The EU Electricity Security Decision-Analytic Framework: Status and Perspective Developments

energies

MDPI

Article

The EU Electricity Security Decision-Analytic Framework: Status and Perspective Developments

Gianluca Fulli [1,*], Marcelo Masera [2], Catalin Felix Covrig [2], Francesco Profumo [3], Ettore Bompard [3] and Tao Huang [3]

1 European Commission, Joint Research Centre, I - 21027 Ispra (VA), Italy
2 European Commission, Joint Research Centre, 1755 ZG Petten, The Netherlands; marcelo.masera@ec.europa.eu (M.M.); catalin-felix.covrig@ec.europa.eu (C.F.C.)
3 DENERG, Politecnico di Torino, 10129 Torino, Italy; francesco.profumo@polito.it (F.P.); ettore.bompard@polito.it (E.B.); tao.huang@polito.it (T.H.)
* Correspondence: gianluca.fulli@ec.europa.eu

Academic Editor: Vincenzo Dovì
Received: 12 January 2017; Accepted: 18 March 2017; Published: 23 March 2017

Abstract: Electricity security, generally referring to a system's capability to provide electricity to its users, is a multi-faceted problem attracting mounting attention from policy makers and scientists around the world. Electricity security encompasses largely different properties based upon the time/geographical scales of the factors affecting electricity delivery; it is challenged by threats surfacing in spheres far beyond the physical one; it involves a myriad of stakeholders spanning manifold disciplines and with considerably different expectations from the electricity commodity or services; it can be studied as a complicated techno-economic problem or as a complex socio-economic problem. All the above reasons, in a framework of changing European Union (EU) and global energy scenarios, render electricity security ever more challenging to assess and critical to safeguard. Against this background, this work presents recommendations to bring science and policy making closer towards evaluating and handling EU electricity security. More in detail, this is done by:

- Characterising electricity security via features at the cross-roads of policy and science.
- Reviewing the electricity security modelling and assessment approaches across sectors.
- Proposing elements for a novel electricity security decision-analytic framework for the EU.
- Contextualising the proposed framework in EU's Energy Union grid design initiatives.

Keywords: electricity security; reliability; vulnerability; policy decision making; Energy Union; integrated analyses

1. Introduction

The EU's energy-related policies pursue three grand objectives: energy security, energy competitiveness/affordability, and energy sustainability. Several policy initiatives have recently addressed the energy security objective: *supply security* is one the five dimensions of the Energy Union; the *European Energy Security Strategy* includes short and long-term measures for critical energy infrastructure; *integration and resilience* are the attributes the EU internal energy market has to attain; *energy import dependency reduction* is fostered via energy efficiency and domestic renewable energy production solutions; *security of network and information systems* is promoted by targeted cooperative initiatives [1–9].

Among all forms of energy, due also to the EU's ambitious energy and climate change policies, electricity seems bound to increase its relative weight. Depending on the scenarios, the share of electricity in the EU's final energy consumption—currently around one fifth—is anticipated to grow

from one fourth in 2030 to one third or above in 2050; additionally, renewable energy—presently covering one fourth of generated electricity—is expected to grow from some half by 2030 up to two thirds and beyond in 2050 [9–11].

The electricity system operations are however challenged by several threats: natural, accidental, malicious and systemic. The latter ones, associated with the low-carbon energy transition, include: the integration beyond the connection of variable renewable energy, the changing role of less variable nuclear and fossil fuel-fired power plants, the constrained peaking and cycling capabilities of all sort of generators, the regulatory-economic factors limiting storage technology deployment, the decentralised actor proliferation in the emerging electricity market arrangements, the rapidly changing flow patterns at cross-border transmission level and at the transmission-distribution interface, the mismatch between market dynamics/transactions and grid operations/flows, the escalating interdependencies between the power system and other (energy, transport, cyber, etc.) systems, the tensions or synergies between the super grid evolution vs. the smart grid (r)evolution [12,13].

Hence, electricity security—generally relating to a system's capability to provide electricity to its users—is progressively moving to the center stage of the political debate and is attracting increasing attention from the scientific community. As a matter of fact, electricity security can be characterised as a multi-faceted, multi-property, multi-stakeholder problem since electricity security: is influenced by events occurring in spheres (geopolitical, regulatory, market, etc.) far beyond the physical one; it exhibits largely different features based upon the time/geographical scales of the phenomena and dynamics affecting the power system; involves a myriad of stakeholders spanning the most diverse disciplines (technical, political, social, etc.); needs to describe both how electricity supply should work and how electricity supply might fail in case of lower probability-higher consequence events; can be studied as a complicated techno-economic problem, still overall ruled by nonlinear equations; can on the other hand be seen as a complex socio-economic problem, hardly representable by closed mathematical formulations [14,15].

This work focuses on (energy and) electricity security, thus one of the three pillars of the EU's energy and climate change strategy, nonetheless touching upon the other two pillars—competitiveness and sustainability—insofar as they impact energy security. The objective is to bring science and policy making closer towards understanding and managing EU's electricity security.

The article is structured as follows: Section 2 describes various properties and features of electricity security; Section 3 examines electricity security models and assessment approaches; Section 4 discusses electricity security stakeholders interactions and actions; Section 5 proposes elements of a novel electricity security decision-analytic framework and contextualises it within the EU's initiatives; and Section 6 provides some conclusions.

2. Electricity Security Characterisation

Electricity security (see also Figure 1) is a multi-faceted problem, since it is [14,15]:

- A *multi-threat* problem. The threats—potentially materialising into adverse events perturbing the power system's delivery mission—can be characterised in terms of impact areas, time duration, provenance (internal or external to the power system), and their intrinsic nature: *natural* (e.g., storms or earthquakes), *malicious* (e.g., cyber or physical attacks), *accidental* (e.g., technical or human errors), and *systemic* (mostly linked to the energy system transition).
- A *multi-time scale* problem. Various time frames need to be considered due to the inherently different electricity security challenges, system performances and actions which can be put in place. The following time frames are considered in this work: *Short-term* (from real time up to tens of minutes), *Mid-term* (up to weeks), *Long-term* (up to years), Very long-term (up to decades).
- A *multi-spatial scale* problem. Electricity security has both local and far-reaching geographical features and this research mostly compares the *EU*, *regional* and national scales.

- A *multi-dimension* problem. The following four overarching dimensions (see Figure 2) of electricity security are identified, and they can be visualised as the physical or virtual corridors across which the electricity commodity/services travel to reach the users:
    - The *infrastructure* dimension, i.e., the electricity value chain;
    - The *source* dimension, i.e., the wider energy system providing the primary sources converted in electricity;
    - The *regulation and market* dimension, i.e., the set of laws, rules, market arrangements and price schemes governing the electricity operations and transactions;
    - The *geopolitical* dimension, i.e., the geographical and political spaces in which decisions on energy infrastructure build and energy resource transportation are made.

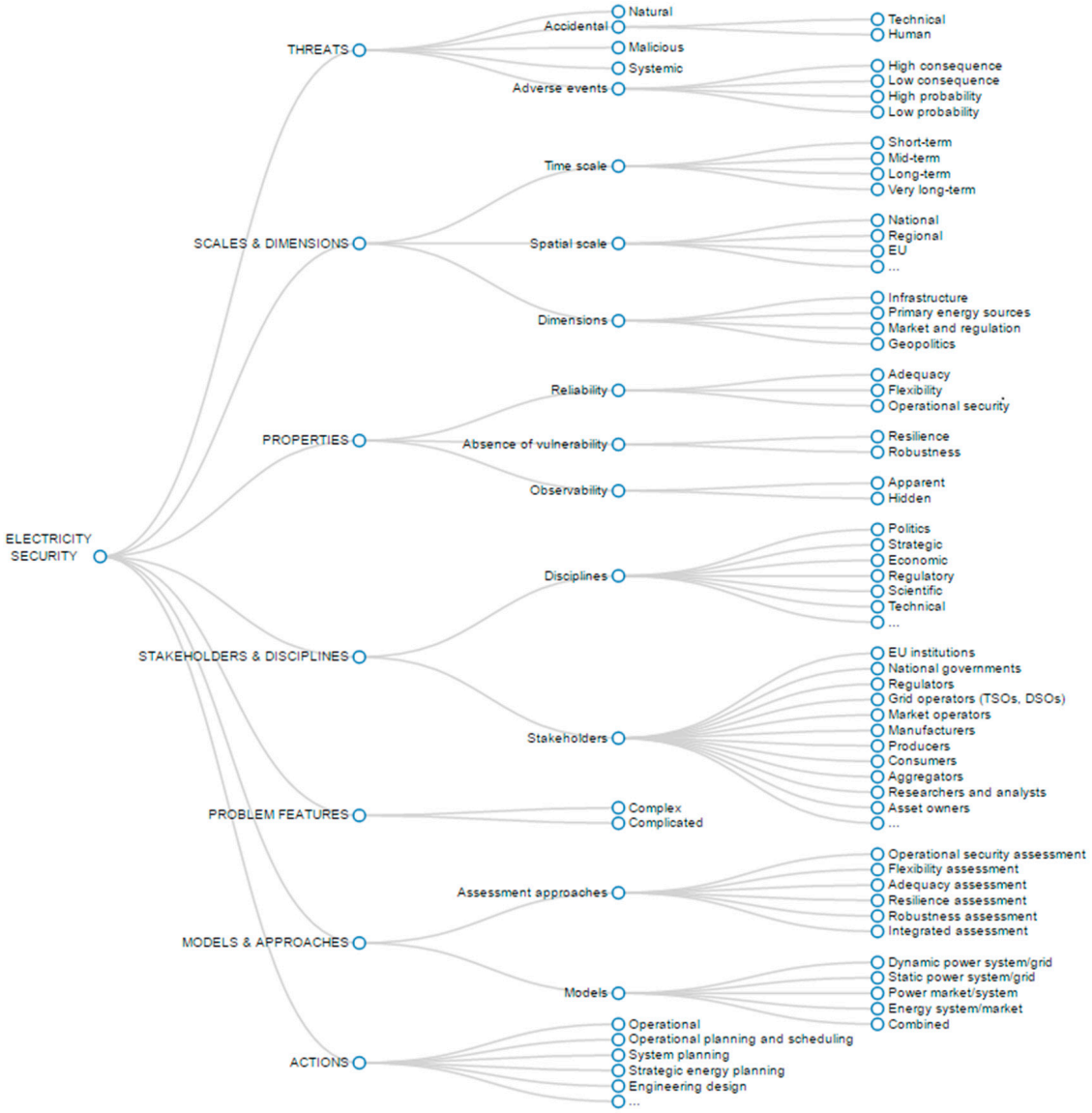

Figure 1. The multi-faceted features of electricity security.

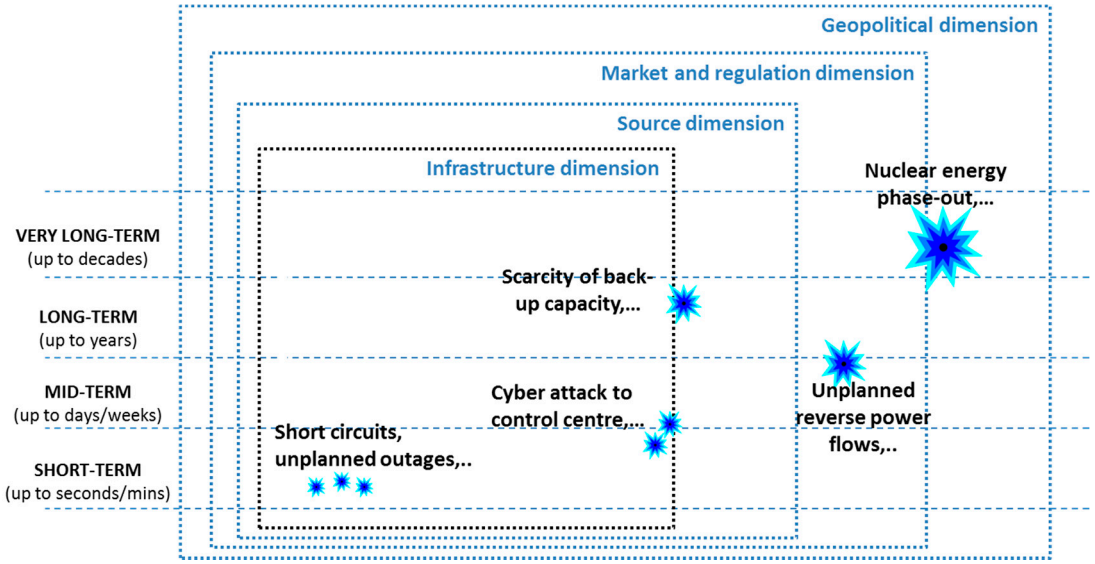

Figure 2. Dimensions of electricity security and examples of strains affecting electricity security.

Additionally, as discussed in detail in Sections 3 and 4, electricity security is:

- A *multi-property* problem. Electricity security can be characterised as a combination of several electricity security properties—presenting though possible overlaps—all having to do with the system's capability to regain a certain performance level after adverse events. Different definitions for electricity security properties can be adopted, also because there is no consensus/standardisation on some of them (flexibility, resilience and robustness). In this work we consider what follows (see Figure 3) [13–19]:
    - *Operational security* is the short-term electricity security linked to events (e.g., short circuits or unplanned outages) mainly occurring in the infrastructure and source dimensions.
    - *Flexibility* is the short-/mid-term electricity security linked to events (e.g., unpredicted variability of renewable energy) mainly occurring in the infrastructure, source and market and regulation dimensions.
    - *Adequacy* is the long-/mid-term electricity security linked to events (e.g., scarcity of back-up capacity) mainly occurring in the infrastructure, source and market and regulation dimensions.
    - *Resilience* is the mid-/long-term electricity security linked to events (e.g., a cyber-attack gradually affecting a control centre's operations, or unplanned reverse power flows from the distribution grids) mainly occurring in the infrastructure, source and market and regulation dimensions.
    - *Robustness* is the long-/very-long term electricity security linked to events (e.g., a policy of nuclear power phase-out or the unilateral decision to interrupt primary energy flows across pipelines) potentially occurring in any dimension: infrastructure, source, market and regulation, and geopolitical.

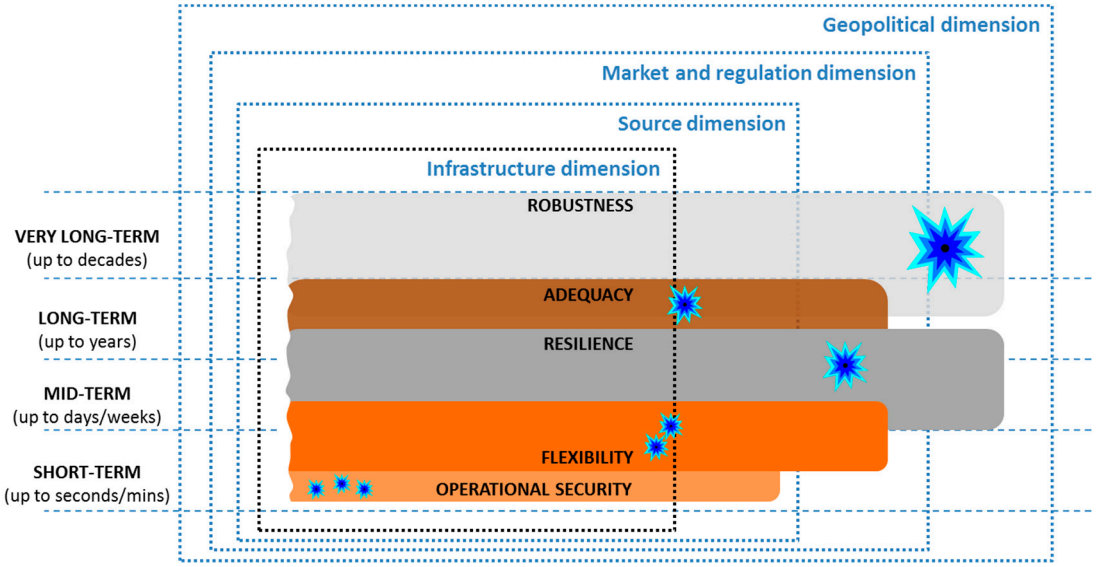

Figure 3. Electricity security dimensions and properties.

The above introduced properties can to a large extent be grouped into two families [20–22]:

- *Reliability*: it mainly covers operational security, flexibility and adequacy.
- (Absence of) *vulnerability*: it mainly covers robustness and resilience (linked to safeguardability).

- A *multi-stakeholder* and *multi-disciplinary* problem. Numerous and diversified players interact in different fields, spatial scales and time frames of the electricity security problem. Electricity security stakeholders with different backgrounds, interests and expertise fields (political, economic, regulatory, scientific, technical, etc.) are involved in observing, assessing and safeguarding electricity security. They include: scientists, academics, project developers, policy decision makers, regulators, practitioners, system operators, market operators, generation companies, asset owners, aggregators, manufacturers, consumers, emerging actors (offering new services and/or proposing new business models) [23–26].
- Both a *complicated* and *complex* problem. Electricity security can "just" be addressed as a complicated problem—the electricity grid is often defined as the most complicated man-made machinery ruled by nonlinear equations—or as a complex problem, where very diverse actors interact in multiple dimensions (infrastructure, source, market and regulation, geopolitical) and layers (component, communication, information, function and business) and whose collective/systemic behaviour can be hardly described by closed mathematical formulations.
- A *multi-model* problem. Several models are deployed, either independently or in combination, and they can be grouped in the following clusters: *dynamic power system/grid models*, *static power system/grid models*, *power market/system models*, *energy system/power market models* [15].
- A *multi-assessment approach* problem. Mirroring the grouping of the electricity security properties, three main electricity security assessment approaches are identified:
  - *Reliability* methodologies (generally addressing operational security, flexibility and adequacy), focusing on the ability of the system to accomplish its intended function [21].
  - *Vulnerability* methodologies (generally addressing the lack of resilience and robustness), focusing on the inability of the system to withstand strains and on the effects of the consequent failures [27–29].
  - Solutions for *integrated analyses*, like those based upon *cost-benefit analyses*, *multi-criteria analyses* and *indicators*, are also deployed [19].

- A *multi-action* problem. Decision makers can promote/deploy several courses of actions to prevent, mitigate and respond to electricity security threats. Depending on the time scale, stakeholders can resort to *operational* actions, *operational planning and scheduling* actions, **system** *planning* actions, *strategic energy planning* (and *engineering design*) actions to safeguard electricity security [15,16].

3. Electricity Security Models and Approaches

As introduced in Section 2, the electricity security models (see also Table 1) are here clustered against the time horizon, the time granularity, the electricity security dimensions and the domains of the electricity value chain they primarily cover [30–36]:

- The *dynamic power system/grid models* provide a detailed short-term description of the power system, grid and protection components. They mainly target the infrastructure dimension of electricity security, i.e., they portray as endogenous factors/variables belonging to the electricity value chain. The typical time horizon is up to seconds (minutes) and the time steps are in the order of milliseconds or their fractions. The dynamic power system/grid models necessarily embed a static model of the power system/grid (see the next bullet point).
- The *static power system/grid models* offer detailed (component by component) representations of the power grid. The static power system/grid models mainly target as endogenous the infrastructure dimension (some elements of the source dimension might be included). The typical time horizon is one or several years. The time steps largely vary depending on the very different models within this cluster (power flow, topological, graph-based, etc.): they might not even be specified (when studying system snapshots or topological features) or they could typically be hours or fractions of hours.
- The *power market/system models* generally represent the demand-supply equilibrium, and might use simplified assumptions to describe the grid ("single node" or more detailed representations). They mainly consider as endogenous factors within the infrastructure and the primary energy source dimensions, as well as some aspects of the market and regulation dimension. The typical time horizon is one to several years and the typical time steps are hours/weeks (or weeks/months).
- The *energy system/power market models* represent the whole energy system and selected portions of the power system/market. They target the source and the market and regulation dimensions (the latter, as well as the geopolitical dimension, may be exogenous to the model). The typical time horizon is up to years or decades and the typical time steps are weeks/months (i.e., a few ten time slices per year).

Table 1. Clustering of electricity security models.

	Features						
Model Cluster	**Time Horizon**				**System Representation Detail**		
	Short Term	**Mid Term**	**Long Term**	**Very Long Term**	**Energy System**	**Power Market**	**Power System/Gird**
Dynamic power system/grid models	X	-	-	-	-	-	H
Dynamic power system/grid models	X	X	X	-	-	M	H
Power market/system models	X	X	X	-	-	H	M/l
Energy system/power market models	-	X	X	X	H	H/m	-

Figure 4 shows model clusters mapped to electricity security properties, indicating the time horizon and the electricity value chain domains covered. The approaches employed to assess the

different electricity security properties make progressively use of model combinations rather than single models. Particularly, static power system/grid models are the main ingredient of nearly every electricity security assessment. Models can be coupled—hard linked or soft-linked—in different manners (sequentially; iteratively; or heuristically), across different scales (e.g., time, geographical) and across different dimensions/sectors (power transmission and distribution, electricity and gas, energy and water, etc.). Properly capturing electricity security properties through models requires finding the trade-off between computational costs, modelling detail needs, model combination advantages and analysis scope [34–37].

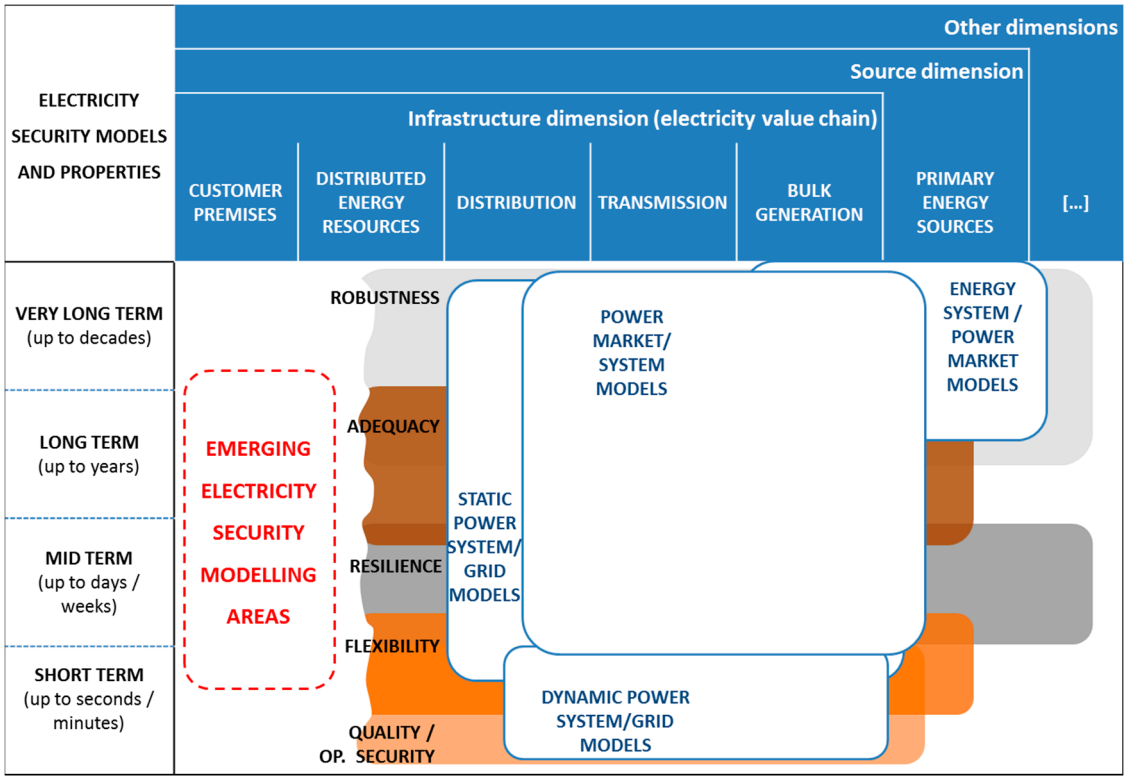

Figure 4. Mapping of power system security models to electricity security properties.

Two major groups of electricity security assessment approaches are considered [20–22]:

- The *reliability assessment approaches*—generally addressing operational security, flexibility and adequacy—target the capacity of the system to perform its intended role and are traditionally used in power system operation, design and planning. Two main methods are employed: deterministic and probabilistic; the deterministic methods are simpler, requires little data and are somehow easier to communicate to policy decision makers; however, they cannot account for inherent stochastic features (e.g., load and renewable energy forecast errors); the probabilistic methods, increasingly more used, are based on the risk models which combine system components reliability performances. Reliability analyses provide insights on the likely system behaviour, in terms of indices defining frequency, duration and magnitude of the expected failures. This information allows decision makers to understand the general capacity of the system to accomplish its intended role and what are some of the causes generating system unreliability. Reliability targets—typically based on historical patterns and common practices—are generally fixed ex ante. Since reliability analyses focus on the likely system behaviour, events assessed to have low probability/frequency of incidence do not grandly—or at all—impact the results (rare events can cover a large fraction of the consequences on the system) [38,39].

As more and more renewable energy is in the system, flexibility and balancing requirements should be analysed with finer time resolutions. There are several flexibility sources (such as transmission, hydropower, thermal plants, or district heating) but current models are not able of representing them accurately without becoming extremely complex, and therefore integrated approaches relying on suites of tools are needed. These new approaches must improve the representation of the decision making processes, consumer behaviour, and the emerging business models, without neglecting market aspects, but these elements lead to even more complex models. Flexibility studies are due to steer the embedding of stability/operational security studies into the decision making/planning process. Flexibility in electrical networks is also naturally connected to the market and the regulatory rules that help in defining procedures. Flexibility requirements are bringing energy/electricity system planning and operation decision-making much closer than in the past. Linking energy system/power market models with one or more of the other three model clusters is a recurring way of addressing flexibility issues [37–42].

- The *vulnerability assessment approaches*—generally addressing the lack of resilience and robustness—focus on the weakness of the network to withstand strains and on the effects of the consequent failures. Reliability analyses illustrate the probable behaviour of the system, but fail to detect less likely scenarios with higher consequences—these are targeted by vulnerability analyses. These latter ones include emerging approaches used within critical infrastructure management. Vulnerability analyses are less concerned with understanding the role of frequency/probability of failures; their emphasis is more on the identification of system flaws accessible to unknown threats, following a system failure or strain. Aspects like threats interdependence, adverse events/failure propagation cannot be easily captured by reliability analyses [43–51].

Over the last years, complex networks theory appeared as a new framework to study electricity as a complex system, relying upon graph-based representations of a power system, essentially capturing its structure. Complex network theory applied to power grids concentrated on three issues: structure, dynamics and evolution. A complete characterisation of a network's topology is motivated by the expectation to better understand its evolutionary, dynamical and functional behaviour. However, capturing the power system dynamics via complex network theories is compounded by the facts that network components may have different dynamic behaviours and flows are often highly variable in space and time. Some of the power engineering areas where complexity concepts have potential for application (also in combination with agent-based modelling) are vulnerability and resilience property assessment, smart grids and interdependent system analysis [52–56].

Even if the borders are blurred, reliability and vulnerability assessment approaches can provide different insights for policy decision making. For cases related to external exposures (e.g., bad weather or malicious threats) or unpredicted failure propagation mechanisms the supposition of failure independence is not suitable. This could infer that the chances of multiple parallel failures projected by the reliability analyses can indicate distorted results. Hence, quantitative risk and reliability assessments need to be flanked by vulnerability analyses to get a thorough understanding of the power system security performances. Trusting only reliability analyses to support decision making could lead to designing a reliable though vulnerable system [20].

The challenge is to understand whether a further level of combination and integration of electricity security approaches is viable and useful for the decision making process. Integrated assessment practices include the following families [19,35]:

- *Cost-benefit analyses.* A balance should exist between the benefits and the costs of improving the security of the energy system. Ideally, also from a societal perspective, as many benefits and costs as possible should be monetised so that the interests of all the stakeholders are properly reflected. However monetary valuation can hardly be used when there is no thorough knowledge on the security threats, the severity of the impact and the prevention possibilities. Other approaches

may be used (e.g., multi-criteria analyses and indicators) when not enough information is available [57,58]

- *Multi-criteria analyses.* Both qualitative and quantitative aspects using this type of analysis (one example would be the analytical hierarchy process). If evaluation targets only the quantitative data, ranking weights can be used to create a complex indicator (see next bullet point) [59,60]
- *Indicators.* Also named complex or composite indicators, they are created by merging into a single index the results from several quantitative indicators. This index value can be read as a representation of an overall level of 'insecurity'. A scoring system is needed as well as a weighting system to generate an index value [39,59–61]

Electricity security aspects related to the growing interdependences within the electricity domains and between different energy systems (gas, heat, etc.) need to be thoroughly studied. Smart grids promise to radically change the way power system is operated, designed and planned. Studying security of supply of smart grids not only requires interlinking transmission and distribution, but changing the prospective from the electricity commodity supply to the electricity service provision [46].

One single model cannot embed and describe all the electricity security aspects because the power system has various dimensions (e.g., time, location, size), is mostly nonlinear, and has both discrete and continuous behaviours. Using the models separately and independently may trigger the risks of adopting contradictory assumptions and endorsing conflicting solutions on how to upgrade electricity security [19,37].

Advanced computational capabilities (including real time simulators) technologies would allow analysts to perform more detailed and accurate system simulations and speed up the response to adverse circumstances, thus reducing the inability to avoid failures and enabling the addition of dynamic analysis into real-time grid operations. These technologies would be especially effective when combined to visual analytics. Although most of the data generated in the electricity sector is considered as proprietary, both because it includes sensitive industrial information about company operations and because it might be used for malicious purposes, producing and sharing representative, synthetic data that is adequate to reflect real operations/performances would foster cooperative electricity security analyses [62–64].

4. Electricity Security Stakeholder Interactions and Actions

The main actors from the policy decision making and the scientific communities, intervening and interacting in different spatial scales, are discussed below [3–6,25,26]:

- At *national level*, even if each EU Member State is still largely in charge of the energy security assessment and safeguard, stakeholders' roles and responsibilities greatly differ. Member States assess different electricity security risks, consider different crisis scenarios, take different emergency measures at different times in response, roles and responsibilities differ. The main electricity security actors are the governmental/regulatory bodies and the Transmission System Operators (TSOs). Member States behave very differently to prevent, prepare and manage crisis situations and national rules and practices tend to disregard what happens across borders. The TSOs own very detailed datasets and dynamic and static models of the national transmission system under their responsibility. The further modelling moves away from grids towards market/energy systems, the larger is the number of actors, including market operators, having a stake (in terms of data ownership) and playing a role (in terms of assessment perspectives). Electricity security models are used for supporting decision making across all the electricity security actions—operation, operational planning and scheduling, system planning, strategic energy planning. The scientific community (R&D actors) frequently contribute to electricity security analyses and propose methodological improvements, however it generally lacks reliable data for the models. The whole range of electricity security analyses is conducted, both on reliability (operational security, flexibility, adequacy) and vulnerability (resilience and robustness)

aspects. Electricity models, from the time frame viewpoint, tend to be more and more combined or at least soft linked; probabilistic approaches (vs. deterministic ones) are increasingly used—but their results are not necessarily embedded in the decision making process—for reliability analyses, whereas vulnerability analyses rely upon the most diversified (and not necessarily sophisticated) approaches, also because there is no common understanding of electricity crisis situations and scenarios [20,23,36].

Possible improvement areas include: better interlinking models, covering more domains/subsystems/systems like: the electricity distribution grid, the gas system, the heat system etc; encouraging utilities to fully incorporate innovative approaches—as e.g., those based on advanced probabilistic/complex system techniques, generally proposed by the R&D community—in the decision making process.

- At the *regional (cross-national) level*, there are emerging actors which started performing electricity security analyses and actions: particularly, the Pentalateral Energy Forum (PLEF), the Nordic Contingency Planning and Crisis Management Forum (NordBER) and other nascent regional operational initiatives (see Figure 5), including the Coordination of Electricity System Operators (CORESO), the Transmission System Operator Security Cooperation (TSC) and—beyond the EU—the Security Coordination Center (CSC). Also, R&D actors are less active than at national and EU level as the regional scale represents a rather recent EU development and entails different cooperation efforts. Electricity models are quite detailed and (compared to the ones at the national scale) better capture the cross-border static and dynamic aspects of the region under study. The electricity security models are used more to support operational planning & scheduling actions and system planning actions (since operational actions and strategic energy planning actions are beyond the current remit of these regional bodies). As for the electricity security analyses, reliability assessments seem to have priority on vulnerability analyses: even though the network codes set out harmonised technical principles for operation planning and scheduling processes (required to anticipate real time operation security issues), common/harmonised administrative and political approaches to help national authorities to prevent and manage crisis situations in co-operation with each other are missing in most EU's regions and countries. Time-wise, selected electricity security models are better linked and probabilistic approaches (vs deterministic ones) begin to be used for reliability analyses [65–70]

Possible improvement areas include: better defining roles and responsibilities of the actors (so that the even accurate and innovative analyses can better support the decision making process), expanding security analyses in the vulnerability and risk preparedness areas and in modelling the interfaces with other energy systems.

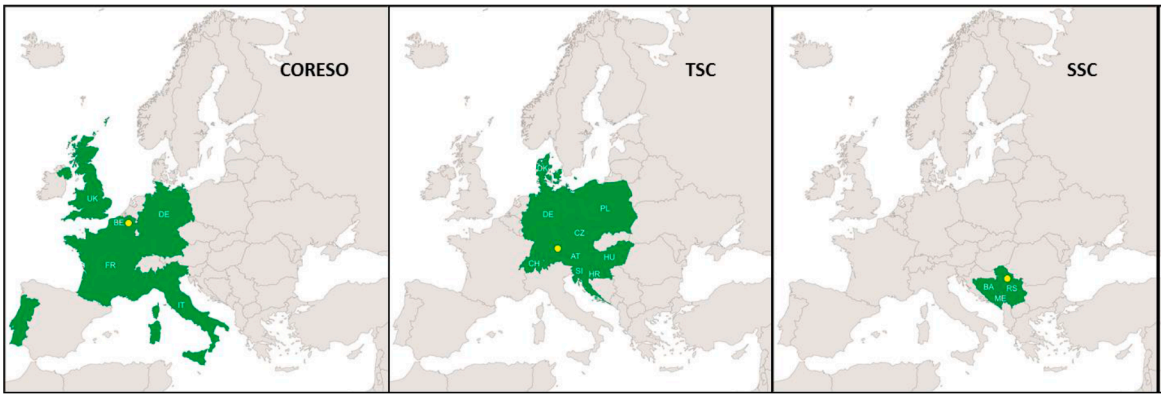

Figure 5. Regional operational initiatives in Europe [67–69].

- At the *EU level*, the main actors are the European Network of Transmission System Operators for Electricity (ENTSO-E), the Agency for the Cooperation of Energy Regulators (ACER) and the European Commission. ENTSO-E is tasked to perform EU-wide analysis and coordinated national/regional studies. ENTSO-E is progressing well in combining primarily static power system/grid models with power market/system models. As explained above for the regional scale, the electricity security models are used for supporting decision making (especially) on operational planning and scheduling actions and system planning actions, (rather than on) operational actions and strategic energy planning actions. In the scientific area, several R&D projects produce advanced models although with partially representative datasets (in the absence of formal agreements with the system operators/data owners). Probabilistic approaches (vs. deterministic ones) begin to be proposed in the reliability assessment area, particularly for power system adequacy and flexibility. As for vulnerability, the Critical Infrastructure Protection initiatives have mainly encouraged bilateral instead of truly supra-national cooperation. At this level, the visibility/observability of dynamics/issues occurring at regional/local level is somewhat limited [71–74]

Possible improvement areas include: deeper assessment of issues occurring at the transmission-distribution interfacing issues, whereas first trials for interlinking gas and electricity models are ongoing, streamlining the modelling interactions and the assessment processes between the EU-wide and the regional scale, advancing the dynamic representation of the whole transmission system (e.g., via real-time simulation) targeting the emerging smart/super electricity systems' challenges and tensions. Figure 6 frames the electricity security actions which can be put in place to maintain/increase the electricity security properties and with respect to the different domains of the electricity supply chain.

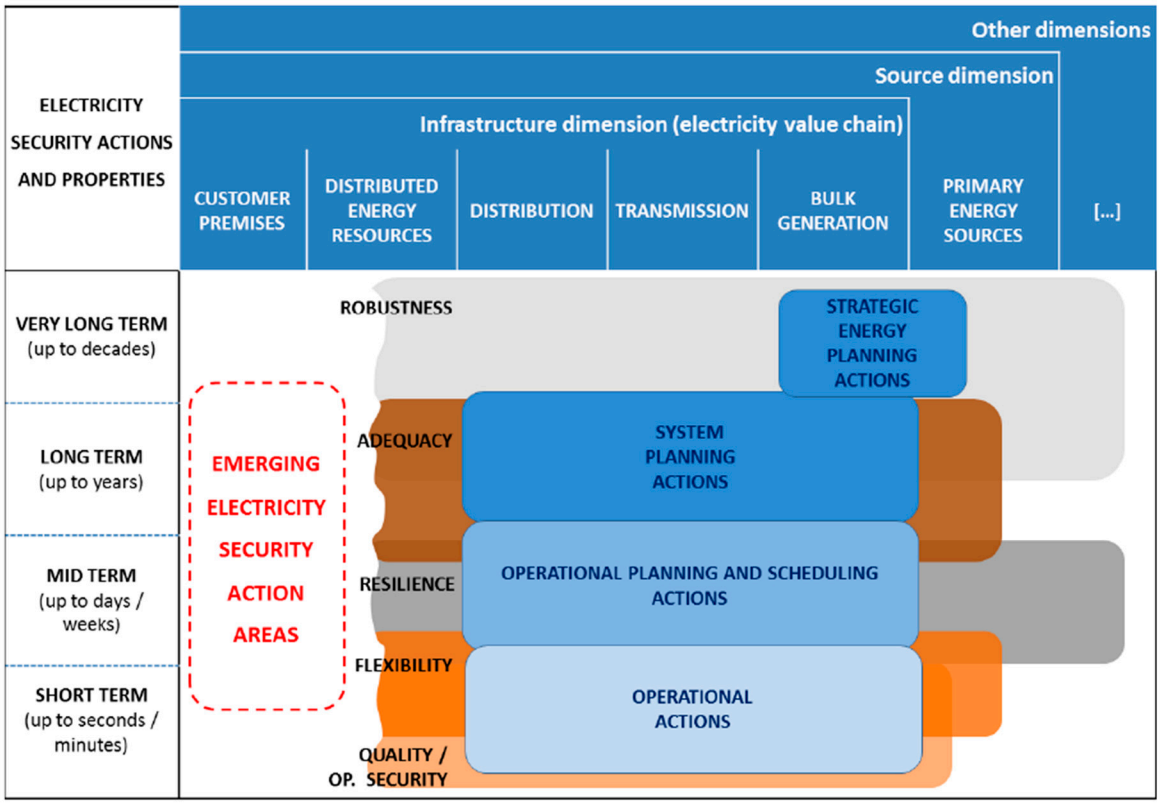

Figure 6. Mapping of electricity security attributes and actions.

The main electricity security safeguard actions in the different time scales include what follows [12–16]:

- *Operational actions* (generally short-term): transient/dynamic stability management, pre-fault and post-fault remedial actions (based on contingency analyses) and system balancing.
- *Operational planning and scheduling actions* (generally mid-term): forecasting, power scheduling, ancillary service procurement, outage coordination and asset management.
- *Planning actions* (generally long-term): system (network) optimisation, enhancement and expansion.
- *Strategic energy planning actions* (generally long-term): strategic energy planning/provision and wide ranging policy and regulatory initiatives (impacting the energy system beyond the electricity system).

In summary, electricity security decision-analytic processes are still a patchwork of practices, rules and methods interacting at different geographical scales. Furthermore, science and policy stakeholders in the electricity security sphere do not generally smoothly work together: whereas electricity security models and analysis are pervasively enshrined in the industry decision making process (particularly in the operational and planning phases), the same does not generally hold for the connections between scientific/technical electricity security analysis and the policy decision making process (especially in the strategic energy planning and risk preparedness areas). There are several reasons for this difficult relation: the political and scientific/engineering communities speak different languages; policy making is a mixture of politics, facts and values, whereas science primarily contributes to facts only; technical results may be too complex to interpret and utilise [42,75].

Increasing electricity security calls for greater cooperation and a more collective approach, since national choices and decisions over energy markets, sources and infrastructure have immediate or unanticipated cross-EU security implications. The local and the regional scales of electricity security should be bridged to allow stakeholders developing common assessment methodologies and discussing cross-cutting electricity security issues and solutions. In the current geopolitical context, the regional scale appears as a strategic playing field where identifying synergies and reaching compromises between the EU and the Member States energy policy orientations. By using a common assessment framework and consistent evaluation methodologies, stakeholders can better compare studies and strategies and they can make the results understandable and replicable. Cooperative decision making and action implementation would improve the overall electricity security performances, thanks to stronger synergies of balancing resources ranging from interconnectors, conventional/renewable generation capacity, storage and demand response [3–6].

5. A Novel Electricity Security Decision-Analytic Framework

Building upon the electricity security aspects and challenges analysed so far, the following elements for a novel decision-analytic framework (see also Figure 7) are identified [15].

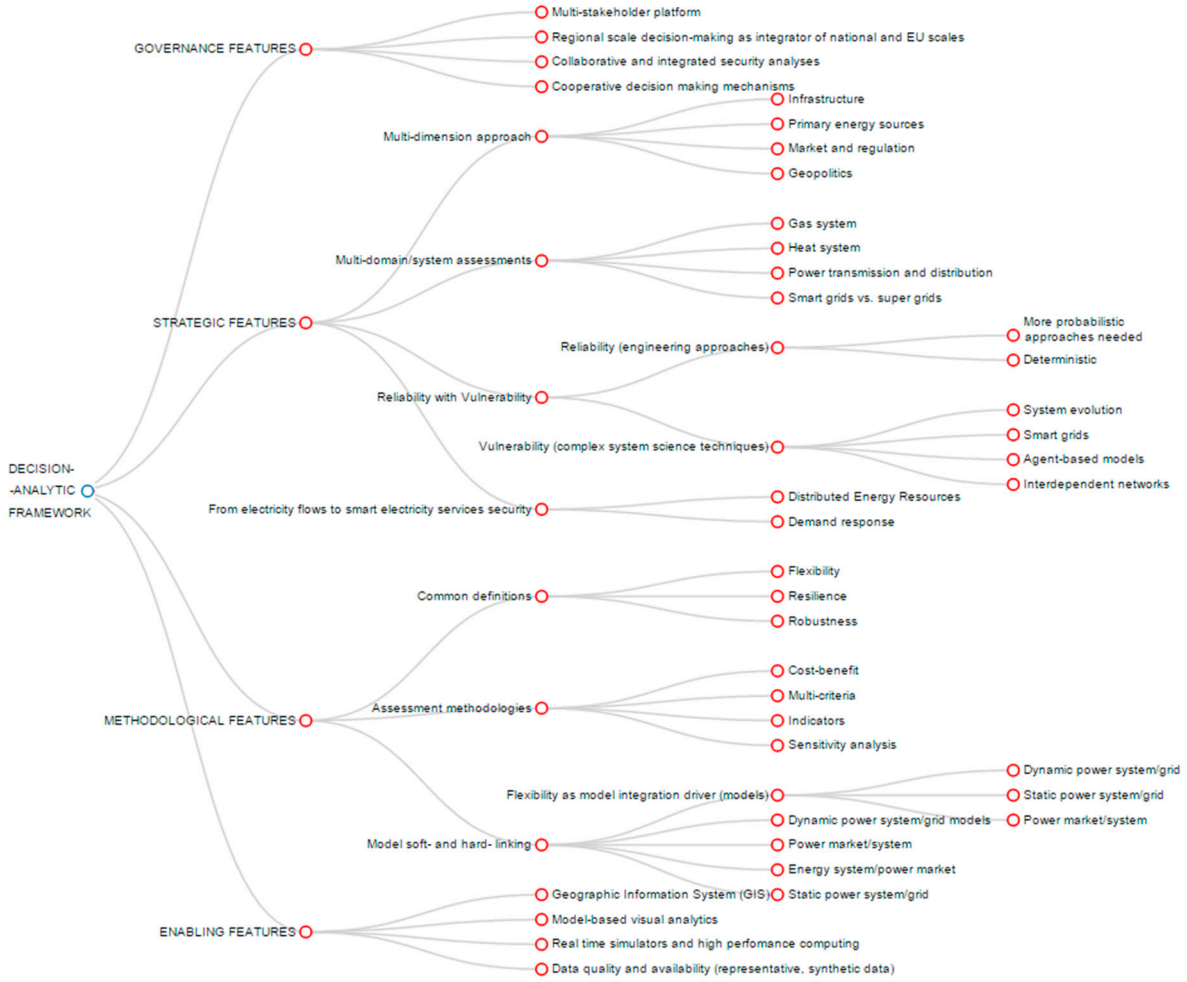

Figure 7. Novel electricity security decision-analytic framework.

5.1. Governance Features

- *Multi-stakeholder platforms*, with proper governance and structured interaction mechanisms, should be further developed at all spatial scales—*national*, *regional* and *pan-European*—to carry out harmonised assessments and concerted actions in the electricity security field.
- The *regional scale of decision making* should be fostered and streamlined. The current regional pilots offer valuable experience and lessons learned; still, harmonising the geographical/physical boundaries of the regions, given the host and the variable geometry of the initiatives currently in place, is a prerequisite.
- More *collaborative and integrated security analyses*—again at a wider geographical scale (than the traditional national one)—should be performed to combine different electricity security aspects and properties. Improved electricity security analyses should take into account the different perspectives/interests of the electricity system stakeholders. Additionally, given the interdependence of the main energy policy objectives—security, affordability and sustainability—these integrated security analyses, even if focused on electricity security, should be framed in a wider socio-economic context.

- *Cooperative decision making mechanisms*, steering the coordinated implementation of concerted actions stemming from the integrated security analyses, should be established. Even if the best spatial scale would be the EU-wide or continental one, since addressing security issues does not just entail solving technical problems but also letting several actors and decision makers interact effectively, it may turn out as more doable to implement regional (cross-national) electricity security analyses-actions, also considering the evolving EU policy framework.

5.2. Strategic Features

- *All the electricity security dimensions should be assessed: infrastructure, sources, market and regulation, and geopolitics*. The electricity security assessment methodologies should be better able to observe and interpret the interactions of the electricity value chain system with the wider energy system and the other dimensions.
- *Smart/super grid and multi-energy carrier systems assessments should be intensified*. The modelling efforts in emerging areas—like distributed energy resources, end user's demand response—shall be boosted with the aim to integrate these aspects in wider national/regional models. On the same note, the modelling efforts and the electricity security analysis on super grids shall be interlinked with the modelling efforts on smart grids since major tensions are emerging at the transmission-distribution interface.
- *Electricity security analyses should expand from covering electricity flow/commodity security to including electricity service security*. This could help identifying different means and pathways to safeguard security and identify different threats and opportunities throughout the supply chain (e.g., linked to demand response).
- Emerging *vulnerability assessment* approaches—increasingly *based on complex network science*—should be promoted further, also at the regional scale, to complement reliability assessment approaches—focusing more on how the system should work.
- A deeper *interplay* between *complex network and engineering approaches* should be pursued as both disciplines have their distinguishing features and might be instrumental to assessing different aspects of electricity security.

5.3. Methodological Features

- Stakeholders should agree upon *common definitions* of crucial electricity security properties—particularly: *flexibility, resilience and robustness*—which (differently from other attributes like operational security and adequacy) are not consented at the EU level.
- *Cost-benefit analyses* should be preferred to *multi-criteria analyses* whenever doable in reliability studies. However this methodology can hardly be used in vulnerability analyses.
- *Multi-criteria analyses and indicators should be used* to help in decision making under uncertainty **if** economic/financial information is not available. Multi-criteria analyses can be used to analyse both qualitative and quantitative aspects. Composite indicators, aggregating data—coming from model outputs and/or expert opinions—over time and/or space, are generally easier to communicate but might conceal and/or underestimate specific security properties.
- *Sensitivity analyses should be embedded in security analyses*. Sensitivity analyses can indeed help systemically explore different scenarios and range variations of factors/variables and can help understanding how initial assumptions and boundary conditions influence the results of the models.

- Energy system/power market *models*, Power market/system models, Static power system/grid models and Dynamic power system/grid models would need to be utilised—and, depending on cases, *soft* or *hard linked*—in so far as they address complementary electricity security aspects and properties.
- *Flexibility* should be increasingly used as *driver for modelling integration* in the reliability analysis area. A consented flexibility assessment approach can help identify the required modifications to system operations and increase renewable energy integration and acceptance.
- *Probabilistic approaches* should complement and—in specific assessment areas (e.g., flexibility and adequacy of power systems with high penetration of renewables)—largely supplant the deterministic approaches *when assessing reliability aspects* of the electricity security problem.

5.4. Enabling Features

- Advanced model-based and *Geographic Information System* (GIS)-based *visual analytics* should be extensively adopted to support the interactions with the policy makers while presenting, analysing and interpreting electricity security scenarios/results.
- Decision makers and analysts should take advantage of *supercomputers*, *real time simulators* and *parallel processing* to develop detailed full-scale models of the power grids, and possibly make the high performance computing technology available for real-time daily operations.
- *Reliable, representative datasets* should be *made available* to researchers and analysts.

Finally, selected elements of this novel electricity security decision-analytic framework are contextualised in the European Union's power system planning process (see Figure 8). It is here noted that the security aspects represent just one of the angles (the others being affordability and sustainability) of the electricity system and cost-benefit analyses. One can distinguish three main parallel though interacting decision-analytic processes at different spatial scales: the institutionalised ones at the EU-wide scale and at the national level and the emerging one at the regional level. The Scenario Outlook & Adequacy Forecast (SOAF) and the Ten-Year Network Development Plan (TYNDP) are among the main products of the EU-wide assessment effort. The national development plans and adequacy analyses are already increasingly contributing to these EU-wide products. The regional interface between the EU-wide and national decision-analytic processes can be strengthened by formalising the role of regional security entities (e.g., the regional operational entities) [70–74].

As for the models deployed (from top to bottom), along with the ones (energy system/power market, power market/system and static power system/grid models) already featuring in the current planning process, also dynamic power system/grid models are utilised for integrated reliability studies. Indeed studying flexibility issues requires getting closer to real time monitoring and assessing of the system performances: flexibility requirements are hence bringing energy/electricity system planning and operation decision-making much closer than in the past [70–74].

The revised electricity security decision-analytic process also needs to encompass two different layers for the reliability and vulnerability analyses, fundamentally conducted by the same actors, and potentially combined through integrated assessment methodologies.

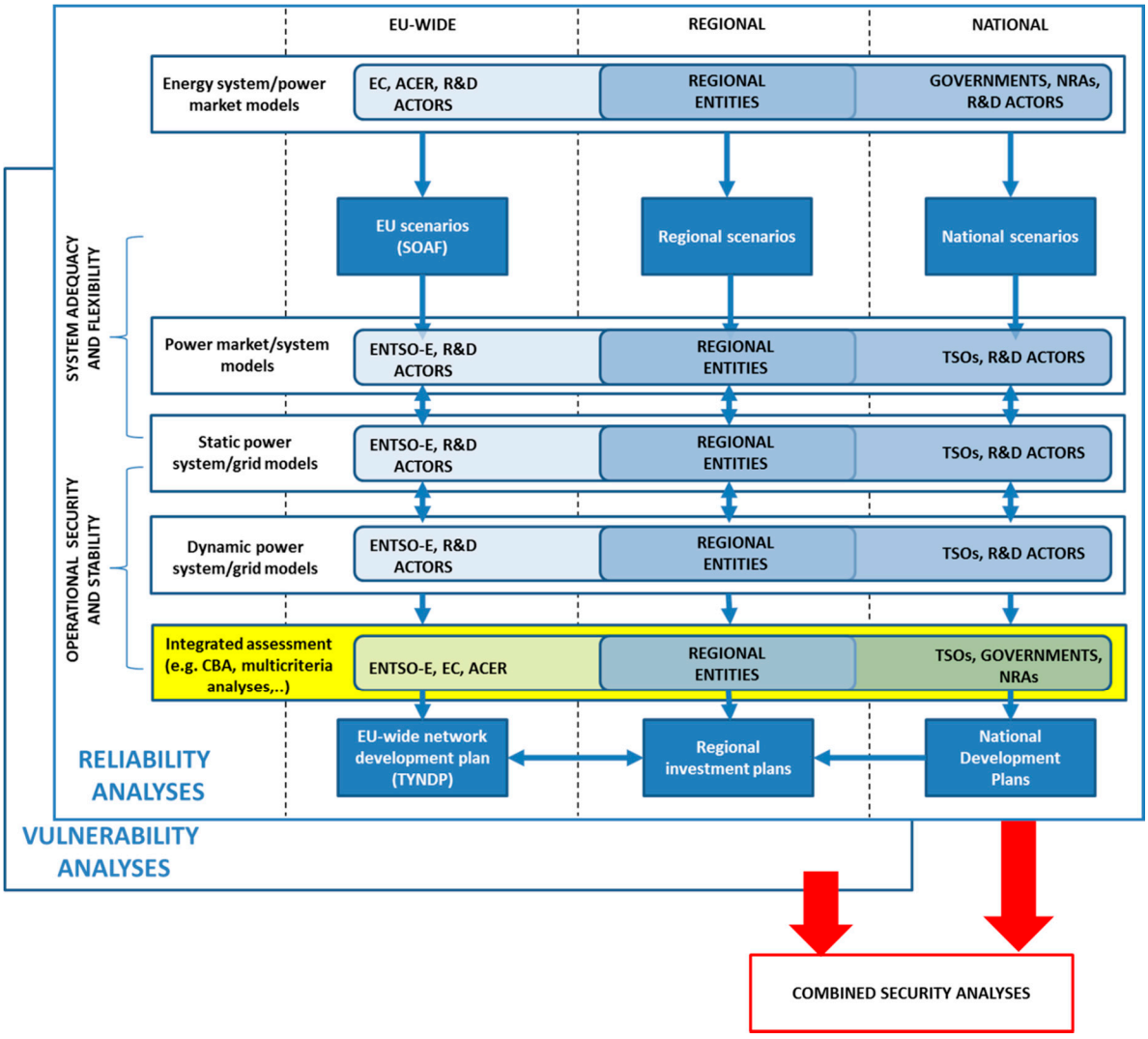

Figure 8. Perspective electricity security analytic-decision process (planning stage).

6. Conclusions

This work explored electricity security in its multi-faceted features, with a special focus on the political-scientific interfacing issues and the reliability-vulnerability components of electricity security. Electricity security characterises the power system performances beyond security of electricity supply: besides covering reliability properties, it includes aspects like risk preparedness, vulnerability, resilience and robustness. Reliability analyses—encompassing operational security and flexibility/adequacy analyses—provide crucial input to decision makers although they do not capture the whole spectrum of security events/aspects (even when based on probabilistic techniques).

Despite some nascent regional and reinforced EU-wide initiatives, several electricity security decision/analytic tasks are prevalently carried out at the EU Member State level; however, national choices and decisions over energy markets, sources and infrastructure have obvious cross-national security implications. Furthermore, electricity security stakeholders—including policy makers, practitioners and scientists—frequently display considerably different understanding or expectations from the electricity commodity and services.

Against this background, this paper proposed a revised decision-analytic framework with four categories of features: governance features, ranging from multi-stakeholder and region-based platforms to collaborative and integrated security analyses; strategic features, focusing on the need to analyse

and tackle all the electricity security dimensions, as well as the multi-energy carrier, multi-service and vulnerability aspects of electricity delivery; methodological features, including better definitions, tailored cost-benefit analyses, multi-criteria analyses and sensitivity analyses; enabling features, encompassing the tools, capabilities and data required for thorough electricity security assessment.

Beside structuring the interaction and cooperation of the institutional electricity security decision-analytic actors, a strengthened collaboration of all those parties—having roles/stakes or competences/skills in the electricity security business/field—would help reinforcing the knowledge required to address the electricity security conundrum in the evolving EU society.

Eventually, electricity security safeguard in a changing energy system is beyond the scope of any single person or entity and is at the same responsibility of all the stakeholders. Only by promptly reaching a certain level of collective knowledge and collaboration society can fully benefit from—someone argues can successfully survive—this transition.

Author Contributions: G. Fulli performed the literature review, conceived the decision-analytic framework and lead-authored the paper; C. F. Covrig contributed to perform the literature review, produced most of the graphics and reviewed the paper; E. Bombard supervised the analytical work and the paper drafting and review; M. Masera and T. Huang provided insights in the energy security field and contributed to the paper review; F. Profumo supervised the overall paper drafting and production. All authors discussed the results and contributed to writing the paper.

Conflicts of Interest: The authors declare no conflicts of interest.

Disclaimer: This work is based on doctoral research carried out in cooperation by Politecnico di Torino and the European Commission's Joint Research Centre. The information and views set out in this publication are those of the authors and do not necessarily reflect the official opinion of the European Union. Neither the European Union institutions and bodies nor any person acting on their behalf may be held responsible for the use which may be made of the information contained therein.

References

1. European Commission. *Energy Union Package, A Framework Strategy for a Resilient Energy Union with a Forward-Looking Climate Change Policy*; European Commission: Brussels, Belgium, 2015.
2. European Commission. *A Policy Framework for Climate and Energy in the Period from 2020 to 2030*; COM(2014) 15 Final; European Commission: Brussels, Belgium, 2014.
3. European Commission. *European Energy Security Strategy*; COM(2014) 330 Final; European Commission: Brussels, Belgium, 2014.
4. European Parliament and Council of the European Union. *Directive 2005/89/EC Concerning Measures to Safeguard Security of Electricity Supply and Infrastructure Investment*; European Parliament and Council of the European Union: Brussels, Belgium, 2005.
5. European Commission. *Proposal for a Regulation of the European Parliament and of the Council on Risk-Preparedness in the Electricity Sector and Repealing Directive 2005/89/EC*; COM(2016) 862 Final; European Commission: Brussels, Belgium, 2016.
6. European Commission. *European Programme for Critical Infrastructure Protection*; COM(2006) 786 Final; European Commission: Brussels, Belgium, 2006.
7. European Parliament and Council of the European Union. *Directive 2009/72/EC Concerning Common Rules for the Internal Market in Electricity*; European Parliament and Council of the European Union: Brussels, Belgium, 2009.
8. European Parliament and Council of the European Union. *Directive (EU) 2016/1148 Concerning Measures for a High Common Level of Security of Network and Information Systems across the Union*; European Parliament and Council of the European Union: Brussels, Belgium, 2016.
9. European Commission. *EU Energy Trends to 2030*; European Commission: Brussels, Belgium, 2009–2010.
10. European Commission. *Energy Roadmap 2050*; COM(2011) 885 Final; European Commission: Brussels, Belgium, 2011.
11. European Commission. *State of the Energy Union*; COM(2015) 572 Final; European Commission: Brussels, Belgium, 2015.

12. Panteli, M.; Mancarella, P. The Grid: Stronger, Bigger, Smarter: Presenting a Conceptual Framework of Power System Resilience. *IEEE Power Energy Mag.* **2015**, *13*, 58–66. [CrossRef]
13. Bompard, E.; Fulli, G.; Ardelean, M.; Masera, M. It's a Bird, It's a Plane, It's a ... Supergrid! Evolution, Opportunities, and Critical Issues for Pan-European Transmission. *IEEE Power Energy Mag.* **2014**, *12*, 40–50.
14. Bompard, E.; Huang, T.; Wu, Y.; Cremenescu, M. Classification and trend analysis of threats origins to the security of power systems. *Int. J. Electr. Power Energy Syst.* **2013**, *50*, 50–64. [CrossRef]
15. Fulli, G. Electricity Security: Models and Methods for Supporting the Policy Decision Making in the European Union. Ph.D. Thesis, Politecnico di Torino, Turin, Italy, 2016.
16. International Education Association (IEA). *Learning from the Blackout*; IEA: Paris, France, 2005.
17. Gracceva, F.; Zeniewski, P. A systemic approach to assessing energy security in a low-carbon EU energy system. *Appl. Energy* **2014**, *123*, 335–348. [CrossRef]
18. Hosseini, S.; Barker, K.; Ramirez-Marquez, J.E. A Review of Definitions and Measures of System Resilience. *Reliab. Eng. Syst. Saf.* **2016**, *145*, 47–61. [CrossRef]
19. Johansson, M.B.; Nilsson, L.J. Assessing energy security: An overview of commonly used methodologies. *Energy* **2014**, *73*, 1–14.
20. Johansson, J.; Hassel, H.; Zio, E. Reliability and vulnerability analyses of critical infrastructures: Comparing two approaches in the context of power systems. *Reliab. Eng. Syst. Saf.* **2013**, *120*, 27–38. [CrossRef]
21. Allan, R.; Billinton, R. Probabilistic assessment of power systems. *Proc. IEEE* **2000**, *88*, 140–162. [CrossRef]
22. Sarewitz, D.; Pielke, R., Jr.; Keykhah, M. Vulnerability and risk: Some thoughts from a political and policy perspective. *Risk Anal.* **2003**, *23*, 805–810. [CrossRef] [PubMed]
23. European Commission. *Review of Current National Rules and Practices Relating to Risk Preparedness in the Area of Security of Electricity Supply—Final Report*; European Commission: Brussels, Belgium, 2014.
24. Agency for the Cooperation of Energy Regulators (ACER). *Regional Initiatives Status Review Report*; ACER: Ljubljana, Slovenia, 2014.
25. Council of European Energy Regulators (CEER). *Security of Electricity Supply Report*; CEER: Brussels, Belgium, 2004.
26. Pierre, I. *Security of Electricity Supply—Roles, responsibilities and experiences within the EU*; Eurelectric–Union of the Electricity Industry: Brussels, Belgium, 2006.
27. Kröger, W.; Zio, E. *Vulnerable Systems*; Springer: London, UK, 2011.
28. Aven, T. On some recent definitions and analysis frameworks for risk, vulnerability, and resilience. *Risk Anal.* **2011**, *31*, 515–522. [CrossRef] [PubMed]
29. Cuadra, L.; Salcedo-Sanz, S.; del Ser, J.; Jiménez-Fernández, S.; Geem, Z.W. A Critical Review of Robustness in Power Grids Using Complex Networks Concepts. *Energies* **2015**, *8*, 9211–9265. [CrossRef]
30. Deane, J.P.; Gracceva, F.; Chiodi, A.; Gargiulo, M.; Gallachóir, B.P.Ó. Assessing power system security. A framework and a multi model approach. *Int. J. Electr. Power Energy Syst.* **2015**, *73*, 283–297.
31. Söderholm, P. Fuel flexibility in the West European power sector. *Resour. Policy* **2000**, *26*, 157–170. [CrossRef]
32. Denholm, P.; Hand, M. Grid Flexibility and Storage Required to Achieve Very High Penetration of Variable Renewable Electricity. *Energy Policy* **2011**, *39*, 1817–1830. [CrossRef]
33. Chaudry, M.; Ekins, P.; Ramachandran, K.; Shakoor, A.; Skea, J.; Strbac, G.; Wang, X.; Whitaker, J. *Building a Resilient UK Energy System*; UK Energy Research Centre: London, UK, 2011.
34. Poncelet, K.; Delarue, E.; Duerinck, J.; Six, D.; D'haeseleer, W. *The Importance of Integrating the Variability of Renewables in Long-Term Energy Planning Models*; KU Leuven: Leuven, Belgium, 2014.
35. Ventosa, M.; Baillo, Á.; Ramos, A.; Rivier, M. Electricity market modeling trends. *Energy Policy* **2005**, *33*, 897–913. [CrossRef]
36. Foley, A.M.; Gallachóir, B.P.Ó.; Hur, J.; Baldick, R.; McKeogh, E.J. A strategic review of electricity systems models. *Energy* **2010**, *35*, 4522–4530. [CrossRef]
37. González, H.; Castello, P.R.; Sgobbi, A.; Nijs, W.; Quoilin, S.; Zucker, A.; Thiel, C. Addressing flexibility in energy system models. *JRC Sci. Policy Rep.* **2015**. [CrossRef]
38. Aien, M.; Hajebrahimi, A.; Fotuhi-Firuzabad, M. A comprehensive review on uncertainty modeling techniques in power system studies. *Renew. Sustain. Energy Rev.* **2016**, *57*, 1077–1089. [CrossRef]
39. Martínez-Anido, C.B.; Bolado, R.; de Vries, L.; Fulli, G.; Vandenbergh, M.; Masera, M. European power grid reliability indicators, what do they really tell? *Electr. Power Syst. Res.* **2012**, *90*, 79–84. [CrossRef]

40. O'Sullivan, J.; Rogers, A.; Flynn, D.; Smith, P.; Mullane, A.; O'Malley, M. Studying the Maximum Instantaneous Non-Synchronous Generation in an Island System—Frequency Stability Challenges in Ireland. *IEEE Trans. Power Syst.* **2014**, *29*, 2943–2951.
41. Holttinen, H.; Tuohy, A.; Milligan, M.; Lannoye, E.; Silva, V.; Müller, S.; Sö, L. The Flexibility Workout: Managing Variable Resources and Assessing the Need for Power System Modification. *IEEE Power Energy Mag.* **2013**, *11*, 53–62. [CrossRef]
42. Koppelaar, R.H.E.M.; Keirstead, J.; Shah, N.; Woods, J. A review of policy analysis purpose and capabilities of electricity system models. *Renew. Sustain. Energy Rev.* **2016**, *59*, 1531–1544.
43. Baldick, R.; Chowdhury, B.; Dobson, I.; Dong, Z.; Gou, B.; Hawkins, D.; Huang, H.; Joung, M.; Kirschen, D.; Li, F.; et al. Initial review of methods for cascading failure analysis in electric power transmission systems. In Proceedings of the IEEE PES CAMS Task Force on Understanding, Prediction, Mitigation and Restoration of Cascading Failures, Power and Energy Society General Meeting, Pittsburgh, PA, USA, 20–24 July 2008; pp. 1–8.
44. Dobson, I.; Carreras, B.A.; Newman, D.E. A loading dependent model of probabilistic cascading failure. *Probab. Eng. Inf. Sci.* **2005**, *19*, 15–32. [CrossRef]
45. Dobson, I.; Carreras, B.A.; Lynch, V.E.; Newman, D.E. An initial model for complex dynamics in electric power system blackouts. In Proceedings of the 34th Hawaii International Conference on System Sciences, Maui, HI, USA, 3–6 January 2001; pp. 710–718.
46. Jansen, J.C.; Seebregts, A.J. Long-term energy services security: What is it and how can it be measured and valued? *Energy Policy* **2010**, *38*, 1654–1664. [CrossRef]
47. Haimes, Y.Y.; Crowther, K.; Horowitz, B.M. Homeland security preparedness: Balancing protection with resilience in emergent systems. *Syst. Eng.* **2008**, *11*, 287–308. [CrossRef]
48. O'Brien, G.; Hope, A. Localism and energy: Negotiating approaches to embedding resilience in energy systems. *Energy Policy* **2010**, *38*, 7550–7558.
49. Yusta, J.M.; Correa, G.J.; Lacal-Arantegui, R. Methodologies and applications for critical infrastructure protection: State-of-the-art. *Energy Policy* **2011**, *39*, 6100–6119. [CrossRef]
50. Carreras, B.A.; Lynch, V.; Dobson, I.; Newman, D.E. Complex dynamics of blackouts in power transmission systems. *Chaos* **2004**, *14*, 643–652. [CrossRef] [PubMed]
51. Bompard, E.; Napoli, R.; Xue, F. Analysis of structural vulnerabilities in power transmission grids. *Int. J. Crit. Infrastruct. Prot.* **2009**, *2*, 5–12.
52. Rosas-Casals, M.; Bologna, S.; Bompard, E.; D'Agostino, G.; Ellens, W.; Pagani, G.A.; Scala, A.; Verma, T. Knowing power grids and understanding complexity science. *Int. J. Crit. Infrastruct.* **2015**, *11*, 4–14. [CrossRef]
53. Hines, P.; Cotilla-Sanchez, E.; Blumsack, S. Do topological model provide good information about electricity infrastructure vulnerability? *Chaos* **2010**, *20*, 033122. [CrossRef] [PubMed]
54. Buzna, L.; Issacharoff, L.; Helbing, D. The evolution of the topology of high-voltage electricity networks. *Int. J. Crit. Infrastruct.* **2009**, *5*, 72–85. [CrossRef]
55. Pagani, G.A.; Aiello, M. The Power Grid as a complex network: A survey. *Phys. A Stat. Mech. Appl.* **2013**, *392*, 2688–2700. [CrossRef]
56. Rinaldi, S.M.; Peerenboom, J.P.; Kelly, T.K. Identifying, understanding, and analyzing critical infrastructure interdependencies. *IEEE Control Syst.* **2001**, *21*, 11–25. [CrossRef]
57. Forsten, K. *The integrated grid—A Benefit-Cost Framework*; Electric Power Research Institute (EPRI): Palo Alto, CA, USA, 2015.
58. *European Network of Transmission System Operators (ENTSO-E), Guidelines for Cost Benefit Analysis of Grid Development Projects*; ENTSO-E: Brussels, Belgium, 2015.
59. Giordano, V.; Vasiljevska, J.; Vitiello, S. *Evaluation of Smart Grid Projects within the Smart Grid Task Force Expert Group 4*; JRC Scientific and Policy Report; Publications Office of the European Union: Brussels, Belgium, 2013.
60. Portugal-Pereira, J.; Esteban, M. Implications of paradigm shift in Japan's electricity security of supply: A multi-dimensional indicator assessment. *Appl. Energy* **2014**, *123*, 424–434.
61. Andzsans-Balogh, K.; Gregor, A.; Habis, H.; Kaderják, P.; Kerekes, L.; Kiss, A.; Mezősi, A.; Pató, Z.; Szolnoki, P.; István Tóth, A.I.; et al. *Security of energy supply in Central and South-East Europe*; Aula Kiadó: Budapest, Hungary, 2011.

62. Huang, Z.; Nieplocha, J. Transforming power grid operations via high performance computing. In Proceedings of the 2008 IEEE Power and Energy Society General Meeting—Conversion and Delivery of Electrical Energy in the 21st Century, Pittsburgh, PA, USA, 20–24 July 2008; pp. 1–8.
63. Nga, D.V.; See, O.H.; Quang, N.; Xuen, C.Y.; Chee, L.L. Visualization Techniques in Smart Grid. *Smart Grid Renew. Energy* **2012**, *3*, 175–185.
64. National Academies of Sciences, Engineering, and Medicine. *Analytic Research Foundations for the Next-Generation Electric Grid*; The National Academies Press: Washington, DC, USA, 2016.
65. Pentalateral Energy Forum (PLEF). *Second Political Declaration*; PLEF: Brussels, Belgium, 2015.
66. *Nordic Contingency Planning and Crisis Management (NCPCM), The Nordic Forum for Emergency Matters Regarding the Power Sector*; NCPCM: Laxå, Sweden, 2005.
67. Coordination of Electricity System Operators (CORESO). Available online: www.coreso.eu (accessed on 11 January 2017).
68. Transmission System Operator Security Cooperation (TSC). Available online: www.tscnet.eu (accessed on 11 January 2017).
69. Security Coordination Centre (SCC). Available online: www.scc-rsci.com (accessed on 11 January 2017).
70. European Commission. *Ecorys, ECN, DNV GL, Options for Future European Electricity System Operation*; European Commission: Brussels, Belgium, 2015.
71. European Network of Transmission System Operators (ENTSO-E). *Ten Year Network Development Plan*; ENTSO-E: Brussels, Belgium, 2014.
72. European Network of Transmission System Operators (ENTSO-E). *Regional Cooperation and Governance in the Electricity Sector*; Policy Paper; ENTSO-E: Brussels, Belgium, 2016.
73. European Network of Transmission System Operators (ENTSO-E). *Target Methodology for Adequacy Assessment*; Updated Version after Consultation; ENTSO-E: Brussels, Belgium, 2014.
74. European Network of Transmission System Operators (ENTSO-E). *Scenario Outlook & Adequacy Forecast*; ENTSO-E: Brussels, Belgium, 2015.
75. Rodilla, P.; Batlle, C. Security of electricity supply at the generation level: Problem analysis. *Energy Policy* **2012**, *40*, 177–185. [CrossRef]