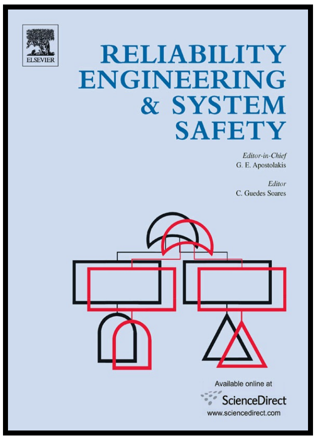

www.elsevier.com/locate/ress

A Quantitative Method For Assessing Resilience of Interdependent Infrastructures

Cen Nan, Giovanni Sansavini

PII: S0951-8320(16)30374-X
DOI: http://dx.doi.org/10.1016/j.ress.2016.08.013
Reference: RESS5624

To appear in: *Reliability Engineering and System Safety*

Received date: 19 January 2015
Revised date: 17 June 2015
Accepted date: 15 August 2016

Cite this article as: Cen Nan and Giovanni Sansavini, A Quantitative Method Fo Assessing Resilience of Interdependent Infrastructures, *Reliability Engineerin and System Safety,* http://dx.doi.org/10.1016/j.ress.2016.08.013

A Quantitative Method For Assessing Resilience of Interdependent Infrastructures

Cen Nan, Giovanni Sansavini*
Reliability and Risk Engineering Lab, ETH Zürich, Zürich, Switzerland
*Corresponding author. Tel.: (41) 44 632 50 38. sansavig@ethz.ch

Abstract

The importance of understanding system resilience and identifying ways to enhance it, especially for interdependent infrastructures our daily life depends on, has been recognized not only by academics, but also by the corporate and public sectors. During recent years, several methods and frameworks have been proposed and developed to explore applicable techniques to assess and analyze system resilience in a comprehensive way. However, they are often tailored to specific disruptive hazards/events, or fail to properly include all the phases such as absorption, adaptation, and recovery. In this paper, a quantitative method for the assessment of the system resilience is proposed. The method consists of two components: an integrated metric for system resilience quantification and a hybrid modeling approach for representing the failure behavior of infrastructure systems. The feasibility and applicability of the proposed method are tested using an electric power supply system as the exemplary infrastructure. The results highlight that the method proves effective in designing, engineering and improving the resilience of infrastructures. Finally, the analysis of system resilience is proposed as a proxy to quantify the coupling strength between interdependent infrastructures.

Abbreviations

ABM, Agent Based Modeling; **ASSAI,** Average Substation Service Availability Index; **CI,** Critical Infrastructure; **CNT,** Complex Network Theory; **CPC,** Common Performance Condition; **CREAM,** Cognitive Reliability Error Analysis Method; **CU,** Communication Unit; **CV,** Coefficient Variation; **ENS,** Energy Not Served; **EPSS,** Electric Power Supply System; **FCD,** Field level Control Device; **FID,** Field level Instrumentation Device; **FIS,** Fuzzy Inference System; **GR,** General Resilience; **HEP,** Human Error Probability; **HLA,** High Level Architecture; **HOL,** Human Operator Level; **HRA,** Human Reliability Analysis; **ICT,** Information and Communication Technology; **IIM,** Input-output Inoperability Modeling; **LAN,** Local Area Network; **MMI,** Man-made Machine Interface; **MOP,** Measurement of Performance; **MTTR,** Mean Time To Repair; **MTU,** Master Terminal Unit; **OCS,** Operational Control System; **PL,** Performance Loss; **PN,** Petri-Net; **R,** Robustness; **RA,** Recovery Ability; **RAPI,** Rapidity; **RBC,** RTU Battery Capacity; **RL,** Resilience Loss; **RTU,** Remote Terminal Unit; **RTI,** Run Time Infrastructure; **SCADA,** Supervisory Control and Data Acquisition; **SD,** System Dynamic; **SoS,** System of Systems; **SUC,** System Under Control; **TAPL,** Time Averaged Performance Loss

Keywords: Interdependent Critical Infrastructure, Resilience, Reliability, Agent-based Modeling, Interdependency

I. INTRODUCTION

A. Critical Infrastructures and Resilience

The welfare and security of each nation rely on a continuous flow of essential goods (such as energy, food, water) and services (such as banking, health care, public administration) provided by a set of systems called critical infrastructures (CI). Their incapacity or destruction would have a debilitating impact on the health, safety, security, economics and social well-being [1, 2]. They have always been "complicated", but in recent years, they have witnessed higher integration and growing interconnectedness, which have turned them into a complex "System-of-Systems" (SoS) [3]. Interdependent infrastructures can correspond to one infrastructure (*internal interdependency*) or more infrastructures (*external interdependency*). In [4], interdependency is characterized as different types: *physical*, *geospatial*, *informational*, *logical* [4]. These interdependencies may provide the tolerance to attacks and failures if well managed (positive impact). For instance, technical failures such as abnormal disconnection of a transmission line can be detected by remotely installed devices at a substation and corresponding alarms can be transmitted to a control center via services provided by coupled telecommunication systems in order to prevent further failure propagations. However, these interdependencies might also be a source of threat generating risks, e.g., the risk of cascading failures, which make infrastructures more vulnerable (negative impact). In power blackout events, service disruptions further propagate to other infrastructures (transportation, telecommunication and water supply) and worsen the overall negative impacts [5]. Even though not preventable, these damages may be minimized, if the capabilities of both direct and indirect affected infrastructures are strengthened and effects of interdependencies are recognized [6-8]. Engineering the coupling among infrastructures, e.g., loosening it by adding buffer capacity, "slack" resources, redundancy or structure modularity, has been suggested in order to decrease the impact of interdependency [9]. It is important to understand if interdependencies are essential, e.g. the dependency of power grids on the control system, or "parasitic", e.g. the dependency of the control system on the controlled grid. The latter can be removed or redesigned. Moreover, the human/social element is recognized to play a key role in the operations of infrastructures.

To better understand the performance of infrastructures, especially their behavior during and after the occurrence of disturbances (e.g., natural hazards or technical failures), resilience analysis [10-14] has grown as a proactive approach to enhance the ability of infrastructures to prevent damage before disturbance events, mitigate losses during the events and improve