GO-201-2020

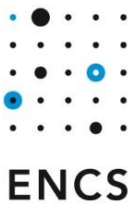
ENCS security program plans for 2020

Version 1.0 (Public)

27 February 2020

This document is shared under the Traffic Light Protocol classification:

TLP White – public



The European Network for Cyber Security (ENCS) is a non-profit member organization that brings together critical infrastructure stake owners and security experts to deploy secure European critical energy grids and infrastructure

Version History

Date	Version	Description
20 January 2020	0.1	First draft for internal review
22 January 2020	0.2	Draft version shared with ENCS members for assembly
12 February 2020	1.0	Final version after assembly approval
27 February 2020	1.0 Public	Public version

ENCS

Table of Contents

1 Introduction

This document describes the plan for the ENCS security programs for 2020. ENCS is running three long term programs on policy, architecture and operations. The programs gather, develop and share knowledge on common security problems that ENCS members face. They aim to address the needs of different groups of security experts working at grid operators, as shown in Table 1.

Table 1 Knowledge being developed by ENCS for different groups of security experts.

Security officers	Security architects	SOC analysts
Policy program	*Architecture program*	*Operations program*
Knowledge on how to improve ISMS: • Security management best practices • Insight in risks • Upcoming regulation	Knowledge on how to build and procure secure systems: • Risk assessments • Security architectures • Market and technology surveys • Procurement requirements • Test methods	Knowledge on how to monitor grid control systems: • Monitoring technologies • Use cases • Threats and vulnerabilities • Organizing security operations

The yearly program for the security programs is approved by the ENCS general assembly at the start of each calendar year. During the year, ENCS gathers the common challenges the members are facing in round table events, workshops, and project for member. ENCS investigates if member experts have an interest in developing common solutions in the security program. Based on these discussions, a draft program for the next year is presented to the ENCS strategy assembly before summer. The final program is then fixed during the fall and sent for approval to the assembly.

The security programs are funded from ENCS membership fees and project funding from members.

2 Policy program

The policy program aims to develop and share knowledge to security officers responsible for organizational security measures. It covers security policies, regulation, and the development of information security management systems (ISMSs).

The focus in 2020 will be on European regulation. ENCS anticipates that grid operators will be affected more and more by European laws and directives on security, such as the NIS directive, the Cybersecurity Act and the network code on cybersecurity. By being actively involved in EU groups, ENCS aims to inform its members on these developments and, where possible, influence regulation so that it addresses topics important to grid operators in the right way.

ENCS will also continue information sharing on the implementation of ISMSs and ISO/IEC 27001 certification.

2.1 EU groups

ENCS will continue the support of expert groups at EU level through the following activities:

- *Support writing network code on cyber-security:* ENTSO-E and the four DSO associations are tasked with writing a draft network code on cyber-security in 2020. ENCS plans to support the writing through its expertise.
- *E.DSO TF4 on cyber-security:* ENCS will continue supporting the E.DSO task force 4 on cyber-security by providing information at meeting and by providing requirements sets to the group.

2.2 ISMS expert group

ENCS will continue the expert group on Information Security Management Systems (ISMSs), supporting information sharing between members setting up an ISMS. The focus will be on the implementation of the ISO/IEC 27000 standard on which many members are working.

2.3 Planned workshops

The security roundtables will be used as the main gathering for security officers. Two roundtables will be organized in 2020.

Event	Date
13th security roundtable	12 May 2020
14th security roundtable	October 2020

3 Architecture program

The architecture program aims to develop and share knowledge to security architects and others responsible for technical security measures. It covers the design of secure systems and setting security requirements for procuring secure components.

In 2020, ENCS will expand its library of security requirements. New requirement sets will be developed to cover distributed energy resources and central systems. The approach developed for testing and certification will be improved and validated in projects. The existing requirements sets for field components will be updated where needed.

3.1 Distributed energy resources (DER)

On request of several members, ENCS has started a member project on the security of distributed energy resources (DER), such as solar and wind farms. The goal of the member project is to determine what measures DER operators and grid operators should take to sufficiently mitigate security risks to the electricity grid.

Activities planned in 2020 are:

- *Assess the security risks of the increasing use of DER:* the risks of cyber-attacks on DER operators will be analyzed. Both the impact to the DER operator itself and to the electricity grid will be considered.
- *Determine organizational and technical measures needed to mitigate these risks:* based on the risk assessment, security measures will be selected. These will include both organizational and technical measures for DER operators, and measures for grid operators to secure their connections to DER infrastructure.
- *Develop requirements DER operators can use to procure secure equipment:* to support DER operators in implementing the security measures, requirements will be developed that they can use to procure secure equipment.
- *Write a position paper on DER security for policy makers:* the conclusions on the security risks and possible mitigations will be summarized in a position paper that can be shared with national and EU policy makers.

3.2 Central system security

ENCS has built a comprehensive library of security requirements for field devices, such as smart meters, RTUs, and IEDs. In 2019 these requirements were extended to cover the central systems used to maintain these field devices. In 2020, they will be further extended to cover SCADA systems and the shared central infrastructure.

The activities planned in 2020 are:

- *Develop security requirements for SCADA / EMS / DMS systems:* the requirements are planned to be developed in cooperation with ENTSO-E to get validation from the TSO community. Draft requirements were already prepared in the ENTSO-E CEF project in 2019.
- *Develop recommendations for access control in OT environments:* different technologies for centralized access control will be compared, such as LDAP, Active Directory, RADIUS, and TACACS. Available solutions for managing remote access will be reviewed.
- *Develop recommendations for key management in OT environments:* both pre-shared keys and Public Key Infrastructures (PKIs) will be considered, with a focus on automating key management for large numbers of field devices.
- *Investigate the risk in moving OT systems to a cloud environment:* the study will cover the confidentiality and integrity of data, but also the availability of systems during power outages.

3.3 Testing and certification

In the 2019 member project on procuring secure equipment, work started to develop testing directly for equipment vendors, instead of grid operators. Doing so should allow more cost-effective testing, as the cost of testing can be shared between all users of a component. ENCS will assess if the testing approach can be used as a candidate certification scheme. In this way, ENSC intends to prepare an alternative for certification schemes being pushed by industry and regulators reacting to the EU drive for certification in the Cybersecurity Act. The work will continue in 2020 with the main goal to develop a viable certification scheme option for grid operators.

The following activities are planned:

- *Validate the developed test plan in test projects:* test plans will be implemented in the ENCS test lab and applied in upcoming test projects. The results will be evaluated and where needed the test plans will be improved.
- *Define a candidate certification scheme together with other associations:* together with other DSO associations, ENCS will work out a system or component certification scheme that is suitable for the electricity sector and meets the criteria of the Cybersecurity Act. If possible, pilots with the certification scheme are started with interested vendors.
- *Investigate current hardware security solutions on field devices:* in 2019 a member project was started on hardware security measures. In 2020, a representative sample of components is tested.

3.4 Updates of requirements for field devices

ENCS has requirements sets covering most types of field devices used by grid operators. The goal for 2020 is to ensure that these stay up to date with developments in technology and in the threat landscapes.

The following activities are planned in 2020:

- *Update the DA requirements based on tender results:* the DA requirements developed in 2019 will be updated based on experiences in tenders and the outcomes on the work on access control (Section 3.2).
- *Update the EV requirements based on testing results and stakeholder workshops:* the first charging station was tested against the requirements in 2019 and more will be tested in 2020. ElaadNL and ENCS will organize workshops with charging station manufacturers and buyers to present the requirements. Minor updates on the requirements are expected to come out of these activities.
- *Validate the smart meter requirements with ENCS members:* the documents for smart metering were completed in the 2019 member project, but it was not possible to gather enough member experts to validate the requirements. As an update set of smart meter requirements was published already in 2019 together with E.DSO, the validation was moved to 2020. In this way, the results from the member project on hardware security can also be incorporated.
- *Complete the requirements documents for IoT and sensors:* this work was planned in the 2019 member project on procuring secure equipment, but could not be completed in that year. Hence, it will be completed in the first quarter of 2020. A risk assessment and market survey will be performed, leading to a security architecture and procurement requirements.
- *Update the SA requirements in the 2019 format and publish them with E.DSO:* The substation automation (SA) requirements were developed in the 2018 member project on substation automation security. They are in a slightly different format than the requirements developed in 2019. For consistency, the SA requirements will be updated in the new format and with the experiences from tenders included. They will then be proposed to E.DSO TF4 in the program to endorse security requirements.

3.5 Planned workshops

The main events for the architecture program will be two workshops, one in the spring and one in the fall covering the activities running at that time. Workshops with external stakeholders will be organized for DER and electric vehicles.

Event	Date
1st workshop DER security (DER operators, suppliers)	5 February 2020
1st architecture workshop: testing and certification, central systems)	April 2020
EV charging workshops with Elaad	April 2020
2nd workshop DER security (grid operators)	June 2020
2nd architecture workshop (testing and certification, field devices)	November 2020

4 Operations program

The operations program aims to develop and share knowledge to security operations analysts responsible for detecting vulnerabilities and incidents. It covers vulnerability management, technologies and use cases for detecting attacks, incident response, and organization of SOC or CSIRT teams.

The main goal for 2020 is to create an active community of security operations analysts at ENCS members that can share operational information about vulnerabilities, threats, and recommendations on how to address them. ENCS will start this group based on the model used for the Netbeheer Nederland Cyber-SOC group. A roundtable will be set up for this community.

ENCS will also update the results of the 2017 member project on security monitoring. The evaluation of OT security sensors will be revisited to also cover sensors placed at substations. Detection use cases will be compared between different SOCs and best practices will be developed for vulnerability scanning in OT networks.

4.1 Incident response

Being able to respond to security incidents is a key capability for all grid operators. In 2020, ENCS would like to facilitate information sharing on this topic through the following activities:

- *Develop best practices in forensics:* best practices on investigating security incidents will be gathered from members and written down in a whitepaper.
- *Investigation into malware in substations:* Netbeheer Nederland is starting a project to search for possible malware on Windows machines in substations. ENCS will support the project and share the methods used in a whitepaper.
- *Develop response exercises:* ENCS will start the development of an incident response exercise for its members in the second half of 2020. Initially the goal is to develop a tabletop exercise. This exercise may then be made more hands-on by using the Red Team – Blue Team environment in 2021.

4.2 Update on OT security sensors

In 2017, ENCS did a market survey on specialized OT security sensors that can be used to detect incidents and vulnerabilities in grid operator control systems. These systems have been further developed since then and ENCS plans to update the documents on this topic, through the following activities:

- *Member project on substation monitoring:* while the 2017 project focused on monitoring centrally, it is becoming feasible to place sensors into each high-

voltage substation. A member project was started to investigate the capabilities such sensors placed in a substation can provide, also in comparison with the centralized model.

- *OT security sensor requirements:* based on the outcomes of the substation monitoring member project and tenders at members, the security requirements for central OT security sensors will be updated.

4.3 Update on organizing OT security monitoring

The 2017 member project on security monitoring provided recommendations on organizing an OT security monitoring team. These recommendations were mostly based on literature review and experiences at IT security operations centers. Since then, many members have set up a security operations team dedicated to OT systems. So, in 2020 the recommendations will be updated to reflect their experiences.

The following activities are planned:

- *Use case comparison:* the use cases implemented at different members will be compared and analyzed for their effectiveness, so that members can learn from each other's experiences.
- *Best practices on vulnerability scanning:* best practices will be developed on vulnerability scanning on OT systems, covering which systems can be scanned, what system knowledge, assessment tools and settings should be used, and how the results should be handled.
- *Roundtable for SOC analysts:* a new roundtable will be set up aimed at analysts working in security operations centers and with a focus on OT systems to improve information sharing among this group.

4.4 Planned workshops

The main events for the security operations program are the SOC roundtables. A separate workshop is planned for the member project on substation monitoring.

Event	Date
Workshop on security monitoring in the substations	April 2020
1st SOC roundtable	11 May 2020
2nd SOC roundtable	October 2020
Pilot incident response exercise	October 2020