Horizon
The EU Research
& Innovation Magazine

European Commission

Europe's power grids readied against cyber attack

Alternative transmission lines and encryption protocols could steel Europe's power grids against a cyber attack – the big question is where to deploy them.

18 September 2015 - By JON CARTWRIGHT

Little has changed in power grids since the first national ones were established in the 1930s. But now scientists, engineers and other experts are rethinking European networks.

The vulnerability of power grids to hackers was demonstrated in 2010, when a computer worm known as Stuxnet derailed nuclear centrifuges in Iran. The worm – which is thought to have been developed by an advanced nation state – was the first known cyber attack on physical infrastructure.

The consequences of a cyber attack on an active power grid could be disastrous. There would be not only the cost of repairing the immediate damage, but also the cost of the disruption to homes, businesses and services that rely on electricity.

Drawing on expertise from power-network security, technology policy, regulatory economics, disaster impact assessment, network simulation and engineering, a project known as SESAME is the first that has been funded by the EU to take on this problem.

‘What we have provided is a comprehensive approach to power-system security,’ said Professor Ettore Bompard, the scientific coordinator of SESAME and a power-systems engineer at the Polytechnic University of Turin in Italy.

Blackout simulator

They’ve designed a blackout simulator which works out how much a blackout would cost, so that operators can decide whether it is worth deploying expensive countermeasures. These could include installing alternative transmission lines in case a regular line fails, and encrypting information.

Prof. Bompard and colleagues from universities and companies across the EU have come up with a system that gives grid operators the information they need to make decisions in the face of a potentially devastating cyber attack.

They tested it on two national power grids: Austria and Romania, for the latter of which they had real comprehensive data. According to Prof. Bompard, independent operators in both countries agreed with the recommendations to install certain support systems to defend their grids in the event of a cyber or conventional attack.

However, it can also partially rely on people who put energy into the grid from domestic wind turbines and solar panels. Should a centralised power station fail, said Prof. Bompard, these people could keep the grid partially flowing with electricity.

‘For security, this is a chance,’ he said. ‘You can keep the neighbourhood power system working even if there is a blackout at a transmission level.’

This distributed power generation model is one ingredient of what have come to be called smart grids – power networks that can respond in more flexible ways to 21st century energy supplies and demands. Such demands come, for example, from electric vehicles, the widespread use of which can exert a massive drain on a power supply at peak times.

Managing smart grids entails the efficient shifting of power from one region to another, and controlling the times of the day when certain power is allocated. But that is also fraught with risk.

On the fly

Technology that's already being tested in an operational power grid in the Netherlands, based at Dutch grid company Alliander, means that in the case of a blackout, the way the grid is managed can be reconfigured on the fly to keep power flowing where it's needed.

It's all thanks to a revolutionary new system known as C-DAX, which was put together in a laboratory at the École Polytechnique Fédérale de Lausanne in Switzerland.

Today's grids are run using stand-alone manned units known as silos, with each one managing separate demands on electricity. However, in the EU-funded C-DAX system, each silo is turned into a virtual representation - known as a topic - which can be adapted and reconfigured as needed.

That flexibility makes it much more resilient to an attack.

‘The topic-based communication provides inherent security since target hosts are obscured,’ explained Dr Matthias Strobbe, a computer scientist at Ghent University in Belgium.

Not only that, but because C-DAX is a new system, they have been able to incorporate security measures such as multi-level encryption right from the start, whereas the silos are inefficient and do not have cybersecurity functions built in.

'C-DAX incorporates proven security measures addressing authentication, privacy and integrity in an end-to-end fashion,' said Dr Strobbe.

Cyber security in Europe

The EU's cyber security strategy includes a proposed directive on network and information security which is aimed at enhancing the resilience of information systems across Europe.

It is a key component of the EU's Digital Agenda, as it sees trust and security as a vital part of a vibrant digital society.

The directive, which is currently under discussion by lawmakers, would require Member States and critical infrastructure operators to take measures to ensure that the digital environment is secure and trustworthy.

For more information: https://ec.europa.eu/digital-agenda/en/cybersecurity

More info

SESAME

C-DAX