

# Working together on digitalising wind

Vasiliki Klonari

Senior Digitalisation & System Integration Analyst

[vk1@windeurope.org](mailto:vk1@windeurope.org)

# Why going digital?



TSO-DSO



Real-time grid support capabilities



Synergies with other power generation



Consumer synergies



Sector Coupling



Storage



Improving productivity



Decrease OPEX



Decrease CAPEX



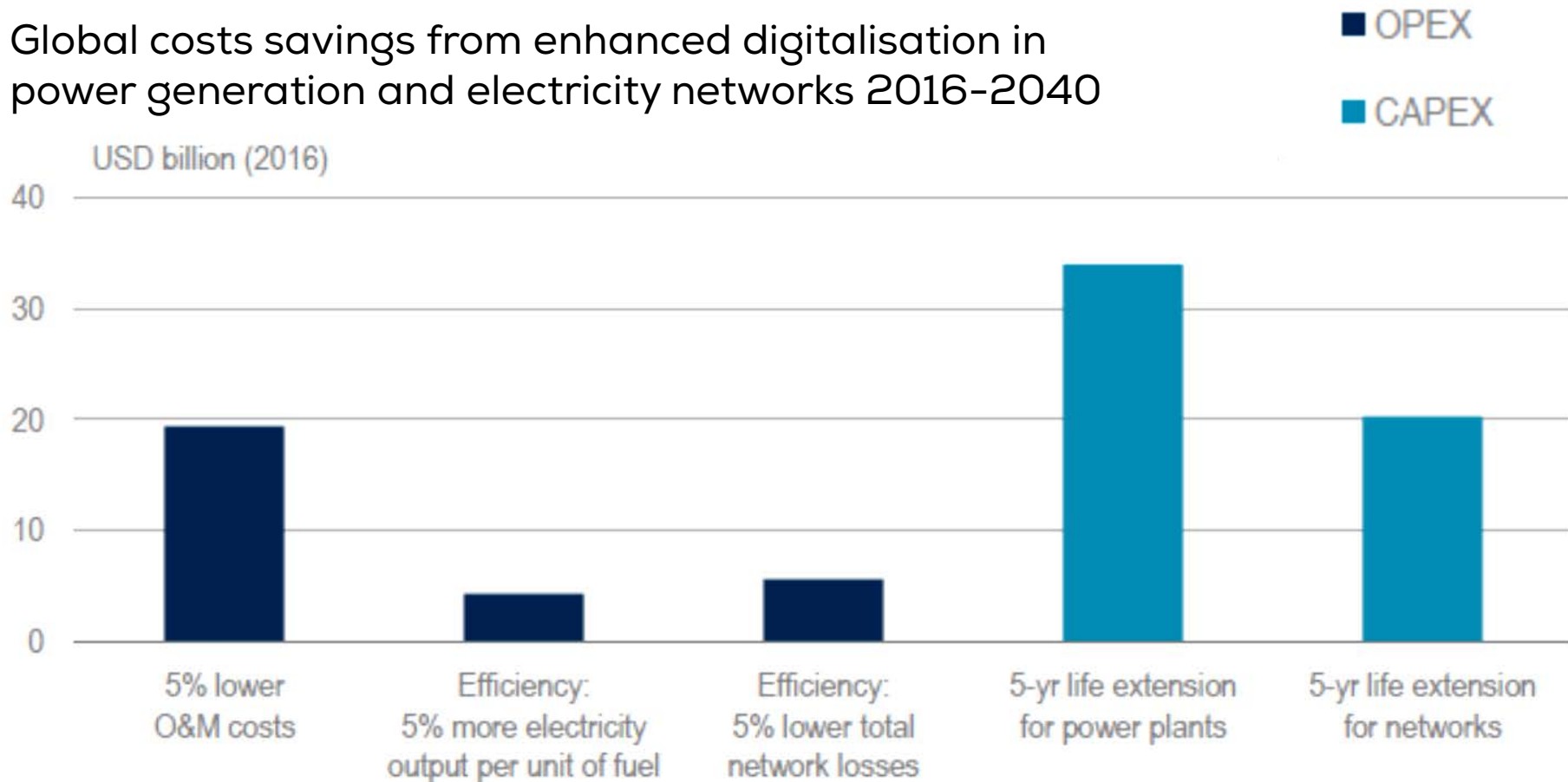
Lifetime extension



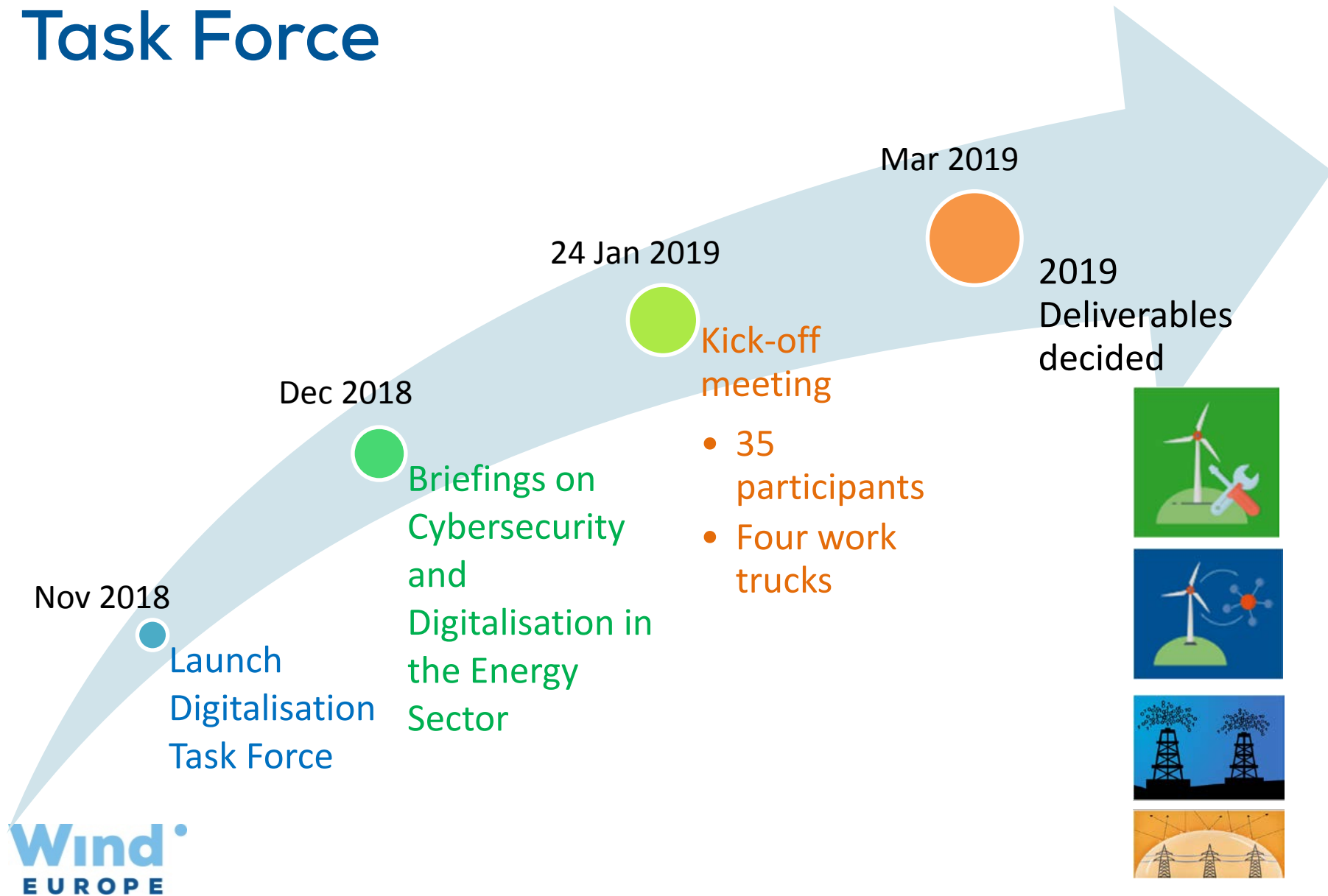
Improving value of each MWh produced

# Why going digital?

Global costs savings from enhanced digitalisation in power generation and electricity networks 2016-2040



# WindEurope launches Digitalisation Task Force



## Briefing on Cybersecurity in the Energy Sector

By Vasiliki Konari, Senior Digitalization and System Integration Analyst, Market Intelligence, WindEurope

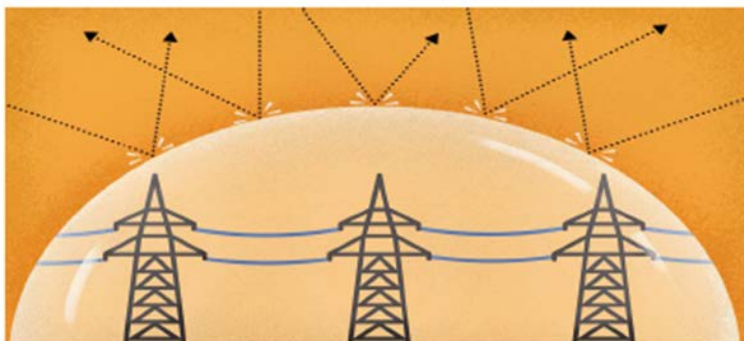


Figure 1 Cyber security for Critical Information Infrastructure. Source: Razonneur

### KEY FACTS

- > Higher penetration of renewables requires flexibility which needs increased connectivity and therefore multiplies the number of cyber-attack platforms.
- > Utilities and energy is the second most vulnerable sector to cyber-crime
- > According to the International Energy Agency, the energy sector believes that companies and public spending in cybersecurity is insufficient, driven by an under-estimation of the threat. As a result, the relevant EU industry remains highly dispersed.
- > In December 2018, the EU Cybersecurity Act has been politically agreed. Cross sector actions are planned. Moreover, the EC recently proposed investments in this key area between 2021 and 2027.

### CYBERSECURITY IN THE ENERGY SECTOR

Cybersecurity in the energy sector serves two principal purposes; securing systems that provide essential services to the society and protecting data exchange in such systems along with the privacy of citizens.

In time line terms, cybersecurity in energy systems relates to real time requirements, cascading effects and short or long term issues of legacy regarding digital technologies.

#### Cybersecurity sectoral approach for energy

In 2015, the European Commission created the *Energy Expert Cyber Security Platform* (EECSF). The platform identified ten energy-specific cybersecurity challenges (Table 1) and concluded that the existing policies and regulations weren't sufficient to tackle these issues. Indeed, thirty nine regulatory gaps were identified. The

For questions:  
Vasiliki Konari  
vasiliki.konari@windeurope.org

## Mapping digitalisation actions in the EU energy sector

By Vasiliki Konari, Senior Digitalization and System Integration Analyst, Market Intelligence, WindEurope



Figure 1 The Impact of digitizing energy. Source: Cisco Newsroom

### KEY FACTS

- > All energy stakeholders are active in the digitalisation process; some of them fully engaged and others still initiating to it
- > For most stakeholder groups, digitalisation has two main roles to play: cost reduction in asset management and new revenue streams thanks to system integration
- > The two main pillars of work are: a) Regulatory framework ruling grid users roles and responsibilities (including data ownership and management, b) technology innovation through EU funds
- > A special focus is put on security and privacy in data sharing, internally or with third parties, which is inherent to every digitalisation process

### DIGITALISATION OF THE ENERGY SYSTEM

Digitalisation of the energy system translates into moving to digital technologies to change business

models and generate new revenue streams and value propositions in the energy sector.

As a concept, digitalisation has been around for almost a decade. Lately, the ongoing electrification and the increasing share of renewables accelerate the digital adaptation of the energy system.

Energy stakeholders have all been active digitising their everyday practices and long term strategies. Some of them are fully committed to the new adventure while others slowly discover the benefits of the process.



Figure 2 Digitalisation breaks down boundaries between energy sectors, increasing flexibility and enabling integration across entire systems. Source: International Energy Agency

# Specific topics to be addressed in 2019

- **Digitalisation of asset management and operation:** adapt operation model to life cycle stage and business model
- **Digitalisation in system integration:** adapt system operation practices to wind generation
- **Cybersecurity** as a practice in the wind sector
- **Standardising exchanges in data marketplaces**

# Let's work together on these questions:

Which are the specific business needs to solve?

Which are the barriers or challenges to solve them?

Current industry practices to address the needs

"Digitised" existing solutions or disruptive new solutions?

How can we work together on these needs?

# Digitalisation of asset management & operation

## Needs

Life time extension

High O&M cost

Performance degradation

Obtaining value for data

Adapt operation to life cycle stage and business model

Logistics optimization

De-risk capital strength

Reduce built-in excess costs

## Barriers

O&M costs “sink”

Getting stakeholders point of view integrated in the supply chain

Accuracy of prediction models

Data quality & ownership

No data standardisation exists

Legacy data systems

How to monetize data



# Digitalisation of asset management & operation

## Solutions

Benchmarking - comparing outcomes

O&M versus asset management

Cloud Systems for small manufacturers

Digital twins

Standardisation of data sharing

Recognition of cost for data effectiveness

Standardise how wind technologies are monitored

## Work together

Better understand the needs of asset owners

Help small operators take accurate predictions on replacement needs

# Cyber security & data exchanges

## Needs

Policies harmonised among EU  
realisable, assessing risks, not  
limiting operations/growth

Stable connection, always online

Multiple direct access to the  
asset

Data: standardized exchange  
templates

Data: aggregation of assets

## Barriers

Balancing business needs with  
security standards

Underestimation of the risk

Lack of expertise in Europe

Underestimation of cyber  
security costs

Lack of clarification of data  
ownership

Companies still reluctant to  
discuss/ estimate the value of  
data

# Cyber security & data exchanges

## Solutions

Data marketplace -  
interesting to  
investigate?

Service for retrofitting  
forecast models  
(sharing data with  
forecasters)

## Work together

Feasibility studies for data  
marketplaces

Regulatory analysis and gaps

Working on one cyber security  
standard

Working on perception of  
cyber security - benchmark  
for different generators

Mapping and definition of  
data to be exchanged

# Thank you!

Ideas to contribute?

Contact [vk1@windeurope.org](mailto:vk1@windeurope.org)

**Wind**<sup>•</sup>  
EUROPE

[windeurope.org](http://windeurope.org)



WindEurope, Rue d'Arlon 80  
1040 Brussels, Belgium