Engineering Structures 59 (2014) 411–433

Contents lists available at ScienceDirect

Engineering Structures

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

# Goal Tree Success Tree–Dynamic Master Logic Diagram and Monte Carlo simulation for the safety and resilience assessment of a multistate system of systems

E. Ferrario [a], E. Zio [a,b,*]

[a] Systems Science and the Energetic Challenge, European Foundation for New Energy, Electricité de France at École Centrale Paris, Supelec, France
[b] Department of Energy, Politecnico di Milano, Italy

ARTICLE INFO

*Article history:*
Received 21 June 2013
Revised 21 October 2013
Accepted 4 November 2013
Available online 10 December 2013

*Keywords:*
Physical resilience
Multistate model
System of systems
Goal Tree Success Tree–Dynamic Master Logic Diagram
Monte Carlo simulation
Seismic Probabilistic Risk Assessment

ABSTRACT

We extend a system-of-systems framework previously proposed by the authors to evaluate the safety and physical resilience of a critical plant exposed to risk of external events. The extension is based on a multistate representation of the different degrees of damage of the individual components and the different degrees of safety of the critical plant. We resort to a hierarchical model representation by Goal Tree Success Tree–Dynamic Master Logic Diagram (GTST–DMLD), adapting it to the framework of analysis proposed. We perform the quantitative evaluation of the model by Monte Carlo simulation. To the best of the author's knowledge this is the first time that a multistate framework of combined safety and resilience analysis relating the structural and functional behaviour of the components to the system function in a GTST–DMLD logic modelling of a system of systems is adopted in Seismic Probabilistic Risk Assessment. To illustrate the approach, we adopt a case study that considers the impacts produced by an earthquake and its aftershocks (the external events) on a nuclear power plant (the critical plant) embedded in the connected power and water distribution, and transportation networks which support its operation.


## 1. Introduction

Resilience is the capacity of a system to survive to aggressions and shocks by changing its non-essential attributes and rebuilding itself [1]; it includes technical, organizational, social and economic facets [2]. In this work, we consider the "physical" resilience of a critical plant exposed to risk of an external event. We limit the analysis to the capacity of recovering from an external aggression or shock, using as representative quantity the recovery time, i.e., the period necessary to restore a desired level of functionality of a system after the shock [2]. For the resistance to the shock and the recovery from the shock, the critical plant is provided with internal emergency devices (internal barriers) to keep it in, or restore it to, a safe state when the main inputs devoted to this purpose fail. Since the internal emergency devices can fail too, we extend the boundaries of the study to the infrastructure systems (external supports) in which the plant is embedded, which also may or may not be left in the conditions to maintain the safety of the plant after the occurrence of a disruptive event. Supporting elements (e.g., roads for access to the sites struck by the disruptive external event) are also considered for the recovery of the failed components of the main inputs, internal barriers and external supports. We adopt the system-of-systems framework of analysis proposed by the authors in [3] and extend it to a multistate representation where different degrees of damage of the individual components are contemplated [2,4,5]. In particular, we consider an original multistate model of structural damage and functional performance at component level, that integrates into a multistate model of safety at system level for well-being analysis [6].

The modelling of the system of systems includes: (i) the connections among the main inputs, (ii) the links among the internal barriers, (iii) the dependencies among the external supports, (iv) the interdependencies between the systems in (i–iii), and the relationships among systems in (i–iii) and the recovery supporting elements. We propose a hierarchical model representation by Goal Tree Success Tree–Dynamic Master Logic Diagram (GTST–DMLD) [7]. This provides an efficient and clear description of the system-of-systems complexity through different hierarchical levels of system goals and functions, by the GT, and objects and parts, by the ST. The interrelationships are represented in a DMLD that translates into a dependency matrix and redefined logic gates, e.g., "AND" and "OR", that assume a different meaning with respect to a binary state model, e.g., Fault Tree [7]. We extend the GTST–DMLD representation adapting it to the framework of analysis proposed. To the best of the author's knowledge this is the first

* Corresponding author at: Department of Energy, Politecnico di Milano, Italy. Tel.: +39 02 23996340.
*E-mail addresses:* elisa.ferrario@ecp.fr (E. Ferrario), enrico.zio@ecp.fr, enrico.zio@supelec.fr, enrico.zio@polimi.it (E. Zio).

0141-0296/$ - see front matter © 2013 Elsevier Ltd. All rights reserved.
http://dx.doi.org/10.1016/j.engstruct.2013.11.001

time that a multistate framework of combined safety and resilience analysis relating the structural and functional behaviour of the components to the system function in a GTST–DMLD logic modelling of a system of systems is adopted in Seismic Probabilistic Risk Assessment (SPRA). We use Monte Carlo simulation [8–10] for the probabilistic evaluation of such system of systems considering multiple levels of safety of the critical plant and physical resilience, measured in terms of the time needed to restore the different levels of safety.

To illustrate the approach, we adopt a simplified case study that considers a nuclear power plant (the critical plant) exposed to the risk of an earthquake and its subsequent aftershocks (the external events). The plant is provided with proper internal emergency devices (internal barriers), and embedded in the connected power and water distribution (external supports), and transportation networks (recovery supporting elements) which support its operation and provide resilience to it.

The reminder of the paper is organized as follows. In Section 2, the multistate model for the safety assessment of a critical plant in a system-of-systems framework is presented; in Section 3, the Goal Tree Success Tree–Dynamic Master Logic Diagram and Monte Carlo simulation are described in relation to Seismic Probabilistic Risk Assessment and within the multistate system-of-systems framework; in Section 4, the case study and the results of the analysis are presented; in Section 5, conclusions are provided. Finally, in Appendix A, an exemplification of qualities, parts and GTST–DMLD within a system-of-systems framework is showed with respect to Sections 2 and 3; in Appendix B, the basic concepts of a Seismic Probabilistic Risk Assessment are introduced, to provide the reference elements needed for the case study; in Appendix C, details of the operative steps of the GTST–DMLD and Monte Carlo simulation for Seismic Probabilistic Risk Assessment are given.

## 2. Multistate model for the safety assessment of a critical plant within a system-of-systems framework

In Section 2.1, the system-of-systems framework is illustrated with reference to three levels of safety and distinguishing its goal and functions, i.e., its qualities, and its objects, i.e., its parts; in Section 2.2, a multistate model for the system of systems is introduced.

### 2.1. System-of-systems framework: safety, qualities and parts

When due to an accident the main inputs to a critical plant stop, safety is assured by internal barriers which provide the inputs in the amount necessary for the safety conditions. These barriers are designed to withstand postulated accidents (design basis accidents) and include multiple, independent and redundant layers of defense to compensate for potential human and mechanical failures (defense in depth) [11]. As mentioned in the Introduction (Section 1), we adopt a system-of-systems view [3] extending the analysis to the external supports for emergency management actions and additional, redundant infrastructure systems to provide the safety-required inputs in case of failure of both the main inputs and the first (internal) barriers. In all generality, we consider also recovery supporting elements, as physical components (e.g., roads for access to the site) and organizational elements (e.g., technical competence of operators), that provide help in the recovery of the internal and external safety systems. On the basis of this system-of-systems framework, we can identify three levels of safety distinguishing the internal barriers (first level), the external supports (second level) and the recovery supporting elements (third level), as illustrated in Fig. 1.

In the present work, for the sake of simplicity, emergency management and organizational supporting elements are not considered. The concept of resilience is limited to the physical characteristics of the components and systems: then, we refer to physical resilience as the underlying concept. On the other hand, the Goal Tree Success Tree–Dynamic Master Logic Diagram (GTST–DMLD) illustrated in Section 3 can accommodate elements of fuzzy logic theory to describe imprecisely known characteristics and logic relations of non-physical facets by linguistic fuzzy terms [7]. For example, specific inputs like the level of experience of the operators can have an impact on the degree of safety of the critical plant in emergency condition: these inputs could be described in the GTST–DMLD by including threshold values [7]. This kind of considerations will be subject of further development in the future research.

In the framework under analysis, we can distinguish between qualities and parts. The former are referred to the goals and functions, i.e., the objectives, of the system of systems; the latter are related to the objects, i.e., the physical elements, that interact with each other to attain the objectives.

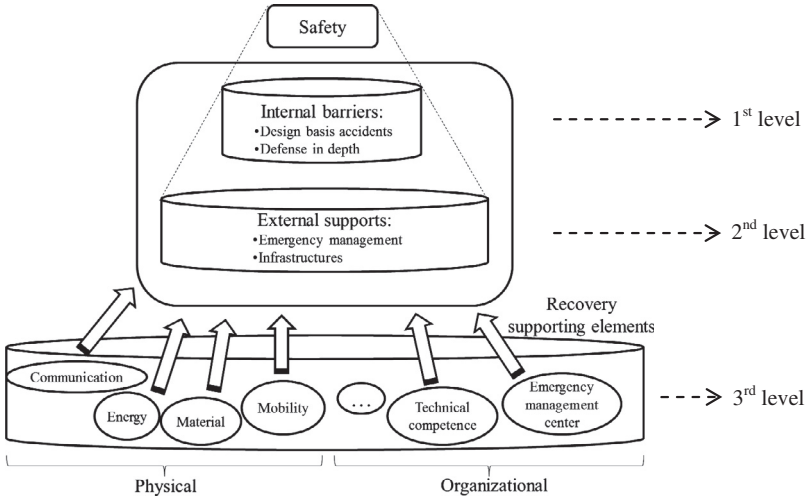


**Fig. 1.** Safety levels of a system-of-systems framework considering a critical plant in emergency conditions. The first level (top) considers internal barriers; the second one (middle) extends to the external supports; the third one (bottom) accounts for the elements supporting the recovery.