Imperial College London

Symposium on Microgrids Aalborg 2015

Smart Grids European Technology Platform:

Network security and resilience and role of microgids

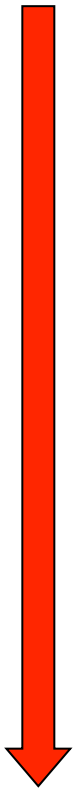
Goran Strbac
Imperial College London

Low carbon system: degradation in asset utilisation

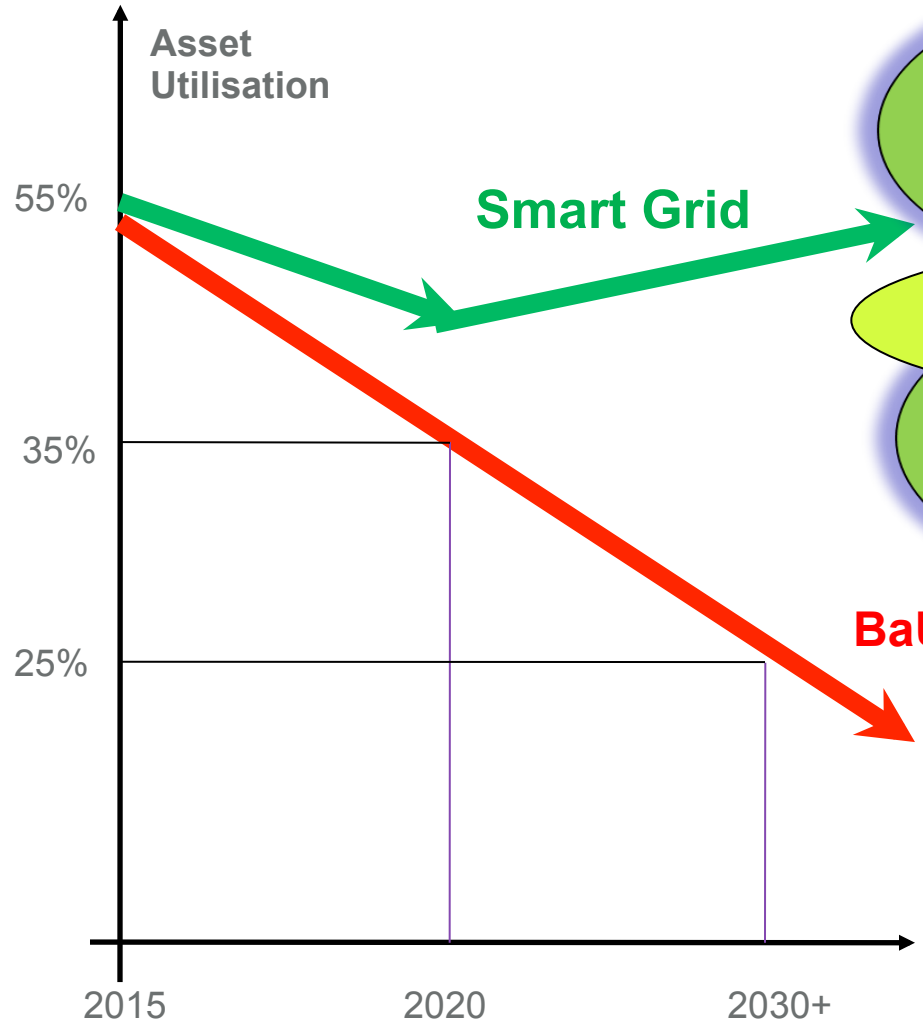
2020: RES will displace energy produced by conventional plant but its ability displace capacity will be limited: more than 35% of conventional generation operating at less than 10% load factor

2030+: Electrification of segments of transport and heat sectors: increase in peak demand disproportionally higher than increase in energy

Year	Utilisation
2015	**55%**
2020	**35%**
2030+	**<25%**



Response to the system integration challenge: Smart Grid



Smart network technologies

Demand Response

Paradigm shift in delivering security of supply: from redundancy in assets to intelligence

Storage

Flexible Generation

Potential volume of the market for smart grid technologies post 2030 in EU >€300b

White paper: content

- Key strengths and weaknesses of the present network security standards
- Context of EU renewable generation policy
- Security & resilience challenges for future EU Smart Grids
- Tests and standards for smart grid solutions and technologies;
- Regulatory and commercial framework

Why network security should be of paramount importance to regulators?

- T & D networks are natural monopolies and need to be regulated. Regulatory concerns:
- ***Operation*: Are the networks delivering good value for money to users? How much capacity is released to network users?
  - Too much: security compromised, risks of outages too high
  - Too little: efficiency compromised, efficient generation prevented from accessing the market
- ***Investment*: Are the network investment efficient? Are the benefits of a network investment greater than the cost?
  - But what is exactly the benefit of network investment and how do we measure (quantify) it?

Historical grid planning and operational standards - areas of interests / concerns /1

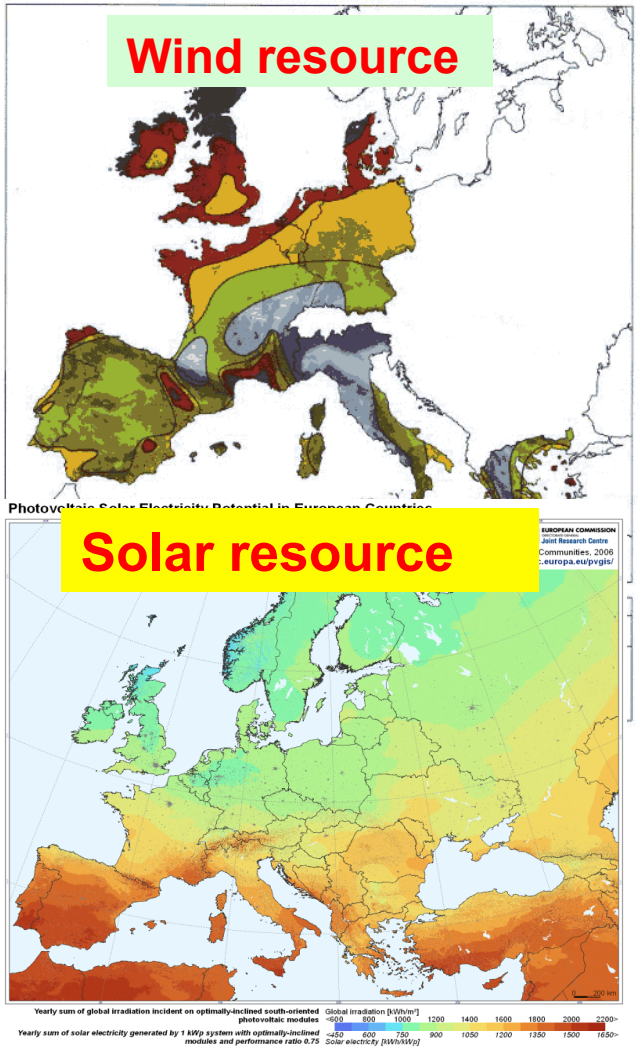
- Historical network design standards have delivered adequate network reliability performance – are these in line with the EU low carbon agenda?
- Are the operation & investment costs and benefits closely align?
- Degree of security delivered to users varies significantly across the system - no direct relationship with costs.
- Is the Redundancy a direct measure for security? Is the degree of security provided optimal in any particular instance? Average or network specific approach?
  - Is the likelihood of network component outages considered by the present standards? For example, faults on a long, exposed line are much more frequent than failures of an actively monitored transformer.

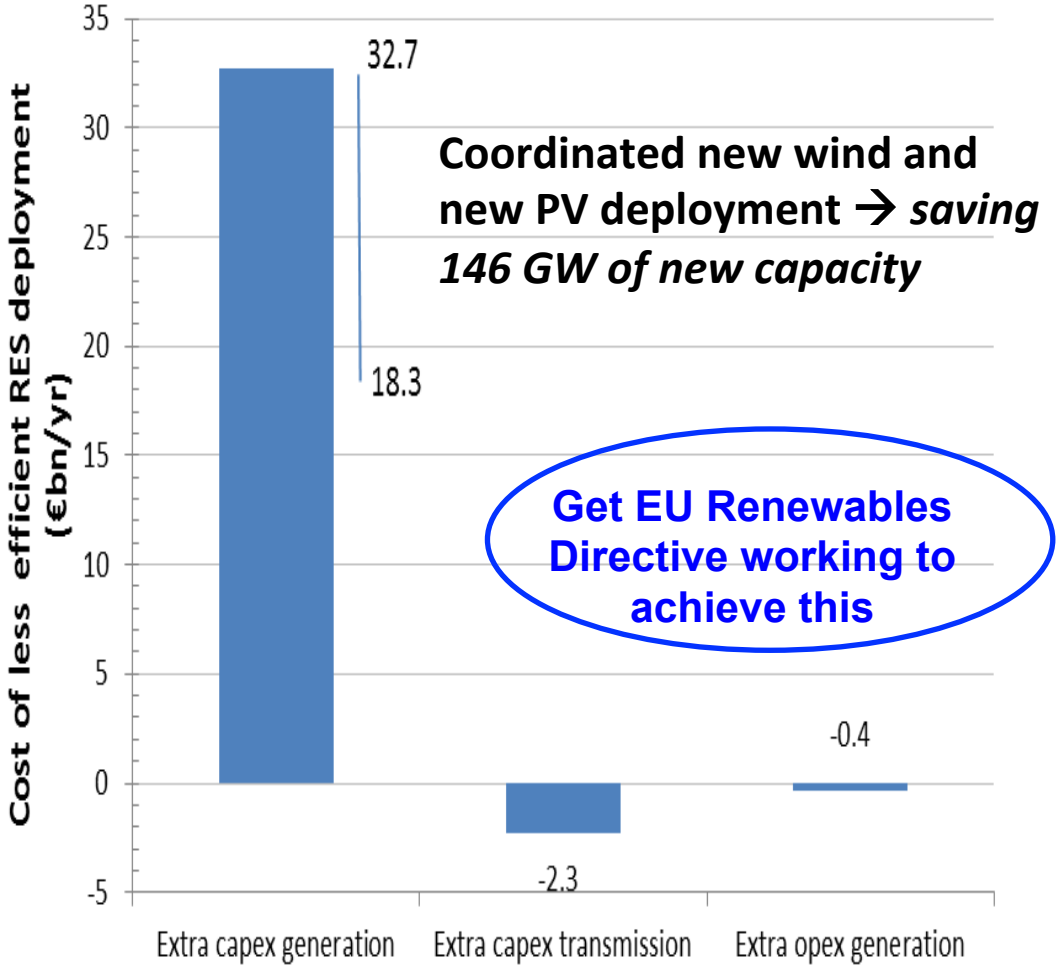
Historical grid planning and operational standards - areas of interests / concerns /2

- Is the binary approach to risk fundamentally problematic?
  - "no" risk at all if compliant with the standard
  - "unacceptable" risk if not compliant to the standard
- Can efficient non-network solutions (e.g. in the form of generation or flexible demand) be considered and applied as an alternative to traditional network based reinforcements?
- Clear trend in enhancing system flexibility: from investment in primary plant to investment into more sophisticated operation and control
- How about resiliency?

EU wide approach (rather than member state centric) to RES deployment

North is Windy & South is Sunny…



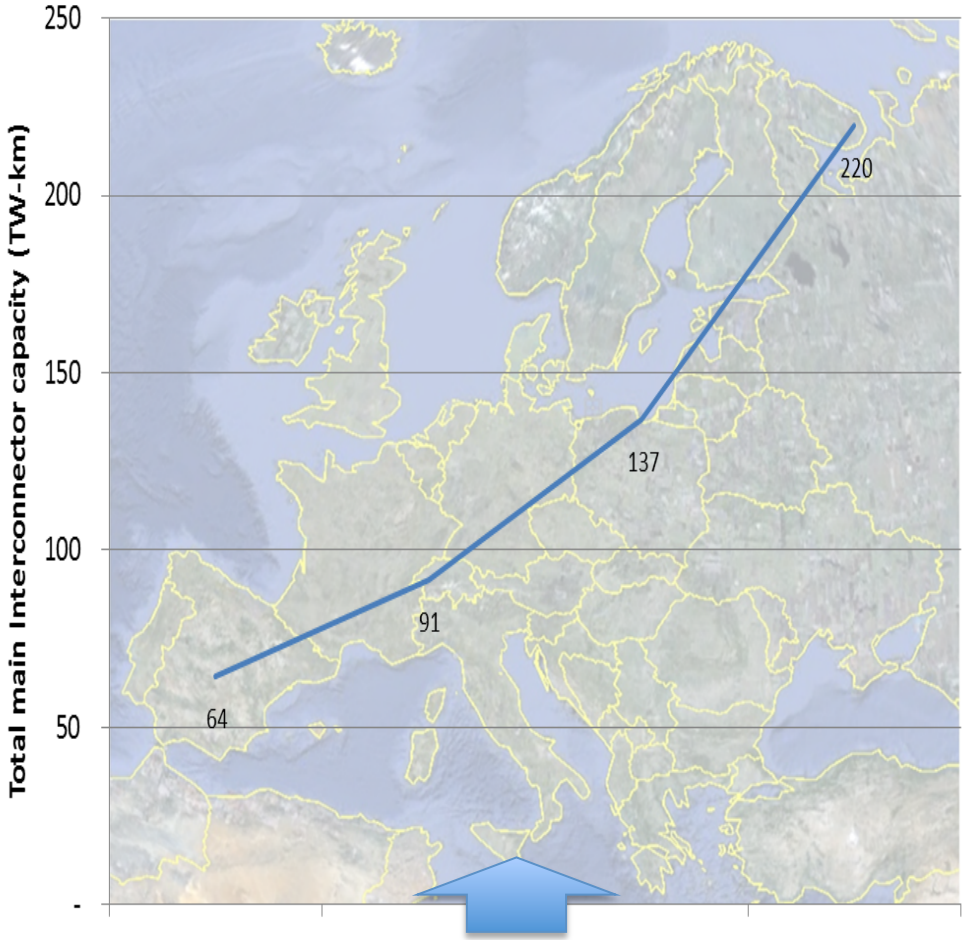


Coordinated new wind and new PV deployment → *saving 146 GW of new capacity*

Get EU Renewables Directive working to achieve this

Coordinated RES deployment needs stronger interconnection

Microgrids: Managing security of European Megagrid



Using EU transmission grid to provide cost effective integration of RES with relaxed security?

Energy transfer:
Megagrid

Smart Network Technologies

Demand Response

Paradigm shift: from redundancy in assets to intelligence

Storage

Flexible DG

Microgrids
Security & resilience

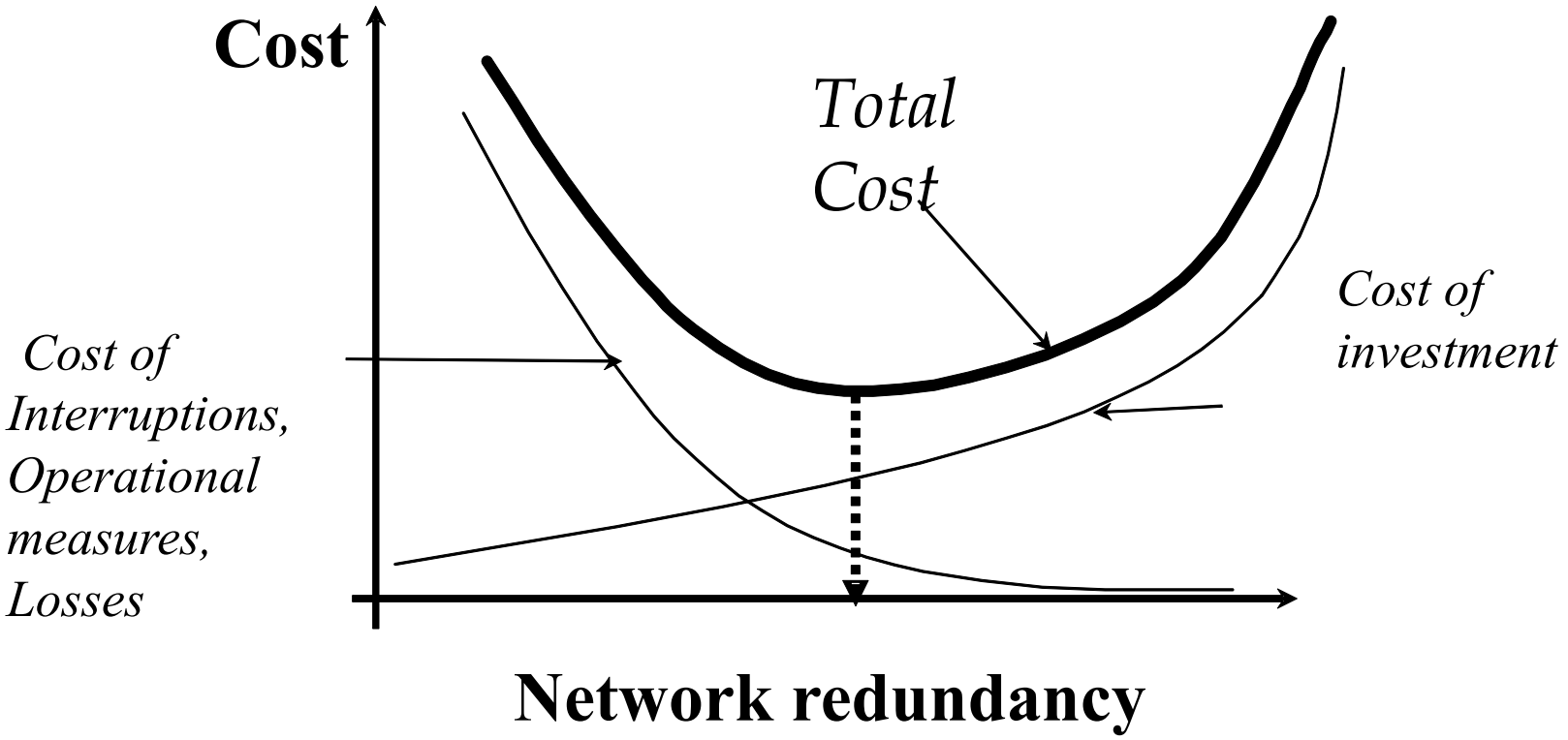
- Community based energy system

- Smart Cities

Fundamental approach to determining optimal level of network security

Cost benefits analysis to determine trade-off

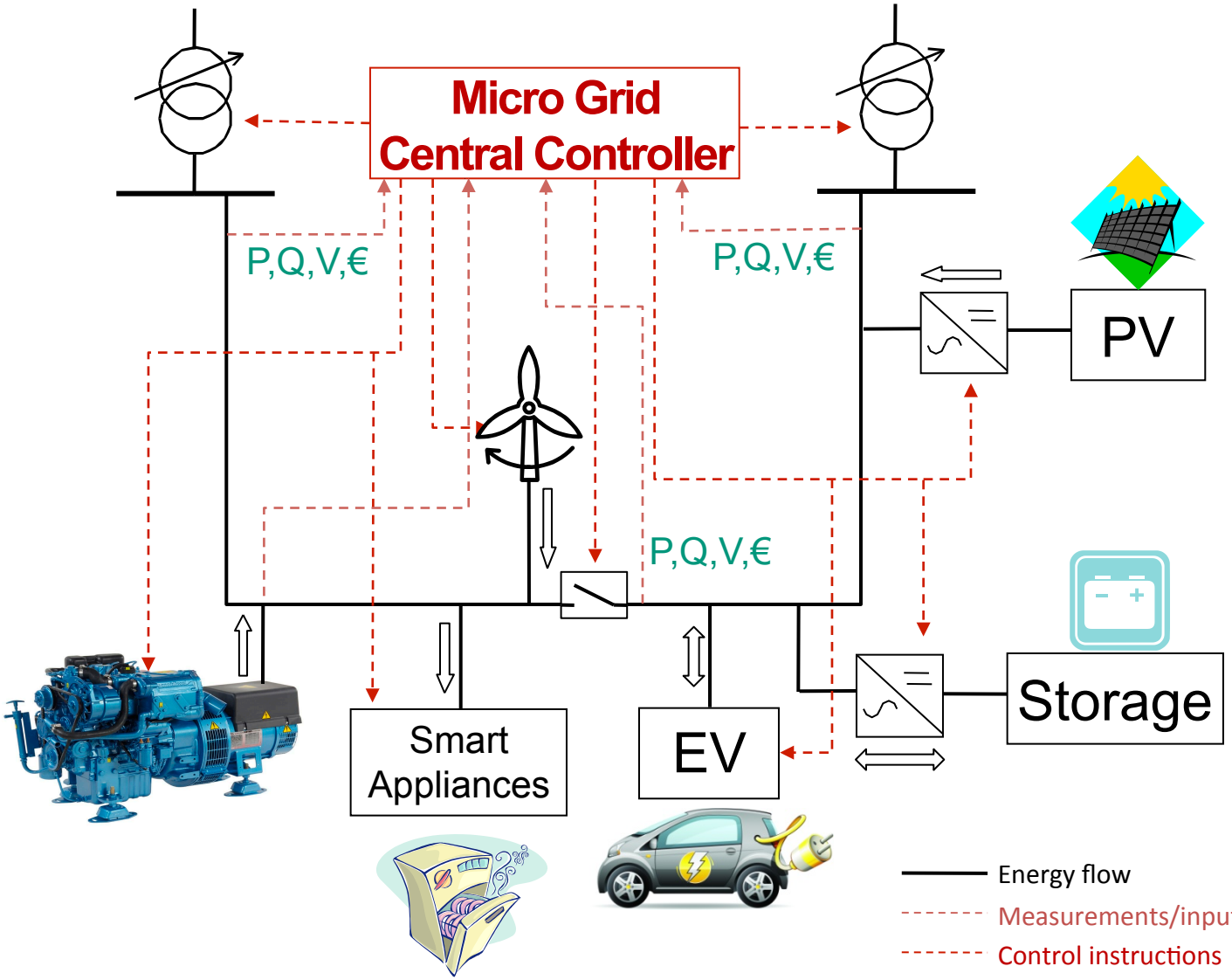
- **Cost of interruptions of supply**
- **Cost of additional investment**



Advantages of a cost-benefit framework

- Risk-based approaches to security and resilience provide more (full) information on which to base operating and investment decisions.
- A proper measure of risk can account not only for the probability of an undesirable outcome, but also for the consequences of such outcome.
- Probabilistic framework provides an opportunity for a range of non-traditional reliability enhancements to be considered, this should, in the long term, lead to an improved network reliability profile.

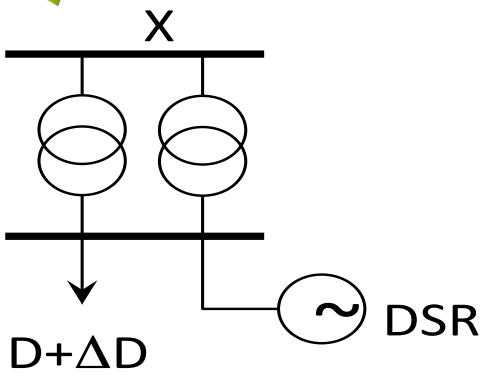
Active network control paradigm



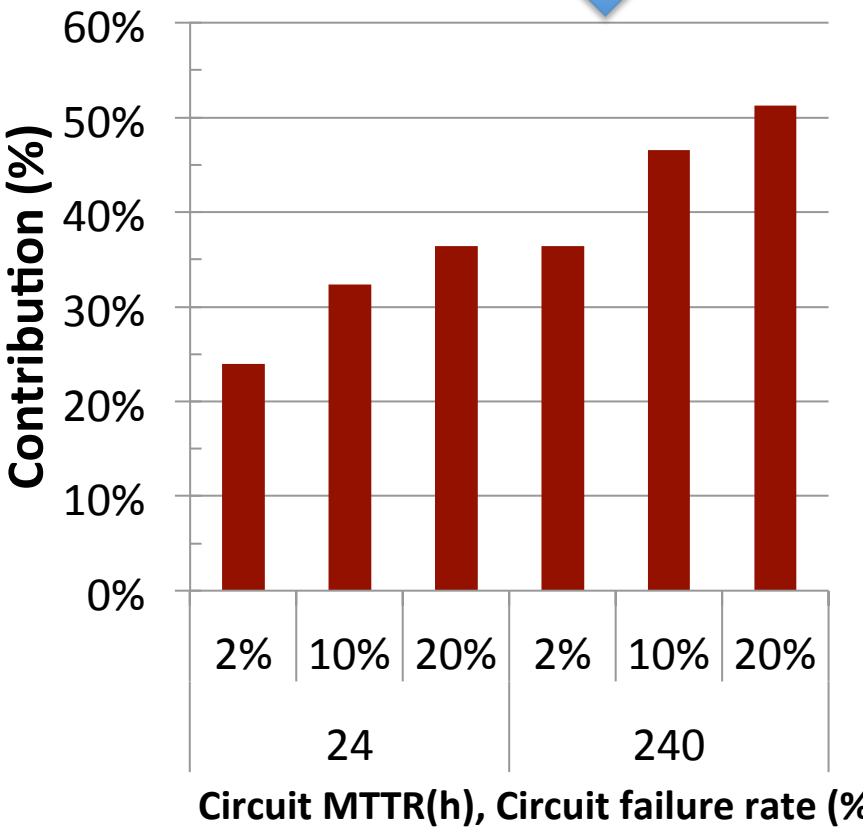
How much of the network infrastructure can be displaced by smart?

Contribution to security of supply:

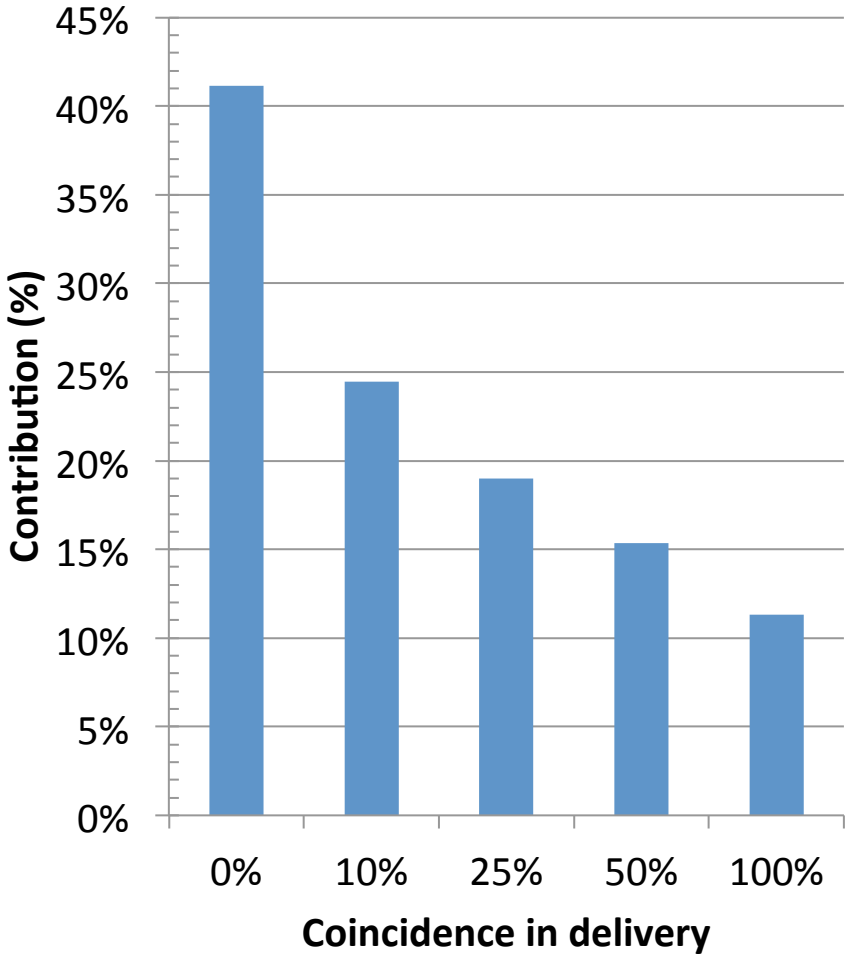
Demand Side Response



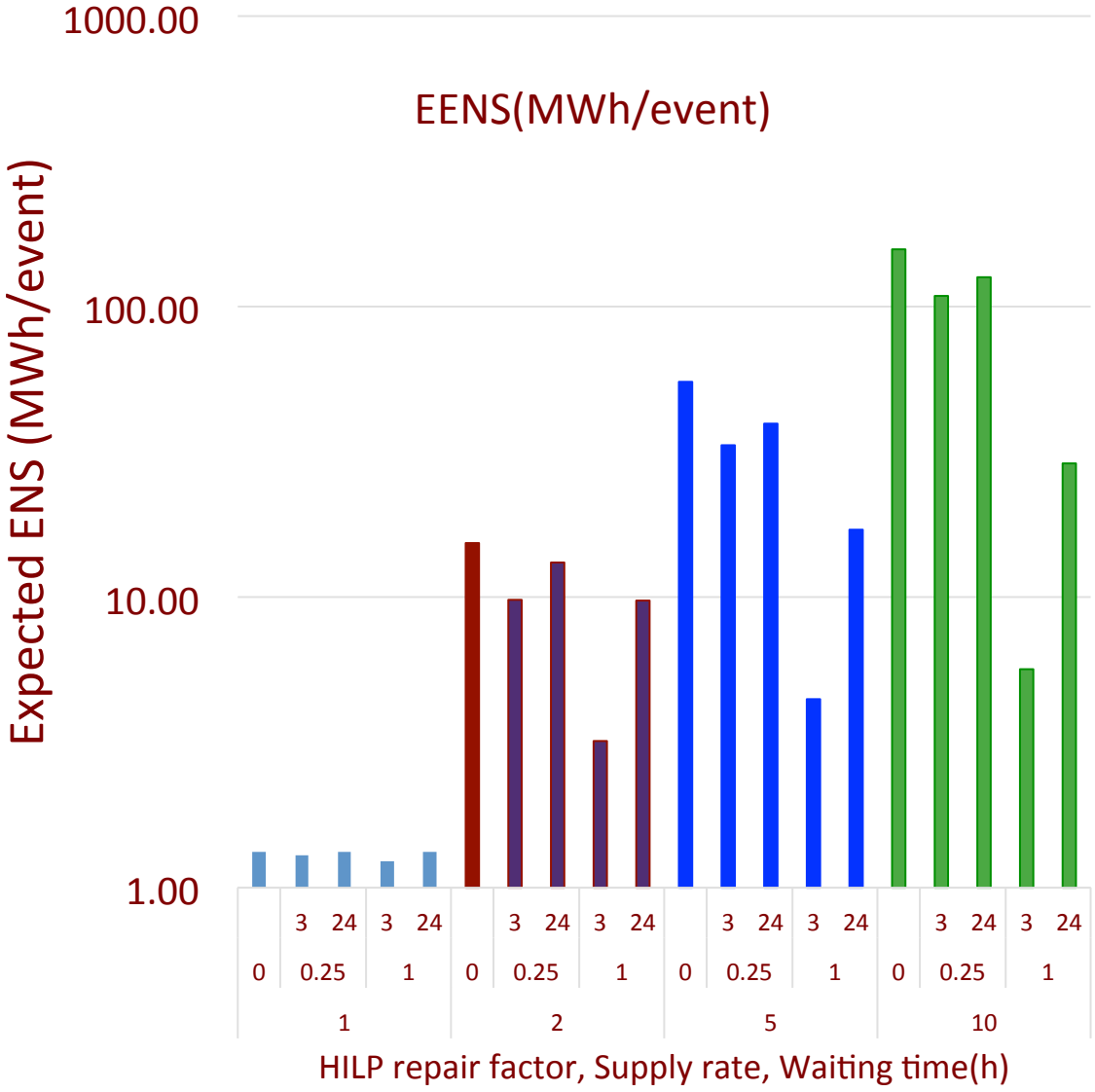
Reliability delivered by DSR against network reinforcement

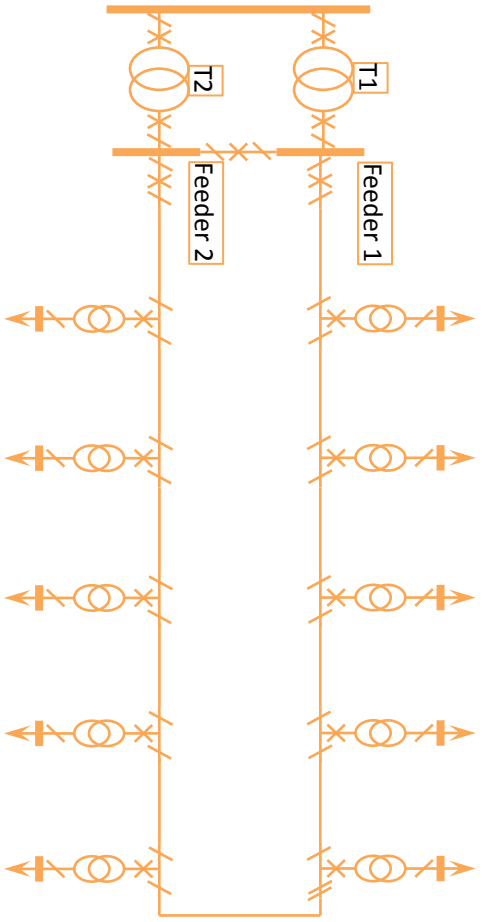


Common mode failure



Dealing with HILP – impact of storms on performance of distribution overhead feeders: support from micro-grids

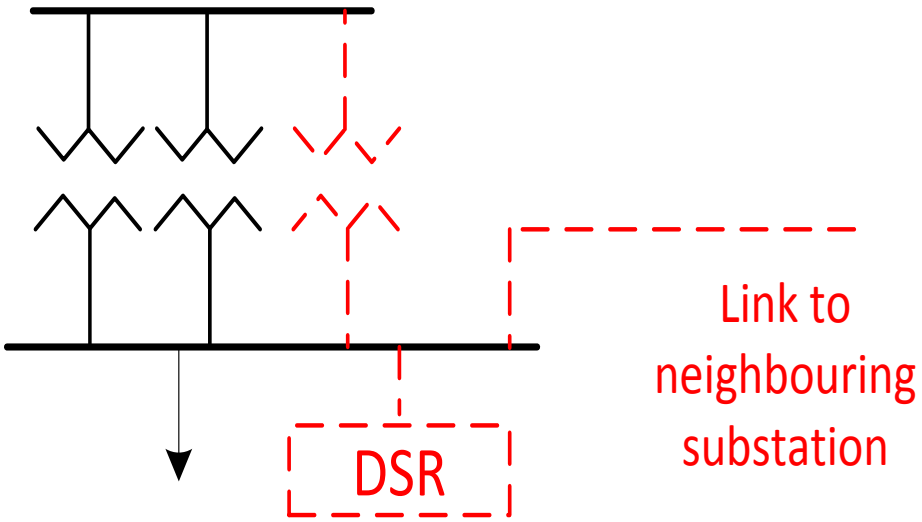




Should HILP be considered in the network standards?

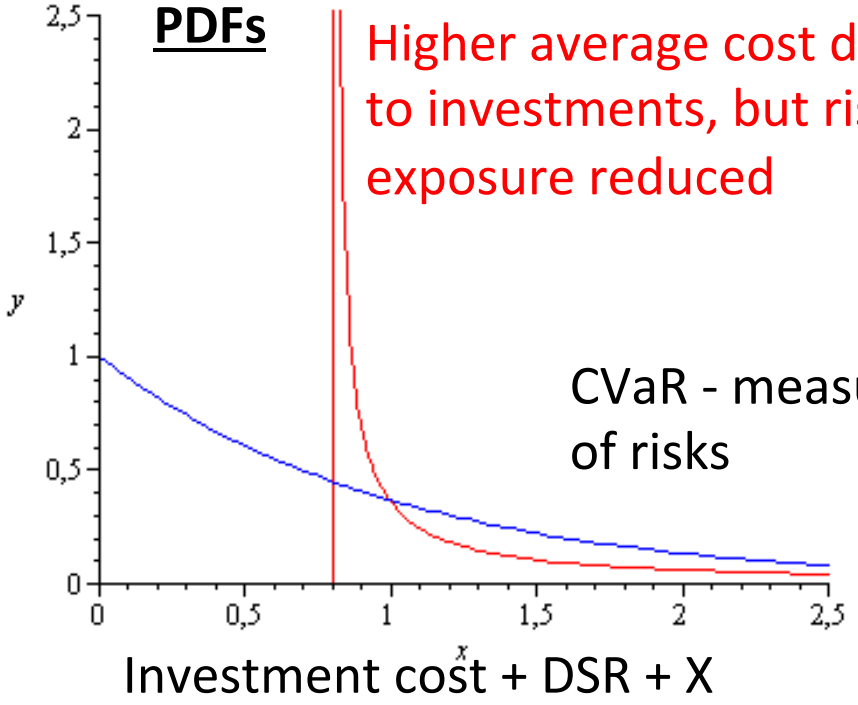
Robust design – *Portfolio of solutions*

DSR or network reinforcement?



PDFs

Higher average cost due to investments, but risk exposure reduced



CVaR - measure of risks

Investment cost + DSR + X

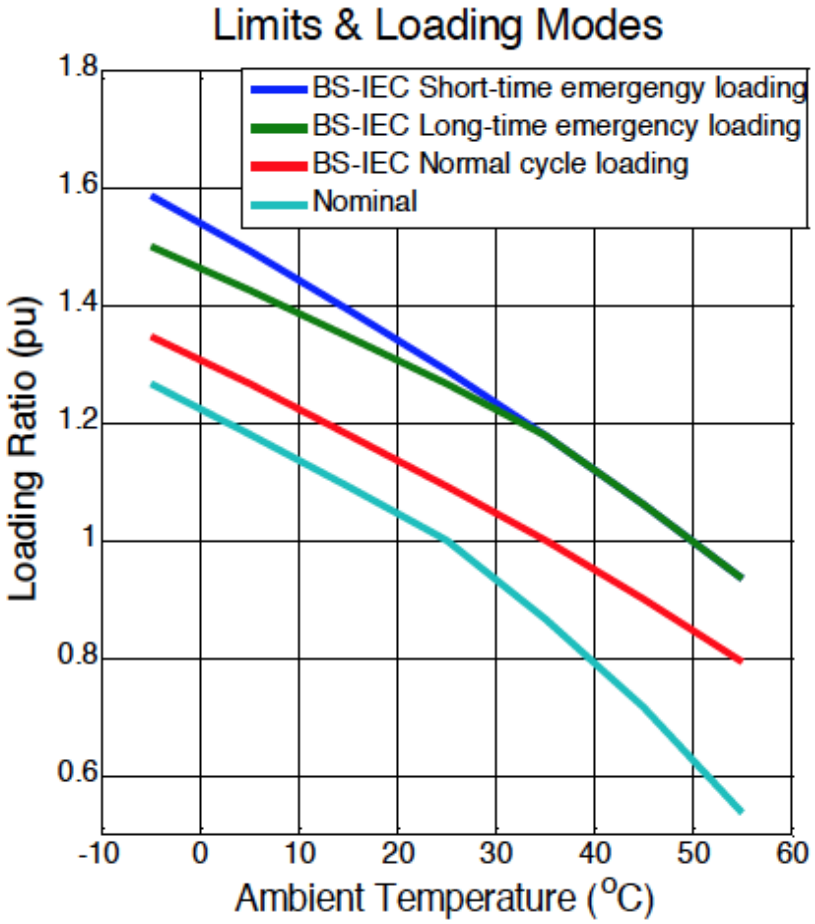
(1) Average cost approach:

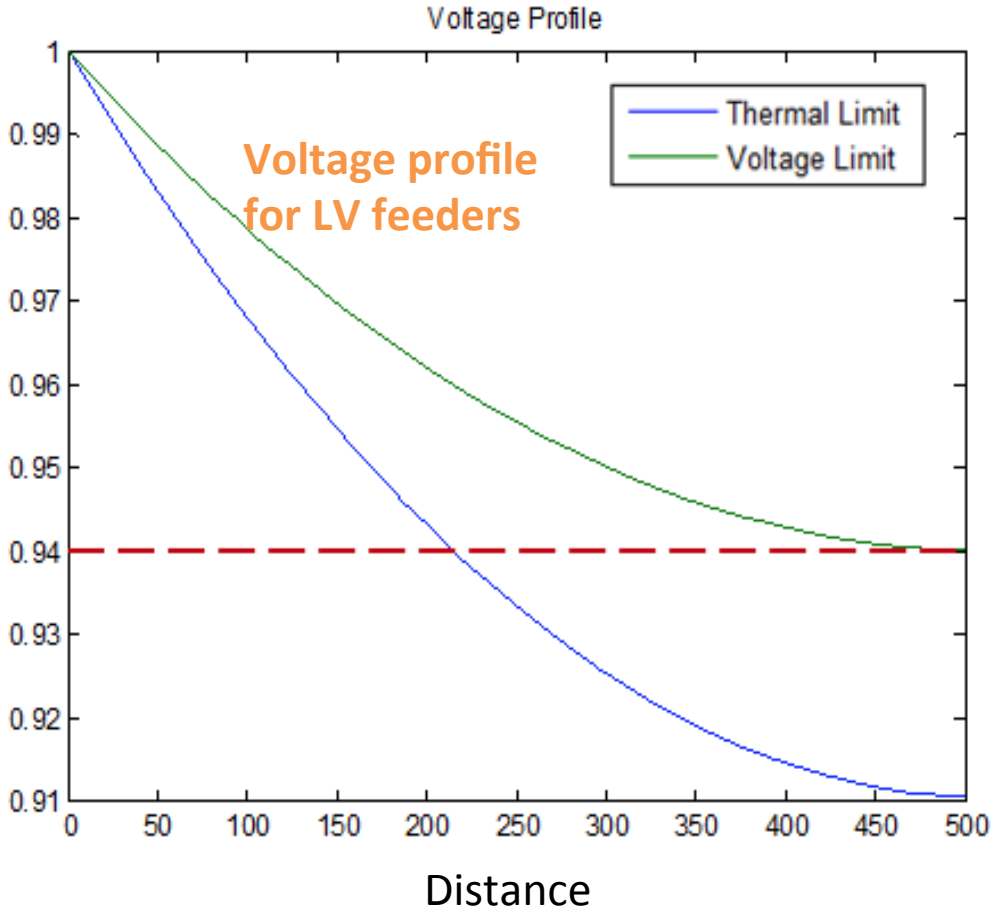
- DSR - no need for network reinforcement
- How about exposure to ICT failures?

(2) CVaR approach:

- ***Portfolio***: both DSR and network solutions
- Lower exposure for HILP

Emergency power and voltage control

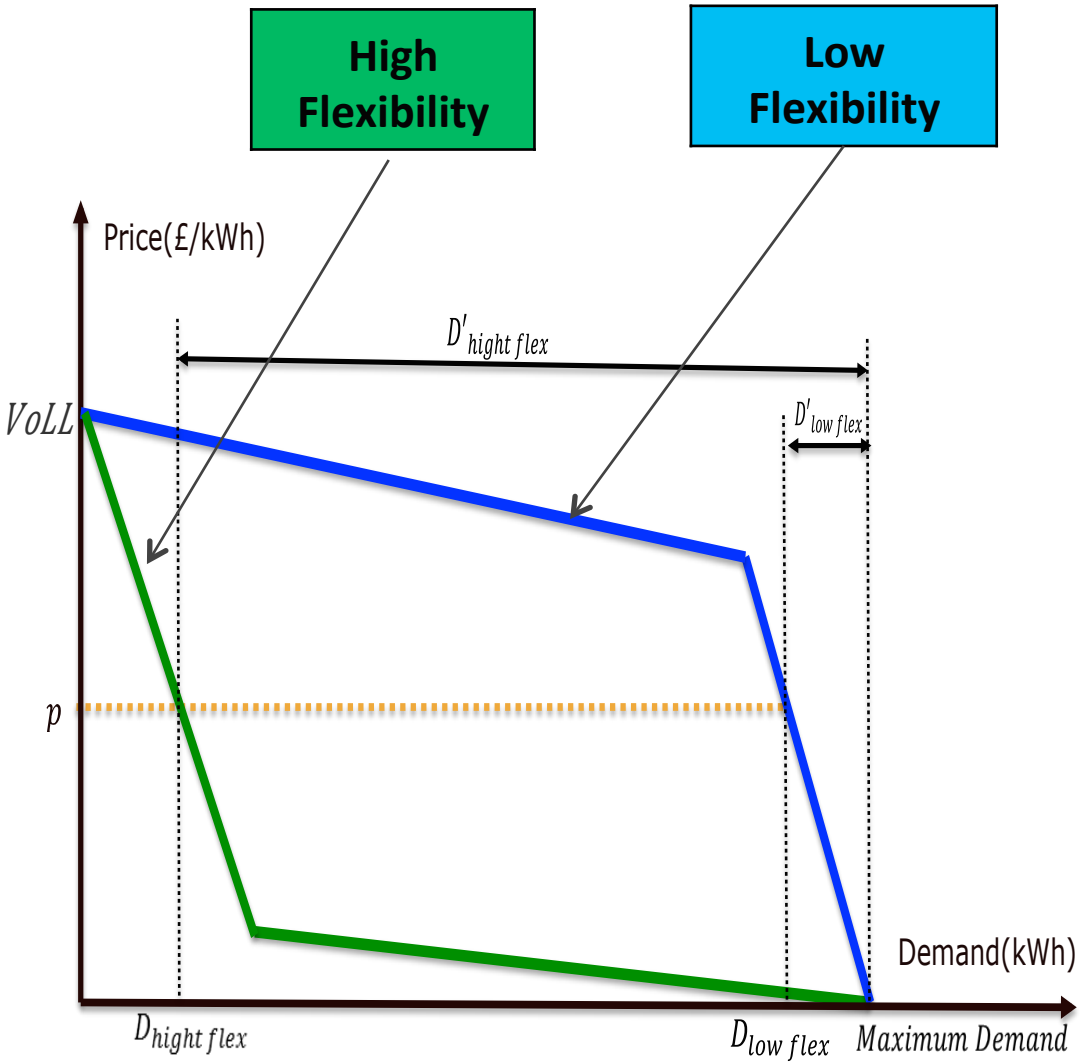




Driving assets harder during emergency conditions

How far the voltage limits can be extended under emergency conditions?

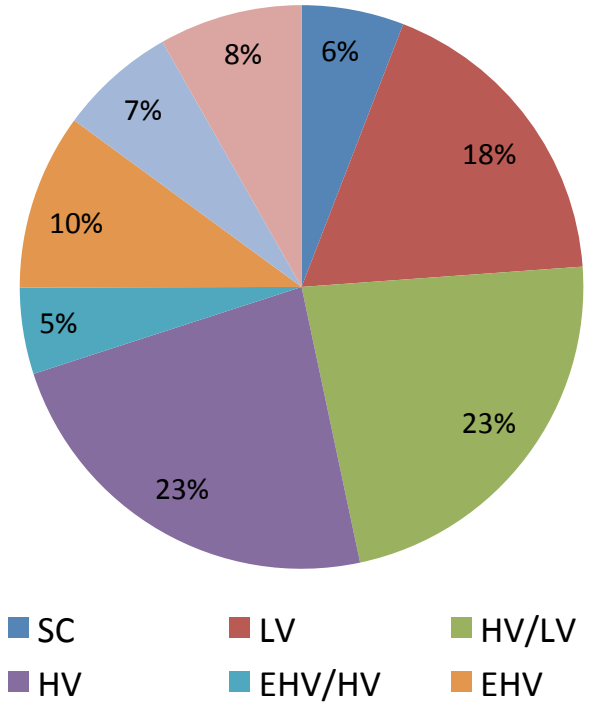
Consumer driven design



- Network congestion can be managed by *scarcity pricing* - consumer would reduce their loads depending on their flexibility and the value they attribute to the service
- Essential supplies would be delivered to all consumers
- Bill for low flexibility consumer would higher than the bill for flexible consumer
- Flexibility will inform extent and time of network reinforcement.

Longer term:
Loss inclusive network design

About 50% -70% of network losses in urban areas are in HV and LV networks



Loss-inclusive network design

Under-ground Cables	Peak Utilisation(%)	Ratio of peak capacity and peak demand
LV	12 - 25	4.0 – 8.3
MV	14 - 27	3.7 – 7.1
HV	17 - 33	3.0 – 5.9

- **Significant opportunity to enhance reliability of supply in future micro-grids - making full use of large network capacity and enhance network security beyond present standard**

Improving current policy and regulatory & commercial regime

- Strategic approach to future T&D network design needed to facilitate cost effective and secure evolution to lower carbon future
- Strengthening the incentives for development & implementation of cost effective smart grid measures, while recognise increased risk and complexity associated with innovation and deployment of new technologies
- Whole-systems approach to network operation and design – enhancing long term security of supply
- Change the role of the Regulator: from acting as a buyer of network services to developing appropriate incentive mechanisms

Imperial team involved in quantitative analysis presented:

Rodrigo Moreno, Predrag Djapic, Simon Tindemans, Dimitrios Papadaskalopoulos, Hadi Karimi, Enrique Ortega, Thomas Frost, Paul Mitcheson, Danny Pudjianto

Imperial College London

Symposium on Microgrids Aalborg 2015

Smart Grids European Technology Platform:

Network security and resilience and role of microgids

Goran Strbac
Imperial College London