Mike Mekkanen, Tero Vartiainen, Kimmo Kauhaniemi

Cybersecurity and Resilience of Digital Energy Systems (CR-DES) development workshop 8th December 2020

Cyber security environment at FREESI lab

Vaasa 2020

Programme for Sustainable Growth and Jobs
Leverage from the EU 2014–2020
European Union
European Regional Development Fund
European Social Fund

Contents

Executive Summary 3

1 First CR-DES project Workshop to develop Cyber Physical Security at FREESI research laboratory environment 4

1.1 Collaborative partners 5

1.2 Preparatory Questioner 5

1.3 Workshop and Questioner contributors 5

1.3.1 Vaasa Ecosystem 5

1.3.2 DSO and energy companies from the southern and central parts of Finland 5

1.3.3 International partners 6

1.4 The summary of the Questioner results 6

1.4.1 Organizations CPS posture/experience 7

1.4.2 Cyber Security standards/state-of-the-art and Information security managements 7

1.5 The summary of the workshop groups work 8

1.6 Cyber Physical Security for Digital Energy System 12

1.7 Digital Energy System Communication Protocols and Testing 14

2 Appendix A 17

References 34

Executive Summary

The energy sector digital transition is a great enabler that enhanced opportunity in achieving sustainability, efficiency but also will increase systems' complexities and on the top the exposure of the cyber threats. Due to this digital transition and the exposure of the cyber threats, adequate knowledge and update/upgrade skills will increasingly needed now and in the future to adapt and outperform this new era. To this end, the understanding/analyzing this digital smart energy system and the identification of the needed knowledge based CPS, define useful cases to study is the first step that will increase system awareness, facilitate and reduce the impact of the cyber threats, foster the necessary actions and lastly lead to achieve system resiliency.

To be able to understand/analyze the digital smart energy system and the identification of the needed knowledge, useful case studies, the CR-DES project develop a workshop based on a questionnaire. The questionnaire was developed in a way that assist with the process of developing cyber physical security (CPS) laboratory, as well as will help to determine the CPS posture based structures and practices for the Organization may have/need in place to identify cyber threats, increase CPS awareness and in future educating others. The questionnaire was widely distributed (sent to 170 persons/Organizations) however, the highest percent (31.25%) from the Questionnaire contributors are expert in Cyber Security, in which that would increase the dependability of the contributors answers. The whole survey is accessible on Appendix A. The most key findings among others are mentioned below:

- There are areas of development/improvement that need to be addresses, even the organizations have an advanced awareness of security and employ the highest security standards and practices.
- The CPS skills gap/need is currently more raised and the Organizations are very likely are going for providing a training to their organization employees on CPS in future.
- We recommend that it is the time indeed for the Organizations to really start looking/implementing these CPS standards/guidelines and testing them, in a way that we can see where the system vulnerabilities might lay/practically in order to increase the CPS awareness and measure/improve the energy system resiliency.

Leverage from the EU 2014–2020

European Union
European Regional Development Fund
European Social Fund

1 First CR-DES project Workshop to develop Cyber Physical Security at FREESI research laboratory environment

Cyber security environment at FREESI laboratory is one from the University of Vaasa's development strategy in which that aims to serve academia and different type of companies in the field of Cyber Physical Security CPS. As modern energy system is becoming more 'intelligent' and increasing in complexity that composed of electrical power system and information communications technology (ICT) infrastructure i.e. The energy grid is becoming more vulnerable to cybersecurity threats by expanding the attack surface. At the beginning of 2017 within the SESP – Smart Energy Systems Research Platform – project University of Vaasa's "Future Reliable Electricity and Energy Systems Integration" FREESI research laboratory development had started. The main target of FREESI lab is to develop and built a real-time simulation and testing platform as a main core of the lab. University of Vaasa will continue the development of their laboratories in a way that should be internationally recognized, be trusted, and agile as illustrated in Figure 1.

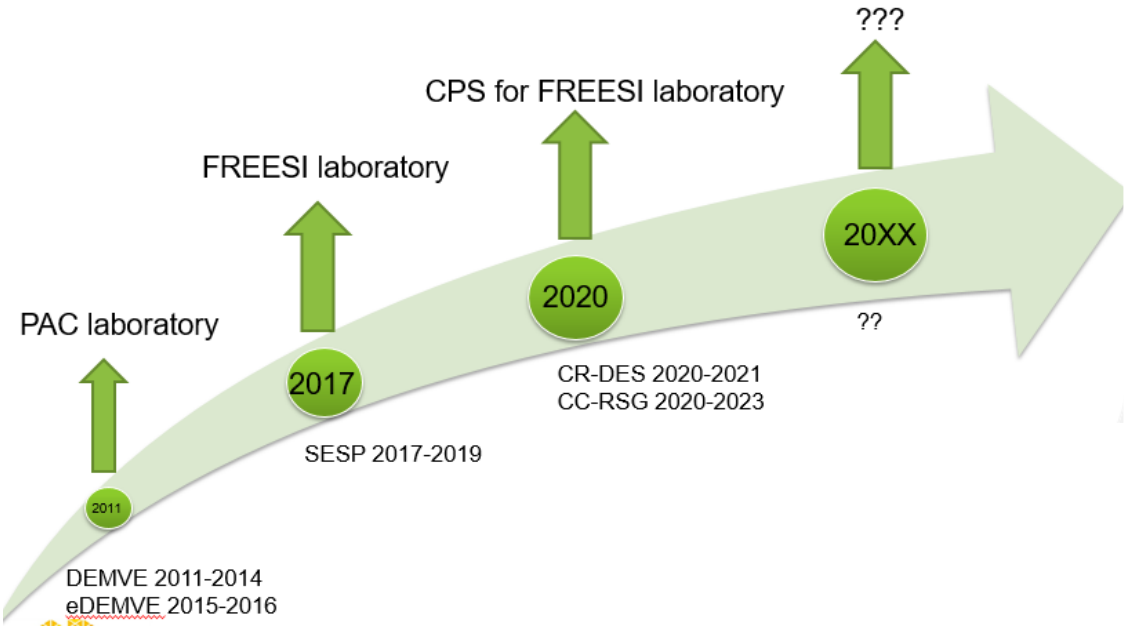


Fig 1. University of Vaasa development labs

1.1 Collaborative partners

Collaborative partners were invited to the first CR-DES project Workshop based on the development of the CPS for FREESI lab environment. The aims of the CPS Workshop is to collect ideas, potential needs and requirements for developing cyber physical security teaching and research laboratory in Meta level. Moreover, it meant as a room for discussions among the project partners/industry in which that will be the key for developing the CPS for FREESI lab platform that encompasses both the CPS knowledge/education and the state-of-the-art technologies for the current and future trends needs.

1.2 Preparatory Questioner

A preparatory questionnaire was conducted before the workshop, doing so is to assist with the process of developing the CPS at FREESI lab environment, as well as will help to determine the CPS posture based structures and practices you may have/need in place to identify cyber threats. The questionnaire will ask firstly few background questions. After this it will ask about the participant's organization CPS posture and their experiences. The questionnaire results would presented at the beginning of the workshop.

1.3 Workshop and Questioner contributors

The invitation to the workshop and the questioner was sent to the contributors,

1.3.1 Vaasa Ecosystem

ABB, Alfen Elkamo, Ampner, Arcteq, Business Finland, Comsel, Danfoss, Devatus, Elisa, Eltel, Emtele, Etelä-Pohjanmaan Alueverkko Oy, Finnkumu, Geyser, Jubic, KKM Power, Kontram, Maviko, Merinova, Netcontrol, P2 Engineering, Pohjanmaan liitto, Satel Schneider Electric, Siemens, ST-pooli, There Corporation, The Switch, TJK Tietolaite, UTU, Vaasan kaupunki, Vaasan Sähkö, Vaasan Sähköverkko, VAMK, Vaspec, VEO, WE Tech,Wapice, Wärtsilä.

1.3.2 DSO and energy companies from the southern and central parts of Finland

Alajärven Sähkö Oy, Caruna & Caruna Espoo, Elenia, Esse Elektro-Kraft Ab, Fingrid (TSO), Fortum, Helen, Helen Sähköverkko, Herrfors Nät-Verkko Oy Ab, Jylhän Sähköosuuskunta,

Järvi-Suomen Energia Oy, Kajave Oy, Keuruun Sähkö Oy, Koillis-Satakunnan Sähkö Oy, Kokemäen Sähkö Oy, Kokkolan Energiaverkot Oy/Kokkolan Energia, Korpelan Energia Oy, Köyliön-Säkylän Sähkö Oy, Lankosken Sähkö Oy, Lehtimäen Sähkö Oy, Leppäkosken Sähkö Oy, Loiste Sähkönmyynti, Naantalin Energia Oy, Nykarleby Kraftverk Ab, Paneliankosken Voima Oy, PKS Oy, PKS Sähkönsiirto Oy, Pori Energia Sähköverkot Oy, Pori Energia, Rauman Energia Sähköverkko Oy & Lännen omavoima, Savon Voima Verkko Oy, Tampereen Sähköverkko Oy, Tampereen Sähkölaitos, Turku Energia Sähköverkot Oy, Turku Energia, Vatajankosken Sähkö Oy, Vakka-Suomen Voima Oy & Lännen omavoima, Vantaan Energia Sähköverkot Oy, Vantaan Energia, Verkko Korpela Oy, Vattenfall, Vimpelin Voima Oy, Sallila Sähkönsiirto Oy & Sallila energia.

1.3.3 International partners

Oldenburg Germany OFFIS - Institute for Information Technology, National Technical University of Athens NTUA; Greek, Technical University of Hamburg Germany TUHH.

Section 1.4 presents the summary of the survey results; Section 1.5 presents the summary of the Workshop groups work; Section 1.6 Cyber Physical Security for Digital Energy System; Section 1.7 Digital Energy System Communication Protocols and Testing/summaries are in Appendix A

1.4 The summary of the Questioner results

The questionnaire was developed by CR-DES research group and conducted using the platform Webropol. Platform like Webropol, collecting and interpreting questionnaire data becomes a simple task that can help identify actionable solutions. Our goal is to use the Questionnaire in away that assist with the process of developing cyber physical security (CPS) laboratory, as well as will help to determine the CPS posture based structures and practices for the Organization may have/need in place to identify cyber threats, increase CPS awareness and in future educating others. Even the questionnaire was widely distributed (sent to 170 persons/Organizations) however, the highest percent (31.25%)

from the Questionnaire contributors are expert in Cyber Security (from the Questionnaire's Q2 answers see Appendix A), in which that would increase the dependability of the contributors answers.

1.4.1 Organizations CPS posture/experience

Organizations CPS posture/experience was analyzed/evaluated in Questions from (3-16). From the Questionnaire contributor's answers, even the organization has an advanced awareness of security, it employs the highest security standards and practices, and that it proactively works on maintaining its overall security posture on an ongoing basis. However, only 19% of the Questionnaire contributors are selecting score 5 (5 = very good) for the general state Cybersecurity in their Organizations. This lower percentage would indicate that there are areas of development/improvement that need to be addresses, by involving the Organizations on developing cybersecurity awareness e.g. (Q7: 56.25%), this highest percentage indicates that the Organizations are very likely interesting to do so, and (Q6: 63% the sum of selecting 4 and 5, 5= very likely) this highest percentage indicates that the Organizations are very likely are going for providing a training to their organization employees on cybersecurity in future.

1.4.2 Cyber Security standards/state-of-the-art and Information security managements

Organizations Cyber Security standards/state-of-the-art and Information security managements knowledge/experience was analyzed/evaluated in Questions from (17-22). The general knowledge/experience of the existing security/communication standards that published from different groups e.g. ISO, IEC, NIST, NERC, CIP etc. which are risk-based, process-based or compliance-based, and energy system communication based are equally-likely/or more, acquired by the Questionnaire contributors as indicated from the answers of the questions e.g. (Q17: 50% and Q18: 63%) this high percentage indicates that the Questionnaire contributors are familiar with the IEC series of standards, however, the relatively newest version of the IEC Cyber Security standard based energy system communication e.g. IEC 6235X and the state-of-the-art simulating/emulating testing tools, there is a lack of knowledge/experience e.g. (Q19: 62% not familiar with

the IEC 6235X, Q22: 69% not familiar with the CPS based real-time simulator). According to these highest percentages of unfamiliarity, it would indicate that there is big gap on these topics of and there are areas of improvement that need to be addresses.

Lastly, we recommend that it is the time indeed for the Organizations to really start looking/implementing these CPS standards/guidelines and testing them, in a way that we can see where the system vulnerabilities might lay/practically do real-time measuring/evaluating in order to fall the standards/guidelines knowledge gaps, increase the CPS awareness and measure/improve the energy system resiliency, reduce security threats and costs, and especially weaken cyber attackers' strength.

1.5 The summary of the workshop groups work

In the group works of the workshop the aim was to get ideas for the practical use cases to be studied with the real time platform. The questions discussed in groups were:

- What are the potential vulnerabilities the attacker would use?
    - What could be the motivation or aim of the attacks?
    - What kind of damage or harm the attacker would like to cause?
- What kind of system configuration would be interesting to study?
    - Power grid including some distributed energy resources.
    - What kind of communication and automation system?
- What cybersecurity and resiliency measures could be tested?
- Other topics to be studied?

Considering the aim of attackers and the vulnerabilities utilized the following points were raised in the groups:

- Aim/motivation
    - Financial/economical motivation, ransomware
    - Terrorism, chaos, damage, war, destabilization, severe damage and get attention

    - APT groups, e.g. China
    - Hackers
    - Diversion strategy, surveillance
    - Data theft, phishing
    - Reducing system safety, destabilization
    - Unsatisfied employer
- Vulnerabilities/attack vectors
    - Malware, e.g. in engineering station or IED
    - Modifying sensor calibrations
    - Tampering of smart meters or automation devices
    - Harmful device in substation
    - Denial of Service
    - Known vulnerabilities (weak systems and software) unfixed bugs, buffer overflows, open system data, weak passwords, social engineering, out-dated infrastructure.

Considering the system to be studied the following ideas came up in the groups:

- Lateral attack from office LAN
- Turbine speed control
- Switching off lines or generators
- Physical access
- Man in the middle attack
- Backdoor access
- IT/OT segmentation
- 5G
- Centralized and distributed control
- Redundant systems and devices
- SCADA
- Home automation and IoT
- Different types of network platforms, e.g. VPN

- Tampered sensors
- Unidirectional data diodes
- Island mode in case of attack
- Cloud based protection
- Various power system configuration and amount of DER

As can be seen on the list above this question was seen very much linked to previous one and ways of attacks were discussed. Considering the system point of view the main part of ideas seem to focus on individual devices or automation/communication systems. On the other hand the larger systems are mentioned but then it is maybe harder to design the specific cyber event.

For cybersecurity measures to be studied the groups bring out the following ideas:

- IEC/ISO/NIST compliance
- Disaster recovery
- IDS, abnormal traffic detection
- Network segmentation
- Real malware
- Windows firewall
- Whitelisting
- Standards for CPS
- Least Privilege RBAC
- Zero trust model
- Host intrusion detection in embedded devices
- Secure reference architecture
- Anomaly detection
- Difference between failure and attack
- Reliable measurements
- Rules for IDS in OT

As can be seen the main measures seem to be well covered here. Basically the needed testing can be divided into two categories: solutions to prevent or mitigate attacks and solutions to detect the intrusions. In the first category it seems that most interest is towards the testing of the performance of the some know solutions such as firewalls. Considering the real time platform it is also interesting to develop methods to detect anomalities in the traffic and/or measurements received.

As a conclusion some initial ideas for potential use case to be further developed and eventually to be implemented in real time environment are described below.

1. **False maneuvering of a circuit breaker**

   In this case the idea is that attacker operates a circuit breaker by opening it which causes a blackout in part of the system. Normally the opening command is executed in SCADA system and the communicated to IED which then operates the circuit breaker. The cyber event may be created here by “man in the middle” approach where opening command is injected e.g. in some router along the communication path applied. Suitable techniques to detect and/or prevent could be studied.

2. **Attack towards home automation system**

   This case may be studied in several ways depending on which kind of harm the attacker wants to cause. One basic approach could be the false interaction with demand response commands or deliberate switching of customer loads, e.g. water heater. Basically very different kind of attack vectors can be employed here and possibly interesting study topic would be to compare the various means to detect the false activities.

3. **Wide area monitoring**

   Wide area monitoring is based on data collected from a large numbers of sensors around the grid. A key technique in this sense is the PMU, phasor measurement

unit. The collected data is used e.g. in state estimation and false data may cause severe problems to system operation. In this case the methods for detecting tampered sensors could be studied. This is possibly the case where most benefit is gained from the parallel simulation of power system and communication network.

The use cases presented above relatively general and can cover wide variety of of scenarios. E.g. in the case 1 the false circuit breaker operation could be generated by inducing false data to the measurement inputs of the protection IED. Furthermore, the attacker might use some advanced technique to hide the attack. By using tampered sensors the attacker could keep on submitting normal status data to SCADA system while continuing some actions in substation.

1.6 Cyber Physical Security for Digital Energy System

How can energy system getting smart but still secure?
How secure is secure enough?
The energy system digitization now/in the future will increase rapidly and must resolve three key, but often contradictory, tasks: ensuring security, raising energy efficiency and working for a clean environment. The modern digitalized energy system will be made up of many small producers, storage facilities, and numerous heterogeneous ICT components for networking, intelligent control and automation.

One challenge facing the energy system is the accelerated rollout of information and communication technology, which dynamically develop and adapt the energy system. In addition to this, external cyber threats represent a significant risk and are a key issue. However, in this application context testing for their interaction and interdependencies have never been taken into consideration until lastly.
The development of cyber physical security Lab based FREESI CPS development environment at University of Vaasa is starting by CR-DES project in which that allows large-scale, real-time co-simulation of energy supply systems and communication system emulation

under realistic conditions. These co-simulation and emulation are used to facilitate integration of new components into the system (HIL); to identify critical situations (what if scenarios); and to develop any adaptations that might be required; study the network behavior with high fidelity, accuracy, and precision.

The research need is to do focuses in ways to increase resilience in Cyber Physical Energy Systems by testing novel Operational Technology OT concepts, since OT has different concentrate and requirements from the traditional IT security as highlighted in Table I,

Table I. IT versus OT

IT Security	OT Security
Focus is on confidentiality and privacy	Focus is on availability and data integrity
Interactions with computer systems are the main drivers for security	Interactions are usually with applications, the main driver is automation functions
Timing requirements are on a "human" scale of multiple seconds, minutes and hours	Timing requirements are (generally) milli-seconds to seconds
Cybersecurity technologies must reflect "people" issues	Cybersecurity technologies must reflect automation/operation issues
Computers can be turned off or applications can be stopped/deleted when alarm raise	Automation functions can NOT be turned off when alarm raise
The main impacts of a cyber-attack are financial and reputational losses	The main impacts of a cyber-attack are physical – safety, power loss

Therefore there is strong need to focus on how the CPS based OT would affect the physical layer of the power system (real physical devices and instruments). Because of the stochastic nature of communication phenomena, we need to run experiments, which consider all these domains in real-time. For the power system simulation, digital twins model running in HYPERSIM is used which is suffices for these kind of experiments. For the communication system emulation, EXATA, is used and both the power system simulations and communication system emulation running in one target in real-time allow us to explore cases in which these devices are either under malicious attacks and/or malfunctions. Therefore energy system cyber physical security was seen very important and addressed by many standards/guiding for security assurance and improve the energy system resiliency.

The understanding of security standards and the added new constraint/requirements for the modern digitalized energy system is seen important. Moreover, development/testing the energy system CPS in laboratory, doing so the laboratory should include state-of-the-art infrastructures for energy system simulation modeling and high fidelity communication system emulation modeling running in parallel/ real time . In addition to standards, it was also seen important to discuss and identify different security breach "What if" scenarios, to study technologies/methods to measure/improve energy system resilience. Following standards and tools were especially mentioned in which that may also be classified as "What" group standard e.g. NIST, ISO/IEC 2700X etc. and "How" group standard e.g. ISO/IEC 62351 etc. In "What" group standard it explains/guides what to do, but not how do it, whereas in "How" group standard it explains how to implement the standard systematically.

- NIST Framework for Improving Critical Infrastructure Cybersecurity Version 1.0
- ISO/IEC 62443 Security Assurance levels
- ISO/IEC 27001 Information security management
- ISO/IEC 62351 Smart Grid protocol security standards

As a result the first CR-DES workshop was held at 8th December.2020. Also, a survey for the development of Cybersecurity and Resilience of Digital Energy Systems at FREESI lab was developed and distributed as mentioned above in 1.3 section.
The workshop aiming to collect ideas and possible needs for developing a successful research platform and laboratory. The workshop willing to be room for discussion among industrial partners and Vaasa University /hear about trend topics/research interests at the general level, collaboration ideas, and requirements.

1.7 Digital Energy System Communication Protocols and Testing

As the information system is just overlaid the existing energy physical system, communication technologies/protocols have become one from the very important layer at the energy system infrastructure. It was seen very important to continue supporting the development of the various communication standard/security protocols. Testing and vali-

dating of the developed communication/security standards based interoperability/compliance at different implementation phases is one of the CR-DES project important tasks. The EXata CPS solution can be used to develop, test and investigate how the communication link/network behave/respond to different threats while energy system physical simulation model is running in real-time. EXata visualization can be used to gain valuable insight into the network dynamics, including how malware spreads via vulnerabilities within the communication network. These include:

- The hop-by-hop path taken by an attack packet from an attacker to a victim.
- Key statistics which are updated dynamically, including memory and CPU utilization at devices (which are often impacted by cyber attacks).
- Cyber assurance state of a node in the network, i.e., whether the node has been compromised and the degree to which it is compromised.
- Post-simulation, statistical data collected during the simulation (for example, number of suspicious traffic packets, number of packets blocked at a firewall, number of services compromised, etc.) can be analyzed to help identify potential issues and the effectiveness of counter-measures.
- Effectiveness of mitigation strategies: The models can be used to run multiple what-if scenarios with different network configurations and attack patterns to assess the effectiveness of different counter-measures

The protocols which especially consider for the energy system communication is the IEC 61850 protocol family and its security standard IEC 6235X for substation communication and for many other purposes.

Summary

Energy systems are currently of interest not only to Cyber-security researchers but also to potential cyber attackers. Modern energy systems transition and complexity of businesses proceed faster than awareness and expertise of cybersecurity grow. Problems have been identified globally and are being addressed in many ways. But still there is a clear need for more joint research, collaboration, and benchmarking, and above all, a clear need

to increase human resources and their knowhow. we recommend that it is the time indeed for the Organizations to really start looking/implementing these CPS standards/guidelines and testing them, in a way that we can see where the system vulnerabilities might lay/practically do real-time measuring/evaluating in order to fall the standards/guidelines knowledge gaps, increase the CPS awareness and measure/improve the energy system resiliency, reduce security threats and costs, and especially weaken cyber attackers' strength.

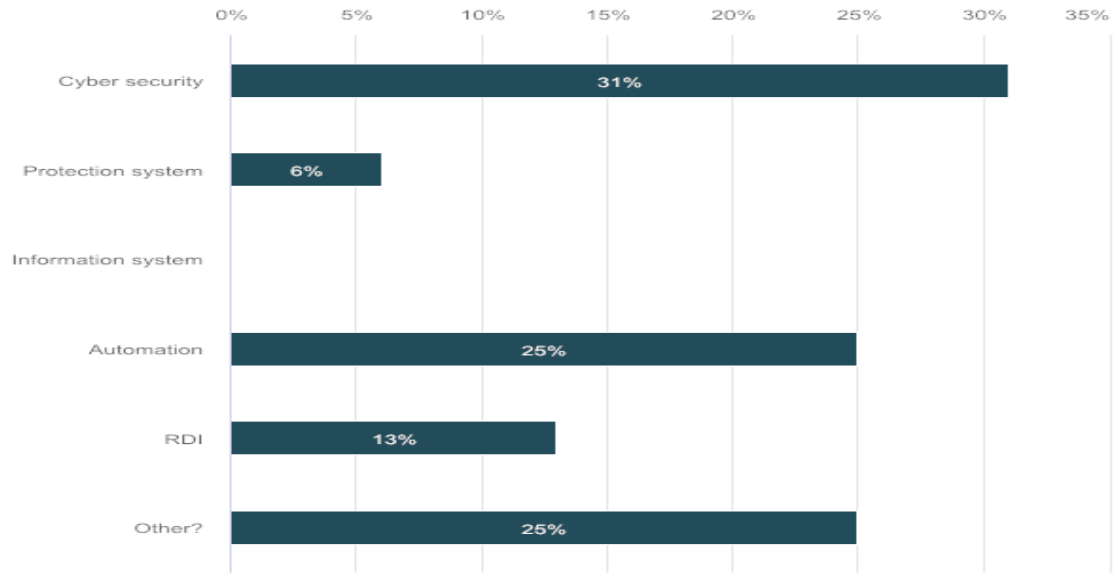
Leverage from the EU 2014–2020
European Union
European Regional Development Fund
European Social Fund

2 Appendix A

Questionnaire,

Question1. Contact Information (Optional)

Question 2. In which filed you are working in?

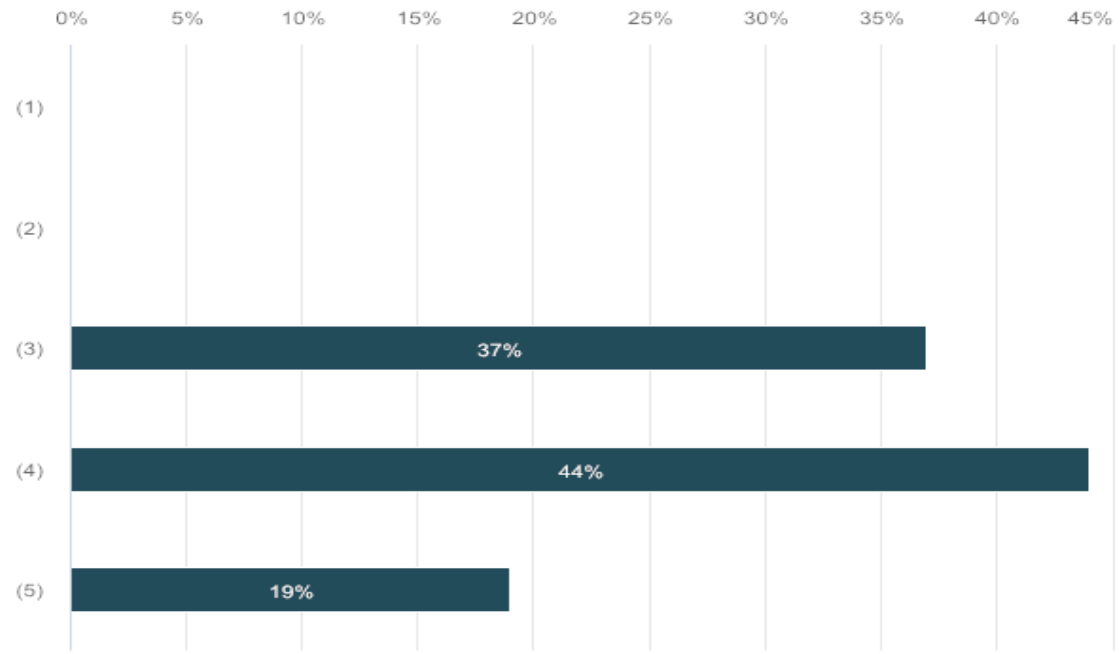


Cyber security	5	31.25%
Protection system	1	6.25%
Information system	0	0%
Automation	4	25%
RDI	2	12.5%
Other?	4	25%

Answers given into free text field

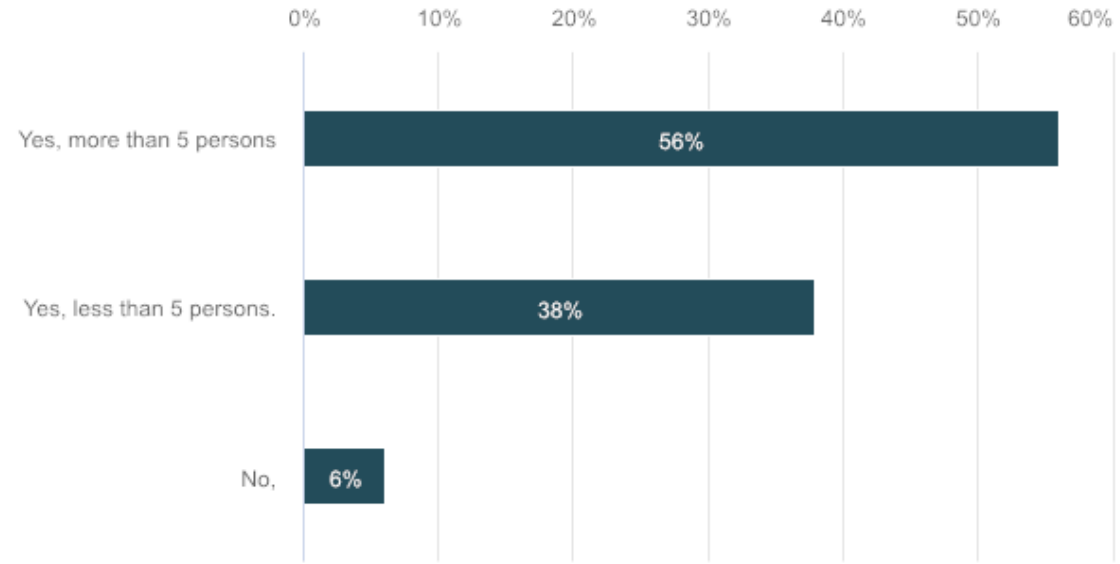
Option names	Text
Other?	Digitalization
Other?	Electrical system including information system
Other?	OT and IT
Other?	Smart Metering / Smart Grid

Question 3. What is the state of cybersecurity in general in your organization? (1= very bad, 5 = very good)



(1)	0	0%
(2)	0	0%
(3)	6	37.5%
(4)	7	43.75%
(5)	3	18.75%

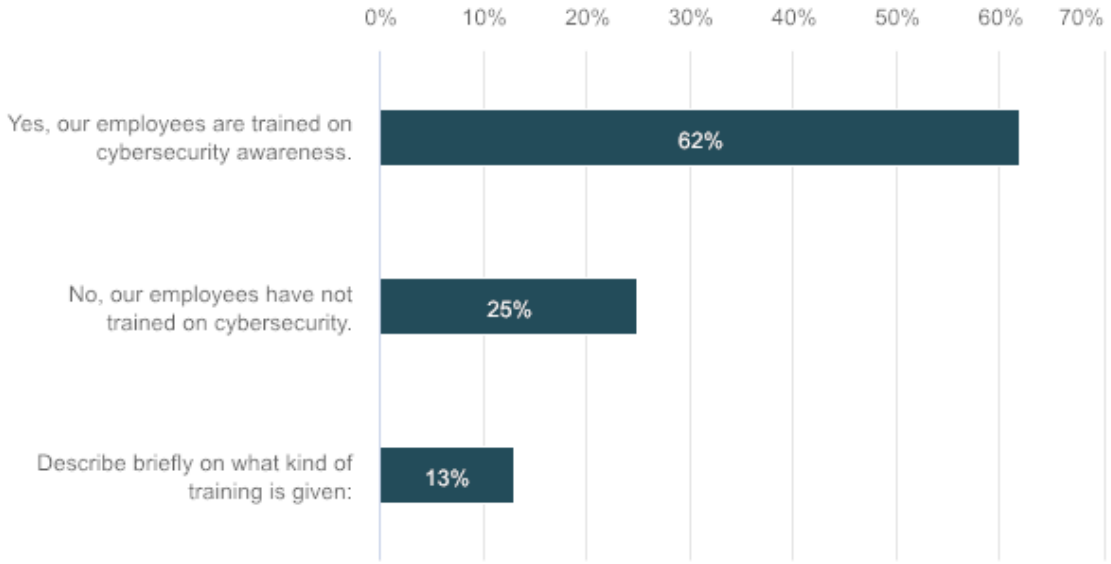
Question 4. Do you have dedicated person or team officially responsible for cybersecurity in your organization?



Yes, more than 5 persons	9	56.25%

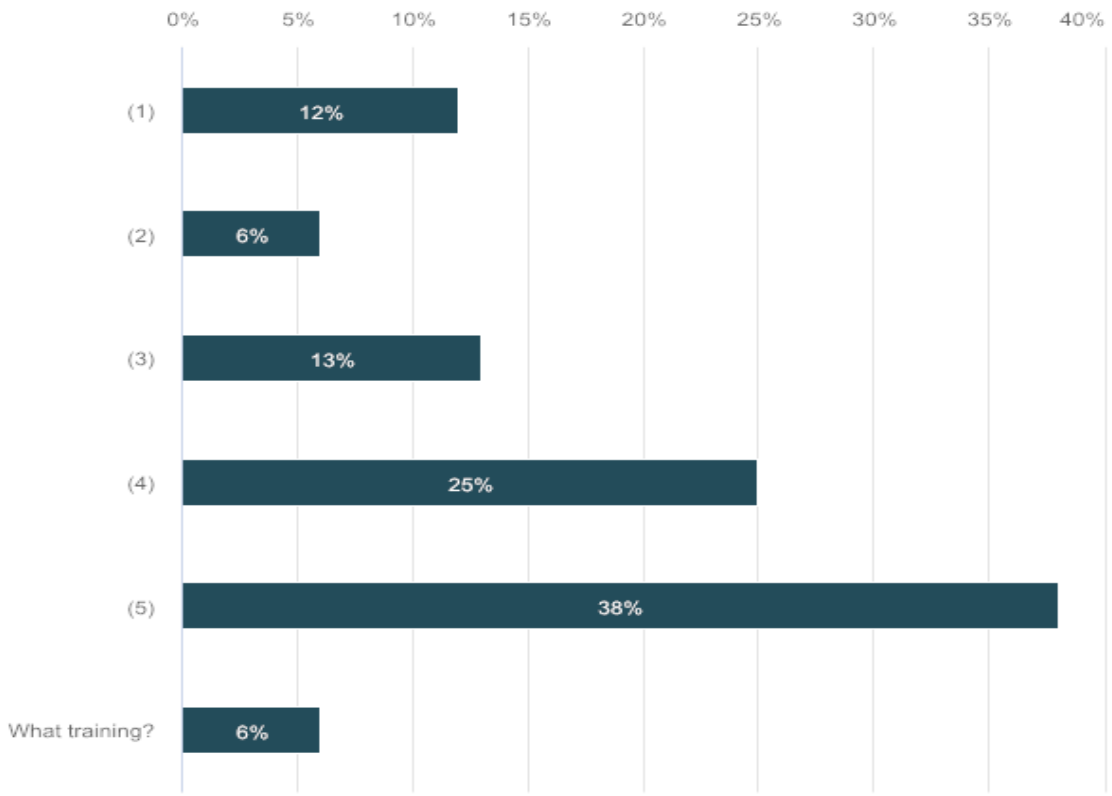
Yes, less than 5 persons.	6	37.5%
No,	1	6.25%

Question 5. Have the employees in your organization been trained for cybersecurity awareness?



Yes, our employees are trained on cybersecurity awareness.	10	62.5%
No, our employees have not trained on cybersecurity.	4	25%
Describe briefly on what kind of training is given:	2	12.5%

Question 6. How likely you are going for providing a training to your organization employees on cybersecurity in future? (1=unlikely, 5=very likely)

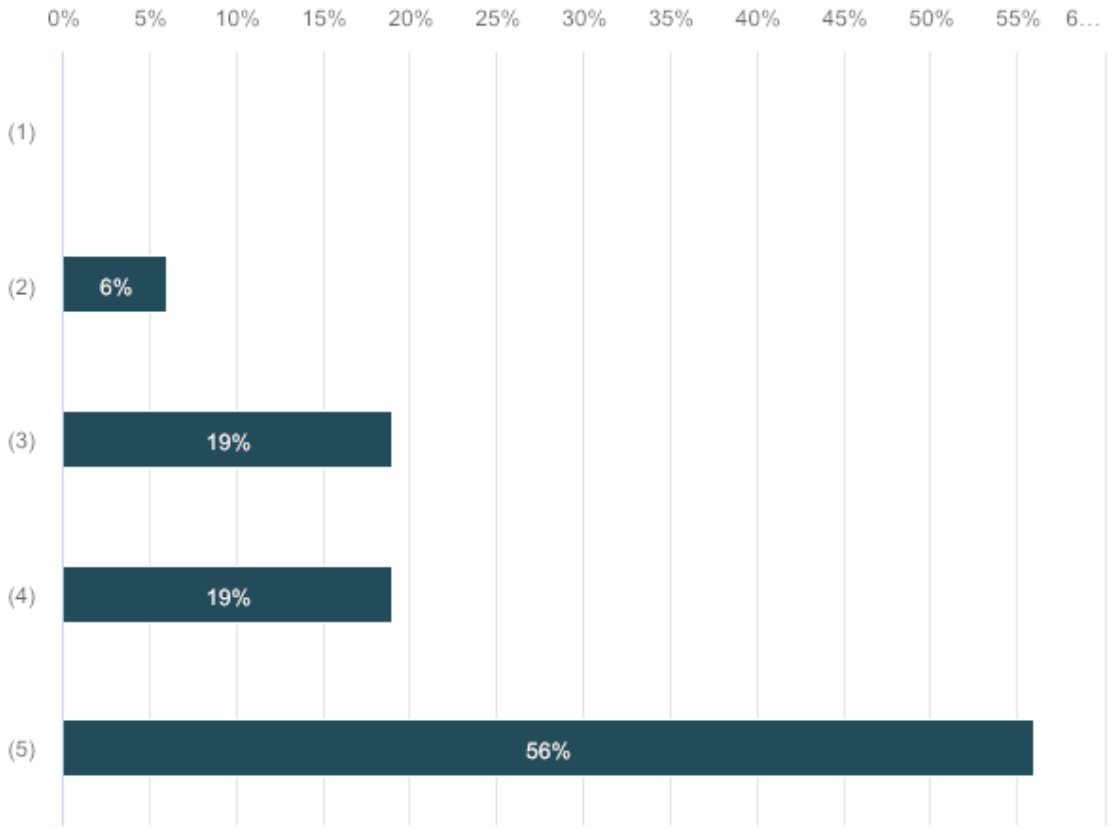


(1)	2	12.5%
(2)	1	6.25%
(3)	2	12.5%
(4)	4	25%
(5)	6	37.5%
What training?	1	6.25%

Answers given into free text field

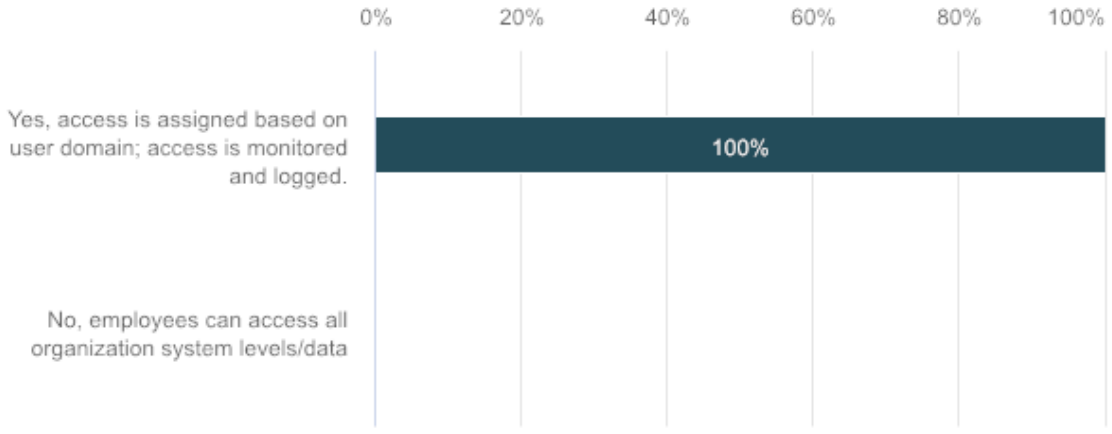
What training?	CPS training

Question 7. How interesting are you/your organization to be involved on developing cybersecurity awareness in nearest future? (1= not interested, 5= very interesting)



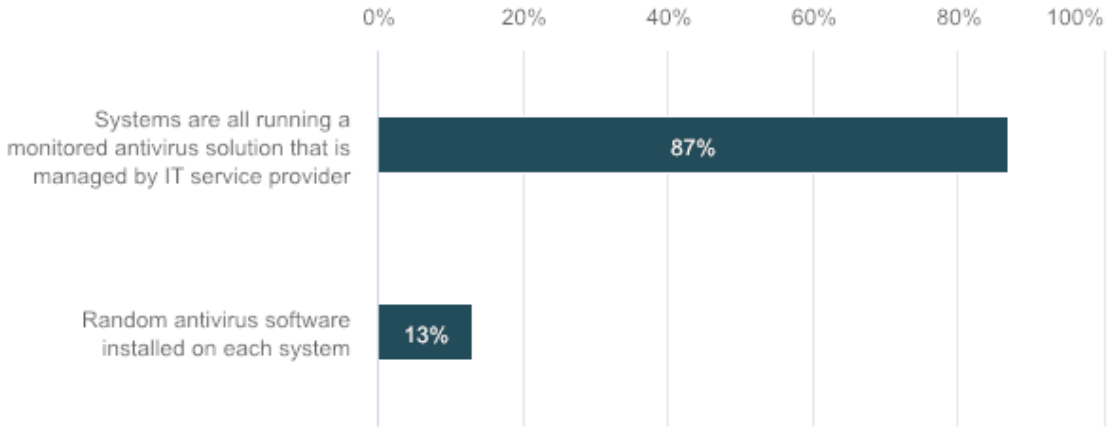
(1)	0	0%
(2)	1	6.25%
(3)	3	18.75%
(4)	3	18.75%
(5)	9	56.25%

Question 8. Have your organization separate accessing to the system/data in to different accessing levels?



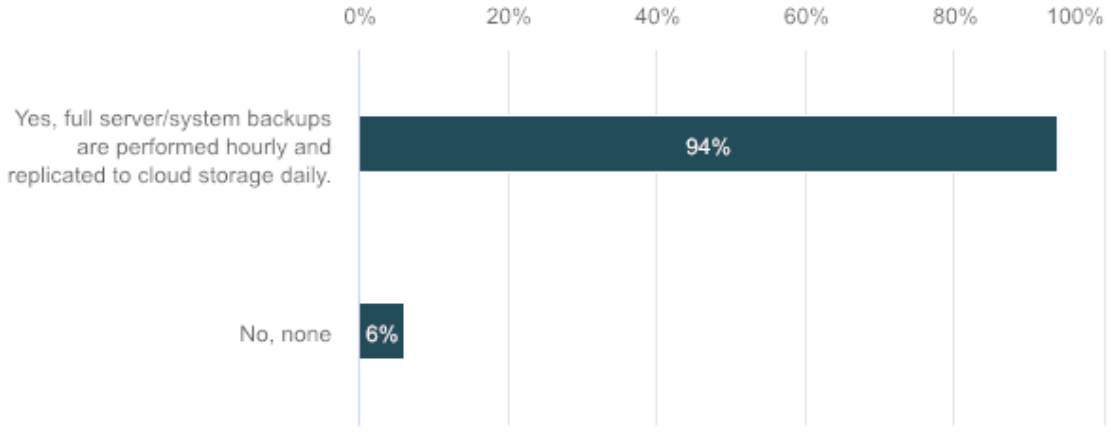
Yes, access is assigned based on user domain; access is monitored and logged.	16	100%
No, employees can access all organization system levels/data	0	0%

Question 9. What kind of computer antivirus solution does your organization use?



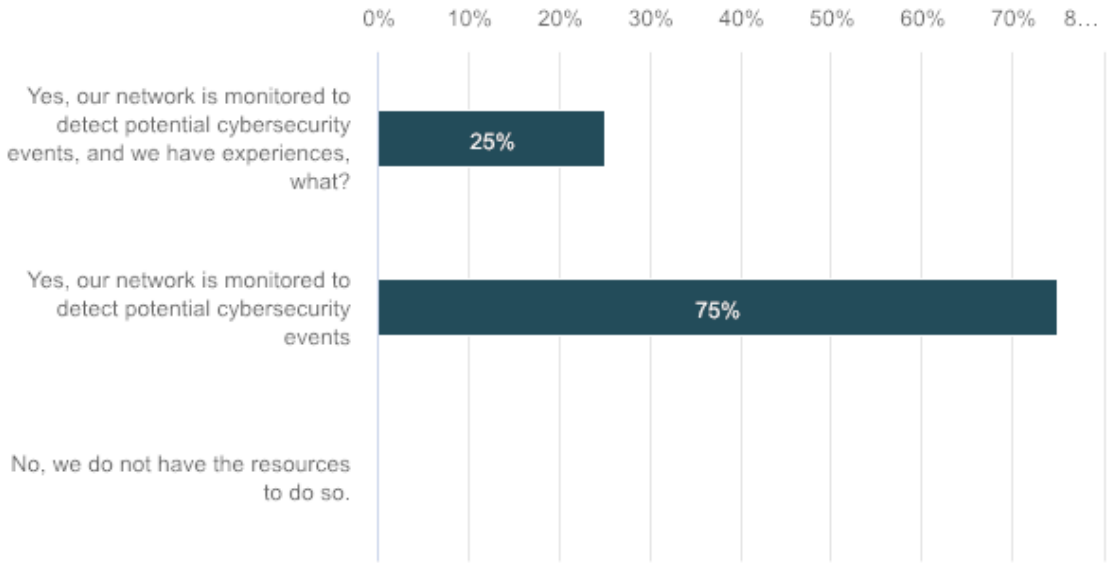
Systems are all running a monitored antivirus solution that is managed by IT service provider	14	87.5%
Random antivirus software installed on each system	2	12.5%

Question 10. Does your organization use backup solution?



Yes, full server/system backups are performed hourly and replicated to cloud storage daily.	15	93.75%
No, none	1	6.25%

Question 11. Is your Organization able to detect cybersecurity threats? Any previous experiences

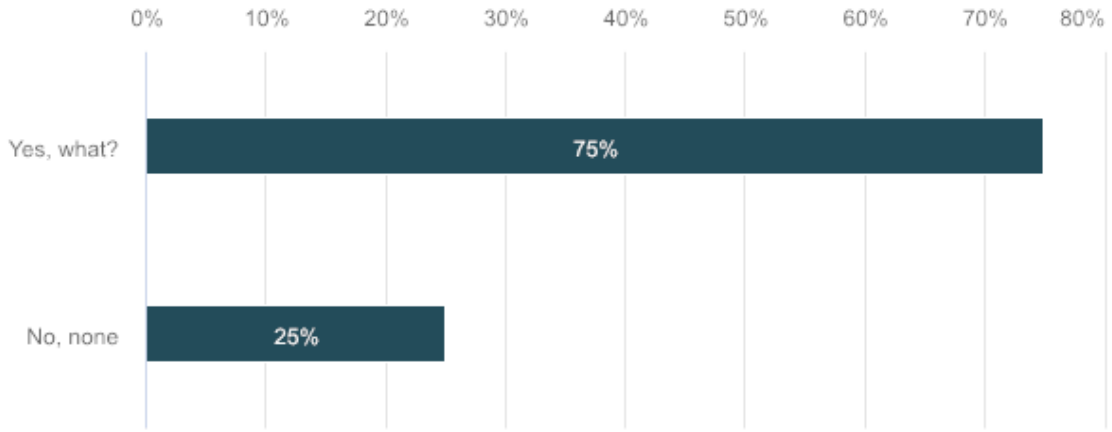


Yes, our network is monitored to detect potential cybersecurity events, and we have experiences, what?	4	25%
Yes, our network is monitored to detect potential cybersecurity events	12	75%
No, we do not have the resources to do so.	0	0%

Answers given into free text field

Option names	Text
Yes, our network is monitored to detect potential cybersecurity events, and we have experiences, what?	I guess so. Our IT-department (Hanne Kivimäki) can tell you more about this.
Yes, our network is monitored to detect potential cybersecurity events, and we have experiences, what?	That the cybersecurity events are rising a lot continuously

Question 12. Does your organization use any commercial devices/software such as station guard, intrusion detection, etc. to detect threats and mitigate the risk before it happen?

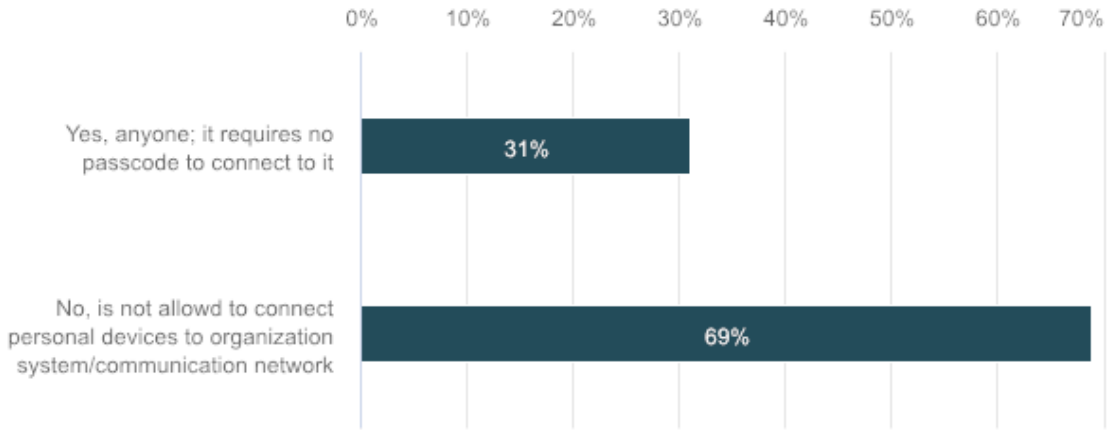


Yes, what?	12	75%
No, none	4	25%

Answers given into free text field

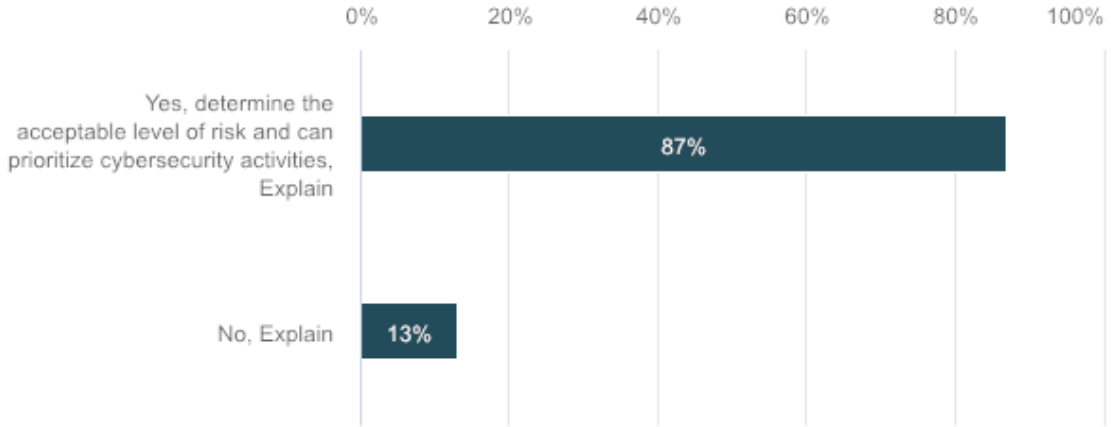
Option names	Text
Yes, what?	Not known
Yes, what?	I do not know. This is the responsibility of the IT department.
Yes, what?	NIDS, NIPS, HIDS, HIPS, SIEM, SOC
Yes, what?	Antivirus software + hosting provider's tools
Yes, what?	Such system is used for company process LAN, not for individual sub-station automation
Yes, what?	This is not public information we share :) ...
Yes, what?	Palo Alto traps

Question 13. Does your organization allow employees to connect personal devices, laptops, tablets, flash derives etc. to the organization system/communication network?



Yes, anyone; it requires no passcode to connect to it	5	31.25%
No, is not allowd to connect personal devices to organization system/communication network	11	68.75%

Question 14. Is your organizational risk tolerance determined and clearly expressed?



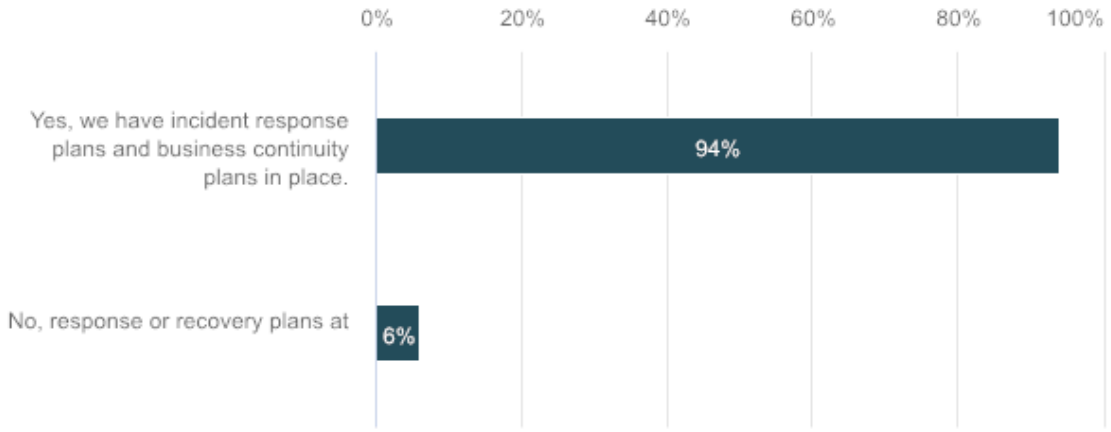
Yes, determine the acceptable level of risk and can prioritize cybersecurity activities, Explain	14	87.5%
No, Explain	2	12.5%

Answers given into free text field

Option names	Text
Yes, determine the acceptable level of risk and can prioritize cybersecurity activities, Explain	We have determined the acceptable level of risk and can prioritize cybersecurity activities.
Yes, determine the acceptable level of risk and can prioritize cybersecurity activities, Explain	Not known

Yes, determine the acceptable level of risk and can prioritize cybersecurity activities, Explain	In my opinion, it is. Our IT-department (Hanne Kivimäki) can tell you more about this.
Yes, determine the acceptable level of risk and can prioritize cybersecurity activities, Explain	Risk analysis has been made
Yes, determine the acceptable level of risk and can prioritize cybersecurity activities, Explain	Cannot explain, partially mother company IT is responsible for that.
Yes, determine the acceptable level of risk and can prioritize cybersecurity activities, Explain	According to ISO 27001
Yes, determine the acceptable level of risk and can prioritize cybersecurity activities, Explain	Teaching activities in laboratory requires some openness
No, Explain	no experience

Question 15. Does your organization has response and recovery plans in place and managed?

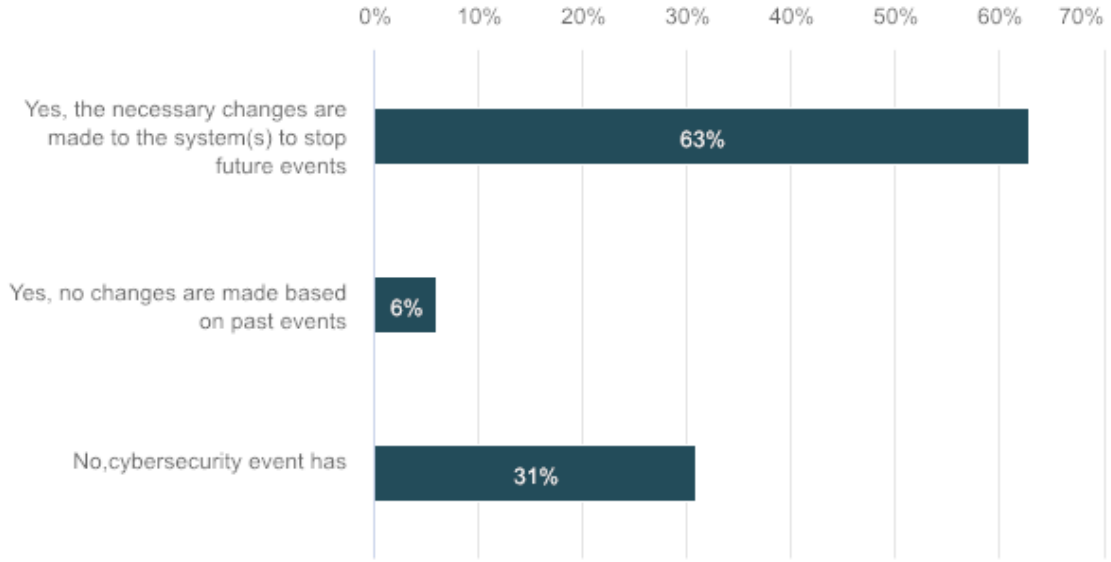


Yes, we have incident response plans and business continuity plans in place.	15	93.75%
No, response or recovery plans at all	1	6.25%

Answers given into free text field

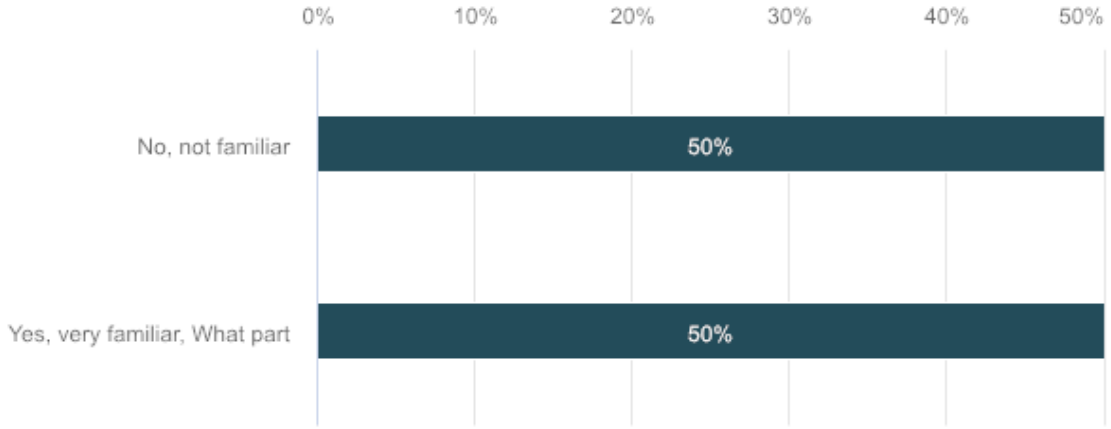
Option names	Text
Yes, we have incident response plans and business continuity plans in place.	Backups and recovery plans
Yes, we have incident response plans and business continuity plans in place.	Cannot explain, partially mother company IT is responsible for that.

Question 16. If a cybersecurity event has occurred in the past, have your organization made changes to your system(s) to ensure that this same event will not occur again?



Yes, the necessary changes are made to the system(s) to stop future events	10	62.5%
Yes, no changes are made based on past events	1	6.25%
No,cybersecurity event has occurred	5	31.25%

Question 17. How familiar are you with ISO/IEC 2700X series for information security management



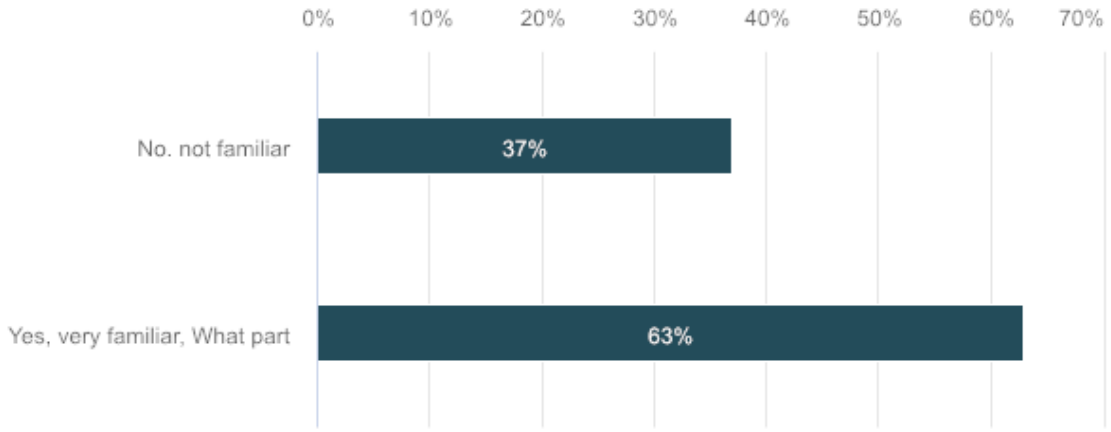
No, not familiar	8	50%
Yes, very familiar, What part	8	50%

Answers given into free text field

Leverage from the EU 2014–2020
European Union
European Regional Development Fund
European Social Fund

Option names	Text
Yes, very familiar, What part	27001
Yes, very familiar, What part	27001
Yes, very familiar, What part	Our IS management system is based on it. We are IEC62443-2-4 certified
Yes, very familiar, What part	We have a ISO/IEC 27001 certificate
Yes, very familiar, What part	1 and 2

Question 18. How familiar are you with IEC 61850 communication protocols?



No. not familiar	6	37.5%
Yes, very familiar, What part	10	62.5%

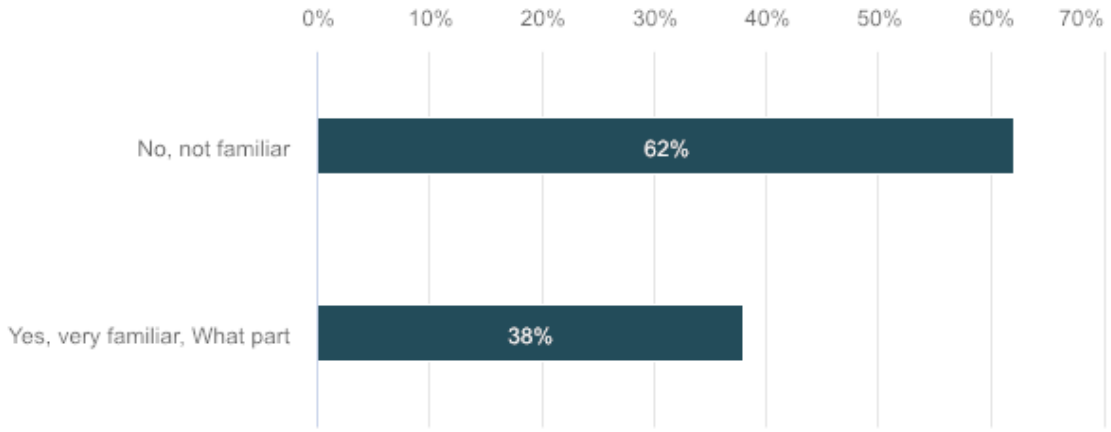
Answers given into free text field

Option names	Text
Yes, very familiar, What part	GOOSE SV MMS
Yes, very familiar, What part	Overview
Yes, very familiar, What part	Substation systems
Yes, very familiar, What part	Parts related to MMS, GOOSE and SV communication.

Leverage from the EU 2014–2020
European Union
European Regional Development Fund
European Social Fund

Yes, very familiar, What part	Not very familiar but with 13 years experience on IEC61850 station bus projects and installations we can at least specify and use those systems
Yes, very familiar, What part	all parts
Yes, very familiar, What part	substation automation
Yes, very familiar, What part	Aware of communication principles - not very familiar

Question 19. How familiar are you with IEC 62351 cybersecurity standard?

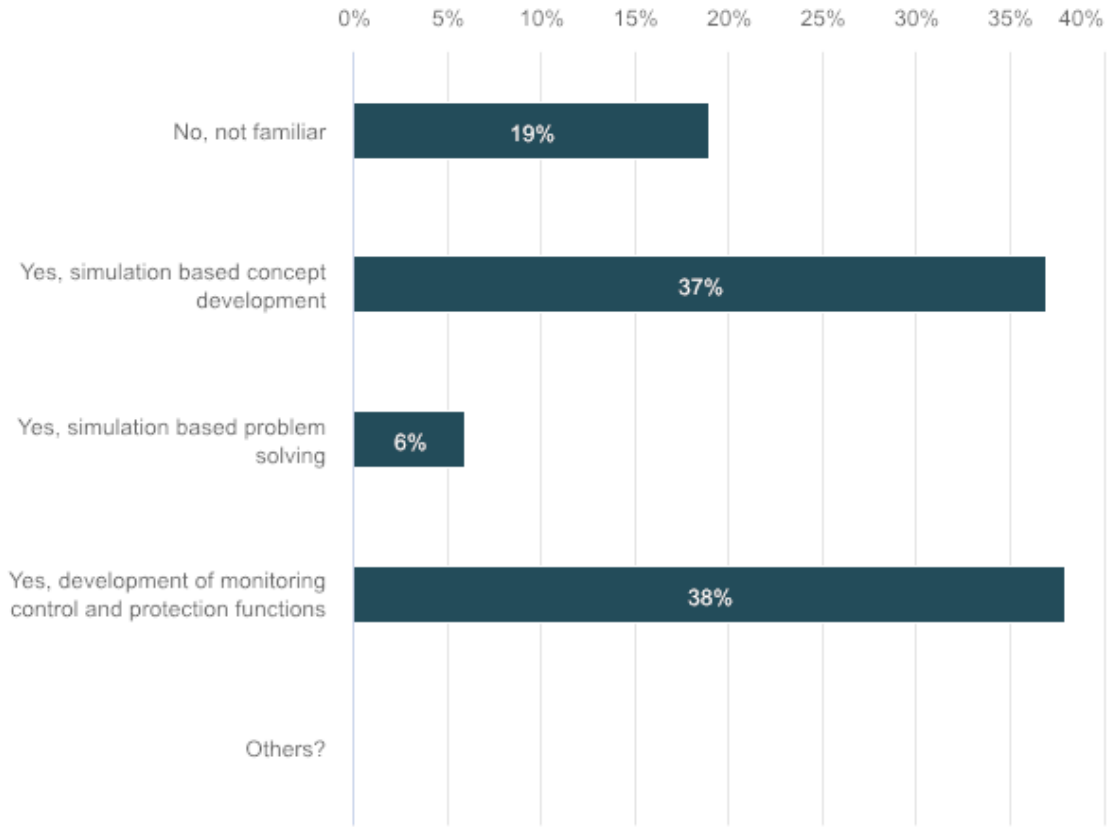


No, not familiar	10	62.5%
Yes, very familiar, What part	6	37.5%

Answers given into free text field

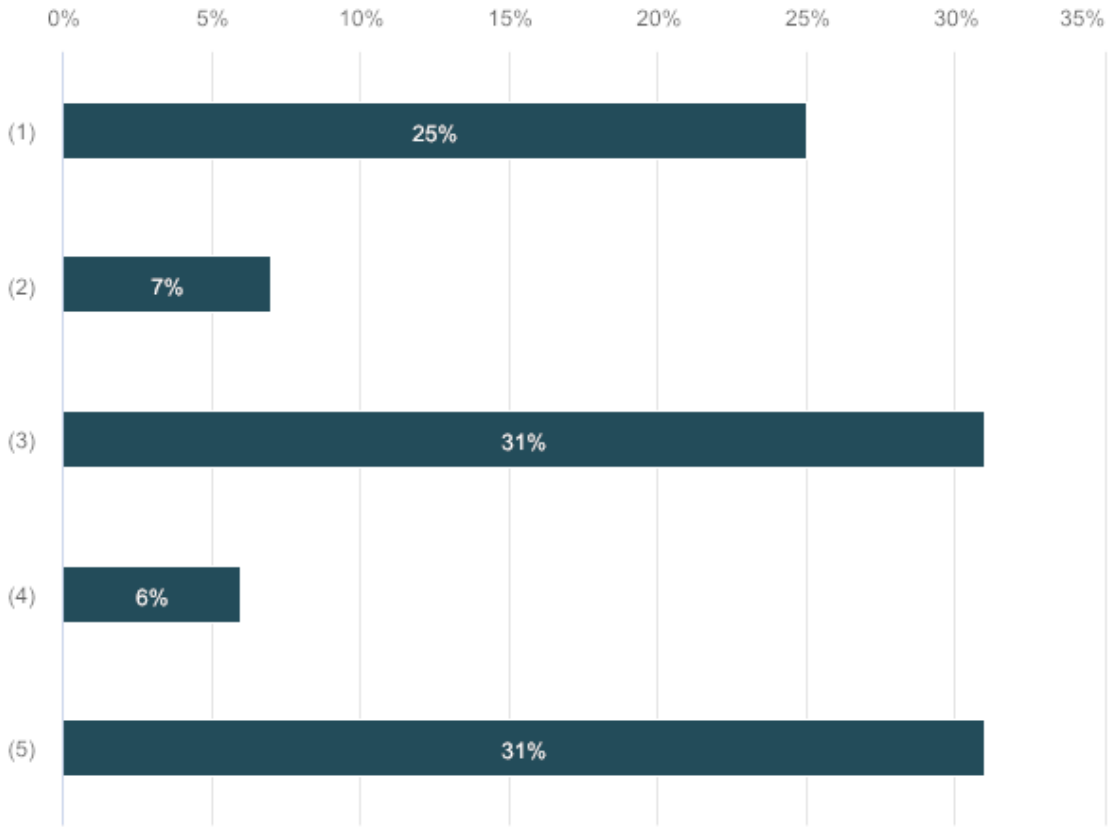
Option names	Text
Yes, very familiar, What part	62351 GOOSE MMS SV
Yes, very familiar, What part	IEC 62351-5
Yes, very familiar, What part	Not very familiar but at least know the standard. It is very complicated and messy.

Question 20. How familiar are you with simulation tools? if the answer is yes for which of the following purposes?



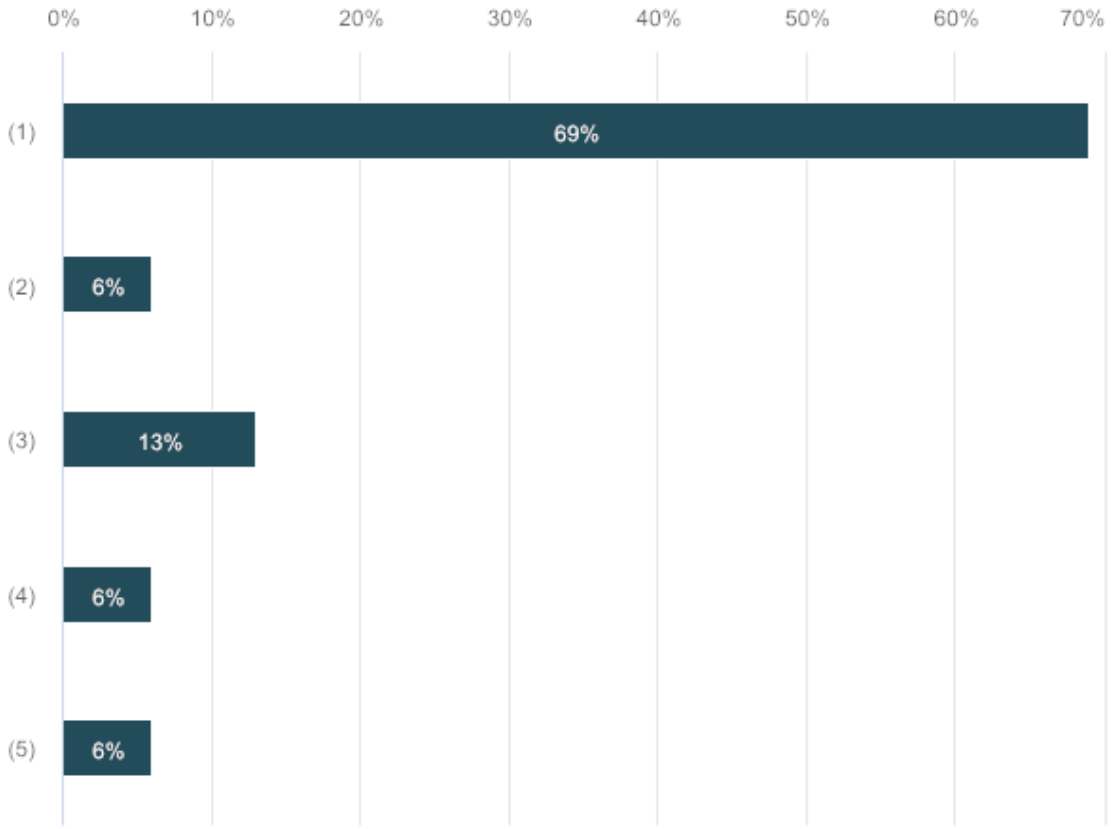
No, not familiar	3	18.75%
Yes, simulation based concept development	6	37.5%
Yes, simulation based problem solving	1	6.25%
Yes, development of monitoring control and protection functions	6	37.5%
Others?	0	0%

Question 21. How familiar are you with real-time simulator based system simulation? (1= not familiar, 5= very familiar)



(1)	4	25%
(2)	1	6.25%
(3)	5	31.25%
(4)	1	6.25%
(5)	5	31.25%

Question 22. How familiar are you with real-time simulator based Cyber Physical System CPS simulation? (1= not familiar, 5= very familiar)



(1)	11	68.75%
(2)	1	6.25%
(3)	2	12.5%
(4)	1	6.25%
(5)	1	6.25%

Question 23. What else should be explored in this area?

Responses
Training based CPS EXata and HYPERSIM
Communication link monitoring, loss/failure of communication link detection, testing procedure for the reliability of communication, differentiation between cybersecurity events (intrusions and modifications) and normal failures.
-
Fundamental instructions about cyber security
Nothing comes to mind now.
large organizations with long history have both old and new equipment. when is the point where it is more beneficial to replace the old equipment rather than maintaining it and take special precaution because of its weakest security?

End to end protection
-
Securing of legacy TCP/IP based communication protocols.
OT cyber security
There are some unclear things in this questionnaire: IT and OT parts are not separated or cleared enough. Personally I am leading our general technical development area and especially substation and network automation and protection areas. Of course for IT part there are very strict cyber security measures. OT part is a little bit different one, because those are isolated systems with restricted access. Similar cyber security measures are not fully used in the OT area. At this moment we are most interested in substation automation patch management. We have demanded that substation automation vendors should inform us all vulnerabilities of their systems and devices and then we decide case by case if there is need for real corrective patch installations. We are starting this service for next year. Of course Finnish cyber security organisation and the vendors also already now inform us about the vulnerabilities but not so systematically.
I am glad for the questions, they are insightful
GDPR
IEC 62443, NIST cyber security framework
a
-

References

[1] Opal RT HYPERSIM installation guide

[2] Scalable EXata installation guide

Leverage from the EU 2014–2020

European Union
European Regional Development Fund
European Social Fund