UNIVERSITY OF
CAMBRIDGE

Cambridge Working Papers in Economics

Issues and Options in the Economic Regulation of European Network Security

Tooraj Jamasb and Rabindra Nepal

CWPE 1425 & EPRG: 1405

UNIVERSITY OF CAMBRIDGE | Energy Policy Research Group

Issues and Options in the Economic Regulation of European Network Security

EPRG Working Paper 1405

Cambridge Working Paper in Economics 1425

Tooraj Jamasb and Rabindra Nepal

Abstract : Incentive regulation needs to adapt to the emerging changes in the operating environment of the electricity networks and take into account the security of these. This paper assesses the current issues and options in economic regulation of network security across the European electricity systems. An output-oriented incentive regulatory approach combines the efficiency promoting mechanisms in a revenue cap framework with output-based incentives such as better provision of network security. Thus, incentive regulation is destined to move from pursuing the optimal to being more practical. The RIIO regulatory framework in the UK and the service quality regulation in Italy provide good examples of application of output-based regulation. We also propose an output-based approach for regulation of network security, which accounts for the risks from natural, accidental and malicious threats. We conclude that regulation for network security may also involve looking beyond economic network regulation and focus on the wider security policy and regulation interface considering the risks facing the electricity networks.

Keywords network security, exceptional events, incentive regulation, output-based

JEL Classification L51 ; L94 ; L98

Contact tooraj.jamasb@durham.ac.uk; r.nepal@uq.edu.au
Publication March 2014
Financial Support European Commission, FP7, SESAME Project

Issues and Options in the Economic Regulation of European Network Security

***Tooraj Jamasb* ***
Durham University Business School, UK

Rabindra Nepal* *
School of Economics, University of Queensland

Abstract

Incentive regulation needs to adapt to the emerging changes in the operating environment of the electricity networks and take into account the security of these. This paper assesses the current issues and options in economic regulation of network security across the European electricity systems. An output-oriented incentive regulatory approach combines the efficiency promoting mechanisms in a revenue cap framework with output-based incentives such as better provision of network security. Thus, incentive regulation is destined to move from pursuing the optimal to being more practical. The RIIO regulatory framework in the UK and the service quality regulation in Italy provide good examples of application of output-based regulation. We also propose an output-based approach for regulation of network security, which accounts for the risks from natural, accidental and malicious threats. We conclude that regulation for network security may also involve looking beyond economic network regulation and focus on the wider security policy and regulation interface considering the risks facing the electricity networks.

Keywords: network security, exceptional events, incentive regulation, output-based

JEL Classification: L51; L94; L98

Acknowledgement: *The authors acknowledge the financial support of the FP7-security project cofounded by the European Commission. The views expressed herein are those of the authors and can therefore in no way be taken to reflect the official position of the European commission. The usual disclaimer applies.*

*Durham University Business School, Mill Hill Lane, Durham, DH1 3LB, United Kingdom, Email: tooraj.jamasb@durham.ac.uk, Phone: +44 (0) 191 3345463.

**Energy Economics and Management Group, School of Economics, Colin Clark Building, Level 6 Rm. 652, Email: r.nepal@uq.edu.au, Phone: +61 7 334 60798.

1. Introduction

The response of the liberalised and regulated European electricity markets to supply security challenges remains a major preoccupation considering the supply security problems resulting from inadequacies in the regulatory framework or the shortcomings in the markets (Arriaga, 2007; CEER, 2012). The electricity networks in Europe face the risk of significant damages and threats from high impact and low frequency (HILF) events. Such threats are partly due to the changing global security landscape. However, the likelihood and impact of threats are also exacerbated due to the growing market integration and cross-border interconnections among member countries in the creation towards a single electricity market.

The HILF events can occur from natural causes (such as natural calamities and severe weather conditions), accidents (such as explosions and nuclear accidents) and human conceived malicious threats (such as terrorist attacks, sabotage, vandalism and coordinated cyber-attacks) that can halt the functioning of the modern electricity systems (Hammond and Waldron, 2008; NERC, 2010). These events are characterised as having low probability of occurrence but with high potential to cause significant and long-term catastrophic damage to the power system and other essential services in the wider economy. The risks from HILF events can transcend other operational and reliability risks facing the electricity networks due their magnitude of impact (Nepal and Jamasb, 2013).

Increasing the number and capacity of interconnections in the European electricity markets can facilitate the transmission of HILF risks from one transmission node to other nodes through the interconnector and create a 'ripple effect' or 'cascading failures' of economic, social and environmental damages post-events (Billington and Allan, 1988; Douglas, 2005). For example, supply side failures led to rolling blackouts, voltage reductions and public appeals for emergency conservation in California, Ontario, Chile, New Zealand, Brazil and India while major network failures in the Eastern and Western U.S. and Italy caused significant disruptions (Bailek, 2004). These technical failures can be attributed to investment inadequacy in new transmission and distribution infrastructures resulting from the design of regulatory framework for generating large-scale investments leading to insufficient response to forecasts of the required levels of investments. Hence, it is questionable if competitive electricity markets and incentive regulation of networks is consistent with achieving acceptable levels of electricity supply security (Joskow, 2007).

As such, the issue of how to treat and incentivise supply security investments under evolving regulatory framework is crucial and is gaining heightened importance among the EU energy regulators. This is because the capabilities of the electricity systems to embrace the risks and threats facing the power networks are closely linked to the future of network regulation. This paper reviews the different approaches to regulate and promote network security in the light of the changing nature of network regulation from an input-based approach to an emerging output-based incentive regulation in Europe. We conceptualise network security as encompassing the conventional elements of electricity supply security such as short-run operational reliability; commercial reliability and long-run resource adequacy (see Joskow, 2007) along with security threats from natural, accidental and malicious (or exceptional) events facing the networks (see Nepal and Jamasb, 2013) in the remainder of the paper.

This paper assumes that addressing the network security challenges is a regulatory matter while network security can, alternatively, be viewed as an aspect of quality of service that can be achieved by incentivising the investments and innovation in the regulation of networks. A useful way to improve network security through regulation is by incorporating network security in the quality of service regulation. However, due to the nature of the network security, it is difficult to design an optimal regulatory framework or mechanism that accounts for all economic, technical, natural and malicious risks faced by the electricity networks. Designing an optimal and workable incentive laden regulatory mechanism that induces the networks to deliver the welfare-maximising levels of network security (even the conventional quality of service) is a difficult task (Sappington, 2005; Joskow, 2011) and beyond the scope of the present paper.

The remainder of the paper is structured as follows. Section 2 provides an overview of the investment challenges facing the liberalised electricity markets in Europe. Section 3 discusses the current approaches to network security regulation and their subsequent effects on investment and innovation. The different regulatory options to address network security are discussed in section 4 as network regulation is changing from an input-based to an output-based incentive regulation approach. Section 5 presents an output-based incentive regulation framework to regulate network security. Section 6 concludes the paper.

2. Liberalisation and Investment Challenges

Liberalisation and economic integration of the electricity sector must constantly adapt to emerging challenges in the operating environment of the electricity networks alongside improving their cost efficiency. Much of the existing electricity networks in Europe is aged and in need of replacement and upgrades (European Commission, 2006). The transition towards low-carbon economies and decarbonisation of energy sectors necessitates that the electricity networks undergo profound technical changes to accommodate the growing share of renewables and the continuing smart technological innovations in meeting the demand for a secure supply of electricity.

The future electricity networks need to move from a passive to an active operation and design providing opportunity for end-users to participate as actors in the market by actively responding to real-time price signals and no longer basing their consumption decisions in the realm of inelastic demand (Joskow, 2012). The advent of smart grids and mobile electricity consumers (electromobility) has also signalled the demise of the long held assumption on the technological maturity of the electricity networks (Schiavo et al., 2013). These technical changes needs to be pursued within the context of electricity market integration and increased interconnections across the European electricity systems.

The need to (a) replace existing network infrastructures, (b) expand network capacity to accommodate the growing share of distributed generation and renewable energy sources and (c) develop innovative infrastructures for greater end-user participation requires significant replacement and new investments and innovations in the transmission and distribution networks for securing electricity supply. However, the lack of adequate and timely investments has been a major regulatory and policy concern across the European electricity markets that have undergone a broader paradigm shift from state-ownership and vertical integration towards more decentralised and unbundled structures, competition, independent regulation and private ownership during the last two decades (Jamasb and Pollitt, 2008; Sanyal and Cohen, 2009; Jamasb and Pollitt, 2011; Newbery, 2012).

Investment in the regulated electricity networks respond to the overall regulatory framework as well as associated institutional constraints (Crew and Kleindorfer, 1996; Vogelsang, 2002;

2006). The networks as natural monopolies are regulated in terms of price, entry and access regulation (Newbery, 2002). Investments and innovation in the networks are not governed by market mechanisms as investment decisions do not rely on expected returns exceeding the cost of capital incurred. The under-investment in network infrastructures can aggravate the existing and new network challenges and risks facing the electricity systems.

However, policies and measures to improve network security need to be effective from a policy viewpoint as well as being economically efficient. This task is considerably complicated by the 'low-probability and high-impact' nature of the accidental, malicious and natural threats. There are two pathways to address the network security challenges. The first pathway is achieved through regulatory agencies and economic regulation of networks by incentivising practices, investments, and innovations that enhance network security. The second path is to treat network security outside of economic regulation and at the security policy level where governments, as central planners, assume responsibility and instruct the sector in this matter. This is because network security is a public good with positive external effects and networks also networks exhibit monopoly characteristics. Hence, market failure that occurs justifies government intervention. We adopt the first pathway and review the different regulatory approaches to address and promote network security given the likely change in the nature of incentive regulation from an input-based approach to an output-based approach.

3. Current Approaches to Economic Regulation of Network Security

The main role of an independent sector regulator is to act as the guardian of public interest (Armstrong et al., 1994). Hence, the regulator aims to ensure that network utilities provide network security while pricing the associated services efficiently and equitably. These goals should be consistent with satisfying a break-even (or budget-balance) constraint for the regulated networks by allowing them to cover the costs of providing adequate security while restraining their ability to create productive and allocative inefficiencies through market power (Joskow, 2008). At the same time, the regulator is constrained to consider that the regulated charges are adequate to allow the networks to undertake new investments and innovation pertaining to network security while offering them incentives for maintaining and improving the production efficiency.

Incentive regime often aims to mimic the discipline of competitive markets in the regulation of network security (Jamasb and Pollitt, 2007). However, regulators are neither fully aware nor unaware about the cost, quality and demand characteristics of the network companies – i.e. regulators have *imperfect and incomplete* information relative to the regulated firms. This *information asymmetry* between the regulator and regulated companies creates potential problems associated with *'hidden action' (or moral hazard)* and *'hidden information' (or adverse selection)* in regulating network security, which, as a result, the regulator should effectively address in the mechanism design process. Using the principal-agent analysis, Laffont and Tirole (1993) showed that using a menu of cost-contingent regulatory contracts with different cost sharing provisions could be optimal considering the information asymmetry between the principal (the regulator) and the agent (the regulated network).

The regulator is also constrained to avoid the bankruptcy of the regulated network company implying that the regulated prices should account for the possibility of high network security costs under conditions of information asymmetry. Hence, the allowed revenue (R) received by the regulated network company is the sum of a fixed component independent of actual network security costs (α) and the actual (or realized network security cost) (C) less the cost-savings undertaken by the regulated company. The cost sharing parameter (β) captures the extent to which the regulated network company's allowed revenue responds to realized network security costs only known to the utility. The sharing parameter is the incentive parameter and provides an opportunity for the firm to deviate from the actual network security costs by varying its effort level only known to the firm and increase profits.

$$\mathbf{R = \alpha + C - \beta C = \alpha + (1- \beta) C} \qquad \mathbf{(1)}$$

Under pure cost-based regulation, $\alpha = 0$ and $\beta = 0$ implying that the allowed revenue of the network company is directly linked to its realized network security costs. The firm has no incentive to reduce its network security costs by exerting higher effort levels, which the regulator cannot evaluate. A strict cost-based regulation does not provide any incentives for the utility to engage in network security innovation in liberalised electricity sectors as there are no additional profits accruing to the network company by undertaking efficiency improvements through innovation. This is the case even when the companies do not bear any cost risk given that additional network security costs would be reflected in higher tariffs

(Bauknecht, 2011). On the contrary, cost savings arising from undertaking network security innovation such as by performing research and development (R&D) would lead to lower tariffs confirming that pure cost-based mechanisms do not give any incentive for network companies to become cost efficient.

However, the provision of regulatory lag in practice means that the efficiency gains achieved through undertaking risk free R&D spending in network security can be retained and firms can earn extra profits for a period. The tariffs will be adjusted and the cost savings are passed to the consumers at the regulatory review. This provides an incentive for the network company to pursue innovation under cost-based regulation (Bailey, 1974; Mayo, 1988). Hence, the impact of cost-based regulation on innovation related to network security can be positive overall as security related R&D spending becomes risk-free. No previous study has directly examined this relationship in the context of a liberalised electricity market structure across Europe.

Under a pure price-based regulation, $\alpha = C^*$ and $\beta = 1$ implying that the allowed revenue of the network company is not linked to its actual network security cost. The company has full incentive to pursue cost savings and expand its profit. C* is the regulator's assessment of the 'efficient' costs of the highest type (Joskow, 1974; 2011). The regulator can apply a Bayesian or non-Bayesian mechanism to determine the value of C*. Modern non-Bayesian mechanism to estimate C* usually involve benchmarking using the Data Envelopment Analysis (DEA) and Stochastic Frontier Analysis (SFA) techniques (Coelli and Perelman, 1999).

The separation of underlying own costs of the regulated network company with the allowed price provide strong incentives for inducing greater managerial effort and thereby improve cost efficiency to increase profits. The individual company and its managers have the highest powered incentives to fully exploit their cost opportunities by exerting the optimal amount of effort and eliminate the costs associated with managerial moral hazard (Brennan, 1989). However, the regulator needs to set an ex-ante price that is adequate to satiate the companies with high network security costs given that the balanced budget constraint provides the firms with opportunities to extract rents at the expense of the consumers and the society. The cost-reducing incentives imply that price-based mechanism is efficient for short-run efficiency in operating cost of network while not being desirable for short and long run network security investments in theory and practice (Helm, 2009).

Likewise, theory suggests that price-based regulation promotes innovation such as those required for network security (Magat, 1976; Clemenz, 1991) while Kahn et al. (1999) argue that incentive regulation such as 'price-cap' or 'revenue-cap' can undermine the development of network security innovation even though there is considerable incentive for companies to improve efficiency through technical change. This is because undertaking security related R&D and other innovative investments become risky under-price-based mechanism while companies are incentivised to reduce costs. Hence, the dynamic efficiency improvements through technical changes and requiring short-term expenditures may take a backseat due to static efficiency improvements prompted by incentive regulation (Bauknecht, 2011). There is some evidence that price-based regulation has led to a decline in R&D expenditure and innovation across the European electricity sectors (Holt, 2005; Jamasb and Pollitt, 2008).

Hence, the regulatory mechanisms for network security can theoretically vary between a pure cost-based mechanism and a pure price-based mechanism and be regarded as two polar cases of regulatory mechanisms. In practice, $0 < \alpha < C^*$ and $0 < \beta < 1$ such that β acts as a sliding scale factor between a pure price cap and a pure cost pass-through in a performance based regulation. Table 1 presents the (generalised and overall) major economic attributes, limitations and trade-offs associated with pure cost-based and price-based regulation. The economic properties suggest the problems of information asymmetry and economic efficiency arguments leading to the paradigm shift from cost-based regulation towards price-based regulation.

For example, rate-of-return regulation contributed to overinvestment and inefficiency in operating cost while RPI-X produced the opposite effects of too little investment but with operating cost efficiency in the UK (Helm, 2009). A strict cost-based regulation leads to excess or gold-plated network security (Averch and Johnson, 1962) due to overinvestment or overcapitalisation. In contrary, a strict price-based regulation leads to too little network security if quality and reliability (or network security) are not suitably defined due to high-powered cost killing incentives among network companies. Ter-Martirosyan (2003) and Ter-Martirosyan and Kwoka (2010) showed that, in the absence of service quality controls within incentive regulation, incentive regulation led to deterioration of service quality in the US electricity networks. This implies that the level of network security delivered by a regulated

monopoly supplier can decline if the regulated prices are not allowed to 'increase as the network incurs greater costs to improve the service quality it provides' (Sappington, 2005).

Dimensions \ Regime	Cost-based regulation	Price-based regulation
Motives	Provides incentive to declare costs but not optimize the process	Provides incentive to optimize the process
Information asymmetry	Moral hazard	Adverse selection
Static efficiency	Allocative efficiency can be achieved but not productive efficiency	Productive efficiency achievable but not allocative efficiency
Long-run efficiency (assuming a fixed cost structure)	Long-run allocative efficiency can be achieved but not productive efficiency	Long-run productive efficiency can be achieved but not allocative efficiency
Investments	Incentivised as capital employed earns a return (but not efficient though)	Not incentivised (given cost reduction motives and risks)
Innovation	Overall incentivised as R&D is risk-free	Overall not incentivised as R&D is risky
Price setting provision	Ex-post	Ex-ante
Information requirement for the regulator	Relatively high but easy to implement	Low but relatively difficult to effectively implement
Regulatory lag	Endogenous and relatively short	Exogenous (set ex-ante) and relatively long
Macroeconomic impact	Can be inflationary	Can be non-inflationary

Table 1: Generalised and overall effects of cost and price-based regulation

Source: Authors' own compilation based

Hence, the regulator needs to find a balance between these two extreme regulatory regimes and assess a possible combination of the two regimes to ensure efficiency and productivity with satisfactory security level accounting for all security risks exposed to the electricity systems. Figure 1 depicts the optimum level of network security considering that the reliability level reflects the consumers' priorities. The optimum level of network security is attained when a profit maximising regulated network company expands network security to the point where marginal benefit of additional network security to consumers equals the companies marginal cost of increasing network security (Sappington, 2005). The total network costs constitute the fixed components (investment and innovation costs) and variable components (operating and maintenance costs, and interruption costs). The right-hand side and left-hand side regions of the optimum respectively denote overinvestment and underinvestment for network security. The need to balance costs-benefits of network security is a challenge while making network regulation more amicable towards ensuring optimal network security.

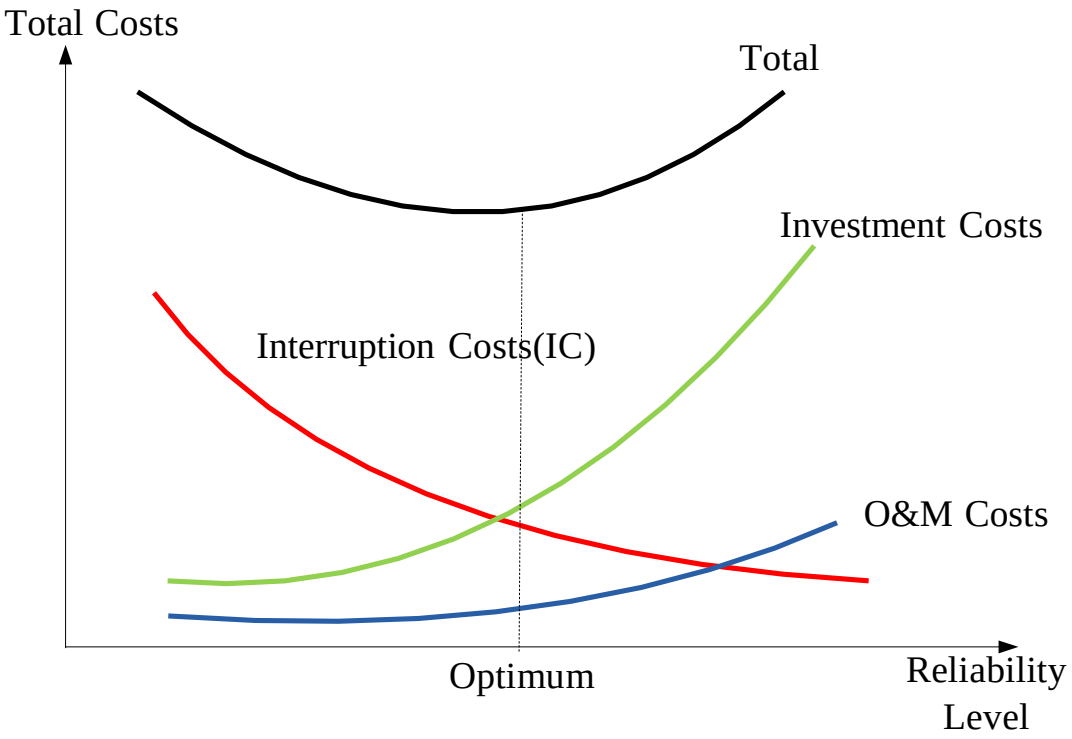

Figure 1: Socio-economic optimization of network security

Source: Authors

4. From Input to Output Based Regulation of Network Security

Economic regulation of electricity networks initially involves the regulator setting the overall budget available to network companies using cost or revenue based approaches. The input based approach focuses on the cost or revenue associated with specific investments to be made. The determination of the budget is often refined through the use of benchmarking in a revenue/price cap framework. The resulting budget can then be modified with inclusion of performance incentives based on measurable outputs. Hence, incentive regulation of network security can either target the network security inputs i.e. costs/expenditures (input-based approach) or network security outputs or performance (output-based approach) of the utilities such as the number and frequency of interruptions..

The *output-based* approach is characterized by complete autonomy of the networks in deciding the network security investments and innovation to be undertaken during the regulatory period (Benedettini and Pontoni, 2012). The role of the regulator is limited to

defining a set of network security related outputs performance standards while the network chooses the technology to meet the security related performance standards at the least possible costs. Over or under performance of the network companies with respect to security related network outputs is accompanied by appropriate incentives (or rewards) and penalties respectively. This incentive structure is in line with the theory of optimal incentive scheme when quality is verifiable (Laffont and Tirole, 1989).

An *output-based* regulation evaluates the firm's performance in terms of quantity and quality of delivered outputs and gives incentivizes to improve these levels (Vogelsang, 2006). The output-based approach is also efficient in addressing the problem of asymmetric information, as the regulator requires less information on the network company's inputs with this approach. For example, the regulator would only specify the appropriate level of network security performance standards as the output in an output-based approach while in an input-based approach, the regulator would specify the scale, location, and type of investments required to achieve the output (Frontier Economics, 2010). For example, the new regulatory scheme proposed by Ofgem as the RIIO (Revenue = Innovation + Incentives + Outputs) model and the existing output based incentives for service quality regulation in Italy are good examples of output-based regulation.

However, the output-based approach requires the regulator to properly ex-ante define and ex-post measure network security. This implies that output-based incentive regulation requires high output observability on the network security outputs of the regulated network company as the output-based approach to network security regulation is only applicable when clear metrics of network security outputs are available (Glachant et al., 2013).

The input-based regulation involves a strong regulatory influence in defining the production function of the network companies as network companies are not responsible for choosing the most cost-effective investments that improve their performance such as in network security. The regulator defines the size, the quality, the timing and the location of the investments towards meeting certain level of network security under an input-based approach. Hence, an appropriate regulatory regime to promote network security may require adapting both cost-based and price-based regimes to deliver the regulatory objective of increased network security rather than comparing and making a choice between them. Table 2 highlights important properties and characteristics of an input-based and output-based

approach of incentive regulation. Both approaches can be used to regulate the network security related costs. Some specific regulatory options are discussed below.

Dimensions \ Types	Input-based approach	Output-based approach
Ease of implementation	Relatively difficult due to high informational requirement	Relatively easy due to low informational requirement
Usefulness	For pursuing specific (or strategic) types of investments	For providing investment incentives related to performances
Applicability within/across sectors	Particularly applicable when a clear performance metric is not available and is applicable to all network industries	Applicable when clear performance metric for outputs are available and is applicable to other network industries depending on availability of suitable measure of outputs
Operational control	Regulator has greater control over network companies operational conduct	Network companies have greater control over its operational conduct as long as the output targets are met
Technology specification	Regulator sets the technology the network companies use by governing inputs	Network companies are responsible for choosing the technology that best meets their performance targets
Stakeholder focus	Focuses more on network companies with incentives provided for cost efficiency improvements and possibilities to extract informational rents	Focuses more on consumers (or the demand-side) with the network companies being able to meet consumer preferences at the least possible cost

Table 2: Generalised properties of input and output-based incentive regulation

4.1. Network security costs pass-through

Cost pass-through is an input-based approach to incentive regulation. This implies treating the costs related to network security such that these are passed to final consumer in a price-based environment assuming that the regulator approves all security costs in the regulatory cost base. These costs are not subject to benchmarking as this would make the network companies appear less efficient in a comparative efficiency analysis (or benchmarking) relative to other networks. Hence, network security investment costs will be treated as operational expenditures of the network companies and subject to direct pass-through under normal price-based environment under this approach.

The pass-through of network security costs in a price-based mechanism does not increase the controllable costs of the networks and do not need to result in efficiency improvements as these costs are not subject to the cost benchmarking exercise. However, innovative network security investments undertaken can help the network company become more efficient in the long run. Thus, the network can benefit from the increased price-cap and costs gap during the

regulatory period by undertaking innovative security investments, which the network customers (or network users) eventually finance. Such cost pass through has been applied to allowed R&D and other approved costs. For example, the Norwegian energy regulator NVE has recently allowed the networks to spend up to 0.3% of the book value of their assets on network related R&D.

There is, however, a potential of network security investments being inefficient as these costs are kept outside of the benchmarking exercise.. The worst possible outcome under this approach is the risk of these strategic investments being both inefficient and ineffective. Hence, the network security related costs that can be passed through should be capped by the regulator.

4.2. Network security costs capitalisation

Under this input-based approach, the network security costs are treated as capital expenditures (i.e. cost capitalisation) and are included in the regulatory asset base (RAB) and are depreciated in line with other assets. However, it can be difficult to include these costs in benchmarking as the statistical benchmarking techniques applicable to operating costs have not yet been developed for capital costs due to significant heterogeneity between networks in terms of the age of the assets, geography, service quality, lumpiness of capital expenditures and other considerations (Joskow, 2008). The capitalised network security costs can earn a rate-of return (or possibly extra rate of return) on any network security related expenditures irrespective of efficiency improvements that the networks experience.

An alternative would be to include network security related capital costs in the benchmarking analysis by undertaking the efficiency analysis at the total expenditures (or total costs) level. Benchmarking of total network security costs creates a more equal treatment of capital costs and operational costs in efficiency analysis and thereby minimises the distortions from input choices in benchmarking. Total costs benchmarking can also allow for efficient trade-offs between operational and capital expenditures related to network security. However, benchmarking total network security costs may not adequately deliver the type of capital investments related for network security implying that network security capital costs may need to be treated outside the benchmarking analysis.

Capitalisation of network security costs would produce a twin effect in a price-based regulation that applies to operational expenditure with investments being cost-based. This is because network security costs are both taken out of the price-based regime while the network companies can earn a rate-of-return on these costs. However, there is a risk of over-investment (or inefficient investment) in network security due to 'gold-plating' under this input-based approach. Likewise, increasing the network security expenditures does not necessarily lead to network security improvements unless the investments are useful. Capitalisation also offers incentives for network companies to shift and declare a major proportion of the costs as network security costs. This necessitates the regulator capping the network security costs that can be capitalised.

4.3. Linking the revenue-cap to network security output criteria

An output-based (or performance based) approach to incentive regulation provides impulse to investments aimed at improving network security related outputs. The revenue earned by the network company becomes more dependent on its performance or output in order to prompt active networks and innovation on network security. This is because, under this approach, the allowed revenue of the company is linked to the performance or outputs and not directly linked to the underlying own costs of the firm. A performance-based regulatory framework should incentivise the networks to out-perform specific network security outputs and thereby allowing the companies to recover some portion of the network security costs through higher revenue.

Thus, the additional revenue allowance of the firm is based on the actual network security related outputs whereas any recovery of the network security costs in a price-based regulation would have to be through cost-savings relative to the revenue cap imposed by the regulator (Bauknecht, 2011). Output-based regulation can also be effective when the regulated network has to perform multiple tasks and the regulator is not aware of the associated costs ex-ante. However, the ex-ante measurement and definition of network security output criteria is crucial and is a complicated task facing the regulator under this regulatory approach.

4.4. Extending the regulatory lag

The extension of regulatory lag provides longer-term incentives to security related investments. Extending the regulatory lags can incentivise the network company to benefit from reducing its costs below the set cap without undertaking any adjustments to the revenue

cap within the regulatory period. For example, the regulator of electricity and gas markets in Great Britain (Ofgem) is considering a new performance based model by setting a longer eight-year price control review period to be implemented for electricity distribution from 2015.

The extension of the regulatory lag prevents the company from passing the gains from undertaking security investments immediately to the consumers. Hence, the lag period between regulatory reviews can be deliberately used by the regulator to influence the network security investment propensity of the regulated network companies. However, the networks may have a tendency to delay the adoption of innovative network security related investments due to the long lag while there is a trade-off between efficiency incentives for the regulated network company and allocative efficiency associated with regulatory lag extension. The extension of regulatory lag can also have an adverse effect on the timing of network security related investments as network companies may continue to postpone the network security related investments and continue to retain the annual cost-savings.

4.5. Regulatory holidays

An alternative approach would be to temporarily exempt a certain part of the network from regulation. The revenue cap is lifted altogether and the network can charge monopoly prices under conditions of so called access or regulatory holidays (Gans and King, 2003). However, this approach may be too radical, as it requires intermitting tariff regulation rather than amending existing network regulation as disused under the input and output-based approaches to incentive regulation. The direct application of regulatory holiday in the electricity sector is not common although Ofgem's Innovation Funding Initiative (IFI) allows the complete pass-through of eligible costs to a certain limit.

In the telecommunication sector, the Australian telecom incumbent, Telstra, intended to invest in a modern Fibre to the Home (FTTH) network in return for a regulatory holiday on its access charges which the regulatory eventually did not approve (Cave, 2007). Nonetheless, it is clear that the theoretical extremes of cost-based and price-based regulation can be combined in different ways to address network security investments while the power of the incentive regulation to deal with information asymmetry and efficiency gains are relevant for generating investments in network security.

4.6. Direct compensation

Ensuring network security may necessitate that network companies undertake specific cost-intensive measures such as cables undergrounding and adopting sophisticated technologies to protect the electricity systems against natural, accidental and malicious threats. These cost-intensive investments are risky and can be beyond the ability and willingness of the network companies to absorb the associated risks by investing into these endeavours. Hence, direct compensation schemes to network companies can turn them to being risk-takers from being risk-averse to undertaking these costly investments. However, who funds these compensation schemes needs to be established beforehand as the choice can usually fall between the ratepayers versus the taxpayers. The pragmatic approach would be that taxpayers fund these initiatives as network security is viewed as a public good and engaging the taxpayers may effectively address the free-riders problem. Thus, the direct compensation schemes need to be discussed and designed at the security policy level.

5. Incorporating network security in service quality regulation

As service quality regulation is poised towards a more output oriented approach, regulators are faced with the challenge of incorporating and treating network security threats from exceptional events in the incentive regulation mechanism. This is because identifying exceptional events on the basis of a statistical methodology is difficult given that these events are rare while declaring an exceptional event based on technical and administrative evidence can be complicated as the understanding of the exceptional event (or the HILF events) varies across the European countries (see Appendix). The concept of exceptional events is commonly used across EU but is applied with different designations and meanings. The understanding and definition of 'exceptional events' varies between the EU member countries. Some countries adopt statistical approaches while others focus their definition on the causes of exceptional events. Therefore, it is not possible to derive a clear conclusion on situations where the concept is applicable and on how to distinguish between “exceptional events” and “normal interruptions” (CEER, 2012).

The statistical methods to address the exceptional events in network security regulation can be based on the level of impacts caused by exceptional events or can be based on criteria such as the number of customers interrupted or the frequency and duration of the interruption.

However, the changing focus of regulation towards an output-based approach implies defining a network security adjustment parameter (Q*) as an output indicator for network security (such as a proxy indicator for interruptions caused by exceptional events). The economic incentives can then be calculated as a function of the difference between a target Q* and the actual (ex-post) Q* where Q* is an output measure of continuity of supply (or service quality) for long unplanned interruptions of at least 5 minutes.

While data for exceptional events are less frequent and rare, considering long unplanned interruption of at least 5 minutes (which can be relatively frequent and relatively non-rare than exceptional events) can mimic the impacts of interruptions engendered by exceptional events while more data also being available for analysis. This is because some interruptions from exceptional events are long and affect a substantial number of customers. On the other hand, it might be advisable to use an average over several years instead of the values for one particular year if exceptional events are included. This would increase the stability of the indicator. For the transmission system reliability, other output indicators such as 'unsupplied energy' or AIT can be used. For example, in 2004, Ofgem developed incentive mechanisms targeted at various dimensions of distribution network service quality. A new incentive mechanism was introduced in 2005 that focused on transmission system reliability as measured by the value of energy not supplied (OFGEM, 2004).

Hence, the allowed revenue or price path (P_t) of the regulated network company is directly linked to an alternative price-cap formula where RPI is Retail Price Index, X is the efficiency gain (or the efficiency factor) and Q* is the network security adjustment parameter (or the network security output indicator). The annual values of the network security parameter Q* are calculated, ex-post on the basis of the network companies' performances and can take a negative or a positive sign. A positive value of Q* implies that network security has improved more than required at the national level and vice versa.

$$\boldsymbol{P_t = P_{t-1}\,(1 + RPI - X + Q^*)} \qquad \textbf{(4)}$$

A statistical methodology to account for exceptional events in incentive regulation has several advantages in terms of simplifying the administrative procedure, being easy to understand and reducing the implementation costs incurred by the network companies and the regulator. However, it may expose the regulatory model to some fallacies of benchmarking as

the target value output indicator (such as Q*) is obtained from benchmarking. This is because a consensus does not exist on the choice of input and output variables to be included in the benchmarking models while the appropriateness of including network security measures in benchmarking models is still a new concept. Nonetheless, a value of Q* can be obtained from national distribution companies while international benchmarking could be used to determine the value of Q* at the transmission level.

The adoption of statistical methods to account for exceptional events will require harmonisation of network security indicators and data collection procedures. The measurement rules can play a crucial role in ensuring fairness in network security regulation. It is also necessary that security data include information about the interruptions that are excluded and included together with all the information about those events that are treated specifically. However, exceptional events, with an apparent intuitive meaning, but in the absence of a clear definition of the manner in which it is being used can lead to misinterpretation (CEER, 2012). Hence, it is recommended that each country use the definitions as set out in their own regulation but in convergence with international standards to facilitate international comparisons.

Hence, incentive regulation of network security, in practice, can be an evolutionary process where one set of mechanisms is tried, their performance assessed, additional data and reporting needs identified and refined mechanisms developed and applied (Joskow, 2011). The future applications of incentive regulation concepts towards network security can consist of elements of tradition cost-based regulation, yardstick regulation and high-powered price-based regulation together with a defined set of outputs. However, the large-scale investment requirements to make the networks active combined with the need to undertake strategic investments to protect the grids from accidental and malicious threats imply that the government may pursue network security objectives with public funding rather than shifting these costs to network users under the incentive regulation framework. This is because the private rate of return to network security investments can be lower than the social rate of return implying inadequate network security under incentive regulation. However, any public funding should be accompanied by a thorough cost-benefit or cost effectiveness analysis to improve the efficiency of expenditure on networks while the results and information associated with such cost-benefit (or cost effectiveness) analyses should be shared between countries. This implies that if network security is also a political issue, then economics of

delivering a desirable level of network security may need to take the back seat and other authorities apart from the regulator shall decide the premises of it. However, ample coordination among member countries at the federal level is required.

The European Commission can strategically promote network security across the EU by monitoring and providing (access to) funding to security related important projects. The EC can initiate a Network Security Enhancement Plan (NSEP) that identifies the key projects crucial for network security improvements in the EU and finance these projects. The monitoring and funding of the network security related project from the European Commission will also place these projects and network security objectives in line with the overall aim of creating an integrated market for electricity in Europe. For example, the Priority Interconnection Plan (PIP) of the EC strategically promotes the development of trans-European networks by providing details and updates on the progress of the 42 projects of European interest (Kerner, 2006). The projects listed on PIP receive special funding consideration from the European banks. The European Commission can initiate similar arrangements for the development of network security.

The design of instruments to promote network security should also consider any support outside regulation when determining relevant incentive parameters. For example, electricity regulators in Norway and UK address the quality of service regulation by incorporating the social costs of network interruptions (or consumer willingness to pay to avoid the interruption costs) in incentive regulation. Hence, promoting network security via incentive regulation is not only limited to the incentive regulation mechanism alone but should be understood in the broader energy and national energy security policy context. The policy-regulation interface pertaining to network security needs to be well understood in the face of changing network regulation.

6. Conclusions

Security of supply and energy infrastructure has become a priority policy for the EU energy policy-makers and regulators together with other energy policy goals of competitiveness, affordability as the European electricity markets continue to liberalise. While wholesale and retail electricity markets across Europe have become competitive with increasing market

integration, unbundling and market opening; network security issues still remain critical and difficult to effectively address across the EU. This is especially the case considering the on-going transition towards a low-carbon energy-economy, increasing digitalization of the grid, increased adoption of renewable energy and growing integration of electric vehicles in the grid amidst the lack of adequate investments in the EU electricity networks.

This paper addressed the current issues and future options in regulating network security and the role the future network regulation can play in improving the network security in the European electricity systems. It suggests that the changing nature of network regulation from an input-oriented approach to an output-based incentive regulation can be made suitable to address the network security risks. The nature of changing regulation, emerging regulatory trends and the need to upgrade the European networks provide an opportunity to integrate network security objectives into these economic activities as well. However, this needs to take place in the coming years to maximize the 'synergy' effects and also make achieving the objectives more cost effective. The European Union may need to require the Member States to include network security objectives in their upgrade plans.

The EU countries also need to harmonise the network security objectives and intensify coordination among each other irrespective of the network security goals being an incentive regulation matter or a policy matter. The output-based regulation of exceptional events will require defining and measuring relevant network security outputs which can be difficult for the regulator. This clearly remains a challenge. Such approach can also run the risk of suffering from the regulator micro-managing the conceptual issues and assessment of network security. Hence, it may be desirable that, in the short run, a 'building blocks' approach to network security regulation is adopted as demonstrated by the successful service quality regulation in Italy.

An output-oriented, complex and forward looking regulatory framework such as the RIIO model as being discussed in the UK can be employed to address network security as regulators gain more experience and become capable through 'learning by doing'. Moreover, the regulation of network security should also be understood in its wider economic regulation and national policy context. This involves considering the investment requirements and innovation challenges combined with the need to protect the electricity networks from natural, accidental and malicious threats.

References

Armstrong, C.M., Cowan, S., and Vickers, J. (1994). Regulatory Reform, Economic Analysis and British Experience, Cambridge, MA: MIT Press.

Arriaga, I.J.P. (2007). Security of Electricity Supply in Europe in a Short, Medium and Long-Term Perspective, *European Review of Energy Markets*, Vol. 2(2), pp. 1-28.

Averch, H. and Johnson, L.L. (1962). Behaviour of the Firm under Regulatory Constraint, *American Economic Review*, Vol. 52, pp. 1059-1069.

Bailey, E.E. (1974). Innovation and Regulation, *Journal of Public Economics*, Vol. 3(3), pp. 285-295.

Bauknecht, D. (2011). Incentive Regulation and Network Innovations, EUI Working Papers RSCAS 2011/02, European University Institute, Italy.

Benedettini, S. and Pontoni, F. (2012). Electricity Distribution Investments: No country for Old Rules? A Critical Overview of UK and Italian Regulations, *Centre for Research on Energy and Environmental Economics and Policy, Working Paper No. 50, Bocconi University, Italy.*

Billington, R. and Allan, R.N. (1987). Reliability Assessment of Large Electric Power Systems, Kluwer Academic, USA.

Brenan, T. (1989). Regulating by Capping Prices, *Journal of Regulatory Economics*, Vol. 1, pp. 133-147.

Cambini, C., Fumagalli, E. and Croce, A. (2012). Output Based Incentive Regulation: Benchmarking with Quality of Supply in Electricity Distribution, Draft, January 26.

Cave, M. (2007). The Regulation of Access in Telecommunications: A European Perspective, Mimeo, Warwick Business School, University of Warwick.

CEER (2012). Fifth CEER Benchmarking Report on the Quality of Electricity Supply, Council of European Energy Regulators, April, Brussels.

Clemenz, G. (1991). Optimal Price-cap Regulation, *The Journal of Industrial Economics*, Vol. 39(4), pp. 391-408.

Coelli, T. and Perelman, S. (1999). A Comparison of Parametric and Non-Parametric Distance Functions: With Application to European Railways, *European Journal of Operations Research*, Vol. 117 (2), pp. 326-339.

Crewe, M.A. and Kleinforfer, P.R (1996). Incentive Regulation in the United Kingdom and the United States: Some Lessons, *Journal of Regulatory Economics*, Vol. 9(3), pp. 211-225.

Douglas, J (2005). Grid security in the 21st Century, *EPRI Journal*, Electric Power Research Institute, Summer, pp. 26-33.

European Commission (2006). European Smart Grids Technology Platform: Vision and Strategy for Europe's Electricity Networks of the Future, Community Research, EUR 22040, Directorate-General for Research Sustainable Energy Systems, Brussels.

Frontier Economics (2010). RPI-X@20: Output Measures in the Future Regulatory Framework, Frontier Economics Ltd. London.

Gans, J.S. and King, S. (2003). Access Holidays for Network Infrastructure Investment, *Agenda*, Vol. 10(2), pp. 163-178.

Glachant, J.M., Khalfallah, H., Perez, Y., Rious, V. and Saguan, M. (2013). Implementing Incentive Regulation through an Alignment with Resource Bounded Regulators, *Competition and Regulation in Network Industries*, Number Vol. 14(3), pp. 264-269.

Hammond, G.P. and Waldron, R. (2008). Risk Assessment of UK electricity Supply in a Rapidly Evolving Energy Sector, Proc. IMechE Vol. 222 Part A: *Journal of Power and Energy*, pp. 623-641.

Helm, D. (2009). Infrastructure Investment, the Cost of Capital and Regulation: An Assessment, *Oxford Review of Economic Policy*, Vol. 25(3), pp. 307-326.

Holt, D. (2005). Where Has the Innovation Gone? R&D in UK Utility Regulation, Oxera, Agenda, November.

Jamasb, T. and Pollitt, M. (2007). Incentive Regulation of Electricity Distribution Networks: Lessons of Experience from Britain, *Energy Policy*, Vol. 35(12), pp. 6163-6187.

Jamasb, T. and Pollitt, M. (2008). Liberalisation and R&D in Network Industries: The Case of the Electricity Industry, *Research Policy*, Vol. 37, pp. 995-1008.

Jamasb, T. and Pollitt, M. (2011). Electricity Sector Liberalisation and Innovation: An Analysis of the UK's Patenting Activities, *Research Policy*, Vol. 40, pp. 309-324.

Joskow, P.L. (1974). Inflation and Environmental Concern: Structural Change in the Process of Public Utility Price regulation, *Journal of Law and Economics*, Vol. 17, pp: 291-327.

Joskow, P.L. (2007). Supply Security in Competitive Electricity and Gas Markets, In C. Robinson (Ed.), *Utility Regulation in Competitive Markets*, Edward Elgar.

Joskow, P.L. (2008). Incentive Regulation and its Application to Electricity Networks, Review of Network Economics, Vol. 7(4), pp. 547-560.

Joskow, P.L. (2011). Incentive Regulation in Theory and Practice: Electricity Transmission and Distribution Networks, NBER Chapters, In: Economic Regulation and its Reform: What Have We Learned? National Bureau of Economic Research.

Joskow, P.L. (2012). Creating a Smarter U.S. Electricity Grid, *Journal of Economic Perspectives*, Vol. 26(1), pp. 29-48.

Kahn, A.E., Tardiff, T.J., and Weisman, D.L. (1999). The Telecommunications Act at three Years: An Economic Evaluation of its Implementation by the Federal Communications Commission, *Information Economics and Policy.*

Kerner, W. (2006). Priority Interconnection Plan – a European View of Energy Networks, European Commission – DG Energy and Transport, ABB Seminar, Estonia, December.

Laffont, J.-J. and Tirole, J. (1989). Provision of Quality and Power of Incentive Schemes in Regulated Industries, Working papers 528, Massachusetts Institute of Technology (MIT), Department of Economics.

Laffont, J.-J. and Tirole, J. (1993). *A Theory of Incentives in Regulation and Procurement*, MIT Press: Cambridge, MA.

Magat, W.A. (1976). Regulation and the Rate and Direction of Induced Technical Change, *The Bell Journal of Economics*, Vol. 7(2), pp. 478-496.

Mayo, J.W. and Flynn, J.E. (1988). The Effects of Regulation on Research and Development: Theory and Evidence, *Journal of Business*, Vol. 61(3), pp. 321-336.

Nepal, R. and Jamasb, T. (2013). Security of the European Electricity Systems: Conceptualizing the Assessment Criteria and Core Indicators, *International Journal of Critical Infrastructure Protection*, Vol. 6(3-4), pp. 182-196.

NERC (2010). High-Impact, Low-Frequency Event Risk to the North American Bulk Power System, North American Electricity Reliability Corporation, June, United States.

Newbery, D. (2002). Privatisation, Restructuring and Regulation of Network Utilities, MIT Press, Cambridge, Massachusetts.

Newbery, D. (2012). State of the Union: Achieving the Internal Market, Presentation to the Conference on 'State of Union: Energy Policy', Florence School of Regulation, Italy.

OFGEM (2004). Electricity Distribution Price Control Review: Initial Proposals, Office of Gas and Electricity Markets, 145/04, June, London.

Sanyal, P. and Cohen, L.R. (2009). Powering Progress: Restructuring, Competition and R&D in the US Electric Utility Industry, *The Energy Journal*, Vol. 30(2), pp. 41-80.

Sappington, D. (2005). Regulating Service Quality: A Survey, *Journal of Regulatory Economics*, Vol. 27(2), pp. 123-154.

Schiavo, L., Delfanti, M., Fumagalli, E. and Olivieri, V. (2013). Changing the Regulation for Regulating the Change, Innovation –Driven Regulatory Developments in Italy: Smart grids, Smart Metering and E-Mobility, *Energy Policy*, Vol. 57, June, pp. 506-517.

Skoczkowski, T. (2007). Energy efficiency policy in the European Union, Leonardo Energy: The Global Community for Sustainable Energy Professionals.

Vogelsang, I. (2002). Incentive Regulation and Competition in Public Utility Markets: A 20 Year Perspective, *Journal of Regulatory Economics*, Vol. 22(1), pp. 5-27.

Vogelsang, I. (2006). Electricity Transmission Pricing and Performance-based Regulation, *The Energy Journal*, Vol. 27(4), pp. 97-126.

Appendix

Country	Designation	Concept	Who classifies?	Included in interruption statistics	Eligible to receive compensation payments
France	Exceptional event	simultaneous interruption for more than 100,000 end users	TSO[1] and DSO	Yes	No
Finland		The concept of exceptional event does not exist			Yes, but interruptions longer than 12 hours are compensated
Germany	Force Majeure	Natural disasters, terrorist attacks and war, legal and official orders	Jurisdiction, National Regulatory Authority	Yes	No
Italy	Exceptional conditions periods	Based on statistical exploration and computational algorithm by NRA	DSO	Yes	No
Czech Republic		The concept does not exist			
Denmark	Exceptional event	Hurricanes and floods	Regulator	Yes	No
United Kingdom	Exceptional event	Weather and non-weather related	NRA	Yes	Yes, only is some situations

[1]TSO stands for Transmission System Operator, DSO stands for Distribution System Operator and NRA stands for National Regulatory Authority.