Transforming a Major Hazard Management System Into a Digital Model: a Case Study Started within the European Tosca Project

Emmanuel Plot, Maria Chiara Leva, Vassishtasaï Ramany B.P., Philippe Decamps, Frederic Baudequin

Transforming a Major Hazard Management System into a Digital Model: a Case Study Started within the European Tosca Project

Emmanuel Plot[a*], Maria Chiara Leva[b], Vassishtasaï Ramany B.P. [c]., Philippe Decamps[c], Frederic Baudequin[d]

[a] Ineris, FRANCE
[b] Technological University Dublin, IRELAND
[c] Snoi, FRANCE
[d] Interactive, FRANCE
emmanuel.plot@ineris.fr

This article explores two questions that can be answered by transforming major risk management systems into digital models. 1/ A pragmatic question: How can we successfully integrate the regulatory requirements, risk assessment and safety management of a Seveso plant into a non-static picture, in order to reduce the gap between risk studies and the ever-changing reality of installations and practices? 2/ An epistemological question: How can we ensure that this non-static picture is an intelligible and acceptable model (validity, veracity sufficient to make decisions)? The pragmatic question and the epistemological one are interlinked, as two sides of the same coin. They are born from a criticism of a certain bureaucracy which leads to be satisfied with a paper documentation of the control of the risks for the "administration", that is static in nature and does not necessarily represent a true picture of the ground truth of safety. This article presents the result of a work started in the TOSCA project (Total Operations Management for Safety Critical Activities), a European Project funded within the context of the 7th Framework Programme (see Leva et al. 2019, Anzirsi et al. 2019). This project aimed at developing an innovative approach able to integrate method and IT tool for improving risk management in the field of environmental and major hazard issues. Within this project, in 2013, INERIS started a case study with the Service National des Oléoducs Interalliés (SNOI). SNOI is responsible for the French part of the NATO pipeline network in Central Europe (CEPS), known as the Common Defense Pipeline (ODC). It thus operates a network of 2,300 km of pipelines and 14 SEVESO depots, including 7 classified as high threshold, for a total capacity of 500,000 m3 distributed among more than 80 buried tanks. Since 2013, INERIS and SNOI continued to work together, every day, to develop a method and a web tool dedicated to the combined management and assessment of major risk, where the data from daily monitoring can also be integrated alongside the requirements from the regulations and the required inspections.

1. Introduction

A classic question for Seveso plants is that often time the major risk studies carried out in the format that complies with the inspection body requirements becomes a static picture that satisfy the legal checks but that may not be a model that actually contains updated risk management and risk monitoring data. An updatable risk model of the plant is a challenging achievement but it can better support the management of facilities and actual practices to ensure that acceptable level of safety is really maintained over time. The administrative compliance requires the capability of displaying the "right form" for a risk study and the emphasis is not necessarily pushed enough on the necessity to have the most up to date and realest "content". The content of course is what reflect the true management of safety and security in the field (Leva et al. 2018). In anticipation of compliance problems managers are led to focus on the documentation that will be used in case of litigation, needed to provide legal evidence for the reality of the facilities. But, would risk management be assured because risk studies would have been made and then validated by the inspection? Of course not. These papers can

often provide a false sense of security, although validated! There are countless examples of situations in which the reality of the operations doesn't always correspond to the parameters considered in these documents. And those who know the real status quo may not be encouraged to speak out, or to reported in a well-integrated way, as part of the ordinary process rather than as part of an incident report.
In a first part, we explore the pragmatic issue. We start with an analysis of the roots of the problem to conclude that the solution seems to be only possible through an IT supported process based on the risk modelling of major risk management. In this paper we aim to briefly present the developed solution to integrate the regulatory requirements, risk assessment and safety management of Seveso plants into a non-static picture, in order to reduce the gap between risk studies and the ever-changing reality of installations and practices. In the second part of the paper we explore the epistemological problem of validating the acceptability of the model (validity, veracity sufficient to make decisions). It is interesting to note that this epistemological issue emerges from the desire to use risk studies as a source for informing the daily management choices of installations and processes and to provide some criteria for their acceptability. In the third part, we discuss the work that has been done on the specific application and the future development planned.

2. The pragmatic issue

How can this tendency to separate documentary and legal compliance from real field management be explained? The root of the problem seems to be similar to the holes of the swiss cheese model James Reason often speaks about (Reason 2000) : 1/ holes in the control of the internal consistency of management documentation systems that must demonstrate the level of acceptable risk; 2/ holes in the control of the correspondence of these documents with the realities in the field, 3/ holes in the control of the true evolutions over time of dangerous phenomena criticality. There are no sufficiently systematic controls, driven by risk assessments that comply with regulatory specifications, that are themselves systematic. So, why should these official papers reflect reality? If there are not enough field checks, they may be nothing more than administrative risk assessments and documents that are quite remote from actual facilities and practices! Our first observation is that the ideal of management based on systematic risk assessments that meet regulatory requirements, in a logic such as the one proposed by ISO 31000 (2009), is not reinforced by sufficient control practices, and is therefore not implemented in most Seveso plants.
The deeper reason seems to be a matter of method and tooling issue. Let's start with the tooling issue, because it is, perhaps, the root of the problem. Industrial installations requires adequately digital support and data management for systematic and thorough controls (Anzirsi et al. 2019). A manager should be able to store and access all the information dedicated to the control of major risks in an appropriate database, info such as the description of each equipment, the related list of key parameters coming from risk assessments, its life cycle history, the planned operations and, above all, the safety functions and or safety barrier role it is supposed to cover. Often this is called a critical asset register. But this can be expanded by incorporating the impact of its potential degradation on the global risk acceptability for the area concerned, and the information to be controlled in the field. So that a clear picture is retained of what needs to be controlled, what is critical, what is not acceptable, and what has to be prioritized. the key point now is to be able to check in the field that the operating conditions correspond to these elements. Obviously, the design of this database is quite delicate, and then it still requires the right technical skills to verify those conditions in the field. But overall, the checks and the inspections should be clearer and easy to perform.
The methodological issue is more subtle, and it is correlated with the lack of integrated supporting tools. Here is one way to interpret the situation. Seveso plants have risk registers and repository of risk assessment, then asset management tools and accident and incident reporting. But those tools appear to be often disjointed and seldomly integrated (Leva et al. 2015, Leva et al. 2014). The Plant Safety Management manual may sometimes report procedure that describe an attempt to integrate the requirements with what needs to be done, step by step, considering all production, safety and environmental risk issues. This is in line with the general spirit of many standards: "write what you do, do what you write". Surely, this approach has the merit of integration: even if studies are siloed into several documents, requirements are finally integrated into procedures. But here are the issues: 1/ "engineers write, and operators do", so firstly, one can question whether what is written in the procedure is what happens as who wrote the procedure and the operators that carry out the activities may be very different people and in different roles; 2/ reality of activities is always very complex so are the blind spots really mastered?; 3/ this logic leads to interweaving many procedures and studies and recording supporting documents, so sometimes the slightest modification can take quite an effort, which encourages the evolution of facilities or practices without changing documents or systems for the administration. By the way, one can notice that many people in charge of piloting these management systems are suffering, frustrated by having to resolve documental burdens rather than field issues, and totally overwhelmed with so many studies, procedures, records that coherence is often lost in translation. It can also be a source of suffering for field teams when they do their

work without sufficient recognition, especially when they take risks to ensure the real safety and thus compensate for the inadequacies of official systems.
Let's summarize the argument. 1/ A large part of the Seveso plants invest in the realization of risk assessments just to formally meet regulatory and normative obligations; 2/ There are not enough controls to force them to guarantee the coherence, the correspondence with the reality of the installations and practices, as well as the maintenance in time of an acceptable level of risk; 3/ This problematic situation also seems to be due to a lack of computerized tools and to the prevalence of compensation practices leading to a documentary tangle that makes the situation even more inextricable.
This is why INERIS started a case study with Service National des Oléoducs Interalliés (SNOI) to develop a system at three levels:
1/ A risk assessment IT solution able to support decisions regarding risk management and provide the rationale to justify SNOI choices also if questioned by the regulator and its own management. This rationale informed the very foundation of the way the system was designed and realized. Above all SNOI wanted the risk assessment to be the foundation of a live picture shared across all levels to provide transparency on the risk faced and the impact that the unavailability or the unreliability of tasks or equipment can have on the accident scenarios the SNOI is exposed to. The computer system tends to become the support tool for the drafting of risk studies. It is capable of managing the hundreds of thousands of pages of these studies and extracting lists of measures (safety barriers) and its critical equipment or tasks linked to exclusions, estimates of hazard potentials, calculations of frequencies of initiating events, and assumptions for modeling the intensity of hazardous phenomena.
2/ An IT monitoring processes to:

- Support the improvement of the risk assessment,
- Demonstrate the congruence between the risk control means considered in the analyses and the resources efficiently managed on the sites,
- Monitor that the evolution of the criticality of the hazardous phenomena remains acceptable over time.

This is a system for reporting real-time updates of risk monitoring data from facility operating systems (maintenance, production, incident management system). The system manages records and monitoring data associated with critical equipment or tasks from which risk acceptability update calculations are periodically performed for an entire installation.
A critical asset is any equipment or key task involved in the realization of a safety measure (cf. the criteria used for the detailed barrier analysis: independence, response time, etc.) that plays a role in the risk assessment (whether it is at the level of exclusion choices, estimates of hazard potentials, calculations of frequencies of initiating events, or even at the level of assumptions for modeling the intensity of the hazardous phenomena). The system can also offer an interactive ground plan of the safety critical assets linked to the database. Once selected the item identified on the ground plan, the risk studies and safety management procedures/ document connected to the items can be displayed. In the GIS mapping other relevant items and related Isorisk curves are made accessible that can be relevant for topological risk mapping related to releases etc. The tool also offers dashboards for monitoring changes in the performance of critical items. This point is crucial as it provides a complete feedback loop between prospective risk assessments and the updated picture of actual equipment and industrial process status and how they impact the SNOI risk profile for the relevant scenarios. This link is visible and simplified in a way that it provides transparency for the outcome of unavailability of critical tasks or equipment connected with relevant safety measures. This knowledge is not available just to the risk expert or the process engineer but shared across all levels of the organizations, easy to understand also for operational personnel. In this sense it can also allow those consideration to update HAZOP and HAZID studies that would otherwise become stale picture of a status quo no longer valid.
3/ An IT rules and proofs management system capable to include:

- All the type of requests and demands received from different inspectors (including updates to risk studies), with a classification according to how clear and easy or not to do they are to realize,
- How to best address them so that recurrent similar request can be dealt in a consistent standardized way
- The lists of evidence that daily answer to requests.

The system allows organizing and storing the internal requirements connected to the external regulatory requirements the plant must comply with. For each internal requirements the plant can store evidence or proof that the requirements have been applied and is being followed on site. Some evidence is also to be found in the risk studies and how they are updated in the system considering the actual reliability data with status updated from the field. Each piece of evidence is also attached to the regulation that is there to address. The regulations have been input into the system by uploading the official PDF of the regulations and each article is translated as an item on the list of requirements. However, these requirements which can be many and varied (approx. 1300 items on the current system database) can be linked and aggregated in company guidelines/procedures

(named “doctrines” in French in the system), following which the organization can safely align themselves to the regulations. They can provide a much more synthetic set of rules/ procedures and the system still safeguards the alignment with the law requirements. For instance, in the current system 86 “doctrines” or company guidelines/rules ensure to translate the 1300 requirements coming from the original regulations. All the rules and procedures can also be classified according to specific themes such as “aging equipment”. It is also used as a management tool as the person and role responsible to maintain the “proof” associated to the alignment with a company rule and or requirements are also stored and managed in the system. All these information can then be used to organize audits. Which is a support to efficiently guaranteeing that the identified safety measures, critical equipment or tasks, are well monitored in accordance with regulatory requirements. Finally, all these information are also used to structure the continuous improvement strategy.

3. The epistemological issue

There is no point in having an integrated web-based risk management tool if it deals with erroneous models (too erroneous for an acceptable calculation of the major risk level). Here arises specifically the problem of complexity necessarily linked to the management of major risks. The real is always complex. It is only simple within the framework of abstractions that man constructs to facilitate his action. However, it is reality that must be mastered if we want to completely control the risks of major accidents (because they are unacceptable). Let us take a banal example. The control of walking is apparently simple. However, we sometimes fall, because the ground is slippery, because we did not see a stone, because we were pushed, etc. We accept these losses of control in our daily lives. We accept these losses of control to the extent that further control of walking would be more costly than beneficial. But we no longer accept them when these losses of control can put our life or health in danger, as is the case of hiking at the edge of a cliff. The control of the same action is different according to the level of success desired. To ensure total success, we must take into account the finer points of reality, everything that can prevent success. Experience shows that this "everything" is never totally predictable, if only because reality is much richer than what our understanding can grasp. Therefore, in order not to fall, prudent mountaineers make great efforts to pay attention and advance roped up (the principle of safety barriers which presupposes that despite all the precautions taken, the control of an activity is never assured and that one must foresee at least one way to avoid its failure). Faced with the complexity of reality, we must recognize the limits of our knowledge, we must know that we are provisionally true (more or less true, more or less provisional), we must accept that we can only regulate systems through cycles of trial and error. And when these errors can lead to catastrophic consequences, deemed unacceptable, we must ensure that their probability is extremely low. This approach is a source of efficiency and reliability. It is the approach of prudence (phronesis), which consists in judging the errors to be acceptable. Prudence consists in defining measures according to what we judge to be known (the reliability that we attribute to our knowledge), and in accepting the risks of an error in this judgment. There is no prudence in those who do not recognize their limitations. This epistemological statement is crucial for us. It is the logical deduction of an actor model with a capacity of autonomy, although subject to multiple cognitive biases, seen as absolutely necessary for systems to self-regulate (Plot 2007). This is the specific basis on which we think about major risk management and its digitalization.

The next logical question is: what to do when we cannot afford to regulate the models through trial and error cycles because of the consequences are catastrophic? If the tests of risk control models cannot be based on accidental feedback, incidental feedback must be multiplied to optimize our modeling process. Let's go a little further to fully express our founding hypothesis: each actor, operators, team leader, manager, in production, maintenance, logistics, engineering departments, but also each subcontractor, auditor, controller, inspector, must be able to criticize the models, at his level, from his own point of view, taking into account his objectives / issues, means / tools (interfaces), contexts, time horizons, using his ability for prudence, his autonomy of judgment. Therefore, the question is: how can risk studies be critiqued by stakeholders in the same modeling process?

It seems easier to manage this issue with an IT system. For two linked reasons. For being able to exercise its critical capacity, each actor must: 1/ be able to reconstruct the reasons for understanding the risk control choices: so, they don't just need the results of the analysis but the whole argument; the demonstration that has been made to justify a data item must be accessible; a data should not be delivered alone, but with all the information allowing these rational actors to think and make autonomous decisions; 2/ be able to understand these arguments: it is therefore necessary to provide each actor with information at the right level of abstraction: his own! This constraint forces us to look for the properties of the concepts that make sense for each actor. This means that knowledge must be diffracted into as many facets as there are levels of abstraction that meet the understanding needs of each stakeholder.

These two reasons that lead to the recomposition of information adapted to each actor is precisely what an object-oriented relational database can help to do. This technology allows multi-faceted representations of

knowledge. Thus, computer science seems necessary to deal with the epistemological questions that cannot fail to arise when one considers the demonstrations of control of major risks not as administrative documents but as models for the management of installations and practices. Be careful, this is where the research question arises: what are the static and dynamic properties of the relevant concepts for each actor? The answer is not given in advance. There is nothing simple in this matter. Let's take an example: What is a hydrocarbon reservoir? In some studies, only the maximum storage capacity is considered. In other studies, the bottom of the tank will be the most important part because the probability of leakage will be considered mainly at this level. In other studies, the interior coating of an epoxy paint will also be considered (height, thickness... there is a whole set of specifications, side parts concerned but also interior posts). And then, the description of the tanks can include, with different levels of precision: the characteristics of the concrete, the roofs of the tanks, the pipes, the filling and drawing valves, the valves interconnecting the filling and drawing pipes, the valves for draining the water from the bottom of the tank, the breathing devices by valve with calibration, the gauging devices, etc. It is the intelligence of the different experts to be able to form the relevant abstractions for their demonstrations, by including the expertise of field operators. We are very often in a case-by-case situation, with exceptions. One tank is only similar to another in an abstraction. These multiple levels complicate the programming. In the end, these are not fixed descriptions of the world, but choices of abstractions that cannot be predicted a priori and that the IT tool has to manage. It is a management of dialogues between strangers who look at the same thing and have to cooperate.

These considerations had a decisive impact on the way we worked with the SNOI. Indeed, this is why we did not choose to develop a turnkey application. We chose to design an IT platform, called MIRA (Management Integré des Risques Actualisés) that offers a flexible logic of components dedicated to risk management, that would allow us to develop as many customized application modules as necessary, to adapt to the specific needs that emerge regularly. Notice that this specificity distinguishes our approach to the digitization of risk management systems from the few tools offered on this market to industry. Notice also that this platform is flexible enough to allow a DevOps approach. We use MIRA both as a research tool, a human factors laboratory on risk management modeling, and as a secure operational tool used on industrial plants.

4. Discussion

This approach is systematic, but it is above all not a question of wanting to immediately face all the risks with it. Its implementation is modular, step by step, risk study by risk study. For instance, at the moment, the SNOI did put it in place to control the risk of small leaks (since 2014). And, now, they are in the process of extending it to other major risks (Seveso safety reports).

It should be noted that this approach helps the SNOI respond in a structured way to some of the regulator's requests that are non-standard and actually require solutions to problems that neither the regulator nor the SNOI has faced before. It is a support to have a logical approach behind the answers that need to be provided to difficult questions asked by inspectors, to obtain exemptions and avoid unnecessary investments.

Following this approach, we believe that we have laid the methodological and IT foundations for a new type of major risk management system, which could contribute to reducing the gap that is too often observed between legal compliance and the reality of management in the field, and to filling the gaps in the control systems. However, we have still several questions.

Firstly, we believe that this approach should be extended beyond risk studies as they exist today to embrace procedures as well, but procedures of a particular kind. We have criticized above the procedures that try to integrate all the tasks to be performed, and that intend to order them, step by step, considering all the issues of production, safety and environmental risks. These are useful, of course. But aren't they rather training tools, “guidelines” on how to manage activities correctly? We think that it would be preferable to have, at the intersection between these "guidelines" and the risk studies, procedures of a particular kind that would extend the detailed analysis of the barriers by explaining the critical equipment and tasks (which play a determining role in the control of risks) from the point of view of the operators in charge of them. They would only summarize the essentials of “What” has to be done, the "Who" and above all the "Why", without going into the details of how to do it, which remains a matter of individual and collective competence and orientation. They would not be conceived in relation to the activities of the actors, but only from the point of view of the security functions to be ensured. Thus, these studies would manage the entirety of the risk control choices up to:

- present to the actors what they have to do; knowing that it will be up to them to check the feasibility of the tasks given to them (and to criticize the models from their point of view),
- specify the control points to be taken into account (with all the important requirements),
- identify the links with the operational data managed by the ERP, CMMS, etc., allowing to set up the monitoring system.

Secondly, we believe that the importance of risk studies will be accentuated with the sensibilization towards sustainability in industry, consisting of asking operators to better guarantee that their productions are integrated into the environment without harming it. We believe that this should be accompanied by a better digitization of practices, all the more so as the stakes are considered to be major. This is why we start seeing our approach and our IT platform as one of the building blocks of a more global risk management at the territorial level. This is why we are working on an articulation with the Vigirisk platform, proposed by the BRGM (Bureau de Recherches Géologiques et Minières), which is dedicated to the analysis of natural risks, in order to improve the management of scenarios combining natural and technological risks. Our perspective would be, in the long run, to contribute to redefine a new holistic framework of risk management, for the management of a living space including dense urban areas, adjoining petrochemical clusters and protected biodiversity areas, in a dynamic of development of the circular economy (steam networks, raw material flows, waste treatment, research and development, subcontracting), of vegetal chemistry and industrial and territorial ecology in the global framework of the energy transition (blue economy and green economy).

5. Conclusion

We make the hypothesis that the digitization: 1/ can support the management in a pragmatic manner of the complexity of industrial knowledge regarding major risk management, 2/ can allow the criticism of the major risk management models by the stakeholders.

Based on this assumption, we have developed, thanks to a close collaboration with the SNOI, anchored in the results of the European Tosca project, an IT platform meeting the specific needs of the SNOI. And we are starting to use it to meet the needs of other industrialists, in the design, construction and operation phases, at site and territory levels. This article closes a first phase of 10 years of work that opens the way to new research on the numerical management of the static and dynamic properties of the concepts necessary for the management of major technological risks.

We are well aware that our concern to use major risk studies as a basis for day-to-day management, and thus to reduce the gap between risk studies and the ever-changing reality of facilities and practices, and thus to integrate the regulatory requirements, risk assessment and safety management into a non-static picture, is in some ways a detour from the current risk studies carried out for the administration which are static and are not really intended to be the basis of daily management. The key point is that we see digital as an opportunity to significantly improve major risk management practices.

References

Aneziris, O., Nivolianitou, Z., Konstantinidou, M., Plot, E. and Mavridis, G., 2019. Knowledge management in total safety for major hazards plants. In Total Safety and the Productivity Challenge (pp. 161-186). Routledge.

ISO 31000:2009, Risk Management—Principles and Guidelines. Geneva: International Standards Organisation, 2009

Leva, C., Angel, C.B., Plot, E. and Gattuso, M., 2013. When the Human Factor Is at the Core of the Safety Barrier. *Chemical Engineering Transactions*, *33*, pp.439-444.

Leva, Maria Chiara, Nora Balfe, Tom Kontogiannis, Emmanuel Plot, and Micaela De Michela. "Total Safety Management: what are the main area of concern in the integration of best available methods and tools." TRANSACTIONS 36 (2014).

Leva, M.C., Kontogiannis, T., Balfe, N., Plot, E. and Demichela, M., 2015. Human factors at the core of total safety management: The need to establish a common operational picture. Proceedings of the Contemporary Ergonomics and Human Factors, Daventry, UK, pp.13-16.

Leva, M.C., Kontogiannis, T., Gerbec, M. and Aneziris, O. eds., 2019. Total Safety and the Productivity Challenge. Routledge.

Plot E. 2007. Quelle organisation pour la maîtrise des risques industriels majeurs ? Mécanismes cognitifs et comportements humains, Paris (L'Harmattan).

Reason J: Human error: models and management. BMJ. 2000, 320: 768-70. 10.1136/bmj.320.7237.768.