Limitations of current risk assessment methods to foresee emerging risks: Towards a new methodology?

Jean Escande, Christophe Proust, Jean-Christophe Le Coze

Limitations of current risk assessment methods to foresee emerging risks: towards a new methodology ?

Jean Escande[1], *Christophe Proust[1,2], Jean Christophe Le Coze[2]

[1] Sorbonne University, Technological University of Compiègne, TIMR lab., 60200 Compiègne, France
[2] INERIS, Parc Technologique ALATA, BP2, 60550 Verneuil-en-Halatte, France

E-mail : christophe.proust@ineris.fr

Abstract

The objective of this work-in-progress is to investigate the potentialities but also the limitations of traditional risks analysis tools especially in the context of emerging technologies and develop a method facilitating the early detection of scenarios of accidents. This is certainly a challenge particularly for new industrial fields since, in this case, very little or no lesson from past accidents is available. It is believed that such situations cannot be conveniently treated using traditional risk assessment methods (HAZOP, FMEA,...) and typical examples are given. The reason is that those methods rely heavily on past accidents and are therefore "trapped" in them so that they are largely “inductive”. In terms of foreseeing the future, the shortcomings of inductive methods are recalled. The possibility to imagine the future with very little clues is then discussed on the ground of theoretical consideration and a way to do so is proposed (abduction, serendipity). Then on the basis of the observation of how the experts work and how discoveries are made, a potential new methodology is outlined.

Keywords: Decision engineering, Hazards identification, Management and planning, Safety

Highlights :

- illustrated examples of various situations where standard risk analysis failed ;
- illustrated examples of the successful identification of a unknown risk within the context of a formatted risk analysis exercise;
- investigation of the way discoveries are made and of the potential links with the risk analysis exercise.

1. Introduction

To identify, rank and control industrial risks a significant number of tools is nowadays available which seems to satisfy the users. Among these tools, ready to use packaged methods such that FMEA, HAZOP, Bow Tie diagrams,… are largely taught in universities and may even be available in laptop softwares (Vinnem, 2014).

Being largely used, those methods and their results have also been, for long, criticized (Mannan, 2012). In particular, they might be ill adapted to emerging technologies because primarily of the lack of feedback from accidents/incidents and secondly because, as they stand (or are currently used) today (in standards, in computer programs, spreadsheet,...) they would lack flexibility to accommodate for totally new situations.

The difficulty is certainly very real since, despite an extensive use of such methods, the Challenger accident of NASA in 1986 or the Fukushima disaster in 2011 did happen. If in very well resourced industrial domains, such as the space and the nuclear industry, where a high level of expertise is available, extreme events of this kind occur, there is certainly still much more to explore about the limits of risk assessment exercises.

So what can go wrong with the risk analysis methods ?

Investigating the limitations of engineering knowledge and the practice of risk analysis is not particularly new because the question of “the unexpected occurrence” is a central issue (Weick and Sutcliffe, 2007; Le Coze, 2016). Early examples exists (Turner, 1978; Perrow, 1984) but more recent ones too (Tierney, 2010; Downer, 2011), suggesting this concern has been lasting for long. The subjective part of the risk assessment is particularly stressed out which is far away from the rational aspects of the relevant methods which are traditionally taught in universities. But risk or safety can also be understood as social constructions (Aven, 2012; Le Coze, 2012).

Note first that HAZOP or FMEA, two major risk analysis methods, were developed in the sixties to help the “safe” development of emerging technologies of that period of time ! New chemical plants, nuclear power plants, nuclear weapons, aviation, space industry… within sometimes (especially nuclear developments) a context of very limited feedback from experience…Second, despite some severe pitfalls, the related systems (nuclear plant, planes, rockets,…) have over time achieved an acceptable level of safety, suggesting that a number of potential problems were identified and cured through the use of these risk analysis methods.

So, before thinking about developing alternative risk analysis methods, it is necessary to look how the “traditional methods” were initially developed and how they are currently being used. The idea is to better understand what works in order to understand why might not especially when facing new contexts.

2. The current practice of traditional risk analysis methods

The “traditional methods” like FMEA, HAZOP, Bow Tie diagrams have been abundantly documented in the scientific and technical literature (Mannan, 2012). In some cases the historical context of the development of the method is invoked, but they mainly describe the procedural aspects. In the examples given, idealized situations are used smearing out many practical difficulties as illustrated hereafter. The bias of this “pedagogical” (communication ?) method is that a superficial know-how is transmitted together with a preformatted method. Following, resulting safety studies might be highly standardized containing only little new information.

Nevertheless, many long experienced experts know that important and fully relevant scenarios may emerge first from a deep analysis of data (including simulating work situations in order to approach closer to the real operating conditions), second from a detailed investigation of the physical phenomena associated to the process and third from keeping the eyes opened on the general context. Illustrations of some of these issues are given in the follow up, partly coming from the experience of the authors.

2.1. Gathering data: the importance of real life situations

This example is about the safe manipulation of a missile to be attached below the wing of a jet (Figure 1). In this particular context, the kind of risk is known (unwanted ignition due to a shock for instance), the relevant information was available, at least on the paper. And all looked fine : for instance the missile had to be approached on a trailer and the wheels of the latter were mechanically blocked as soon as the operator removed his hands from the trailer (when for instance manipulating other parts of the missile). During a demonstration, because of the limited space below the wing, the operator had, without any other option, to bypass the mechanical safety brake so as to be able to position correctly the trailer. The conditions for an unwanted hazardous situation were met.

Figure 1 : plane and missile example

This is not due to insufficient knowledge but to incomplete information of real life working constraints. The description of the technical lock was given on paper but another piece of information, without words or figures, but accessible only through the observation of the real task performed by the operator, was given out only by the real life simulation.

2.2. Expertise of physical (or chemical) phenomena

This aspect pertains to the interpretation of the information and is linked to the level-breath of expertise the risk analysis team incorporates.

To illustrate that point, the example of BP Texas City refinery big explosion is first given. In this accident, the overflooding of a distillation column was not detected and resulted in a massive flammable mixture leading to a large scale explosion. One of the key reasons why the team did not succeed in preventing the overfilling of the distillation column was that they did not know that the level indicator would tell that all is OK when the highest measurable level would be significantly surpassed. Note that many maintenance, integrity, management issues were associated with this disaster as root causes (Hopkins, 2012), but this example is given to show that a risk analysis team working on the distillation column would have failed in identifying this accident scenario if not aware of the functional details of the level detectors.

This is certainly not an isolated example. The following tells more about the kind of spectrum of physical knowledge which should sometimes be engaged. In this LNG harbor (Figure 2),, the LNG filling line is provide with several automatic isolation valves placed in series in particular to prevent a massive leakage. To investigate further the reliability of the device, an FMEA was performed. Immediately it came out that if the energy supply went down, all valves closed jointly because they were chosen « failed closed ». A priori, no more massive leakage : safe! would claim the process control engineer, but…the physicist would comment further that because the lines are never perfectly insulated, the LNG contained between the valves will vaporize and the internal pressure would theoretically rise by tens of atmosphere, breaking the equipments potentially leading to the undesired event, which might, in the present case, even be the worst with the largest consequences.

Figure 2 : LNG lines in a harbour

In those examples, the expertise does exist somewhere but may easily not be implemented if not made available. Turner (Turner, 1978) commented that earlier, talking about disasters which he described as information problems.

2.3. General context: humans, organizations & societies

A striking example of ignoring part of the general context in which humans and societies evolve is now given.

Planes are equipped with safety doors separating the pilot cockpit from the passenger cabin. The motivation is to avoid highjacking by terrorists. This reinforced door needs to be locked all the time and can only be opened from the cockpit side. But in the particular situation of the German Wings disaster (Figure 3), the secondary pilot suffered from mental troubles and wanted to commit a suicide. The captain went in the passenger cabin for a while, but could not come back in the cockpit. Note that it could have been the same if the copilot had lost consciousness for some other reasons. The outcome was that the worst scenario, the crash of the plane, happened.

Figure 3 : Safety door in a plane and the German Wings crash (flight n° 9525) in the south of France (Mars, 25, 2015)

Again this is not an isolated case, and discovering the worse beyond what designers think to be under control happens regularly. Major banks know that they could be in serious troubles if, because of a major event affecting their commodities, a disruption of their activity happens. It may even produce a major economical crisis. As a consequence, they perform regularly a risk ranking exercise. For instance, a fire is always possible, and this would destroy the bank's headquarters. This situation is foreseen and backup buildings are designed for this. These buildings are shared and maintained by several banks. This strategy is generalized to cover other catastrophies like, for the specific case of Paris, a major flooding from the river La Seine (figure 4). But, because of the geographical configuration, many banks would be affected by the same natural event and would need to use the same backup building. In this situation, the available space and resources in the backup building would not be sufficient (by far…) to maintain the banks' activities. The unwanted scenario would in this case happen and derives from the fact that banks are part of a wider society of organizations with other banks sharing a common mode of failure.

Figure 4 : flooding in Paris (1910)

3. Improving / modifying the traditional risks analysis methods?

At the time of writing these lines, the historical details of the foundation of HAZOP, FMEA,… are still unclear to the mind of the authors and it is not really known if the inventors of such techniques conceived them in such a way that they were to identify any scenario even the most tricky ones. In the meantime, these original methodologies were continuously extended and sometimes incorporated in computer code suite. For instance, the HAZID method (McCoy et al., 1999) is a computer application of the HAZOP methodology incorporating from the beginning a sort of PI&D description and MFM-HAZOP (Rossing et al., 2010) incorporates a knowledge/rule management system to generate the HAZOP tables. The original FMEA method, best suited to the failure of single component was extended to other entities like computer based control systems or event human procedures (Ishimatsu et al., 2010). The authors do not overlook these progresses but think they do not change significantly the landscape as far as identifying emerging risks is concerned. Mc Coy acknowledges this when saying HAZID should only be seen as a potential aid since HAZOP is fundamentally a creative process. Paltrinieri (Paltrinieri et al., 2013) recognized implicitly that, even when incorporating systematically the incident/accident databases in the HAZID process (as proposed in their code DyPASI), the improvement expected is merely to try and incorporate "weak signals" but not to extract events that never occurred.

Nevertheless, in a number of situations, it can be noted that unexpected hazardous configurations do emerge while implementing the traditional risk analysis methods : an FMEA analysis was performed about the LNG line when the dangerous situation appeared and a risk ranking exercise was in progress in the case of the banks.

So what can be said however is that these methods certainly trigger a process of "framed imagination". By relying on a series of principles including decomposition of systems into manageable parts combined with systematic exploration of the possibilities of failure according to parameters (e.g., too much pressure, too much temperature, etc in a HAZOP study), a number of scenarios can be identified which may not come out spontaneously.

But something more was required.

3.1. The "singular point", the clue ?

So, at least, the risk analysis exercise can be considered as a substrate for discovering unexpected situations but again is not enough. In the examples given above, a "singular point" during the course of the study was first met: a mismatch between the information laid in the documents and the reality in the case of the missile, the knowledge that insulated line are never perfect and that LNG vaporization will produce large overpressures in the second case, the information given that the backup building is shared and should shelter many banks in case of a major flooding,… Note that capturing such a "saddle point" requires a certain culture which in turn comes from curiosity. Second, a desire to go deeper into the analysis is needed which sometimes requires going out of the frame of the ongoing risk analysis method. For instance, in the case of the LNG line, an FMEA was in progress but the rupture scenario could not be produced by such technique. It is the curiosity, imaginative mind certainly relying on the science of phenomena to perform different kind of analogies and perhaps the quality of the interactions between experts which were behind.

So there is certainly more than applying a technique. There seems to be something added on like observing-investigating-searching-imagining-discovering. Coming to that point, it might be useful to investigate how scientific discoveries have been described and understood in the literature. This literature includes history, sociology and philosophy of science. Authors such as Turner were pioneers of the strategy consisting in finding inspirations and theoretical support outside their domain to conceptualize the limits of risk analysis exercises and the genesis of disasters (Le Coze, 2016). Relying on this background, Francois Jacob, a French Nobel price biologist (Jacob, 2000), once wrote « On peut presque mesurer l'importance d'un travail scientifique à l'intensité de la surprise qu'il provoque » (the importance of a scientific work may nearly be measured by the degree of surprise it provokes), a notion of surprise that

Turner applied to disasters. “*It becomes clear that the answer to the question ‘who is surprised when the large-scale accident does occur?’ is an important one for the present analysis*” (Turner, Pidgeon, 1997, 72).

3.2. Scientific discoveries

The principles of what called the ‘scientific method’ is associated with the historical period of “Les lumières”, and slowly emerged during the Renaissance in Europe (Toulmin, 1991, 2003). What constitutes the scientific mode of investigation drew the attention of many disciplines. It involves issues of causality, determinism, law, induction, realism,… The present authors selected only specific aspects which they judged relevant to the present debate.

Based on Kepler, Galileo’s work and on a number of practices of his time, Francis Bacon (Conner, 2005) codified the methodological principles of how laws and theories could be established. This is obvious to us now, but it was surely not at that time. His idea was to first establish facts (and not impressions/interpretations) from observations, then, infer laws from which predictions can be made. The first step is called induction (infer laws from facts) and the second one deduction which consists in “deducing” a set of consequences (or potential causes) from facts using laws. But induction was criticized by Hume then later by Russel and Chalmers (Russel, 1912; Chalmers, 1982). This philosopher used a story to make his point about induction’s limit. A turkey, a highly inductive animal, noticed repeatedly that it was fed every morning at the same time and, therefore, induced that it would remains so, not inducing that the day before Xmas, it would be killed (Figure 5) …

Figure 5 : inductive reasoning

The problem of induction is that, on purely logical ground, it is impossible to justify by repeated observations that phenomena will reproduce as they did so far. Popper (1936) made another radical proposition in order to provide a normative structure for the practice of science despite the limits of induction. His idea is that there is no observation without a background theory, but that this theory is formulated in such a way that it can be refuted by experience. More precisely, by formulating predictions with the help of laws derived from a theoretical background, scientific propositions are set in a position to be refuted. To some extent, looking for a contradicting fact is a way for the research to progress. Science progresses “negatively”, by refuting previous theories. On such grounds, Anders (Anders, 2012) considers that the inductive approach fails because it tends to ignore the differences between the various facts/observations in such a way that a general law can be obtained.

Pierce (Pierce, 1878) suggested another kind of cognitive step in the process of science called “abduction”. It is described as follows. Surprises, disturbing anomalies, annoying elements are experienced when observing and sensing something that does not evolves “as expected”. In order to make sense of that surprise, an explanatory assumption (often based on analogies) is produced (figure 6). This assumption generates the type of information (data) that is needed for its validation (Catellin, 2004). The paramount importance of this contradicting or annoying fact is remarkably illustrated by Ginzburg (Ginzburg, 1980). This author investigates the way three different professionals work : G. Morelli, a renowned expert in paintings, S. Holmes (and behind the author of the novels : A. Conan Doyle), the famous detective and S. Freud, the psychiatrist. The first one claims that, in order to distinguish the original painting from a copy, tiny details are the clues on which new assumptions can be built (the shape of a nail for instance), the second unravels puzzling investigations from small illogical details and the last one look for lapses such as a small mismatch of the language to penetrate the psyche of individuals.

Note that all of them were physicians or studied medicine. They were accustomed to look for symptoms to deduce deeper problems. Looking deeper in the history, Ginsburg analyses the way hunters do to trace the animals since millenaries. In particular, a famous oriental tale is quoted (Princes of Serendip) in which the princes were able to describe in details a camel without having ever seen it, just on the basis of the traces left by the animal and establishing the link between them. This technique is sometimes called "serendipity" (Walpole, 1764) and was illustrated by Voltaire in Zadig (Voltaire, 1748) who knew the oriental tale. Abduction and Serendipity use the same ingredients, the former insisting more on the establishment of a plausible "working assumption" and the latter on the organization of the facts in a coherent way (Catellin, 2004; Andel and al., 2013).

Figure 6 : abduction

3.3. Improving the practice ?

It seems now clear that "the surprise" matters. It can be used to refute a theory (Popper, 1936) to propose a new working assumption (Pierce, 1878), to enlarge a perspective (Ginzburg, 1980)…

The difficulty is certainly to trap, isolate, and stimulate surprises or anomalies. Note that in the practice of risk analysis described above in examples 1 and 2, a detail was trapped and combined to other data to imagine what could be an unwanted scenario. These are clearly cases of abductions and serendipity. But for this to be possible, imagination, supported by simulation of work or the presence of experts in cases 1 and 2 above, is part of how the risk analysis actually should work. Anders (Anders, 1980) acknowledges this saying " So paradoxical it may look like, imagination is what we perceive from the present. We can know the present situation only if we can imagine what can happen".

In this respect, excess of formalism when applying methods may be detrimental. The risk analysis methods tend to be formalized, sometimes standardized, and even mandatory. For instance, in France, the bow-tie diagram to work on the safety barriers and some sort of quantified risk analysis are heavily « advised » by the authorities. As a result of this, much of the effort is devoted into implementing the method, in calculating the risks (probabilities and consequences). Imagination, the qualitative and core dimension of trying to foresee what could go wrong, is very likely to be undermined by the numbers.

4. Conclusion and perspectives

When considering emerging technologies, some consider that traditional risk analysis methods are inappropriate because they have failed in a number of situations even for standard or well known engineering systems. However, it is recalled here that these same risk analysis methods were developed within the context of earlier emerging technologies (space industry, nuclear power plants and weapons,..) and have been as such very useful for the development of solutions in these areas.

It is the opinion of the present authors that failures of those methods would pertain to the way they were implemented. This question is certainly not limited to some spectacular failures, which could be isolated cases, but seems much deeper : a recent investigation of the global outcome of the safety studies tells that the frequency of occurrence of major technological accidents is at least tenfold higher in reality than foreseen (Lannoy, 2015). A similar finding is reported by Mannan (Mannan, 2012).

The present work suggests that there might be a qualitative difficulty to identify the root causes of the accidents but also to foresee the whole extent of each scenario. In this perspective, there is certainly a need to :

- Investigate how risk analysis methods are implemented (observing engineers, experts, the dynamics of the working teams,..) to better ground our understanding of the conditions under which these methods produce really what they are expected to produce ;
- Work on the way learning from past accidents is used. An analogy with the medical approach could be favored: identifying symptoms and interpreting them. Qualitative reasoning using analogies should be used in fields where too little is known to stimulate imagination;
- Enrich our traditional risk analysis method with some additional creative method. On this point, the TRIZ method appeared to the present authors as a possibility (Alshuller, 1984; Regazzoni and Russo, 2011) although the real potential (and practicality) needs to be assessed (in the TRIZ method the user is invited to formulate his problem so as to extract the internal contradictions. The resolution of the contradiction provides innovative solutions).

5. References

Alshuller, G.S. (1984), Creativity as an Exact Science: the Theory of the Solution of Inventive Problems, Translated by Williams, *A. Gordon and Breach Science Publishers Inc*

Andel (van), P. ; Bourcier, D. (2013), *Serendipity in science, technology, art and law : lessons from unforeseen facts* (in french : « De la sérendipité dans la science, la technique, l'art et le droit : leçons de l'inattendu »), Hermann

Anders, G. (1980), *Obsolescence of manhood 2* (in german : « Die Antiquiertheit des Menschen 2. Über die Zerstörung des Lebens im Zeitalter der dritten industriellen Revolution"), C. H. Beck, Munich.

Anders, G. (2012), *The battle of cherries : dialogue with Hannah Arendt* (in german : "Die Kirschenschlacht. Dialoge mit Hannah Arendt"), C. H. Beck, Munich

Aven, T. 2012. On the critique of Beck's view on risk and risk analysis. Safety Science. 50. 1043-1048.

Catellin, S. (2004), *Abduction : a practise in science and in literature* (in french : « L'abduction : une pratique de la découverte scientifique et littéraire »), Hermès.

Catellin, S. (2014), *Serendipity : from tales to concepts* (in french « Sérendipité : du conte au concept »), Le Seuil.

Chalmers, A. (1982), *What is the thing called science ? an assessment of the nature and status of science and its methods*, University of Queensland Press, St Lucia.

Conner, C.D. (2005). *A people's history of science: miners, midwives and "low mechanics"*. Nation Books, New York.

Downer, J. (2011). 737-Cabriolet: The Limits of Knowledge and the Sociology of Inevitable Failure. *American Journal of Sociology*, vol 117., pp. 725-762

Ginzburg, C. (1980), *Signs, traces and tracks : roots of a paradigm of the clue* (in french : « Signes, traces, pistes. Racines d'un paradigme de l'indice »), *Le Débat*, n° 6, nov.

Hopkins, A. (2012). *Disastrous Decisions: The Human and Organisational Causes of the Gulf of Mexico Blowout.* Sydney, NSW: CCH.

Ishimatsu, T., Leveson, N., Thomas, J., Katashira, M., Miyamoto, Y., Nakao, H. (2010). Modeling and Hazard Analysis Using Stpa, *Proceedings of the 4th IAASS conference*, may 2010, Hunstville, Alabama, USA

Jacob, F. (2000), *The mouse, the man and the fly* (in french : « La souris, l'homme et la mouche »), Odile Jacob

Kuhn, T. (1970), *The structure of scientific revolutions*, The University of Chicago Press, Chicago.

Lannoy, A. (2015), *Limits, shortcomings and benefits from present probabilitic approaches* (in french : « Limites, insuffisances et apports des approches probabilistes actuelles : quelles leçons tirer ? »), IMdR Les entretiens du risques 2015

Le Coze, JC. (2016), Managing the unexpected. In *Handbook of Safety Principles*. Forthcoming.

Le Coze, JC. (2012). Towards a constructivist program is safety. Safety Science. 50. 1873-1887.

La Porte, T. (1981). Design and Management of Nearly Error Free Safety, in Sills, D. (ed.) *Social Science Aspects of the Accident at The Three Mile Island.* Colorado: Westview press.

McCoy, S.A., Wakeman, S.J., Larkin, F.D., Jefferson, M.L., Chung, P.W.H., Rushton, A.G., Lees, F.P., Heino, P.M. (1999). HAZID, a computer air for hazard identification. *Trans IChemE*. vol. 77, part B, pp 317-327.

Pierce, C.S. (1878). Deduction, Induction, and Hypothesis, *Popular Science Monthly*, n°13, pp. 470-482.

Mannan, S. (2012). *Lees' loss prevention in the process industries, vol., 4th edition*, ISBN 978-0-12-397210-1, Elsevier

Popper K., (1936). The Logic of Scientific Discovery (in german : « Logik der Forschung »)

Regazzoni, D.; Russo, D. (2011), TRIZ tools to enhance risk management, *Procedia Engineering* vol.9, pp. 40–51

Rossing, N.L., Lind, M., Jensen, N., Jorgensen, S.B. (2010). A functional HAZOP methodology. *Computer and Chemical Engineering.* vol. 34, pp 244-253.

Russel, B. (1912), *The problems of philosophy*, Oxford Univesity Press, London.

Tierney, K. (2010). *Risk analysis and their social dimensions* (in french : « L'analyse des risques et leurs dimensions sociales »), *Télescope*, vol. 16, n° 2, p. 93-114.

Toulmin, S. (2003). *The Return to Reason.* Cambridge: Harvard University Press.

Toulmin, S. (1989). *Cosmopolis. The hidden agenda of modernity*. The university of Chicago press.

Turner, B. (1978), *Man-Made Disasters. The failure of foresight*. Butterman-Heiworth.

Turner, B.; Pidgeon, N. (1997), *Man-Made Disasters. The failure of foresight. Second Edition*.

Vinnem, J.E. (2014), *Offshore Risk Assessment, vol. 2, third edition*, ISBN 978-1-4471-5212-5, Springer-Verlag

Weick, K., Sutcliffe, K. (2007). *Managing the unexpected. Resilient performance in an age of uncertainty. Second Edition*. San Francisco, CA : Jossey Bass.

Figure 1 : plane and missile example

Figure 2 : LNG lines in a harbour

Figure 3 : Safety door in a plane and the German Wings crash (flight n° 9525) in the south of France (Mars, 25, 2015)

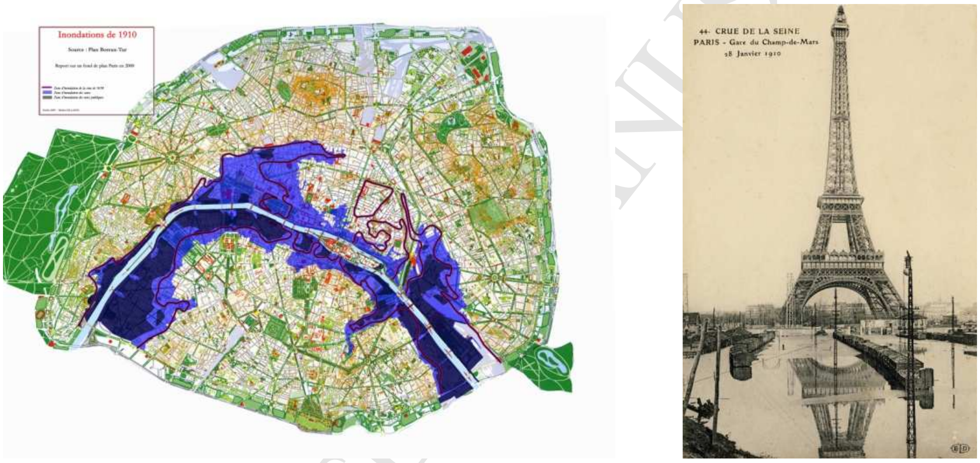

Figure 4 : flooding in Paris (1910)

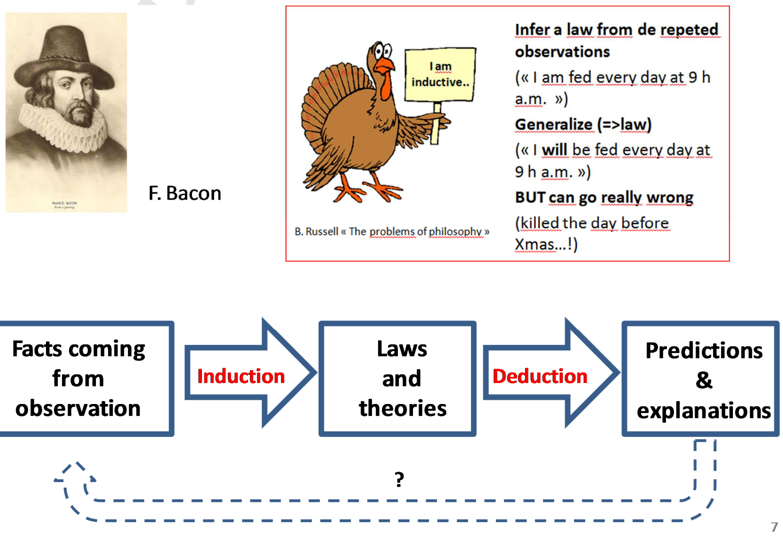

Figure 5 : inductive reasoning

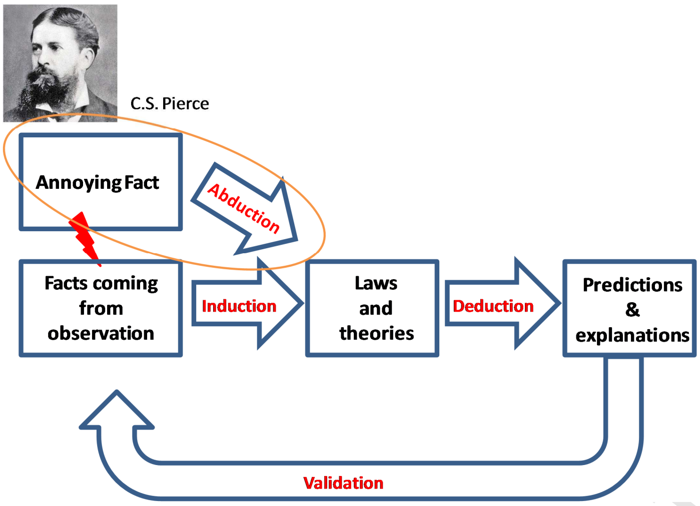

Figure 6 : abduction

Highlights :

- illustrated examples of various situations where standard risk analysis failed and explanations;
- illustrated examples of the successful identification of a unknown risk within the context of a formatted risk analysis exercise;
- investigation of the way discoveries are made and potential link with the risk analysis exercise.