Towards a safer smart grid framework

The European solar/PV industry of the near future will live and die by the strength and effectiveness of smart grids, and the organisation charged with ensuring its longevity is the European Network and Information Security Agency. The organisation’s Ulf Bergstrom talks us through some security recommendations for the public and private sector involved in the definition and implementation of smart grids, and offers workable steps forward...

**Improve the regulatory and policy framework**

The EC should take the lead and develop specific policy documents and regulations on cyber security and privacy of the smart grid in order to improve the current regulatory and policy framework. This extended framework should define and develop, by taking into account existing regulations and policies on smart grid, the root principles, challenges, goals and needs of a long-term European-wide cyber security and privacy strategy for the grid of the future. Policies and regulations should at least look for: 1) considering privacy and cyber security as two intrinsically interdependent topics; 2) defining security measures to be considered in current smart grid deployments (e.g. smart meter roll-outs); 3) demanding grid operators for mandatory risk assessments; 4) demanding manufacturers, integrators, services providers and grid operators to comply with specific security certifications; 5) establishing regulatory pressures (e.g. fines) for not complying companies; 6) making public the compliance results; 7) demanding operators to report on cyber security related incidents to a national or supranational entity.

**Objective**

The articulation of a broad and complete regulatory and policy framework would bring cyber security to the front-line of action, recognising these matters as key factors for its success and as an essential and fundamental part in the definition of smart grid business models, functionalities, services, etc. Establishing regulatory pressures for not complying companies will help change their mentality, which will be important for evaluating cyber security at the pilot phase or for avoiding companies dismissing cyber security for budgetary or lack of experience reasons. It would change the perception that Europe is not paying enough attention to cyber security and privacy in smart grids. Moreover, cyber security and privacy would be treated as a whole and not as two separate disciplines.

On the other hand, this legal framework would help harmonise existing policies and regulations addressing cyber security, and will be considered as a reference with which to align policies and regulations on other aspects. This would be the case of those promoting smart meter roll-outs or the integration of different energy types (e.g. heat, gas and electricity) at the metering infrastructure. In combination with other recommendations provided in this document, this new framework will ensure a minimum level of harmonisation on security and resiliency requirements across Member States, establishing the basis to allow National Regulatory Authorities (NRAs) to effectively measure security and to make comparisons among different companies.

**Steps**

- At the European level, the necessary contacts network has to be established: DG ENER, DG CONNECT, DSOs, TSOs, CEN/CENELEC/ETSI SGSG, Smart grid Task Force, etc.
- Regulatory pressures and other mechanisms are analysed in detail with the involved stakeholders
- The previous regulatory actions are analysed and considered as a basis for improvement
- A strategy for implementing the regulatory framework is defined
- Policy documents, EC communications and Directives are prepared and published according to the previous strategy

**Foster awareness raising and training initiatives**

Under the umbrella of the aforementioned PPP, EC, ENISA and the MS and the should foster the creation of initiatives targeting awareness-raising of C-level (e.g. CEO, CTO, etc.) staff of grid operators, electricity services providers, manufacturers and end consumers in relation to the importance of the cyber security and data privacy in the smart grid. Besides, specific training initiatives should also be created for manufacturers on how to build secure devices and applications, for grid operators on the threats and risks affecting the resiliency and security of the grid, as well as for services providers and end consumers on fraud prevention, privacy, etc.

**Objective**

Fostering awareness and training will probably contribute to change the generalised perception that cyber security is not a first interest matter in the development of the smart grid. For instance it will probably help changing mentality to avoid situations where utilities do not consider cyber security as an important issue until massive roll-outs. Training, adapted to the profile of the trainees (e.g. specific training according to staff positions, end consumers, etc.), manufacturers, etc. will also contribute to establish a security culture in organisations and end consumers as well as raise their expertise in the field.

Among the basic objectives of CERT organisations contributing to raising security awareness is one of the most
relevant. For this reason, CERTs – preferable those specialised in industrial ICT – are very well positioned to contribute to the purposes of this recommendation.

**Steps**

- Build a network of C-level contacts for the main grid operators and services providers in Europe.
- Identify the forums and events of interest of C-level staff.
- Prepare the appropriate media for raising awareness on smart grid security aspects of C-level staff.
- Participate in the identified forums and events.
- Organise through the appropriate channels (e.g. ENISA) specialised technical events for raising awareness and training.
- Analyse, in cooperation with CERTs and other platforms such as ENCS (former CyberTECH), the alternatives for fostering awareness rising and training.

**Foster dissemination and knowledge-sharing initiatives**

Under the umbrella of the aforementioned PPP, EC, ENISA and MS should actively involve security providers and academia in current knowledge sharing initiatives, as well as increase DSO/TSO leadership in cyber security initiatives. Besides, dissemination of the results of existing initiatives should be actively encouraged. Moreover, the creation of a platform for knowledge sharing among DSOs and TSOs – and possibly other stakeholder – should be analysed. To this respect CERTs could play a role as a unified point for information exchange among smart grid stakeholders as well as a reference for valuable information (e.g. good practices distribution).

**Objective**

Grid operators will have a central role in the development of the smart grid and should be the ones providing the largest number of security requisites. For this reason it is necessary that they have a leading role in cyber security initiatives. Additionally, encouraging existing initiatives to actively disseminate their work will help reduce their lack of visibility while an EU level coordinating entity for smart grid cyber security initiatives is created.

In addition to contributing to raising security awareness, CERT organisations are also expected to be a reference on valuable information about ICT security. For this reason, CERTs – preferable those specialised in industrial ICT – are very well positioned to contribute to the purposes of this recommendation.

**Steps**

- Build a network of C-level contacts for the main grid operators and services providers in Europe.
- Identify the forums and events of interest of C-level staff.
- Establish a global strategy for disseminating the activities and results being undertaken by active initiatives.
- Apply the dissemination strategy in a coordinated and coherent manner.
- Leverage the built network of contacts to achieve that DSOs and TSOs have a leading role in information sharing initiatives as well as to actively involve academia/R&D.
- Analyse, in cooperation with CERTs and other platforms such as ENCS (former CyberTECH), the alternatives for establishing a knowledge sharing platform.

**Develop a minimum set of reference standards and guidelines**

The EC, in collaboration with ENISA and the MS competent authorities and the private sector, should develop, by leveraging existing initiatives, a minimum set of reference standards and guidelines on cyber security for the smart grid. The set should include at least: 1) a common reference architecture; 2) a reference risk assessment methodology; 3) technical requirements for smart grid systems; 4) guidelines on security governance for legal entities involved in the future grid; 5) guidelines for achieving fool-proof home networks. This body of standards and guidelines shall set a basis for conducting assessments and support the development of a European certification scheme for vendors and grid operators.

**Objective**

Smart grid companies along the value chain are getting more and more interconnected and interdependent. Therefore, there is the necessity of an end-to-end security approach, from the lowest levels (meters, physical, etc.) to the upper ones (application systems, integration with corporate systems, value-added services, etc.) and all along the smart grid value chain. It is considered that having a standard architecture of the smart grid is on the basis of such a strategy. Moreover, a consensus-based reference standard architecture is central to avoid cyber security initiatives being “paralysed” from addressing challenges such as the secure integration of legacy systems in a robust, resilient and smart grid, or segmenting ICT infrastructures devoted to “competitive” aspects (e.g. added-value services for consumers) from non-competitive ones (e.g. metering or grid operations).

Cyber security and privacy should be addressed at the design phase so as to minimise costs and maximise security. Defining standard technical requirements for smart grid systems will allow vendors to take them into account during the design phase. Moreover, they would set a basis for defining a security certification scheme for smart grid products. These requirements should not only focus on smart meters but be further extended to other critical smart grid subsystems, especially secondary distribution substations, primary distribution substations, transmission substations, micro grids, control centres operated by SCADA systems, and the IT and telecommunication systems linking all them together. These technical standard requirements should be based in existing initiatives such as ISA 99 on security controls for embedded devices or WIB’s requirements for vendors.

Finally, since Home Area Networks are directly dependent of end consumers, associated systems need to be completely fool-proof, and for this purpose secure and security technology will play a key role. Specific guidance on this topic is necessary to allow defining the best suited architecture or selecting the most appropriate technologies (i.e. encryption).

**Steps**

- Analyse the current work being done by initiatives such as the SGIS working group or DG CONNECT’s ad-hoc EG.
- Leverage existing information sharing platforms to fully understand industry expectations, compare them against existing work, and identify gaps.
- Establishing a common reference architecture should be set as the main priority.
- Develop the common reference architecture.
- Leverage previous experience on smart grid risks assessment methodologies by actively involving DSOs and TSOs.
- Develop a risk assessment methodology coherent with the common reference architecture.
- Based on the common reference architecture, define a number of technical requirements for smart grid systems.
- Develop best practices guidelines on security governance, and for achieving a fool-proof HAN/IAN/BAN.

PES would like to thank ENISA for this extract. For the full report and list of steps, please visit [www.enisa.europa.eu](http://www.enisa.europa.eu).