Proceedings of the 33rd European Safety and Reliability Conference (ESREL 2023)
Edited by Mário P. Brito, Terje Aven, Piero Baraldi, Marko Čepin and Enrico Zio
 Published by Research Publishing, Singapore.
doi: 10.3850/978-981-18-8071-1_P102-cd

Computational ontologies: discussion of a research protocol in human sciences on the organization of industrial risk management

Emmanuel PLOT

Ineris, France. emmanuel.plot@ineris.fr

Maria Chiara LEVA

Technological Université Dublin, IRELAND. mariachiara.leva@TUDublin.ie

Micaela DEMICHELA

Politecnico di Torino, Italy. micaela.demichela@polito.it

Vassishtasaï RAMANY B.P.

SNOI, France. vassishtasai.ramany@developpement-durable.gouv.fr

Frederic BAUDEQUIN

Interactive, France. frederic.baudequin@interactive.fr

Marine BOUTILLON

Ineris, France. marine.boutillon@ineris.fr

Industrial risk management in applied setting is more and more faced with the need to provide a unified conceptual picture favourable to the elaboration of risk assessments and risk monitoring approaches, while at the same time accommodate the use of a plurality of data, knowledge, models and expertise that come from different areas, stem from different point of view (field operator vs designers), and reflects also different belief. A central difficulty would be to find bridges between the different levels of abstraction and conceptualization that experts may use, manipulating notions that are only apparently common. It is a problem of conceptualization, because it is the concepts that make it possible to organize the representations, to manipulate the data, the methods, the models and to coordinate the contributions of the different experts. Here, the use of digital technology is essential, as databases allow more easily than paper (or pdf files) to embrace diversity, heterogeneity, and dynamic interactions of knowledge. The question is how to design the right application or platform to help solve this problem, and also to help deliver a common operational pictures that can be operationally deployed. What are the underpinning concepts that can deliver such a purpose. This paper presents the results of a research, started in the framework of the European project Tosca (2013), on the development of ontologies as a support for the safety management systems (cf. Seveso regulation). The thesis that we wish to present in this article is that computer language is indispensable for the design of concepts useful for risk management, as soon as these risks are "major" and their management therefore requires an important level of precision. Computer tools should be considered as a research protocol in human sciences, not only as a support to instantiate concepts that could be elaborated before their computerization. In other words, IT is essential for thinking about major risk management organizations.

Keywords: complexity, cognitive bias, risk assessment, risk management, dialogue, digitization.

1. Introduction

What is the fundamental problem addressed?

Faced with the complexity of reality of major risk installation, we must recognize the limits of our knowledge, we must know that our assumptions and decision can only be considered provisionally true. And when errors can lead to catastrophic consequences, deemed unacceptable, we must ensure that their probability is extremely low. In this perspective, the fundamental problem is in constructing in advance a minimal representation of the situation to be mastered, which provides a maximum of comprehension, anticipation and guidance capacities (a representation of effective and safe scenarios/possible solutions). (Plot et al. 2022, and Plot 2007).

If our representation of reality escapes our precision requirements, how can we be sure that all major industrial risks have been properly assessed and continuously managed?

Another way of asking the question is as follows. Given the major nature of the risk, how can we coordinate teams to try to be as precise as necessary, as systematic as possible, in the inventories, in the analyses, and in the monitoring of the controls in place?

Finally how can we provide a unified conceptual picture favourable to the elaboration of risk assessments and risk monitoring approaches, while at the same time accommodate the use of a plurality of data, knowledge, models and expertise that come from different areas, stem from different point of view (field operator vs designers), and reflects also different beliefs?

These questions meet the requirement raised by a new decree of the French regulation (post-Lubrizol legislation, in reference to the major accident that occurred in 2019 at the Lubrizol site near Rouen). In the decree n°2020-1168 of September 24, 2020 (art. 5), it is written that “the operator proves [that ...] the data and information received in the hazard study accurately reflect the situation of the establishment”.

This regulation makes up for a difficulty for the inspection of classified installations to put the non-conformities at the charge of the industrialists for an inadequacy between the studies provided to the administration and the reality of the installations and the practices on the ground.

It seems to us that this decree also shows (implicitly) the difficulties encountered by industrialists and their design offices in order not to be at fault in this matter.

How can we help industrialists, design offices and inspectors to meet the challenge of constantly adapting assessments to the reality of the industry in the field, in all the complexity of its materiality?

The solution lies in a conceptualization capable of finding bridges between the different levels of abstraction at which experts work, manipulating notions that could only be apparently common. As a matter of fact, only the deployment of a multiplicity of controls, i.e. of views, on the realities of the field, combined with the effort to make the multiplicity of these points of view coherent, can allow us to hope to approach sufficient precision with regard to the major requirements of risk control.

It is the intelligence of the experts to know how to constitute the relevant abstractions for their observations and demonstrations, and it is a challenge to successfully tune these intelligences into a common operation picture useful for risk management.

While working on this question, we realized to our surprise that we had not found a way to make a conceptualization precise and useful enough without using computer tools. The use of digital technology seems essential, as only databases can embrace with a sufficient level of accuracy for the management of major risks the diversity, heterogeneity and interactions between data, methods, models and experts.

But the biggest surprise is not at this level. We realized that computer technology is not simply a medium to manipulate data, methods, models and to manage interactions between experts. It is also an instrument to conceptualize with precision!

The thesis that we wish to present in this article is that computer language is indispensable for the design of concepts useful for risk management, as soon as these risks are "major" and their management therefore requires an important level of precision. Computer tools should not be considered only as a support to instantiate concepts that could be elaborated before their computerization. In other words, IT is essential for thinking about major risk management organizations.

The paper present the interim results and attempt achieved by a research project initiated in the framework of a European project in 2013 called Tosca (Leva 2019), that is now being continued as part of internal activities carried I out by INERIS.

2. The practical need: accuracy when managing the complexity of materiality of facts and practices.

Let's project ourselves in a computer application dedicated to risk management in order to better understand the complexity raised by the requirement of precision.

For example, let's imagine a module dedicated to risk studies enables an inventory of installations (in the regulatory sense, this refers to equipment with characteristics that enable them to be classified in the nomenclature of installations that must be authorized to operate; because of the nature or quantity of hazardous substances, etc.).

Each installation can be characterized, described, linked to the regulatory requirements or good practices of such and such a guide. The description integrates photos, plans, geolocation (and therefore a view in a GIS), documents, results of studies, records, inspections.

The regulatory characterization can be more or less detailed, presenting the inventory of substances potentially used, the maximum quantities, the hypotheses of activities, the types of processes, and their participation in the status of the site from the administrative point of view (integrating the rules of accumulation).

None of this information is "free". It is a matter of listing the aspects of the actual activities that will be considered in the risk assessment and identifying the thresholds to be respected in order to guarantee over time that these thresholds will not be exceeded and therefore that these elements that serve as a basis for demonstrating the acceptability of the risks will always be valid. For this reason, each of these pieces of information can be linked to one or more requirements for the Safety Management System, which will be translated into safety measures whose performance must be guaranteed over time.

Importantly, facilities whose characteristics are below the regulatory authorization thresholds are excluded from the requirements for further demonstration of risk control. The inventory of excluded installations is established in the computer application, as well as the reasons for these exclusions. These are translated into requirements to be maintained over time via safety measures (e.g., measures to monitor the nature of the substances stored or storable in a building, using classification categories of families of substances, or measures to monitor the quantities used) which will be integrated into the specifications of the Safety Management System.

Each installation can be broken down into systems and sub-systems. A system is an abstraction allowing to group together a set of elements which will be the subject to a chapter of the risk assessment. These systems are also characterized (e.g., by activity phase), described and documented.

Thus, the systems are broken down, by activity phase, into risk analysis tables around central feared events, themselves linked to causes and consequences, some of which are hazardous phenomena, etc.

In the detailed risk analyses, the tables are specified in accidental sequences represented in the form of cause trees, consequence trees, butterfly nodes, with a characterization of initial frequencies, probability propagations, barriers and their failure modes, etc.

The approach is no more and no less than that of the methodological risk assessment guides. This is not a coincidence. In the logic we describe, the IT solution is structured by the methods used by the experts, around the concepts proposed by these methods.

One quickly realizes the difficulty of following these methods step by step in a systematic way and as close as possible to the materiality of the processes. This is why experts proceed by simplification and abstraction. And this is why the management of major risks is so difficult. Reality is not an abstraction, and it is not fixed but constantly evolving, and this is what must be managed.

The question then arises: how can we give experts the means to resort as little as possible to simplifications likely to mask reality and deprive managers of the means to master it in a satisfactory manner?

The practical need can be formulated as follows: experts must be given the means to manipulate representations with precision, as close as possible to the materiality of facts and practices, accepting abstractions only if this does not risk masking important realities for the management of major risks.

3. Theoretical needs: be precise when conceptualizing, so use computer language

Handling representations requires conceptualization. But it's about being practical. The concepts must allow for the subsumption of data, the orchestration of methodological processing of data, and their articulation within models that support the decision and action of the various experts and operators in charge of major risk management. It is not about writing a book but rather a recipe. More than that, the concepts we need are tools to program the machines that will manipulate the data. These types of concepts machine-operated have a name: they are ontologies, in the computer sense (Bachimont, 2007).

A new question then arises: how to design these ontologies? This question immediately raises two others: Are these ontologies built on paper before being implemented in computerized form? Should we speak of an ontology dedicated to risk management, in the singular, or of several specific ontologies for each industrial operation or each family of operations?

As our research progressed, we realized that although elements of a sort of meta-ontology were emerging, we were not able to design an ontology that would be valid for all industrial operators. For the moment, our observation is as follows: each new field is a discovery of specificities that lead to the modification of concepts. This means that ontologies must always be specified. The amazing thing is that we can't know in advance what will need to be specified. We only find out when we design the ontology, when we do user testing, when we write the code.

Today, it seems to us that the only way to define useful concepts for data management, risk assessment methods and models seems to be through a process of trial and error, as close to the end users and computer language as possible (without going through a paper phase).

Why? Because the challenge is to design precise concepts. Each concept must be correctly characterized and described. To do this, the computer language brings several added values. Firstly, computer language is a tool to track down ambiguities, much better than the semantics used in everyday communication or even in communication between experts. The computer language forces precision. Secondly, interactions between concepts, and especially conditional dynamic interactions, are very difficult to express outside a robust formal logic as proposed by the computer language. Better, it is by instantiating them in numerical language that the right questions to ask to think about useful concepts become clearer. And, even more surprisingly, it is very difficult to explain this precision outside of numerical language. Thirdly, and this is also fundamental, computer help for testing. Each end-user will critique the solution and contribute to enrich it. The ability to make ontologies work in real-life situations is the only way to hope to track down errors.

Let's take an example, knowing that it is difficult to explain the approach we want to illustrate outside a computer language. Our example focuses on the concept of a central hazardous event (CE).

In the glossary of technological risks in the circular of 10/05/10 summarizing the methodological rules applicable to hazard studies, in application of the French law of 30 July 2003, the CE is defined as follows: "An event conventionally defined, in the context of a risk analysis, at the center of the accidental chain. It is generally a loss of containment for fluids and a loss of physical integrity for solids. Upstream events are conventionally called "pre-accident phase" and downstream events "post-accident phase".

In the context of our research, how has this notion been transformed?

In our computer language, the characterization of a concept is done at the following three levels: static level (classes, associations, attributes), dynamic level (workflows), user level (interfaces, permissions and web services). In this paper, we will only touch on the static level.

From a static point of view, the computer language (we use an object approach) allows to manipulate the nesting of abstraction levels, so that concepts are structured as Russian dolls where common items are managed at the same levels. Only the specific attributes and associations are managed at the class level of the considered concept. Thus, our Central Hazardous Events (CE) are managed in a class that inherits the properties of classes common to other concepts. In our computer model, the CE class is an inheritance of the "StructureItem" class, itself an inheritance of the "ProjectItem" class, which is an inheritance of "Item", which inherits from "Document". The latter allows to manage the history of the CE (label, operations performed, successive states), but also the states of the CE, which will be defined in the dynamic rules of the workflows. The Item class is used to manage the actors responsible for this CE or the participants in its management, but also the citations in the published documents where this CE appears.

The ProjectItem class allows to manage the requests and the action/response plans. And so on. This CE class also inherits several generic attributes (such as a title, a description, geographical coordinates, a start date and an end date, etc.), and has its own attributes (such as an activity phase, a frequency class, etc.). The CE class inherits generic associations (with files, plans, PIDs, etc.), and has business associations (with causes, consequences, etc.), and technical associations to facilitate queries (with hazardous phenomena, measures/barriers/MRMs, etc.). There are CE dedicated to the preliminary phases of risk analysis, CE dedicated to probability propagation calculations, and finally CE instantiated in connection with specific "monitoring-investigation" equipment. The list of structural characteristics of CE is long, more or less generic, more or less business oriented, specifiable according to the end-users' habits, practices and methods. In the end, the ontological structure allows to manage the articulations between the CEs and :

- the identification of facilities, functional units, systems/ hazard potentials to be assessed ;
- the CEs capitalized during different assessments of similar facilities, units and systems;
- the regulations specific to the CE under consideration;
- the causes likely to degrade the systems;
- the possible consequences ;
- the hazardous phenomena that will be modeled and that will make it possible to judge the criticality of the accidental sequences associated with the CE;
- the measures/barriers positioned on these accidental sequences;
- the probability propagation calculations;
- the instances of this CE during the monitoring or investigation work.

How can all these relationships be designed, in detail, conditionally, without computer language?

Basically, what does the use of computer science to design concepts capable of managing the heterogeneity of data, methods, models and experts in the management of major industrial risks change? Many things, but mainly one: it is a new method of investigation, a research protocol in human sciences.

A formatting problem (bold, italic...)? one click too many? a data truncation that seemed anecdotal? a dashboard that cannot be finalized? a number of attributes that are too tedious to fill in? a problem with the management of read and write rights? a calculation that is not perfectly accurate? a processing time that is a few seconds too long? etc. These are details? No, an abyss of perplexity at the same time as an opening onto concrete systems of action (a technical notion in the sociology of organizations), cognitive paralogisms widely analyzed in sociology (Bronner, 2007), and real organizational strategies that explain real practices (Baechler, 2022).

The protocol consists in going to the end of all these practical obstacles, in their incongruous details. The heuristics of research appear during the coding and its tests, in the face of undecidable implicits, in the implementation of real data, in the face of gaps – cf. Souriau's notion of instauration- (Bruno Latour, 2012), in the step-by-step accompaniment of users in the face of inconsistencies, and, perhaps above all, in the complete oblivion of this meticulous work, these detours, these errors, these failures, these questionings, when in the end, everything works and responds naturally to a kind of obviousness known by all in advance.

The researcher's posture is one of humility. Humility in the face of problems of data processing, methods, and models that he has not yet fully understood, that resist him and that must be re-explained for the umpteenth time. Humility in front of future users who are often in a hurry, whose attitudes are complex to understand, who live their problems in a largely unconscious mode, who do not have the capacity to make them explicit in a functional specification (they do not know what they would need in the short, medium and long term), who formulate requests that often do not conform to their needs (but only become aware of this at the time of testing), who forget what they have asked for, who constantly reformulate and who may contradict themselves without realizing it ...and end up not using the computer screens that they have validated as being in conformity with their requests.

4. Conclusion

Is it all that original? Not really for computer scientists. Isn't that what the object-oriented approach is all about? What's original (in our opinion) is that we're not computer scientists, so we're fully immersed in our business concepts, and it's not a question of translating them to implement them, but of using computer language to think about them in a human sciences approach. This is what changes everything.

Some may wonder how you can use computer language without being a computer scientist. We use an almost bespoke computer platform (called InOV, designed by the company Interactive), which provides access to computer language for conceptualization without writing complex code.

This article does not deal with completed research, but with the beginnings of human science research into safety management systems (cf. Seveso regulations), the scope and limits of which are not yet fully appreciated.

5. References

Bachimont, B. (2007). Ingénierie des connaissances et des contenus : le numérique entre ontologies et documents. Paris, Hermès.

Baechler, J. (2022). L'intime. Paris. Hermann.

Barberousse, A (2019). L'attachement obstiné aux croyances fausses. In Des têtes bien faites. Paris.

Bronner, G. (2007). L'Empire de l'erreur. Éléments de sociologie cognitive. Paris, PUF

Di Nardo, M. (2016). Safety Management System: a system dynamics approach to manage risks in a process plant. International review on modelling and simulations.

Flamino, S. et al. (2013). Social Simulation in the Social Sciences: A Brief Overview. Social Science Computer Review.

Latour, B. (2012). Enquête sur les modes d'existence : Une anthropologie des modernes. Paris, La découverte.

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., Leva M.C., Moulin L., Ramany V.,Decamps P., Boudequin F., (2022). The Development of a holistic IT platform for major risk assessment and management: the MIRA tool. Proceedings of the 32nd European Safety and Reliability Conference (ESREL 2022) Edited by Maria Chiara Leva, Edoardo Patelli, Luca Podofillini, and Simon Wilson ©2022 ESREL2022 Organizers. Published by Research Publishing, Singapore. doi: 10.3850/978-981-18-5183-4_R25-04-124-cd

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

Vogrin, M. (2022). Confirmation Bias as a Mechanism to Focus Attention Enhances Signal Detection. Journal of Artificial Societies and Social Simulation 26.