Energy Community

BLUEPRINT energy SOLUTIONS

New Frontiers: Cybersecurity in the gas sector

Blueprint Energy Solutions GmbH
Aleš Hvala

Ljubljana, 25.09.2019

Cybersecurity in the energy sector

- **Real-time requirements** - energy systems needs to react so fast that standard security measures (command authentication, digital signature verification) cannot be introduced

- **Cascading effects** - electricity grids and gas pipelines are strongly interconnected across europe and well beyond the EU. An outage in one country might trigger blackouts or shortages of supply in other areas and countries

- **Combined legacy systems with new technologies** - many elements of the energy system were designed and built well before cybersecurity considerations came into play. "Legacy" must now interact with the new state-of-the-art equipment for automation and control, such as smart meters or connected appliances, and devices from the 'internet of things' without being exposed to cyber-threats

Tackling cybersecurity challenges in European Union

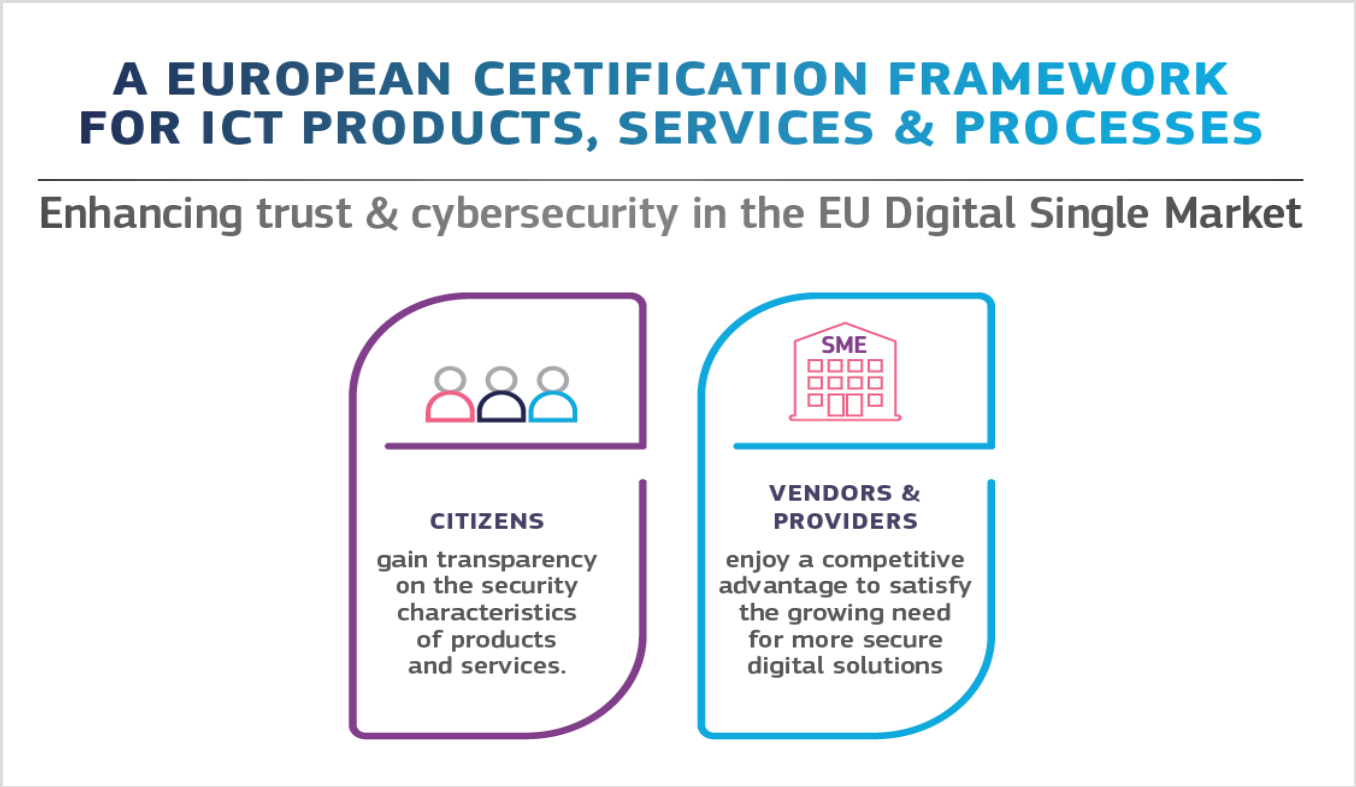
- NIST directive
  - The directive on network and information security (NIS) , from August 2016, requires each member state to establish a Computer Security Incident Response Team (CSIRT) and a competent national authority for NIS
- ECI directive
  - Directive 2008/114 on the identification and designation of European Critical Infrastructures and the assessment of the need to improve their protection sets out approach to the protection of critical infrastructures in the EU
- EU Commision Recommendations of 3.4.2019 on cybersecurity in the energy sector
- The EU Cybersecurity Act
  - The EU Cybersecurity Act from June 2019 revamps and strengthens the EU Agency for cybersecurity (ENISA) and establishes an EU-wide cybersecurity certification framework for digital products, services and processes.

Cybersecurity Act – ENISA in focus

A new era dawns on european union cybersecurity agency

- 7th June 2019, the EU Cybersecurity Act was published in the Official Journal of the European Union and came into force on 27th June 2019
- ENISA have a key role in setting up and maintaining the European cybersecurity certification framework (products, processes, services)
- ENISA is mandated to increase operational cooperation at EU level (national CSIRT secretariat,

Cybersecurity Act – ENISA in focus



Following the entry into force of the Cybersecurity Act on 27 June 2019, the European Commission has requested ENISA to prepare a candidate cybersecurity certification scheme to serve as a successor to the existing SOG-IS Mutual Recognition Agreement.

https://www.enisa.europa.eu/news/enisa-news/call-for-expression-of-interest-for-the-first-ad-hoc-working-group-on-cybersecurity-certification

ENISA activities regarding the EU Cybersecurity Act

- 4th September 2019, ENISA publishes a report to guide incident response teams forming a community to choose secure communications solutions.
- The methodology presented could also be valid for other operational teams grouped in an information sharing and analysis centre (EE-ISAC)
- ENISA is tasked to actively support the CSIRTs cooperation, provide the secretariat and active support for incident coordination

https://www.enisa.europa.eu/topics/csirts-in-europe/csirts-network

Study project of Energy Community

Study on Cybersecurity in energy

- Objectives:
  - Identify and assess key weaknesses, risks and exposure to cyber threats in the energy systems
  - Identify the existing regulatory framework and regulatory gaps for cybersecurity governance
  - Identify the relevant provisions of the NIS Directive and the Directive on European critical infrastructure and provide an impact assessment of their implementation in the Energy Community
  - Propose the necessary measures to improve cybersecurity in Contracting Parties (national level)
  - Propose a model for regional cooperation in managing cybersecurity risks and reporting incidents as well as a common cooperation platform, common certification framework and common framework for research, education and training programmes
  - Explore the possibility for the participation of Contracting Parties in the work of the European Union Agency for Network and Information Security (ENISA).

Study project of Energy Community

On the basis of Procedural Act 2018/2/MC-EnC: on the Establishment of an Energy Community **Coordination Group for Cyber-Security and Critical Infrastructure**, created among other to promote a high level of security of network and information systems and of critical infrastructures within the Energy Community, a coordination group for cyber-security and critical infrastructure was set up.

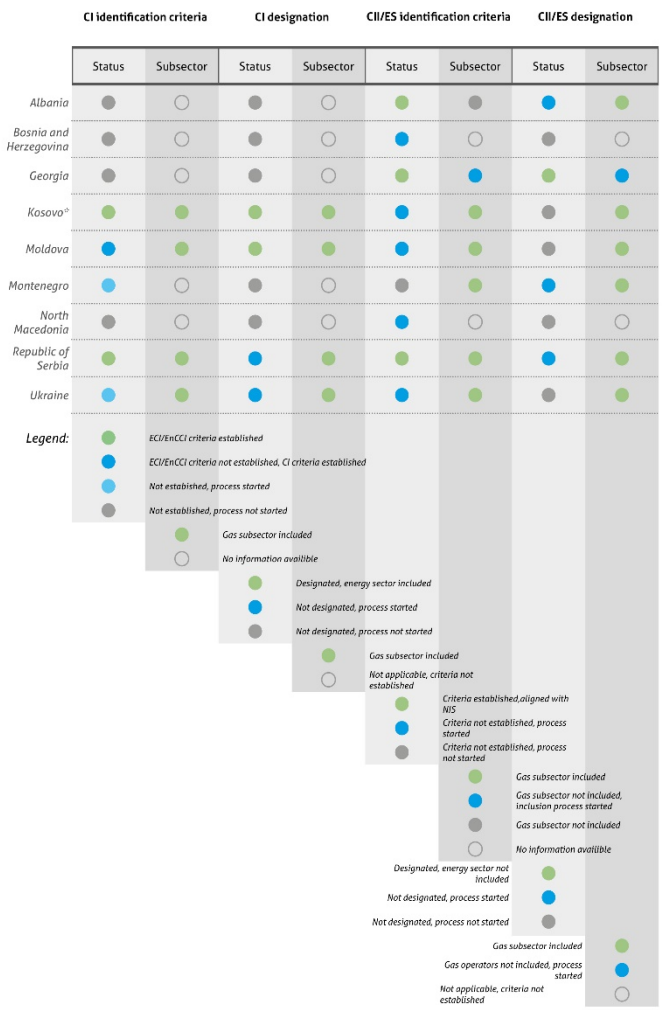
1st Cybersecurity Day in the Energy Community - gathering representatives from Ministries, regulatory bodies and system operators from Albania, BiH, North Macedonia, Georgia, Kosovo*, Moldova, Montenegro, Serbia and Ukraine

Overview, assessment and gaps of cybersecurity related institutional and legal frameworks in the energy sector of Contracting Parties

While the criteria for identification of ECI/EnCCI are present in the national legislation only in two CPs, situation is much better with the criteria for identification of essential services which are already established or in preparation in more than half of CPs.

Situation related to the identification of CI is very similar in the electricity and gas subsectors of the energy sector, the only difference being that CII/ES designation criteria in Albania does not include gas subsector

Gas ->



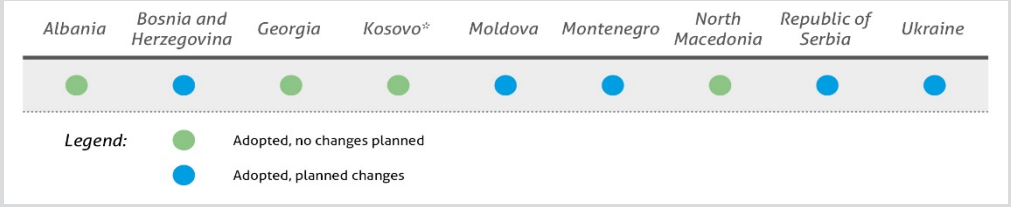
Abbreviation	Meaning
CI	Critical Infrastructure
CII	Critical Information Infrastructure
ECI	European Critical Infrastructures
EnCCI	Energy Community Critical Infrastructure

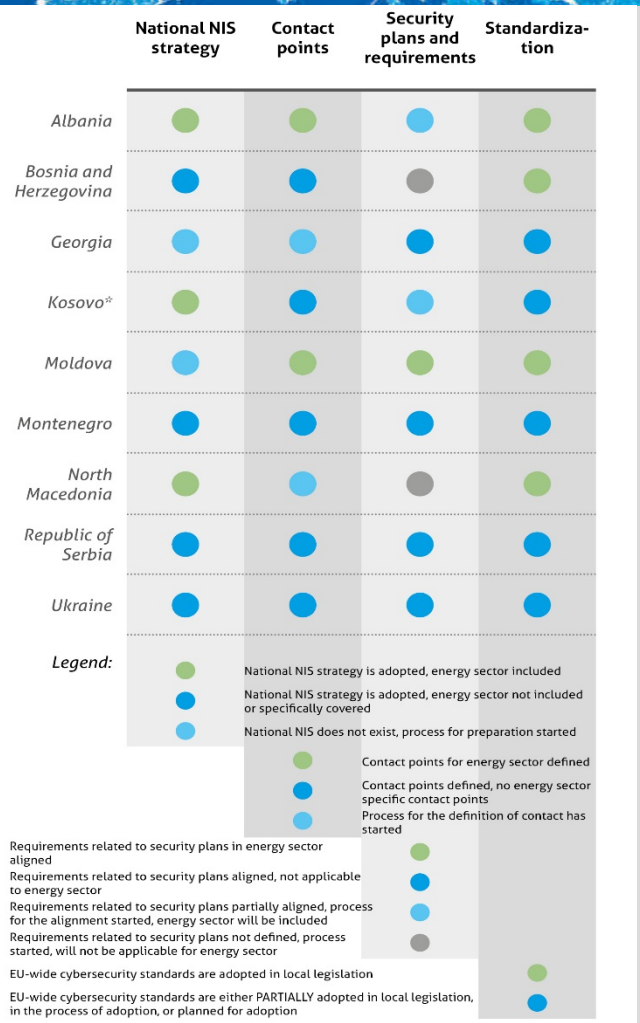
BLUEPRINT energy SOLUTIONS

Overview, assessment and gaps of cybersecurity related institutional and legal frameworks in the energy sector of Contracting Parties

Legal and institutional cybersecurity framework presents an overview of the current situation in each of the CPs of the Energy Community, regarding the existing cybersecurity and strategy processes that are in place or expected to happen in the short term.

Planned amendments of cybercrime legislation give an overview and assessment of on-going or planned activities related to transposition of EU wide cybercrime legislation in the national legislative framework.





BLUEPRINT energy SOLUTIONS

Overview of cyber threats and risks for EnC members

- The energy sector cybersecurity threat landscape changes in 2019 for EnC member states made significant shift in focus towards critical infrastructure protection.

- The possibilities of domino/cascading effect (cross-sectorial and cross-national as well) during cybersecurity incidents are in rise as legacy systems are overlapped with new technology (smart grid, virtual power plant etc.). The source of those developments was a shift in motives and tactics of the most important threat agent groups, namely cyber-criminals and state-sponsored actors hence a significant rise of cyberwarfare in energy as a threat.

- Based on the detailed risk assessment two categories of high risks were identified, which are very important to be taken into consideration for the EnC member stakeholders:

  - **IT and OT systemic/inherent risks** which are causing the most danger as they are undermining the security of supplies. These risks are often coming as a results of poor decisions in the past and must be addressed daily to correct them by operational controls.
  - **Organisational risks** which are originating from lack of standardized and functional operational controls in the energy sectors of EnC members. The operational controls[3] are supposed to eliminate IT and OT systemic/inherent risks or at least lighten them to acceptable levels. From the standpoint of EU these risks in EnC member states are often seen as compliance risks.

Overview of cyber threats and risks for EnC members

Cyber Threat							
Malware	Web Based Attacks/Web application attacks	Social engeneering/Phising/ Spam	Denial of Service (DoS)	Insider Threat	Cyber Espionage Cyberwarfare	Ransomware	Botnet
MEDIUM RISK for CA/NRA	NOT APPLICABLE for CA NRA	HIGH RISK for CA/NRA	HIGH RISK for CA/NRA	HIGH RISK for CA/NRA	CRITICAL RISK for CA/NRA	MEDIUM RISK for CA/NRA	MEDIUM RISK for CA/NRA
LOW RISK in cascading effect to other energy stakeholder		MEDIUM RISK in cascading effect to other energy stakeholder	LOW RISK in cascading effect to other energy stakeholder	HIGH RISK in cascading effect to other energy stakeholder	HIGH RISK in cascading effect to other energy stakeholder	MEDIUM RISK in cascading effect to other energy stakeholder	LOW RISK in cascading effect to other energy stakeholder
HIGH RISK for TSO	MEDIUM RISK for TSO	HIGH RISK for TSO	LOW RISK for TSO	HIGH RISK for TSO	HIGH RISK for TSO	HIGH RISK for TSO	HIGH RISK for TSO
MEDIUM RISK in cascading effect to other energy stakeholder	LOW RISK in cascading effect to other energy stakeholder	HIGH RISK in cascading effect to other energy stakeholder	LOW RISK in cascading effect to other energy stakeholder	HIGH RISK in cascading effect to other energy stakeholder	HIGH RISK in cascading effect to other energy stakeholder	HIGH RISK in cascading effect to other energy stakeholder	HIGH RISK in cascading effect to other energy stakeholder
MEDIUM RISK for DSO	MEDIUM RISK for DSO	HIGH RISK for DSO	LOW RISK for DSO	MEDIUM RISK for DSO	HIGH RISK for DSO	HIGH RISK for DSO	HIGH RISK for DSO
MEDIUM RISK in cascading effect to other energy stakeholder	LOW RISK in cascading effect to other energy stakeholder	MEDIUM RISK in cascading effect to other energy stakeholder	LOW RISK in cascading effect to other energy stakeholder	LOW RISK in cascading effect to other energy stakeholder	MEDIUM RISK in cascading effect to other energy stakeholder	HIGH RISK in cascading effect to other energy stakeholder	MEDIUM RISK in cascading effect to other energy stakeholder
LOW RISK for Generation	LOW RISK for Generation	MEDIUM RISK for Generation	LOW RISK for Generation	MEDIUM RISK for Generation	MEDIUM RISK for Generation	HIGH RISK for Generation	MEDIUM RISK for Generation
MEDIUM RISK in cascading effect to other energy stakeholder	LOW RISK in cascading effect to other energy stakeholder	LOW RISK in cascading effect to other energy stakeholder	MEDIUM RISK in cascading effect to other energy stakeholder	LOW RISK in cascading effect to other energy stakeholder	MEDIUM RISK in cascading effect to other energy stakeholder	MEDIUM RISK in cascading effect to other energy stakeholder	MEDIUM RISK in cascading effect to other energy stakeholder
LOW RISK for Exchange	LOW RISK for Exchange	LOW RISK for Exchange	LOW RISK for Exchange	LOW RISK for Exchange	LOW RISK for Exchange	MEDIUM RISK for Exchange	LOW RISK for Exchange
LOW RISK in cascading effect to other energy stakeholder	LOW RISK in cascading effect to other energy stakeholder	LOW RISK in cascading effect to other energy stakeholder	LOW RISK in cascading effect to other energy stakeholder	LOW RISK in cascading effect to other energy stakeholder	LOW RISK in cascading effect to other energy stakeholder	LOW RISK in cascading effect to other energy stakeholder	LOW RISK in cascading effect to other energy stakeholder

Overview of cyber threats and risks for EnC members

- Examples 1:

Stakeholder: Country cybersecurity authority (CA) and/or National Regulatory Agency (NRA)

CA/NRA

Scenario 2 – False communication

Due to a spoofed false email to the CA it declared state of emergency which force the energy sector companies to work in critical conditions. A 24 hours a day shift was introduced at gas TSO critical supervisory operation control room unit. The reporting requirement was upgraded to once a minute. A government held a special meeting to discuss the cyberattack from which they release a special note to address the public. As the CA realises that there was a spoofed e-mail with false information, they try to stop the operation but it is too late as the information leak to public.

			Quantified Impact on Energy Sector		
Threat	***Vulnerability***	***Likelihood***	*Health/Safety*	*Economic*	*Social*
Phishing	Lack of security awareness Lack of proof of sending or receiving a message Unprotected sensitive traffic Lack of e-mail usage policy	***Probably***	***1***	***2***	***2***

Overview of cyber threats and risks for EnC members

- Examples 2:

Stakeholder: Country Transmission System Operators (TSO) Gas

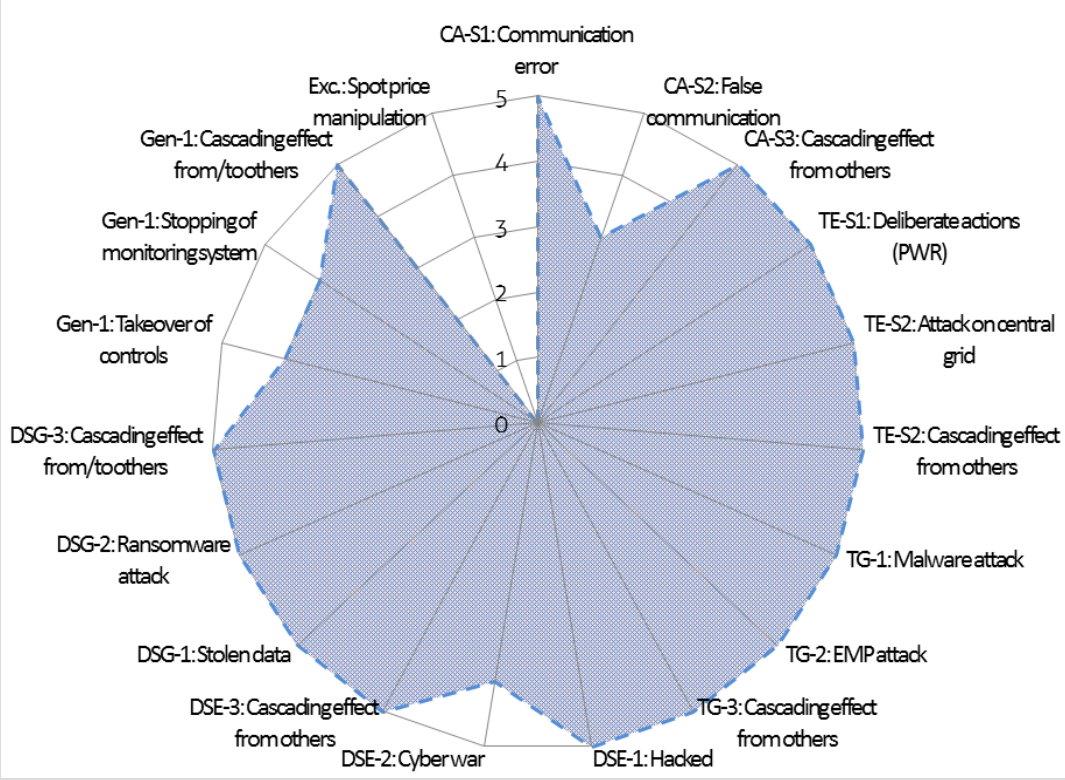
Scenario 2 – EMP attack

During an EMP[1] (electromagnetic pulse) attack or CMI (coronal mass injection of the sun) the TSO SCADA system is severely damaged. The replacement parts of the system can be delivered only 30 days after the incident. For 15 days the gas transmission is halted, after that period the TSO transfers to manual handling. Finally, the replacement parts arrived after a month and TSO tries to replace them but fails during lack of proper documentation. The vendor is urgently informed and provides the information and restores the SCADA after 60 days.

			Quantified Impact on Energy Sector		
Threat	***Vulnerability***	***Likelihood***	*Health/Safety*	*Economic*	*Social*
DoS attack	Sensitivity to electromagnetic radiation Lack of periodic replacement schemes Lack of documentation Lack of back-up copies Single point of failure Lack of procedures of risk identification and assessment	Possibly	2	3	5

Overview of cyber threats and risks for EnC members

- The risks were assessed based on the prioritisation of likelihood and impact quantified of scenarios
- If we broke down the risks with the type of cyber threat vectors to impact different stakeholders we can get a more precise picture of inherent risks



The Next Steps of Cybersecurity study

- Activities and organisational structures proposed to align the existing Contracting Parties energy cybersecurity framework with the EU legislation with proposed measures
- Recommendations per each CP
- Impact assessment of implementation of proposed measures and acts in the Energy Community Contracting Parties and in the Energy Community
- Proposed roadmap and timing for the implementation

Key Takeaways

- **MANGE** - Cybersecurity is not only technology related matter
- **COOPERATE** - Information sharing and trust are key elements in cybersecurity
- **LEARN AND IMPROVE** - Follow activities of EC, ENISA, Entso-G, international organisations,....
- **BE ACTIVE** - Join the initiatives of Energy Community Secretariat on the Cybersecurity in late in 2019
    - ECS "CyberCG" meeting
    - Last workshop as part of Cybersecurity study
    - Publication of Study on Cybersecurity in the energy sector of the Energy Community

Questions?

BLUEPRINT energy SOLUTIONS

Contacts & further information:

ALES HVALA
Managing Partner

Blueprint Energy Solutions GmbH
Am Gestade 3/1E, 1010 Wien, Austria
M: +386 41 663 823
E: ales.hvala@blueprintenergy.at
W: www.blueprintenergy.at

www.blueprintenergy.at