Reliability Engineering and System Safety 141 (2015) 83–91

Contents lists available at ScienceDirect

Reliability Engineering and System Safety

journal homepage: www.elsevier.com/locate/ress

Factors underlying organizational resilience: The case of electric power restoration in New York City after 11 September 2001

David Mendonça*, William A. Wallace

Rensselaer Polytechnic Institute, 110, 8th Street, Troy, NY 12180, USA

ARTICLE INFO

Available online 17 March 2015

Keywords:
Resilience engineering
Disaster response
Organizational resilience

ABSTRACT

The 2001 World Trade Center attack resulted in widespread and highly non-routine failures to critical infrastructure systems. An immediate priority following the attack was the restoration of electric power in lower Manhattan. A study of the organization responsible for conducting this restoration is here presented in order to provide a productive critique of factors theorized by Woods (2006) [1] to affect organizational resilience. Data sources include logs of the behavior of the electric power infrastructure and extensive interviews with personnel at various levels of the organization. The conclusions of the analysis are used to frame a refined set of factors that shape organizational resilience, and to provide observations on the processes that underlie how organizations achieve—or fail to achieve—the potential for resilience.

1. Introduction

Considerable attention has been devoted to identifying opportunities for engineering organizational resilience both to minimize the impact of disruptions on normal operations, and perhaps to capitalize on the opportunities for learning lessons from organizational response to challenging, unforeseen circumstances. This work has included new technologies and new work practices, as well as new categories of workers (e.g., resilience engineers), particularly within organizations that operate in safety-critical environments. Yet large-scale studies of organizational resilience are relatively rare, perhaps owing partly to the unpredictable timing of events that test resilience, as well as to difficulties in gaining access to data from organizations as they respond to these events.

The overarching objective of this study is to provide an empirically grounded critique and extension of the factors (articulated by Woods [1]) which have been theorized to contribute to organizational resilience. Study data are associated with the restoration of electric power in the borough of Manhattan in New York City following the 11 September 2001 attacks. The approach is case study-based, driven by analysis of both subjective data (collected from individuals occupying operational to strategic roles) and objective data (collected from technological elements of the system, using both established and ad hoc instrumentation). The factors are critiqued by exploring alternative approaches for their measurement using these data, while also identifying opportunities for refining or otherwise emending them. A secondary objective of this work is to describe decision making processes in the cases in order to contribute to process-level theories of organizational resilience. The paper concludes with a refined set of resilience factors, observations on processes underlying resilient performance, and implications for Woods' [1] original framework.

The paper proceeds as follows. In Section 2, theoretical background on factors underlying resilience is presented within a more general framework of vulnerability to hazard. An overview of the effects of the 11 September attacks, along with a description of the research methodology, is given in Section 3, followed by a presentation and discussion of the results of three related case studies (Section 4). The paper concludes with an overall discussion (Section 5) and conclusions, including suggestions for future work (Section 6).

2. Vulnerability and resilience

As framed by Smit and Wandel [2], a system's vulnerability to hazard may be understood as a function of two factors: *exposure to hazard* and an *ability to cope with*, *adapt to*, *or otherwise withstand hazard*. New technologies, ranging from sensor-based systems [3,4] to predictive models [5], seek to reduce uncertainty concerning risks associated with the first factor [6]. The second factor relates directly to the concepts of adaptive capacity and resilience (see [7] for a discussion). *Adaptive capacity* [8] may be described as “the ability or capacity of a system to modify or change its

* Corresponding author. Tel.: +1 518 276 4222; fax: +1 518 276 8227.
E-mail addresses: mendod@rpi.edu (D. Mendonça), wallaw@rpi.edu (W.A. Wallace).

http://dx.doi.org/10.1016/j.ress.2015.03.017

characteristics or behavior so as to cope better with existing or anticipated external stresses" [9]. Adaptive capacity "is difficult to gauge because of its latent nature, meaning that researchers often struggle to measure it until after its realization or mobilization within a system" [10]: that is, until it has been manifested as *adaptive behavior* [10,11], whether manifested before event onset (anticipatory) or after it (reactive) [12].

Resilience may be viewed more broadly, as expressing not only the capacity to adapt, but also the morphology of adaptive behavior (see [13] for a recent review). As expressed by Woods [1], "resilience is concerned with monitoring the boundary conditions of the current model for competence (how strategies are matches to demands) and adjusting or expanding that model to better accommodate changing demands." Among the aspects of resilience are an ability to resist disorder [14], as well as an ability to retain control, to continue and to rebuild [15].

Yet, as with adaptive capacity, resilience may be difficult to measure or otherwise assess before a system has been exposed to a hazard (i.e., before it has been manifested as resilient performance) [1]. Central to both adaptive capacity and resilience perspectives is the notion of emergent behavior either in anticipation of hazard or in reaction to it [16,17]. As documented below, the emergent nature of resilient performance creates a number of challenges related to measurement and, to some extent, in the development of frameworks in which to situate explanations of why this emergent behavior succeeds or fails [17].

Within a framework that is implicitly systems-oriented, Woods [1] postulates a number of factors thought to affect organizational resilience:

- *Buffering capacity*: The size or kinds of disruption that can be absorbed/adapted to by the system without a fundamental breakdown in its performance/structure;
- *Flexibility/stiffness*: The system's ability to restructure itself in response to external changes/pressure;
- *Margin*: "How closely or how precariously" the system is operating relative to some performance boundary;
- *Tolerance*: How the system behaves in proximity to some boundary (i.e., whether the system "gracefully degrades" or "collapses" as stresses/pressures increase); and
- *Cross-scale interactions*: Downward, how context leads to (local) problem solving; upward, how local adaptations can influence strategic goals/interactions.

These factors are adapted and condensed in slightly modified form by Jackson and Ferris [18] into capacity, flexibility, tolerance and cohesion (i.e., "the ability of a system to act as a unified whole in the face of a threat"), each of which is then further expressed in terms of principles for achieving resilience (one of which corresponds to Woods' [1] "margin" factor). Related factors are proposed elsewhere: for example, those presented in [19] include controllability, limitation of effect and minimization of failure, all of which relate closely to *buffering capacity*, *flexibility* and the distinct factor of early detection. Woods' [1] factors have been explored through a qualitative study of teamwork in emergency response [20]. (It should be noted that factors shaping organizational resilience have also been viewed from other perspectives, such as those emphasizing safety culture (e.g., [21]).) Related research emphasizes the importance of capturing system dynamics in order to understand and properly frame resilient performance [13]. For example, in a discussion of "enterprise" (e.g., business) resilience by Erol et al. [16], *recovery time* refers "the time taken for an enterprise to overcome disruption and return to its normal state," while *level of recovery* refers to the extent to which the enterprise can provide an appropriate level of service or functionality.

A number of theoretical and empirical issues have arisen in attempts to capture and analyze data for evaluating factors thought to underlie organizational resilience. First, exposure to profound stresses in organizations is, by definition, rare, thereby challenging efforts to establish performance boundaries before exposure has occurred. The issue is further accentuated by the possibility that, post-event, the design of the affected system will evolve in unexpected ways. Put simply, the operating envelope of the organization may be in constant flux and, perhaps more importantly, its ultimate form may be impossible to determine until the performance has concluded.

Second, despite ongoing advances in sensor and other technologies [22–25], data collected from contemporary systems continue to be difficult to situate within established or new theoretical frameworks [26,27]. For example, research on adaptive capacity in human ecology [9] provides indices that tend to be aggregated, static, and derived from socioeconomic measures such as census data (e.g., [28]). A recent parallel line of theoretical research, however, strongly suggests that "adaptive capacity is context-specific and likely shaped by dynamic variables that are not easily generalizable and do not carry equal weight between contexts" [10]. A similar case may be made for organizational resilience.

To help address these issues, the factors proposed by Woods [1] regarding organizational resilience may be viewed as bridging a conceptual gap between larger frameworks of resilience (e.g., those at the community level) (e.g., [29]) and studies seeking to develop empirical indicants of resilience, particularly for organizations (e.g., [21]). As has been echoed elsewhere, the availability of a theoretically salient conceptual layer facilitates the conceptual and discriminant validation of case-specific empirical indicants against a common set of concepts [30].

A third and final issue arises from the degree to which one organization is linked to others via shared information, physical resources, personnel or other mechanisms. Recent work has begun to extend resilience engineering concepts and practices from studies of *independent* systems to studies of *interdependent* ones. In independent (or minimally dependent) organizations, organizational (and thus performance) boundaries are controlled by the organization itself. Indeed, as discussed by Leveson [31], a recognized limitation of conclusions on high reliability organizations (HROs) [32] is that the organization has "nearly full knowledge of the technical aspects of operations" and that "the people in these organizations know almost everything technical about what they are doing" [33]. In interdependent organizations, by contrast, resilience is the by-product of the efforts of multiple dependent organizations, with consequent uncertainties about human and technical aspects of organizational operations.

A rich vein of research on interdependent critical infrastructure systems—in part motivated by the attacks of 11 September—has sought to conceptualize [34–36], measure [37–39], model [13] and support [40,41] the management of the links between systems such as electric power, water, wastewater, telecommunications and transportation, among others (for recent reviews, see [42,43]). Critical infrastructures (CIs) are here viewed as mixed human–machine systems composed of a large number of interacting components exhibiting nonlinear relationships, thus limiting their ability to be described, controlled or predicted at a systems level. Recent work has emphasized the need for further progress in understanding and predicting adaptation and resilience in relation to hazards that face critical infrastructures [44]. To support this work, a panoply of technological [45,46] and social [44] sensors is now available, though—for reasons discussed previously—data produced by these technologies must be cast in relation to theoretically grounded constructs of organizational resilience.