Technol Econ Smart Grids Sustain Energy (2016) 1: 14
DOI 10.1007/s40866-016-0013-2

ORIGINAL PAPER

A Criticality-based Approach for the Analysis of Smart Grids

Polinpapilinho F. Katina[1] · Charles B. Keating[1] · Enrico Zio[2] · Adrian V. Gheorghe[1]

Received: 22 February 2016 / Accepted: 30 September 2016 / Published online: 19 October 2016

Abstract Smart Grids offer higher level capabilities intended to meet current and future energy demands. These demands include improved performance related to concepts of reliability, resiliency, environmentally friendly generation, transmission, and distribution as well as turning consumers into prosumers. This study focused on two primary objectives: (1) to understand how the concept of risk is currently being addressed in Smart Grids, and (2) to suggest a more holistic view of risk for Smart Grids. Pertinent literature on Smart Grids was collected and synthesized for the concept of risk which indicated the prevalence of two factors, probability and consequence, as the main factors for Smart Grid risk quantification. However, it was discovered that current literature appears to focus on risk within the different domains of Smart Grids (i.e., generation, transmission, distribution, customer, service provide, operations, markets) without consideration Smart Grids as an integrated whole. A criticality-based approach (CBA) is proposed and then used as the basis for development of an extended listing of measures, including dependency, interdependency, and resiliency, as well as accepted risk factors (i.e., probability and consequence). This confluence of factors can be utilized in a holistic Smart Grid analysis. Implications for CBA and future research directions for realizing enhanced Smart Grid capabilities are provided.

Keywords Critical infrastructure · Criticality-based approach · Operating landscape · Risk formulation · Smart Grid

Introduction

There is wide recognition that modern society depends on goods and services provided by a set of complex systems typically referred to as *critical infrastructures*. These systems are often referred to as *critical* since they are essential for maintaining and sustaining public well-being, safety, and economic prosperity [26, 42, 55, 73]. The domain of critical infrastructures revolves around chemicals, commercial facilities, communications, critical manufacturing, dams, defense industrial bases, emergency services, energy, financial, services, food and agriculture, government facilities, healthcare and public health, information technology, nuclear reactors, materials, and waste water systems [67]. Lately, there is increasing interest in the energy sector with respect to the critical importance of *Smart Grids* as a critical infrastructure [11, 15, 54, 57, 72, 75]. Arguably, Smart Grids, similar to all critical infrastructures, operate under conditions of uncertainty with respect to natural events such as earthquakes and hurricanes as well as

✉ Polinpapilinho F. Katina
pkatina@odu.edu

Charles B. Keating
ckeating@odu.edu

Enrico Zio
enrico.zio@polimi.it

Adrian V. Gheorghe
agheorgh@odu.edu

1 National Centers for System of Systems Engineering, Department of Engineering Management & Systems Engineering, Old Dominion University, 2101 Engineering Systems Bld., Norfolk, VA 23529, USA

2 Energy Department, Nuclear Division, Laboratory of Signal Analysis and Risk Analysis, Politecnico di Milano, Via Ponzio 34/3 20133, Milano, Italy

man-made events such as acts of sabotage and cyber-threats [42, 80, 86, 92]. Moreover, Smart Grids must be designed, operate, and evolve in a difficult context. This context is marked by elements of: (1) ambiguity associated with an increasing lack of clarity and situational understanding, complexity *associated* with large numbers of richly and dynamically interacting systems and subsystems with behavior difficult to predict, (2) *emergence* with respect to the inability to deduce behavior, structure, or performance from constituent elements, and (3) *interdependency* associated with mutual influence among different complex systems through which the state of a system influences, and is influenced by, the state of other interconnected systems [12, 51].

Against this backdrop, current research tends to focus on the potential benefits of Smart Grids [23] as well as issues and risks in implementation such as new cyber-threats and vulnerabilities [7, 13, 14, 36, 37]. Moreover, and perhaps due to the nascent nature of this topic, researchers are still *debating* the definitions of Smart Grids [21, 40, 70, 78] as well as focusing on particular aspects and parts/elements of Smart Grids, including design for next-generation control centers [91], optimizing distributed power systems [75] effects of plug-in-hybrid-electric vehicles [33], security issues [4, 6, 8, 62, 64], Smart Meters [90], standards and best practices [32, 87], and classification of threats [4, 15, 54] among others. However, there is still a scarcity of literature discussing quantitative methods that could be used in support of risk quantification for Smart Grids.

The idea of risk quantification for Smart Grids is not new. Concepts of *probability* of occurrence of an event and its *consequences* have been adapted for Smart Grids [11, 32, 40, 57–59, 62, 72, 90]. However, adapting traditional risk formulation without accounting for other relevant measures is limiting in analyzing Smart Grids. Moreover, current literature could be considered atomistic since there is a tendency to focus on specific elements such as smart metering systems and integration of distributed power generation of the Smart Grid, without consideration of Smart Grids as a totality. Thus, there is a gap in the literature for developing more robust formulations of risk related to more holistic considerations for integrated Smart Grid systems. This research attempts to address this gap by exploring a robust set of measures (and their properties) that could be used for more holistic examination of Smart Grids. *The purpose of this paper is to propose and develop an alternative framework that could be used to explore the 'criticality' of Smart Grids.* For purposes of this research, the term criticality is related to the importance of a Smart Grid to public well-being.

The paper is organized around three primary development thrusts to support the purpose of the research. First, we describe Smart Grids in terms of the present domain and major characteristics that delineate the domain. The aim of this section is to articulate the complexities involved in developing, implementing, and evolving Smart Grids. Special emphasis is placed on the more holistic view of Smart Grids as an integrated system that includes technologies, information (availability, accessibility, utility), human and social influences, organizational and managerial supporting arrangements, and political (policy) constraints as well as facilitation considerations. Second, the concept of risk is explored. Specifically, the literature is reviewed with respect to risk and factors commonly used in current quantification efforts related to risk for Smart Grids. Third, we provide a preliminary extended set of measures that could be used in addressing criticality of Smart Grids. This set of measures and their properties is developed by contrasting current factors with previous research of criticality-based measures. This research concludes with proposed future research directions based on the current investigation implications.

Smart Grid Characteristics and Landscape

The topic of Smart Grid is relatively new and as such there is no one widely accepted definition [40, 70]. Thus, it is necessary to explore the concept of Smart Grid to develop a foundational perspective before delving into the concept of risk for Smart Grids. At a fundamental level, a Smart Grid can be considered "an upgrade to the current electrical power grid" ([8], p. 24). Consequently, a Smart Grid is expected to meet current needs while offering significantly higher capabilities that are intended to meet ever changing societal demands of the 21st century and beyond [54]. These social demands are highlighted by the need for reliable, resilient, scalable, manageable, and environmentally friendly energy generation, transmission, and distribution systems that also embody concepts of interoperability, cost effectiveness, and intelligence [6, 23, 31, 54]. Unfortunately, there is no one consistent perspective of what a Smart Grid entails. Table 1 is provided to illustrate the varying representative perspectives of Smart Grids.

Although, there is no one accepted perspective of Smart Grids, the selected set of perspectives begins to offer insight into essential aspects, components and characteristics of Smart Grids. A common theme of transforming the structure of electrical energy generation, delivery and consumption with an increasing emphasis on information and technology and interests of the consumer, appear to be driving the evolving paradigm of Smart Grids. The Institute of Electrical and Electronics Engineers (IEEE) definition, "integration of power, communications, and information technologies for an improved electric power infrastructure serving loads while providing for an ongoing evolution of end-use applications" ([38], p. 3), appears to capture most

Table 1 A representative set of perspectives on smart grids

Author(s)	Description of the selected perspective
Baumeister [8], p. 1	an electrical power infrastructure that makes intelligent decisions about the state of the electrical power system to maintain a stable environment
McBride and McGee [62], p. 91–92	evolution of the power grid entails upgrading the infrastructure to a 'smart grid' to support two-way communication between electric generation, transmission and distribution infrastructure, and consumers of power [and involves] emerging smart grid applications such as advanced metering infrastructure (AMI), synchrophasors, distribution automation (DA), automated demand response, electric vehicles, and microgrid management
Pearson [70], p. 5212	. . .a network that can intelligently integrate the actions of all user connected to it – generators, consumers and those that do both – in order to efficiently deliver sustainable, economic and secure electricity supplies. . .fusing the physical delivery network with any number of separate ICT[information and communication technology]-enabled applications such as intelligent sensors, software, communications, and distributed control technologies. . .bring[ing] a host of benefits to both consumers and producers of electricity alike
Ray et al. [72], p. 276	. . .a paradigm shift in ways electric energy is produced, traded and consumed. Most visions of modernization of the electricity generation and delivery infrastructure would involve integration of diverse, connected, interdependent and adaptive functions and applications to enhance grid reliability, improve capital and operational efficiency and ensure security of the electric grid. . . comprising of advanced sensing, control, communication and information processing, emergent intelligence distributed across various segments of the power grid will transform the grid to a highly interactive and adaptive system
European Union [22], p. 45	. . .means an electricity network that can integrate in a cost efficient manner the behaviour and actions of all users connected to it, including generators, consumers and those that both generate and consume, in order to ensure an economically efficient and sustainable power system with low losses and high levels of quality, security of supply and safety

perspectives. To further expound on these representative perspectives, we now turn attention to the common basic components and characteristics of Smart Grids.

Similar to differing Smart Grid perspectives, there are also different perspectives on components (elements) that constitute Smart Grids. Baumeister [8], from a cybersecurity perspective, suggests that there are five *categories* of major themes for Smart Grids. Table 2 presents these categories along with their typical associated elements. These themes are directly related to each being a "component of the Smart Grid" ([8], p. 6) from the security perspective of Smart Grids.

Describing Smart Grids in terms of security domain appears as a dominant theme in literature. This might be attributed to increased coupling of information in the energy sector which has created new vulnerabilities [61]. These new vulnerabilities are especially inclusive of threats of the cyber-kind [13, 78, 86, 87].

An alternative approach for describing Smart Grids is provided through the lens of architectural representations. A *block diagram* is provided by Balaji and Ram [6] to illustrate Smart Grid as a "vast network comprising utilities and customers who are linked by the power transmission as well as communication infrastructure. The other entities in the network are involved in providing value added services for improving efficiency and facilitation of buying and selling of power driven by supply demand dynamics" ([6], p. 2903). A *hierarchical architecture model* has also been suggested by Moslehi and Kumar [63]. Their approach is based on the need for "harnessing modern communication and information technologies to enable an IT [Information technology] infrastructure that provides gridwide coordinated monitoring and control capabilities" and as such, it is mainly focused on "operating concerns in categories such as performance enhancement, equipment limits, operating limits, system protection, and rapid recovery" ([63], p. 60) with an emphasis on functional tasks of the elements comprising a Smart Grid. Yet another model of a Smart Grid is suggested by Komninos et al. [54] in the form of a *multi-layered conceptual model* that illustrates three major sections of a Smart Grid as well as its parts and their interactions. These representations provide a means by which a typical Smart Grid can be viewed as a complex of interrelated parts and elements [10, 32]. Consequently, these views are compatible with contemporary research trends of focusing on elements, their interactions in a grid, and exchange of information [32, 62, 72].

Perhaps a more comprehensive view of the Smart Grid is provided by IEEE's Standard 2030-2011 [38]. This standard articulates major entities and functions of a Smart Grid that aligns with the National Institute of Standards and Technology [NIST] framework for Smart Grids. Figure 1 is adapted from NIST [65] to depict the seven domains of a Smart Grid. The solid blue lines indicate the secure information and communication flows. The red dotted lines represent electricity flows.

Table 2 Baumeister's [8] categories and components of the smart grid

Security component	Area of focus	Description
Process control system [PCS] security	Supervisory control and data acquisition (SCADA)	Deals with controlling and monitoring the physical aspects of the electrical power grid. This aspect is essential since Smart Grid elements are often geographical distributed
Smart meter security	Smart meter	Deals with Smart Meters which are installed into consumer homes and serve as an interface between a home and the energy provider for exchange of information. There is a growing concern that Smart Meters could acts as access-points and manipulated
Power system state estimation security	Power system state estimation	Deals with having the ability to control physical properties of an electrical power system to maintain a stable state - making informed decisions in response to changes in demands
Smart grid communication protocol security	Communication components	Smart Grid relies on exchange of information and data between different components and elements of the system in order to function
Smart grid simulation for security analysis	Models and simulations	Power systems are expected to be operational on a continuous basis, testing any Smart Grid designs or changes are difficult task. Instead, it is possible to develop models that can be used for analysis

Each of the seven 'domains' can contain a number of interrelated complex systems along with logical interfaces (i.e., access points) in which information can enter/exit a domain [38, 65]. Table 3 depicts the seven domains of a Smart Grid as well as entities commonly associated with those domains. While this table does not place emphasis on the interfaces among the different domains of a Smart Grid, it forms the basis for suggesting that each domain could be viewed as a complex system. Guckenheimer and Ottino's [30] four distinctive properties of a complex system (i.e., many interacting parts, emergent behavior, adaptation and change, systems uncertainty) appear present for Smart Grids. For example, Advanced Metering Infrastructure, which is a building block for the customer domain, is described as a complex set of interrelated elements [4, 17, 62].

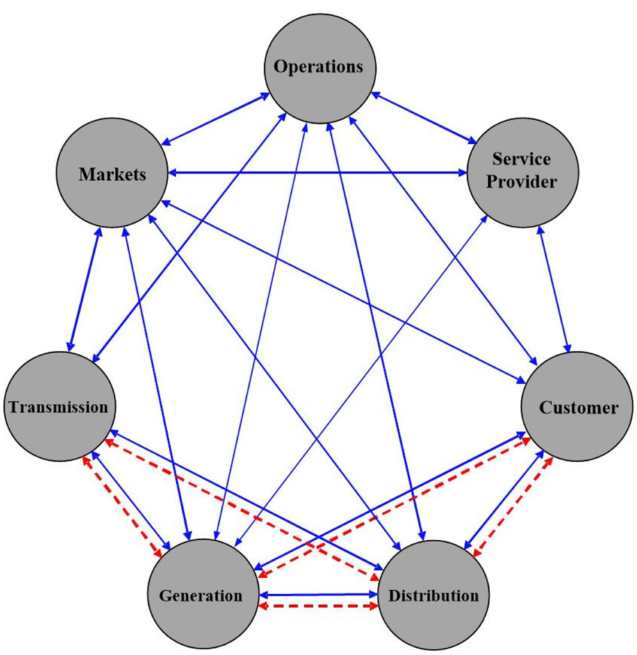

Fig. 1 A conceptual model of a smart grid

Arguably, when it comes to describing Smart Grids, none of these perspectives are incorrect. In fact, these perspectives are all necessary to set the basis for developing best practices for designing, maintaining, and realizing the premises of Smart Grids [32, 70, 84]. In fact, the perspectives also serve as the basis for creating measures and indicators that are instrumental in assessing performance of Smart Grids [78]. Inevitably, these perspectives can be used to enhance our understanding of the logic of various domains and their interrelations in Smart Grids [62]. Beyond the different articulations of Smart Grids, and perhaps more importantly, is the fact that there appears to be a set common themes that describe general 'characteristics' of Smart Grids [6, 14, 63, 68, 78]. Table 4 provides a set of common set of 'characteristics' of Smart Grids that are drawn from pertinent literature.

The discussion regarding components and the unifying 'characteristics' of Smart Grids were purposefully selected to illustrate three important points. First, the topic of Smart Grid is still in its infancy and therefore should be expected to be loosely bounded and harbor a degree of diverging and sometimes conflicting perspectives. Having diverging perspectives is not troubling. Rather, as [48] suggest, different perspectives put forward "show the potential sources of divergence in the development of the [Smart

Table 3 Domains and entities of a smart grid

Domain	Domain description	Typical entities
Operations	This domain is responsible for managing smooth movement of electricity including reliable and efficiency operations of electrical power systems [65]. Operations provides the necessary control mechanisms that "keep the grid up and running" ([38], p. 32)	A typical system/entity found in this domain is *fault management.* It "enhance[s] the speed at which faults can be located, identified, and sectionalized, and the speed at which service can be restored" ([65], p. 198). Other entities/operations include monitoring, control, analysis, reporting and statistics, real time network calculations, training, records and asset management, operational planning, maintenance and construction network extension planning, and customer support [65]
Service provider	This domain is responsible for connecting electricity market domain and the end users. It contains "third parties and utilities that provide electrical power-related services... [including] additional power supply options, such as discounts for less consumption during peak hours" ([38], p. 32). In short, these are "organizations providing services to electrical customers and to utilities" ([65], p. 126)	A typical entity found in this domain is an *electrical service provider* who might provide installation and maintenance services such as "installing and maintaining premises equipment that interacts with the smart grid" ([65], p. 197). Other services include customer management, building management, home management, billing, and account management [65] as well as "additional power supply options, such as discounts for less consumption during peak hours ([38], p. 32)
Customer	This domain is characterized as customers who are connected to the electrical distribution or transmission network. This domain "may include customers with only loads and customers with any combination of loads, generation, and storage...includes all loads whether they are connected at the transmission or distribution level, but it does not consider generation and storage connected at the transmission level" (IEEE [38], p. 31). In short, the domain of customer is simply the "end users of electricity" ([65], p. 190)	A typical entity found in this domain is a *building/home automation.* This is a "system that is capable of controlling various functions within a building, such as lighting and temperature control" ([65], p. 193). It certainly includes a Smart Meter as well as a plug –in electric vehicle (PEV) and distributed energy resources (DER) that aggregated to provide power necessary to meet regular demand. Furthermore, industrial automation, micro-generation, and storage are considered part of customer domain [38, 65]
Distribution	This domain is characterized by those who are involved as "distributors of electricity to and from customers. [Distributors] may also store and generate electricity" ([65], p. 190). Traditionally, this domain has had radial configurations with humans at the center of all communications [65]. Under the Smart Grid paradigm, "distribution domain will communicate in a more granular fashion with the Operations domain in real-time to manage the power flows associated with a more dynamic Markets domain and other environmental and security-based factors" ([65], p. 204)	A typical entity of this domain is a *distribution measurement and control devices* which include different "types of measurement and control systems to measure, record, and control, with the intent of protecting and optimizing grid operation" ([65], p. 205). Distribution substations, distributed energy resources (e.g., solar and wind) and distributed storage systems, capacitor banks, and sectionalizer contribute to this domain [38]
Generation	This domain is considered the first process in the delivery of electricity to consumers. Specifically, "electricity generation is the process of creating electricity from other forms of energy, which may include a wide variety of sources, using chemical combustion, nuclear fission, flowing water, wind, solar radiation, and geothermal heat" ([65], p. 199)	A typical entity of this domain is a *hydropower power plant*. It uses flowing water to produce electrical power. In 2013, hydropower accounted for about 6% of total US electricity generation and 52% of generation from all renewables [44]. A variety of other forms of energy generation (i.e., biomass, geothermal, nuclear, shale gas, wind) form this domain. However, since domain is electrically connected to other domains (e.g., transmission) the boundary of this domain includes other domains with applications such as communication, controlling and protecting playing major roles [65]

Table 3 (continued)

Domain	Domain description	Typical entities
Transmission	This domain involves the “carriers of bulk electricity over long distances” ([65], p. 190) with a major focus on reliable operations. NIST [65] also notes that “energy and supporting ancillary services...are procured through the Markets domain; scheduled and operated from the Operations domain; and finally delivered through the Transmission domain to the Distribution domain and ultimately to the Customer domain” (p. 202)	A typical entity of this domain is a *transmission system operator*. This is “an operator that transmits electrical power from generation plants over the electrical grid to a region or local electricity distribution operators” ([16], p. 50). It has been noted that such an operator tends to a monopoly changed with managing and developing the transmission grid infrastructure, maintaining balance in the system (i.e., supply and demand), and facilitating market operations [16]. Examples of physical entities/actors in this domain include remote terminal units, substation meters, protection relays, power quality monitors, phasor measurement units, sag monitors, fault recorders, and substation user interfaces [65]
Market	This is the domain that involves the buying and selling of grid assets [65]. This domain is “logically connected to with any of the generation, load control, and storage entities. Control by markets can be done directly at generation, load control, and storage, but it can be done via the operations and control domain. Additionally, as new markets emerge, the customer may seek to interact directly with the marketplace” ([38], p. 32)	A typical entity of this domain is a *market management*. These actors or market managers such as independent systems operator (ISO) for wholesale markets. They are also involved in transmission, services, and demand response markets as well [65]. Retailing, DER aggregation, trading, market and ancillary operations are all part of the market domain that tends to focus on “exchange price and balance supply and demand within the power system” ([65], p. 194)

Grid] field...[with] Each perspective brings[ing] a logic which provides its own internal validation to the community which produces and consumes the perspective” ([48], p. 240). Second, the field of Smart Grids can be identified as existing within the domain of critical infrastructure which “addresses elements of assessment, remediation, indications and warnings, mitigation, response, and reconstruction pertaining to hazards, risks, and threats from natural and manmade events affecting public well-being, public safety, economic vitality, and security” ([25], p. 194). Increasing concerns about frequency of occurrence of risk events, such as breaches, as well as their potential effects on public well-being, highlights the relative importance of Smart Grids as it relates to public well-being, including considerations of health, security, and economic impact [11, 47, 62, 90]. Third, the operating landscape/environment for Smart Grids is characteristically complex, involving a range of socio and technical issues [92]. The articulation of the current state of the Smart Grids problem domain can be characterized consistent with earlier works [45, 46, 48–51] and the notion of ‘messes’ by [1] as well as ‘wicked problems’ by [74]. Table 5 provide articulates characteristics of a landscape from which Smart Grids are projected to operate. This operating landscape suggests a need for robust analysis methods in all aspects of realization of Smart Grids.

One key aspect of realization of Smart Grids is risk. There is a growing support suggesting the need to address ‘risk’ related to Smart Grids [11, 15, 32, 33, 40, 54, 57, 62, 72, 75, 90, 91]. The following section provides an initial exploration into the concept of risk for Smart Grids as well as its quantification.

The Concept of Risk in Smart Grids

There is no one widely accepted definition of the term ‘risk.’ However, risk is typically defined in terms of probability of occurrence of an event and the magnitude of the resulting consequences [5, 24]. The vast literature on this topic also suggests that elements of event sequence and probabilities [71], technical factors in a system life cycle [39], probabilities of unknown outcomes and uncertainties [28], uncertainty [35, 53], perception of risk [88], mental constructs of risk [26], and ‘unknown unknowns’ [69] are also essential considerations related to risk quantification. Most recently, the concept of *interdependency* is increasingly incorporated into risk quantification [47, 73, 79]. Regardless of subtle and wide ranging distinctions related to the risk, a general consensus is that occurrence of a risk event can cause undesirable effects related to such issues as cost, schedule, and or technical performance of a system [18].

There is no shortage of risk events that can affect performance of Smart Grids. These range from natural events such

Table 4 Unifying characteristics of smart grids

Smart Grid characteristic	Description	Supporting Sources
Three indispensable factors for Smart Grid reliability are *availability*, *confidentiality*, and *integrity*	There are evident of the importance of security measures for Smart Grids [4, 62]. At the same time, Baumeister [8] notes that countermeasuring procedures against threats should "not impede power availability or safety" ([8], p. 4). In addressing security issues, three objectives of availability, confidentiality, and integrity have taken precedence: • *Availability* - is described as "the most important security objective" ([8], p. 4) which involves "ensuring timely and reliable access to and use of information is of the most importance in the Smart Grid" ([86], p. 1348). Loss of availability is in itself a disruption since it prevents access and use of information which can further undermine electricity delivery • *Confidentiality* - "Preserving authorized restrictions on information access and disclosure is mainly to protect personal privacy and proprietary information. This is in particular necessary to prevent unauthorized disclosure of information that is not open to the public and individuals" ([86], p. 1348) • *Integrity* – "Guarding against improper information modification or destruction is to ensure information non-repudiation and authenticity. A loss of integrity is the unauthorized modification or destruction of information and can further induce incorrect decision regarding power management" ([86], p. 1348)	[4, 8, 17, 19, 20, 38, 40, 65, 66, 72, 82, 86, 90]
Enabling informed participation by customers	Consumers help balance supply and demand, and ensure reliability by modifying the way they use and purchase electricity. Under the paradigm of Smart Grid, a consumer evolves into 'prosumer' who not only consumes electricity but produces and stores electricity [29]. This is meant to enable prosumers to have choices that motivate different purchasing patterns and behaviours related to electricity usage and influencing pricing as well as incentives [68]	[14, 63, 68, 78]
Accommodating all generation and storage options	A smart grid accommodates not only large, centralised power plants, but also the growing array of customer-sited distributed energy resources. Integration of these resources - including renewables, small-scale combined heat and power, and energy storage - will increase rapidly all along the value chain, from suppliers to marketers to customers ([68], p. 7)	[14, 38, 63, 65, 68, 78]
Enabling new products, services and markets	The paradigm of Smart Grid enables efficient market operations that enable the prosumers to choose among competing services. Some of the independent grid variables that must be explicitly managed are energy, capacity, location, time, rate of change and quality. Markets will play a major role in the management of these variables. Regulators, owners/operators and consumers need the flexibility to modify the rules of business to suit operating and market conditions [68]	[14, 38, 63, 65, 68, 78]
Provides the power quality for the range of needs	Not all commercial enterprises, and certainly not all residential customers, need the same quality of power. A smart grid supplies varying grades (and prices) of power. The cost of premium power-quality features can be included in the electrical service contract. Advanced control methods monitor essential components, enabling rapid diagnosis and solutions to events that impact power quality, such as lightning, switching surges, line faults and harmonic sources ([68], p. 7)	[14, 38, 63, 65, 68, 78]

Table 4 (continued)

Smart Grid characteristic	Description	Supporting Sources
Optimises asset utilisation and operating efficiency	A smart grid applies the latest technologies to optimise the use of its assets. For example, optimised capacity can be attainable with dynamic ratings, which allow assets to be used at greater loads by continuously sensing and rating their capacities. Maintenance efficiency can be optimised with condition-based maintenance, which signals the need for equipment maintenance at precisely the right time. System-control devices can be adjusted to reduce losses and eliminate congestion. Operating efficiency increases when selecting the least-cost energy-delivery system available through these types of system-control devices ([68], p. 7)	[14, 38, 63, 65, 68, 78]
Providing resiliency to disturbances, attacks and natural disasters	Resiliency has been defined as "the ability to withstand, recover from, and reorganize in response to crises" ([60], p.7) and includes elements of "defensive characteristics (e.g., deterrence, detection, delay, response, time to recovery; system defensive properties (e.g., physical barriers), maintenance capability to resist attacks; susceptibility, adaptive capacity, time to repair, availability of warning systems, and critical time" ([25], p. 195). Smart Grids are expected to be resilient to *all hazards* [78] as well have having the *self-healing* capability to reduce interruption of electricity delivery to prosumers [68]	[14, 38, 63, 65, 68, 78]
Enabling two-way communications model	A Smart Grid opens up the means for prosumers and utility to interact. Traditionally, meters provided reading for a total consumption of electricity over a given period of time. However, a Smart Grid, especially the introduction of an advanced metering infrastructure (AMI), introduces a number of technologies, in addition Smart Meters that enable two-way flow of information including real-time pricing and consumption. AMI functionalities include, among others, remote consumer price signals, which can provide time-of-use pricing information [68]	[14, 38, 54, 63, 65, 68, 68, 78]
Smart grid deployment enables significant CO_2 emissions reductions	Although electricity consumption only represents 17 % of final energy use today, it leads to 40 % of global CO_2 emissions, largely because almost 70 % of electricity is produced from fossil fuel...Taking these direct and indirect emissions reductions into account, the ETP BLUE Map Scenario estimates that Smart Grids offer the potential to achieve net annual emissions reductions of 0.7 Gt to 2.1 Gt of CO_2 by 2050 ([68], p. 27). The increased awareness of effects of emissions as well is advanced technologies provide the industry an incentive to develop Smart Grids [6]	[2, 6, 14, 17, 68]

as extreme weather conditions [57, 75] to man-made acts such as cyber-threats [4, 21]. The increasing frequency of such events coupled with their potential negative effects on public well-being suggests a need for development of risk-related approaches that could be used in understanding such emerging risks as well as aid in decision-making processes to mitigate their impact and/or prevent their occurrence altogether. However, we contend that current literature related to risk in relationship to Smart Grids suffers from two primary deficiencies: (1) it accounts for a limited set of traditional factors for quantification of risk and (2) it is atomistic in analysis for Smart Grids since it focuses on specific domains and elements of Smart Grids (e.g. transmission). These issues form the basis for remainder of this article as well as development of an extended set of measures that could be used in a more systemic analysis to aid in understanding and designing Smart Grids.

First, it is essential to recognize that the traditional risk formulation has been adapted for application to Smart Grids. For example, [59] suggests that an overload risk

Table 5 The operating landscape for smart grids and implications

Characteristic	Description	Smart grid problem domain implications
Proliferation of information	The information explosion has created unparalleled levels of quantity and access to information	Rapid technological changes and the quantity of information on Smart Grids could make it difficult to filter information resulting in poorly informed decisions, and lack of appropriate/timely information straining decision processes [89]
Conflicting perspectives and divergence in stakeholder views	Given the abundance of information and varying degrees of interpretation, conflicts in perspectives concerning situations, and the appropriate path forward for their resolution, are inevitable	Without adequate means to identify, explore, and resolve the underlying sources of diverging perspectives in Smart Grids, decisions, actions, and interpretations of Smart Grids is left to the inherent inefficiencies created by disparities in underlying worldviews such that ideas about the system are not be the same for all interested and disinterested parties [9]
Scarce and dynamically shifting resources	Resources have always been scarce and constrained. However, the short view and demands for immediate response to emergent issues creates a climate of instability in assurance of continuing resource availability	In a traditional form of planning, there is an assumption regarding stability in the environments. However, it is increasingly evident that there is uncertainty regarding availability and performance of Smart Grids due to security related issues [78], intermittency in distributed energy resources [75], and a lack of knowledge base [65]. These instabilities create a potential for a dramatic shift in resource availability and capability
Unintended consequences	High degrees of uncertainty and incomplete knowledge exacerbate the occurrence of behaviours and patterns that were not intended or anticipated	There has always been a desire to precisely understand direct cause-effect relationships [3, 70]. For Smart Grids this degree of prediction, understanding, or control is not attainable, forcing robust designs to deal with emerging patterns of behaviours
Ambiguous boundaries	Boundaries are essential to determine what is included and excluded in a complex system. They can be arbitrary, permeable, and dynamically shifting	There is a large degree of ambiguity as to the boundary of Smart Grids. This issue is more evident in attempts to generate a general criterion for definition of a Smart Grid. The boundary of what is included/exclude appears to shift based on the topic of research
Politically charged positions	Politically charged environments for complex systems are marked by attempts to pursue strategies to influence decisions, actions, and interpretations	Politics exist in all complex systems involving humans. Politics are neither good nor bad. However, politics and policy must be accounted for in the development, design, analysis, and execution of Smart Grid, not ignored. Certainly, this involves the means to obtain rights-of-way to build long-distance transmission lanes crossing local and national boundaries [92]
Solution urgency	There has always been an urgency to resolve issues related to complex system problems. However, current environments are increasing demands for instant gratification and resolution of system problems	Increasing urgency for solutions causes premature tradeoffs of time for other essential aspects of Smart Grid problem domain understanding and evolution. Premature conclusions of analysis are likely to result in superficial treatment of symptomatic, incomplete solutions, and unresolved deep system issues [41, 49]
Unclear entry point or approach	The degree of complexity for modern systems and their resulting problems occur on a continuous basis. There is no prescription or clear point of entry or exit to address related issues	Left without a clear entry point, the inevitable result is that each entry point for Smart Grid will offer both advantages and disadvantages. These may change over time as shifts occur in the context as well as understanding of Smart Grid operating landscape

assessment for a transmission line can be drawn from probability overload at a given line and the severity of the overload on the system. Rocchetta et al. [75] have also developed a simulation-based risk-cost optimization framework that accounts for high wind, solar irradiation, and lightning as major issues affecting failure rates in the overhead distribution lines of Smart Grids. The summation of *probability* of undesired events and the *severity* of the related consequences are used as the primary factors for risk articulation related to Smart Grids. Corresponding contingency frequencies related to unexpected loss of one or more elements (e.g. distribution line, transformer, etc.) and overload are used for risk estimation. Specifically, Rocchetta et al. [75] used a Monte Carlo simulation approach with a continuous Weibull distribution to illustrate the importance of integrating distributed power systems into a Smart Grid environment to counter the effects of extreme weather on availability of electricity. These approaches are similar to those of [40] and [91] with both using traditional factors of probability and consequence, although in different context, architecture of a Smart Grid for the former and Smart Control Center for the later.

Undoubtedly, electric, hybrid electric, and plug-in hybrid electric vehicles present a desirable potential for substantial impact on pollution, climate change, and energy utilization. However, and as indicated by Hashemi-Dezaki et al. [33], increased and especially unmanaged charging of these vehicles "may adversely [the] affect electric distribution system" ([33], p. 262). Hashemi-Dezaki and his colleagues [33] suggest that implementing managed charging with a schedule for charging plug-in hybrid electric vehicles is beneficial as it does not compromise the reliability of a Smart Grid. Similar to [75], Hashemi-Dezaki et al. [33] also uses a Monte Carlo simulation. However, risk is directly tied to reliability measures of *mean time to failure (MTTF)* and *mean time to repair (MTTR)*. These examples point to the need for holistic consideration of Smart Grids to better capture unintended consequences which may accrue as the system operates.

Beyond measures articulated above, literature also indicates a unique set of factors that could be used in association with analysis of Smart Grids. For example, [62] suggests that risk analysis for a utility system could involve the *goal of the adversary (i.e., motivation for attacking a business), threat agent availability, potential threat vectors, exposure, target attractiveness, and impact of attack*. These measures, according to [62] are instrumental in identification of vulnerability, prioritization of the threats, and development of countermeasures. Table 6 is a summary of literature depicting risk-related measures in different areas of Smart Grids.

This section was developed to illustrate how *risk* is currently being addressed in the Smart Grid literature as well as the implications for further development. Authors draw two primary conclusions based on this literature. First, it is evident that contemporary literature focuses on risk separately in the specific domains and elements associated with Smart Grids. This would then suggest that approaches for

Table 6 A synthesis of literature positioning in different aspects of risk for smart grids

Author(s)	Traditional factors (i.e., probability and consequence)	Area of application	Additional unique set of factors
[11]	Yes	A defined focus of interest	Vulnerability; Potential attack paths
[15, 32]	Yes	Smart Grid (Whole)	Probable effectiveness of security measures; Lack of security measures
[33]	Yes	Charging of plug-in hybrid electric vehicles	Reliability
[40]	Yes	Smart Grid Architecture	–
[59]	Yes	Transmission line overload	–
[57]	Yes	Smart Grid Architecture	Risk index system for Smart Grids
[62]	Yes	Risk from a security perspective	Availability of threat agents; Potential treat vectors; Exposure; Attractiveness of the target; Ease of attack
[72]	Yes	Smart Grid security	Effectiveness of countermeasures; Vulnerability; Tolerance of stakeholders
[75]	Yes	Distributed power generation systems	Total number of lines in the system; Total number of nodes
[90]	Yes	Smart Meter	Vulnerability
[91]	Yes	Smart control center	–

risk quantification would necessarily be expected to vary from domain to domain within Smart Grids. For example, the approach for transmission lines [59] significantly varies from a security-related approach [62]. It might be reasonably expected to have different approaches in the different domains of Smart Grids since certain factors are domain-specific. However, this focus on risks related to the constituent domains offers limited utility to those who might be involved at an integrated level of Smart Grids, which exist beyond individual domains. At the higher (systems) level of Smart Grids, risks cannot be assumed to be aggregates of mutually exclusive and independent risks of the constituent domain risks. Thus, risks at the Smart Grid exist at a different logical level than those of the constituent domains and cannot be simple inferred from domain level risks. An analysis based on simple extrapolation of constituent domain risks are tenuous at best and outright wrong at worst. If the objective is to analyze Smart Grids at a system level, we must look beyond simple aggregation of risks from constituent domains. Second, traditional risk formulation of probability and consequence is prevalent across the literature and in the individual constituent domains for Smart Grids and offers a good starting point to rethinking analysis of the higher logical (systemic) level for Smart Grids. More advanced, and arguable more appropriate, risk literature also points to consideration of a more robust set of factors that might be useful quantifying risk for Smart Grids (e.g. dependency, interdependency, resilience). It is from this perspective that we propose developing an extended set of factors that could be used in more holistic analysis of Smart Grids.

Holistic Risk Formulation for Smart Grids

The need for holistic approaches to risk analysis for Smart Grids is not new [32, 40]. It has long been recognized that the evolving nature of threats coupled with the 'E+I' (i.e., energy and information) paradigm [26] have transformed the thinking from the traditionally isolated systems perspective into a more "highly interconnected and interdependent system of local and wide area information and communication systems" ([72], p. 276) perspective. This means consideration of interactions and interdependencies

Table 7 A set of factors for smart grid risk quantification

Author(s)	Unique set of factors	Operational description
[62], p. 98	Attractiveness of the target [F1]	How motivated an attacker would be to compromise the target - which can be related to the potential reward, the geopolitical or military significance of the target, the value of the information and the general public's interest in information on the target (including privacy-related aspects)
[62], p. 98	Availability of threat agents [F2]	Availability of threat agents – agents including "company employees, terrorists, espionage agents, extortionists, hackers, cyber-criminals, customers, and outsourced maintenance staff" that are willing to realize a threat"
[11, 62]	Availability of attack routes [F3]	Presence of routes/paths that can be used to exploit a system a Smart Grid and involves such mediums as wireless access points, intranet, mobile devices (e.g., USB devices) and Smart Meters
[15, 32, 62, 72]	Ineffective protection measures [F4]	Exploitability of a system which relates to how easy a Smart Grid can be attacked because of lack of security measure or having ineffective security measures such that "probability of [an] interception [of a threat] and the probability of neutralizing a given threat" ([32], p. 4) is low
[62]	Exposure [F5]	Entails a "condition of being unprotected from a severe condition" ([47], p. 15) and involves being 'exposed to' threats
[33]	Reliability [F6]	The probability that a system will perform its intended mission(s) when called upon to do so [47]. In a Smart Grid, reliability is related to being available "in the widespread presence of PHEVs [plug-in-hybrid-electric vehicles]" ([33], p. 263)
[72]	Tolerance of stakeholders [F7]	The willingness to allow existence of some risks and/or behavior that one does not necessarily agree with
[75]	Total number of lines [F8]	The number of lines (e.g., power lines, communication nodes, etc.) used in transmitting electricity and information from one point to another
[75]	Total number of nodes [F9]	The number of points on a transmission line where two or more transmission lines meet
[90]	Vulnerability [F10]	A feature of a system that represents a susceptibility to a threat. A vulnerability may be a weakness, flaw or deficiency, or it may be an intentional aspect of the system" ([90], p. 88)

among different domains of Smart Grids (i.e., generation, transmissions, distribution, customers, markets, operations, and service providers) as well as the other systems in the environment [40]. Under this emerging paradigm, Ray and his colleagues suggest the development of a unified risk model that considers "interconnections of domains...variety of dynamic and structural interactions" for Smart Grids ([72], p. 281). In light of these insights, there is an increased call to rethink how risk is formulated [42, 43, 47] with respect to the complexities that are endemic to modern systems and higher level domains such as Smart Grids.

In this section, we develop an extended list of factors that can be used for analysis of Smart Grids. Although it is not presented as the definitive listing of factors, it is offered as a first articulation for moving beyond the narrower conceptions of risks in Smart Grids. As such, the factors can, should, and will evolve with further development, insights, and applications. As a first step in this exploration, we examine a set of extended factors identified from the Smart Grid literature. A review of existing factors suggests that a total 10 factors from the literature (i.e., *attractiveness of a target, availability of threat agents, availability of attack routes, ineffective protection measures, exposure, reliability, tolerance of stakeholders, total number of lines, total number of nodes, and vulnerability*). These factors are in additional to the two traditional factors of *probability* and *consequence* that are used in different risk-related approaches for Smart Grids. Many of these factors are terms or phrases that have an exact or nearly the same meaning used in different contexts – that is they are synonyms. For example, Bologna et al. ([11], p. 6) refers to "potential attack paths" to suggest a route that could be used to attack a system. On the other hand, McBride and McGee ([62], p. 97) use the words "potential threat vectors" to suggest potential 'channels' such the "Internet, wireless access points, the enterprise intranet, mobile devices (including USB devices), remote endpoints (including meters), the supply chain, and the company's own systems development organization" that could be used in attacking a system. Clearly, the different phrases address congruent issues and are referring to availability of routes/paths that can be used to exploit a system - in this case, a Smart Grid. The same logic is used to combine concepts of *ease of attack*, *effectiveness of countermeasures*, and *lack of security measures*. Table 7 summarizes a synthesis of similar terms into seemingly unique factors that can be applied at the level of Smart Grids for risk quantification.

Arguably, Katina and Hester [42] have developed a comprehensive set of factors that can be used to determine 'criticality' of infrastructure systems [85]. To this end, we can

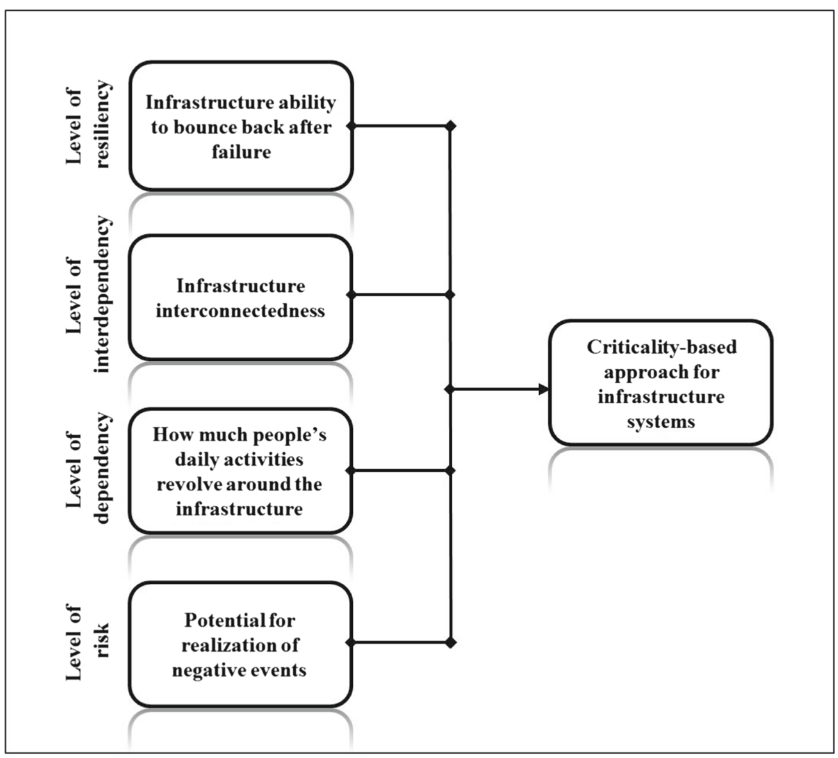

Fig. 2 Areas of a criticality-based approach

Table 8 Mapping contemporary Smart Grid risk-related factors into criticality-based model for infrastructure systems

Criticality-based measures	Properties for each factor	Smart Grids risk factors	Implications for Smart Grid research
Dependency	Economic importance	–	An economic importance of a Smart Grid through dependency lens. More value would be assigned to those good and services of a Smart Grids appearing to support public well-being in economic terms
	Effects	–	A level of effects brought through dependencies (internal or external) that could enable or disable a Smart Grid and subsequently affecting public well-being
	Criticality	–	A value of a Smart Grid and/or its components in relation to meeting pre-determined public well-being goals
	Community awareness	–	Amount of work that has historically been done to mitigate hazards to Smart Grids. *Intense* activity could indicate extent to which stakeholders grasp level of dependency
	Importance	F1	Extent of urgency or necessity of doing work to address a threat [56]. These effects could be driven by the fact that an attacker sees a Smart Grid or its components as an 'attractive' target
	Satisfaction	–	Degree to which public needs and expectations are derived from performance of a Smart Grid. This could also entail acceptance of level at which Smart Grid stakeholders are working to prepare for, respond to, or mitigate potential hazards
	Critical quality	–	Extent to which reduction in the quality of the expected service of a Smart Grid can be reduced before it begins to affect public well-being
	Scope	–	Breadth and reach products and services of a Smart Grid or its component on public well-being
	Impact on system users	–	Magnitude and impact of a failure that could affect public well-being as a result of dependency on goods and services of a Smart Grid. A high magnitude corresponds to high dependency
	Political relevancy	–	Degree to which local, state, and federal authorities depend on goods and services of a Smart Grid
	Cost to repair	–	Cost associated with restoring a Smart Grid or its component
Interdependency	External relationships	F5	Number of external relationships to a Smart Grid. These relationships (i.e., links) could expose a Smart Grid to threats originating from interdependent systems
	Critical proportion	–	Percentage/proportion of entities and/or people that are intrinsically interconnected to a Smart Grid. The performance of a Smart Grid would be affected by increased number of interdependencies. However, this relationship would be in form of an *inverse proportion* such that a single relationship is what is enable/disables a Smart Grid
	Interconnectedness	F8; F9	Level of intricate relationships within a Smart Grid. This includes relationships among the domains, components, and parts of a Smart Grid that attribute to structural complexity
	Decentralization	–	Dispersion of a Smart Grid as a system and its parts. There might be more systems interdependent connected to a highly decentralized Smart Grid

Table 8 (continued)

Criticality-based measures	Properties for each factor	Smart Grids risk factors	Implications for Smart Grid research
	Location	–	Locality of a Smart Grid. A Smart Grid is likely to be located in an area where is can have most positive impact on the users. This increases the number of interconnections
Resiliency	System protective characteristics	–	Number of a variety of mechanisms intended to pre-emptively boost protection measures of a Smart Grid
	System defensive properties	F4; F6	Taking a reactive model of approach to Smart Grid threats. This could be done through implementation of a number of measures that could be used to resist attacks on a Smart Grid
	Maintenance capability	–	Availability of capability to preserve or improve the state of Smart Grid operability despite attempts distort it
	Deterrence	–	Availability of means to discourage an attack on a Smart Grid in order to keep its operability status
	Detection	–	Ability to identify presence of concealed threats that could affect Smart Grid operability
	Delay	–	Ability to impede an attacker from penetrating into a Smart Grid, physically or otherwise
	Adaptability	F7	Ability to respond and recovery from a threat as soon as possible which is related time to repair and well as willingness to tolerate inoperability status of a Smart Grid
	Susceptibility	–	A state of being likely to be influenced and/or harmed by extraneous agents including severe weather conditions and new policy
	Capacity	–	Having a long-term capacity to deal with a variety of sudden changes and threats while learning from such changes to evolve into a more resilient Smart Grid
	Availability of warning systems	-	Apart from having ability to detect and delay threats, a well-designed Smart Grids need to have capability to alert of future intrusions [52]
Risk	Safety	–	Ability to address concerns of being unprotected from causes of danger, risk, or injury to public well-being
	Environmental factors	–	A consideration of elements in the environment [77] which exert a degree of control over the processes and behavior of a Smart Grid
	Vulnerability[1]	F10	A consideration of multi-dimensionality of disasters including environmental, technical, human which if exposed to a Smart Grid will damage its goods and services
	Probability of event	P1	A consideration of the likelihood that a risk event will occur to halt operations of a Smart Grid. The operating landscape for Smart Grids appears to suggest a higher likelihood of occurrence of risk events
	Consequences	C1	Accounting for the ramifications of occurrence of risk events on operability of a Smart Grid as well as public well-being
	Exclusivity	–	Designing a Smart Grid easily accessible to everyone. Total access is provided to a select number of people. Inclusiveness could contribute system threats

Table 8 (continued)

Criticality-based measures	Properties for each factor	Smart Grids risk factors	Implications for Smart Grid research
	Intent	F2	Accounting for availability of agents, including but not limited to rogue nations and their machinations, who have the will and intent to attack a Smart Grid
	Frequency	–	Accounting for the rate at which attacks on a Smart Grid or its domains are repeated over a particular period of time. Frequency of occurrence is not equivalent to occurrence of a risk event. However, increasing rate could suggest a greater change of failure occurrence

[1]Vulnerability has also been described as a 'state of a system' and defined as a 'threat, a predictive quantity reflecting system's selective stress reaction toward a respective threat' [83]. Authors suggests that this view may be essential when it comes to development of criticality-based models that could be used for quantification of different measures as suggested in this research. However, current research efforts are predicated upon establishing different measures (factors) that ought to be considered in the analysis of Smart Grids

compare contemporary Smart Grid risk factors to criticality-based factors to develop a comprehensive set of factors to support analysis of Smart Grids. Katina and Hester [42], researchers with the National Centers for System of Systems Engineering, in their attempt to create a generalizable and transportable method for prioritizing critical infrastructures, postulated that current methodologies are sector-specific approaches and/or based on regional factors. They proposed a four-tuple of 'criticality' factors of *levels of resiliency*, *level of interdependency*, *level of dependency* along with *infrastructure risk*[1] as fundamental to ranking and prioritization of infrastructures regardless of sector or region. The term 'criticality' in this sense relates to the importance of an infrastructure (e.g., a Smart Grid) to public well-being. Each of the four factors of criticality are associated with a set of properties that could be used for measuring each factor and contributes to a set of higher level criticality measures for a system. Figure 2 is drawn to capture the essence of Katina and Hester's [42] four-tuple criticality-based measures.

A mapping of the 10 seemingly unique factors from the Smart Grid literature into the criticality-based measures reveals a number of issues. First, several factors from the Smart Grid literature can be merged into single factors of the criticality-based approach. For example, *total number of lines [F8]* and *total number of nodes [F9]* are essentially addressing the effects of having a great number of interconnected systems. Nodes represent systems and lines represent the means by which such systems are interconnected. Failure in such a system, from a criticality-based analysis approach, is described in terms of number lines that fail after an attack, which in turn affects nodes in a Smart Grid. This issue is addressed in the interdependency criticality-factor since it includes interconnectedness of a system [42]. F4 is also combinable with F6 inasmuch as F6 is not possible if a system has ineffective protection measures. Table 8 provides a mapping of contemporary risk factors for Smart Grid risk (synthesized from literature) to those proposed by [42].

Second, there is a gap in how risk for Smart Grids is addressed. As indicated in Table 8, there are a number of properties that could be associated with one another. For example, 'community awareness' is associated to 'measure of dependency', 'external relationship' is associated to 'measure of interdependency', 'system protective' characteristics is associated to 'resiliency' and 'environmental factors' associated to 'risk.' These properties, in addition to probability and consequence, can be used to inform a more robust and holistic analysis for Smart Grids. While these properties are not presented as exhaustive, they offer a more extensive set of 'metrics' for a deeper and more rigorous analysis of Smart Grids.

Finally, applying traditional measures of *probability* and *consequence* to a specific domain of a Smart Grid offers only a partial view of the landscape within which Smart Grids operate. Subsequently, there is a need to consider the interrelationships among the seven different domains of Smart Grids. Arguably, these relationships could be explored in terms of dependency, where functioning of a given domain (e.g., distribution) is dependent on another domain (e.g., transmission). The interdependency measure recognizes that each domain (e.g., customer) influences and is also influenced by the remainder of the domains of a Smart Grid. The resiliency measure initiates the discussion

[1] There are different configurations of risk assessment approaches (e.g., see [34, 81]). However, the key appears to be in the consistency of the logic in which the assessment for risk could be done. In this research risk is taken as one of the elements that must be assessed in the analysis of a Smart Grid.

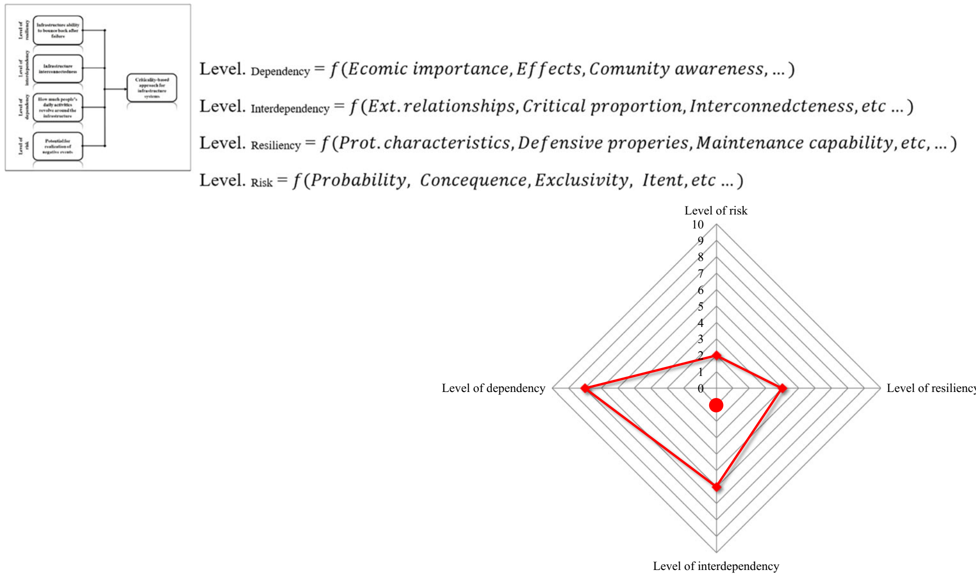

Fig. 3 Criticality measures for Smart Grid and their representation in a radar diagram

about designing Smart Grids that can withstand or rapidly recover from threats and hazards. These measures are in addition to the traditional considerations of probability and consequence associated with risk. Together, the four measures of the criticality-based approach (CBA) for analysis of Smart Grids account for several properties that could be instrumental in design, development, and analysis of Smart Grids. An operand for the proposed approach is provided as:

$$Cr_{SmartGrid} = f(Level_{Dependency} Level_{Interdependency} \ominus Level_{Resiliency} \ominus Level_{Risk})$$

Each level of measure, which for simplicity might range 0 to 10, could be assessed based on the proposed properties as suggested below to offer information and insights on the state of a Smart Grid. The combination of these measures could then be used in a radar chart for the analysis of a Smart Grid as indicated in Fig. 3. Each spoke of the radar chart represents one of the four measures. In Fig. 3, the observation of a 2 for a measure of risk suggests a low risk level in a given scenario.

The proposed four-tuple measures certainly contribute to current research in different ways. At the framework level, current instantiations of risk-based frameworks have a "set of optimal steps [phases] that can be used identify, evaluate and control risk to mitigate potential negative effects in Smart Grid[s]" ([90], p. 89). Typically, these phases include risk identification, risk characterization, risk evaluation, risk mitigation planning, risk management, risk communication, and monitoring and review process at the conclusion. The proposed approach complements risk-based frameworks for Smart Grids in identifying potential issues that could affect performance as well as areas that could be in need of attention. For example, the properties associated with dependence such *economic importance* could enable the analyst to consider where the provision of goods and services of a Smart Grid are economically feasible. In the consideration of economic feasibility, the analyst might deliberate the role of malicious, technical, and/or natural hazards affecting the system. Therefore, this research offers a different lens through which policy-makers, Smart Grid owners, and operators might analyze Smart Grids beyond the traditional perspective of risk limited to probability and consequence. Also, observations of the different levels (continuous or incremental) of the properties might offer insights into the state of the Smart Grid such that indicators supporting more robust changes could be detected and examined.

Conclusions and Future Directions

Smart Grids, to meet the challenges and satisfy the needs of the context from which they are derived, will fundamentally be required to address a variety of issues present in their current operating landscape. Arguably, the operating landscape for Smart Grids requires that we rethink how to address risk to truly realize the full potential and contributions sought for Smart Grids. A strict view of *risk* that considers only *probability* of occurrence of an event that could halt Smart Grid operations and *consequences* of such an event on public well-being, offers limited utility for application to the complex nature of Smart Grids. Such a limited approach is likely to produce an overly narrow and short-term view of risk for practitioners who must contend with a spectrum of issues that could affect performance of Smart Grids. This paper proposes an approach: criticality-based approach (CBA), for the analysis of Smart Grids with four measures: dependency, interdependency, resiliency, and risk (inclusive of traditional probability of occurrence and consequences). Each category measurement involves a set of properties that could be used in design, analysis, and evolution of Smart Grids as well as the development of countermeasures for issues associated with performance of Smart Grids.

While a CBA for analysis of Smart Grids is a necessary step in a robust analysis, much research remains for realization and operationalizing this approach. A primary area for development remains how to measure the different properties that contribute to the different measures associated to CBA centered on dependency, interdependency, resiliency, and risk. A starting point should certainly involve on a review of how the elements of the four-tuple are currently measured. For example, a measure of interdependency has been proposed in literature [47, 76]. These could be adapted for Smart Grid research as well as linguistic measures (i.e., low, medium, and high) which could then be translated into numerical values [15, 27, 72]. This becomes a starting point for applications and quantification of the proposed approach for analyzing Smart Grids. Two major contributions would be: (1) the ability to compare and contrast the states of different Smart Grids and impacts of improvement initiatives and (2) establishing a baseline against which the development and improvement of a Smart Grid could be more rigorously measured.

A Smart Grid is part of the energy sector and thus related to critical infrastructures enabling production of goods and services essential for public well-being. Public well-being is intrinsically tied to measures of the CBA in Smart Grids analysis. However, there are no known well-articulated indicators or tools for measuring public well-being in relationship to Smart Grids. In response to this gap, such indicators could be developed and explicitly attributed to goods and services provided as a result of Smart Grids. This might provide a basis for relating each of the measures of the proposed approach, as well as their properties, to public well-being. This 'measurable' relationship could then form the basis for more informed decisions-making concerning allocation of scarce resources, prioritization of Smart Grid development, exploration of potential scenarios, and establishment of the level of tolerance for different issues affecting Smart Grids. In accordance with the latest reports (see [10]), such tools have to be developed and 'lab tested' to ensure operability in the real world.

Acknowledgment The researchers acknowledge funding from the *Department of Engineering Management and Systems Engineering* at Old Dominion University (Norfolk, Virginia, USA) and the *Energy Department - Nuclear Division*, *Laboratory of Signal Analysis and Risk Analysis* at Politecnico di Milano, (Milano, Italy).

References

1. Ackoff RL (1974) Systems, messes, and interactive planning. In: Redesigning the future: systems approach to societal problems. Wiley, New York, pp 20–33
2. Aillerie Y, Kayal S, Mennella J-P, Samani R, Sauty S, Schmitt L (2013) Smart grid cyber security: smart grid deployment requires a new end-to-end security approach (White paper). Santa Clara, CA, Intel. Retrieved from http://www.mcafee.com/tw/resources/white-papers/wp-smart-grid-cyber-security.pdf
3. Aldeen M, Saha S, Alpcan T, Evans RJ (2015) New online voltage stability margins and risk assessment for multi-bus smart power grids. Int J Control 88(7):1338–1352. doi:10.1080/00207179.2015.1012557
4. Amin SM, Giacomoni AM (2012) Smart Grid - Safe, secure, self-healing. IEEE Power Energ Mag 10(1):33–40
5. ASCE (2009) Guiding principles for the nation's critical infrastructure. American Society of Civil Engineers, Reston
6. Balaji AJ, Ram DSH (2015) FPGA based system for denial of service detection in smart grid. J Eng Appl Sci 10(7):2903–2906
7. Battaglini A, Lilliestam J, Bals C, Haas A (2008) The SuperSmart Grid. In: European Climate Forum. Postdam Institute for Climate Impact Research, Potsdam
8. Baumeister T (2010) Literature review on Smart Grid cyber security, p 34. University of Hawaii, Honolulu. Retrieved from http://csdl.ics.hawaii.edu/techreports/10-11/10-11.pdf
9. Becker HS (ed) (1966) Social problems: a modern approach. Wiley, New York
10. Blanco MP, Prettico G, Andreadou N, Guardiola MO, Fulli G, Covrig CF (2015) Smart grids laboratories inventory 2015 (JRC Science and Policy Report No. EUR 27155 EN). Joint Research Centre, Luxembourg
11. Bologna S, Khurana H, Precsenyi Z, Rambi J, Banayoti H, Eckmaier R (2012) Assessment methodology for relevant assets: expert Group on the security and resilience of communication networks and information systems for Smart Grids (Work Package 1.4 No. DRAFT 0.9). Commission of the European Communities, Brussels, p 9
12. Calida BY, Katina PF (2012) Regional industries as critical infrastructures: a tale of two modern cities. Int J Crit Infrastruct 8(1):74–90. doi:10.1504/IJCIS.2012.046555
13. Choo K-KR (2011) The cyber threat landscape: challenges and future research directions. Comput Secur 30(8):719–731. doi:10.1016/j.cose.2011.08.004
14. Clastres C (2011) Smart grids: another step towards competition, energy security and climate change objectives. Energy Policy 39(9):5399–5408
15. Clements SL, Kirkham H, Elizondo M, Lu S (2011) Protecting the smart grid: a risk based approach
16. Covrig CF, Ardelean M, Vasiljevska J, Mengolini A, Fulli G, Amoiralis E, Jimenez MS, Filiou C (2014) Smart Grid projects outlook 2014. Publications Office of the European Union, Petten
17. CSU - Sacramento (2012) Smart Grid cyber security potential threats, vulnerabilities and risks (No. CEC5002012047). California Energy Commission, Sacramento, p 83. Retrieved from http://www.energy.ca.gov/2012publications/CEC-500-2012-047/CEC-500-2012-047.pdf
18. de Weck OL, Roos D, Magee CL (2011) Engineering systems: meeting human needs in a complex technological world. MIT Press, Cambridge
19. ENISA (2012) Appropriate security measures for smart grids Guidelines to assess the sophistication of security measures implementation [2012-12-06]. European Network and Information Security Agency, Heraklion, p 84

20. ENISA (2013) Smart Grid threat landscape and good practice guide. Agency for Network and Information Security, Heraklion, pp 1–83
21. Ericsson GN (2010) Cyber security and power system communication - essential parts of a smart grid infrastructure. IEEE Trans Power Delivery 25(3):1501–1507
22. European Union (2013) Regulation (EU) No 347/2013 of the European Parliament and of the Council of 17 April 2013 on guidelines for trans-European energy infrastructure and repealing Decision No 1364/2006/EC and amending regulations (EC) N. 713/2009, (EC) No 714/2009 and (EC) No 715/2009. Off J Eur Union L 115:39–75. Retrieved from http://eur-lex.europa.eu/legal-content/EN/TXT/?uri$=$celex%3A32013R0347
23. Fazio M, Puliafito A, Villari M (2014) IoT4S: a new architecture to exploit sensing capabilities in smart cities. Int J Web Grid Serv 10(2/3):114–138
24. Garvey PR, Pinto CA (2009) Introduction to functional dependency network analysis. In: The 2nd international symposium on engineering systems. Massachusetts Institute of Technology, p 17. Retrieved from http://esd.mit.edu/symp09/day3.html
25. Gheorghe AV, Katina PF (2014) Editorial: resiliency and engineering systems - research trends and challenges. Int J Crit Infrastruct 10(3/4):193–199
26. Gheorghe AV, Masera M, Weijnen MPC, De Vries JL (eds) (2006) Critical infrastructures at risk: securing the European electric power system, vol 9. Springer, Dordrecht
27. Gheorghe AV, Vamanu DV (2004) Towards QVA – quantitative vulnerability assessment: a generic practical model. J Risk Res 7(6):613–628. doi:10.1080/1366987042000192219
28. Gibson JE, Scherer WT, Gibson WF (2007) How to do systems analysis. Wiley-Interscience, Hoboken
29. Grijalva S, Tariq MU (2011) Prosumer-based smart grid architecture enables a flat, sustainable electricity industry. In: Innovative Smart Grid Technologies (ISGT), 2011 IEEE PES, pp 1–6
30. Guckenheimer J, Ottino JM (2008) Foundations for complex systems research in the physical sciences and engineering, Northwestern University: National Science Foundation, Evanston. Retrieved from http://www.math.cornell.edu/∼gucken/PDF/nsf_complex_systems.pdf
31. Guérard G., Amor SB, Bui A (2012) Survey on Smart Grid modelling. Int J Syst Control Commun 4(4):262–279
32. Habash RWY, Groza V, Krewski D, Paoli G (2013) A risk assessment framework for the smart grid, pp 1–6. Presented at the 2013 IEEE Electrical Power Energy Conference (EPEC), Halifax, NS, Canada. doi:10.1109/EPEC.2013.6802930
33. Hashemi-Dezaki H, Hamzeh M, Askarian-Abyaneh H, Haeri-Khiavi H (2015) Risk management of Smart Grids based on managed charging of PHEVs and vehicle-to-grid strategy using Monte Carlo simulation. Energy Convers Manag 100:262–276
34. Hill KN (2012) Risk quadruplet: integrating assessments of threat, vulnerability, consequence, and perception for homeland security and homeland defense (Ph.D.) Old Dominion University, United States – Virginia
35. Holton GA (2004) Defining risk. Financ Anal J 60(6):19–25
36. Hossain E, Kabalci E, Bayindir R, Perez R (2014) Microgrid testbeds around the world: state of art. Energy Convers Manag 86:132–153. doi:10.1016/j.enconman.2014.05.012
37. Hou H, Zhou J, Zhang Y, He X (2011) A brief analysis on differences of risk assessment between Smart Grid and traditional power grid (pp. 188–191). Presented at the 2011 4th international symposium on knowledge acquisition and modeling (KAM). Sanya doi:10.1109/KAM.2011.57
38. IEEE (2011) IEEE guide for smart grid interoperability of energy technology and information technology operation with the electric power system (EPS), end-use applications, and loads. IEEE Std 2030-2011, pp 1–126. doi:10.1109/IEEESTD.2011.6018239
39. INCOSE (2011) Systems engineering handbook: a guide for system life cycle processes and activities. (H. Cecilia, Ed.) (3.2 ed.). INCOSE, San Diego
40. Kammerstetter M, Langer L, Skopik F, Kupzog F, Kastner W (2014) Practical risk assessment using a cumulative Smart Grid model. In: SMARTGREENS2014. Barcelona, pp 31–42. doi:10.5220/0004860900310042
41. Katina PF (2015) Emerging systems theory–based pathologies for governance of complex systems. Int J Syst Syst Eng 6(1/2):144–159. doi:10.1504/IJSSE.2015.068806
42. Katina PF, Hester PT (2013) Systemic determination of infrastructure criticality. Int J Crit Infrastruct 9(3):211–225
43. Katina PF, Pinto CA (2012) On critical infrastructure interdependency. In: The 33rd international annual conference of american society for engineering management. Curran Associates, Inc, Virginia Beach, p 10
44. Katina PF, Unal R (2015) Application of fuzzy sets in decision analysis for prioritising critical energy infrastructures. Int J Decis Sci Risk Manag 6(1):1–15. doi:10.1504/IJDSRM.2015.072762
45. Katina PF, Despotou G, Calida BY, Kholodkov T, Keating CB (2014a) Sustainability of systems of systems. Int J Syst Syst Eng 5(2):93–113. doi:10.1504/IJSSE.2014.064833
46. Katina PF, Keating CB, Jaradat RM (2014b) System requirements engineering in complex situations. Requir Eng 19(1):45–62
47. Katina PF, Pinto CA, Bradley JM, Hester PT (2014c) Interdependency-induced risk with applications to healthcare. Int J Crit Infrastruct Prot 7(1):12–26. doi:10.1016/j.ijcip.2014.01.005
48. Keating CB, Katina PF (2011) Systems of systems engineering: prospects and challenges for the emerging field. Int J Syst Syst Eng 2(2/3):234–256. doi:10.1504/IJSSE.2011.040556
49. Keating CB, Katina PF (2012) Prevalence of pathologies in systems of systems. Int J Syst Syst Eng 3(3/4):243–267. doi:10.1504/IJSSE.2012.052688
50. Keating CB, Katina PF (2015) Editorial: foundational perspectives for the emerging complex system governance field. Int J Syst Syst Eng 6(1/2):1–14
51. Keating CB, Katina PF, Bradley JM (2014) Complex system governance: concept, challenges, and emerging research. Int J Syst Syst Eng 5(3):263–288
52. Klump R, Kwiatkowski M (2010) Distributed IP watchlist generation for intrusion detection in the electrical smart grid. In: Moore T, Shenoi S (eds) Critical infrastructure protection, vol 4. Springer Berlin Heidelberg, New York
53. Knight FH (1921) Risk, uncertainty, and profit. Hart, Schaffner & Marx; Houghton Mifflin Co, Boston
54. Komninos N, Philippou E, Pitsillides A (2014) Survey in smart grid and smart home security: issues, challenges and countermeasures. IEEE Commun Surv Tutorials 16(4):1933–1954
55. Kröger W, Zio E (2011) Vulnerable systems. Springer-Verlag, London
56. Li H, Apostolakis GE, Gifun J, VanSchalkwyk W, Leite S, Barber D (2009) Ranking the risks from multiple hazards in a small community. Risk Anal 29(3):438–456
57. Liu R (2013) Preliminary analysis of Smart Grid risk index system and evaluation methods. Energy Power Eng 5:807–810. doi:10.4236/epe.2013.54B155
58. Li W (2014) Risk assessment of power systems: models, methods, and applications. Wiley
59. Li X, Zhang X, Wu L, Lu P, Zhang S (2015) Transmission line overload risk assessment for power systems with wind and load-power generation correlation. IEEE Trans Smart Grid 6(3):1233–1242. doi:10.1109/TSG.2014.2387281

60. Martin-Breen P, Anderies JM (2011) Resilience: a literature review. The Rockefeller Foundation, New York, p 64. Retrieved from http://www.rockefellerfoundation.org/blog/resilience-literature-review
61. Masera M, Stefanini A, Dondossola G (2006) The security information and communication systems and the E+I paradigm. In: Gheorghe AV, Masera M, Weijnen MPC, De Vries JL (eds) Critical infrastructures at risk: securing the european electric power system. Springer, Dordrecht, pp 85–116
62. McBride AJ, McGee AR (2012) Assessing Smart Grid security. Bell Labs Tech J 17(3):87–103. doi:10.1002/bltj.21560
63. Moslehi K, Kumar R (2010) A reliability perspective of the Smart Grid. IEEE Trans Smart Grid 1(1):57–64. doi:10.1109/TSG.2010.2046346
64. Myagmar S, Campbell R, Winslett M (2008) Security challenges of reconfigurable devices in the power grid. In: Goetz E, Shenoi (eds) Critical infrastructure protection. Springer Berlin Heidelberg, Boston, pp 147–160
65. NIST (2014) NIST framework and roadmap for smart grid interoperability standards, release 3.0 (No. NIST Special Publication 1108r3). National Institute of Standards and Technology, Gaithersburg, p 246. Retrieved from doi:10.6028/NIST.SP.1108r3
66. NISTIR (2014) Guidelines for smart grid cybersecurity: Volume 1: smart grid cybersecurity strategy, architecture, and high-level requirements, Volume 2: privacy and the smart grid, Volume 3: Supportive analyses and references (No. NISTIR 7628, Revision 1 (3 Volumes)). National Institute of Standards and Technology, Gaithersburg, pp 1–668. Retrieved from doi:10.6028/NIST.IR.7628r1
67. Obama BH (2013) Critical infrastructure security and resilience. The White House, Washington. Retrieved from http://www.fas.org/irp/offdocs/ppd/ppd-21.pdf
68. OECD-IEA (2011) Smart grids: technology roadmap. International Energy Agency, Paris
69. Parsons VS (2007) Searching for “Unknown Unknowns”. Eng Manag J 19(1):43–46. doi:10.1080/10429247.2007.11431721
70. Pearson ILG (2011) Smart Grid cyber security for Europe. Energy Policy 39(9):5211–5218
71. Price JWH (1998) Simplified risk assessment. Eng Manag J 10(1):19–23
72. Ray PD, Harnoor R, Hentea M (2010) Smart power grid security: a unified risk management approach. In: 2010 IEEE international carnahan conference on security technology (ICCST), pp 276–285. doi:10.1109/CCST.2010.5678681
73. Rinaldi SM, Peerenboom JP, Kelly TK (2001) Identifying, understanding, and analyzing critical infrastructure interdependencies. IEEE Control Syst 21(6):11–25
74. Rittel HWJ, Webber MM (1973) Dilemmas in a general theory of planning. Policy Sci 4(2):155–169
75. Rocchetta R, Li YF, Zio E (2015) Risk assessment and risk-cost optimization of distributed power generation systems considering extreme weather conditions. Reliab Eng Syst Saf 136:47–61. doi:10.1016/j.ress.2014.11.013
76. Setola R (2010) How to measure the degree of interdependencies among critical infrastructures. Int J Syst Syst Eng 2(1):38–59
77. Skyttner L (2005) General systems theory: problems, perspectives, practice, 2nd edn. World Scientific Publishing Co. Pte. Ltd, Singapore
78. Sun Q, Ge X, Liu L, Xu X, Zhang Y, Niu R, Zeng Y (2011) Review of Smart Grid comprehensive assessment systems. Energy Procedia 12:219–229
79. Theoharidou M, Kotzanikolaou P, Gritzalis D (2011) Risk assessment methodology for interdependent critical infrastructures. Int J Risk Assess Manag 15(2/3):128–148
80. Thissen WA, Herder PM (2003) Critical Infrastructures: state of the art in research and application. Kluwer Academic Publishers, Boston
81. Tokgoz BE (2012) Probabilistic resilience quantification and visualization building performance to hurricane wind speeds (Ph.D.) Old Dominion University, United States – Virginia
82. Tritschler M, Mackay W (2011) UK Smart Grid cyber security. Energy Networks Association, London, pp 1–81
83. Vamanu BI, Gheorghe AV, Katina PF (2016) Critical infrastructures: risk and vulnerability assessment in transportation of dangerous goods, vol 31. Springer International Publishing, Cham
84. van Opstal D (2012) Supply chain solutions for smart grid security: building on business best practices. U.S. Resilience Project, Great Falls, pp 1–36. Retrieved from https://www.controlsystemsroadmap.net/ieRoadmap%20Documents/SupplyChain-Solutions-for-Smart-Grid-Security.pdf
85. Vugrin ED, Turnquist MA, Brown NJK (2014) Optimal recovery sequencing for enhanced resilience and service restoration in transportation networks. Int J Crit Infrastruct 10(3–4):218–246
86. Wang W, Lu Z (2013) Cyber security in the smart grid: survey and challenges. Comput Netw 57(5):1344–1371
87. Wang Y, Ruan D, Gu D, Gao J, Liu D, Xu J, Chen F, Dai F, Yang J (2011) Analysis of Smart Grid security standards. Presented at the 2011 IEEE International Conference on Computer Science and Automation Engineering (CSAE), pp 697–701. Shanghai doi:10.1109/CSAE.2011.5952941
88. Weiss JW, Anderson D (2003) CIOs and IT professionals as change agents, risk and stakeholder managers: a field study. In: Proceedings of the 36th annual Hawaii international conference on system sciences, 2003. doi:10.1109/HICSS.2003.1174639
89. Xenias D, Axon CJ, Whitmarsh L, Connor PM, Balta-Ozkan N, Spence A (2015) UK smart grid development: an expert assessment of the benefits, pitfalls and functions. Renew Energy 81:89–102
90. Yesudas R, Clarke R (2013) A framework for risk analysis in smart grid: perspective based approach. In: Luiijf E, Hartel P (eds) Critical information infrastructures security. Springer International Publishing, Cham, pp 84–95
91. Zhang P, Li F, Bhatt N (2010) Next-generation monitoring, analysis, and control for the future smart control center. IEEE Trans Smart Grid 1(2):186–192
92. Zio E, Aven T (2011) Uncertainties in Smart Grids behavior and modeling: What are the risks and vulnerabilities? How to analyze them? Energy Policy 39(10):6308–6320

Polinpapilinho F. Katina serves as a Postdoctoral Researcher with the National Centers for System of Systems Engineering and is an Adjunct Assistant Professor with the Department of Engineering and Systems Engineering at Old Dominion University (ODU), Norfolk, Virginia. He holds a PhD in Engineering Management and Systems Engineering from ODU. He has research interests in complex system governance, critical infrastructures, and system of systems engineering. He has authored more than 40 peer-reviewed papers to international conferences and journals including, *International Journal of Critical Infrastructure Protection, International Journal of Critical Infrastructures, International Journal of System of Systems Engineering*, and *Requirements Engineering*. He is a co-editor of a critical textbook on “*Infranomics: Sustainability, Engineering Design and Governance.*” His most recent book, “*Critical Infrastructures: Risk and Vulnerability Assessment in Transportation of Dangerous Goods*” is in press.

Charles B. Keating serves as Professor of Engineering Management and Systems Engineering and Director for the National Centers for System of Systems Engineering (NCSOSE) at Old Dominion University. His research focuses on Systems Engineering, System of System of Systems Engineering, Management Cybernetics, and Complex System Governance. He is a Fellow, Past President, and 2015 Sarchet Award recipient from American Society for Engineering Management for his pioneering efforts in the field. His research has spanned defense, security, aerospace, healthcare, R&D, and automotive industries. He holds a B.S. in Engineering from the United States Military Academy (West Point), a M.A. in Management from Central Michigan University, and a Ph.D. in Engineering Management from Old Dominion University. His memberships include the American Society for Engineering Management, the International Council on Systems Engineering, the Institute for Industrial Engineers, and the International Society for System Sciences.

Enrico Zio is the Director of the Chair in Complex Systems and the Energetic Challenge of the European Foundation for New Energy of Électricité de France (EDF) at École Centrale Paris and Supélec and serves a full professor Graduate School in Politecnico di Milano. He holds a BSc in Nuclear Engineering from Politecnico di Milano, Milan, Italy, a MSc in Mechanical Engineering from the University of California, Los Angeles, Los Angeles, California, and PhD in Nuclear Engineering from Politecnico di Milano, Milan, Italy. He also holds a PhD in Nuclear Engineering from Massachusetts Institute of Technology Cambridge, Massachusetts. He serves on a number of editorial boards including *Reliability Engineering and System Safety*, *Journal of Risk and Reliability*, and *International Journal of Computational Intelligence Systems*. His research focuses on characterization and modeling of failure/repair/maintenance behavior of components, complex systems and critical infrastructures.

Adrian V. Gheorghe holds a M.Sc. in Electrical Engineering from the Faculty of Power Engineering, Bucharest Polytechnic Institute, Bucharest, Romania, a PhD in Systems Science/Systems Engineering from City University, London, United Kingdom, an MBA from Academy of Economic Studies, Bucharest, Romania, and a M.Sc. Engineering-Economics, Bucharest Polytechnic Institute, Bucharest, Romania. He serves as Senior Scientist with the European Institute for Risk and Communication Management, Bucharest, Romania and Vice President World Security Forum, Langenthal, Switzerland. He is a Professor of Engineering Management and Systems Engineering and is the Batten Endowed Chair on System of Systems Engineering with the Department of Engineering Management and Systems Engineering at Old Dominion University, Norfolk, Virginia.