Fukushima-Daiichi, engineering thinking in an ongoing emergency

Franck Guarnieri, Sébastien Travadel

PAPIERS DE RECHERCHE CRC WORKING PAPERS SERIES

CRC_WP_2014_22

(July 2014)

FUKUSHIMA-DAIICHI, ENGINEERING THINKING IN AN ONGOING EMERGENCY

Franck Guarnieri, Sébastien Travadel

CENTRE FOR RESEARCH ON RISKS AND CRISES
MINES ParisTech
PSL - Research University
Rue Claude Daunesse CS10207
06904 Sophia Antipolis Cedex, France
www.crc.mines-paristech.fr

CENTRE FOR RESEARCH ON RISKS AND CRISES
MINES ParisTech
PSL - Research University
Rue Claude Daunesse CS 10207
06904 SOPHIA ANTIPOLIS Cedex, France
www.crc.mines-paristech.fr

Fukushima-Daiichi, engineering thinking in an ongoing emergency

Franck GUARNIERI and Sébastien TRAVADEL

Centre for Research on Risks and Crises, MINES ParisTech, July 2014

franck.guarnieri@mines-paristech.fr

To cite this document: Guarnieri, F., Travadel S., 2014, Fukushima Daiichi, engineering thinking in an ongoing emergency. Research paper published by the Centre for Research on Risks and Crises (CRC), MINES ParisTech, July 2014.

Abstract: The lessons learned from the Fukushima-Daiichi accident have focused on prevention measures designed to protect nuclear reactors and conventional crisis management methods. Although there is still no end in sight to the accident that occurred on 11 March 2011, the way in which engineering operations to secure the facilities have been carried out offers new insight into the capacity of organizations to adapt in situations that go beyond deterministic frameworks. In this article, we examine this extreme engineering scenario, which we call “engineering thinking in emergency situations”.

Keywords: nuclear accident, engineering thinking, defence-in-depth, emergency, engineering

While the accidents at Three Mile Island and Chernobyl led to the development of new concepts in nuclear safety, studies of the accident at Fukushima Daiichi have paradoxically remained confined to improved defence-in-depth and guidelines for the management of a severe accident. However, it is important that this lack of analysis does not encourage the idea that the accident in Japan can be reduced to a series of failures or widespread destruction. Instead we argue that the event should be understood as a chain reaction which, for over three years, has created repeated crises in the context of a societal emergency. From this perspective it can be argued that in general, concurrent engineering projects that aim to contain risks and enable fuel extraction can also be viewed as initiatives taken by operators and industrialists to maintain control of their installations and ensure that safety levels meet global requirements and can respond to environmental challenges. In this paper, we develop the concept of "engineering thinking in emergency situations" to designate the specific mode of intervention in such a context.

The sequence of events that led up to the Fukushima Daiichi accident, and current activities on-site illustrate an emergency resulting from a situation that overwhelmed the classical engineering scenarios which form the basis for plant design and operation. Post-accident, the dramatic events at Fukushima Daiichi called into question the ability of actors at the plant to transition into "resilience", in a context that went far beyond deterministic safety frameworks (1). In this paper we look at potential ways forward, and propose in this context the concept of "engineering thinking in emergency situations". This concept, if properly formalized, may be an effective strategy that can be used to respond to an extreme situation (2). More generally, it sheds new light on the fundaments of nuclear safety management: consequently, as a complement to prescriptive safety methods, the capacity to transition into a dynamic of resilience may increase the robustness of an operator that is faced with an "unthinkable" situation (3).

1 THE EMERGENCY, ENGINEERING FAILURE

The initial analyses of the causes of the accident at Fukushima Daiichi highlighted shortcomings in safety standards used by the operator and oversight authorities (1.1). Similarly, the ongoing crisis that dates back to 11 March 2011 demonstrates that the multitude of engineering operations that have been implemented to contain the many threats are insufficient, not least because safety measures themselves proved to be inadequate in an emergency (1.2). Consequently, any lessons that are learnt from the accident must lead to improvements in the ability of operators to transition into a resilient dynamic (1.3).

1.1 INADEQUATE DESIGN AND OPERATING STANDARDS

We now know[1] that the earthquake caused the automatic shutdown of the reactors and the loss of all external power supplies. Emergency generators took over and supplied the emergency cooling systems of reactors 1, 2 and 3. The tsunami that followed flooded generators, rendering monitoring equipment and valve control mechanisms inoperable. Operating conditions in the control rooms and communication between these rooms and the on-site crisis centre became particularly difficult. Reactor 1's isolation condenser (IC) emergency cooling system was automatically shut down, while the reactor core isolation cooling (RCIC) systems of reactors 2 and 3 continued to operate normally; later the high-pressure coolant injection (HPCI) system of reactor 3 took over when the RCIC failed.

[1] Official Report of the Independent Commission of the Japanese Parliamentary Inquiry into the Accident at Fukushima, available from: http://www.nirs.org/fukushima/naiic_report.pdf

The sequence of failures in reactors 1, 2 and 3 were relative independent as their control in an emergency was the responsibility of the shift supervisor at each unit[2]. However, there were shortcomings in overall monitoring by the on-site crisis centre, mainly due to the transmission of incorrect or incomplete information by shift supervisors.

The failure to detect the automatic shutdown of the IC in reactor 1 (due to operators' lack of system knowledge), the failure of the RCIC in reactor 2 after three days of operation, and the intentional shutdown of the HPCI in reactor 3 (in anticipation of a possible failure) led to intermittent core cooling, without the operator having properly assessed the status of the reactors. Furthermore, the damage to facilities and lack of preparedness for such a situation delayed the implementation of alternative cooling solutions involving the injection of seawater. At the same time, the difficulty of providing a power supply to pressure relief valves and venting systems severely disrupted the ability to control container pressure, which delayed the injection of water. The three reactors were therefore left uncooled for several hours. Explosions, probably due to hydrogen generated by oxidation and cracking of fuel cladding during core meltdown damaged the structure of reactors 1 and 3. This was followed by a deflagration at the building of reactor 4, whose pipework was connected to reactor 3, which weakened the fuel storage pool in this unit. Leaks were detected in the walls of reactor 2. Altogether, this damage led to significant release of radioactive material.

The independent commission of inquiry established by the Japanese Parliament pointed out the shortcomings in the action taken by the Tokyo government, Japanese nuclear authorities and the operator (the Tokyo Electric Power Company; TEPCO) in their immediate management of the crisis, daily monitoring of safety-related events, updates to the risk analysis and design standards, and in the oversight of the operator[3].

However, it should be noted that the precise causes of the accident must be further investigated in the course of the decommissioning of the plant. The reasons for the shutdown of the RCIC at reactor 3, which led to the explosion that caused structural damage and the extent of the damage generated by the corium formed during core meltdown, remain unknown.

1.2 THE SHORTCOMINGS OF EMERGENCY SAFETY MEASURES

As time has passed, the operator TEPCO has set up alternative cooling and nitrogen inerting systems in the reactor containment vessels and tanks. As the site remains exposed to seismic and flood risks, some of this equipment has been placed in raised areas and tsunami protection systems have been built. The operator has installed control systems to monitor key parameters and remote monitoring systems have been implemented for the detection of leaks in order to stabilize the infrastructure.

Since the accident, around 400 m^3 of cooling water has been injected into the cores of reactors 1, 2 and 3 on a daily basis. To avoid tank overflow, the operator initially implemented a closed-loop cooling system to treat caesium contamination, with the support of foreign companies. Since then, a water decontamination system for all radionuclides has been developed, but it has proved very unreliable and is regularly subject to outages. In addition, the seal between the cooling circuit and groundwater is not impermeable. Every day, about 800 m^3 of water is pumped from the reactors to

[2] Nevertheless, there were cases of events occurring at one reactor that could affect another: for example, the explosion at reactor 3 disrupted the installation of the mechanism for the injection of seawater at reactor 2. In this respect, the proximity of the reactors to each other could be seen as a shortcoming.

[3] Official Report of the Independent Commission of the Japanese Parliamentary Inquiry into the Accident at Fukushima, op. cit.

be treated[4], but the high level of contamination of the recovered water prevents its release into the ocean. Some of this water is therefore stored in temporary reservoirs that are not always completely reliable, in difficult operating conditions. In order to maintain reactor cooling on a long-term basis, the International Atomic Energy Agency (IAEA) advised TEPCO to study the conditions under which it would be possible to carry out a controlled discharge of some of the stored water into the ocean (IAEA, 2013). In December 2011 the operator issued a "recovery of control" plan, which was approved by the Japanese government and has since been updated (TEPCO, 2013). It outlines plans to remove fuel from the spent fuel pool in reactor 4 prior to plant decommissioning. To this end, TEPCO has undertaken extensive preparatory civil engineering work, in particular aimed at strengthening the structure of the spent fuel pool and constructing areas for fuel handling: this work has been going on for more than two years. The removal of fuel has now begun and is expected to continue for another year in conditions that are potentially unsafe given the uncertainties about state of the fuel. At the same time, a research and development program has been established to provide scientific support to waste treatment activities (IAEA, 2013).

Further work is being carried out in the following areas: prevention of the infiltration of water from or into groundwater; the provision of access to reactor containers 1, 2 and 3; clearing debris; and the preparation of storage locations for radioactive waste. An impermeable wall is being constructed to restrict the flow of contaminated water into the ocean.

It is clear that TEPCO is carrying out an intense programme of activities in order to contain radioactive pollution and regain control of the facility. The operator must establish a mode of operation that both meets the legitimate concerns of civil society regarding safety requirements, and enables plant decommissioning (which is expected to take until 2050). The extent to which these operations gain support from the Japanese public and the international community is partly dependent on the reliability of the safety equipment and transparency of measures of radioactivity – a sensitive issue given the damage to the site. This work is regularly interrupted by emergencies, notably due to vapour emissions or leaks, for example in reactor building 3 (TEPCO, 2014). Other critical issues that have had an impact on the work are high levels of contamination in areas around the plant and the failure of water decontamination systems.

1.3 INITIAL LESSONS, NEW PERSPECTIVES AND THE CAPACITY TO TRANSITION INTO RESILIENCE

Given the scale of the Japanese accident, the authorities of member countries of the Nuclear Energy Agency (NEA) carried out additional safety studies, in order to take into account "beyond-design" (level 4) scenarios or those involving multiple failures. These complementary studies and scenarios concluded that there was no imminent risk to active nuclear facilities, and reaffirmed the validity of the defence-in-depth concept (NEA, 2013). Nevertheless, much work remains to be done for the concept to be effectively implemented.

The outcome of the ongoing feedback from the Fukushima Daiichi experience has therefore been to strengthen specific safety systems in order to bolster safety margins in the case of exceptional events. Work continues at both the normative and technical level to improve the integration of rare and extreme threat scenarios, improve crisis communication and the performance of frontline actors in degraded situations, and to specify criteria for the location of nuclear plants. Other ongoing work includes improvements to the robustness of electrical equipment and the safety of hydrogen ventilation systems, and to improve methods for the analysis of risks caused by natural phenomena.

[4] Source: Japanese Ministry of Economy, Trade and Industry. Available (in Japanese) from http://www.meti.go.jp/earthquake/nuclear/pdf/140115/140115_01c link.pdf

The idea that several installations on the same site can be simultaneously damaged has been integrated into the guidelines for severe accident management, given that it requires additional resources over a long period of time. Some operators have organized rapid response teams that are ready to intervene on-site during such a crisis, in order to provide technical and human support.

In the academic world, the accident has raised the question of the resilience of complex socio-technical systems that are affected on a long-term basis by catastrophic events. Generally speaking, the "resilience" of a system can be defined as its intrinsic ability to adjust its functioning prior to, during or following changes or disturbances, so that it can sustained required operations under both expected and unexpected conditions (Hollnagel *et al.,* 2005). From this perspective, the capacity to adapt is not limited to functional and procedural responses to threats that can be anticipated in the design stage and whose scope is based on safety assumptions (Fujita *et al.,* 2013). In particular, it should be noted that while the dispatch of technical support teams or material resources to a site where there has been an accident can reinforce the emergency planning procedure it does not, in itself, guarantee the capacity of the organization to adapt to an unexpected, ongoing situation. Moreover, some authors have noted that even the guidelines for severe accident management that have been developed following the Fukushima Daiichi accident are based on limited assumptions (Vayssier, 2012).

As long ago as 1977, Carlsen and Fink (1978) raised a very similar, pertinent question following power outages that occurred in the United States. The authors defined various states for the power supply network and highlighted that the normal operating mode could not, structurally, meet the requirements needed to manage the system in an emergency. In conditions characterized by a lack of resources and time pressure, the operator would have had to be able to take action on a heroic scale, coordinated at many different points in the network in order to avoid the collapse of the system and then recover nominal operations as soon as possible.

Fukushima Daiichi reminds us of the progress that remains to be made. Specifically, the situation TEPCO currently faces illustrates how difficult it is for an organization to curtail the unfolding of events in conditions that are critical on both a physical and organizational level. This was the motivation for our interest in the capacity of an organization to transition into resilience, in other words the ability of a socio-technical system to quickly recover to a state that ensures (at a minimum) that the situation does not get any worse, in emergency conditions and under significant social pressure. In such a situation, the system must be able to mobilize all available resources – although they may initially seem limited – following an event which causes damage of such magnitude that activities are severely disrupted or even completely destroyed.

It should be noted that resilience is the capacity to act, in the time before, during and after the emergence of a threat. The study of the organizational factors that help a system to transition into resilience has little to learn from a static and formal division into "accident – state of emergency – post-accident phase"[5]. Instead we must develop a perspective that reflects the timing of events. Moreover, although the "official" emergency phase has ended at Fukushima Daiichi, the risk of pollution or even a nuclear accident cannot be dismissed. Securing the plant's fuel stores is proving difficult and the threat of another earthquake (whether followed by a tsunami or not) remains real.

[5] Governmental working groups address the concept of resilience; formally it is considered in the post-accident context. Nevertheless, they focus on the conditions for the return to normal life of populations affected by radioactive pollution. A notable example from the United States is the work of the National Council on Radiological Protection and Measurements, Approach to Optimizing Decision-Making for Late-Phase Recovery from Nuclear or Radiological Terrorism Incidents.

At Fukushima Daiichi there are encouraging signs that the system is becoming resilient: two years after the accident, the IAEA noted the progress made by the operator TEPCO, which has adopted an increasingly proactive approach to plant decommissioning based on innovative technological solutions (IAEA, 2013). Furthermore, the French Institute for Radiation Protection and Nuclear Safety (*Institut de radioprotection et de sûreté*, IRSN) highlights that TEPCO has benefitted from earlier experience of operating incidents to improve engineering work in the design stage (IRSN, 2013). Such actions have contributed to the operator becoming more resilient, even if unexpected problems continue to arise. In this context, it is reasonable to examine the factors that may have helped the operator to transition into resilience more quickly, from the first moments following the accident, in order to prevent the ongoing succession of adverse events that have occurred since 11 March 2011. In the case of a highly technical activity such as the operation of nuclear facility, it is thus essential to examine the execution of engineering work in unusual conditions and in an extremely hostile environment.

2 ENGINEERING, A RESPONSE TO THE EMERGENCY

Safety standards prescribe the expected performance of an engineering project. As we have noted, catastrophe can ensue if they are overwhelmed – whether because of unexpected events or the failure to apply operating procedures. However, the engineering strategies used to meet technical requirements can also enhance the organization's capacity to adapt and transition into resilience. As, to the best of our knowledge there is no formal definition of such an activity, we here refer to it as "engineering thinking in emergency situations". We begin with a definition of the concept of engineering (2.1), then we introduce the concept of the emergency (2. 2), and finally, that of "engineering thinking in emergency situations" (2.3).

2.1 A DEFINITION OF THE CONCEPT OF ENGINEERING

In general, engineering is defined as the comprehensive study of all the aspects of an industrial project (technical, economic, financial and social) and the coordination of in-depth studies by specialists. By extension, it is used to refer to the study of, or activities concerned with the modification or development of technical applications that correspond to a field of knowledge in the Sciences. Engineering is an activity that structures the design and manufacturing processes of products that meet a specific need. Engineering activity is formalised into a cascade of processes and phases, from design to on-site execution via purchasing activities[6], which underpin project planning and its traceability.

Koen (1985) proposed a definition of the "engineering method" as a strategy that would offer the best possible change using the available resources in a poorly understood situation, or one subject to uncertainty. In this sense, the engineer is unlike the academic researcher, who searches for the true or false predicates that underlie a body of knowledge. The engineer approaches science from a technical perspective in which the most important issue is effectiveness: performance is judged by the way the product is commissioned. As Koen highlights, the first step taken by the engineer is to formalize a need for change expressed by a social entity. This conceptual step carries an element of uncertainty about the final outcome and how to achieve it. The stated purpose of the change is also likely to evolve as the project unfolds. In order to deal with such vagaries, engineering methods such

[6] For a detailed description in the domain of nuclear power see Cacuci, 2010.

as those formalized in the "AGILE manifesto" began to appear; first in the domain of computing and then in manufacturing[7].

The advantage of Koen's definition is that it highlights the importance of resource constraints: the engineer can only provide an approximate answer to a given question, as the answer depends on available resources. Engineering therefore includes an element of uncertainty that heuristics, based on the results of previous experience, aims to control. A skilled engineer uses various heuristic methods to solve a given problem, and the success of the result is assessed on socio-cultural criteria. This idea is one of the foundations of the Design Thinking School (Brown, 2008).

The particular role played by time should be highlighted. Time management underlies many definitions of engineering in the context of planning, which translated into the development of productivism (Boneville *et al.*, 2006). In addition, the time allocated for a project cannot be considered as an available resource.

We now examine the specific case of engineering activities in the emergency situation at Fukushima Daiichi concerning the treatment of contaminated water. Our analysis is based on publicly-available information (presentations and public reports, the media, etc.).

Beginning in March 2011, the reactor tanks at Fukushima Daiichi reached their maximum storage capacity and TEPCO sought to establish a system for recycling injected cooling water. The operator asked various industry specialists including the French company Areva, the American company Kurion and the Japanese companies Hitachi and Toshiba to assess the project. Given the volume of water to be treated, there was no standard, established solution. Areva offered a modified version of its standard decontamination system for use with the Actiflo®/ Multiflo™ units developed by the company Veolia, while Kurion designed a specialised system for the pre-treatment of caesium. Two points emerge from these interventions in the context of our introductory remarks on the definition of engineering.

On the one hand, the problem formulation, the decision to treat the radionuclide caesium as a priority, the scale of the equipment needed and risk assessments was based on a heuristic approach. Key figures were selected from historical data and technical solutions were gradually formalized through a process of trial and error: as a result, several alternative methods were discarded following the test period. The basis for the solution eventually deployed is a proven method used by Areva to treat radioactivity at their Marcoule site in France, which was modified in order to work with equipment originally intended for the purification of wastewater (Veolia's Actiflo® system). In turn, this equipment, which is used to process large amounts of water, had to be modified for use in radioactive environments with a specific set of chemicals. Similarly, the protection of on-site teams from radiation was managed on the basis of estimates of exposure levels to radiological pollutants. However, as the these levels evolved significantly as the work was carried out, the initial estimates had to be revised, and consequently engineering studies comprised a significant element of uncertainty.

On the other hand, there were significant constraints in terms of time, environment and material and human resources. Therefore Areva adopted an approach that took advantage of the resources already available in Japan (such as Veolia's Actiflo® systems). The system was implemented in under three months, during which time engineers had to conduct safety studies and simulations that took account of both the marine environment and radioactivity levels. As far as possible, studies were conducted in parallel in order to save time; nevertheless, many problems emerged. Project managers

[7] See for example the wikispeed project at wikispeed.org.

were faced with incompatibilities between the technical schedule and legal provisions for worker protection. Furthermore, on-site implementation was a particularly difficult challenge for engineering and technical teams. In particular, the construction of Areva's Actiflo-Rad® unit mobilized up to two hundred people on-site who were all required to wear a mask at all times; teams struggled to meet tight deadlines and handle resource constraints. For example, various equipment modifications had to be carried out directly on-site and work schedules had to take into account the hostile environment, which required mandatory medical supervision. According to Areva, the hostile environment and the difficulty of communication and decision making in multicultural engineering teams had a negative impact on the quality of the work.

The system was finally commissioned in time to prevent the overflow of tanks and was able to treat caesium. However, its subsequent operation was intermittent, and in July 2011 there was a leak of contaminated water resulting from a poorly-designed PVC joint that connected a hose to a water pipe. From the engineering perspective, the question of the extent to which the nature of the emergency had an impact on the selected strategy remains open. The same argument applies with respect to the problem of sludge storage and the coordination of the various solutions put forward. On this latter point, we note that both the Areva and Kurion systems proved to have shortcomings which interrupted the treatment of contaminated water, whereas, in fact, the two systems could have been operated independently. This example illustrates the extent to which "classical" engineering can be negatively affected by factors that are inherent in an emergency. Tight deadlines and high levels of uncertainty can have a significant impact on selected strategies. Therefore before we describe the concept of "engineering thinking in emergency situations", it is first necessary to define the role the "emergency" plays in determining the objectives of engineering strategy.

2.2 THE CONCEPT OF THE EMERGENCY

Roux-Dufort (2007) and Albala-Bertrand (2000) were the first to argue that emergencies reflect a twofold reality:

- on the one hand, a scenario with adverse consequences is very likely in the short term;
- on the other, only swift action and the mobilization of massive resources may be able to prevent damage.

This understanding of the emergency is based on the idea of an extraordinary deadline that brings the actor face-to-face with the limits of their resources and expertise. The concept of the emergency therefore requires careful thought, beyond that of the organizational frameworks that structure daily activity. Such frameworks are largely based on repeated actions linked to procedures, and the fragmentation of knowledge that translates – at the organizational level – into a division of labour and skills.

Here, an "organization" is understood as a structure that is the result of a decision and which minimally consists of a hierarchy, rules, a group (the "members") and instruments for supervision and sanction that are applicable to an area of activity with a specific purpose (Ahrne *et al.,* 2010). In the domain of engineering, it also includes specific tools (methodological, material, informational, etc.). The formal framework that surrounds the activity of a socio-technical system tends to create an equivalence between available resources and the corresponding organizational structure. The identification of available resources and decision-making strategies that are applied in an emergency are therefore directly related to a specific organization. Consequently, a lack of time and resources can create a conflict with the standardized execution of the organization's activity, to the point that it significantly degrades its level of performance.

Furthermore, the degree of the "emergency" is partly determined by the social context and, in the case of nuclear safety, by an overriding obligation to respond to the threat of radioactive contamination. Industrial organizations must therefore take account (to a greater or lesser extent) of the social acceptability of a failure to act. It should be noted that, within a particular organization, these decisions are essentially personal: consequently, the choices and preferences of decision makers may not only be challenged (Ahrne *et al.,* 2010) but also, in an emergency, they must be seen as legitimate in the eyes of groups external to the organization.

The context is therefore one of crisis. At the managerial level, "crises" are closely linked to the difficulty of decision making in response to an adverse event. The crisis can be fed by situations where decision makers find it difficult to formulate their goals or different actors disagree about objectives.

From our point of view, the emergency can act as a catalyst for the recomposition of networks of actors and organizations. In the case of Fukushima Daiichi it includes populations that are exposed to risk, safety authorities and engineering teams that are responsible for the management of reactor cooling and the containment of pollutant discharges. These groups of actors are created and take action around shared values (avoid the unacceptable), and interact with each other on the basis of representations framed by perceptions of hazard and time pressure. In this dynamic environment, engineers are faced with various obstacles, notably:

- the lack of collective memory (for example, when faced with an unprecedented event)
- the lack of standard modeling (in the case of an extreme phenomenon)
- shortcomings in norms and standards that usually underpin working practices (in the case of a physical environment that represents an exceptional threat).

For managers of an engineering project, subjective perceptions of the emergency can be divided into three equally important objectives: management of deadlines (when faced with an imminent threat), the effectiveness of the outcome (when the aim is to reduce risk) and the reliability of the end result (which should not create new risks).

2.3 A DEFINITION OF "ENGINEERING THINKING IN EMERGENCY SITUATIONS"

As we have seen, engineering methods consist of strategies to achieve an optimal result, given available resources and uncertainties about the technical feasibility of the solution. When engineering is impacted by an emergency, it may run into several problems:

- a pronounced state of uncertainty;
- a critical lack of resources, which may become all the more significant as the environment becomes increasingly hostile (for example in the context of a disaster). The hostility of the environment can translate directly into the resources that are available to complete the project (restricted access to information, work rates adjusted to radiation levels, complicated logistics, etc.). In this respect, overly-rigid legal provisions (for example concerning radioprotection) may limit the availability of resources in critical situations;
- high societal expectations, in terms of meeting deadlines, efficiency and the reliability of the eventual solution. The "approximate" solution adopted by the engineer will be judged in terms of the actions that needed to be taken in response to the emergency.

Decision-making strategies that maximize results based on one or another of these constraints may prove incompatible, and decision makers can find it difficult to adapt to contextual changes that require the initial strategy to be revised (Bettman *et al.,* 1996). As time pressure increases, cognitive strategies tend to minimize the use of resources, although the need for effectiveness and reliability

favour an in-depth analysis of all potential solutions. Consequently, in conditions where immediate deadlines must be met and high levels of reliability and effectiveness are required, strategic decision making becomes difficult. In the same vein, although experiments can be carried out to remove uncertainties or develop new heuristic approaches, this reduces the time available to deal with the emergency. Moreover, in the face of risk, the decision maker may prove averse to innovation (Bonneville *et al.,* 2006), although uncertainty should encourage the exploration of new avenues. When engineering methods that are designed for "traditional" project management with fewer constraints and uncertainties are applied to an emergency, *mutatis mutandis*, it is likely that the strategy will derail. A particular issue concerns the validity and relevance of "classical" risk assessments in an emergency. When innovative methods are applied in the heat of an emergency under severe time constraints, it is likely that critical shortcomings (from the point of view of society) are not taken into account. A specific example is the failure of the joint installed on Areva's Actiflo-Rad® equipment (see 2.1 above).

The concept of "engineering thinking in emergency situations" describes engineering activities that are difficult to conduct due to emergency conditions. The indicators of an emergency basically concern tension between high socio-cultural expectations of performance and a lack of readily-available resources in an uncertain situation. It should be noted that management instruments, together with technical knowledge and expertise are considered as resources.

We therefore define engineering thinking in emergency situation as:

> *Engineering activities that are significantly impeded due to a lack of resources in the face of a societal emergency.*

In practice, engineering thinking in emergency situations is an extreme case of engineering, which, in order to be implemented, requires organizational changes that are specific to the management of this type of project.

Resources, which include current knowledge and know-how, do not in themselves constitute a limited set from which the result is optimized. On the contrary, their boundaries can be adjusted and become a control parameter of the optimization function – should the organizational framework be disrupted. In addition, the final outcome must offer guaranteed performance and have the support of civil society. It is imperative that its design meets the deadlines imposed by the emergency, as a solution that is implemented following the manifestation of a threat is likely to be ineffective. In large part, these criteria for the evaluation of the performance of the end result are imposed on the engineer, and constraints tend to be applied to the targeted objective.

The issue is therefore one of innovation, based on the development of specific organizational methods that guarantee effective engineering in situations where it is used as a crisis management strategy.

3 ENGINEERING THINKING IN EMERGENCY SITUATIONS, A NEW NUCLEAR SAFETY CONCEPT

The effectiveness of engineering thinking in emergency situations is measured by the capacity of an organization to adapt its working methods and the management of engineering procedures to provide technical solutions that meet the expectations of society in a crisis (3.1). To be fully effective, such a concept must draw upon broader conceptual frameworks for safety management. The aim is

to enable the socio-technical system to transition into resilience as quickly as possible (3.2) and to establish new foundations for the conventions that underline risk management (3.3).

3.1 A CAPACITY FOR ORGANIZATIONAL ADAPTATION

As we have seen, in the context of an emergency an organization must sometimes restructure its engineering activities in order to meet the expectations of society and to overcome any related difficulties (for example, a lack of appropriate tools or the division of labour). In such a situation, it is important that engineering activities are not thought of in a conceptual framework of "project execution", but rather in terms of a new organization. In the project execution framework, planning and control processes draw upon concepts such as "tools" and "users" and focus on a definite timescale. By contrast, the concept of the "organization" draws upon ideas such as "expectations – actions – learning" loops that are inherent in interactions between individuals (Packendorff, 1995). The potential for creation and adaptation can only be realised if a new organization and associated management modes are adopted that are specific to engineering activities in an emergency situation. For example, the companies that were brought in to develop the water processing system at Fukushima Daiichi partially modified their working conditions and changed their usual organizational framework by mobilizing the necessary resources. These initiatives are an example of a need that justifies the implementation of an organization specific to the emergency for the conduct of engineering activities. However, the approach they took was one of project execution under severe time pressure, rather than a framework of temporary organizational change. This decision clearly limited their ability to foresee the shortcomings mentioned above and no doubt led them to confine their understanding of the expectations of society to the ability to meet deadlines. In summary, the concept of "engineering thinking in emergency situations" should be taken into account by operational actors who must formalize organizational changes for the execution of engineering activities when such change is required by the context of an emergency.

The first step in the effective implementation of engineering thinking adapted to emergency situations is a definition of the purpose of the activity: not only must it create a technical solution for hazard prevention; its outcome must also win the support of civil society. A technical solution is seen as an effective response to an imminent hazard only insofar as its performance with respect to risk characteristics is socially acceptable. Upstream, engineering thinking begins with the formalization of the problem, which involves a degree of approximation. If the project is to eventually succeed, it is crucial that at this stage the expectations of civil society are taken into account. Consequently, engineering activities are broadened to include other communities of actors through an assessment of the true goals of the activity (Engeström, 2011), which must also have value in the societal environment. For example, the decision to prioritize the treatment of caesium in the contaminated water at Fukushima Daiichi was eventually deemed inadequate and major engineering works followed to design a treatment system for almost all radionuclides. The delay in commissioning this system, which failed on numerous occasions during testing, was a critical factor for judging performance. In this project, one of the goals of the engineering teams was enshrined in a set of "target rates" for water decontamination. The expanded version of this goal would have led to the definition of these rates taking into account the expectations of the affected populations, which would have opened up the possibility that the waste could be discharged into the sea.

In this reformulated framework, a general lack of resources (materials, methods, information, etc.), the poor division of labour and the large number of communities involved justified an organizational move away from the context of project execution in emergency conditions. In the context of this new paradigm, timeframes and deadlines play a much more important role as structural factors than

those that can be set via the usual project planning tools. Consequently, from the moment when engineering activities become a strategic component of an organization in an emergency situation, they have to integrate this "one-off" initiative through a "temporary" organization (as defined by Lundin *et al.,* 1995). In practice, such engineering activity only exists in the time window defined by the emergency and disappears with it.

It is particularly important that the temporary organization enables the emergence of new resources that can meet the expectations of the public. It should be noted that the need for greater resources can result from a disaster context: the fact that the situation is beyond the scope of standard engineering practice means that the socio-technical system may be in an unforeseen state following the emergency (e.g. if its activities have been significantly disrupted or interrupted due to the destruction of essential functions). Consequently, the organization must put its efforts into innovation under time pressure and explore new options. Innovation, as described here, is a process that can take many forms including the creation of new methods or engineering instruments, modifications to existing resources or an assessment of related resources. In this respect, the importance to society of engineering projects undertaken in an emergency is so significant that creative solutions can emerge. This is in contrast to "classical" engineering activities, which take place in situations (including emergencies) where the existing organization is able to design solutions that fully meet the expectations of society given the current state of knowledge and the resources immediately available[8]. It is important to highlight here that appropriate changes to the organization and broadening the goals of activities so that they meet societal expectations can also help to mitigate the risk of criticism, which is a natural consequence when personal decisions are taken in a hierarchical structure (see 2.2 above).

The capacity of an industrial organization to adapt in order to successfully carry out engineering thinking in emergency situations can therefore be evaluated by at least three criteria: its capacity to expand the goals of its activities and incorporate the expectations of civil society; its capacity to temporarily change its structure to achieve these reformulated goals; and finally its capacity, through this new organization, to promote innovation that supplies resources. These three criteria help the organization to transition into resilience more quickly when faced with an extreme situation.

3.2 ACCELERATING THE TRANSITION INTO RESILIENCE

No amount of lessons learned from previous experience will lead to the development of infallible standards (Quarantelli, 1986), and it is a mistake to try to provide an exhaustive description of dysfunctional scenarios or overestimate the performance of agents in a critical situation[9]. Operators are irremediably exposed to risks that cannot be accounted for in deterministic safety management frameworks. Attempts to mitigate the consequences of such events must focus on improving the overall robustness of the socio-technical system from the moment the disaster first manifests.

Paradoxically, deterministic approaches to safety dramatize uncertainty: when the aim is to create order, the introduction of disorder is destabilizing. The capacity of an industrial organization to transition into resilience after an accident depends on its capacity to quickly switch from a normal and stable operating state to a more adaptive and innovative mode that ensures vital functions. Systems whose survival is threatened are faced with a paradox: they must find effective solutions in

[8] This clearly distinguishes work on emergency engineering from other research into project engineering methods where the aim is to compensate for critical failures that are beyond the scope of maintenance projects cf. Wearne, 2002.

[9] In the context of working groups on human and organizational factors, cf. NEA, 2013.

conditions where resources may have been partially destroyed by the accident. Strategies for transitioning into resilience consist of reconfiguring the organization and decision-making strategies in order to optimize the availability of all resources, including those that only emerge from an innovative dynamic.

A counter-example of the resilience approach is seen in the problems encountered at Fukushima Daiichi concerning the restoration of electrical power to safety relief depressurization valves (SRV). Workers found it very difficult to improvise sources of power such as mobile generators or car batteries. This example from the Japanese site shows that a delay or failure in the execution of engineering work can itself be an aggravating factor in the crisis, as it generates new risks and erodes public confidence. Although only one element of operations that are undertaken in a catastrophic situation, engineering activities can make a significant contribution – in this case, through restoring functions necessary to operate the reactors or designing ways to handle contaminated discharge. However, whether it concerns heroic action in uncertain conditions or an intervention supported by an instrumented strategy, the success of engineering in response to an emergency depends on the readiness of the organization. This leads us to conclude that is necessary to develop specific working methods that aim to enable the organization to transition into resilience, which go beyond ideas put forward by some industrialists of planning engineering resources for a crisis situation.

3.3 RETHINKING THE RULES AND THE STANDARDS

The lessons that have been drawn from the Fukushima Daiichi accident have led to improved safety standards. In particular, more stringent performance requirements for critical equipment and its operation have been put in place and the validity of the defence-in-depth concept has been reaffirmed (NEA, 21013). The approach has been shown to be effective and it is appropriate that oversight authorities prioritise the effective implementation of associated precepts. The corpus of standards describes both the scope of risks and the methods to be implemented to manage them. However, this approach does not promote the ability to become resilient. To this end, we argue that organizational issues should form part of the defence-in-depth concept, thereby providing the ability to handle “unthinkable” scenarios. To this end, engineering thinking in emergency situations represents a mode of operations that enables a socio-technical system (that is initially helpless) to regain technical control in a context that is so traumatic that it has completely destroyed all the resources necessary to take action.

These epistemological considerations require radical changes to an organization, especially in the nuclear context. The main changes apply to the plant’s safety culture and the understanding of risk management roles. When conditions are so degraded that engineering thinking specific to an emergency situation is required, it is not enough to mobilise technical resources through the application of established procedures; instead specific operating procedures must be developed, i.e. a reconfiguration of engineering activities and associated management tools appropriate to the emergency. The implementation of engineering thinking in such situations may involve changes in decision-making procedures, a new distribution of roles in engineering departments and the formalization of project management indicators tailored to the conditions of design and implementation, and the intervention. It follows that it is the responsibility of the actors in the reorganized structure to take actions in response to the disaster in order to achieve a favourable outcome, by implementing, where appropriate, *ad hoc* means.

We can therefore foresee a situation where nuclear safety oversight authorities require operators to demonstrate their ability to implement an effective engineering strategy in emergency situations and, more generally, to demonstrate their capacity (skills, expertise, methods, etc.) to quickly

transition into resilience. The goal set for the operator (including its surrounding community) would no longer be to simply contain a critical failure: its safety performance would be assessed on the basis of the capacity of its engineering systems to adapt. This capacity for adaptation must enable the recovery of key critical functions following a major disturbance (planned or not) on such a scale that it cannot be contained or controlled by the implementation of state-of-the-art equipment.

This on-site requirement for operators should be accompanied by a point-by-point relaxation of procedures for the issue of permits and monitoring functions. In serious situations, the operator should be able to waive legal provisions that protect individuals when this appears necessary to uphold the public interest. This should only happen in exceptional situations and be subject to appropriate control, if necessary *ex post factum*.

We end with a societal argument for the implementation of this new concept. The resources mobilized by the Japanese government and TEPCO in order to secure the Fukushima Daiichi site should be seen in terms of their appropriateness. Although various experts have argued that contamination levels at Fukushima warranted (without undue risk) the discharge of waste into the sea (Lake, 2013), the need to ensure a "zero" pollution risk has become a societal issue. The failures in the contaminated water treatment systems that were noted shortly after they were commissioned clearly had an influence on the general population, which deemed the risks to the environment created by the discharge of treated water into the sea unacceptable. Consequently, considerable human, material and financial resources have been deployed to prevent the risk of radioactive release generated by the treatment of contaminated water, to the likely detriment of the management of other risks. This demonstrates how a deterministic framework can create a lack of understanding in the general population, should safety measures implemented by decision makers fail. In an emergency situation, the capacity to adapt and respond effectively to new technical problems can become essential in order to ensure the trust and backing of the general public and the international community. The reward for more successful engineering thinking in response to risk during a crisis may be a better way to "integrate" the risk into society, with the aim of optimizing resources allocated to prevention.

4 CONCLUSION

In the nuclear domain, engineering standards define the realm of the acceptable. Failures are recorded and associated with prevention measures, which are themselves broken down into engineering performance requirements that are framed in terms of design or operations. Despite these attempts to create certainty, emergencies reveal the limitations and errors in prior decisions.

The situation at the Fukushima Daiichi site has highlighted another potential function of engineering. In addition to traditional safety approaches, which are framed by standards or regulations that are developed in the initial design stages, engineering thinking in emergency situations aims to contain the risks in a socio-technical system at a time when its core functions have been partially destroyed or are threatened. The challenge is to integrate a social dimension into engineering activities, and go beyond the numerical expression of a basically technical analysis. Temporary changes to the organization must provide a managerial framework that enables innovation to emerge in an emergency context. The challenge has a strategic dimension, as a successful engineering in an emergency is likely to help a system that is overwhelmed by a disaster to transition into resilience more quickly.

These initial thoughts on the concept of engineering thinking in emergency situations suggest a fundamental rethink of ideas of resilience and how to achieve it. Designing resilience requires appropriate conceptual references that take into account changes to a system in an emergency. While traditional safety models[10] are able to describe the sequence of events that may lead to damage, and the appropriate prevention measures that must be put in place, they cannot represent the state of the system or, in particular, its evolution during a prolonged disaster. This issue means that it remains difficult to measure the impact of current events at Fukushima Daiichi. It is clear that we need to renew our conceptual tools in order to fully understand the events that have unfolded since 11 March, 2011 and learn to think about "the never-ending accident".

5 REFERENCES

Ahrne G., Brunsson N., 2010, "L'organisation en dehors des organisations, ou l'organisation incomplete", Le libellio d'AEGIS, Vol. 6, n° 1, pp. 1–18, Spring 2010.

Albala-Bertrand J.M., 2000, "What is a 'Complex Humanitarian Emergency?', An Analytical Essay", Working Paper N° 420, Queen Mary University of London, October 2000.

Bettman J. R, Luce M. F., Payne J.W. , 1996, "When Time is Money: Decision Behavior Under Opportunity-Cost Time Pressure", Organizational Behavior and Human Decision Processes, Vol. 66, N 2, pp. 131–152, May 1996.

Bonneville L., Grosjean S., 2006, "'L'Homo-Urgentus' dans les organisations: entre expression et confrontation de logiques d'urgence", Communication & organisation, n°29, pp. 23–47.

Brown T., 2008, "Design Thinking", Harvard Business Review, June 2008.

Cacuci D.G., "Handbook of nuclear engineering", Springer, 2010.

Carlsen K., Fink C., 1978, "Operating under Stress and Strain", IEEE Spectrum, pp. 48–53, March 1978.

Engeström Y., 2011, "Théorie de l'activité et management", Revue Management & Avenir, n° 42, pp. 170–182, 2011 (2).

Fujita Y., Hollnagel E., 2013, "The Fukushima Disaster – Systemic Failures as the Lack of Resilience", Nuclear Engineering and Technology, Vol. 45, n° 1, pp. 1–8, February 2013.

Hollnagel, E., Leveson, N., Woods, D.D., 2005, "Resilience Engineering. Concepts and Precepts", Aldershot, UK: Ashgate.

IAEA (International Atomic Energy Agency), 2013, "Mission Report – IAEA International Peer Review Mission on Mid-and-Long-Term Roadmap towards the Decommissioning of TEPCO's Fukushima-Daiichi Nuclear Power Station Units 1-4, 25 November – 4 December 2013".

IRSN (*Institut de radioprotection et de sûreté*), 2103, "Nuclear accident at Fukushima Daiichi. Management of contaminated water from the damaged reactors. Situation at the end of June 2013", available from http://www.irsn.fr/EN/newsroom/News/Documents/IRSN-Fukushima-contaminated-water-management-20130807.pdf

Koen B. V., 1985, "Definition of the Engineering Method, American Society for Engineering Education", Washington.

[10] To a large extent, these models are derived from Reason's model of organizational accidents (Reason, 1997).

Lake H. B., 2013, “Fixing Fukushima’s Water Problem”, The Bulletin of Atomic Scientist, 9 September 2013, available online at http://thebulletin.org/

Lundin R., Söderholm A., 1995, “A Theory of the Temporary Organization”, Scandinavian Journal of Management, Vol. 11, n°4, pp. 437–455, December 1995.

NEA (Nuclear Energy Agency), 2013, “The Fukushima-Daiichi Nuclear Power Plant Accident – OECD/NEA Nuclear Safety, Response and Lessons learnt”, NEA n° 7161.

Packendorff J., 1995, “Inquiring Into the Temporary Organization: New Directions for Project Management Research”, Scandinavian Journal of Management, Vol. 11, n° 4, pp. 319–333, December 1995.

Quarantelli E. L., 1986, “Disaster Crisis Management”, Preliminary Paper n° 113, International Conference on Industrial Crisis Management, New York, 6 September 1986.

Reason J., 1997, “Managing the Risks of Organizational Accidents”, Ashgate.

Roux-Dufort C., 2007, “Is Crisis Management (Only) a Management of Exceptions?”, Journal of Contingencies and Crisis Management, Vol. 15, n° 2, pp. 105–114, June 2007.

TEPCO (Tokyo Electric Power Company), 2013, “Progress Status and Future Challenges of Mid-to-long Term Roadmap towards the Decommissioning of Units 1-4 of TEPCO Fukushima Daiichi Nuclear Power Station (Outline)” , updated 28 November 2013.

TEPCO (Tokyo Electric Power Company), 2014, “Water Flow Identified at First Floor of Unit 3 Reactor Building -Water which flows from near the Main Steam Isolation Valve Room to the Drainage Ditch on the Floor”, Press release of 20 January 2014

Vayssier G., 2012, “Present Day EOPS and SAMG: Where Do We Go From Here?”, Nuclear Engineering & Technology, Vol. 44, n°3, pp. 225–236, April 2012.

Wearne S. H., 2002, “Management of Urgent Emergency Engineering Projects”, Proceedings of the ICE – Municipal Engineers, Vol. 151, Issue 4, 1 December 2002.

Notes 

FUKUSHIMA-DAIICHI, ENGINEERING THINKING IN AN ONGOING EMERGENCY

Keywords : nuclear accident, engineering thinking, defence-in-depth, emergency, engineering

Abstract

The lessons learned from the Fukushima-Daiichi accident have focused on prevention measures designed to protect nuclear reactors and conventional crisis management methods. Although there is still no end in sight to the accident that occurred on 11 March 2011, the way in which engineering operations to secure the facilities have been carried out offers new insight into the capacity of organizations to adapt in situations that go beyond deterministic frameworks. In this article, we examine this extreme engineering scenario, which we call "engineering thinking in emergency situations".

Franck GUARNIERI
MINES ParisTech
PSL - Research University
CRC - Centre for Research on Risks and Crises
rue Claude Daunesse, CS 10207
06904 Sophia Antipolis Cedex, France

Sébastien TRAVADEL
MINES ParisTech
PSL - Research University
CRC - Centre for Research on Risks and Crises
rue Claude Daunesse, CS 10207
06904 Sophia Antipolis Cedex, France