow them to find the password of the person just knowing the email address. So even a common information like email address can be used by malicious people to make a cyber-attack and so threaten the company's security.

Matteo: So even if it is information that is not necessarily critical, do companies host information that is not necessarily critical? Can it still give indications to pirates to have an access path, except the example of the email address?

P5: I see what you mean, but I think there can still be an access in the sense that if you tell me that there is a social network, there are two people, there are employees. I don't know if in your social network everyone will be anonymized, even if everyone is anonymized with a nickname, you can have access to an email address, and you can go back up. I think it can still be a door. But if there is already little critical data that is released on the social network, it can happen, but there will always be a risk.

Matteo: Okay, I see. And in all that is good digital practice. Do you see the use of using a social network, whether it is internal or external? Is it something that can be useful for you?

P5: I think, for example, like phishing, I think it can be interesting. Teams, because often people will receive X mails in a day and will maybe zap some of them, whereas we tend to be more vigilant on Teams messages. So I think it can be interesting in some respects. So to talk about phishing, and also to talk about the cyber-attacks that are common for this type of company, for this sector. Really, to talk about if there is such a cyber-attack that occurs, what will happen to you? What will change your job? So tomorrow, there is no more network, and an attack, you can't work. You use Teams, you have to talk to your client, you use SharePoint, etc. That's just an example. But it can be, for example, for the industrial sector, there could be an attack that cuts the power and there is a machine that may not work. Or we are in a hospital, no more power, or there is someone who manages to enter from a physical security point of view and does anything, and starts to hit patients. So there is also this physical aspect that you told me about earlier. So no, I think we still have to talk and raise awareness because people are not sensitized enough. For me, according to my experience, when we did crisis exercises, I noticed that some people were really left out from a cyber point of view. They didn't necessarily understand the interest. And when there is an attack, they don't know how to react. That's not normal.

So in particular, I had the opportunity to do a crisis exercise in a hospital and we see that they are completely left out and they don't know. Tomorrow, there is a cyber-attack, I doubt that they will be able to...

Matteo: we use social networks as a means of communication, is it something that is relevant for you to use for safety culture? And how can it be useful compared to more traditional methods? You told me that you had done a crisis exercise and you found something more in the face. How can social networks facilitate the dissemination of these messages and good practices?

P5: I think it can facilitate in the sense that we manage to set up a regular dissemination. Not necessarily consistent because I think the longer the message is, the more it will be zapped. For example, I don't know, every day a news or something on a cyber-attack and you see it just a little, it will wake up the minds a little. I think it can be interesting. And yes, today, as I said, there are people who can be more or less sensitive to cyber security. There are some who don't necessarily have the knowledge. Sometimes, even if we organize meetings, e-learning, they won't necessarily follow, we lose the thread. So doing this daily reminder, I think it will still help them. And really, I think that in the dissemination, really try to show them what is happening on their side. Not just from an IT, cyber point of view. Because often people, so professional teams, functional people, they will zap a little for them cyber and IT, when there is a cyber-attack, it affects just these two sectors. While not at all, it will affect everyone. And so, more the involved in it. Because the biggest risk in cyber, ok, there are cyber-attacks, ok, the economy of cybercriminal increases a lot. But the biggest problem is the human risk. That is to say that people are not very sensitive, so the most common attacks, by phishing, by a person who manages to usurp identity, by downloading malware, etc. Even if there are still flaws, but the big one is often the cyber attackers, they will go for the least expensive flaw, in terms of energy and in terms of money. Because they put more and more money in this economy, because they know it's easy to find a flaw.

Matteo: I see. Do you tell me that it is mainly on the practical side of the user where there are really big problems of cyber and therefore security of companies? Does the fact of passing messages through a social network format to show good practices, etc. Because for you it is something that can be useful. What are the strengths of this?

P5: I will answer your question in the meantime. It depends on the format content transmitted by the social media. For example, videos are great format content to show practical situations and communicate about security rules and practices, but if the format is a video of 4 minutes, 5 minutes or 10 minutes, frankly, I doubt that people will remember the message. But if you can do 15 seconds, 30 seconds, people have to spend as little time as possible. You have to realize that today we are doing more and more training and we see that it doesn't change that much. We see that the human risk is still as high. There is a problem. The message does not pass. I think that doing, especially today, or people, whether they are older or younger, we see that people have more and more a problem with attention. I think you really have to involve them from the beginning and really try to do either a small explanatory video of 30 seconds, 8 minutes or maybe try to be inventive and try to watch it, try to organize or prepare a short film. A small short film of 5-10 minutes but with a little plot and talking

about cyber, maybe it will really interest people and that in the end, people, by watching these videos, will understand that cyber is important. We have to do this practice. Do it by theme. I think it could be interesting. On this format, yes. But if you just send a video of 5-10 minutes where we explain to you, it's just a political speech, it's not going to interest people.

Matteo: I really see the practical aspect of doing even functional jobs to embody the thing more than a speech or CTO.

P5: That's it, that's it. They're going to say, what is CTO telling us again? They're going to say, but it doesn't concern us. Whereas if you take people, I don't know, I think try to make a video and talk about each job. A video per job Tomorrow, it's about Product Owner. Put a video on Product Owner, I'm going to watch it because it concerns me, I'm a Product Owner. Or I'm an analyst, or I don't know, I'm a secretary.

Matteo: If I understand correctly, an internal social network, can it help to broadcast this kind of video?

P5: I think it's a good idea, the social network. And even to extend on another version a little less critical data, a little lighter, a little lighter for our customers and our peers. Because if we manage to sensitize our customers and also sensitize our peers, we're going to reduce cyber-attacks considerably. Because we shouldn't just think about us, we try to improve the whole society.

Matteo: Yes, I see. So all our suppliers because in terms of cyber-attacks, if a supplier or a client is careful, let's say, it can hit you.

P6: Yes, of course. Especially if your supplier is, for example, the one who provides the cloud, your provider. Tomorrow, your cloud attacked it. Or if your client is careful and you work on something with him, he can have access to your platform etc. It can create problems.

Matteo: OK. And even if it's a bit part of cyber, you know the ERPs?

P5: Yes. From a practical point of view, it's good for the three parts because everything is centralized. But yes, from a cyber point of view, it's sure that if we manage to have access, we can maybe unroll and access the other parts. So yes, from a cyber point of view, it's not the best thing. After, I don't know about it, from an ERP solution point of view, I imagine that there are cyber-ERP solutions with resilience, detection and response etc. I imagine. But yes, I think that these are solutions to really reinforce, to be careful that there is not this access. But maybe in ERP, maybe it's divided. I don't know if it's like the clouds where you have a cloud, a big cloud which can be public and inside there are private clouds. I don't know if it's the same in the ERP solution, maybe.

Matteo: And so, in private clouds, it's actually, you have a common cloud for clients, suppliers, producers.

P5: A community cloud, we call it.

Matteo: Ok. And then everyone has a private cloud. But suddenly, if there is, for example, my client who is cyber attacked, will it only be on his private cloud?

P5: Yes.

Matteo: And there is no way to have access to the common cloud?

P5: Even if they touch the public cloud, they don't have access to the other. So it can really isolate the most critical data. I don't know if in ERP, there is a principle in the network called network segmentation. So if there is segmentation in your ERP solution, that's not bad. But for me, you really have to do something as if there was a big block. There are small blocks, but the blocks are still independent of each block. For social media, you obviously have the same notion of segmentation that allow you to isolate critical data.

Matteo: Ok. Ok, I see. It means that the risks are very limited if my client or supplier is attacked.

P5: For me, there is a risk almost zero. And even if there can always be a risk, that's why you have to try to have in contracts either with clients or partners, to put a kind of chart in case of problems, to clarify who is responsible.

Matteo: Ok. I see. Because you told me that everyone had to be sensitized so that there could be impacts on others. So if I'm not mistaken, it's rather limited impacts if one is cyber-attacked in your chain. If your client is a supplier or a producer, if your client is attacked and you are the producer, the impact will be limited. It depends on your segmentation.

P5: If it's a segmentation, it depends on you.

Matteo: And often, there is a segmentation or not?

P5: It depends on the companies, on the means put in place. I'm going to tell you that in theory, it's supposed to be done, but in practice, no. Because often, it's a bit too complicated. People want to have

quick access to things to be able to share documents easily. But there are solutions that are offered, I imagine, at the level of ERP. If you should ask for access, it's a bit too restrictive. And that's why often, we ask, for example, a person who is going to work with such a client, to have a client PC to avoid this problem.

Matteo: Ok. I just have one last question. It's about the mission, whatever it is, about your last professional experiences. Did you see a use of social media, as I told you in a very broad sense, to disseminate good practices on security?

P5: At **[name of the company blurred],** I saw that there is a link page called **[name pf the page blurred]** and they talk about everything related to IT, cyber, they even do conferences, they also talk about it in one of their big events, it's called Big Media, and they invite a lot of people, big entrepreneurs, and they talk about various topics, including cyber here, and even a little more business-related topics. For example, they brought back Enoch Stagg, so really big people who have had a real success in the business world. So there is this kind of community initiative, I think it's interesting and it has developed, especially when you're in a big group or a big company, I think it's a primordial thing to do.

Matteo: Did you know if the employees of **[name of the company blurred]** were in this group, were they watching or not?

P5: In fact, **[name of the page group blurred]** is an entity that was created within the DIC, which talked a little about all the subjects of the DIC. And so all the people from the DIC, and even I think that other people from **[name of the company blurred]** know anyway, will participate in the events. I think it was at least once every two weeks or once a month, a kind of meeting, but we talk a little about a lot of subjects. It can be about a world of data, then talk about cyber, etc. And it takes questions, it interacts. And I remember I went there often and really the room was full, there were a lot of people who were interested. So I think that the fact of creating a community like that, of giving an identity, I think it can make people want to come. Because the feeling of belonging, it can really, it will involve the person. Today, why is there a risk and a consequence? It's that people don't necessarily have that feeling of belonging. They say to themselves, ok, I'm not IT, I'm not cyber, I don't care about IT and cyber. They don't want to. It's a bit of a problem.

Matteo: So if I understand correctly, even the social network, it can help this feeling of community. That's it. Belonging and therefore perhaps better apply the safety guidelines.

P5: That's it. I think you even have to try to mix up the directions.

Matteo: At the hierarchical level, you mean? When you say direction, you mean?

P5: When I say directions, it's for example the CTO, the shoulder rather than the direction.

Matteo: Oh yeah, like CTO, HR…

P5: HR, that's it. Because often people from the CTO stay between people from the CTO. Even here, you have people from IT with IT and cyber. I think that in my experience, for example with the **[name of the company blurred]** mission, I saw that like IT and cyber, yet we're going to say to ourselves from a point of view, if I'm an outsider in this field, I'm going to say to myself, it looks a bit like it, they have to understand each other, etc. They have totally different needs. And since they have totally different needs, everyone just wants to think about their own business. And so, during my current mission, we struggled a bit to really try to create a relationship, a collaboration between the two, because everyone has different interests and one does not want to take the step towards the other. And so, while here it's IT and cyber, so it's still close. So when you talk about cyber and HR, which are so far apart, there is even less collaboration and less communication. So I think we really need to improve this aspect.

Matteo: Precisely, social networks can help?

P5: Yes, social networks are a very good way, I think, to do that. To make everyone communicate and make them understand that if there are security rules, which can be restrictive for a domain, it's because other domains exist and have constraints. That's it. You have to try to make communication a support for an entity. And this entity, we see it on networks, via conferences, talks, etc. And even if we want to go into a bigger aspect, there are events, as we have seen, for the French country.

Matteo: Okay. I don't know if you have anything else that comes to mind on the subject of advantages, disadvantages, everything we've said. If there are things to add, on the fact of applying social networks to spread good security practices.

P5: The disadvantage is perhaps to have reluctant people to change. Yes, to change, to put in place social networks. There are people who say, I already have enough stuff, I'm bored to be on social networks. Or just people who are just not very social networks and who don't want to use and exchange too much and who say to themselves, it's already working well, plus this problem there. Afterwards, we will also have to be vigilant on how to communicate, communication strategies, what we put forward, not to make too heavy communication, but not too light either. You have to find the right environment and diversify the communication methods. So via videos, videos on Twitter, via stories, via posts, create groups, community groups, etc. I think for example, like what we see on WhatsApp, we have the same group and we can create subgroups. I think this kind of thing is interesting. You create a resilience group, a hacking group, a phishing group, etc. and you have a little bit of all the subjects. When you want to inform yourself on a subject, you can directly choose the subject you want, make subgroups. I think it's not bad. And you really have to think about how, because the social network is a very good way, but how do you use it? And that's the most important thing. The social network, if you use it well, of course it is relevant to solve these problems. But if you use it badly, it can just be one

more problem and it can even, if you share confidential data, for example, you do it via a social network that is really public, so you say, I don't know, you talk about your procedure in detail, you talk about, I don't know, customer data, data from your partners, you talk about it on your LinkedIn page, on your Twitter page, that's it. Tomorrow you will have a call, or even in a minute, you will have a call from your client or your partner.

Matteo: Ok. Well, thank you very much.

P5: You're welcome.

Interview of the sixth participant P6: professor of environmental security

P6: Well, tell me everything. So you did INSA, when did you finish?

Matteo: Me, I finished in February.

P6: Ah, you didn't finish INSA?

Matteo: No, I didn't finish INSA. I'm still a student, but I'm in the final stage of my studies. I'm not going to INSA anymore. OK. And in fact, I'm doing a double degree with Polytechnique Turin. And in fact, in this context, I have to do a thesis. And so my subject is on security, rather industrial security. And see, so it's exploratory research, see how we can apply social networks. What are the possible applications to improve security? And the advantages, disadvantages, etc. And so in this context, I do a lot of interviews. What do I mean by social limits? There are a lot of social limits. But it's still a subject.

P6: What did you do in INSA?

Matteo: I'm an industrial genius. Yeah, but there's the security side. We'll see, it fits into the scope, let's say. After that, there's still a little social, a little philosophical, in fact. Security, it's still a little... I mean, it's still big principles, more than...

P6: Yeah, yeah, yeah, there's culture, there are big principles. But there are fundamentals, anyway. So, on the other hand, let's be clear, on the social network side, I'm totally ignorant. I'm two years from retirement. No, four years from retirement. So yeah, so me, social networks, if you will. The other day, I have a friend who sent me something on Instagram. I said, well, no, but it's not going to be possible. So there you go. So I have WhatsApp, like everyone else. But Instagram, Facebook, my only social network is LinkedIn. So I jumped on it to see your face. But there you go, it stops there. So you're warned. I don't have social network skills. So everything I can... After, I'll answer your questions.

Matteo: In fact, social networks, already the definition that we are told in literature, is quite broad. Because it's an application that allows you to share information between people and connect to the Internet. So in fact, Teams is considered a social network. That's why it's so broad.

P6: For me, it's a tool... I agree. But in the literature... In the literature, we consider it a social network. Yeah.

Matteo: I think you use Teams.

P6: Well, yes, we have another tool. We have another tool. We have another thing, but there you go. We have another tool at the university, but I personally use Teams.

Matteo: In fact, all the tools connected to the Internet that allow you to share information, it's considered a social network. Because you can maybe get things in...

P6: Yeah, yeah, yeah. There you go. How did you know you had to come and ask me?

Matteo: I had made a request to **[name of the university blurred],** that's it. And they redirected me to you.

P6: Oh, okay. Yeah. So just a few words about me. So I'm much older than your mother. I'm an engineer. I'm an agronomist. Sorry. So I know biology, me, and the living, me. So I did agronomy studies a long time ago. So I worked in the chemical industry. But then more on the business side. For a while. He didn't want me anymore. And then I think that somewhere, I realized that I was swallowing eggs that I didn't want to swallow. I was at Dario Chemical. Largely orange and stuff like that. So they are very strong for brainwashing. But I think that at one point in my head, it was less ... It didn't go well. I'm a bobo ecologist. Like, who has tile toilets. Who recycles nitrogen. So suddenly, I know what I'm talking about. There you go. So there you go. So I sang. But hey, when I started working, I wasn't even 25 years old. So I didn't know that at some point I could have a crisis of faith. No, but there you go. In the face of values, it's normal. When you start your job, I don't think you have to ask yourself too many questions. After 8 years, he didn't want me anymore because I was a bit of a pain in the ass. I said what I thought. It didn't always go well in the multinationals. And on top of that, I started to tell myself that I would get along with people. I left with a good package. I left with an outplacement. The outplacement is the thing that helps you find another job when you're fired. Properly. And it's very pleasant. Because you're going to say, in fact, I had an office. Bring the army to Paris, sir. So there you go. It was also used at the time. It was used as a manager. To have a pied-à-terre and a secretary. While no longer in employment. No, but we're still in years where the standing is the army. To have an army and a secretary. Sorry. So I didn't care at all. On the other hand, in the outplacement, there is the material side. There is also the side of having people who help you look for your professional project. I'm telling you this because it can happen to you in these 8 years. And suddenly, I came across very good people. I did psychotechnical tests. And she ended up telling me. The lady didn't know me. And she said to me, you're not really made to be a manager. I had understood. Because I'm starting to do the job of the people I give the job to. Because I don't want to overload them. I do the cleaning before my wife arrives. So she said to me, you're not made for this. It's going to crucify you. It's going to overload you, crucify you. On the other hand, you are given advice. Transmitting, that's your thing. Great, ma'am. What do you want to do in life? I would be a good consultant. Go ahead, it's your role. So I went to environmental consulting. At the time, it didn't exist. All I knew, I had learned in books. Because there was no training or formations like here **[the interview was conducted in a university classroom].** And because I didn't have the chance to do a Phd. There was a Phd that was open to take advantage of the agronomy. And it wasn't me who had it at the time. Anyway. At the age of 29, I found myself being a consultant in the environment. First in a study office which has since melted bridges. But I learned everything with a very

good gentleman. And I learned the ISO 14001. I don't know if it speaks to you. So I am an industrial environmentalist. First, I was given advice. Then to my account. And there, I had the 14001. I did the audit of the 14001. I realized that I was very strong to understand the regulation. Not to be afraid of the regulation. And to explain it to others.

Matteo: In what sense, not to be afraid?

P6: People see a text. It's very badly written. I eat from it every day. It's very badly written. And again, the labor code, I think it's worse than the environmental code. It's badly written, it's badly explained. People are not trained at all. I mean, in INSA, at some point, 20% of your promotion is going to be business manager. Nobody knew the industrial regulation applicable. There is not even an ounce of weight. There is INSA Valor which does things completely based on waste. But none of you know what are the obligations of a business manager in terms of waste. Nor security. And me, people are not used to reading them. People are afraid to read them. People don't care because it's regulation, not even the police. So you multiply that. When you are a consultant, you live very, very well when you manage the regulation. When you know how to read it. To say, this applies, this does not apply. You have to do this, you have to do that. Then you have to understand, you have to have some basic knowledge to understand the texts. Honestly, it's chemistry, but you just have to know the name of the molecules. And maybe have done a little bit of industrial engineering to know that, to make a distillation, you have to boil things. When you boil things at a temperature higher than their point of glare, it can go wrong. No, but that's the security. So yes, you have to know things. But you don't have to go out of Jupiter's kitchen to do the regulation. But when you do that, you earn relatively well your life. So I started with the environment. So here I am in this little advisory cabinet. It didn't go well. A bad manager. The box melted the boards, I went to my account. And since then, I've been at my account. It's been more than 25 years since I've been at my account. And it's going pretty well. So a little management of the environment, security. So I started with the environment, I added security. Because I think we can't talk to people about little birds either. They're not cool, they don't go to work quietly. And then I do quality. Because when we talk about management systems, environment, security, quality. Today, the standards are the same. 14,000, 1,000, 1,000, 1,000, 1,000, 1,000, 1,000. It's a thing. And you didn't come for that. You came to ask me questions. So that's my job. I have companies of all sizes, so rather in the agro-industry, except that they don't have a circle to pay for a consultant, so we're not much in the agro-industry. I work with chemical companies, pharmacies, and mechanics. So these are my clients. And at the same time, I'm a professor because I like to study, I like to go alone. It allows you to adjourn, to work for your former students, which is quite pleasant. Well, I don't know that feeling. No, but I'm telling you, for me, it's still a pleasure. Students I've seen for two years, we got along well, and then one day they come back. Some of them come to teach here, and then some of them call me as a consultant. It's not unpleasant. So I learned everything by myself, since the training didn't exist. Environment, safety, and then quality, but more on the management side. For example, in agro-food, I understand what they do in terms of health, but food safety, which is still a safety thing that's a bit borderline, but I understand, but I'm not a fine technician. I've missed out on a few things. But men's safety. No, no, I'm kidding. I try to find my little ones. And I work with people who try not to have accidents. For the sake of safety, in the end. That's it. Now that you know me, I don't know what to say.

Matteo: No, but it's super interesting, because it allows me to bounce back. Can you explain a little more to me? Because you have a more environmental approach, but by safety, right? If you can tell me a little more about that.

P6: No, I have an environmental approach, environmental. Waste, water, water protection, air, not polluting the neighbors. To do all this on the ground, you have to sensitize people. Okay. But I have a hard time sensitizing employees by telling them that it's good to protect the little birds if they are insecure in their job. Okay. So, inevitably, I was interested in men's safety, because I wanted to talk to them about environmental safety. Okay. That's it. And you, on your side, did you define what you meant by safety? What was your field of research?

Matteo: By safety, there is everything that is industrial safety, operational, and also everything that is cybersecurity safety. So it's super broad, actually. It's really security in the broad sense, so avoiding accidents, avoiding stops, etc. So the object is man, goods, and also the environment, so HSE, etc. And knowledge, cybersecurity, data, man, goods and data. That's it. So there is also the environmental side in there. It's one of the questions that I'm going to ask you too, but I have the impression that on the HSE standard, on everything that was HSE, the environmental side is very, very secondary.

P6: It's small things. Objectively, if the question is for me, personally, I save a man before saving the environment, before saving the birds and the environment, that's it. A priori, I save men after the mammals. No, but here we are, if I have to save one, we have a pyramid of preferences. Except that today, by our environmental behaviors, we can influence the security of men tomorrow. For example, I mean, climate change is fires. Fires are people who burn things and maybe people who die. Climate change is hurricanes, floods, stuff, it's people who die. Resource refactoring, etc. Yeah, so that's it. Today's environment, in which we are well in France, it's not very dangerous more than that. We're not in Bangladesh where everyone drowns every day. But it could happen. that's the long term. But I think it's not necessarily your subject. You think about the human environment, the employees and the inhabitants. Well, also the environment in the sense that the goal is not to spoil the environment. It's also in there.

Matteo: And so what we're looking for is the role of social networks in there. That's it, how it could possibly improve the culture of security in a very broad sense. What are the possible applications that can be done? Typically, the interviews I've been able to do right and left, there are applications that exist to be able to share real-time photos of accidents, stuff like that. There are advantages and disadvantages. The disadvantage is that it can stimulate people. There is no boundary between the professional and the personal. That's all I'm exploring. And then I synthesize.

P6: Did you prepare a questionnaire?

Matteo: I had a few questions, but you can go ahead. The goal is to be semi-directive.

P6: First, define your domain. What is security? Then, on the security of industrial processes, your thing is hyper-tentacular. The social network, direct proximity, can save lives. Before, there was the bell that rang, people knew they had to flee. Today, we have the fireman's siren, but we also have social networks. I'm going to transpose to another. It's not usable like that. At the university, it's not a social network, it's an alert network based on SMS in the event of a terrorist attack. Tomorrow, there is a factory in Feyzin. First, we'll talk on the radio. I think I have an alert. In the metropolitan area, I think I signed up for the alert. Even if I don't hear the discontinued siren that says it blew up there and I shouldn't go there, I think I'll have it on my phone. I think the well-imagined that is, having people in a network that can be warned quickly, in the case of Aleppo, it's not bad. The advantage is that it goes fast. Yes, and especially now, you have to imagine a social network that can be pulsated on others to warn everyone at the same time because no one listens to the same radio anymore. No one listens to the radio anymore, except me, I'm 24 hours on the radio. People don't listen to the radio anymore, but it's true that the social network can go through SMS. And I think it's the **[name of the metropole area]** that we have compared to an industrial one. Here, locally, at **[university],** we have one on terrorism. So I think if ever an industrial event goes beyond its limits, it's a bit heavy. You know, we trigger a certain number of PPI. Ah, the POI and the PPI. When we are at the PPI stage, we have to warn the population. So it's true that there is a social network that allows you to warn the population very quickly. Another example, I also live in Haute-Loire, in a small village, and we have a social network called Illiwap, which allows all the town halls to put their little announcements. I found a pair of glasses at the town hall, ah, I lost my cat, but by way of a heat alert or a drought alert or a fire alert, a ban on farmers, for example, it was in the middle of the day. The social network allows you to pulse information very quickly. So that, I think, for a heat alert, it's good. That was for the industrial part of things. Inside the industry, you're right, there are social networks that allow you to broadcast images of accidents, but I don't think that's necessarily the smartest thing to do. Indeed, it can shock people when you never know. Once I saw a video of a guy falling off his truck and dying, I think it was a mistake. Some people were really shocked. I had negative feedback.

Matteo: The video was taken on the Internet. On YouTube?

P6: Yes, on YouTube, and we knew the guy. I didn't broadcast it. It's not very simple. On the other hand, the social network inside a company can bring up dangerous situations. We always have a problem in a company, because the security culture involves everyone's cooperation. And especially everyone's cooperation, not to denounce their neighbor, but to denounce situations that are unsafe. A guy who's at the end of the factory and realizes that, I don't know, a rambler broke his face. Or at the end of a construction site. You know, the anomaly sheets. It never works. On the other hand, he has an internal social network. We'll have to ask people at FH because they do that. He has an internal social network that allows him to take a picture. It geolocates, it takes his name. We know who he is. It's anonymous. Well, it's anonymous to others, but we know who set the alarm, when, why. In this case, he doesn't denounce anyone. He takes his picture. Watch out, pole fell, risk of electrocution. I say anything. It's done, it's rolling. There's one up there who gets the alert. He says, wow, he's right, Robert. Thank you, Robert. It allows you to be quick to respond. People will only report if we act on the fact that they reported and we make the modifications afterwards. To have feedback from the field, you always have to put more energy to thank and respond to the field. The field only makes efforts if it's useful and it has the results. The social network is to thank and say, we send a team right away, thank you for your report. It's supposed to be a reactivity. The social network can be interesting because it generates a possibility of reporting and it also generates a reactivity of response and a possibility of acting that we

noted what the person said. It's not so much the fact that it's a social network, it's that it's quick communication, that everything is tracked, that the social networks, the applications allow you to compile the data and process it. You can have them go back to the office of the good boss without Robert saying to Gustave, Gustave who says something, something that crosses things, he says, in fact, you see, there's a pole that fell. So the social network, tic-tac, it addresses the right person. It formalizes the process. It allows for shorter processes without going through the hierarchy and without going through the guys who will forget to pass the message. So it's good for reporting and it's good for good ideas. Because even if it's not a dangerous situation, a guy who sees something and says, guys, I'm taking a picture, guys, if we put, I don't know, a bridge, a small alley, something, a small step, it would be better. At least we say, thank you, George, for the idea. We don't have the means, we're not going to do it anyway, there won't be any more, oh, thank you, George, for the idea, I send a guy to do it right away. So it can be good for reporting dangerous situations and for good ideas. Because the idea box doesn't work anymore.

Matteo: What I was going to say, I was going to ask you about your experience between notebooks and idea boxes.

P6: Yeah, there are some, I'm in a factory where people have files, but we were more on CSR, we were more on social, there were key prices. It was a different process, you had to make a file, there was a key price, we earned something for ourselves or for the association, for the association, I don't remember. But it could be slow. It could be slow and on paper. Whereas George comes along and says, no, it would be better if we had a piece of paper so that it's faster. So there are cases where it has to be fast. And when it has to be fast, the social network, the modern communication of our time is good. I'm for it. And so, as it allows us to thank George, that's how we create a culture. I don't think a culture is something like go ahead, I'll give you the security culture, you take care of it, it's a culture, it's made of picking up messages, but above all, listening to the ground. They realize that we're listening to them and so it makes them want to join in. It's just a thing that's quite improving. Very long to build, very quick to put together.

Matteo: So I think, if I understand correctly, it can also allow people to get involved and build a culture, not just of security, but of business, belonging.

P6: In a way, the good cultures have been combined, they have been passed on to security. Then, on my fundamentals, on security, on customer service, but that's more in things where the customer is at the center of the company. You have to do shipments for a car, difficult, or screws, by thousand per minute, on the company, on the beauty of the product. Of course, when you're at Hermès, it takes the girls 7 days to sew a bag, and the bag doesn't start at 4,000 euros, and so on. She's proud of her bag, and there's her name on it. A guy who makes a badge of 5,000 pieces per minute, what pride! So there's only security left. The environment can be a good thing. But the culture that is based on bringing money to the shareholder, it doesn't work at all since the 1980s. It's over. We're proud to belong to a company because it's going to grow. It doesn't work at all. No. The guy at the base has lived it all. He knows that people are licensed in companies that work well just to please the shareholder, and he can't do it anymore. It's not about that that we create cultures. except for luxury, we're proud of the product. But

I think that today, to create a culture on the pride of belonging to a company. So I believe a lot in cultures based on values. Security, environment, that's part of it. It can make the link between the management to be caricatural and the jobs, the operational part. It allows you to make a good link that is a little bit perverted because there is no more pride.

Matteo: It allows you to make the link between, let's say, the management to be caricatural and the jobs, the operational part.

P6: Yeah, it allows you to make a good link which is a little bit perverted because there is no more pride in being in the same team. So that's for inside the company. We talked about outside, on the alert. Inside, on the rise of incidents, good ideas, the passage of fast messages with an unpleasant corollary. It's that if people are listening on their phones, they don't ensure their own safety. Precisely in some, you may know it, but in some industries where the operators are on machines, they forbid personal phones. So that they are not distracted. Which is normal.

Matteo: Yes, which is normal. But what raises questions about the application and social networks, in the sense that can they really take a picture right away?

P6: There are cases where it is possible, there are cases where it is not possible. And in fact, a guy who has his workplace, he doesn't move, he's not the most useful guy in the world. In terms of security, what is interesting, it's the security guard who moves, who sees a lot of things. And the maintenance guy, who moves and sees a lot of things. So no, but you have to cut this conflict between no social network, no disturbance, and social networks to report. That means they don't use it all the time. So we can help social networks, it can be private phones, it can be workstations, work tablets on which the guy, on a production computer, you can very well have a social network, so there are no pictures, but I'm in the room, the chairs are broken, thank you for replacing the chairs. It's true that someone broke the figure, or three chairs are broken, thank you for having them removed before someone sits on them. We gained a little in security. After that, it won't replace the meetings, the guys who think, because in the culture of security, there are people who think together. So the social network is a bit of a solitary thing. It allows you to do that, except to come across teams, but there it's collaborative, it's not even a social network, it's a network that allows... So what's good here is that it can cause people who are very far from each other and who have the same problems. But it's not an operator.

Matteo: If I understand correctly, the social network can be a support in addition to physical meetings, workshops, training, it can help pass a message.

P6: The social network is a tool, you just have to use it as it is, not a thing, like IA. I'm afraid to say, no, not me. But IA is good for telecommunications. So the social network, I think you have to use it as a tool. So it's not a yes or a no to the answer. For the moment, I'm giving you examples where I think it's useful.

Matteo: You told me about Fages too, which have a specific application.

P6: They have a kind of application where the guys write in real time. It's also used to write... It's also used to write... There are applications now that also serve to write if the guys are there, for a team leader, when he has large construction sites, to know that these guys have entered on such a perimeter. So it allows him to know that you don't have to go... Well, over there, there may be guys on foot, because his employees are over there. So it also allows you to visualize where people are when they have a very large construction site. I think. But it's actually a communication tool more than anything else. It allows you to get messages. Everything goes through social networks. The most stupid messages, the most intelligent messages. I don't know if... I think that's it. It's pretty bad. When you don't know who's talking to you, I prefer to go see people. So, Teams, it's good because it allows you to put people who are far from each other They can see each other, in quotation marks. They can speak their own words. It allows you to put them in contact even if we are far away, even if there is COVID. It's good. I think that, from you to me, they are well thought out with their binoculars.

Matteo: Any concerns about cybersecurity and social media?

P6: As soon as you have information circulating somewhere, there is a risk. I think it's easier to do it on the ground. No, but honestly... But... There are a lot of things and a lot of security that are based on computer signals. Things that transmit messages to other things. So, there are things that are well done. For example, fire doors, when there is no more electricity or if the signal is bad, they close. It's a positive security. But I am sure that there are... Even in serious cases like dangerous factories, there are cases where the security is ensured by the machine. If we hack the machine, we should be able to do nice things. Funny.

Matteo: At INSA, we were taught to make attacks on production lines.

P6: Yes, I am not surprised. When the production line runs out of drinking water, we should be able to play with it. Very nice. Information is available everywhere. So, we can... Yes, we are pretty smart. So, I think that on cyber security, there are risks... It can lead to physical risks precisely because our systems are not protected or can't be protected. I don't know. It's time to... To steal jewelry at the Louvre, you just need a scale. And that's it. So, from now on, why invent complicated things? You shouldn't have done INSA to steal jewelry at the Louvre. You should have a scale. That's what I can tell you about... I think it's a tool. Social networks. And we should use them intelligently.

Matteo: With the disadvantages that I noted.

P6: A tool that allows speed, traceability, compilation, data processing, computerization. The construction industry has a lot of networks. There is a newsletter that is free called *"Info BTP".* It's a newsletter because often there are people who develop apps. I think that OPVTP the security network

of the office of the professional of the building. I think they have an idea about it. There is a newsletter. Sign up. Sign up in a month. It's called *"Batinfo actualité".* From time to time, there are small ads where you surf their website. There is advertising for young people who develop social networks to help make security in the company. There are products that are developed. It's up to us. In conclusion, having thought about it with you, it's up to us.

Matteo: And in the companies that call you as a consultant, are there projects that go in that direction or not necessarily? In the sense that we develop internal tools.

P6: We are more in the group. It's just to inform good practices. Meetings. You go to SNCF **[France's national railway company],** for example, when they have their meetings of superior excellence. The morning meeting. What happened the day before? What are we going to do during the day? At the managers' level, the technicians in the region go to Doriac, to Modane. So the guys don't come every morning to Lyon to discuss Boudgra. So it's done with the big boss. What kind of incident do you have? Stuff, stuff, stuff. I show the incidents that came. Rails, trips, other sectors. It's done. It's a social network. It's Power BI for numbers. It's Teams for ... It's their social network. And it allows information to travel quickly. Once again, the social network allows information to travel quickly to everyone. And everyone shared it. But it's a tool. It's a tool. When I want to organize something, I do a big WhatsApp. It's a social network, we agree. At my level.

Matteo: How do you do it?

P6: I don't know. I want to organize something, whether it's Christmas, a trip, a WhatsApp group. During Covid, we did that. I had a Friday WhatsApp group, a Saturday's aperitif WhatsApp group, I had a girls' WhatsApp group, I had a lot of WhatsApp groups. Because it's the only way to select people to talk to. If you're a little smart to do that. And yeah, it's a good tool. Mark Zuckerberg made a product, not a tool.

Matteo: Is a product something we can use from A to Z?

P6: Yeah, but if you configure, I imagine, I'm not on Facebook, but if you configure who can enter your Facebook and your thing, and what the themes are, and you moderate the 20-20, it can be used for security. It can be used for something; it becomes a tool. If it's just for everyone to exchange things on everything and anything, it's not for us, it's a product. It's useless, except to mess up people's heads.

Matteo: Because of the interviews I had with security directors, some made LinkedIn groups between them to share good practices, etc.

P6: Yeah, I know, I don't know how to do it, but that's how it's done. When we follow someone, I don't follow anyone because I don't want to leave a trace, but we do start to follow people and see... It's interesting. Once again, you need neurons behind. It's not LinkedIn that makes your intelligence. It's you who have the intelligence to use it properly. We're still in this. You have to take control.

Matteo: We always come back to the same thing. It's a tool. It can be useful, but we have our own intelligence.

P6: No, it's a thing. It's a product. It becomes a tool. If you have it, I can put a piece of metal at the end of a piece of wood. It won't be a shovel, it won't be a tool. Because if I don't put it in the right axis, if the two are not in solidarity, if the shovel is not well sharpened, it will never be used to dig a hole. It's a piece of metal and a piece of wood. I can plug them into each other. It will be one thing. If I think about it, Facebook is the same. If there are smart people who have managed to make smart groups, they have made products put on the market by Zuckerberg to make a tool that is useful to them. It's a tool. You have to think about it. The little spoon is not a piece of metal. It's rounded in it to hold the white cheese. It's a tool. Oh, yeah. Yeah. The chimpanzees sharpen things to get to... When they go looking for... No, it's not a chimpanzee. Yes, they go looking for tools. They make tools. They don't take any branch. They take any branch. They speed it up a bit. They sharpen it to be able to go... It's a tool. The difference between things and tools is intelligence. Or animals, in the case of chimpanzees. That's it. The difference between Facebook and smart networks is that it's even worse.

Matteo: For you, do you see any prospects on applying social media for the safety culture? Is it still an interesting thing?

P6: Imagine. Before, if **[name of an oil plant]** was doing an exhibition, there was a guy in the street with his drum saying alert, alert, alert. We made the bells ring because the wolves were coming to Paris or the Germans. Obviously, progress is undeniable. Becoming stupid is also a bit what we are.

Matteo: In addition, with the AI, we have become slaves of the AI, in some cases.

P6: I don't understand anything. My students ask the AI things that I ask Google. First, I get the answer much faster and I consume energy. Google, being underpinned by an AI, eats more carbohydrates, worse than the one before. Before, I was super strong to do Google searches. I had good keywords. Now that there is the AI behind, I have to ask him things in French. What I want is information. Progress is always good. It gives quick answers. We are still many. We can't link so many connections with living beings. Especially as we age, we don't remember who we are. No, I think it's fabulous. Fabulous. At the average level of the population. I'm not sure we're doing a good job.

Matteo: Its good for me. Thank you very much for this interview

Interview of the seventh participant P7: civil engineer

Matteo: So we're going to do an interview on the links between social networks and the culture of security. So on both terms, I'm going to have to define them. So the framework in which I place myself is very broad. Everything we define by social networks is an online resource, connected to the Internet, which allows people to interact. So it's very, very broad. And the culture of security is both physical security of people, as well as information technology, data, etc. So in relation to that, I will have several questions during this interview. So the first one is, could you give me a list of the social networks you use at work right now?

P7: Teams, Outlook, everything that is, I don't know if we call it the Microsoft suite, SharePoint, because it's a place to share docs, at work, and then sometimes there are what are called management jets [EDM], I don't know what, documents, electronic documents, which are platforms, each time different for the sharing of documents on the different operations. I'm thinking. Then, basic, phone. I don't know if it's, no, it's not connected to the Internet, it doesn't work.

Matteo: And is there more specific content to the culture of security that is conveyed on the platforms that you told me about?

P7: Yes. On each operation, there is a security controller. On each site, on each construction operation. There is a security controller called a CSPS, which is in charge of the physical security issues of the people who work on the site, and who establishes reports each time. For example, the firefighter's voice is not clear. There are people who work without a safety harness or without a helmet, things like that.

Matteo: And then these reports are transmitted, are deposited on?

P7: Yes, they are transmitted by email and deposited on a jet when it is available. And so the concerned people have to correct the things to be corrected.

Matteo: Ok. So you would say what are the advantages of these tools compared to traditional methods?

P7: What do you mean by traditional methods?

Matteo: For everything related to the culture of security, there were methods to transmit information, security rules in the past, typically with posters, posters, etc. And now we use more and more.

P7: After the posters are always present, I can't say if they are mandatory or not. But on all the sites, I think they are mandatory. So you have a display panel at the entrance saying, wear mandatory safety equipment, so safety boots, helmet, vest. And so there are always these displays there. And so yes, compared to a display, it is rather a more relevant follow-up, in the sense that the displays are rather general things that are rather obvious. And then these relationships are specific to the situation, the security of the sites is different depending on the site, even if the regulations are the same.

Matteo: Ok. So if I understand correctly, social networks in the context of the culture of security is a complement to the old traditional methods, classic displays, etc.

P7: I have the impression that it is rather the displays that have become a complement, in the sense that these displays, if they are removed, the impact is minimal, even non-existent, because no one pays attention to it. While the GSP reports, which we are obliged to respect, there can be penalties in relation to that in the contracts. And in addition, big companies organize, when I say big companies, I think of Bouygues, Eiffage, etc., or even other smaller ones. They often organize training weeks, or I know that Bouygues sometimes does, once a month or Monday morning, a security session with their workers. But it does not fall within the framework of the social network, since it is live. But I got lost. It is to say that it is not the methods used today, via social networks, therefore the sending of reports by email, it is not complementary to traditional methods. It is rather that it has taken its place.

Matteo: And on these face-to-face sessions that you were telling me about, on security, do you know if they use social networks during training sessions?

P7: I do not know how to say. No, I do not know. I just know, however, that it is more a question of communication to others, that sometimes there are publications on LinkedIn, saying point security with our workers this morning, to show that the issue of insecurity is important for these companies.

Matteo: So if we go back to the question I asked before, which was about the advantages of social networks, what advantages would you see in social networks to promote the culture of security?

P7: We are sure to reach the target, insofar as if we make a display, whether it is seen or not, whereas when it is the sending of an email, the person is supposed to have read or seen the message. There is that as an advantage. There is the advantage of monitoring too. We know what information was transmitted at what time. Yes.

Matteo: Would you see limits, obstacles, to social networks that have security? Not like that.

P7: So no, I don't see a limit. The only limit, which is not really one, is that this transmission is not done to all the people who intervene on the site, but to the managers of each company, and they then have the duty to pass it on to their workers. After, how do they transmit it? Is it verbally? Do they need to transfer information through the tool? I don't know, they have the obligation, but in any case, yes, that's it.

Matteo: Ok. And so social networks, in your opinion, can it promote the commitment to the participation of people, etc., to pay more attention, especially in terms of security?

P7: It's hard, it's hard to say, because from the moment a person's life is in danger, or even their physical health, inevitably there is a certain commitment. I would not say that it promotes it, I would say that it maintains it, comforts it, I don't really know how to say, insofar as, in fact, we constantly have an email and a reminder from the CSPS, so we always have this question, even if we always have it in mind in the background, in fact, it comes back to the foreground quite regularly, which allows us to say to ourselves, ah yes, I would have to make a point with my teams, for the person who receives the information. So in a way, it promotes commitment, but it's not the thing that will make us commit. I mean, if there wasn't that, if there weren't these points and these relationships, that's not why we didn't consider the question of security.

Matteo: And typically, because in everything that is construction site, these are still situations that are very practical, do you broadcast, do you have workers intervene on videos to then broadcast them to show the good practices, the bad practices, security rules, etc.? Is that something that is done?

P7: In some companies, yes. I was talking earlier about companies that sometimes did posts on typically LinkedIn. It's more about the purpose of the company's communication than towards people. Yes, this kind of video exists, but it's really the big companies that do it, that organize it, either to show them within their internal training, or in the case of communication on social networks to show that the question of security is an important issue for the company.

Matteo: So it's rather about institutional communication?

P7: Yes, at least in the form of videos, yes. And there, when I also talk about institutional communication, typically it is one of the important issues of the Vinci group, security. So we can find on their website a big communication on it. Is it a social network, an internet site? In a way, yes. So at that point, yes, it's more communication to say, for us, yes, the question of security is important. Yes, for the image of the company and for the people who may also want to get involved in this company and for whom this question is important.

Matteo: Does this institutional communication, even if it is, as you said, not directly addressed to internal people, can it still reach, let's say, internal people and affect internal people? In the sense that it's not just communication, but does it have a usefulness, an efficiency?

P7: I can't say if it's useful or efficient, but when you work in a company, you know a little bit about the values or the directions, the objectives, etc. of a company. And the fact of having in mind that security is an important question, yes.

Matteo: And typically, when there is an accident on site, how does the alert procedure go?

P7: I have no idea. I don't know. It never happened to me, but I don't know how it goes. I imagine there is a declaration of work accident, but ...

Matteo: But do you know, there are still messages on, you mentioned Teams, etc. Is there ...

P7: No, because then, in fact, in the context of my work, I don't work for a company that directly does the work. So yes, I don't work for a company that directly manages employees, so I don't know the procedure.

Matteo: And are there still sensitive documents or sensitive data that you share via all the platforms that you told me, and that could pose problems, that can, you can tell yourself, maybe a risk in terms of whether these data are leaked?

P7: Yes, for example, when there is a team working on a competition, so there are between the different actors, there are documents related to the offer that will be proposed. And inevitably, when there are competitors who are working on the same competition, there is this risk there. And then, yes, it's the only risk I see, but confidential information.

Matteo: But suddenly, is it something that can prevent you from using social networks more?

P7: No, because even if the risk is there, it is not something frequent or that happens to say, well, we got hacked to make the documents of the offer on such or such project be disclosed. The risk is rather inside, in order to be careful that a person does not share them, because they have an interest in giving these documents to another company, or to give information on the offer that is being proposed to a competitor. Yes, the risk would come more from a human being than from the social network itself.

Matteo: Because typically, on social networks, there are a lot of leaks, often, on the data, and so it's not something that you have already suffered, first question. And second question that worries you particularly.

P7: No, it has never happened to us, and is it something that worries us? No. The concern comes more from the fear of losing all our documents, but not from a leak.

Matteo: It means that in the advantages of social networks, there is also the fact that it allows you to centralize documents.

P7: Yes, that's it, it's sharing documents between different actors who are on an operation. And in fact, internally, we have internal servers for the sharing of company documents. Otherwise, social networks, yes, it's more for when we work with other companies on this or that operation.

Matteo: And what type of social networks do you use when you work with providers?

P7: Well, what I mentioned before, SharePoint, EDM... No, precisely, that's with companies, but internally, for document sharing, it's an internal server, it's not a social network.

Matteo: Is it a SharePoint?

P7: No, it's a network.

Matteo: We talked before about the subject that social networks could promote the engagement and participation of people. You were quite nuanced on my question. Can it allow, in your opinion, to make a link between very operational functions and more managerial functions?

P7: I'm not sure I understand what it would allow to do. I want to say yes. It's a bit like the definition of... In the definition of the social network, there is this story of links. So I don't see how a network is a link between two things. And so, yes, it creates a link between a managerial and operational function.

Matteo: Can it facilitate links and therefore relationships?

P7: It's hard to answer these questions because in the context of my work, I don't have this position of manager who transmits his security instructions, nor the position of operator who receives them from an external point of view. I would rather say that these social networks don't promote the link between a manager and an operator because there is nothing better than a direct contact to promote relationships. It's always very cordial, an information transmitted by a network within the framework of a company. Afterwards, yes.

Matteo: If I ask you to give me a concrete example in which social networks have been able to improve security issues, you wouldn't necessarily be able to give me a concrete example?

P7: No.

Matteo: Do you have anything else to add or that comes to mind on this subject, social networks and security, or that we haven't necessarily addressed?

P7: Yes, I was thinking about one thing. These were mainly security issues related to people. Is there also a security issue for people, but related to equipment? In the sense that in a construction site, there are always electrical and heating installations, etc. It's very specific to the field of construction. There are fire regulations, the walls must be cut to a certain degree, etc. At that time, it's another person, what is called a control office, who comes to look at the technical equipment to be installed, and at the same time make reports to say that something is poorly installed. Indirectly, it's a security issue. I don't know if it's ...

Matteo: Do these companies use social networks to communicate, whether it's with you, the people on the site?

P7: No, it's the same for reports. We make a visit to an operation, we make a report saying, such and such a company, be careful, this is not right. And sometimes it's things that concern security. Typically, there is such an installation that is in a room that is not isolated from the fire, as it should be in the regulations. The concerned company must make the necessary changes to make it happen. But no, there is no particular communication on this.

Matteo: Do you see other points that have not been addressed or that come to mind on this link between social networks and security?

P7: No, I have the impression that in this area, social networks are a tool for the transmission of information, in general, and that in this information, there are things related to security. It's the link. In the sense, it's not a specific tool. It's a tool that is used for that, but that is not specific to that.

Matteo: And the messages that are transmitted, you were telling me that it facilitates the messages transmitted. I would say that these are rather long messages.

P7: It depends. Sometimes when it's a report, it's more or less long depending on the size of the site and the number of points that the person in charge raises. So really very variable. And then it can be very short because it's rather something urgent in the sense that the firefighter's access road is blocked by someone who parked his car there. And at that moment, it's more of an emergency e-mail saying Urgent, there is a car parked in front of the firefighter's access. That's it.

Matteo: Ok, well, if you don't have any other elements to add, we can stop. Thank you.

References

2025 Social Media Facts & Stats: Usage, Platforms, and Growth. s. d. Consulté 4 novembre 2025. https://www.broadbandsearch.net/blog/social-media-facts-statistics.

Accidents at work claimed 3 298 lives in the EU in 2023. 2025. https://ec.europa.eu/eurostat/web/products-eurostat-news/w/ddn-20251014-1.

Aichner, Thomas, Matthias Grünfelder, Oswin Maurer, et Deni Jegeni. 2021. « Twenty-Five Years of Social Media: A Review of Social Media Applications and Definitions from 1994 to 2019 ». *Cyberpsychology, Behavior and Social Networking* 24(4):215-22. doi:10.1089/cyber.2020.0134.

Anaba, David Chinalu, Azeez Jason Kess-Momoh, et Sodrudeen Abolore Ayodeji. 2024. « Health, Safety, and Environmental (HSE) Standards in Industrial Operations: A Comprehensive Review ». *International Journal of Applied Research in Social Sciences* 6(7):1321-32. doi:10.51594/ijarss.v6i7.1269.

Battista, Daniele, et Gabriele Uva. 2023. « Exploring the Legal Regulation of Social Media in Europe: A Review of Dynamics and Challenges—Current Trends and Future Developments ». *Sustainability* 15(5):4144. doi:10.3390/su15054144.

Boyd, Danah M., et Nicole B. Ellison. 2007. « Social Network Sites: Definition, History, and Scholarship ». *Journal of Computer-Mediated Communication* 13(1):210-30. doi:10.1111/j.1083-6101.2007.00393.x.

Braun, Virginia, et Victoria Clarke. 2006. « Using Thematic Analysis in Psychology ». *Qualitative Research in Psychology* 3(2):77-101. doi:10.1191/1478088706qp063oa.

Braun, Virginia, et Victoria Clarke. 2024. « A critical review of the reporting of reflexive thematic analysis in Health Promotion International ». *Health Promotion International* 39(3):daae049. doi:10.1093/heapro/daae049.

Carhartt CEO says he's still mandating staff vaccinations. Now he's facing a boycott. - CBS News. 2022. https://www.cbsnews.com/news/carhartt-covid-vaccine-mandate-boycott-ceo-mark-valade/.

Cole, Kerstan, Susan Stevens-Adams, et Caren Wenner. 2013. *A Literature Review of Safety Culture.* SAND2013-2754, 1095959, 463474. doi:10.2172/1095959.

Dello, Simon, Ken De Smet, et Walter Sermeus. 2025. « Care Left Undone Among Physicians: An Explorative Thematic Analysis ». *BMJ Open Quality* 14(4):e003657. doi:10.1136/bmjoq-2025-003657.

Dhingra, Manish, et Rakesh K. Mudgal. 2019. « Historical Evolution of Social Media: An Overview ». *SSRN Electronic Journal*. doi:10.2139/ssrn.3395665.

EEG power spectral measures of cognitive workload : Psychophysiology. s. d. Consulté 30 janvier 2026. https://www.ovid.com/journals/psych/fulltext/10.1111/psyp.14009~eeg-power-spectral-measures-of-cognitive-workload-a.

Fu, Shaoxiong, Hongxiu Li, Yong Liu, Henri Pirkkalainen, et Markus Salo. 2020. « Social media overload, exhaustion, and use discontinuance: Examining the effects of information overload,

system feature overload, and social overload ». *Information Processing & Management* 57(6):102307. doi:10.1016/j.ipm.2020.102307.

Guldenmund, F. W. 2000. « The nature of safety culture: a review of theory and research ». *Safety Science* 34(1):215-57. doi:10.1016/S0925-7535(00)00014-X.

Hafezad Abdullah, Khairul. 2022. « PUBLICATION TRENDS AND THEMATIC EVOLUTION OF SAFETY MOTIVATION RESEARCH: A BIBLIOMETRIC REVIEW ». *Proceedings on Engineering Sciences* 3(2):187-98. doi:10.24874/PES03.02.006.

Hennink, Monique, et Bonnie N. Kaiser. 2022. « Sample Sizes for Saturation in Qualitative Research: A Systematic Review of Empirical Tests ». *Social Science & Medicine* 292:114523. doi:10.1016/j.socscimed.2021.114523.

Jafar, Zain, Jonathan D. Quick, Heidi J. Larson, Verner Venegas-Vera, Philip Napoli, Godfrey Musuka, Tafadzwa Dzinamarira, Kolar Sridara Meena, T. Raju Kanmani, et Eszter Rimányi. 2023. « Social media for public health: Reaping the benefits, mitigating the harms ». *Health Promotion Perspectives* 13(2):105-12. doi:10.34172/hpp.2023.13.

Laroche, Elena, Sylvain L'Espérance, et Elaine Mosconi. 2020. « Use of social media platforms for promoting healthy employee lifestyles and occupational health and safety prevention: A systematic review ». *Safety Science* 131:104931. doi:10.1016/j.ssci.2020.104931.

Meltwater. 2024. « Digital 2024: Global Social Media Users Pass 5 Billion Milestone ». https://www.globenewswire.com/news-release/2024/01/31/2820696/0/en/Digital-2024-Global-social-media-users-pass-5-billion-milestone.html.

Meta CEO Zuckerberg says Instagram has grown to 3 billion monthly active users. 2025. *Reuters*, septembre 24.

Nævestad, Tor-Olav, Ingeborg Storesund Hesjevoll, Karen Ranestad, et Stian Antonsen. 2019. « Strategies regulatory authorities can use to influence safety culture in organizations: Lessons based on experiences from three sectors ». *Safety Science* 118:409-23. doi:10.1016/j.ssci.2019.05.020.

Naji, Gehad Mohammed Ahmed, Ahmad Shahrul Nizam Isha, Abdulsamad Alazzani, Muhammad Shoaib Saleem, et Mohammed Alzoraiki. 2022. « Assessing the Mediating Role of Safety Communication Between Safety Culture and Employees Safety Performance ». *Frontiers in Public Health* 10:840281. doi:10.3389/fpubh.2022.840281.

Nieminen, Hannu, Claudia Padovani, et Helena Sousa. 2023. « Why Has the EU Been Late in Regulating Social Media Platforms? » *Javnost - The Public* 30(2):174-96. doi:10.1080/13183222.2023.2200717.

Odrakiewicz, Dr Peter. s. d. « CHAIR OF EDITORIAL BOARD ».

Pendleton, Marcus, Richard Garcia-Lebron, et Shouhuai Xu. 2016. « A Survey on Security Metrics ».

Rebello, Clara B., Kiana L. C. Reddock, Sonia Ghir, Angelie Ignacio, et Gerald C. Cupchik. 2024. « Self-Regulation of Internet Behaviors on Social Media Platforms ». *Societies* 14(11):220. doi:10.3390/soc14110220.

Safety Culture and Social Media. s. d. Consulté 30 octobre 2025. https://proactsafety.com/articles/safety-culture-and-social-media.

Sajithra K, Sajithra K. 2013. « Social Media – History and Components ». *IOSR Journal of Business and Management* 7(1):69-74. doi:10.9790/487X-0716974.

Shamsuddin, KA, MNC Ani, AK Ismail, et MR Ibrahim. s. d. « Investigation the Safety, Health and Environment (SHE) Protection in Construction Area ». 02(06).

Sharma, Kapil, et Shobhit Srivastava. 2018. « Failure Mode and Effect Analysis (FMEA) Implementation: A Literature Review ».

Tkalac Verčič, Ana, et Dejan Verčič. 2025. « The Internal Communication Paradox: Balancing Digital Convenience with Face-to-Face Satisfaction ». *Public Relations Review* 51(3):102587. doi:10.1016/j.pubrev.2025.102587.

Yang, Maya. 2022. « Clothing Brand Carhartt in Conservative Crosshairs for Issuing Vaccine Directive ». *The Guardian*, janvier 20.

Zhou, Song, Qingli Guan, Huaqi Yang, et Yiheng Cao. 2024. « Navigating the Social Media Landscape: Unraveling the Intricacies of Safety Perceptions ». *Humanities and Social Sciences Communications* 11(1):1420. doi:10.1057/s41599-024-03836-2.

Hart Blanton and Charlene Christie. 2023. “Deviance Regulation: A Theory of Action and Identity” DOI: 10.1037/1089-2680.7.2.115

Marina Rizzi. 2014. “Self-Regulation of Social Media and the Evolution of Content: a Cross-Platform Analysis”

Muhammad Muslim Rusli1*, Zalina Abdul Halim2, Amirah Sabirah Mujahid.2025. “Regulating Social Media Responses to Online Harms: A comparative study between the European Union (EU) and Malaysia”. DOI: https://doi.org/10.21834/e-bpj.v10iSI33.7065

Andrzej Pacana, Karolina Czerwińska. 2025. “Validation of the use of KPIs to measure information security management system performance in manufacturing companies “. DOI: 10.30657/pea.2025.31.26

V S Serdyuk et al 2020 IOP Conf. Ser.: Earth Environ. Sci. 408 012025. IOP Publishing. “Ensuring safety of labor on the basis of the method “Curve of Badles” “ doi:10.1088/1755-1315/408/1/012025

Jean-Christophe Le Coze. De l’investigation d’accident à l’évaluation de la sécurité industrielle: proposition d’un cadre interdisciplinaire (concepts, méthode, modèle). Gestion et management. École Nationale Supérieure des Mines de Paris, 2011. Français. NNT: 2011ENMP0030. pastel-00636888

“Road Safety Perception Questionnaire (RSPQ) in Latin America: A Development and Validation Study” Fabricio Esteban Espinoza Molina, Blanca del Valle Arenas Ramirez, Francisco Aparicio Izquierdo and Diana Carolina Zúñiga Ortega. 2021. “Road Safety Perception Questionnaire (RSPQ) in Latin America: A Development and Validation Study”. DOI https://doi.org/10.3390/ijerph18052433.