# European Distribution System Operators for Smart Grids

## Akıllı Şebekeler İçin Avrupa Dağıtım Sistemi Operatörleri

**Network and information security (NIS):**
Recommendations for information sharing and risk management

**Ağ ve Bilgi Güvenliği:**
Risk Yönetimi ve Bilgi Paylaşımı ile İlgili Tavsiyeler

**September** / Eylül 2014

EDSO
for smart grids

Elder
tarafından bastırılmıştır.

EDSO
for smart grids

# European Distribution System Operators for Smart Grids

## Network and information security (NIS): Recommendations for information sharing and risk management

*September 2014*

# Executive summary

Our modern society is highly dependent on a constant power supply, and Distribution System Operators (in cooperation with Transmission System Operators) are in charge of maintaining a high-level quality of service and guaranteeing the security of supply. In the rare cases that outages occur, public life quickly comes to a halt, billions of euro can be lost and the continued delivery of vital services cannot always be guaranteed.

The European Commission highlighted this fact on March 30th 2009 in its Communication on Critical Information Infrastructure Protection, a paper on protecting Europe from cyber disruptions by enhancing the security and resilience of key infrastructure. In 2012, a new Directive was proposed for a high level of common network information security (NIS Directive), aiming to improve risk management, cooperation and trust between public and private authorities for this purpose. However, the guidelines provided in the text to help member states reach these objectives are limited.

EDSO has prepared this paper to address NIS from the perspective of a critical energy infrastructure operator, and to help member states to implement the future Directive through the promotion of risk management procedures and set-up of efficient information sharing networks.

Based on experience from existing information sharing platforms, interviews with security experts and drawing on existing ENISA publications, EDSO recommends that member states:

## Recommendations related to cyber risk management

- Promote the use of risk management methods and standards (examples listed in the paper)
- Promote certification schemes for organisations which comply with a set of standards for cyber security risk management
- Create guidelines that commit all organisations to nominate, and appropriately train, senior members of management teams to be responsible for cyber risk management.

## Recommendations related to information sharing

- Limit the scope of each information sharing platform to one economic sector, better still, support the creation of European information sharing platforms, sector by sector
- Invite, where relevant, governments, service and technology providers to be directly involved in the platforms while at the same time limiting the number of participants and encouraging companies to, where possible, involve the same representatives over time in order to build trust among group members
- Encourage all participants to share accurate information, including threat, vulnerability, impact and risk assessments
- Set clear information sharing procedures (e.g. traffic light protocol) for disseminating information, taking into account their sensitivity
- Create tools to facilitate information sharing, e.g. an information hub, broadcast mechanisms, secure email, secure chat and discussion groups
- Ensure access to the platforms is free of charge
- Ensure the authority coordinating the platforms is a legal entity capable of taking disclosure responsibility for the information being shared, held and disseminated
- Invest in building the necessary expertise to analyse, coordinate, and act upon the data received.

# Table of contents

# 1. Introduction

Our society is highly dependent on a constant power supply, and Distribution System Operators (in cooperation with Transmission System Operators) are in charge of maintaining a high-level quality of service and guaranteeing the security of supply.

In the rare cases that outages occur, public life quickly comes to a halt, billions of euro can be lost and the continued delivery of vital services cannot always be guaranteed. With the ongoing development of automation and monitoring of medium and low-voltage grids, and the resulting increase in data flows, the operation of the power grid is becoming more dependent on information and communication technologies (ICT). These systems offer numerous advantages for network control, but these are currently coupled with the risk of malicious use. It is, therefore, essential that the necessary protection against cyber threats is established.

The European Commission highlighted this fact on March 30th 2009 in its Communication on Critical Information Infrastructure Protection (CIIP)[1] a paper focused on protecting Europe from cyber disruptions by enhancing the security and resilience of key infrastructure. Two years later, in March 2011, the European Commission announced follow-up actions in a new Communication on CIIP entitled Achievements and next steps: towards global cyber-security[2]. This Communication concluded that purely national approaches to tackling security and resilience challenges were not sufficient, and that Europe should continue its efforts to build a coherent and cooperative approach across the EU.

As a result, the European Commission proposed a Directive on measures for a high level of common network information security (NIS Directive)[3], currently being discussed by the EU institutions, and expected to be approved by the end of 2014. This draft Directive goes one step further by seeking to improve risk management, cooperation and trust between public and private entities. It states that information collected from private companies will be collected and checked by a central national authority and will be shared with other companies and countries. Industry-specific national networks of experts, in particular in the area of critical infrastructure operators, will be assembled to share knowledge about cyber threats to vital economic sectors. These two requirements are, however, kept very vague and would benefit from the addition of indications for member states on how to implement them.

Last but not least, in 2013, the European Commission launched the NIS Platform, with the aim of providing guidance on how to increase cyber security in Europe. The platform has successfully gathered a large number of representatives from ICT companies, although few energy sector representatives have, so far, been involved.

EDSO has prepared this paper to help bridge this input-gap by addressing NIS from the perspective of critical energy infrastructure operators, and to help member states to implement the future Directive by setting up efficient information sharing networks and developing a risk management culture.

[1] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0149:FIN:EN:PDF
[2] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0163:FIN:EN:PDF
[3] http://ec.europa.eu/digital-agenda/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security

## 2. Protecting critical infrastructure through information sharing and risk management

The European Parliament has already provided a first reading position on the NIS Directive, emphasising two aspects of cyber security: risk management and information sharing. Revised article 5.a.1 requests that member states establish a "risk management framework to establish a methodology for the identification, prioritisation, evaluation and treatment of risks, the assessment of the impacts of potential incidents, prevention and control options, and to define criteria for the choice of possible countermeasures"[4].

As for information sharing, the text only calls on national governments to set up a national strategy, including cooperation mechanisms between the public and private sectors, without further elaboration.

These two aspects of cyber security are complementary and require both the companies concerned and national governments to build trust and work together to reach a high level of security. Already setting some core guidelines so these strategies can one day fit under European umbrella risk management and information sharing systems could help to reduce efforts and costs later down the line.

### a. Developing a risk management culture

Smart grids entail introducing millions of new intelligent components to energy infrastructures that communicate and control energy distribution in much more advanced and optimal ways than in the past. Such new components, however, introduce new risks and vulnerabilities that have to be faced in carefully thought-out and innovative ways.

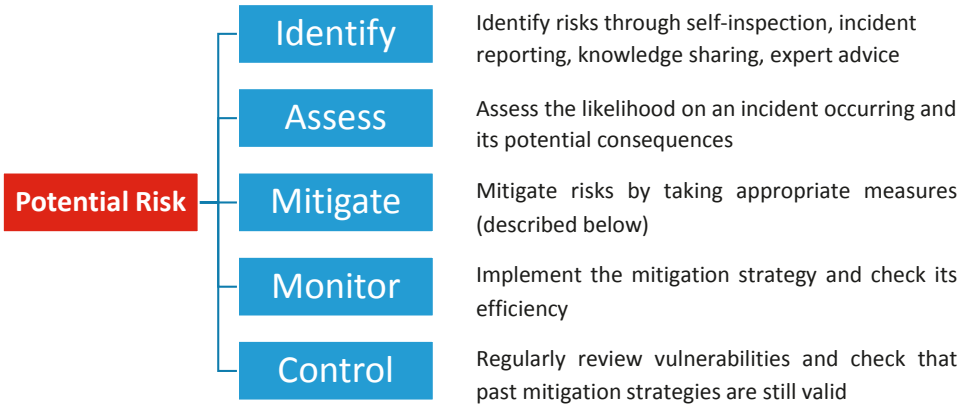
Risk management planning is a key aspect of guaranteeing the processes for, and technical means of, ensuring potential risks and vulnerabilities in smart grid information systems have been fully addressed.

Furthermore, in order to develop appropriate security measures, each organisation must first identify and classify the risks. This involves undertaking security assessments of smart grid information systems and interconnections to identify critical components and any areas deemed weak in terms of security. The risk identification and classification process should be continually performed in order to determine the compliance status of smart grid information systems.

Risk management is based on steps that can be summarised, as per Figure 1 below, and which include: identifying, assessing, mitigating, monitoring and finally, controlling.

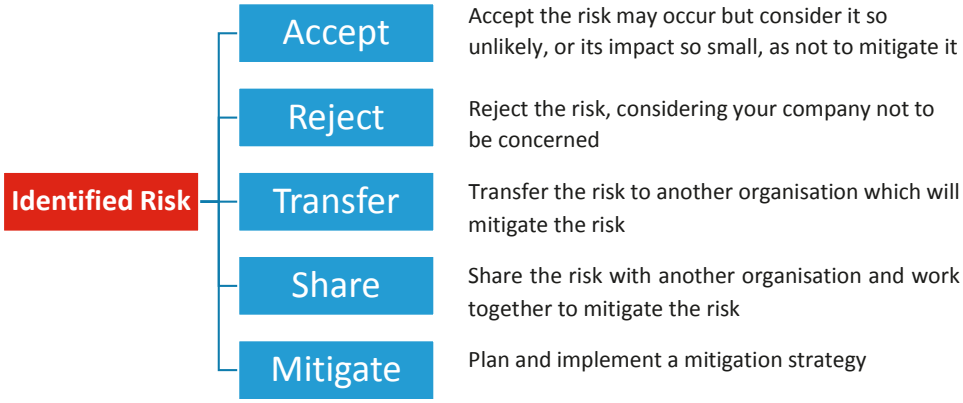
[4] http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2014-0244+0+DOC+XML+V0//EN

**Figure 1: Risk identification and mitigation process**




Following the assessment of cyber security risks, resolution and mitigation are undertaken and should, as summarised in Figure 2, result in one or more of the following actions for each risk: accepting, rejecting, transferring, sharing and / or mitigating[5].

**Figure 2: Management process of an identified risk**




This risk management process will continue on a constant basis to monitor and update the list of identified risks and assess the efficiency of the mitigation strategies used. For DSOs and all operators of critical infrastructure, risk management should also include the supply chain, ensuring that equipment manufacturers and service providers connected to the networks carry out the necessary risk assessments and mitigation activities. This requires having trained professionals available to carry out such assessments and to encourage all employees to always consider risks and security when doing their jobs, including at the highest level of companies. **Active promotion of training and certification would thus be a positive step for all companies managing critical infrastructure.**

[5] ENISA, Smart Grids Threat Landscape and Good Practice Guide, December 2013

Regarding risk assessment methods, several methodologies are already being used by the industry. Although this paper does not recommend one, it introduces a number of risk assessment models and explains how they relate or diverge.

There are two main categories of risk assessment methodologies. The *quantitative* are more objective and benefit from a more assertive approach to cost-benefit analyses, given that assessments are based on calculations and estimations of the probability of a risk, its cost, and the cost of prevention. The *qualitative* approach is more subjective, since it does not involve calculations and mainly results from the opinions of the experts. These methodologies also have varying degrees of abstraction (from concrete methods specifying which equipment to use, to more abstract methods explaining how to design your security system) and look at different timeframes. From the methodologies available, the more frequently used are listed in Table 1, below.

**Table 1: Summary of common risk assessment methodologies**

| Focus | Temporal | Functional | Comparative |
|---|---|---|---|
| **Abstract** | Red Team | Schneier | GAISP |
| **Mid-Level** | Pen Test | OCTAVE | ITIL |
| **Concrete** | Scripts | CRAMM | ISO 27001<br>ISO 27019 |

Even though risk management is a key step towards ensuring the security of smart grids against cyber threats, it needs to be accompanied by an appropriately developed information sharing system if the full benefits are to be drawn from the exercise.

## b. Making information sharing work among critical infrastructure operators

DSOs have become increasingly aware of cyber threats and risks in recent years. The critical nature of the energy sector is making it an attractive target for criminal activities. Therefore, most energy sector stakeholders, particularly utilities and vendors, have been developing their own cyber security strategies. These are, however, separate efforts. There is currently no common understanding of the threats across the sector, and there have not been sufficient pushes for coordinated actions at national or European level to reduce energy infrastructure cyber security risks to acceptable levels.

To add to this, secrecy remains of high importance for the electrical equipment and ICT manufacturing business, often discouraging companies to share important details about their products that could affect the security of entire energy infrastructures.

Through information sharing, DSOs can potentially reduce the impact of an incident. For instance, in case a cyber-incident occurs on DSO network X, sharing the lessons learnt and response to the incident with the European DSO community could potentially avoid the same type of incident occurring for DSO network Y. At the very least, the incident could be responded to in a more efficient and appropriate way than if the information had not been shared. Furthermore, sharing best practices on privacy and security by design for smart grid related use-cases can increase the quality of the services offered by DSOs.

Information sharing is not a burden, but should be considered a potential source of benefits and savings. In 2010, ENISA commissioned a survey[6] to better understand the motivation of experts involved in cyber security cooperation networks. Among the responses were:

- Cost savings from avoided threats
- Timely, specific and useful data sharing
- Privileged information from government or security services
- Clear and easy processes and structures for sharing

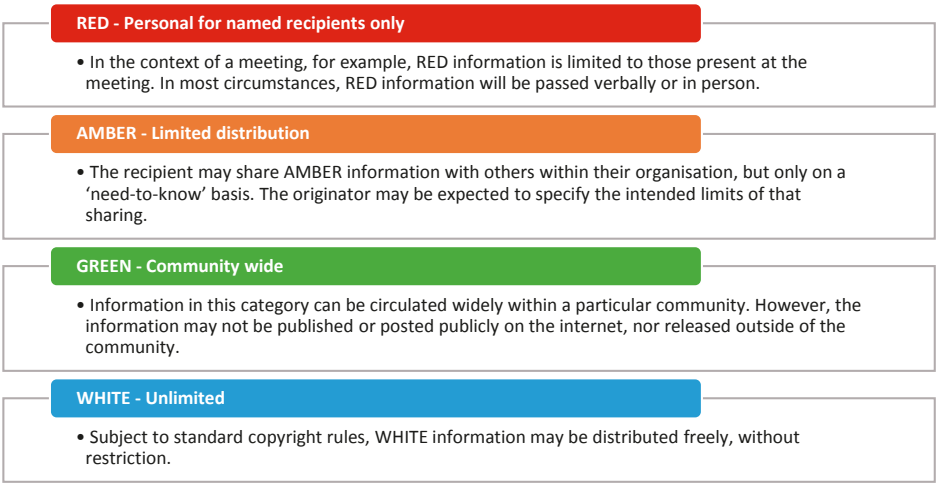
In addition to the incentives listed by ENISA, others should be taken into account. Sharing information may facilitate the adoption of new cyber security technologies and practices in a technologically and vendor-neutral manner that will help to keep pace with emerging terrorist and other cyber security threats and developments. Support to research, development and innovation will also continue to play an important role here. DSO networks would be more secure if:

- Threat and incident data, alerts, vulnerabilities and patches were shared
- Trend analyses were used to plan appropriate operational and management responses for enterprise-wide attacks
- Threats or risks of attack that could lead to operational, market and reputation disruptions and/or regulatory and compliance failures were shared outside of the sector, with the appropriate authorities / affected sector platform
- Best practices were drawn from the shared information and applied from control rooms across Europe.

To make the most of information sharing, all studies and surveys among experts undertaken by ENISA show that trust is pivotal to creating a community of people willing to share and process critical information efficiently**. To build trust, groups sharing information are usually limited in size, membership is set to remain stable and clear guidelines are provided for communicating information**. A method like the traffic light protocol (abbreviated as TLP and presented in Figure 2 below) is an example of a clear and simple way to share information. Each piece of information shared with the group is labelled by the information provider with one of four colours, to indicate what further dissemination, if any, can be undertaken by the recipient(s).

[6] ENISA, Incentives and Challenges for Information Sharing in the Context of Network and Information Security, 2010

**Figure 2: Description of the Traffic Light Protocol (TLP) for information sharing**




In order to improve communication between participants, it is also important that the coordinator of the group, which is usually a **governmental body, is the one taking responsibility for sharing a piece of information with a wider audience**, if deemed necessary. In this way, participants of the platform are encouraged to share sensitive information, reassured by the fact that the legal entity managing the platform will be responsible in case of leaks, and not the individual sharing the information in the first place.

However, building trust is not only about setting up functional communication processes. The behaviour of the participants and of the convenor have a significant impact on the efficiency of the platform. As mentioned in the ENISA report[7], a number of shortcomings can lead an information sharing platform to failure and inefficiency:

### Poor quality of information exchanged

Detrimental to the platform's success are the presence of non-experts who can only gather information but not use it directly or contribute to the discussion, or very vague guidelines on which information is expected to be shared.

### Participants following "security by obscurity" principle

Participants purposely limiting their contribution to avoid revealing what could give a competitive edge to other participants.

### Sharing "trust factors" not well defined and/or agreed by participants

Unclear guidelines given by the convenor of the group regarding to whom the information can be disseminated and shared with.

[7] Ibid.

### Fear for reputation if vulnerability disclosed

Disclosing past incidents or vulnerabilities can be considered a risk to company reputation, especially if revealed to the general public.

### Fear of legal actions by customers if security breach revealed

Linked to the previous concern, the fear of leading a company into legal difficulties should it be revealed publicly that there has been a data leak can lead participants to retain information.

### Composition and poor management of information sharing platforms

An information sharing platform gathering too many members, and especially from different sectors with different interests, is inefficient. Furthermore, delays in the transmission of alerts and information by the convenor to the group lower the value of the platform.

### Culture of secrecy within governments

The participation of different governmental services from countries with a culture of secrecy is sometimes reported as being an obstacle to cooperation, with government representatives only releasing important information to participants when the news of a vulnerability is already known of the public.

### Companies reluctant to invest in security when no specific threats identified

The company culture is also listed as a potential obstacle, with some companies reluctant to invest time and effort in a knowledge sharing network when no clear threats are identified.

Building trust and a sustainable information sharing platform is a difficult task which several countries have already undertaken, and which many more are yet to set-up. To help assess in non-abstract terms what such platforms could look like, Section 3 of this paper looks at how information sharing platforms have been set up in the United States, the first to create such a platform, and in the Netherlands, where the existing platform meets practically all of the requirements set out in the NIS Directive proposal.

# 3. Learning from existing cyber security cooperation networks

Several countries have set up information sharing networks or platforms, but this trend is still limited. The United States (US) was the first to organise such a cooperation facility and the Netherlands was a frontrunner in Europe, operating today a network that meets practically all requirements laid out in the proposed NIS Directive. These examples are presented below, followed by details of a planned EU-funded project that will aim to set up a European platform for DSOs.

## a. Existing cyber security cooperation networks

### Cyber security cooperation in US electricity sector

In 1998, the US created[8] the Information Sharing and Analysis Centers (ISAC) for critical sectors. ISACs are trusted, sector-specific organisations that establish their sector's information and intelligence requirements for security incidents, threats and vulnerabilities. There are currently 17 active ISACs covering all key economic sectors (banking, transport, emergency services, etc.). One is dedicated to critical energy infrastructure, the Electricity Sector ISAC (ES-ISAC).

The ES-ISAC, operated by the North American Electric Reliability Cooperation (NERC) is a not-for-profit international regulatory authority whose mission is to ensure the reliability of the transmission power system in North America. The management and staff of ES-ISAC are NERC employees, however, they are segregated from the NERC compliance staff. The government connection for ES-ISAC is the US Federal Department of Energy, who acts as "sector liaison" with the federal government.

The ES-ISAC serves the electricity sector by facilitating communications between industry participants, the federal government and other critical infrastructures. The ES-ISAC promptly shares threat indications, analyses, warnings, and interpretations to assist industry in taking protective actions.

Membership in ES-ISAC is not mandatory, but is strongly encouraged. Reporting of cyber incidents to ES-ISAC is mandatory for utilities, but non-members can also report incidents. Any registered entity under NERC standards can become a member of ES-ISAC. It includes Canadian and Mexican companies. Membership gives access to private-level information on security threats, including:


In order to encourage wide participation, no direct fee is applied. Operation of ES-ISAC is covered by the NERC budget, which is itself funded by a portion of the charge paid by utilities for participating in the electricity market.

[8] Presidential Decision Directive 63, signed May 22nd 1998

## Dutch experience of information sharing

In 2011, the Dutch Ministry of Security and Justice produced a Strategy of Cyber Security[9], which was followed-up with the launch of a National Cyber Security Centre[10] in 2012, designed to organise information sharing and defend more efficiently the sectors most vital for society. Following the US example, several cooperation and information sharing platforms, called Information Security and Analysis Centres (ISACs), were created for each key economic sector:

- Energy ISAC
- Financial Institutions ISAC
- Multinationals ISAC
- Telecoms ISAC
- Managed Services Providers ISAC
- Health ISAC
- Insurance ISAC
- Water ISAC
- Nuclear ISAC
- Harbour ISAC
- Airport ISAC

The Energy ISAC includes all network operators, the DSOs and the TSO together. Participation is not compulsory but highly encouraged by the government. **In order to lower barriers to participation, membership is free.** Meetings are organised every six to eight weeks, and each participating company appoints one or two security officers to the ISAC. The meetings are facilitated by the government, but the agenda is mainly based on the topics, concerns and issues brought forward by the company representatives involved. As meetings are organised roughly every two months, in between, a newsletter reporting relevant news and threats is sent to the members of the groups. An additional newsletter, containing less sensitive information, is sent to a wider group of security experts.

In case of repeated non-attendance, an individual can be expelled from the group, but the company can appoint a replacement without penalty. Members have to sign a non-disclosure agreement and no records of the meeting are kept, for confidentiality reasons.

Membership is partially open. The first members have been invited by the government but new members can join. To be accepted as a participant in the platform, an existing member has to propose the inclusion of a new company in the group. A unanimous vote is then needed to accept the new participant.

Another procedure has been put in place to enable external experts to join a specific meeting and share their knowledge. One can join a meeting for a specific presentation, upon invitation only, if previously agreed with the other members of the group. The external participants can only be part of the meeting for their presentation and have no possibility to stay past that timeslot.

Information is controlled and instructions are given on which information can be shared, with whom, using a system close to the abovementioned traffic light protocol.

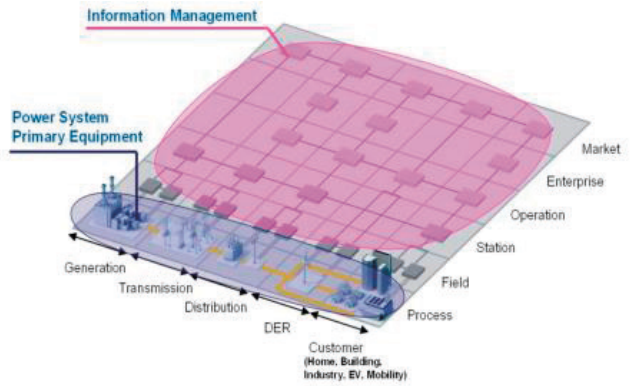
In case one member of the group spots a security breach, he must inform the Dutch cyber security centre. The experts from the centre then decide if this information has to be disseminated to the whole ISAC or to other ISACs, since ISACs are separated and do not interact with each other.

[9] Dutch Ministry of Security and Justice, National Cyber Security Strategy, June 2011
[10] https://www.ncsc.nl/english

## b. New industry initiative for network operators: DENSEK project

Beyond national platforms, a new European-funded project, DENSEK (www.densek.eu), will aim to move towards an integrated European energy security approach. The abbreviation DENSEK refers to Distributed Energy Security Knowledge and is part of an EU Critical Infrastructure Protection (CIP) program from the Directorate General Home Affairs of the European Commission focusing on 'prevention, preparedness and consequence management of terrorism and other security related risks'. The DENSEK project, launched in July 2013, explicitly targets all stakeholders in the energy distribution value chain, since each stakeholder forms a potential internet entry to the grid.

**Figure 3: Information Management layer of the Smart Grid[11]**




DENSEK aims to improve the resilience of European energy networks, which it plans to achieve through the implementation of a multi-layered knowledge-sharing base consisting of:

| | |
|---|---|
| 1 | A European Energy-ISAC (EE-ISAC), providing a trusted Information Sharing and Analysis Centre for its members. The ISAC will be sharing relevant energy related information and experiences on cyber security, executing analyses of cyber security alerts/incidents and providing the results to its members. |

In order to equip the EE-ISAC with the required tools to perform its role adequately, two information systems are being developed and implemented:

| | |
|---|---|
| 2 | An Information Sharing Platform, that provides the ISAC and its members with a trusted communication channel through which they can liaise with each other and exchange information. |
| 3 | A Situation Awareness Network, which continuously monitors the safety of the relevant energy supply chains for cyber threats. Any threat that may occur will immediately be communicated to all members of this trusted network in the form of alerts. |

The project will run for 24 months. At the end of this period, in July 2015, the multi-layered knowledge community should be in place and the information systems successfully tested and fully operational. This project is a first instance of DSOs voluntarily setting up an information sharing platform together and might be used as "food for thought" for national and European policy makers when designing their own platform.

[11] Source: CEN-CENELEC-ETSI Smart Grid Coordination Group Smart Grid Reference Architecture, November 2012

# 4. Conclusions and summary of recommendations

With increased automation and ICT technology supporting the operation of electricity infrastructure, new risks arise. Distribution System Operators are potential targets of external attacks and thus considering the best ways to maintain quality of service and security of supply. The future NIS Directive is an opportunity to further develop a risk management culture among DSOs and to increase information sharing on cyber threats.

Based on the examples presented in this report, the experts interviewed and the literature analysed, increasing cyber security for critical infrastructure is a challenge that requires close cooperation between the public and private sector.

Based on this assessment, a series of recommendations can be made for policy-makers striving to make their critical infrastructure more secure:

## Recommendations related to cyber risk management

- Promote the use of risk management methods and standards (examples listed in the paper)
- Promote certification schemes for organisations which comply with a set of standards for cyber security risk management
- Create guidelines that commit all organisations to nominate, and appropriately train, senior members of management teams to be responsible for cyber risk management.

## Recommendations related to information sharing

- Limit the scope of each information sharing platform to one economic sector, better still, support the creation of European information sharing platforms, sector by sector
- Invite, where relevant, governments, service and technology providers to be directly involved in the platforms while at the same time limiting the number of participants and encouraging companies to, where possible, involve the same representatives over time in order to build trust among group members
- Encourage all participants to share accurate information, including threat, vulnerability, impact and risk assessments
- Set clear information sharing procedures (e.g. traffic light protocol) for disseminating information, taking into account their sensitivity, and create tools to facilitate information sharing, e.g. an information hub, broadcast mechanisms, secure email, secure chat and discussion groups
- Ensure access to the platforms is free of charge
- Ensure the authority coordinating the platforms is a legal entity capable of taking disclosure responsibility for the information being shared, held and disseminated
- Invest in building the necessary expertise to analyse, coordinate, and act upon the data received.

# 5. References


CEN-CENELEC-ETSI, Smart Grid Coordination Group Smart Grid Reference Architecture, 2012

CEN/CENELEC/ETSI, Cyber Security Coordination Group (CSCG), White Paper No. 01, "Recommendations for a strategy on European Cyber Security Standardisation", 2014

ENISA, Good Practice Guide Network Security Information Exchanges, 2009

ENISA, Incentives and Challenges for Information Sharing in the Context of Network and Information Security, 2010

ENISA, Appropriate security measures for smart grids -Guidelines to assess the sophistication of security measures implementation, 2012

ENISA, Smart Grid Threat Landscape and Good practices guide, 2013

ENISA, National Cyber Security Strategies in the World, various dates

European Commission, Communication on Critical Information Infrastructure Protection "Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience", 2009

European Commission, Communication on Critical Information Infrastructure Protection 'Achievements and next steps: towards global cyber-security', 2011

European Commission, Proposal for a Directive concerning Measures to ensure a high common level of network and information security across the Union, 2013

European Parliament, First reading position on a Proposal for a Directive concerning Measures to ensure a high common level of network and information security across the Union, 2014

Netherlands Ministry of Security and Justice, The National Cyber Security Strategy (NCSS), 2011
World Economic Forum, "Risk and Responsibility in a Hyperconnected World", 2014

Netherlands Ministry of Security and Justice, National Cyber Security Centre (NCSC)

United Kingdom Department for Business, Innovation & Skills, 10 steps to cybersecurity: executive companion, 2012

United States Government, Presidential Decision Directive 63 (PDD-63): Policy on Critical Infrastructure Protection, 1998

EDSO
for smart grids

*EDSO for Smart Grids is a European association gathering leading Electricity Distribution System Operators, cooperating to bring smart grids from vision to reality.*

**www.edsoforsmartgrids.eu**


Elder


**Türkiye 'de gerçekleşen planlı tüm elektrik kesintilerini bulabileceğiniz tek internet sitesi.**

**@ www.ekesinti.info**