Organising Human and Organisational Reliability

Pierre Le Bot[a*] and Hélène Pesme[a]
[a] EDF Lab, Clamart, France

Abstract: Human Reliability (HRA) and the HRO (High Reliability Organising) approach are two major trends theorising the design, monitoring and improvement of safety in high-risk industries such as the generation of nuclear power. Human Reliability is increasingly requested in current design projects for new reactors or for the renovation of existing reactors in order to incorporate human factors and technical constraints for safety. Based on our observations on simulators and accident analyses, using the MERMOS method we illustrated how human failures in the operation of reactors assessed by Human Reliability for the Probabilistic Safety Assessments (PSA) need to be analysed at an organisational level. An absence of robustness (execution errors), a lack of anticipation (design flaw) or a failure in organisational resilience (lack of reconfiguration based on a new context) generate situations in which safety is threatened. Failure is sure to arise where an organisation is not sufficiently adapted in these situations (lack of recovery). We modelled this logic with the Model of Resilience in Situation that justifies MERMOS. In this paper, we will show how the MRS can be linked to the HRO mindset and how the resulting Human Reliability approach can contribute to High Reliability Organising at the human and organisational level.

Keywords: HRA, Resilience, HRO, Human Reliability.

1. INTRODUCTION

Using the Model of Resilience in Situation (MRS), we justified the collective aspect of our Human Reliability approach by incorporating the organisational aspect. This approach underpins our second-generation MERMOS Probabilistic Assessment of Human Reliability method.

MERMOS was built gradually from our empirical observations on full-scale simulators where we assessed the handling of incident and accident scenarios by EDF power station operators, as well as actual events such as the Three Mile Island nuclear power station accident in 1979. We built MERMOS based on the interpretation of our observations using cognitive psychology, ergonomics and systemic approach theories supported by psychology researchers, engineering researchers and ergonomics researchers. Using MERMOS, we succeeded in creating a failure model that is in keeping with our empirical findings and places human failure leading to a serious nuclear accident at the level of collective operation rather than individual error, and by deviation not from procedures but from functionally required operation.

Secondly, we consolidated this modelling with the MRS [1] based on the sociological theory of Social Regulation, which enabled us to dynamically describe the management of a high-risk situation for an ultra-reliable industrial process by alternating between stable organisational periods of monitoring the rules in place and reconfiguration periods in a situation to change rules in an effort to adapt to developments in the situation (Figure 1).

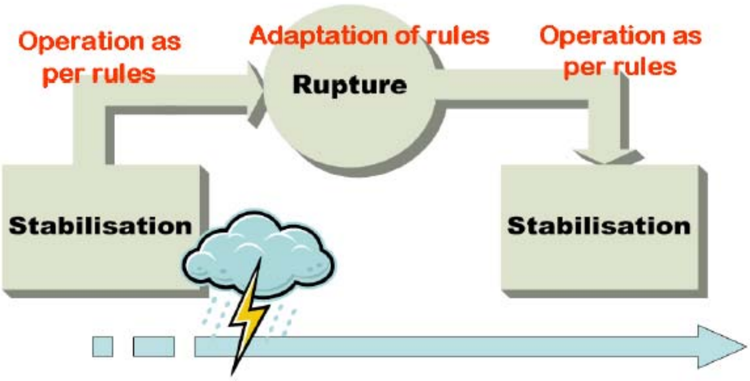
By working with the HRP (Halden Reactor Project), we were able to examine in detail the MRS processes in sub-functions to refine the functional description of an EOS (Emergency Operation System) [2].

The general principle of the MRS is to describe this management of high-risk situations based on an ongoing process described by functions that are ensured by the control system and the organisation via its management, before and after the occurrence of these situations.

[*] Contact e-mail: pierre.le-bot@edf.fr

The aim of this paper is to illustrate how the MRS encounters the HRO (High Reliability Organising) principles as described in the review by Karl Weick et al. [3], as well as the principles of Resilience Engineering explained by Erik Hollnagel et al. [4]. We would also like to suggest some developments for the MRS resulting from its use and to better comply with the HRO principles. In particular, we propose a better distinction between the organisation's different processes (anticipation, adaptation, safe operation, etc.) providing the qualities required for its overall high reliability characteristic (robustness, autonomy, vigilance, etc.), which allows people to trust it.

Figure 1: The dynamics of emergency operation in the Model of Resilience in Situation [1]



When examining these three approaches, differences in points of view seem to emerge.

- For Resilience Engineering, resilience makes it possible to move beyond the reliability approach to safety: "In contrast, resilience engineering tries to take a major step forward, not by adding one more concept to the existing vocabulary, but by proposing a completely new vocabulary, and therefore also a completely new way of thinking about safety." [4]
- Human Reliability, as we saw with the MRS, considers resilience in a situation as an ability of the organisation that is essential for making the human and organisational contribution reliable enough to ensure the system is safe.
- The HRO approach views resilience as a component of reliability: "We then move to the heart of the analysis and argue that organizing for high reliability in the more effective HROs, is characterized by a preoccupation with failure, reluctance to simplify interpretations, sensitivity to operations, commitment to resilience, and underspecified structuring." [3].

In fact, these points of view seem compatible to us by defining the approach in terms of the organisation's performance and as an ongoing looped process, which actually fits in well with the latest HRO (High Reliability Organising) development described in [3] – increasing the reliability of the organisation's performance. Thus, to sum up, the organisation's reliability is the trust we can put in it because it is safe, and it is safe because it is resilient.

We therefore need to understand Human and Organisational Reliability as described in [5]:

- A quality expected from the organisation: "In the industrial world, human reliability is the behavioural quality companies (and by extension the public and legal authorities regulating industrial operations) expect from the people with whom they entrust the running of a facility." Organisational reliability is not a useful quality first of all for the organisation itself, but for those who wish to trust in the operation of a high-risk system without managing it themselves directly.
- A requirement for robustness: "The technical approach allows us to manage a facility by anticipating operational situations. The robustness of the performance is understood as the

lack of operator error in following instructions on implementing and managing the process." Robustness is the collective ability of the operating team to manage a high-risk situation in accordance with the rules built technically by anticipating these situations. Traditionally, the initial Human Reliability approaches have been focused on this concept of robustness, i.e. the foreseeability of performance based on the consistency of behaviours and cognitive processes in collective interactions by ensuring there are no deviations in an effort to guarantee performance.

- A requirement for adaptability: "In contrast, the managerial approach (often called "security management") relies more on humans by delegating the management of situations in keeping with their skills." Robustness is a requirement for compliance with instructions without deviation as much as trust relies on the ability of individuals and groups to take initiative in a situation.
- A capacity for resilience: "The ability to combine the two [i.e. robustness and adaptation] characterises their human and organisational resilience, which comes into play in real-time in actual situations. Most of the time, the facility is run by closely following procedures. If an unexpected situation arises, the team in charge shifts into adaptation mode." Resilience is the ability to interrupt robust operation to make way for a phase of adaptation to developments in the situation in order to start again with a phase of robust operation. Resilience thus makes it possible to resolve the paradox of combining the incompatible approaches of robustness and adaptation.

2. HOW TO ORGANISE RELIABILITY

2.1. A dynamic, active ongoing looped process

As Weick states, reliability is the result of the stability of organisational and cognitive processes (of which we will try to offer a list and a description later in this paper):
"Thus, to understand how organizations organize for high reliability, we need to specify what is done repeatedly – in our case this is cognitive processes – and what varies – in our case this is routinized activity manifest in performance." [3]

We can distinguish between two types of processes:

- The processes directly linked to operation, which make operation of the system reliable (either in anticipation or in a situation), generally constitute what we call High Reliability Organising.
- The processes that feed those mentioned previously, taking account of these operation situations, whether real or simulated, generally constitute Organisational Learning.

Organisational Learning draws upon the results of High Reliability Organising, which it in turn feeds. We thus have a looped, dynamic and ongoing overall process where each individual process is both upstream and downstream from the others. Therefore, depending on the points of view, we can see one of the organisation's qualities offered by these processes, such as robustness or resilience, expertise or knowledge, as dependent on another, or conversely as determining it.

2.2. High Reliability Organising

Our proposition primarily concerns the modelling of High Reliability Organising around two main processes – **anticipation** and **adaptation**[†]. We also look at the **alert** process. In developing the MRS [1], we have now taken a less in-depth look at Organisational Learning and will therefore briefly offer a few pointers in Section 2.3.

[†] Please note that in the previous descriptions of the MRS, we used the quality of "adaptability" – we prefer to clarify the model by explaining the process of "adaptation", which offers the organisation's qualities of resilience and autonomy.

Anticipation (cf. Figure 2)

The anticipation process organises operational robustness and contributes to resilience in a situation. In general, the means for this organisation will be the following:

- From a Human Reliability point of view, functional organisation as modelled in the MRS for the operating teams in the event of an incident or accident (cf. Table 1)
- From a human factor point of view, through the organisation of the group, the roles and the skills of the operators
- From a technical point of view, through the interfaces, procedures and communication methods

Table 1: MRS Functions [2]

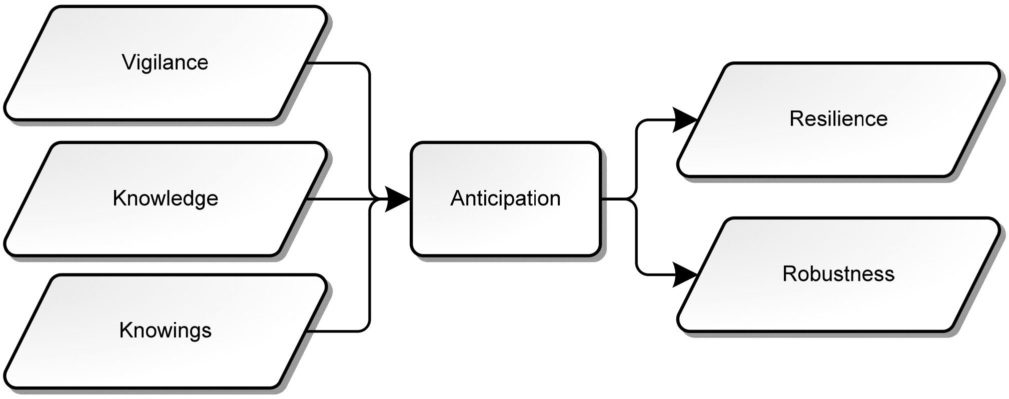
MRS Functions
Information selection and exchange
Execution
Control
Verification
Reconfiguration

Organising robustness is the most common means of technically organising reliability. For example, the distribution of the roles of the members of the team in the control room will give the supervisor the task of controlling the application of the procedure by the operators responsible for acting on the system. This control function is a barrier helping to ensure that the rules determining the operation required in a given situation are effectively and correctly applied. This barrier contributes in particular to protecting against operator errors. However, the role of the supervisor is not necessarily the only resource for the control system enabling it to recover from these deviations from the expected operation. A “forgiving” procedure will be able to recover from an operator error by asking them to check the state of a system after having carried out an operation on it. An oversight or an incorrect action can thus be recovered from by noticing that the state of the system does not match the expected state. For example, after starting a pump, the operator will be asked to check the flow rate of the line. This control function, distributed within the control system, thus helps ensure that the operation expected in the engineering offices is correctly implemented.

Engineering, based on general technical knowledge, knowledge of the organisation’s specific operation gained via the feedback process, new knowings developed through research (from outside or within the company) and vigilance resulting from the alert process needed to take action in time, is constantly revising the operation rules and the organisation. The goal is to at least maintain, if not improve, the level of prevention against the occurrence of high-risk situations via the correction of technical and organisational deviations observed, and to call upon operators to implement the planned prevention measures in a situation.

Design engineering must also anticipate that a situation may not be anticipated and, as far as possible, put organisational resources in place enabling operators to stop the operation in progress and determine in time which operation should be implemented from that point onwards. For example, when managing an incident, the safety engineer continuously monitors the reactor variables and as soon as they notice any deterioration, they will ask the operators to stop the operation in progress and change procedures or take emergency action immediately. This verification function contributes to the resilience of an organisation which anticipates that it cannot anticipate everything and that an operation worked out in advance, even if initially relevant, may become inadequate for controlling an accident.

Figure 2: Anticipation



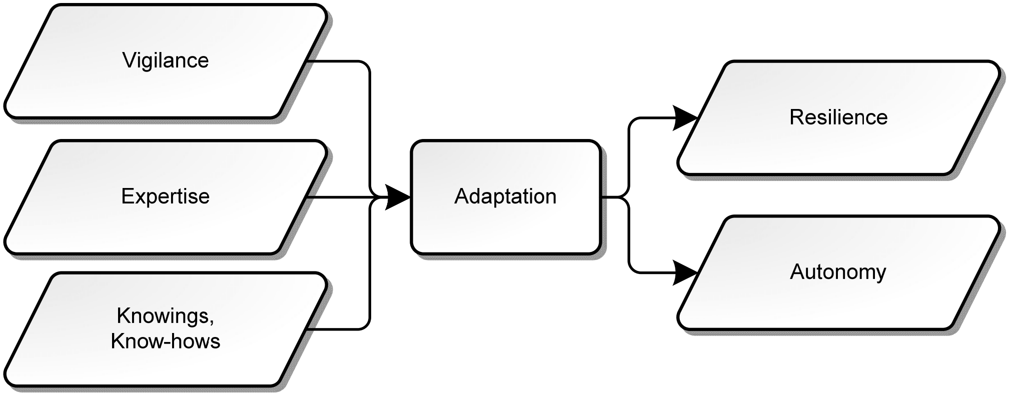
Adaptation (cf. Figure 3)

Adaptation complements the organisational anticipation of situations. Adaptation is a process implemented in a situation to reconfigure the operative system as soon as the operation in effect is diagnosed as unsuitable for the situation. The organisation thus switches from robust operation following shared collective rules [1] to adaptive operation selecting, developing and validating new rules that are adapted to the situation that has unfolded.

Adaptation based on vigilance, expertise and the individual and collective know-how of the operators in a situation functions temporally on the ongoing verification of the suitability of the operators' behaviour for the situation in progress on the one hand, and then when necessary on collaboration, cooperation and negotiation in a situation in order to result in new rules to be applied by collective expert decision through delegation in a situation.

For example, when the Three Mile Island accident occurred in 1979 (cf. [6]), the adaptation process did not work. The operators continued operation for a relatively frequent transient (a known transient increasing the pressuriser level following an emergency shutdown), postponing treatment of the inconsistency between a low reactor coolant pressure and the state of the reactor that they thought had occurred based on what they knew about this transient. They lacked the necessary expertise not only to assess the importance of this discrepancy, but also to decide on the action to be taken in this pressuriser leak situation (had they been able to diagnose it) in order to compensate for the lack of organisational anticipation of this type of transient (the proper procedure arrived shortly afterwards on-site, and thus too late).

Figure 3: Adaptation



The alert process (cf. Figure 4**)**

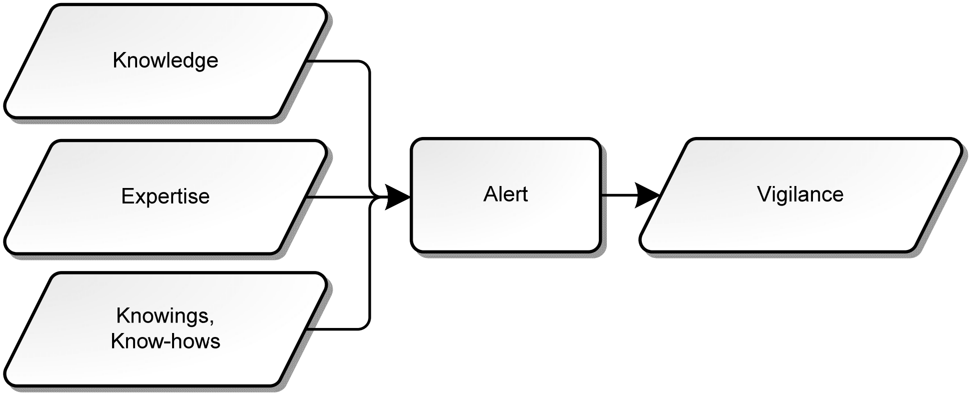
The alert process is supported by the organisation's individual and collective expert expertise. In non-real time, it makes it possible to detect, through the updating of knowledge about itself that the organisation carries out reflexively and continuously, as well as through an industrial watch showing it the behaviour of the other installations, that the way it operates is potentially incorrect in its preparedness for high-risk situations. This diagnosis may concern the following:

- a technical or organisational malfunction diagnosed but not yet corrected (via the anticipation process) even though it is an emergency
- a weak signal, i.e. an event (or a set of several events) that does not call into question operational robustness based on engineering knowledge, but rather through expert intuition with a potentially strong impact, i.e. that significantly calls into question operational robustness without being able to justify it immediately and thus requires investigation

In real time, in a situation, this alert process makes it possible to detect, by checking the suitability of the operation for the situation, that the operation retains its robustness through its suitability for the situation. In this case, it triggers the interruption of the operation in progress and a phase of adaptation to the new situation.

For example, "whistleblowers" are those who trigger the alert process. Generally, there is an organisational inability to process their alerts when they are merely compensation through individual initiative for an organisational malfunction. Indeed, an expert individual may recover, at their own initiative and using their expertise, from a malfunction in the feedback process (in non-real time) or detect a failure in the checking of the situation in progress (in real time, in a situation), and justify it in technical terms. However, whistleblowers are often expected to systematically justify their alerts with the technical rationality of a discrepancy correction request resulting from feedback, even though they may be based on expert intuition. In fact, this type of alert (provided it comes from a legitimate expert) is a weak signal that the organisation needs to process in order to judge whether or not it is a strong signal. Illustrating this with an example is tricky, since retrospective analysis of the alerts issued prior to a serious event is biased by the knowledge we have of the event that occurred. However, examining the organisational process may reveal an organisational failure, if only through the absence of this process of taking alerts into account.

Figure 4: Alert



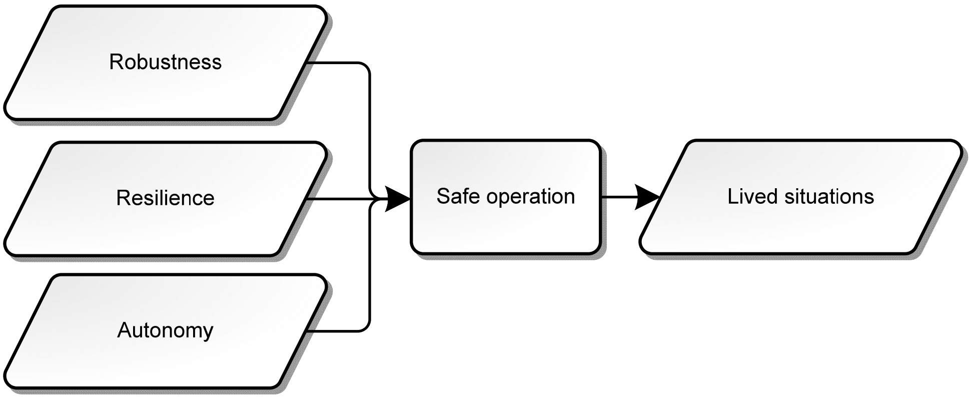
Safe operation (cf. Figure 5)

In our model, safe operation is thus achieved as far as possible through these organisational qualities of robustness, resilience and autonomy offered by the anticipation, adaptation and alert processes.

This modelling means first of all that a human or organisational failure affecting the safety of operation is potentially possible as soon as one of the processes ceases to function as expected:

- Either the functions it ensures are not in place or do not have the means to reach their objectives – this malfunction will present itself as a failure of one of the expected organisational qualities,
- Or the organisation's upstream qualities enabling these processes to function are lacking (knowledge, knowings and know-how, expertise).

Figure 5: Safe operation



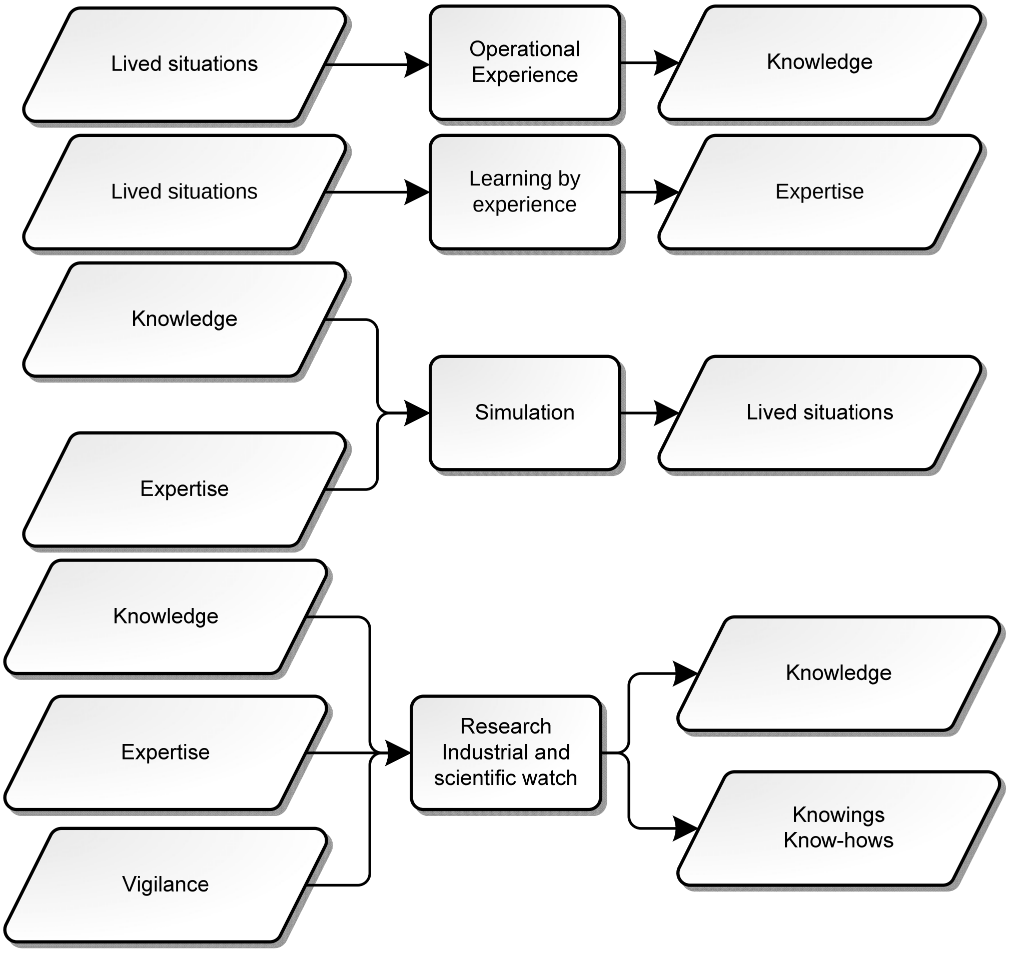
The safe operation of high-risk industries generates lived situations in the sense that it accumulates the near-miss events that it encounters (it memorises their signs, describes them and studies them namely to supply feedback) and recognises where the organisation's robustness, resilience and adaptation have been tested.

2.3. Learning Organisation

We will offer a schematic description of the Learning Organisation drawing on that which is based on deferred regulation ("deferred joint regulation" in the description of the MRS in functional terms, cf. [1]). Here, we present a schematic representation (cf. Figure 6), the aim of which is to illustrate how the organisation process loops starting from lived situations in order to organise its reliability on a continuous basis in accordance with the HRO principles.

Our proposition for modelling draws on four processes – Operational Experience (OPEX); Learning by Experience; Simulation; Scientific and Industrial Watch, and Research.

Figure 6: Learning Organisation



The lived situations are the starting point for the Learning Organisation. Based on these lived situations, the Operational Experience process will offer the organisation knowledge about itself and the Learning by Experience process will generate expertise for the direct (operators) or indirect (managers, designers, researchers) stakeholders. Learning by experience is very different to training related to anticipation, as it does not employ the same principles and is essential namely for decision-making in a situation (all operators must be considered experts), cf. [7].

Simulation makes up for the lack of high-risk situations experienced by the organisation. This necessity has long been highlighted by the HRO approach. Simulation should be considered in a general sense: “Simulation in its most common sense, for accident mode control of nuclear power stations, consists of using control centre simulators with an active operating system (control room simulators for nuclear power stations). PSA (Probabilistic Safety Assessments) can also be deemed to be simulations. These are assessments where system behaviour is evaluated to its limits by modelling. But there are other possibilities: in particular accounts that agents share from memory of an event that they have experienced (war stories, storytelling). Indeed, accounts of past events, through the storytelling effect, transport us to the context of the incident which occurred, like some sort of simulation of this event for the person listening to or reading the account.” [1].

The Industrial and Scientific Watch completes this Organisational Learning by examining the knowledge and knowings that can enhance what the organisation knows about itself by learning from others or through innovation.

Ultimately, these processes contribute to High Reliability Organising by offering knowledge, expertise and knowings/know-how.

2.4. Correspondence with Resilience Engineering and the HRO approach

From a Resilience Engineering point of view, as described by E. Hollnagel in [8], anticipation through offering robustness and adaptation contributes to the initial highlighted organisational ability of "Knowing what to *do*": "Knowing what to *do,* that is, how to respond to regular and irregular disruptions and disturbances either by implementing a prepared set of responses or by adjusting normal functioning. This is the ability to address the *actual*."

The process of adaptation through autonomy and alerting through vigilance contribute to the second ability required: "Knowing what to look for, that is, how to *monitor* that which is or can become a threat in the near term. The monitoring must cover both that which happens in the environment and that which happens in the system itself, that is, its own performance. This is the ability to address the *critical*."

Lastly, the Learning Organisation learns lessons from the past and enables anticipation of the future as required in the final two organisational abilities stated by Hollnagel: "Knowing what to *expect*, that is, how to anticipate developments, threats, and opportunities further into the future, such as potential changes, disruptions, pressures, and their consequences. This is the ability to address the *potential*. Knowing what *has happened*, that is, how to learn from experience, in particular how to learn the right lessons from the right experience—successes as well as failures. This is the ability to address the *factual*."

We saw from the modelling that the continuous loop between the High Reliability Organising and Learning Organisation processes corresponded to the dynamic of organising reliability based on the HRO approach.

A fundamental characteristic of our model is to clarify processes distinguished namely by their temporality and their dynamic (in a situation / after or before situations, in real time / in non-real time), and the rationality underpinning them (technical and engineering for anticipation, management and human factors for adaptation, without this list being exhaustive). Paradoxically, this indicates that these processes may contradict or compete with each other, namely anticipation and adaptation, bearing in mind that high-risk organisations know how to manage this contradiction through their resilience. This paradoxical building of reliability was highlighted by Karl Weick: "HROs suggest that the acceptance of paradox continues to create high effectiveness when systems become more tightly coupled and more interactively complex. As we have seen, HROs pursue simultaneous opposites such as rigidity and flexibility, confidence and wariness, compliance and discretion, anticipation and resilience, expertise and ignorance, and balance them rather than try to resolve them." [3]. We can even deduce that ambiguity is contingent on reliability, as is addressed in Stoessel's thesis [9].

This description and explanation of the processes characterising the human and organisational component of reliability offers fundamental knowledge for the design of high-risk socio-technical systems beyond the reliability assessment.

4. CONCLUSION

Our applied research approach in the field of human and organisational reliability adopts a principle alternating between empirical assessment, researching theories that explain our findings, predictive modelling justified by the theories, and back to empirical assessment supported by our models while trying to widen their scope, empirical assessment and new theoretical consolidation, etc.

After having built a human failure model supporting the MERMOS method and transcending reliability approaches focused on human error, we then extended our modelling to the functional characteristics necessary for a safe approach to managing incidents and accidents with the MRS. This was supported by Reynaud’s Theory of Social Regulation [11], allowing us to explain the functioning of the groups responsible for risk. In particular, this approach allowed us to maintain the link between the modelling of operator actions and the organisational factors that influence them, and thus to formulate recommendations for designing High Reliability Organisations. This theoretical model has already been applied and has helped design the control system for future nuclear reactors.

In this paper, we have shown how we attempted to extend this modelling of the MRS to the organisational processes of an approach to organising reliability as implemented for the safe operation of a nuclear power station. We rely on the most fundamental aspects of the HRO approach, which describes a process maintaining a constant level of performance in terms of reliability, and of Resilience Engineering, which states how the organisation must be capable of being robust and autonomous based on our interpretation. The next step will consist of dealing with the functions and their description in depth, firstly for High Reliability Organising, as we have begun with the EOS approach [2], which supplies us with a framework for describing a power station control system. Then, we will study the functional aspects of the Learning Organisation with a view to extending our recommendations to this field of the organisations.

References

[1] P. Le Bot and H. Pesme. "*The Model of Resilience in Situation (MRS) as an Idealistic Organization of At-risks Systems to be Ultrasafe*", PSAM 10, Seattle, Washington, USA, (2010).

[2] S. Massaiu, P. Ø. Braarud and P. Le Bot. "*Including Organizational and Teamwork Factors in HRA: the EOS Approach*", EHPG 2013, Storefjell Resort Hotel, Gol, Norway.

[3] K. E. Weick, K. M. Sutcliffe and D. Obstfeld. "*Organizing for high reliability: Processes of collective mindfulness*", Crisis Management, Vol. 3, 81–123, (2008).

[4] E. Hollnagel, D. D. Woods and N. Leveson, eds. "*Resilience engineering: Concepts and precepts*", Ashgate Publishing Ltd, 2007.

[5] P. Le Bot. "*The Dictionary - Human (and organizational) reliability*", Laboreal, Vol. IX, (December 2013).

[6] P. Le Bot. "*Human reliability data, human error and accident models—illustration through the Three Mile Island accident analysis*", Reliability Engineering & System Safety, Vol. 83, 153–167, (2004).

[7] G. Klein. "*Sources of power*", MIT press, 1999, Cambridge, Mass., London.

[8] E. Hollnagel. "*Resilience engineering in practice*", Ashgate, 2011, Farnham, Surrey, England, Burlington, VT.

[9] C. Stoessel. *"Décisions risquées et organisations à risques: autonomie au travail et reconnaissance sociale dans la conduite d'une industrie de process"*, Conservatoire national des arts et metiers-CNAM, 2010.

[10] P. Le Bot *et al. "Mermos: an EDF project for updating probabilistic human reliability assessment"*, REVUE GENERALE NUCLEAIRE-INTERNATIONAL EDITION-, 32–39, (1998).

[11] J.-D. Reynaud. "*Les Règles du jeu*", A. Colin, 1997, Paris.