Engineering thinking in emergency situations: A new nuclear safety concept

Franck Guarnieri, Sébastien Travadel

Engineering thinking in emergency situations: A new nuclear safety concept

Franck Guarnieri and Sébastien Travadel

Bulletin of the Atomic Scientists 2014 70: 79 originally published online 21 October 2014
DOI: 10.1177/0096340214555109

Bulletin of the Atomic Scientists

IT IS 5 MINUTES TO MIDNIGHT

Feature

Bulletin of the Atomic Scientists
2014, Vol. 70(6) 79–86

DOI: 10.1177/0096340214555109
http://thebulletin.sagepub.com

Engineering thinking in emergency situations: A new nuclear safety concept

Franck Guarnieri and Sébastien Travadel

Abstract

The lessons learned from the Fukushima Daiichi accident have focused on preventive measures designed to protect nuclear reactors, and crisis management plans. Although there is still no end in sight to the accident that occurred on March 11, 2011, how engineers have handled the aftermath offers new insight into the capacity of organizations to adapt in situations that far exceed the scope of safety standards based on probabilistic risk assessment and on the comprehensive identification of disaster scenarios. Ongoing crises in which conventional resources are lacking, but societal expectations are high, call for "engineering thinking in emergency situations." This is a new concept that emphasizes adaptability and resilience within organizations—such as the ability to create temporary new organizational structures; to quickly switch from a normal state to an innovative mode; and to integrate a social dimension into engineering activities. In the future, nuclear safety oversight authorities should assess the ability of plant operators to create and implement effective engineering strategies on the fly, and should require that operators demonstrate the capability for resilience in the aftermath of an accident.

Keywords

adaptability, emergency, engineering, engineering thinking, Fukushima, resilience

While the accidents at Three Mile Island and Chernobyl led to the introduction of new concepts in nuclear safety, investigations of the Fukushima Daiichi Nuclear Power Station disaster have not gone beyond proposals for improved safety systems, design standards, and management guidelines for severe accidents. This worrying lack of analysis suggests that the Japanese accident can be reduced to a sequence of failures.[1]

An alternative approach is to take a step back and understand the event as a chain reaction that, for more than three years, has continued to trigger crises in the context of a societal emergency—for instance, critical failures of water decontamination equipment and multiple radioactive leaks. An approach that we call "engineering thinking in emergency situations" offers a new perspective on how to handle such an ongoing emergency that affects an entire society.

In the academic world, the Fukushima Daiichi accident led to the re-examination of "resilience" in the context of a long-term catastrophic event. The resilience of a system is its intrinsic ability to adjust its functioning prior to, during, or following changes or disturbances, so that it can sustain required operations under both expected and unexpected conditions (Hollnagel et al., 2005). The ongoing events at Fukushima Daiichi demonstrate how difficult it is for an organization to transition into resilience—that is, to manage the consequences of an accident in order to increase the likelihood that the situation will be brought under control.

If organizations are to develop this capacity to adapt, their response to a threat must go beyond traditional standards-based approaches which involve prescribed functions and procedures (Hollnagel and Fujita, 2013). In particular, organizations cannot assume that the availability of technical support teams or material resources that can be rapidly dispatched on-site is proof that the organization can adapt to an unexpected, long-term situation. A pertinent observation comes from Vayssier (2012), who points out that even the guidelines for the management of severe accidents that have been developed since the Fukushima Daiichi accident are limited in their assumptions. For instance, estimates of the reaction time to recover from the failure of critical equipment might not be realistic; scenarios might not take into account areas outside the reactor containment building; and, generally speaking, the assumptions might underestimate the difficult material conditions prevailing on-site after a disaster.

At Fukushima Daiichi there are, however, encouraging signs of change: Two years after the accident, the International Atomic Energy Agency (IAEA) noted that the plant's operator (the Tokyo Electric Power Company, or TEPCO) had adopted proactive approaches to decommissioning based on innovative technologies (IAEA, 2013). It seems that the operator has incorporated feedback from earlier incidents and used it to improve engineering at the design stage. One battle may be won, but the war is far from over. Organizations such as TEPCO have not yet figured out how to manage "unmanageable" scenarios as they unfold. One answer may lie in the organization of the engineering activity itself.

The Fukushima emergency as engineering failure

The Fukushima accident began with a combination of two powerful natural phenomena: an earthquake, which triggered the automatic shutdown of the reactors and the loss of all external power supplies; and a tsunami, which then flooded generators (National Diet of Japan, 2012). The lack of electricity made it difficult to monitor and control the state of the reactors. On-site damage severely disrupted the operating conditions in control rooms, as well as communication between these rooms and the on-site crisis center.

Although the sequences of reactor failures were relatively independent, shift supervisors failed to transmit correct and complete information to the on-site crisis center, which led to shortcomings in overall monitoring. Consequently, reactors were left uncooled for several hours, which led to the release of significant levels of radioactive waste. The Japanese investigation highlighted shortcomings in the actions taken by the federal government, Japanese nuclear

authorities, and TEPCO with respect to risk analysis, design standards, and oversight by the operator (National Diet of Japan, 2012).

Fukushima recovery and response

Since the disaster, about 800 cubic meters of contaminated cooling water are pumped from the reactors every day (METI, 2014); some of this water is stored in temporary reservoirs that are not always completely watertight. A decontamination system to remove radionuclides was developed but has proven extremely unreliable. To sustain reactor cooling over the long term, the IAEA recommended that TEPCO study the conditions for a controlled discharge of some of the stored water into the ocean (IAEA, 2013).

In December 2011, the operator issued a mid- and long-term post-disaster recovery plan that was approved by the Japanese government and has since been updated (TEPCO, 2013). This plan proposes the removal of fuel from the spent fuel pool of Reactor 4 prior to plant decommissioning. At the same time, a research and development program has been established to provide scientific support for waste treatment activities (IAEA, 2013). Work has already begun on the dismantling of fuel rods and is expected to continue for another year. It is a dangerous job, given how little is known about the state of the fuel rods.

To make matters worse, nobody is quite sure whether the Japanese public will support decommissioning, given the repeated malfunctions, the uncontrolled high level of contamination on-site and in surrounding areas, and the failure of water decontamination systems. In the midst of this ongoing emergency, TEPCO is carrying out an intense program of on-site activities. The aim is to contain radioactive pollution, regain control of the facilities, and complete decommissioning by the year 2050.

Elsewhere, members of the Nuclear Energy Agency (NEA) have carried out their own safety studies designed to take into account "beyond-design" and multiple-failure scenarios. NEA member states concluded from these studies that there was no imminent risk to their operating facilities. Although the NEA (2013) reaffirmed the validity of the defense-in-depth concept—which uses multiple independent and redundant safety systems to protect against failures and unanticipated events—it is clear that the concept needs a lot more work if it is to be effectively implemented. All that has been learned so far is that specific safety systems should be strengthened to bolster safety margins in exceptional circumstances.

The role of engineering

Engineering usually encompasses the many and varied aspects of an industrial project (technical, economic, financial, and social). By extension, it refers to the study of, or activities concerned with, the modification or development of technical applications that correspond to a scientific field of knowledge. A particular additional feature of nuclear engineering is that quality control standards are extremely high (Cacuci, 2010). 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 or uncertain situation. Given the constraints, it is no surprise that engineers can only provide

approximate answers; ultimately, society decides whether the outcome is a good one.

Time management underlies many definitions of engineering. In a nuclear crisis, time is an indicator of an emergency situation. Roux-Dufort (2007) and Albala-Bertrand (2000) argue that emergencies reflect a twofold reality: a scenario with adverse consequences is very likely in the short term; and only swift action and the massive mobilization of resources may prevent damage.

Organizations affected by emergencies are largely based on ritualized processes, fragmented knowledge, and a division of labor and skills—and they are made up of people who may have differing opinions on what constitutes an emergency. Consequently, their decisions are open to challenge, both from within the organization and from external groups (Ahrne and Brunsson, 2010).

Thinking in an emergency

Engineering project managers are in the hot seat. Their subjective understanding of an emergency has to respond to three equally important objectives: meeting deadlines (when the threat is imminent), finding effective and reliable solutions that reduce risk, and avoiding the creation of new risks. Engineers faced with an emergency have several problems to solve:

- They don't know the full extent of the situation.
- They face a critical lack of resources, especially technical knowledge and practical know-how. If the environment becomes hostile (in the context of a disaster, for instance), this only gets worse.
- Society expects a lot from them. Deadlines must be met, and solutions must be found.

Solutions based on only one of these constraints can be incompatible, and decision makers are often slow to adapt when they have to make changes to their initial strategy (Payne et al., 1996). At the same time, decision makers don't care for innovation when the risks are high (Bonneville and Grosjean, 2006), despite the fact that uncertainty offers an opportunity to explore new avenues.

"Engineering thinking in emergency situations" therefore describes the difficult activities that engineers have to conduct, with limited resources, in an emergency that affects the general population. What is an emergency? At a minimum, it describes the tension between society's high expectations that a solution can be found, and a lack of readily available resources in an uncertain situation. We therefore define engineering thinking in emergency situations as (Guarnieri and Travadel, 2014: 10): *Engineering activities that are significantly impeded due to a lack of resources in the face of a societal emergency*.

At its simplest, engineering thinking in an emergency situation is an extreme case of engineering. However, when it is used as a crisis management strategy, the goal is to foster the ability to innovate, through specific organizational changes that increase adaptability and resilience.

Adaptable organizations

Effective engineering thinking in emergency situations is measured by the ability of an organization, in a crisis, to modify its working practices and provide technical solutions that meet the

expectations of society. This requires a radical rethinking of how engineering activities are organized.

The conventional solution, which takes the form of a project framework (including planning and control processes that are materialized by "tools" and "users") working within a known timescale, isn't much use in an emergency. A more helpful framework introduces the concept of a "temporary" organization (Lundin and Söderholm, 1995). In itself, the concept of "organization" reflects the "expectations-actions-learning" loops found in interactions between individuals in working situations (Packendorff, 1995). Furthermore, incorporating social acceptability into engineering not only increases community involvement but also integrates the activity into its environment by a redefinition of its goals.

A good example of this comes from Fukushima Daiichi, where none of the various systems that were implemented to treat contaminated water were considered adequate. Engineers could not see beyond a set of "target rates" for water decontamination. Alternatively, the objectives of the engineering activity could have been expanded to take into account the expectations of the affected populations. The target rates could then have been defined accordingly, thus opening up the option of discharging waste into the sea. Expanding the objectives of the activity poses new challenges, so the temporary organization must make it possible for new resources to emerge, and must promote innovation in order to meet the expectations of society.

Traditionally, emergency management has consisted of the deployment of technical resources and the application of established procedures. Engineering thinking in emergency situations goes far beyond this. It looks for ways to reconfigure the organization of engineering activities and associated management tools, depending on immediate needs. It can include changes to decision-making procedures or the redistribution of roles within the organization. In exceptionally severe situations, it may even involve deviating from legal requirements when they are clearly not in the public interest and limit the capacity of the organization to adapt.

Engineering thinking in emergency situations cannot happen if the organization is not adaptable. Adaptability can be assessed using three criteria: the organization's ability to widen the scope of its activities and goals to include the expectations of civil society; its ability to temporarily change its structure to achieve these reformulated goals; and its capacity, through this new structure, to promote innovation that supplies resources. Organizations that can fulfill these criteria can quickly transition into resilience in a catastrophic situation. But, to be fully effective, organizations need a broader conceptual framework for safety management.

Resilience as a new safety requirement

No matter how many disasters there are, and no matter how much experience is gained, standards will never be infallible (Quarantelli, 1986). It is difficult to provide an exhaustive description of dysfunctional scenarios, and easy to overestimate the performance of agents in a crisis (NEA, 2013).

Paradoxically, deterministic approaches to safety that attempt to anticipate every

outcome can actually make a crisis more dramatic: When the aim is to create order, disorder is destabilizing. The transition to resilience requires a quick switch to an adaptive operating mode, which may imply the reconfiguring of the organization and its decision-making strategies in order to optimize the availability of resources. Indeed, when the survival of critical infrastructure such as nuclear reactors is threatened, effective solutions must be found even though significant resources have been destroyed by the accident. This raises the vision of a future in which nuclear safety oversight authorities require operators to demonstrate their ability to implement an effective engineering thinking strategy in an emergency situation and, more generally, to demonstrate their capacity (skills, expertise, methods, etc.) to ensure a rapid transition into resilience.

Fukushima Daiichi provides good examples of what happens when the resilience approach is not followed. On a small scale, when they were faced with the loss of electrical power and the subsequent impossibility of activating relief valves, workers found it difficult to set up new power sources such as mobile generators and car batteries. As a result, the cores of the reactors were left uncooled for several hours and started to melt down.

On a bigger scale, engineering makes a significant contribution to disaster management—whether through the restoration of functions necessary to operate reactors, or the design of ways to handle contaminated waste. On the other hand, a delay or failure in the execution of engineering work can be an aggravating factor in a crisis, as it generates new risks and erodes public confidence.

Beyond traditional safety models

The situation at Fukushima Daiichi has highlighted a potential new function of engineering. A topical example is the work being done to decontaminate the large volumes of cooling water injected into the reactors. Traditionally, safety has been framed by standards developed in the design stages of a project. However, there is also an opportunity for engineering thinking in emergency situations to enhance safety and contain risks in an organization that has had its key functions destroyed. Critical to this end is how to integrate a social dimension into engineering activity and move it beyond an essentially technical, number-crunching exercise. Temporary organizational change must also provide a managerial framework that encourages innovation in an emergency. This is a strategic challenge, because effective engineering thinking in emergency situations can accelerate the transition into resilience for a system that has been overwhelmed by a disaster.

Practical considerations about how to achieve resilience through appropriate organization raise questions about resilience itself. Thinking about resilience implies the modeling of changes to the system facing an emergency. This is where traditional safety models break down. Although they offer some help in describing hazardous scenarios and outlining measures to prevent failures from propagating, they cannot represent the state of the system or changes to it, particularly in the context of a long-term emergency that continues even after natural disasters and official crisis periods have come to an end. This may be why it is difficult to measure the full extent of events at Fukushima Daiichi.

The shortcomings of traditional frameworks should not be used as an excuse to underestimate problems—a phenomenon that is particularly evident in assessments of the epidemiological consequences of nuclear accidents (Perrow, 2013). A new conceptual framework is needed to fully measure the impact of the events that have unfolded since March 2011, and to find better ways to think about the "never-ending" disaster.

Funding

This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

Note

1. This article is adapted from a working paper published earlier this year by the Centre for Research on Risks and Crises at MINES ParisTech.

References

Ahrne G and Brunsson N (2010) L'organisation en dehors des organisations, ou l'organisation incomplète. *Le libellio d'AEGIS* 6(1): 1–18. Available (in French) at: http://crg.polytechnique.fr/v2/fic/Le_Libellio_printemps2010.pdf.

Albala-Bertrand JM (2000) What is a 'complex humanitarian emergency'? An analytical essay. Working paper no. 420, October. Queen Mary University of London. Available at: http://www.econ.qmul.ac.uk/papers/doc/wp420.pdf.

Bonneville L and Grosjean S (2006) L'"Homo-Urgentus' dans les organisations: Entre expression et confrontation de logiques d'urgence. *Communication & Organisation* 29: 23–47. Available (in French and English) at: http://communicationorganisation.revues.org/3367.

Cacuci DG (ed.) (2010) *Handbook of Nuclear Engineering*. New York: Springer.

Guarnieri F and Travadel S (2014) Fukushima-Daiichi, engineering thinking in an ongoing emergency. Working paper published by the Centre for Research on Risks and Crises, MINES ParisTech, July. Available at: http://hal-ensmp.archives-ouvertes.fr/docs/01/02/11/98/PDF/engineering_thinking_ongoing_emergency_july2014_CRC_22.pdf.

Hollnagel E and Fujita Y (2013) The Fukushima disaster – systemic failures as the lack of resilience. *Nuclear Engineering and Technology* 45(1): 13–20.

Hollnagel E, Woods DD, and Leveson N (eds) (2005) *Resilience Engineering: Concepts and Precepts*. Aldershot: Ashgate.

International Atomic Energy Agency (IAEA) (2013) 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. IAEA second mission report. Available at: http://www.iaea.org/newscenter/focus/fukushima/final_report120214.pdf.

Koen BV (1985) Definition of the engineering method. Washington, DC: American Society for Engineering Education. Available at: http://files.eric.ed.gov/fulltext/ED276572.pdf.

Lundin RA and Söderholm A (1995) A theory of the temporary organization. *Scandinavian Journal of anagement* 11(4): 437–455.

Ministry of Economy, Trade and Industry (METI) (2014) Fukushima Daiichi Nuclear Power Station Storage conditions of tritiated water and contaminated water treatment. Available (in Japanese) at: http://www.meti.go.jp/earthquake/nuclear/pdf/140115/140115_01c.pdf.

National Diet of Japan (2012) The official report of the Fukushima Nuclear Accident Independent Investigation Commission. Executive summary. Available at: http://www.nirs.org/fukushima/naiic_ report.pdf.

Nuclear Energy Agency (NEA) (2013) The Fukushima Daiichi Nuclear Power Plant accident: OECD/NEA nuclear safety response and lessons learnt. Report no. NEA 7161. Paris: OECD. Available at: http://www.oecd-nea.org/pub/2013/7161-fukushima2013. pdf.

Packendorff J (1995) Inquiring into the temporary organization: New directions for project management research. *Scandinavian Journal of Management* 11(4): 319–333.

Payne JW, Bettman JR, and Luce MF (1996) When time is money: Decision behavior under opportunity-cost time pressure. *Organizational Behavior and Human Decision Processes* 66(2): 131–152.

Perrow C (2013) Nuclear denial: From Hiroshima to Fukushima. *Bulletin of the Atomic Scientists* 69(5): 56–67.

Quarantelli EL (1986) Disaster crisis management. Preliminary paper #113. Written version of shorter oral remarks made at International Conference on Industrial Crisis Management, New York, September 6. Available at: http://udspace.udel.edu/bitstream/handle/19716/487/PP113.pdf?sequence=3.

Roux-Dufort C (2007) Is crisis management (only) a management of exceptions? *Journal of Contingencies and Crisis Management* 15(2): 105–114.

TEPCO (2013) Progress status and future challenges of Mid-and-Long-Term Roadmap towards the Decommissioning of Units 1–4 of TEPCO's Fukushima Daiichi Nuclear Power Station (outline). Report, Council for the Decommissioning of TEPCO's Fukushima Daiichi Nuclear Power Station, June 27. Available at: http://www.tepco.co.jp/en/nu/fukushima-np/roadmap/images/d130627_01-e.pdf.

Vayssier G (2012) Present day EOPS and SAMG: Where do we go from here? *Nuclear Engineering and Technology* 44(3): 225–236.

Author biographies

Franck Guarnieri is director of the Centre for Research on Risks and Crises at MINES ParisTech in France, and scientific advisor to the French software company Preventeo. He is also a designated expert in the European Union's Horizon 2020 program and the French National Research Agency, and a member of the Foundation for an Industrial Safety Culture.

Sébastien Travadel is a chief engineer for the French Ministry of Transport and Equipment. He also holds a PhD in law and is qualified as a senior mathematics teacher. He has held several managerial positions in the French agency in charge of aircraft accident and incident investigations, notably as head of major investigations. He headed the Airspace and Air Navigation Regulation Department at the French Civil Aviation Authority before co-founding the company Safety Line which produces decision support software. He is now Associate Professor with the Centre for Research on Risks and Crises at MINES ParisTech.