FINAL REPORT ON A PROJECT

"Large-scale empirical investigation to develop a compendium of best practices to improve the quality of internal risk information transmission within critical industries"

Principal Investigator	Prof. em. Dr. Didier Sornette
Co-applicant	Dr. Dmitry Chernov
Project team	Dr. Dmitry Chernov, Prof. em. Dr. Didier Sornette, Dr. Ali Ayoub (MIT), Prof. Dr. Giovanni Sansavini
Type of project	Research Professorship Scholarship / Fellowship Infrastructure / Equipment Teaching
Project status	Running Finished
Key words	Risk information transmission, critical industries (nuclear power, oil and gas, chemical and petrochemical industries, hydropower power, mining)
Department at ETHZ	Chair of Entrepreneurial Risks (D-MTEC)/ Reliability and Risk Engineering (Institute of Energy and Process Engineering)
Background	Prior to industrial disasters — such as Challenger space shuttle accident in 1986, the Chernobyl nuclear disaster in 1986, the Deepwater Horizon oil spill in 2010, Fukushima-Daiichi nuclear disaster in 2011 — some employees of the affected organization were aware of dangerous conditions that had the potential to escalate to a critical level. However, for a variety of reasons, the information about these risky conditions was not delivered to decision-makers in time.
Project description	The Project aims at developing solutions and practical recommendations for improving the internal transmission of risk information within critical infrastructure companies. The objectives of the project are as follows: · To establish practical solutions to improve the quality of internal risk information transmission within critical industries based on interviews with top management, technical managers and safety managers of leading critical infrastructure companies all around the world (nuclear power, oil and gas, the chemical and petrochemical industries, hydropower power and mining). · To elaborate detailed improvements of the internal risk transmission practice to be recommended to organizations/industries that have met with disasters caused by a failure of risk transmission. · To systematize the existing best available corporate practices in internal risk transmission that can be found in leading companies in critical industries all around the world. · To develop a handbook clearly explaining the best practices and effective solutions in internal risk transmission systems in critical industry companies. When timely risk information exchange could become the standard practice within the critical industries, insurers will be able to assess more adequately the risks of the insured and, more importantly, major industrial accidents could be averted. The project thus combines various fields of research and technical cooperation such as general management, organizational studies, communication theory, risk communication and decision-making.
Timeline	Start: 2019 End: 2022
Donors	SCOR Foundation for Science and ETHZ's Reliability and Risk Engineering (Institute of Energy and Process Engineering) (co-financing of the Project from June 2018 until the end of 2022)

EXECUTIVE SUMMARY OF PROJECT FINDINGS

Between October 2018 and June 2021, the project team conducted 100 interviews with top management, technical managers and safety managers of 65 leading critical infrastructure companies in Western Europe (41% of all respondents), Russia (32%), North America (10%), the Middle East (9%), Africa (5%) and Australia (3%). Interviewees were drawn from the following industries: power generation and transmission (40% of all respondents), oil and gas (36%), chemicals and petrochemicals (9%), mining (6%), metallurgy (6%) and other industries (3%). The team asked practitioners managing critical infrastructure for their views on why employees are reluctant to disclose risks when dealing with managers, why managers are reluctant to receive risk information, who is primarily responsible for creating an internal climate where it is not acceptable to talk about problems in an organization and what needs to do in order to improve the speed and quality of risk information transmission within a large critical infrastructure company. On the basis of their answers, the team wrote the handbook "*Averting disaster before it strikes: how to make sure your subordinates warn you while there is still time to act*" in 2021-2023.

This handbook is about how to transform the way large critical infrastructure companies communicate about safety and technological risks. It aims to support senior managers to get the information they need from their subordinates concerning the risks they are facing, in order to prevent accidents before it is too late.

The handbook is written for the owners, senior managers, and industrial safety directors of critical infrastructure companies. It is also relevant to consultants in the field of labor protection and industrial safety, specialists in the field of industrial risk insurance, and regulators of critical infrastructure facilities.

This handbook has several goals:

- to show that the problem with the prompt and accurate reporting of risks exists in many critical infrastructure companies and has been the cause, or one of the causes, of several major disasters at critical infrastructure facilities worldwide (Chapter 1);
- to elaborate the reasons why information about risks is concealed within large industrial companies — why subordinates hide the risks they can see in their area of competence from management, and why managers do not want to hear about the problems and risks their subordinates face (Chapter 2);
- to make practical recommendations to the owners and senior managers of critical infrastructure companies on how they can significantly improve intra-organizational risk communication (Chapter 3);
- to give a practical example of a pilot project to radically improve the quality and speed of risk information transmission in a world-leading industrial company (Chapter 4);
- finally, to discuss (I) the prospects for automating the collection of risk-related information when it comes to the operation of equipment in critical infrastructures, and the potential role of artificial intelligence in this endeavor, (II) the potential benefits and drawbacks of disclosing information about the critical risks of large industrial companies to insurance companies in exchange for lower insurance premiums, and (III) the discernible variations in the way risk-related information is communicated in companies across different countries, cultures, and regions (Discussion section).

The recommendations of 100 leaders were also tested in the pilot project, in an industrial company which is the world leader in its sector. More than 400 managers at various hierarchical levels and employees at several of the company's industrial plants took part in the pilot project.

Most importantly, the handbook explains what senior managers can do for improving the quality and speed of reporting about safety and technological risks within companies that operate critical infrastructure facilities. The handbook is intended to provide leaders of these companies with simple and practical solutions to overcome the problems of intra-organizational transmission of information about risks.

THE PROBLEM (CHAPTER 1)

After a major disaster, when investigators are piecing together the story of what happened, a striking fact often emerges: before disaster struck, some people in the organization involved were aware of dangerous conditions that had the potential to escalate to a critical level. But for a variety of reasons, this crucial information did not reach decision-makers. Therefore, the organization kept moving ever closer to catastrophe, effectively unaware of the possible threats. In the event of an accident, losses and costs for dealing with the consequences are often hundreds — or even thousands — of times greater than the finances that would have been required to deal with the risks when they were first recognized, and before they led to a major accident. Due to the asymmetry of risk information at different levels of the corporate hierarchy of critical infrastructure companies, preventive decisions were not taken in a timely manner. Ultimately, this led to the organizations facing catastrophic events. This observation has been documented in the following major technological accidents: Challenger space shuttle explosion (USA, 1986); Chernobyl nuclear power plant disaster (USSR, 1986); Sayano-Shushenskaya hydropower plant accident (Russia, 2009); Deepwater Horizon oil spill (USA, 2010); Fukushima-1 nuclear power plant disaster (Japan, 2011); methane explosions at American and Russian coal mines in the 2010s, and in several other disasters. Detailed information on the importance of this issue for many critical infrastructure companies worldwide is presented in Chapter 1.

WHY THE PROBLEM EXISTS (CHAPTER 2)

Chapter 2 takes a detailed look at the reasons why there is a problem with transmission of objective information about safety and technological risks in large critical infrastructure companies.

WHO CREATES AN INTERNAL CLIMATE WITHIN AN ORGANIZATION WHERE IT IS NOT ACCEPTABLE TO TALK ABOUT PROBLEMS?

97% of interviewees (97 out of 100 respondents) answered that most of the blame lies with managers. 2% of respondents argued that the responsibility is equally shared by managers and subordinates. 1% of respondents believed that the reasons for such an internal corporate atmosphere lay mostly in the personal qualities of individuals and their relationship with colleagues, and not in their organizational roles, whether manager or subordinate. None of the respondents placed the main responsibility on employees.

TOP 10 REASONS WHY LEADERS DO NOT WANT TO HEAR ABOUT PROBLEMS FROM THEIR SUBORDINATES

1. Tackling reported problems will be costly, and owners and shareholders are imposing strict financial and production targets (58%: 58 out of 100 respondents). Senior managers do not want to hear about problems from their subordinates because the costs of addressing any serious issue in a critical infrastructure company will be very high. In addition, owners and shareholders are often imposing strict financial and production targets on their senior managers already. Reports from employees about any serious safety and technological problem may threaten the implementation of these plans, as well as negatively affecting the career and the earnings of senior managers.

2. Managers are afraid of being seen as incompetent if they take responsibility for previous bad decisions that have created current problems (38%). When employees inform managers about any serious problem and risk, they are indirectly hinting towards the bad decisions and mistakes made by managers in the past that have led to the problem developing in the first place. Rather than admitting that they may have made a mistake, managers try not to hear about or respond to current problems.

3. Senior management assume that, once they have been told about a problem, they will need to solve it (36%). Managers are afraid that, if an employee informs them about a problem, the responsibility to solve it is automatically transferred on their shoulders.

4. Senior managers expect employees to solve problems independently in their area of responsibility (28%). Some managers prefer not to pay attention to warnings from employees, because they believe that employees are paid well enough and should be able to deal with problems that arise independently, without involving them.

5. Senior management prefer not to know about risks, in order to avoid being held responsible (including legal responsibility) if things go wrong (27%). Some managers do not want to hear about existing risks from

their employees because they do not want to be held legally responsible for an accident or emergency. Irrationally but perhaps understandably, they believe that, if risk information does not reach management, the responsibility for the onset of an emergency remains entirely with their subordinates who are managing the facility involved. This has some basis in experience. During investigations following major accidents in critical industries worldwide, some senior executives were able to avoid criminal liability because they claimed they had not been aware of the problems that ultimately led to the accidents — while their subordinates, unable to plead ignorance, were punished.

6. Leaders do not want to step out of their comfort zone to solve complex questions (26%). Some leaders do not want to step out of their comfort zone, change their routine, and take on extra work to react to problems their employees have warned them about. This may as well sometimes imply that managers have to rush to a production site in a remote region to deal with the problem on the spot.

7. Leaders are people too — like anyone, they would rather hear good news than bad ones (24%). One should remember that leaders are just humans underneath, and it is just human nature to prefer good news rather than bad.

8. Managers see issues reported by employees as unimportant (23%). From the perspective of some managers, most of the problems employees bring to senior management are insignificant. As a result, some executives are reluctant to hear about the concerns of rank-and-file employees and do not want to have to respond, as for them these are minor issues. But with this approach, there is the chance that vital information about critical risks may be overlooked.

9. Short-term contracts for managers (19%). The reluctance of some managers to hear about serious problems is influenced by their own short-term contracts, as part of a company's short-term corporate goals. The short-term contracts of senior managers (up to 3 years) are detrimental to creating a favorable environment for the reporting of information about risks. Leaders feel under pressure to show shareholders a quick positive result, therefore they are unwilling to receive bad news about production issues that will require time and money to rectify. Solving serious problems in critical infrastructure companies generally requires sustained effort over many years.

10. A common corporate leadership culture pervades the entire company and industry (15%). An industry's accepted "*code of conduct*" and a company's accumulated corporate culture together predetermine the behavior of senior managers in any given company, and in turn foster a pathological corporate culture that discourages honest and accurate communication through the corporate hierarchy.

TOP 10 REASONS WHY EMPLOYEES ARE RELUCTANT TO DISCLOSE RISKS TO THEIR SUPERVISORS

1. Fear of blame and punishment from executives: subordinates assume that they will be held responsible for the occurrence of any problem they report to their managers (63%). Employees are afraid that, if they raise the alarm about a problem, management will accuse them of having caused or exacerbated it through their mistakes. In most cases, problems do not arise from nothing. They usually develop partly because of poor decision-making by managers (for example a refusal to approve adequate resources to keep facilities running safely) and partly through the actions of employees who may have been forced to violate operational safety to meet production targets dictated by managers.

2. Employees are afraid of losing income and ruining their career prospects by looking incompetent in the eyes of their bosses (48%). The fear of losing earnings and damaging their own career prospects stops many employees from reporting serious problems and risks within their area of competence.

3. Inertia of corporate culture (43%). Most employees will go along with the corporate culture that exists in their company. If that culture dictates secrecy about problems, demands only good news, and punishes staff for the presence of problems on their watch, then most employees will simply not inform the authorities. If managers are unwilling to listen when employees raise concerns, this will eventually lead to an ingrained culture of lies at every level of an organization.

4. Fear of destroying relationships with colleagues or line managers (32%). Many employees do not disclose risks to their bosses because they think this will ruin their relationship with their colleagues, or with their immediate supervisor.

5. Fear that employees will be expected to solve any problem they report (27%). Employees are afraid that, if they report a problem to senior management, they will be left to handle it themselves with no extra resources to do so.

6. Employees do not fully understand the risks they are running, and lack the training or experience to assess their criticality (22%). Sometimes employees do not realize the risks they encounter in their day-to-day work, so they do not inform their superiors about them. If people are not aware they are taking risks, they are unlikely to think that they are doing anything wrong, and will see no reason to inform anyone. It will generally be employees who are unqualified or inexperienced, who fail to recognize or assess risks. Sometimes employees only care about their own area of work and do not want to look at the risk picture across the entire production process. In this case, they are unlikely to report problems outside their own limited area of competence.

7. Employees feel it is pointless to report risk information because managers failed to respond to similar messages in the past (21%). Some employees see little point in informing their superiors about problems or risks, because there has been no response to previous warnings and the problems have remained unsolved. Frustrated by this lack of action, some employees simply stop telling their superiors about problems, assuming that their efforts will be futile.

8. Fear of being seen as disloyal to a company, as a rebel who wants to "*rock the boat*" or as a "*bad news guy*" (20%). When employees start to "*ring the alarm bells*" and draw attention to problems, they will be perceived by their superiors as rebels, *"black sheep",* troublemakers who want to *"rock the boat"* or "*go on the rampage*". Most managers are afraid of such potential disruption, which could lead to earlier management mistakes coming to light. Consequently, they will often berate would-be whistle-blowers: "*All your colleagues are quite happy, but you always seem to have a problem with something. You think you're special and you want to wash our dirty linen in public*".

9. Industrial safety performance indicators and reward systems encourage concealment (15%). Corporations use many key performance indicators to manage their productivity. Some of these metrics can incentivize employees to downgrade an incident, and under-report equipment problems or anything else that could stand in the way of hitting ambitious corporate targets.

10. Some employees are confident that they can solve the problem on their own (13%). Employees can sometimes be overconfident in their own capabilities to solve a problem. If subordinates have a strong sense of ownership, they will be tempted to solve problems by themselves and then report their success, rather than reporting the problem to the manager and waiting for them to come up with a solution. In doing so, they may overestimate their capabilities and convince themselves that there is no immediate need to inform their superiors about it.

HOW THE PROBLEM CAN BE SOLVED (CHAPTERS 3 and 4)

RECOMMENDATIONS FOR OWNERS AND SENIOR MANAGEMENT: TEN PRACTICAL WAYS TO IMPROVE THE QUALITY AND SPEED OF RISK INFORMATION TRANSMISSION WITHIN CRITICAL INFRASTRUCTURE ORGANIZATIONS

The handbook draws on information received from 100 practitioners in industry, and the results of a decade of research on the reasons for concealing risks before and after major technological accidents. Together they inform some clear practical recommendations for owners and managers of large industrial companies, who want to fundamentally improve the transmission of risk information within their organization, in order to prevent serious industrial accidents. A detailed account of the recommendations is presented in Chapter 3.

1. Owners and senior management should be willing to give up short-term profits in exchange for the long-term stability of critical infrastructure. Fundamental improvements in the quality and speed of reporting critical risks within a critical infrastructure company are possible only when the owners and senior management are willing to focus on the long-term ownership of the company. This involves accepting that the significant costs required to manage existing serious and critical risks may impact short-term profits, but are essential to protect the long-term reliability, sustainability, and value of the company. If owners are willing to allocate resources to prevent critical problems, then their managers will follow suit and begin to pay attention to these safety issues. The changed view regarding safety in the minds of senior management will lead over time to a change in attitudes and working practices throughout the company. To operate

sustainably in the long term, a critical infrastructure company must find a balance between safety, finance, and production. The task of top management is to create a system that allows managers at every level to freely analyze and discuss risks and to find the acceptable balance.

2. Senior management should be approachable about problems, and have the desire and resources to control and mitigate identified risks. Everything comes from leadership. Employees will report problems if managers want to hear them. Managers should want as much information as possible about potential risks. If the management support is not there, all other interventions are doomed to fail. The only way to improve the situation regarding feedback in an organization is if leaders have a genuine desire to hear about risks from their subordinates — and communicate this to them — and then take decisions and allocate resources to stop risk escalation. Senior managers should have the necessary support — moral and practical — from owners and shareholders to implement risk reduction measures. Having secured this, they should then take the initiative to implement cultural change, dismantling any system of penalties for reporting risks or incidents, and making it clear that they actively want to hear about problems. Only then will employees, inspired by the evident commitment of their leaders to a safer workplace, be willing to report the risks they have encountered.

3. Risks must be prioritized, as it is impossible to manage every risk within an organization simultaneously. It is impossible to effectively manage all risks — prioritization is essential. Resources are always limited and will never be sufficient to mitigate every possible risk. Without establishing clear priorities, managers have so much information to handle that they cannot distinguish what is important from what is not. A gradation of risks immediately makes the situation clearer — what further information is required, which risks need monitoring, and which demand urgent action so that *"major negative events"* can be prevented. It is vital that critical risks and problems that may threaten the work of an entire enterprise come swiftly to the attention of senior managers so that they can immediately inform the highest level of the hierarchy, while less serious risks can be delegated to appropriate lower levels of management for further action. For effective decision-making, you need to have a system in place to deliver an integrated risk assessment of production processes, where all the key risks of an industrial facility are assessed and then ranked by severity. This will enable an organization to prioritize the allocation of risk management resources. Not all employees in the organization are dealing with critical risks — only a limited circle of managers and employees is responsible for this. Senior managers should start by working on the control and reduction of critical risks with those managers and employees who manage them.

4. Senior managers must be leaders in safety. It is imperative that any initiative to prioritize safe operation of critical infrastructure comes from senior management. In highly hierarchical companies, the example set by the leader is paramount. Most critical infrastructure companies have several management levels and are quite bureaucratic. If subordinates see that safety is extremely important to the CEO, and the entire corporate system makes it a top priority, then most employees will imitate senior management and follow the principles they are espousing. If safety is made the top priority by the CEO, then production site workers have no grounds for relegating it down the list of their own priorities, and will instead be willing to place it first, above production and profitability indicators.

5. Senior management should build an atmosphere of trust and security so that employees feel safe to disclose risk-related information. Without trust in the leadership, there can be no high-quality feedback from employees on the problems of an organization. Often, employees evaluate the possible consequences of disclosing risk information based on rumors about how senior management reacted in a previous situation with colleagues. Employees project both the positive and negative experiences of their colleagues onto themselves. Employees need to have security guarantees, both for their careers and for their colleagues. Managers must guarantee the security of their sources and take responsibility for solving any significant problem they are informed about. If an environment can be established where employees do not feel under threat, they will begin to give candid feedback. To increase employee confidence, it is essential to reduce their uncertainty about the actions of managers. Managers need to demonstrate exactly how employees are treated when they give honest feedback. Only through repeated positive responses from managers will it be possible to dispel the common perception that an organization can be dangerous to employees who speak out. The first step is for senior management to make a declaration that feedback is encouraged at all levels of a company. Nevertheless, this is not enough in itself: employees must see the truth of the statement applied in practice, with employees receiving praise and not punishment for offering honest feedback. The message that senior management actively wants to hear about problems, and that it is safe for employees to tell them, should come right from the top of the hierarchy. It is important that the CEO and senior executives give employees specific examples of their colleagues' positive experiences of communicating problems to their seniors. It is also vital that managers demonstrate respect for their subordinates, including a sincere interest

in their well-being, safety, and progress. If these principles are applied reliably across the board, then even the most cautious employees will gradually come round to the idea that a company is a safe environment, where they can confidently reveal their concerns about the situation on the ground without any negative consequences.

6. Middle management are allies of senior management in building an organization where active dialogue between superiors and subordinates is welcomed. Senior management can only build an effective system to obtain accurate information about risks, and change the safety culture in a company, by working with the middle managerial level. Therefore, the best strategy is to make middle managers allies and not enemies. The middle managers in charge of the production facilities know more about the situation at an organization than shop floor employees and lower-level managers. If senior managers only ask for the opinion of shop floor employees about the critical risks of an organization, they may not always get an accurate assessment of the situation. Getting information about critical risks only from lower-level employees may just lead to an increase in information noise, making it more difficult for senior management to understand the true picture of safety at a site. Once honest dialogue has been established between senior management and owners about critical risks and how to handle them, the next step is to establish the same honest dialogue between the leadership and the middle management level. Senior management should emphasize that they trust middle management. They must ensure that middle managers disclosing risks and problems are not penalized or dismissed. They must show that they want to work together with middle managers to solve problems, and not leave them to tackle issues alone. They must appreciate and reward subordinates who provide accurate information. It is also important that middle managers have the opportunity to adjust the production plans set by headquarters, so that they have the authority to stop suspicious pieces of asset for repair and the resources to carry out these repairs.

7. Use different upward risk transmission channels. In addition to receiving information through the traditional management hierarchy, senior managers are encouraged to regularly visit industrial sites to hear directly from managers and employees regarding the critical risks they are facing. It is also recommended to use other alternative channels for obtaining information about risks, such as: fault logs or risk registers/databases; safety training observation program cards; smartphone apps to allow shop floor employees or lower-level managers to timely report risks to senior managers directly; independent production monitoring systems; process improvement proposals; problem-solving boards; and anonymous mailboxes and helplines.

8. The words of leaders should be supported by their actions: problems once identified need to be solved. Leaders should never say one thing and then do another — their words must be matched by their deeds. This is especially relevant if senior managers call for risk disclosure, and then consistently address the issues that their subordinates bring to their attention. When employees report risks and problems, they do so in the belief that managers will make the right decisions to solve the problem or at least reduce the risk. A critical infrastructure company may well not have enough resources to solve all the problems identified at any given time. If this is the case, then managers must be sure to feed back to the employee who reported an issue, and assure them that they will tackle the problem when they can. If identified problems are not satisfactorily solved, then employees will inevitably lose faith, and will not bother to disclose risks to their superiors anymore.

9. Do not penalize specific employees: look for systemic defects within the organization. Executives should not penalize individual employees for incidents, but instead look for the systemic shortcomings in a company's operations that forced the employees to commit safety breaches.

10. Reward employees for disclosure of safety and technological risks. The best way to reward employees is to recognize their important contribution to an organization, as everyone derives fulfillment from having their work appreciated and praised. Management should deliver this not just through a private conversation, but in front of the whole workforce. Expressing gratitude publicly in this fashion provides an opportunity for senior management to highlight the kind of behavior and performance they wish to see from all their employees. Public recognition will motivate the employee to even greater efforts and encourage colleagues to communicate new risks and problems up through the hierarchy. According to most respondents, non-financial motivation is more effective than material incentives, which have many disadvantages. There are many effective ways to motivate employees for disclosing information about risks, which do not involve financial reward.

PILOT PROJECT EXPERIENCE OF INTRODUCING A SYSTEM FOR TRANSMITTING INFORMATION ON SAFETY AND TECHNOLOGICAL PROBLEMS WITHIN A CRITICAL INFRASTRUCTURE COMPANY

Chapter 4 presents detailed information about the pilot project, which tested various methods for significantly improving the quality and speed of reporting information about safety and technological problems within the critical infrastructure company. The project involved more than 400 employees (from senior management to shop floor employees) of an industrial company that is a world leader in its field. Within the just first few months of the introduction of the project, shop floor employees and line managers disclosed seven critical risks to senior management that they believed had the potential to lead to accidents resulting in either the death of personnel, long-term decommissioning of production facilities, and significant environmental issues. All these risks were quickly addressed by senior management and production site leaders. In several cases, these prompt disclosures and interventions prevented serious incidents from developing. Employees also disclosed to senior management 104 other problems that were compromising the industrial safety of four of the company's production sites. Most of these issues have also now been resolved.

The success of the project indicates that, with suitable information transmission systems in place, shop floor employees and line managers are willing to disclose to senior management serious safety and technological problems in their area of responsibility, in order to prevent emergencies.

The authors of the handbook aim to create a proven mechanism — a universal standard — over the next 10 years to fundamentally improve the quality and speed of reporting about critical risks in companies operating critical infrastructure by implementing similar projects in different countries worldwide. The overarching goal is clear: to prevent industrial accidents and disasters from occurring in the first place, to save people's lives, reduce environmental damage, and increase the resilience of critical infrastructure facilities.

DISCUSSION

The handbook ends with a discussion on the following three topical issues.

AUTOMATING THE COLLECTION OF INFORMATION ABOUT EQUIPMENT OPERATION IN CRITICAL INFRASTRUCTURES, AND THE PROSPECTS FOR ARTIFICIAL INTELLIGENCE (AI)

Most of the interviewees are positive about developing automated systems to collect complex information about the functioning of critical equipment, which continuously transmit feedback on their condition and operation to headquarters.

Most of the respondents stressed that the degree of automation of information collection depends primarily on economic feasibility. The main criterion for assessing the feasibility of introducing an automated system should be the level of risk that it can remove.

The obvious advantage of such automation is its ability to reduce the influence of the subjective human factor: once it is set up and running reliably, there is no further need for the manual collection, processing, and transmission of information about critical risks through the traditional management hierarchy. It is very important that, in such automated systems, there is no manual data entry to exclude the possibility of any manipulation of data by employees or managers at different levels. However, assessing feedback from the system and informing a management decision is hardly possible without human involvement. Therefore, at this stage automation is only possible up to a certain extent.

It is important to note that the influence of the human factor will never drop to zero in the coming decades. Automated systems cannot replace highly professional employees, who can diagnose the operation of complex but outdated equipment — basing their assessments not only on data from sensors, but also on the intuition they have developed over many years of experience. This experientially grounded intuition is particularly important when analyzing the work of complex interdependent technical systems.

Cyber risks should also be considered when implementing automated systems: with the growth of automation, the risk to companies from network failures and unauthorized access will grow.

Respondents expressed skepticism about extending AI to making decisions in the operation of critical infrastructure. Many risks can be introduced if AI is allowed to independently decide on serious operational issues. Therefore, the final decision must still be left to professional operators, supported by analytical

information from the AI system. AI can be allowed to make secondary decisions, where the scale of any possible damage is limited. AI is best used to analyze large amounts of data, creating broader analytics to inform smarter leadership decisions. Additionally, AI is helpful for generating various scenarios of future situations in the company.

DISCLOSURE OF CRITICAL RISKS TO INSURANCE COMPANIES IN EXCHANGE FOR REDUCED PREMIUMS

As part of the in-depth interviews with the executives of critical infrastructure companies worldwide, the authors wanted to know their views on whether it is worth disclosing the critical risks of their businesses to insurance companies in exchange for lower insurance premiums.

In the study, 93 respondents answered this question. 57 of them (61%) reacted positively to the idea that a critical infrastructure company should fully disclose to the insurer all information it knows about its own critical risks in exchange for a reduction in insurance premium. 24 respondents (26%) expressed skepticism or were against such an exchange. 12 respondents (13%) found it difficult to answer this question.

This section portrays the divergent views on the pros and cons of a proposal to disclose information about risks in exchange for a reduction in insurance premiums. Successful practical examples of interaction between critical infrastructure companies and insurance companies are also presented.

IMPACT OF NATIONAL CULTURE ON RISK INFORMATION TRANSMISSION WITHIN CRITICAL INFRASTRUCTURE COMPANIES

Some of the respondents have worked in several countries and continents. They were asked if they noticed an effect of national and cultural differences on the reporting and discussion of risk. All the leaders interviewed, who have international work experience, agreed that communication about risks within organizations is significantly influenced by the peculiarities of national culture, religion, and worldview. The interviewers asked the respondents to compile their subjective ratings of the quality of internal risk communication in the countries where they have worked. First, the respondents gave examples of countries and cultures where they felt that risk information from subordinates to superiors was significantly distorted in reports. Then, they described countries where risk information was transmitted without significant distortion. They explained why they thought some countries and cultures have problems with objective feedback, while in other countries this problem does not seem to be so pronounced.

Many respondents expressed the view that, in all cultures on the planet, people want to present themselves to others in the best possible light. In any society, any group of people, nobody likes to receive bad news — so nobody wants to be the bearer of bad news. The only question is how it is customary in different societies to react to it. There are hierarchies in every society, but the management style — the way managers manage their subordinates — differs.

All the interviewees in their own way conveyed the idea that the key factors affecting the quality of information sent up a company hierarchy are the power distance between managers and employees, and related to that, the traditions of authoritarian (monologue) or democratic (dialogue) governance in the country.

CONCLUSION

The goal of writing this handbook was to provide executives that operate critical infrastructure with practical tools and solutions, so that they can improve the quality and speed of risk communication in their companies. Better information makes for better decisions, and these in turn have an impact on reducing the likelihood of severe accidents at industrial facilities. The authors hope that this handbook will help prevent major emergencies and save many lives.

APPROVED PUBLICATIONS OF THE RESEARCH'S RESULTS

- **2022 (Switzerland):** Dmitry Chernov, Didier Sornette, Giovanni Sansavini, Ali Ayoub, *Don't Tell the Boss! How poor communication on risks within organizations causes major catastrophes*, Springer, 2022 (results of the team's research into why there is a problem with the objective reporting of safety and technological risks in large critical infrastructure companies).
- **2023 - June-August (Switzerland):** Dmitry Chernov, Ali Ayoub, Giovanni Sansavini, Didier Sornette, *Averting disaster before it strikes: how to make sure your subordinates warn you while there is still time to act*, Springer, 2023 (English language)
- **2023 - April (Russia):** Dmitry Chernov, Ali Ayoub, Giovanni Sansavini, Didier Sornette, *Как руководителям получать информацию о риске наступления аварии до того, как эта авария может произойти*, State University of Management, 2023 (Russian language)

POTENTIAL PUBLICATIONS OF THE RESEARCH'S RESULTS

- **2024 (Japan):** Dmitry Chernov, Didier Sornette, Ali Ayoub, Giovanni Sansavini, *Don't Tell the Boss! How poor communication on risks within organizations causes major catastrophes + Averting disaster before it strikes: how to make sure your subordinates warn you while there is still time to act*, Soshisha Publishing Co., 2024 (In 2017, Soshisha Publishing Co. published the project leaders' previous book "*Man-made Catastrophes and Risk Information Concealment"*. The book received very positive responses from Japanese readers. The project team has an idea about the publication of a superbook — combining "*Don't Tell the Boss!"* and *"Averting disaster before it strikes"* under one title — in Japan. As of February 2023, the team does not have an agreement with the publisher, but will work towards this during spring 2023. If there is a positive decision, the superbook will be prepared for publication during 2023 and could be published in 2024).