Available online at www.sciencedirect.com

ScienceDirect

Procedia CIRP 60 (2017) 536 – 541

www.elsevier.com/locate/procedia

27th CIRP Design 2017

Towards the Design of Resilient Large-Scale Engineering Systems

W. H. Jonathan Mak[a]*, P. John Clarkson[a]

[a]*University of Cambridge, Trumpington Street, Cambridge, CB2 1PZ, United Kingdom*

* Corresponding author. Tel.: +44 1223 748562. *E-mail address:* whjm2@cam.ac.uk

Abstract

Resilience has mostly been thought of as the ability to recover from adversity. However, it is now increasingly recognised that resilience should not only serve as a means for organisations to survive hardship, but also to thrive and prosper. For large-scale engineering systems, such as telecommunications networks and power grids, this is vital due to relatively long life cycles leading to large uncertainties, and also due to the significant investments involved. Exactly how this and thus resilience should be designed into such systems, however, is less well defined. Here, the term resilience is explored through engineering, organisational and ecological literature to understand differing perspectives from select domains before distilling these into the three engineering design lifecycle properties: robustness, adaptability and flexibility. In particular, a distinction is highlighted between adaptability and flexibility following findings in literature. These properties and the concept of resilience are discussed with reference to system performance in order to serve as requirements for designing large-scale resilient engineering systems.

Keywords: Resilience; engineering systems; engineering design

1. Introduction

Resilience has traditionally been associated with negative connotations: the ability to recover from adversity or trauma. Indeed, a basic definition from the Oxford English Dictionary [1] gives: “The quality or fact of being able to recover quickly or easily from, or resist being affected by, a misfortune, shock, illness, etc.; robustness; adaptability”. While this similar in other dictionaries [2,3], there is less consensus across domains in academia and in industry.

The term “resilience” was first popularised by Holling within the field of ecology to assess the stability and resilience of interacting populations and the environment [4]. In their work, the term is defined as the “persistence of relationships within a system and is a measure of the ability of these systems to absorb changes of state variables, driving variables, and parameters, and still persist”. This concept of a system’s interaction with the environment and surviving disturbances is similar to the foundations for resilience in many other fields including supply chain management [5], crisis management [6], psychology [7] and resilience engineering [8]. However, there is now growing recognition that resilience not just allows for recovery, but also to allows for the ability to thrive and prosper following difficult times [9].

This is especially relevant for large-scale engineering systems, such as communication networks and energy production plants, which have relatively long life cycles, typically 10 or more years, and incur significant investments. As a result of such long time scales, such systems not only need to withstand imminent shocks but also have to be designed such that it can cope with and build upon evolving technologies into the future. It is thus argued here, that by designing large-scale engineering systems to be resilient, they are better equipped to weather hardship and also succeed in the future.

Exactly, how resilience is designed into engineering systems, however, is less well established. To better understand how resilience may be incorporated for large-scale engineering systems, this paper first examines literature from engineering, management and ecology to understand different views of resilience. These fields are specifically included since contrasting insights were found. Following this, these

doi:10.1016/j.procir.2017.01.034

views were then related to engineering design concepts to form requirements for the design of resilient engineering systems and discussed for applications to a large-scale engineering systems.

2. Views of Resilience

Resilience has demonstrated applicability to many domains. Through exploration of the resilience literature, it was found that a system must be designed to withstand disturbances, yet also continue to perform well as the environment changes. Further examination of the resilience literature suggests that this may be achieved through three characteristics: absorbing disturbances, adapting for change and thriving for the future.

2.1. Absorbing Disturbances

Traditionally in engineering and most domains, resilience has been typically thought of as a recovery from some disturbance. This can be achieved through simply having enough resources or redundancy to absorb shocks. For example, a bridge may be built to have sufficient structural strength to withstand all foreseen loads.

This view of resilience stems from early work in designing High Reliability Organisations which focused much more on risk and safety management in engineering [10]. Early case studies involving resilience thus focus on high risk industries such as nuclear plants [11], offshore helicopter transport [12], and the Columbia Space Shuttle disaster [13]. As such, much of this analysis revolves around analysing vulnerabilities, risk analysis and calculating the probability of failure in engineering systems so that the system performs as expected in operation.

These ideas evolved to recognize that it is impossible to conceptualise every failure in the system and that it is better to enable the system to respond appropriately to disturbances when they do occur [14]. This view of resilience is therefore achieved by designing the system to be robust so that it simply absorbs all disturbances within some margin and continues to perform, giving some desired output. Such behaviour may be achieved through buffering capacity [15], redundancy [16] or by including tolerance into the system [17].

The key idea amongst these terms is that the system is able to maintain performance without the need to change the system if the disturbance is within a certain margin.

2.2. Adapting for Change

Absorbing disturbances alone is not sufficient for resilience, however, and the key factor that separates resilience from other system properties such as “brittleness” or “vulnerability” is the need for adaptive capacity in the system to continue normal operations [14;18]. In this sense, a recovery requires actual change in the system to maintain a desired output. This could be a reorganization of resources, as typically seen in management and organizational literature, or control systems where feedback loops maintain a desired output.

This is typically employed where the margins are too large or impractical to be “absorbed”. That is, the range of disturbances may be sufficiently large such that one robust design may not be enough or practical to maintain system performance. Studies with this view of resilience include how communities handled the aftermath of Hurricane Katrina [19] and the terrorist attacks of 9/11 [20]. In both cases, it was found that having a contingency plan was a clear benefit and helped to save lives. However, another study further investigated the effect of the destruction of the Emergency Operations Centre during the 9/11 attack which disrupted planned protocols. It was found that key to maintaining operations was integrating the adaptive capacity of the response organization with the resources of New York City, private entities, and government at all levels. These examples highlight the need to be prepared for eventualities in order to “absorb” disturbances through contingency plans, but also demonstrate that the ability to adapt, when there is no clear plan, is necessary to achieve resilience. Dalzielle and McManus [16] captures this by defining resilience as a combination of having “enough redundancy to provide continuity of function, or through increasing the ability and speed of the system to evolve and adapt to new situations as they arise”. As such, resilience, in these domains is measured by the recovery time to return to a previously undisturbed state [21;22].

The key idea of adaptation in this sense is that the system is able to maintain performance with some internal change to the system.

2.3. Thriving for the Future

While the ability to adapt is essential for resilience, adaptation takes a slightly different, yet significant, view in the field of ecology. From an ecological resilience perspective, adaptation refers to a system moving between states of equilibria [23]. Ecology focuses on the interactions of a systems, be it organisms or natural systems such as lakes, and the environment. Such work concentrates on maintaining equilibrium in systems and a disturbance may, for example, cause a fluctuation in population numbers of interacting species. If there is a significant disturbance, an introduction of a species say, the system of species will fall into a different set of equilibria or states which may lead to the extinction of a species. Therefore, adaptation in the ecological sense refers to a system moving between system states and resilience is defined as the “ability to absorb change and disturbance and still maintain the same relationships between populations or state variable” [4]. With such a definition, resilience in ecology is measured by the amount of disturbance the system can take until the system changes to another equilibrium or state [24;25].

This notion of changing or evolving the system between states in resilience has carried over to other domains and it is now recognised that in order to achieve resilience, the system should also “thrive” by adapting for opportunities for better performance [9]. Adaptation in this context thus involves