The role of mathematics in the enhancement of safety

"Again I tell you, it is easier for a camel to go through the eye of a needle than for someone who is an expert in nuclear safey to enter the kingdom of Probabilities".
(Matthew, 19:24)

Beauzamy Bernard
Chairman and CEO, Société de Calcul Mathématique SA
111 Faubourg Saint Honoré,
75008 Paris, France

To be presented at the 53rd European Safety, Reliability & Data Association Seminar, November 2017

Abstract

There is a strong tendency, nowadays, oriented by the word "innovation", which considers that everything which deals with the past has no value at all, at best, and negative value, in many cases. We strongly disagree with such an approach, and we consider that any scientific approach to foresight should be based upon a careful examination of existing data, and not on a "crystal ball".

In fact, starting in the years '70, many sectors, including the nuclear industry, decided that, for instance, the failure rate of components was given by some specific probability law (exponential, Gauss, Gumbel, and so on). Such choices were legitimate at that time, because very few experimental data existed, but they should now be reviewed in the light of the numerous observations which were made since then. Our experience is that, in general, the observations contradict the initial choices. We intend to present the basis of a scientific approach for the challenge of foresight, including the so called "Early Warning Signals".

Keywords: Probabilities, failure rate, guaranty

1. Mathematics and the laws of Nature

People commonly think that the Industry masters completely the life duration of their products; a common belief is "programmed obsolescence", which means that, if a product has a guaranty of two years, it will inevitably collapse after two years and one day, and reduce to a small amount of useless ashes. This is of course just one among the numerous grievances people have against Industry in general, and if this Seminar may contribute to a better understanding, it will be most welcome.

In fact, in general, Industry has very little knowledge about the life cycle of their products, and they wish they had more, for obvious reasons: it conditions the replacement of parts, the guaranty, the possibility of life extension, and so on. This applies to the nuclear sector (which in France is quite ancient) and, as well, to

carmakers. We had, for instance, to work for Peugeot about the possible extensions of a guaranty (after the normal two year period, the owner may buy an extension, but what should it cover and how much should it cost ?) and early warning signals: if a sufficient number of (for instance) Peugeot 407 show a specific defect, what is the probability that a large number may be affected ? This is an important question for the carmaker, because they have to devote enough resources (in spare parts and work force) to answer the consumers' needs.

It should be quite clear for anyone with good faith and good will that these questions are probabilistic in nature: nobody can predict with certainty the instant of failure of a component, even if thousands of similar components have been observed for quite a long time. One can say (and this is quite interesting) that the more numerous the observation is, the more concentrated the probability law will be, meaning that the "confidence interval" will be smaller. The confidence interval should not be confused with the set of possible values; for instance, for a normal (gauss) law, the set of values ranges from $-\infty$ to $+\infty$, but a 95% confidence interval may be taken in $[-2,2]$.

Probabilities, at least in France, are poorly taught: they are presented in an academic setting, with axioms, which do not allow the application to the laws of Nature. Unfortunately (for mankind in general), these laws are fundamentally probabilistic; conversely, the engineers like deterministic statements, such as: above this threshold, you are ok, under it, you are in danger. Unfortunately, as we say in French "Satan conduit le bal".

Of course, at the end, a decision has to be taken, and this decision is deterministic by nature: should we continue operating a plant, should we replace some equipment ? So we have a deterministic decision, based upon probabilistic information. How is this possible ? This is indeed quite difficult, and becomes every year harder and harder, because the public in general understands nothing to "risk management"; they take shelter behind some "precautionary principle" (which, in France, has become constitutional) and refuse any consideration in which the risk appears. For instance, the "seismic hazard" is used by ecologists in order to require the shutdown of nuclear plants, but also oil factories. One cannot "prove" that in Paris we will never see an earthquake of magnitude 9, though all historical information as well as all geological studies indicate that this is very unlikely.

Seismic hazards are a good example; France has a map of all such hazards, and is divided into "zones" (see [1]). But this map is not completely correct (we had to work on that for the French "Commissariat à l'Energie Atomique") and strongly overestimates the risk, due to the improper use of probabilistic laws, the parameters of which were incorrectly calculated: we will come back on this later. In fact, when one wants to establish such a map, two difficulties must be taken into account :

- Proper reconstitution of historical events, which is always difficult. One may hope to have a proper understanding for the last 2000 years in Europe, much less in other continents ;

- Possibility of "transposing" an event, which occurred in one place, as a piece of valuable information in another place. Is this transposition acceptable ?

Even if the map is not perfect, it is better than no map at all: at least, it gives a basis for a discussion and for a decision. So, here is the approach we recommend: based upon historical facts and physical studies, a "risk map" is elaborated; then a discussion starts about the admissible threshold, and then a deterministic decision is taken. At least, we see clearly the steps, and we can proceed, avoiding endless discussions.

And this is where the role of mathematics comes in: it provides the grounds to a scientific approach, based upon facts and observations, instead of "wars of religion" we regularly see on such topics.

The first role of mathematics is to provide an understanding about the data: their abundance and their quality. This may seem absurd, but we have seen a lot of stupid decisions, based upon insufficient or erroneous data. Typically, this is how the politicians proceed: they pickup the data which go in the sense they want, check nothing, eliminate all other data, and use what they kept in order to justify a decision which was taken long before. Of course, sooner or later, Nature gets its revenge; as we already said "Satan drives the show". But, meanwhile, people suffer a lot, lose their jobs due to absurd political choices (for instance the so-called "energy transition", which has never been justified).

Since the politicians pretend they act in a scientific manner (who would dare saying the converse ?), mathematics here play also their role, putting in evidence the logical mistakes in the reasonings. This hardly stops the politicians, but it may be useful anyway, in the long run.

Since mathematics is the oldest scientific discipline (around 6,000 years old), one might think that all rules are well determined and accepted. This is not so at all, and especially in this relatively young branch, probabilities (around 350 years old). At least in France, there is a common concern among engineers, which tries to eliminate all probabilistic approaches, and replace them by deterministic rules.

In the years 70-80, the Industry started to develop a general preoccupation about life cycles, return period of events, and so on. Since at that time very few data existed, people agreed to use some specific probability laws. For instance, it was accepted that, for electrical circuits, one would use an exponential law for the failure rate, and for extreme events, such as earthquakes, one would use Gumbel's laws or Weibull's laws. This was necessary at that time, because no other approach was possible. The use of such laws is quite pleasant, because one has to "tune" only a few parameters (usually the mean and the variance), based upon the existing data.

Concretely, it was mere arrogance. It meant "Look, we understand so well the laws of Nature that we have decided that the rate of failure of this type of circuits is this formula", and all experts agreed on this formula, which became a standard, the same as a circular motion of the Sun around the Earth was the rule among all experts, before Copernic.

But then Satan came in, as He regularly does, and he said "Look, you are nice guys, I like you very much, but the data collected over the last 50 years contradict your formula". This did not trouble the experts, because they were experts and did not care

so much about observations contradicting their expertise. As Max Planck said in 1906 [2]: "A new scientific truth does not triumph by convincing its opponents and making them see the light, but rather because its opponents eventually die, and a new generation grows up that is familiar with it.". The opponents to the Theory of Quanta were convinced in one generation, because they were open-minded, high level scientists, but it takes much longer to the engineers in charge of probabilistic assessments, because they are "experts", relying upon the notoriety of their institution. A physicist, by definition, is open to the outside world and ideas, which is not the case of an expert. If we may paraphrase the Bible (Matthew, 19:24) [3], we would say: "Again I tell you, it is easier for a camel to go through the eye of a needle than for someone who is an expert in nuclear safey to enter the kingdom of Probabilities".

So the first task of mathematics is to come with an assessment about the quality and relevance of the data.

The second task is to come with a mean of analysis which relies upon assumptions (we mean here model assumptions) which are as weak as possible. This is precisely the step where all fictitious laws should be eliminated, because they represent assumptions: hidden assumptions, which are dissimulated in the model, and well hidden, because they are accepted by all experts. Here, there is considerable work to be done, in reviewing all models used in all types of safety predictions, life cycle estimates, and so on.

Let us take an example in order to illustrate our point. In 2013, we had a contract with COSEA, a group of industries, with leader "Vinci Constructions Grands Projets", in charge of the new high speed train between Paris and Bordeaux. The question was about the flooding references for two rivers, "Vienne" and "Creuse", which the train needed to cross, and the type of construction of this crossing depended upon the estimate for the flooding.

First, there was a disagreement between COSEA and the French Authorities about the level of flooding to be considered: both used Gumbel's laws, but did not tune them the same way, and did not reach the same result. We were asked to come with a method which would set the dispute.

The preliminary question was about the data. Records were made, over unequal periods, in 7 stations, but they were not coherent. Finally, we could show that 3 stations presented coherent information: one on each river and one at the confluent. Using this set of data, we developed a mathematical method, which did not rely upon any parametric law, but made only one assumption, namely: the more extreme the phenomenon is, the smaller its probability. The theory and results are presented in the book [4] and, finally, our conclusions were accepted by both parties.

We had a similar contract with Total: some pollution occurred in a harbor (Brittany, west of France) and a few samples were taken, at irregular places and in a small number. From the same set of data, one party concluded that there was pollution everywhere and the other party concluded to no pollution at all. We were asked to provide our own methods, which were non-parametric. Both parties were unhappy

with our conclusions, but they accepted them and the dispute stopped. This study is presented in the book [5].

One thing is of importance: if you accept parametric statements (such as this thing has a linear behaviour, this one follows a Gauss law, and so on), conclusions are easy to obtain. Most of the times, you just put the data in the computer and push some button, and the result appears. This is one reason why such assumptions and such practices are so popular. Conversely, a true probabilistic study usually requires a significant intellectual work, of mathematical nature; this is what we call a "demonstration", for those who still know what this word means.

A demonstration of nuclear safety usually relies upon some computational code, such as CATHARE, for thermohydraulic questions. Such codes, developed starting in the years 70, are intended to simulate the behaviour of a system; they are extremely complex and rely upon 40 parameters or more. Each run may take hours. So, a question, asked by the Safety Authorities, is about the validity of a demonstration obtained by such means.

Assume that each parameter takes 10 values and assume we have 40 parameters; then the space to be explored represents 10^{40} possibilities.

The area of Siberia roughly represents 13 million square km, that is $13\times10^{12} m^2$. You want to explore Siberia, and for this, you will launch 10 rockets; each of them sees only $1\,mm^2$, that is $10^{-6}\ m^2$. So the total area you explore by such means is $10^{-5}\ m^2$ that is a percentage of $\frac{10^{-5}}{13\times10^{12}} \approx 0.8\times10^{-18}$ of the total area: one may consider that such an exploration is very poor. It would not come to the idea of anyone with common sense to say that we can explore Siberia with ten views of $1\ mm^2$ each.

But the exploration we realize with 10 000 runs of the code represents a percentage of $\frac{10^4}{10^{40}} = 10^{-36}$, which is billions of billions…of billions worse !

The experts say: we will launch our runs at random, and use some probabilistic method, such as Wilks method, in order to justify this. But the use of any probabilistic method in such a case is incorrect, as we showed in [6]. There is here a lack of common sense: we want to detect a very specific situation, which may lead to an accident; obviously, a random blind exploration cannot do the job. As Henri Poincaré once said (see [7]): "The use of probabilities should not prevent the experts from showing common sense".

2. Malfunctions of sensors

Of course, the data collected, for instance to ensure safety, usually come from a set of sensors. Our experience in this domain is quite ancient and conclusive: the Industry, in general, does not take into account the malfunctions of these sensors. They were not anticipated; the system is not regularly checked and the errors are not corrected.

In 2007, a disaster occurred in a mine of Zasyadko, Donetsk region, East of Ukraine, and more than 100 miners were killed by a methane explosion. The enquiry showed that the network of sensors did not work correctly. Our Company was consulted by local authorities: could we improve the safety of the network ? Our answer was that each sensor must be permanently monitored, using a comparison with its neighbors. So, the network must be quite dense. And when this is done, multiply by 2 the number of sensors, and again by 2 ! This is a vital piece of equipment, and when people are 1 000 meters below the Earth surface, there is no place for mathematical optimisation.

Concerning a network of sensors, people should ask the following questions:

- What do we want to monitor (temperatures, pressures, debits, and so on) ?
- What will happen if part of the network does not work correctly ?
- How do we treat the false alarms ?

In fact, there are three types of malfunctions, which must be addressed separately:

- The network does not work at all;
- The information is not precise;
- The network sends false alarms.

In a recent work for the French IRSN, we had to study the network TELERAY, which realizes a permanent control of radioactivity in France. The results of our study were presented by Guillaume Damart in the 2017 ANIMMA Conference; see [8]. Our main conclusion is that the network has too many false alarms, so the number of sensors should not be increased. Instead, we suggested that most of these sensors should be replaced by mobile units, to be used only when a danger of radioactivity is anticipated. Together with IRSN, we have developed a general research program about malfunctions of sensors: see [9]. In a previous work [10], also with IRSN, we studied the protection-system of GEN III+ reactors, which partially relies on self-powered neutron detectors (SPNDs), in-core devices measuring the neutron flux. We estimated the robustness and reliability of those detectors for surveillance purposes, using probabilistic models. Here, contrarily to the other example, we found that the design of the system was satisfactory: even in the event of failure of several sensors, information remained sufficient in order to control the neutron flux.

Why do we observe so little consciousness, not to say interest, from the Industry, about the malfunction of sensors ? The answer is simple: those who sell these equipments always presented them as perfect. Quite dishonestly, they were "oversold" by the manufacturers. Any equipment of this type requires a regular inspection, including tuning and analysis of performance. But, when we have a contract on these issues, we regularly hear: "this is the first time we question the validity of our data".

Mathematical methods for such questions are also of probabilistic nature: permanent comparison of a sensor with its neighbors, analysis of "coherence" of data (for instance comparison of upstream and downstream, detection of leaks, and so on).

3. Early Warning Signals

This is one of the major issues of this Conference, and the topic becomes more and more significant to the Industry. The question is: can we, using some observations, detect in advance that something will go wrong? Of course, the question is fairly general and not well-posed.

We already met an example with Peugeot. The question was: we have a small number of failures of a component (for instance a gear-box) on some model (for instance Peugeot 307), do we have any reason to believe that a large number of failures will occur ? The question is simplified in the sense that the signal corresponds to the component itself, namely the gear-box.

A preliminary analysis is of probabilistic nature: using the historical data, find the variability of the failures of that component, and check if the specific data exceed considerably the natural variability. In other words, among several millions of vehicles sold, there are always a few problems with gear boxes; do we have significantly more ? This concept of variability is essential in order to understand what early warning signals may be.

In general, the Industry means this: we have a system (a plant, an engine, and so on), and we monitor permanently dozens of parameters (physical, electrical, chemical,…). Looking at these parameters, is there anyway to predict that something will go wrong ?

In order to answer such questions, a probabilistic approach needs data, as always. We would need two sets of data: one set where something did go wrong (preferably on several situations) and one set where everything worked fine (preferably on several situations). We would analyze all parameters, study their natural variability (in general, the parameters do not remain constant) and find if, in the failure case, some of these parameters showed significant variations. We have methods in order to classify the parameters, depending on their importance (see [9]), but this assumes of course that the relevant parameters were correctly monitored. So I would say that this question of Early Warning Signals comes after the question of a correct information system. Only when the relevant parameters have been identified, only when one understands their natural variability, only when we are sure that they are correctly monitored, at that time we can expect to identify the circumstances leading to a possible failure. At this point, the data collected about the systems are usually insufficient (not precise enough, not complete enough) in order to allow a prediction about errors or failures.

Acknowledgements

We wish to thank Dr. Giovanni Bruna, Scientific Director, IRSN, for his numerous comments upon the first version of this paper.

References

[1] Zonage sismique de la France :
http://www.planseisme.fr/Zonage-sismique-de-la-France.html

[2] Max Planck, Wikipedia : https://en.wikiquote.org/wiki/Max_Planck

[3] Matthew 19:24 http://biblehub.com/matthew/19-24.htm

[4] Bernard Beauzamy : Méthodes probabilistes pour la gestion des risques extrêmes. SCM SA. ISBN 978-2-9521458-9-3, ISSN 1767-1175. Relié, 208 pages. Juin 2015. http://www.scmsa.eu/archives/SCM_GRE_order.htm.

[5] Olga Zeydina - Bernard Beauzamy : Probabilistic Information Transfer, SCM SA, ISBN 978-2-9521458-6-2, ISSN 1767-1175, relié, 208 pages. April 2013.
http://scmsa.eu/archives/SCM_PIT_order.htm

[6] Bernard Beauzamy : La Méthode de Wilks : Utilisation incorrecte pour les études de sûreté.
http://www.scmsa.eu/archives/BB_Wilks_2016_01_11.pdf

[7] Henri Poincaré : Rapport établi à la demande de la Chambre Criminelle de la Cour de Cassation dans le cadre de l'affaire Dreyfus, 1904 - https://sabix.revues.org/124.

[8] Guillaume Damart : Malfunctions in radioactivity sensors' networks; presentation at the 2017 ANIMMA Conference (article by Guillaume Damart (SCM), Veronika Khalipova (SCM), Bernard Beauzamy (SCM), Giovanni Bruna (IRSN))
http://www.scmsa.eu/archives/SCM_ANIMMA_Presentation_2017_06_21.pdf

[9] SCM SA Working program : "Malfunctions in sensors' networks".
http://www.scmsa.eu/fiches/SCM_Malfunction_sensors.pdf

[10] Bernard Beauzamy, Hélène Bickert, Olga Zeydina (SCM), Giovanni Bruna (IRSN): Probabilistic Safety Assessment and Reliability Engineering: Reactor Safety and Incomplete Information.Proceedings of ICAPP 2011 Nice, France, May 2-5, 2011 Paper 11399
http://scmsa.eu/RMM/ART_2011_ICAPP_11399.pdf

[11] SCM SA : Probabilistic methods, robust methods.
http://www.scmsa.eu/fiches/SCM_robust_methods.pdf