Risk Analysis: Challenges and Perspectives

Jean-Christophe Le Coze, Thomas Marcon, Agnès Vallée, François Massé, Emmanuel Plot, Chabane Mazri, Marine Boutillon

Risk Analysis: Challenges and Perspectives

Jean-Christophe Le Coze*, Thomas Marcon, Agnès Vallée, François Massé, Emmanuel Plot, Chabane Mazri, Marine Boutillon

Ineris, Verneuil en Halatte, France

jean-christophe.lecoze@ineris.fr

Risk analysis (RA) is at the heart of the risk management process and has been the subject of methodological, reflective or critical questions for many years. These questions challenge the foundations, practice and uses of risk analysis (Escande et al, 2016). Drawing on work in science and technology studies (STS), many authors emphasise the subjective, constructed and historically situated nature of risk analysis as opposed to a vision that would be objective and purely rational, detached from contexts. This methodological, reflective and critical knowledge is particularly important in a context of major global changes (Le Coze, 2020). In France, RA is framed by regulations which require operators to produce a safety case. The AZF accident (2001) changed the regulations (Bachelot law of 2003) integrating the probability and greater consideration of the territories and their issues through consultation mechanisms. For the past ten years or so, there have been few developments or questioning of these post-AZF developments. However, RA are confronted with new changes, this time no longer regulatory but digital and environmental. These changes tend to modify the threats, vulnerabilities, expectations and objectives of RA. The purpose of this text is to explore this new context. In the first part, critical work on RA is introduced in order to consider its limits. This clarification is followed by a presentation of initiatives that develop new perspectives on RA then by a discussion.

1. Risk analysis, an analysis from a STS perspective

In recent years, social sciences and philosophy have explained that RA is not an objective practice, but a construction whose limits are intrinsic (Jasanoff, 1993). RA depends on the knowledge available, the models used, the choices on the parameters, the expertise mobilized when identifying the scenarios, etc. However, this assertion that RA is constructed and not purely objective, perfectly accepted from a research point of view, is regularly a source of tension. After Fukushima, a series of arguments were advanced to preserve RA's rationality (Downer, 2014). First, the accident took place because the event fell outside the design provided for by the RA. The 20m wave was well outside what was admitted as possible, and without the wall, the damage would have been much greater. Second, if the accident occurred, it is because the engineers who made the calculations were wrong, and their errors are not representative of the industry, whose standards are higher than those observed in this accident. A third rhetoric relates to the lack of compliance of the company in question (here Tepco for the Fukushima plant). The validity of the calculations are not intrinsically challenged because the operators did not do what was expected of them, thus distorting the calculations, which remain valid. Finally, the last rhetoric, if the accident did happen, it is indeed important to learn the lessons so that it does not happen again. The design and calculations must therefore incorporate this experience feedback to be more able to comply with the reality of the risks. In other words, the AR is improving.

These four arguments help soften the criticism that RA are not objective. However, for each of them, it is highly questionable. Let's go through them, one by one. A scenario beyond design of what was planned is indeed proof of the limits since it amounts to admitting that the RA did not take this possibility into account, for various reasons. The approach is therefore not objective and contains an element of subjectivity. Calculations errors by engineers who would in practice be unrepresentative of the profession is a possibility, but Japan was until then considered to be at the forefront (with plants based on American designs). The lack of compliance of the operator with what

was planned tends to protect RA but also exposes its limits. If RA only considers an ideal that is unrealistic given the concrete operational realities of systems, then such limitations are intrinsic.
Finally, if RAs need to learn from their failures, the question remains whether this learning cycle remains an endless one, because the mistake of the past is unlikely to be the mistake of the future. Protecting the plant better against a tsunami will not help against a meteorite or cyber attack. From Downer's insights based on these 4 arguments, we can retain four limits of the AR: the intensity of scenarios (1), the limits of probability calculations (2), the question of the compliance of practices with the expectations of the AR (3) and finally the endless learning quest (4). This subjective side, or constructed approach to risk analysis makes a lot of sense in current evolutions in the context of safety critical industry and includes issues of cybersecurity, alignment of RA with practices, natech, domino effects or environmental consequences of major events.

2. Risk Analysis Challenges

2.1 Digitalisation and cybersecurity

Today's control systems, developed in the era of Industry 4.0 and Industrial Internet of Things (IIoT), are highly digitalised and connected systems. They rely on communication technologies similar to those found in the IT systems with which they are interconnected. These systems, which have an action in the physical world, manipulate more and more data. They are therefore subject, like all sectors of activity, to more and more cyber attacks. A study by the French Senate shows a multiplication by 4 of ransomware targeting companies in the first half of 2021 compared to the first half of 2020. These attacks can have direct or indirect physical consequences on populations, production assets or the environment. This context leads us to consider cyber threats in the overall analysis of the risks that industrial facilities present to people and the environment.
Well-defined regulatory frameworks, standards and methods exist for the analysis and control of accidental risks, but they are not adapted to the consideration of cyber security. Indeed, the assessment and control over time of risks linked to known accidental phenomena, or at least for which we assume that knowledge is progressing, and risks linked to a conscious and evolving threat are fundamentally different. In addition, the safety of industrial installations only partially takes into account the ICS: the analysis is limited to sensors, actuators and logic controllers (PLCs) whose failures are identified as causes of major accident scenarios or to safety PLCs which operate as risk reduction measure on these scenarios. Finally, accidental RA focuses on the major risks to people, while cybersecurity must also take into account attacks on the availability of production systems and data confidentiality.
On the basis of the risk analysis and assessment - which allows the identification of attack or accident scenarios and the evaluation of their severity and likelihood - technical, human and organizational measures must be implemented to maintain the operation of the installation within the framework defined during the risk analysis. Here again, the control of accidental risks and cybersecurity risks are different: in the first case, the aim is to verify that the hypotheses used for the analysis are verified in the field and that there is no deviation in the set of elements identified for the control of risks; in the second case, it is also necessary to be able to take into account the evolution of the threat, for example by monitoring the publication of vulnerabilities in equipment or software integrated into the industrial control system.
To take into account these new challenges, INERIS has developed a general methodology for the combined analysis of cybersecurity risks and major accident risks. The objective of the approach is to identify attack scenarios with potentially serious consequences for people and the environment. It allows to take into account the physical process and the occupational risk in an extended way in a cybersecurity approach. This approach is based on the coordination of existing methods for the analysis of accidental risks on the one hand and the analysis of risks linked to cyber security on the other: an analysis of physical risks for people and the environment, derived from Preliminary Risk Analysis methods, whose scope of analysis is extended to take into account the specificity of scenarios related to attacks on the industrial control system [6], and an approach derived from computer security focused on the identification of scenarios that may have physical consequences. The articulation of these two approaches leads to a unique representation model called AT/BT (Attack Tree / Bow Tie) (Kriaa et al, 2015).
This articulation requires the use of new skills, linked to computer security, during the risk analysis of an industrial installation to extend the scope of the analysis. This can cause practical difficulties, as the principles, vocabulary, metrics and objectives can sometimes diverge. The common analysis framework between safety and security allows to deal with these antagonisms, to enhance the mutual reinforcements and to reach a more complete vision of the risks generated by hazardous industrial installation (Massé et al, 2018). This new analysis framework introduces new complexities and requires a systemic vision of the installation. Moreover, the control of cybersecurity relies on a permanent monitoring of the threats and vulnerabilities related to the equipment and software used. Digital tools for system description, risk analysis and operational monitoring are necessary to

reach these objectives. Ineris' developments on digital management of RA presented in the following paragraph could help to address these new issues.

2.2 Digitalisation and RA Management

Since 2014, INERIS, with several industrial partners, has been developing an approach on the use of digital technology to improve RAs and their uses. The idea is the following. The more RAs are integrated into operational safety practices, as close as possible to the installations, the more they will be able to improve by coming into contact with the empirical knowledge of operators (design, maintenance, production, logistics, etc.). At the same time, the more the RAs can be criticized and amended, the more they will be able to blend in with the subtleties of singular realities, and the more they will be able to help operators in their daily decisions. Understood as a subjective intellectual construct, RAs face a well-known challenge in management science being the one of actionability. Said simply, actionability refers to the extent to which a knowledge produced by or for an organization is implementable by the intended final users (Antonacopoulou, 2007) in a way that improves their ability to carry their tasks. The question is how to do this? Information technology can help to link and develop safety reports and operational documents (procedures, operating methods, records, etc.). Let's take the example of the management of level detectors for hydrocarbon storage tanks. Several dimensions are to be articulated:

- Regulatory requirements
- The RA which specifies:
  - The functions performed by these detectors within a barrier, and the critical nature of their proper operation given the overall safety architecture
  - The requirements specific to these detectors, which must be respected to qualify them as reliable technical elements
- The management rules for these detectors, throughout their life cycle
- Evidences of compliance with these rules
- Learning from events
- Management of change

The computer tool can facilitate qualitative checks, checks on overall consistency, by facilitating rapid navigation between all these dimensions, to enable the following questions to be answered. Is the response time of the detectors, specified in the analysis of the safety barrier, considered in the choice of equipment? And in the monitoring program? And in the training of the operators in charge? Does the operational management ensure a satisfactory control of all the requirements of the barrier? The IT tool can facilitate quantitative inputs, for example, verification that, over a given period, maintenance actions not carried out or possible malfunctions of the detectors do not jeopardize the achievement of an acceptable criticality from the point of view of accidental and chronical risks. The IT tool can also facilitate the management of modifications, allowing easy navigation in the history of safety cases and operating documents, in order to prepare and trace modifications. For the study and management of a single detector, IT is not useful (it would even be counter-productive). But when you have to manage dozens of detectors, with specificities linked to contexts of use, with dozens of studies, dozens of procedures or operating modes, and hundreds of annual records... and when you have to manage thousands of pieces of equipment... paper documents obscure readability, controls and traceability.

And then, what could be better than to be able to go to the field with a tablet providing the history of the data on the equipment, as well as the procedures and the related RA, and the possibility of entering, directly, in the right place in the computer system, the results of the controls, and to record photos showing the compliance or the possible defects? From this point of view, in no case does the computer system replace the safety case or the operational documents. It only facilitates the control of their coherence, and thus their elaboration. This point is important, because it specifies the scope of the tool, its added value, but also the pace of its implementation and evolution. The use of the IT tool, on which INERIS is currently conducting its operational research moves towards an improvement of safety management.

2.3 RA and Natech

Climate change is another category of change along with the digital which requires reflection on the adaptation of RA. The impact of natural hazards on technological risks (Natech) has been a growing concern for several years now, in a context that has resulted in extreme weather phenomena in certain regions of the world. Like the WHO, which in a recent report underlined the increase in the frequency and intensity of natural disasters as a consequence of climate change, many international bodies, such as the OECD and UNECE for example, have taken up the issue to alert public decision-makers and risk managers. Although relatively dated studies have shown that Natech accidents constitute only 5% of industrial accidents reported in accident databases (Rasmussen, 1995) this value is probably underestimated because some minor events are not counted (Casson

Moreno, 2019) In view of the increasing trend of climatic disasters, the occurrence of Natech accidents will probably increase accordingly (Mahan, 2018).
This global trend does not spare French industrial sites since, as BARPI points out in its inventory of technological accidents in 2018, 107 of them were impacted by natural phenomena (rain-flooding, lightning, strong heat and intense cold), which represents almost 9% of the events recorded in the ARIA database, on the same perimeter and in the same year. In this same report, BARPI also indicates that since 2010, the number of meteorological events impacting industrial sites in France has been constantly evolving, underlining to a certain extent the increase and intensity of these phenomena.
The prevention and control of industrial risks is based on a risk analysis that must take into account both the risks intrinsic to industrial installations and the potential aggressors linked to the local context of the site, whether man-made or natural. Unlike the risks inherent in the production tool, which since 2003 have had to be quantified in terms of probability, the French regulations currently in force authorise special treatment for certain natural events and thus allow:

- to exclude certain external and extreme initiating events (e.g. flooding greater than the reference flood according to the rules in force, climatic events of greater intensity than historically known or foreseeable events that could affect the installation, according to the rules in force, etc.)
- not to consider certain natural events in the probabilistic quantification of major accidents if the associated regulatory elements or good practices are respected (e.g. the case of flooding if the industrialist provides justification for the sizing of these installations for their protection against the reference flood (as defined, for example, to date in the guide to flood risk prevention plans (PPRi) of the Ministry of Sustainable Development))

The intensification of certain natural events, in terms of frequency and amplitude, raises the question of whether such a position should be maintained in future RA. Indeed, do the reference levels used in the existing Natural Risk Prevention Plans (PPRN) take into account the increase in these phenomena? If, since 2011, the Natural Coastal Risk Prevention Plans (PPRL) have had to include a level surge in the definition of the reference level to take into account the increase in sea level linked to climate change, is this also the case for the other flood management plans at the territorial level? Are we able to predict the intensification of climatic events sufficiently to define a reference level in the case of phenomena that are, in essence, extreme? Are the accidental sequences identified for foreseeable floods still relevant in this type of situation? It is on the basis of the previous work carried out and driven by these questions that Ineris is continuing its work to take better account of Natech in the analysis of the risks of industrial systems.

2.4 RA and Environmental consequences

In the current context of climate change beyond the natech concern developed in section 3.3, loss of biodiversity and the collapse of living populations. A reflection is in progress concerning safety cases, to evaluate the severity of a potential industrial accident on the Environment. The Seveso III Directive aims to "prevent major accidents which could have possible consequences on industrial activities and to limit the consequences for human health and the environment". However, French regulations mainly focuses on the number of humans affected (see the definition of the effect thresholds in the decree of September 29, 2005). To our knowledge, there is no national rule for estimating environmental severity.
Ineris aims to develop a method that allows any voluntary industrialist to estimate the environmental consequences that a potential accident could have on their site. The method follows the different stages of the hazard study so that it can be easily integrated into it. However, it must be self-supporting so that an operator of a site not subject to safety case can also use it. The method’s guideline is quite simple: hazardous substances present on the site could, due to an accident (pipe leak, fire, retention bowl overflow, explosion, etc.) be transferred outside the site and impact receptors. However, from these first three stages, technical difficulties emerge. Hazardous substances properties are defined through their flammable, explosive, toxic, infectious nature, etc parameters. If these properties vary with the substance phase (aqueous, solid, gaseous), then possible phase evolution during transfer has to be taken into account. Toxical properties and threshold are deeply linked on the species used for the experiment (which are not necessarily the species impacted by the substance when the accident occurs). Besides, reactions between the substance and the crossing medium can occurs, eventually leading to formation of secondary products with own hazardous properties.
According to the accidental scenario, transfer routes can be multiple: fumes (particles in the air), cloud (substance in gaseous form), watercourses (solid substance dissolved or transported in small particles, liquid substance), elution in soils (liquid or solid substance dissolved or transported in small particles), etc. The extent then depends on an infinite number of parameters: meteorological conditions, type of soil, characteristics of rivers, substance density, etc. At this stage, we come up against the limits of current scientific knowledge (eg: the elution of pesticides is not yet systematically known).

Identifying and prioritization of sensitive issues is also complex. Defining all the receivers present within a given area is nearly impossible and selecting the species of interest for the study (eg: protected or threatened species) raises ethical questions. Not less questionable is to choose for a more macroscopic scale taking into account only protected areas, national reserves, etc. Indeed, can we only estimate the tonnages of dead animals and hectares of vegetation, as is frequently done in post-accident situations? Consideration of resources also comes with a lot of questions: What and how resources should be taken into account (eg does polluted agricultural land translate into the number of unemployed farmers or should we consider the degradation of this artificialized living space in a different way?). Another way of thinking could be considering the Environment's resilience.
Then come the issues relating to scoring and the determination of severity, or even acceptability. On this point, a benchmark of the methods developed elsewhere at the international level is in progress. In order to enrich the RA usually carried out in hazard studies by integrating the effective preservation of the environment, it emerges that technical and scientific obstacles will have to either be removed or be the subject of approximations. Likewise, the method raises ethical questions and consensus must be found. The advantages of this method are multiple: easily integrated into the RA approach with which engineers in industries are familiar, an educational communication tool, and support for continuous improvement for the preservation of biodiversity.

2.5 RA and Dominos effects

The last theme to consider is domino effects. Good knowledge of domino effects and their control is a real issue both within an industrial establishment and within industrial zones, where several installations or establishments using hazardous substances are close. Accidents involving domino effects are indeed among the most destructive and can cause serious consequences for people, buildings / infrastructures or / and natural environment in the vicinity of the installations. As proof, reference should be made to the accidents of Feyzin (1966), San Juan in Mexico (1984) and Tianjin in China (2015). Domino effect is the action of a dangerous phenomenon (thermal effect, overpressure and projection) occurring on a first equipment, impacting a second equipment and causing a second dangerous phenomenon on the latter equipment, causing an aggravation of the consequences generated by the first equipment.
For more than ten years, methodological developments have been undertaken by Ineris to integrate domino effects into the risk analysis of industrial processes. More extensive work has been carried out on the resistance of structures to accidental aggressions. Ineris has developed a method for evaluating domino effects. The process for domino effect sequences analysis consists, first of all, in identifying aggressive industrial equipment likely to cause dangerous such as fires, explosions and causing damage to other equipment located nearby, as well as industrial equipment likely to be attacked and which in turn could lead to dangerous phenomena.
The possible domino effect sequences are then determined by crossing the intensity of the effects of the dangerous phenomena that occur on the aggressive equipment and the vulnerability of the receiver equipment. To do this, standard equipment vulnerability thresholds can be used, as a first approach (for example, the domino effects thresholds of 8 kW/m^2 for thermal effects and of 200 mbar for overpressure). But it is also possible to make a more complex analysis based on charts or more precise models of the behavior of the attacked equipment according to the characteristics of the potential accidental aggressions. This step is crucial in the identification of domino effect sequences, but currently, it is based, in the majority of cases, on the standard thresholds. The numerical data for assessing more precisely this vulnerability, according to the type of equipment studied, are still little available and used.
The risk associated with each of the domino effect sequences can then be characterized by determining the severity of the consequences and the probability of occurrence of the accidents. The positioning of the different accidents in a gravity / probability crossover grid will make it possible to judge the assessment of the domino effect sequences, and to initiate, if necessary, a risk reduction process. For unacceptable sequences of domino effects at first glance, it may be necessary to have a new RA by refining the hypotheses for the assessment of vulnerability or the assessment of thermal or overpressure effects for example and / or by studying the measures put in place or to be put in place to reduce the risks (safety barriers, etc.).
In addition to the risk assessment process, identify potential domino effects can be very interesting in the context of drawing up emergency plans for industrial sites, because it is useful to establish priority in the actions to be taken during the accident. The notion of dynamics, i.e. the time for a first dangerous phenomenon on a equipment to lead to other dangerous phenomena on neighboring equipment, also takes on its full meaning here but is difficult to assess. The analysis of domino effects can be complex when the number of installations and dangerous phenomena to be analyzed is large, hence the need for tools to automate certain steps of the process.

3. Discussion

One aspect which emerges of this study is the systemic nature of these threats. Cybersecurity requires maintaining an overview of the facilities because attacks are likely to simultaneously affect all prevention and protection devices (up to emergency resources). Likewise, natechs (e.g. a flood) potentially expose an entire industrial site almost simultaneously rather than part of it (just as they can thwart emergency response). For these two themes, domino effects are also at the heart of this systemic dimension. Seeking to anticipate the interaction of several equipments and phenomena more or less concomitantly is at the heart of domino effects. If we add to this theme the question of environmental consequences, we also see that the systemic dimension of the challenge expands. Taken together, these themes show the interest of questioning the evolutions of RA and the limits thereof, in a context of change.

4. Conclusion

This article questions the evolution of RA in France. It introduces works questioning the limits of RAs, showing that they are based on choice of scenarios, causality models and calculation principles which are always questionable. These limits challenge the nature and extent of potential adjustments to current RA practice and use. Several questions can be asked following the presentation of the different themes (cybersecurity, natech, digital management, domino effects and environmental consequences). A first point to note is that the themes addressed cover several of the limitations identified by Downer (2014). The type and intensity of scenarios (1) is dealt with by domino effects and environmental consequences (sections 3.4, 3.5). The problem of probability calculation (2) and compliance (3) are covered by the digital approaches (sections 3.2). Finally, the limits from the perspective of new scenarios (4) are addressed by the themes of cybersecurity and natech (sections 3.1, 3.3).

References

Abdo, H. Kaouk, M. Flaus, J-M., Massé, F. “A new approach that consider cybersecurity within industrial risk analysis using a cyber bow-tie analysis”, Computers & security, vol. 72, pp. 175–195, 2018.

Antonacopoulou, E. P. (2007). Actionable knowledge. Dans S. Clegg, & J. R. Bailey, International Encyclopedia of Organization Studies. Sage publications.

Casson Moreno V., Ricci F., Sorichetti R., Misuri A., Cozzani V., 2019, Analysis of Past Accidents Triggered by Natural Events in the Chemical and Process Industry, Chemical Engineering Transactions, 74, 1405-1410 DOI:10.3303/CET1974235.

Downer, J. 2014. Disowning Fukushima: Managing the Credibility of Nuclear Reliability Assessment in the Wake of Disaster. Regulation & Governance 8, 287-309.

Escande, J., Proust, C., Le Coze, JC. 2016 Limitations of current risk assessment ... Journal of Loss Prevention in the Process Industries, n°43, pp.730-735.

Jasanoff, S. 1993. Bridging the two cultures of risk analysis. Risk Analysis. Vol 13, Issue 2, pages 123–129.

Kriaa, S., Pietre-Cambacedes, L., Bouissou, M., Halgand, Y. 2015. “A survey of approaches combining safety and security for industrial control systems,” Reliability engineering & system safety, vol. 139, pp. 156–178.

Le Coze, JC. 2020. Post Normal Accident. Revisiting Perrow’s classic. Boca Raton, FL, CRC Press. Taylor & Francis.

Mahan, P., Liserio, F., 2018. Managing the risk associated with severe wind and flood events in the chemical processing industries, in: Hazards 28. pp. 1–10.

Massé, F., Flaus, J.M., Abdo, H. 2018. Comment intégrer les cyberattaques dans l’évaluation globale des risques pour les installations classées? Proposition d’un cadre général d’analyse des risques,” Congès Lambda Mu 16-18 ocotobre 2018.

Rasmussen K., 1995, Natural events and accidents with hazardous materials, Journal of Hazardous Materials, 40, 43-54.