

Training Day

Regulatory frameworks for electricity network resilience

Clara Poletti – Florence School of Regulation

- 1 Understanding resilience**
- 2 Measuring resilience**
- 3 Regulating resilience**
- 4 Regulatory experience and implementation challenges**

What do we mean by network resilience?

Power-system resilience is the ability to limit the extent, severity and duration of system degradation following an extreme (low probability) event (CIGRE)



Resilience is not reliability

Reliability

Continuity and quality of supply under normal or reasonably foreseeable conditions

Resilience

Disruptive, low-probability / high-impact events, historical frequency is a poor guide to future risk

Regulation built for reliability will not, on its own, deliver resilience against extreme events

Why has resilience become a regulatory issue?

Three structural shifts are moving resilience from an engineering concern to a regulatory one

■ Hazards

Climate change is shifting the frequency and severity of heat, wildfire, flooding and storms

■ Exposure

Electrification deepens dependence on electricity, raising the economic and social cost of outages

■ Interdependencies

Electricity failures propagate into telecoms, water, transport and gas networks

The evidence, and what it means for regulation

IPCC

Hot extremes have become more frequent and more intense across most land regions since the 1950s

Economic loss

Economic losses from weather, climate and water-related disasters increased sevenfold from the 1970s to the 2010s

Implication

Frameworks relying predominantly on historical outage data may understate future resilience needs

Why is resilience difficult to regulate?

Certain costs today weighed against uncertain avoided losses tomorrow, losses that may never materialise during the regulatory period

In practice

01

Tail risk is hard to value

Exp-value methods may understate tail risk

02

History is not enough

Incentives rely on observed interruptions; resilience needs forward judgements

03

No single metric

Customers affected, duration, extent, restoration speed, cascading effects

04

Responsibilities are split

Across operators, NRAs, governments and civil-protection authorities

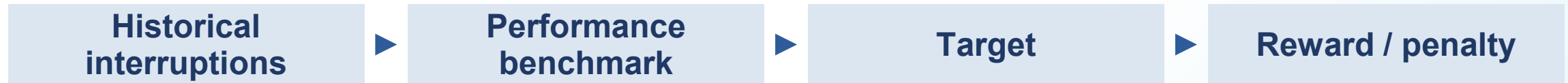
What is the efficient degree of resilience?

The efficient level is not maximum resilience. Regulators must compare the cost of additional resilience with the value of the risk reduction it delivers

From reliability metrics to risk-based regulation

Traditional reliability logic

Backward-looking: what already happened sets the target



Resilience: risk-based logic

Forward-looking: expected future risk sets the priority



How would you describe electricity-network resilience in your jurisdiction today? (Poll 1)

- 1** We are already taking action
- 2** Work is underway, but the framework is still developing
- 3** Mainly a prospective concern
- 4** Not currently a significant regulatory issue



How do we measure resilience? Five assessment steps

1 Identify relevant events

Wildfire, flooding, storms, extreme heat

2 Use climate scenarios

For climate hazards use forward-looking scenarios, not historical frequencies

3 Measure exposure

Which assets, customers and territories are exposed

4 Assess vulnerability

Given exposure, how likely is failure or degradation?

5 Quantify consequences

The key regulatory step

How do we measure resilience? The case of California (1)

The California Public Utilities Commission defines the common framework and reporting requirements

Risk-Based Decision-Making Framework:

- probabilistic
- granularity and comparability are relevant
- Climate information must be integrated into risk assessment

Utilities develop and apply risk-specific models

The California Public Utilities Commission reviews and challenges the methodology and the results

The regulator standardises the method rather than computing the risk itself

How do we measure resilience? The case of California (2)

The utility applies the method to estimate the risk



How do we measure resilience? The case of California (3)

LoRE

Probability that a given risk event occurs, conditioned on relevant risk drivers and exposure information

- example wildfire: probability that utility infrastructure contributes to an ignition
- Conditioned on asset type and environmental drivers such as wind and fuel, and operating state
- Estimated per risk-relevant area or asset

×

CoRE

Distribution of possible monetised consequences, conditional on the risk event occurring.

- Safety: fatalities and serious injuries.
- Reliability: customer-minutes interrupted, outage duration.
- Financial: direct monetary losses.

* **Monetisation: converting outcomes into one comparable metric**

Each consequence is first measured in its natural unit, then converted with standard values: the value of a statistical life for safety, interruption-cost values for reliability. Components are summed in dollars.

Risk = LoRE × CoRE

Overall probability distribution of consequences

Risk assessment identifies

- Baseline risk
- Where risk is concentrated
- Possible mitigation measures
- Monetary value of risk
- Residual risk after mitigation

Regulation must then decide

- 1 What level of resilience should be required?**
- 2 Which mitigation expenditure should consumers fund?**
- 3 Are additional incentives needed to induce efficient investment and preparedness?**

1

Minimum standards and planning

Resilience and adaptation plans, engineering standards, emergency preparedness

Sets a floor only

2

Risk-informed expenditure review

CAPEX and OPEX justified against resilience factors

Embedded in general regulatory framework

3

Performance-based incentives

Remuneration linked to expected or verified risk reduction / resilience improvement

Pays for outcomes

4

Adaptive mechanisms

Cost pass-through following qualifying natural-disaster events

Covers the unforeseen

No single instrument is sufficient: effective regimes may combine all four

Which regulatory approaches to network resilience currently used in your jurisdiction?

Select all that apply (Poll 2)

- 1 Resilience standards or preparedness obligations
- 2 Ad hoc ex-post mechanisms for exceptional events
- 3 Incentives linked to resilience improvements or risk reduction
- 4 Other



Affordability and distributional impacts matter

Costs are often socialised. Benefits may be highly concentrated

WHO PAYS



All network users, through tariffs

WHO BENEFITS



Specific geographies, customer groups and critical infrastructures

Funding a public-policy objective entirely through network tariffs is a distributional choice, not only an efficiency one

Resilience regulation challenges regulators too

Everything proposed here assumes a regulator equipped to do it

01	Capabilities	Probabilistic risk, climate, engineering, data and economic valuation require new expertise
02	Resources	Forward-looking risk scrutiny can be substantially more resource-intensive than ex-post performance regulation
03	Information asymmetry	Sophisticated utility risk models raise the need for transparency, standardisation and independent challenge
04	Governance	Critical infrastructure and societal risk tolerance require coordination with governments and other authorities

Building resilience regulation means building regulatory capacity alongside it

Resilience regulation is not something a regulator can simply switch on by adopting a sophisticated methodology. It is a capability-building process

It requires: high quality data, probabilistic and climate-risk modelling, engagement with consumers, stakeholders and other public authorities

Implementation may therefore need to be progressive and sharing of best practices highly valuable



Clara.Poletti@eui.eu