Reliability Engineering and System Safety 167 (2017) 198–217

Contents lists available at ScienceDirect

Reliability Engineering and System Safety

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

Preliminary interdependency analysis: An approach to support critical-infrastructure risk-assessment

Robin E. Bloomfield[a,b], Peter Popov[a], Kizito Salako[a,*], Vladimir Stankovic[a], David Wright[a]

[a] The Centre for Software Reliability, City, University of London, EC1V 0HB, London, UK
[b] Adelard LLP, 24 Waterside, 44-48 Wharf Road, London N1 7UX, London, UK

ARTICLE INFO

Keywords:
Interdependency analysis
Risk assessment
Cascading failure
Critical infrastructure resilience

ABSTRACT

We present a methodology, *Preliminary Interdependency Analysis* (PIA), for analysing interdependencies between critical infrastructure (CI). Consisting of two phases – qualitative analysis followed by quantitative analysis – an application of PIA progresses from a relatively quick elicitation of CI-interdependencies to the building of representative CI models, and the subsequent estimation of *any* resilience, risk or criticality measures an assessor might be interested in. By design, stages in the methodology are both flexible and iterative, resulting in interacting CI models that are scalable and may vary significantly in complexity and fidelity, depending on the needs and requirements of an assessor. For model parameterisation, one relies on a combination of field data, sensitivity analysis and expert judgement. Facilitated by dedicated software tool support, we illustrate PIA by applying it to a complex case-study of interacting Power (distribution and transmission) and Telecommunications networks in the Rome area. A number of studies are carried out, including: 1) an investigation of how "strength of dependence" between the CIs' components affects various measures of risk and uncertainty, 2) for resource allocation, an exploration of different, but related, notions of CI component importance, and 3) highlighting the impact of model fidelity on the estimated risk of cascades.

1. Introduction

It is recognised that one of the challenges in enhancing the protection of *Critical Infrastructures*[1] (CIs) against accidents, natural disasters, and acts of terrorism (including cyber terrorism) is establishing and maintaining an understanding of the interdependencies between infrastructures. Governmental agencies responsible for protecting national critical infrastructure need methods and tools to assess risks (including those related to interdependencies) and evaluate the alternatives available for mitigating these. The owners and operators of critical infrastructure need to know the likely impact, on their services, of disruptions from other infrastructures, so they can develop mitigations (e.g. in their emergency planning) and make considered investments in *resilience* [1].

Once one recognises the importance – in terms of risks – of interdependencies between critical infrastructures, one is then faced with the feasibility and cost of a risk-assessment [2–5], since critical infrastructures are typically large and very complex systems. Model-based risk-assessment can offer a feasible and cost-effective assessment approach for an assessor, *if* the assessor can gain enough confidence that her models are representative of the system's behaviour, capturing what she judges to be essential interdependencies. Faced with numerous choices about model structure, fidelity and parameters, our assessor can gain confidence in a model by a succession of model *refinements*, each refinement resulting from verifying and validating an earlier version of a model and making judgements about what changes to the model are needed for an improvement while, at the same time, *not* putting in more detail than she judges to be necessary for her needs. So, for instance, if an assessor has certain *risk-measures*[2] in mind (e.g. the distribution of loss in network-connectivity resulting from component failure or the distribution of loss in supplied electrical power due to line-outages in a snow storm) which, to be computed, require the model to explicitly have dynamics of a certain kind (e.g. packet-routing algorithms or electrical power flow models), then these dynamics will need to be incorporated in a revision of the model.

Clearly, with so many choices to make, the task of model building and refinement can be a daunting one, with serious ramifications for the

[2] In this paper, for ease of presentation and without-loss-of-generality, a *risk-measure* is a probability distribution of unwanted events arising from random changes in a CI's state.

* Corresponding author.
E-mail addresses: reb@csr.city.ac.uk, reb@adelard.com (R.E. Bloomfield), ptp@csr.city.ac.uk (P. Popov), k.o.salako@city.ac.uk (K. Salako), Vladimir.Stankovic.1@city.ac.uk (V. Stankovic), d.r.wright@city.ac.uk (D. Wright).

[1] As defined by the U.S. Department of Homeland security (see https://www.dhs.gov/what-critical-infrastructure).

http://dx.doi.org/10.1016/j.ress.2017.05.030
Received 8 July 2015; Received in revised form 21 March 2017; Accepted 18 May 2017
Available online 22 May 2017

risk-assessment to be carried out. Any methodology/tools which support an assessor in this endeavour should afford the assessor the flexibility to (1) create models at any desired level of abstraction, (2) alter/add/remove stochastic and deterministic processes, and (3) define any risk-measure of interest. To this end, we propose *Preliminary Interdependency Analysis* (PIA) – a systematic method to support building, refining and analysing models of interdependent *Large Complex Critical Infrastructures* (LCCI). PIA starts off at a high-level of abstraction, supporting a cyclic, systematic thought process, directed towards identifying dependencies between components of CIs. Eventually, (hybrid) probabilistic models are deployed, once they have been judged to be appropriate for risk-assessment; these are used to conduct studies focussed on computing different measures of interests, e.g. the likelihood of cascade failure under a given set of assumptions, or the identification of the weakest link in the modelled system. And, if modelling with even greater detail is required, PIA can assist in this process too, e.g. by adding models of the consequences of LCCI operator actions, or by introducing various constraints on such actions, such as limiting the maintenance resources available in the case of a major disaster, or adding deterministic models specific to a particular LCCI (e.g. power flows for power systems).

The PIA method is applicable as both:

1. a lightweight method used to provide an initial identification of interdependencies and to scope the options for more detailed studies. The approach should be accessible to a range of stakeholders, particularly *Small-to-Medium Enterprises* (SMEs) in support of their business continuity planning
2. a more heavyweight method of studying, with an increasing level of detail, complex regional and nationwide CIs by combining probabilistic and deterministic models of the CIs.

There are numerous studies about CI interdependencies, including some which rely on complex dynamic models. As pointed out in a recent survey [6] summarising research on interdependencies in power systems for the last 5 years, many studies analyse interdependencies without detailing *how* these interdependencies were identified in the first place, giving the impression that the interdependencies are *all known* to the analyst. Systematic methods which can be followed to identify interdependencies are lacking in the literature. The authors of the survey, therefore, recommend that methods for interdependency identification be given high priority. We agree, and PIA provides significant support in this direction.

We illustrate the use of PIA on a realistic case study: a regional system of two CIs, namely the power grid and the telecommunication network around Rome, Italy (i.e. Rome case-study). In the study, we used a set of tools – the PIA Toolkit – which consists of two software applications we developed:

- Using the PIA Designer, a modeller can construct and parameterize a visual representation of interdependent CIs. The PIA Designer converts this visual model into a probabilistic model ready to be solved via Monte Carlo simulation. The Designer uses third party proprietary software called ASCE [7].
- The Execution Engine allows for Monte Carlo simulation using models created with the PIA Designer. The Execution engine uses Möbius [8], which we customised extensively to 1) allow for various forms of dependencies between the modelled elements, and 2) for integration of third party software in simulation (e.g. various deterministic flow models, typically used with the CIs).

The rest of the paper is organised as follows. Section 2 presents related research, while an overview of the PIA method – both its qualitative and quantitative aspects – is given in Section 3. Section 4 details the mathematical family of models underlying quantitative PIA, including models of interdependent CIs and their dependent constituent components. In Section 5 we describe the case study used to illustrate our approach. This is followed by a presentation of results obtained, and a discussion of their plausibility, in Section 6. In Section 7, we discuss our findings, and open issues for future research, while finally concluding the paper in Section 8. Appendix A contains a detailed illustration of model development over various stages of PIA, using PIAs tool support in the aforementioned case-study.

2. Related research

The authoritative paper by Rinaldi et al. [9] established interdependency related terminology and concentrates on high level dependencies between infrastructures. It was noticed, however, that such an approach, although useful at a conceptual level, is inappropriate for risk quantification as further elaboration is needed. Many authors, including ourselves, have since argued in favour of service-level models of a different flavour.

An overview of CI interdependency research is provided in our earlier study on interdependencies for UK agencies [10,11]. A more recent survey is [12], in which a number of modelling and simulation approaches are grouped into six categories: 1) Empirical, 2) Agent-based, 3) Economic-based, 4) Complex-Network based, 5) System-dynamics based and 6) “Others”, which covers all approaches not included in the previous categories. According to this classification, our work belongs to the “Others” category, partly because our work incorporates approaches from more than one category. We compare these approaches to PIA below.

PIA allows one to estimate risk using alternative, consistent models, thereby allowing risk-measures resulting from these models to be directly compared. We see this capability as a useful step in addressing the research gap identified at the end of section 4.1.2 in [12]. As an empirical modelling approach, PIA can be used for 1) identification of frequent and significant failure patterns, as well as 2) quantification of any risk-measures chosen by an assessor.

Agent-based models, consisting of dynamically interacting rule-based agents, are based on the idea that complex behaviour or phenomena emerge from many individual and relatively simple interactions of autonomous agents [13–15]. In terms of emergent model properties, there are similarities between PIA and agent-based modelling approaches. The deterministic rules that govern the behaviour of agents can be modelled in PIA as well, as the deterministic responses of components to a system’s random changes in time. But, PIA extends this concept by introducing *stochastic associations*, which define deterministic rules governing *how* the uncertainty in the model depends upon the state of the system and its components.

In contrast with the “bottom-up” approach of Agent-based models, *System-dynamics* approaches take a “top-down” view [16–18] by focusing on the nonlinear behaviour of systems over time, using *stocks* and *flows*, internal *feedback loops* and time delays. This nonlinear behaviour is typically characterised by a set of differential equations capturing the behaviour of systems with *fixed network topologies* – some see this as a significant limitation [12]. PIA is fully compatible with these techniques, but in addition allows an assessor to analyse a system with uncertainty in network topology.

The quantitative analysis of risk typically requires the evolution of a CIs state be modelled as a stochastic process; the process is defined by a collection of joint probability distributions over a very large state-space. While, to some extent, there exist tools and formalisms to aid an assessor with this, such as PRISM [19–21], difficulties can arise if 1) the state-space is exceedingly large (e.g. too large to explicitly fit in computer memory), making infeasible the solution of such problems using transition-rate matrices, 2) the inter-event times for the process have no known mathematical closed-form. However, PIA, by using a combination of stochastic associations, deterministic state-transitions and the competing-risks algorithm [22,23], affords a user the ability to both specify sophisticated joint distributions and simulate the resulting process. These resulting processes are *hybrids* of semi-Markov processes and embedded deterministic state-transitions. Furthermore, *any* inter-event