Another look at rule-based and managed safety… Some further thoughts in response to René Amalberti

In early 2021, FonCSI's Director, René Amalberti, wrote an "Industrial Safety Opinion Piece" on the relationship between rule-based and managed safety, and expertise (2021-03). Jean Pariès, Scientific Director of ICSI-FonCSI, has already addressed the notion of expertise in his "Opinion Piece" *Is expertise dangerous?* (2021-05). In this second "Opinion Piece", he follows-up with some thoughts on the question of rule-based and managed safety. Is it just a semantic difference…?

In his "Opinion Piece", René Amalberti addresses the topic of expertise and its relationship to safety but, beyond that, he raises an underlying question: the autonomy of frontline operators to depart from the organization's rules, and the link to safety. This is an important question. If we adopt the language used by ICSI and FonCSI (which I joined a year ago), it is answered by distinguishing between 'rule-based' and 'managed' safety. I've reflected a lot on this distinction, both in terms of the vocabulary and the underlying concepts. In this second response, I would like to explore my ideas.

In my experience, *rule-based* is used in practice within the Industry to describe the activities of frontline operators that comply with instructions, while *managed* refers to other activities that are not covered by the rules — either because the rules do not apply in the situation, or because operators decide to depart from them. At the same time, rule-based safety is assumed to apply in foreseeable situations, while managed safety is found in unforeseeable conditions. René Amalberti describes this usage as *a bit of a stereotype*. He's right. But when the stereotype becomes so widespread that the original has been forgotten, it's often because the original is also problematic.

> **"There is always a need for a little 'management' to accompany the rules."**

Rule-based/managed and Irish fishermen

René Amalberti reminds us that the dichotomy rule-based/managed finds its origins in an article that drew upon work presented in a thesis on commercial fishing that he co-directed. The article introduced the idea that safety has two components. The first, termed *safety through constraints*, refers to framing risk-taking using predefined prohibitions and protections. The other, called *managed safety* or *resilience*, was defined as the ability of frontline operators to manage risk in real time, by taking initiatives based on their experience and expertise. When these ideas were transposed to the industry, *resilience* was abandoned in favor of *managed*, and *constraints* became *rule-based*. The rule-based/managed twins were born, supported by references to the historical distinction in French ergonomics between *task* and *activity*. However, as there is no such thing as purely 'execution' work, there is no such thing as purely 'rule-based' safety either. There is always a need for a little 'management' to accompany the rules — and all the more so as the situation becomes less-and-less foreseeable. In practice, rule-based/managed has become a euphemism for another pair — obedience/disobedience. René Amalberti's "Opinion Piece" therefore, and rightly in my opinion, seeks to return to the original definition.

> **"In practice, rule-based/managed has become a euphemism for another pair — obedience/disobedience."**

However, here, I would like to address two points. First, I think that, while a return to the roots is overdue, we should not return to the terms rule-based and managed. Second, I think that the meaning of the terms *safety through constraints* and *expert safety* needs to be clarified.

The appearance of success?

The original intention was excellent. The aim was to help the industry move beyond the popular, but limited vision of the time. This vision was based on a Taylorian model that equated obedience, compliance and safety, and idealized a purely rule-based approach. The industry was encouraged to acknowledge the inevitable and, it could be said, necessary, complementary dimension of managed safety, and to recognize the need to manage the balance with rule-based safety. Although this was a genuine step forward in safety culture, it also raised a thorny problem of vocabulary...

Because managed safety is, at its simplest, by definition, the management of safety. It goes far beyond any residual activities that are not (yet) covered by the rules, or operator initiatives, or their unreliable behaviors. Basically, safety is the outcome of management, i.e., trade-offs between risk and various dimensions of performance (efficiency, safety, health, comfort, etc.) at all levels of the organization — especially the highest ones. 'Managed' is, therefore, not just reserved for ground-level operators. It is often a lack of 'management' and trade-offs at the highest level of the organization that leads to the need to 'manage' in the field. By limiting the term 'managed safety' to real-time management by frontline operators, the formulation perpetuates and reinforces an a-systemic understanding that is focused on individuals and their behaviors, and on human rather than organizational factors.

> **"Because managed safety is, at its simplest, by definition, the management of safety."**

Turning to rule-based safety, the situation is no better: rules are not external, let alone contradictory to management. Rules and management are simply not on the same level. Rules are an element of management, they are one of many other tools in the management toolbox (along with others, such as economic, financial, accounting, safety, etc.). Safety management systems are, essentially, systems of rules that tell you how to manage safety properly! Creating an opposition between the two notions creates a conceptually dissonant dichotomy. It also leads to a narrow understanding of the notion of rules, which stems from their socio-cultural use as a means to exercise power. Rules are not synonymous with the idea of a constraint on freedom or a limit on autonomy. They can often drive creative solutions. One example comes from computing, where the fundamental notion of a constraint that provides freedom is seen in the TCP/IP protocol. This protocol has made it possible to connect any technology to the internet, and opened up a huge new world of communication possibilities. In the same way, we can say that establishing the rules for a game literally creates the space to play the game.
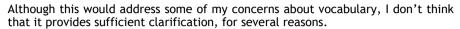
> **"Rules are not external, let alone contradictory to management."**

Both in theory and in practice, the terms rule-based and managed safety are, therefore, problematic. Clearly, the formula sounds good, and is easy to remember. Too easy. It chimes perfectly with 'the manager's experience' – the very situation we want to change. However, it hijacks the vocabulary of a global safety model and limits its use to the question of operator autonomy. In doing so, it legitimizes an understanding of safety that is focused on workers and their compliance, and propagates the idea that the real problem is a lack of discipline among operators. I therefore think that it would be useful to do what Paul Valéry called, 'cleaning up the verbal situation'. There is a need to clarify both the concepts and the vocabulary.

But what was the question?

To paraphrase a well-known joke, we are in a situation where we can say: *rule-based/managed isn't the right answer but — what was the question?* In other words, we need to look again at the original dichotomy presented in Gaël Morel's thesis, which opposed safety through constraints and managed/resilient safety.

Although this would address some of my concerns about vocabulary, I don't think that it provides sufficient clarification, for several reasons.

The expressions 'constrained safety' or 'managed safety' are also aimed at strategies focused on the operator, and my criticism of the a-systemic vision of rule-based/managed still applies. While the question of modulating the degree of operator autonomy is clearly an important component of any safety model, in a systemic perspective it cannot be used to characterize it alone.

The original use of 'resilient safety' to refer to real-time risk management based on expertise is not particularly helpful. Resilience is a property of a system, not a dimension of its performance (in this case, its safety performance). Although we can talk about the resilience of a commercial fishing boat, for example, talking about the resilience of its safety sounds strange, a bit like… the reliability of its quality.

If we are really interested in the resilience of a commercial fishing boat (i.e., its capacity to withstand the hazards in its environment), the original article highlights, remarkably, that it is the result of ongoing trade-offs, determined by the captain, between hoping to get a good catch, the market for fish, the cost of fuel and, far behind, in last place, safety. The balance between these factors in the trade-off defines the level of risk exposure. Safety is a condition, or parameter, of resilience, not the other way around. As the recent history of the Boeing 737 MAX has shown, the search for resilience can be disastrous for safety.

To a very large extent, the level of safety achieved by a system is defined by its exposure to risk, much more than its ability to manage it. To take my favorite example, NASA invented most current risk management methods, and continues to apply them more professionally than the airlines that adopted them. Yet the space shuttle program has a per-flight accident rate that is nearly 100,000 times higher than that of the best airlines! The reason is obvious: it operates at the limits of scientific and technical knowledge, with extreme levels of energy and uncertainty — in other words, levels of risk — that cannot be compared to the day-to-day experience of airline companies.

> **"The level of safety achieved by a system is defined by its exposure to risk."**

What defines exposure to risk is the company's area of operations and strategy, in short, its business model. Commercial fishing is extremely dangerous, but not because the captain is a super-expert, who believes that they are stronger than they really are, but because he or she is both a member of the crew and the leader, because he or she must make trade-offs, in real time, at sea, between his or her own safety and economic survival. The captain is both an economic strategist and an operational tactician, a manager and a frontline operator. And this is what biases his or her decision to accept a high level of risk. With regard to risk exposure and, therefore, safety, expertise is a second-order variable: it marginally modulates the perception of risk, confidence in the ability to manage it, and the ability to manage it in practice.

> **"What defines exposure to risk is the company's area of operations and strategy, in short, its business model."**

Towards an ontology of safety

A first, key criterion for categorizing safety models is, therefore, how decisions about strategic trade-offs, notably between safety and productivity are taken. Are they predetermined, or made as events unfold in real time? Are they taken by the operator, by the system designer, or the project manager? The relative weight of these two dimensions plays out differently in decisions taken by fishing crews, firefighters, people working in the process industries or cockpit personnel. Depending on the case, the notion of expertise and, therefore, autonomy with respect to instructions, does not have the same meaning.

Of course, trade-off modalities cannot, alone, fully define a safety model. We must go back to the basics: risk, uncertainty, order, disorder, foreseen,

unforeseen, etc. For example, in Gaël Morel's thesis, as in the explanation of rule-based/managed, there is the idea that anticipation, predetermination and rules apply to what can be foreseen, and that initiative and expertise apply to the unforeseeable. However, although this distinction, which is a cousin of the list Fitts developed in 1951 to describe the 'correct' division of roles between humans and machines, is intuitive, it is wrong. Initiative can be ineffective or even detrimental in unexpected, emergency situations. While it may seem paradoxical, some rules still need to be followed even when managing the unexpected. A key principle of resilience engineering in an unforeseeable situation is to create and manage margins. In all industries, safety rules require 'oversized' or precautionary margins with respect to design, operation, maintenance, etc. In aviation, there are very precise and strict rules regarding how much fuel should be carried by an aircraft. These rules are designed to cover unforeseen events, and unpredictable flight conditions. This brings us back to the notion of constraints that provide freedom. Other examples of rules that govern a strategy for managing uncertainty are the choice between etiologic or symptomatic treatment in medicine, or between operations governed by events or states in the nuclear industry.

> **"While it may seem paradoxical, some rules still need to be followed even when managing the unexpected."**

Another idea that underlies the pairings of rule-based=foreseen/managed=unforeseen is that by extending the rules, we can limit what is unforeseen, and that this is the only strategy that will allow us to attain very high levels of safety. Recent progress in robotics, artificial intelligence, self-learning systems and big data is bringing new life to the idea put forward by Pierre-Simon de Laplace and the positivists, namely that there is a digital twin of the world that will allow us to pre-determine everything. There is also — but that is a topic for another day — an illusion that Henry Mintzberg called the *fallacy of predetermination*: the belief that greater proceduralization reduces uncertainty. But it only crystallizes the known certainty. Even in mathematics, each solution to an unsolved problem gives rise to two new problems. In a complex system, there is no end to the unexpected. A one-track strategy of systematic predetermination ends with a set of Maginot lines, and only serves to make our systems less able to withstand the unexpected.

> **"There is also an illusion […]: the belief that greater proceduralization reduces uncertainty."**

Conclusion

Rule-based/managed, obedience/initiative, compliance/expertise, automation/humanization, constraint/freedom… the list of dichotomies is long, fragmented and even incoherent. Nevertheless, the fact that it exists reflects an idea that I believe to be correct: safety management is bipolar. One pole is proactive. It is based on stability, invariants, greater order, the development of algorithmic models of the world derived from past experience, and their projection into the future to be able to anticipate what will happen next and predetermine safe responses. The other is reactive, dynamic, based on agility, adaptability, managing disorder, the construction of the meaning of what is happening, the management of margins, and resilience. As we have seen, the first cannot be reduced to the application of rules, nor the second to management. So, what should we call them ?

> **"Safety management is bipolar.
> One pole is proactive […]
> The other is reactive."**

James Reason said that the best metaphor for safety is immunity. Immunologists talk about, respectively, 'innate' and 'adaptive' immunity to designate two complementary mechanisms: the genetic memory of past infections that have been successfully defeated, and the recognition of new intruders. I like the notion of 'adaptive' safety, but 'innate' safety doesn't really make sense. Personally, I have used 'normative' a lot in the past, but I admit that it is as reductive as 'rule-based'. For lack of a better idea (your thoughts are welcome), I would simply suggest 'proactive', which makes it clear that it is founded on predetermination.

●●●

Now, I'll take a deep breath — like the one you take before diving off a cliff — and suggest that we replace the pairing rule-based/managed safety with the terms proactive/adaptive safety.

I can already hear the angry crowd clamoring for my resignation…

> **"I suggest that we replace the pairing rule-based/managed safety with the terms proactive/adaptive safety."**

FOR MORE INFORMATION:

- Morel G., Amalberti R., Chauvin C. (2008) Articulating the differences between safety and resilience: the decision-making process of professional sea-fishing skippers. *Human Factors: The Journal of the Human Factors and Ergonomics*, 50(1):1-16. doi: https://doi.org/10.1518/001872008X250683

- de Winter, J.C.F., Dodou, D. (2014) Why the Fitts list has persisted throughout the history of function allocation. *Cogn Tech Work*, 16, 1–11. doi: https://doi.org/10.1007/s10111-011-0188-1

- Mintzberg H. (1996) *The rise and fall of strategic planning*. Free Press, New York

- Dupuy J-P. (1982) *Ordres et désordres : enquête sur un nouveau paradigme*. Seuil, Paris

Jean Pariès

Jean Pariès is an Ingénieur des ponts, et des eaux et forêts (IPEF). *He worked for 15 years with the French Civil Aviation Authority (DGAC). He then joined the* Bureau d'enquêtes et d'analyses *(Accident Investigation Office) for civil aviation safety. From 2000 to 2004, he was also associate research director at the CNRS. He was Chairman of Dédale SAS for 25 years. Finally, he has been Scientific Director of the ICSI and the FonCSI since the beginning of 2020 .*
jean.paries@foncsi.icsi-eu.org

FONCSI
Fondation pour une culture
de sécurité industrielle