Automation in Construction 90 (2018) 253–264

Contents lists available at ScienceDirect

Automation in Construction

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

Cognitive infrastructure - a modern concept for resilient performance under extreme events

Naser M.Z.[1], Kodur V.K.R.[*,2]

Department of Civil and Environmental Engineering, Michigan State University, East Lansing, MI, USA

ARTICLE INFO

Keywords:
Cognitive structures
Extreme events
Disaster management
Resiliency
Internet of things (IoT)

ABSTRACT

The increasing frequency and intensity of natural disasters, as well as escalation of manmade threats, are posing significant threats to the built environment. Further, much of civil infrastructure in developed countries, built after World War II, is experiencing age-related deterioration and thus are vulnerable to damage under extreme events. This vulnerability of infrastructure under severe loading conditions can be assessed through a coupled sensing-structural framework that extends principles of the recently developed "Internet of Things" (IoT) technology into civil infrastructure. This concept aims at monitoring key response parameters (i.e. temperature, strain, deformation, vibration levels etc.) by incorporating cognitive abilities into a structure through interaction of various sensing devices and socio-environmental factors. These response parameters can be utilized to trace performance of critical infrastructure during the course of a disaster so as to predict signs of imminent failure and to provide first responders and occupants with much needed situational awareness. The practicality of the proposed concept in enhancing resilience of new and existing infrastructure is illustrated through two case studies.

1. Introduction

Civil infrastructure primarily constitutes of facilities, such as high-rise buildings, highways, airports, dams, and power plants etc. In general, 10–15% of civil infrastructure is considered to be critical and vital to the functionality of the society. As such, their destruction or incapacitation, in the aftermath of a disaster, would disrupt welfare of the public and overall safety, security, and economy of the country [1–4]. Critical infrastructure is designed to last for 50+ years, and recent surveys have indicated that existing infrastructure continue to operate past their intended service life [1,2]. During this long service life, infrastructure is often subjected to numerous hazards and environmental conditions (i.e. disasters) making them highly vulnerable to damage [3,4].

A disaster is defined as an event or incident that causes loss of human life, socio-economic damage, ecological disruption, deterioration of health and health services on a large scale to warrant an extraordinary response from outside the affected zone. The impact of natural, manmade and natural hazard triggering technological disasters (NATECH) from earthquakes, tsunamis, terrorist attacks, nuclear meltdowns etc. has affected more than 4.4 billion people over the past few decades. For example, the reported losses arising from natural disasters occurring in the US, in 2016 alone, was estimated at $175 Billion [5]. Unfortunately, these losses are growing on yearly basis due to increasing population pressure on urban infrastructure, as well as lack of measures for upkeeping of infrastructure to withstand these disasters [6]. With the expected increase in likelihood of more intense disasters, losses in the aftermath of any disaster are likely to increase as well. In order to minimize adverse effects of disasters, recent studies have highlighted the need for integrating resiliency into design of critical infrastructure [7,8].

Resiliency is a multidimensional concept that was introduced by Holling to describe ecological systems and since then been adopted by several engineering disciplines [9]. For instance, resiliency in structural engineering is defined by the ability of a structure to maintain acceptable levels of functionality during and after breakout of a disaster (see Fig. 1). Resilient structures, due to their superior performance, can perform satisfactory before undergoing high level of damage and may able to withstand severe conditions (without triggering progressive collapse). This facilitates evacuation of occupants and provides first responders with enough time to tackle the adverse effects of disaster.

In current practice, structural resilience can be achieved through

* Corresponding author.
E-mail addresses: nasermoh@msu.edu (M.Z. Naser), kodur@egr.msu.edu (V.K.R. Kodur).
[1] Post-doctoral Research Fellow, Civil and Environmental Engineering, Michigan State University.
[2] University Distinguished Professor and Chairperson, Civil and Environmental Engineering, Michigan State University.

https://doi.org/10.1016/j.autcon.2018.03.004
Received 31 August 2017; Received in revised form 12 February 2018; Accepted 1 March 2018

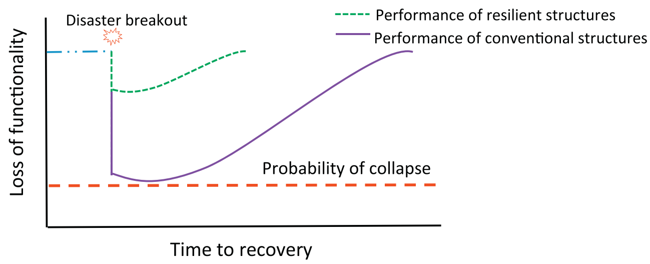

Fig. 1. Concept of resiliency during a disruptive event.

number of design strategies such as applying proper detailing to ensure ductile response in seismically active areas, installing adequate fire protection measures in buildings to enhance fire safety etc. Implementation of such strategies can meet resiliency requirements and can enhance performance under low-to-medium sized disasters. However, these conventional strategies may not be sufficient to achieve satisfying performance under extreme loading events (resulting from earthquake, blast, fire) or a combination of loading events (ex: impact followed by fire or tsunami followed by earthquake) as seen during the collapse of WTC twin towers, Fukushima Daiichi nuclear accident etc. [10,11]. Further, due to unique characteristics (i.e. structural system, service requirement, environmental exposure etc.) in some critical infrastructure such as bridges and tunnels, implementation of conventional systems may not be practical nor economical [3,12]. Thus, in order to achieve high level of resiliency, designers are encouraged to seek other innovative and effective solutions that can complement currently used conventional strategies.

The recent technological advancements in sensing and communication technologies, such as RFID (Radio Frequency IDentification) and WSAN (Wireless Sensor and Actor Networks), that enabled development of "Internet of Things" (IoT) can also be utilized to monitor structural performance under extreme disaster events. IoT technology provides a global platform to collect and exchange data between sensing devices, physical objects, and environment. Unfortunately, most of the research-to-date with regard to IoT has focused on developing advanced sensing devices [13], communication systems [14], and processing technologies [15] that enable integration of IoT into micro applications i.e. computing services etc., whilst the implementation of IoT into large-scale applications such as monitoring of infrastructure, from structural point of view, is still not fully explored yet [16,17].

This paper hypothesizes that an intelligent adoption of IoT technology can institute a platform to enable more resilient design of new and existing critical infrastructure. Unlike conventional health monitoring systems, which are limited in application and targets passively monitoring conventional factors i.e. carbon emission, corrosion in reinforcement etc., a cognitive design is dynamic in nature with the ability to continually assess "in real time" structural response of infrastructure taking into account baseline and dynamic conditions of users (i.e. occupants, first responders behavior), infrastructure (system-level structural behavior), and environment (severity of disaster) all of which continuously interact in a typical built environment. Based on such assessment, cognitive infrastructure can estimate magnitude of damage, predict signs of imminent collapse, and notify occupants and first responders with locations (zones) of high damage etc. Further, cognitive structures can be tailored to perform series of pro-active actions i.e. shut down fire doors to prevent fire spread, scan facilities for trapped users, direct evacuee to safest/quickest egress paths etc. as to improve structural resilience, facilitate orderly evacuation, and aid disaster response operations. The applicability of the proposed concept is illustrated through two case studies.

2. History, evolution, and limitations of Internet of Things (IoT)

The "Internet of Things" (IoT), was popularized through the work carried out at the Auto-ID Center at the Massachusetts Institute of Technology (MIT), which started to design radio frequency identification (RFID) infrastructure [18]. IoT is described as a self-configured dynamic global network with interoperable communication protocols between physical and virtual "things" [18]. The concept of "things" in a typical IoT network refers to any real or virtual participating actors such as human beings, objects, data etc. Since IoT provides the ability for real-time monitoring of any tagged actor within an environment, IoT is often used to create an environment in which the basic information from any of its actors can be efficiently shared with others.

Hence, IoT possesses the ability to provide comprehensive data about the surrounding environment by tracing its users and/or other objects through number of technologies, such as RFID sensor networks, Global Positioning System (GPS), or infrared sensor detection etc. Over the past few years, IoT has been applied in limited disaster mitigation applications; for example, Zambrano et al. [18] applied Sensor Web Enablement Framework (SWE) and Message Queue Telemetry Transport (MQTT) to develop an early warning system. This framework collects data through wireless IoT communication platform, i.e. smartphones, to anticipate outbreak of an earthquake. In a recent study, Zelenkauskaite et al. [19] proposed a network-based framework of IoT for disaster management using social network analysis. The developed framework, which dynamically links objects, uses a combination of graph theory and social networking tools to analyze collected data. Although the developed framework was only tailored towards the use of social media networks to aid in crisis management, this framework can also be applicable in other IoT enabled smart environments. Similar platforms have been proposed in other applications such as transportation [20], marketing [21], logistics [22] etc.

Although findings from few recent applications have been promising, it is generally accepted that IoT technologies and applications are still in their infancy [23] as these technologies are facing number of challenges in real life applications, specifically under extreme disaster-type events. For example, most of the proposed frameworks relies on internet as a medium to collect, analyze and transfer data. As a result, successful implementation of IoT is tied to the availability of the internet which may not be accessible during extreme disaster conditions as in fire (collapse of twin towers on 9/11), earthquake (failure of oversea cables breakage during Japan earthquake in 2011), severe snow storms (failure of the internet infrastructure in Italy blackout in 2003).

Vermesan et al. [24] stated that some of the major limitations of realizing IoT technology potential relates to lack of Service oriented Architecture (SoA), scalability and associated high cost. Other limitations such as reliability of context awareness, inter-machine communication, integration of memory and processing power, and the ability to withstand harsh environments were also highlighted. According to Vermesan et al. [24], availability of low-power consumption wireless sensors, low cost object monitoring and networking, are fundamental for successful integration of IoT in large scale infrastructure. In a separate study, Hu et al. discussed number of challenges associated with applicability of IoT technology to civil infrastructure (i.e. bridges) [23]. Some of these challenges include data transfer, processing, and management as well as complexity in developing efficient wireless sensor networks, data transmission for long distances and limited transmission band width. Hu et al. noted that data processing and identification, in terms of automated detection of localized damage out of the large amount of collected data on a daily basis, are other key challenges to integrating IoT technology in large structures.

Issues related to energy storage, especially those associated with integrating IoT for large infrastructure applications, has become a key obstacle. Current technologies such as Wireless Sensor Networks and Active RFID suffer from bulky battery packaging and short life times, and hence require recharging or replacement of the integrated batteries. Lack of available and reliable hardware systems such as data acquisition and synchronization, compatibility between sensors and