



SINTEF



Human and Organizational Risk Modelling in Cybersecurity for SMEs

Gencer Erdogan

Summer School Cyber In Normandy

24 June 2024 – 5 July 2024, Caen, France



SINTEF

Agenda

09:00 – 10:30 Part 1

- Background
- Cybersecurity Awareness and Capacities of SMEs (a survey of 141 SMEs)
- Needs and Challenges Concerning Cyber-risk Assessment in the Cyber-physical Smart Grid (interviews with domain experts)

10:30 – 11:00 Coffee break

11:00 – 12:30 Part 2

- Introduction to the Customer Journey Modelling language and tool
- Play a puzzle game to learn Customer Journey Modelling (you need a laptop)



SINTEF

Background

- Cybersecurity \leftrightarrow information security and critical infrastructure protection
- Cyber risk management and risk assessment
- SMEs
- Cybersecurity and risk challenges for SMEs

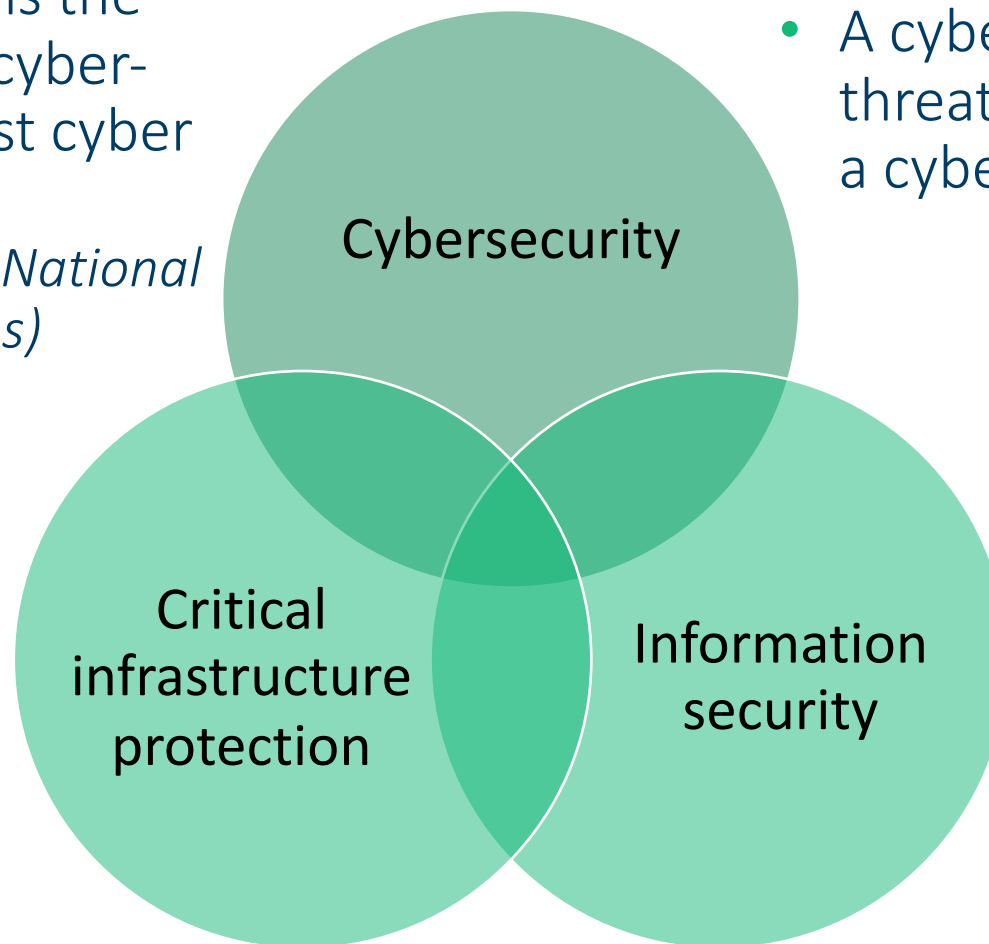


SINTEF

Cybersecurity

- Cybersecurity is the protection of cyber-systems against cyber threats.
(Committee on National Security Systems)

- Critical (information) infrastructure protection is concerned with the prevention of the disruption, disabling, destruction, or malicious control of infrastructure.
(ISO/IEC 27032)



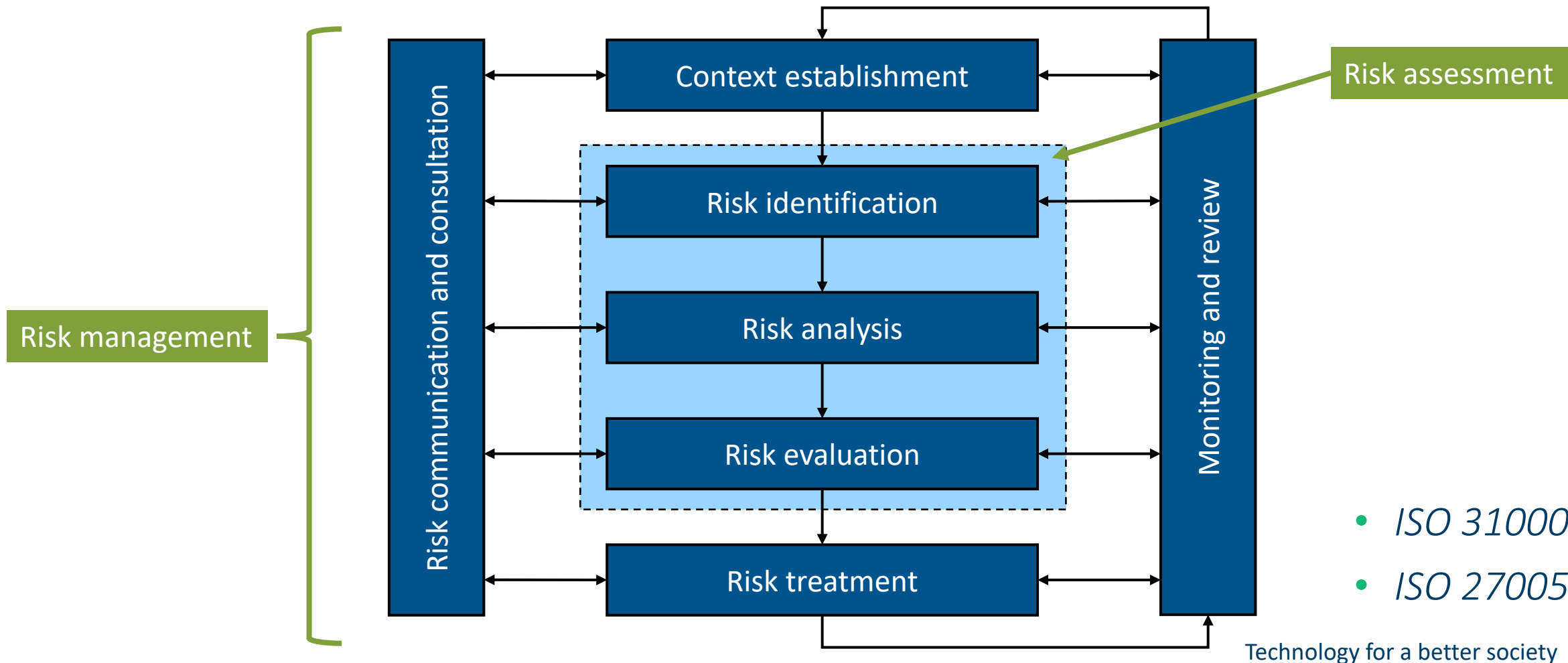
- A cyber-threat is a threat that exploits a cyberspace.

- Information security is the preservation of Confidentiality, Integrity, and Availability of information.
(ISO/IEC 27000)



SINTEF

Cyber risk management and risk assessment





SINTEF

SMEs

- Small and medium-sized enterprises (SMEs) represent 99% of all businesses in the EU.

Company category	Staff headcount	Turnover
Medium-sized	< 250	≤ € 50 m
Small	< 50	≤ € 10 m
Micro	< 10	≤ € 2 m



SINTEF

Cybersecurity and risk challenges for SMEs

1. Regulatory Compliance:

- SMEs must comply with cybersecurity regulations to avoid legal sanctions but often lack the resources and expertise to do so effectively.
 - The General Data Protection Regulation (GDPR), Directive on Security of Network and Information Systems (NIS2), EU Cybersecurity Act, EU AI Act...

2. Human Factors:

- Employees and clients can be targets for cyber-attacks, posing significant risks. SMEs need to address these vulnerabilities through training and awareness.



SINTEF

Cybersecurity and risk challenges for SMEs

3. Information Sharing:

- SMEs in supply chains are often reluctant to share their cybersecurity status, hindering collective security efforts.

4. Resource Constraints:

- Limited resources and expertise make it challenging for SMEs to implement robust cybersecurity measures.

Cybersecurity and risk challenges for SMEs

Top 8 Cyber Attacks – 2024



1 Phishing Attack
The use of deceptive emails, texts, or websites to gain sensitive information.



2 Ransomware
Malware that can encrypt data and make you pay to get them back.



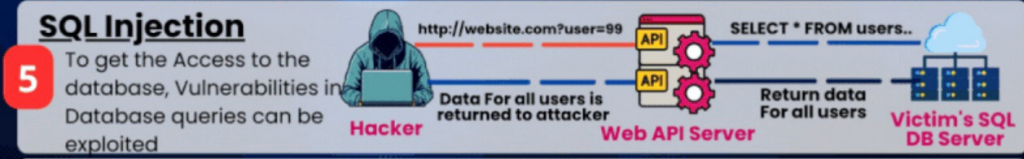
3 Denial-of-Service (DoS)
Loading excessive load on a machine or network so that it stops working normally.



4 Man-in-the-Middle (MitM)
Engaging in covert interception and manipulation of communication between two parties without noticing it.



5 SQL Injection
To get the Access to the database, Vulnerabilities in Database queries can be exploited.



6 Cross-Site Scripting (XSS)
Putting malicious code into websites that other people visit.



7 Zero-Day Exploits
Attacks take advantage of unknown vulnerabilities before programmers can fix them.



8 DNS Spoofing
Sending DNS queries to malicious sites so that they can be accessed without permission.

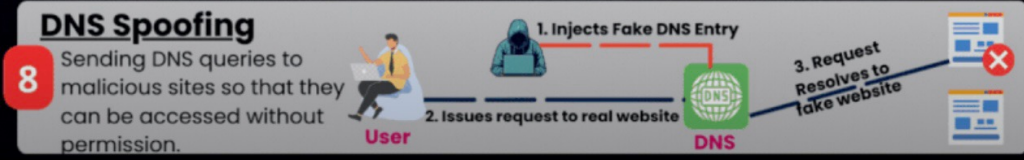


Image: Ethical Hackers Academy® on LinkedIn



Cybersecurity Awareness and Capacities of SMEs

(A survey of 141 SMEs)

- Survey intro and method
- Cybersecurity awareness of SMEs
- Cybersecurity practices of SMEs
- Conclusion



SINTEF

Survey intro and method

Target group

- Employees from SMEs.
- SME: an enterprise fewer than 250 persons (EC).
- In total, 141 SMEs based in the UK were recruited.
- One participant per SME.

Sampling and data collection

- UK was chosen because 40% of UK-based businesses report on security breaches and attacks.
- Approach respondents in their native language.
- Recruitment via Norstat recruitment agency for online research. QuenchTec.

Questionnaire design

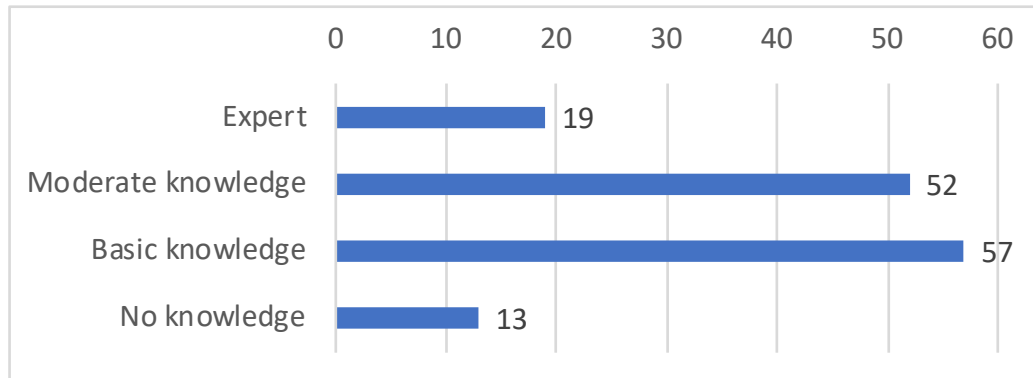
- Iteratively developed and piloted with N=23 participants.
- In total 27 questions: company, participant, infrastructure, cybersecurity awareness, cybersecurity practices.
- Focus of this presentation: awareness and practices. 13 questions.



SINTEF

Knowledge of the employees and their company's awareness

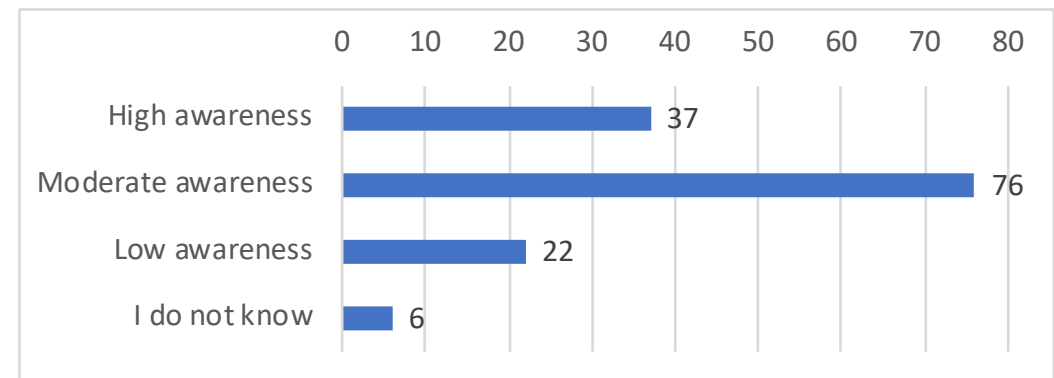
How would you characterize your own knowledge about cybersecurity?



- 19+52=71 of the 141 respondents (50%) characterize their own cybersecurity-knowledge as moderate or expert.

- only 51 of the 141 respondents work with cybersecurity, but 71 assess themselves as moderate/expert:
The perception about their own security awareness is rather optimistic.

How would you characterize your company when it comes to cybersecurity awareness?

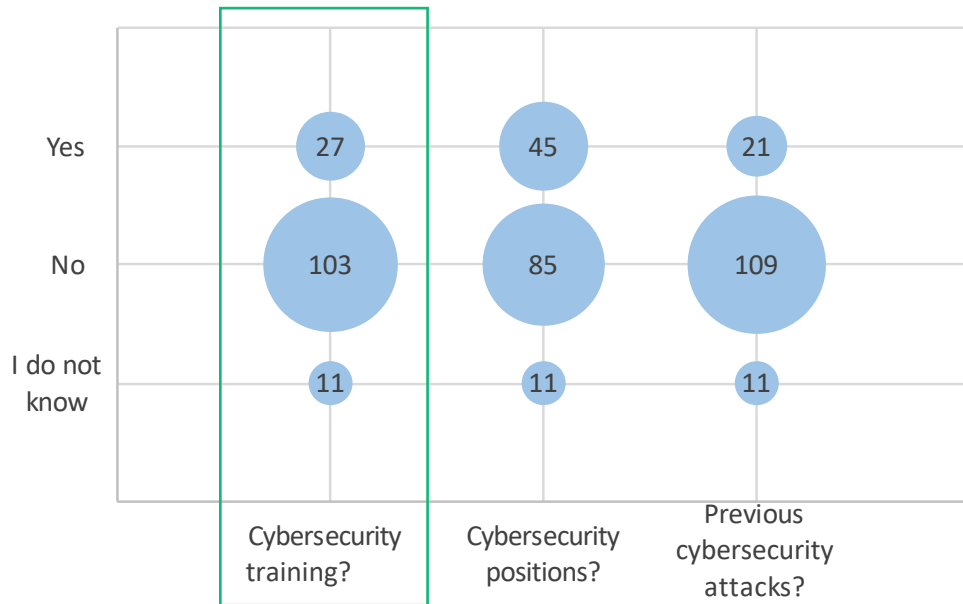


- 37+76=113 of the 141 respondents (80%) characterize their company's cybersecurity-awareness as moderate or high.

- People tend to trust that cybersecurity is dealt with in other parts of the company. "If people think someone else is responsible, then they won't take action themselves" (Paek & Hove, 2017).

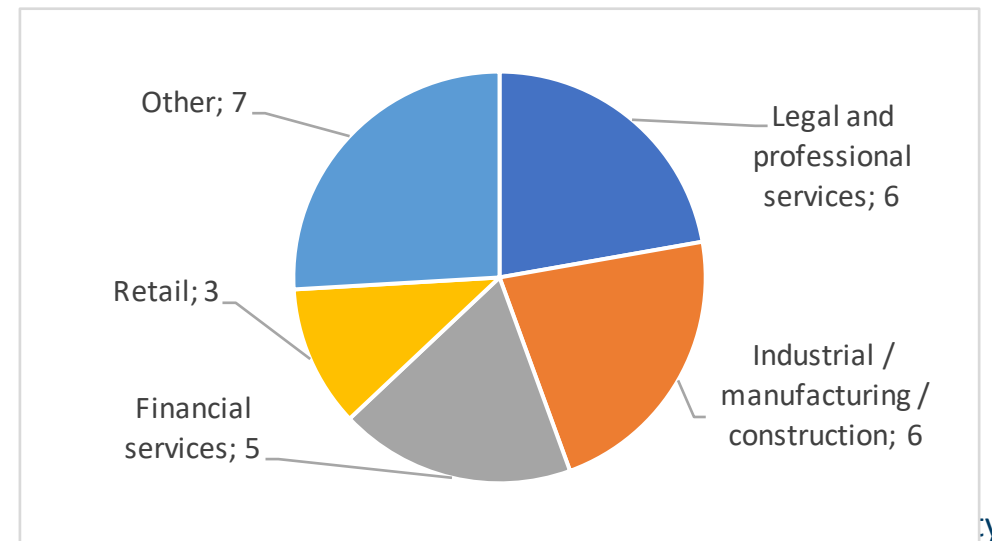
Training capabilities

Does your company offer courses or training material for employees to raise awareness about cybersecurity?



- Despite the 50% moderate to high cybersecurity awareness, only 27 provide cybersecurity training for their employees.
- The training offered is limited to the basics of security and privacy that employees need to be aware of at work.
- The frequency of training is either once at onboarding or at best yearly repetitions.

• Domains:

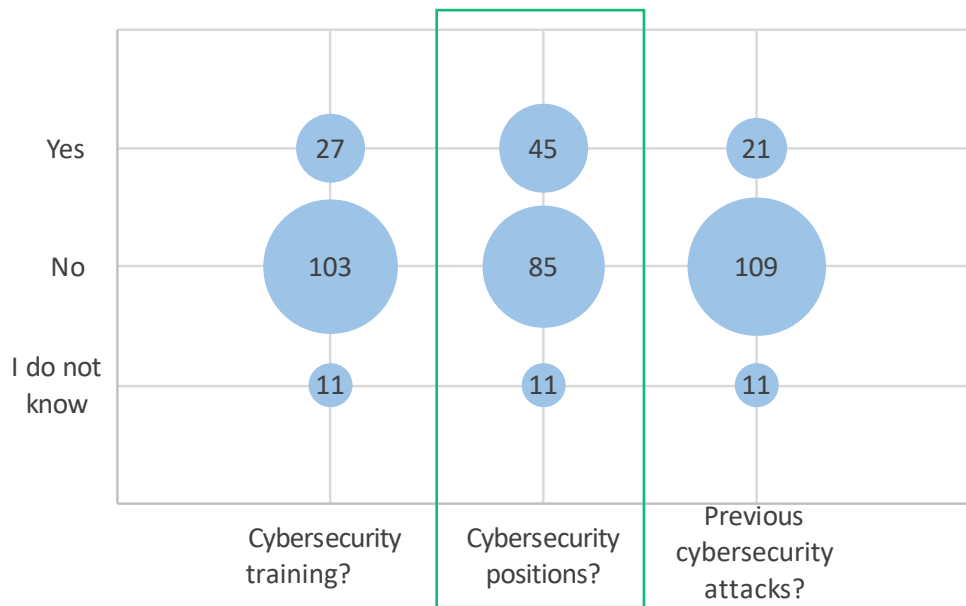




SINTEF

Security positions

Does your company have positions dedicated to cybersecurity at any level?



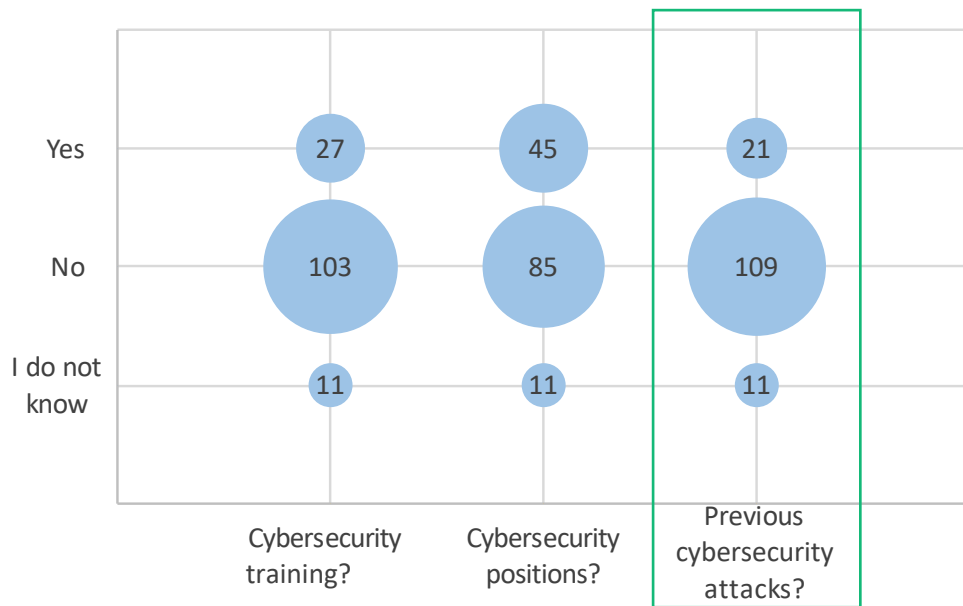
- 45 of the 141 respondents (32%) confirm that their SME have positions dedicated to cybersecurity.
- The question regarding dedicated cybersecurity positions scored the highest (45 out of 141) compared to other yes/no questions. This indicates that the SMEs should be better prepared than indicated in the survey results in general.
- Positive: from the 45 respondents that do have cybersecurity positions, the industry sector is quite diverse: Software and computer service, retail, health, manufacturing, financial services, ...



SINTEF

Previous cybersecurity attacks

Were there any previous cybersecurity attacks on your company that you know about?



- Only 21 of the 141 respondents (15%) were aware of previous cybersecurity attacks.

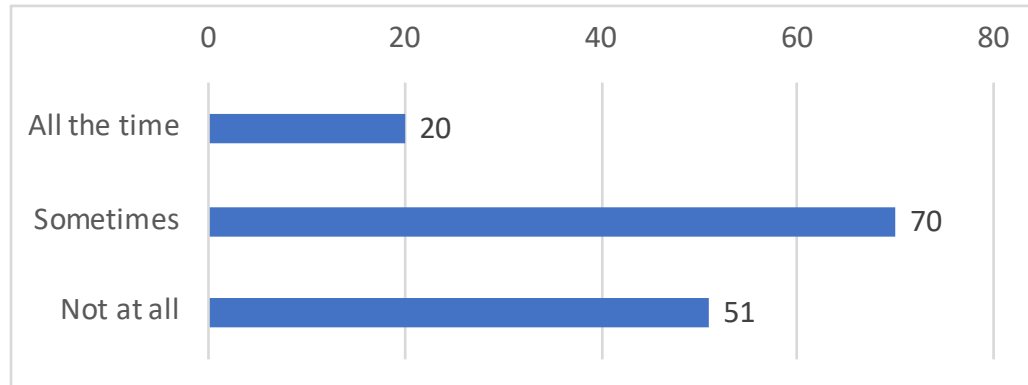
- An attack harmed one or more security qualities:
 - 12 attacks altered the integrity of information
 - 11 attacks rendered the information system unavailable
 - 6 attacks caused a breach of confidential information



SINTEF

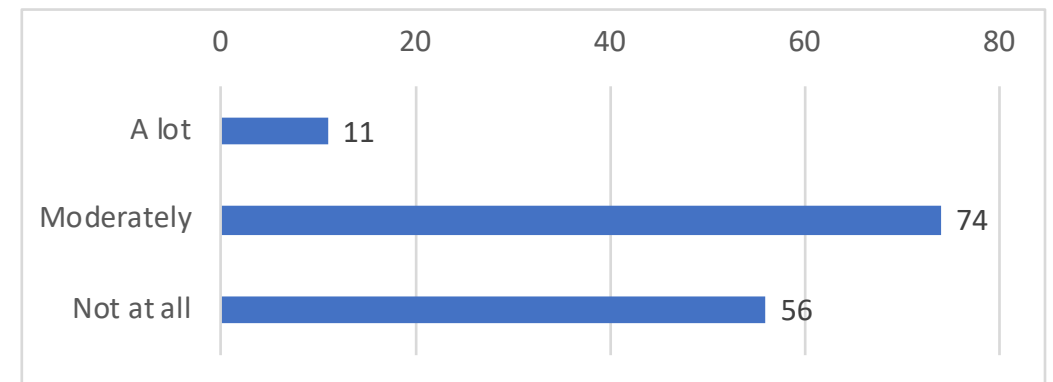
Discussing cybersecurity issues, and fear of attack

Do you discuss cybersecurity issues on your company meetings or presentations or, in general, internally in your company?



- Only 20 of the 141 respondents (15%) mention that they regularly discuss security issues as part of company processes.
- This indicates a lack of focus on security issues and clear security processes, but this problem is also linked to lack of security positions and available resources.

To what degree do you fear for a cybersecurity attack towards your company?



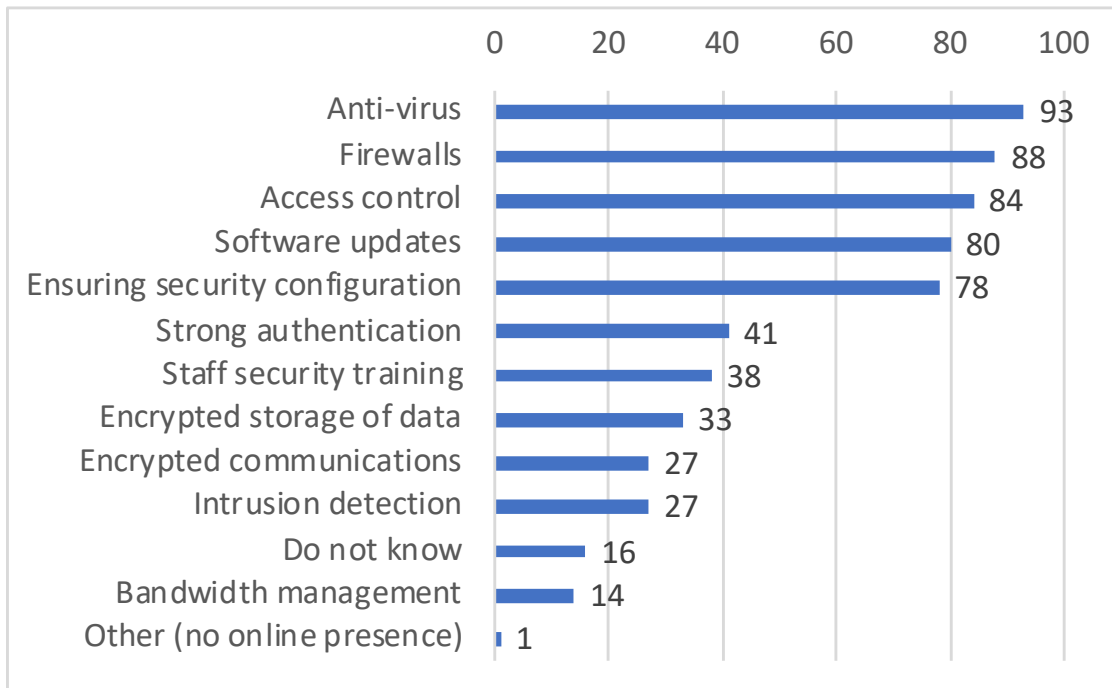
- $11+74=85$ of the 141 respondents (60%) have a “moderate” or “a lot” of fear that their company will be attacked.
- SME’s are to some extent aware, but the lack of focus on security, training, dedicated positions, and awareness of attacks may indicate that SME’s do not feel responsible.



SINTEF

Security measures to avoid cybersecurity attacks

What security measures is your company taking to avoid cybersecurity attacks?



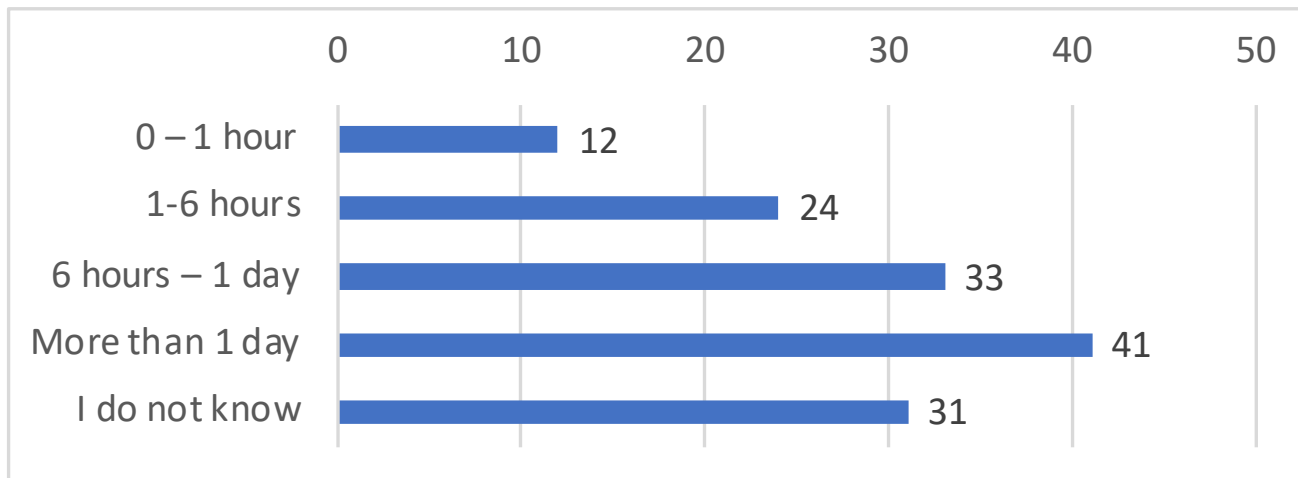
- Basic security tools such as Anti-virus and Firewalls are the main security mechanisms in use.
- Tools for training and the identification of threats and vulnerabilities are less used, but this may be because of lack of appropriate tooling with low threshold.
- SMEs need more training and easy-to-use tools to help carry out tasks such as threat and vulnerability identification and risk assessment.



SINTEF

Availability criticality

How long do you think your critical applications and systems can be shut down before significant disruption is caused to the company?



- The fact that $41+31=72$ of the 141 respondents (over 50%) replied “more than 1 day” or “I do not know” indicates that the respondents may not have the full overview of their critical assets.
- That is, SME’s need better tool support to assess and understand their critical assets.



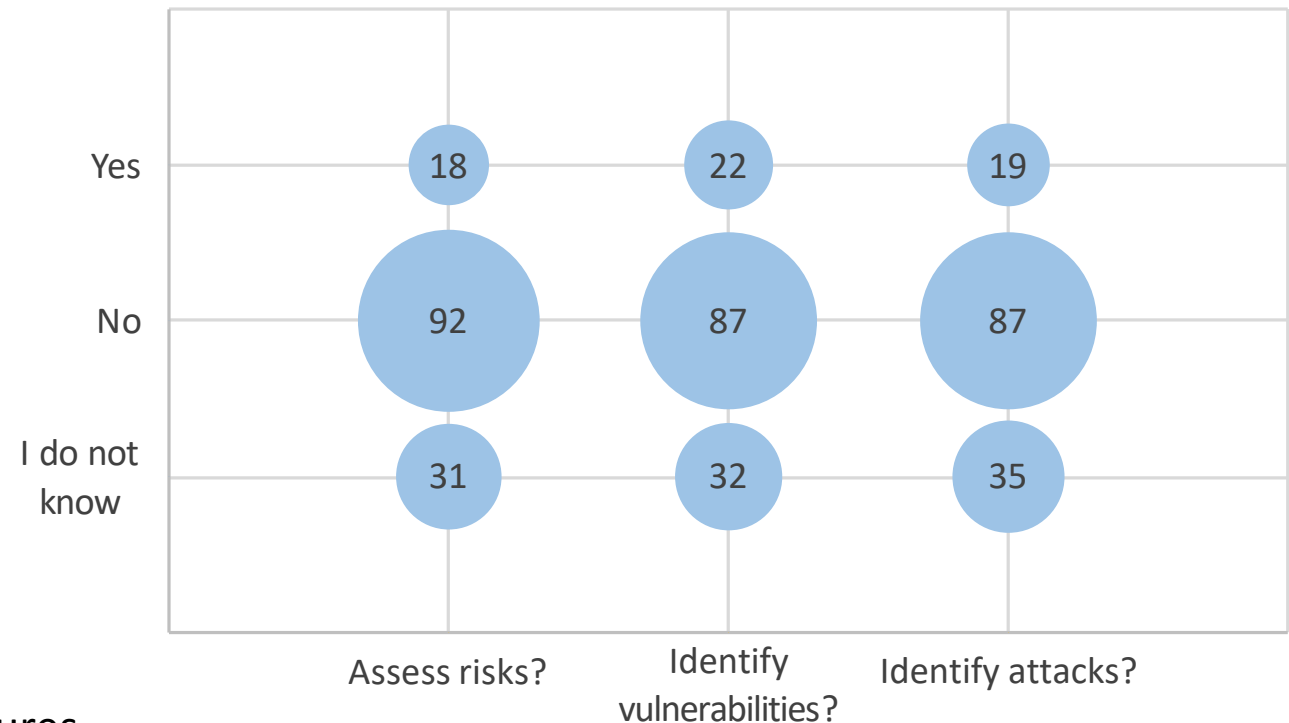
SINTEF

Processes and tools

Does your company use specific processes or tools

- to assess risk to its IT assets?***
- for identifying vulnerabilities?***
- for identifying attacks?***

- Hardly any of the SMEs use tools or have processes in place to assess cybersecurity risks, identify vulnerabilities, and identify attacks.
- This indicates lack of appropriate tools to encourage awareness, and tools to easily capture and present threats and their corresponding measures.





SINTEF

Conclusion

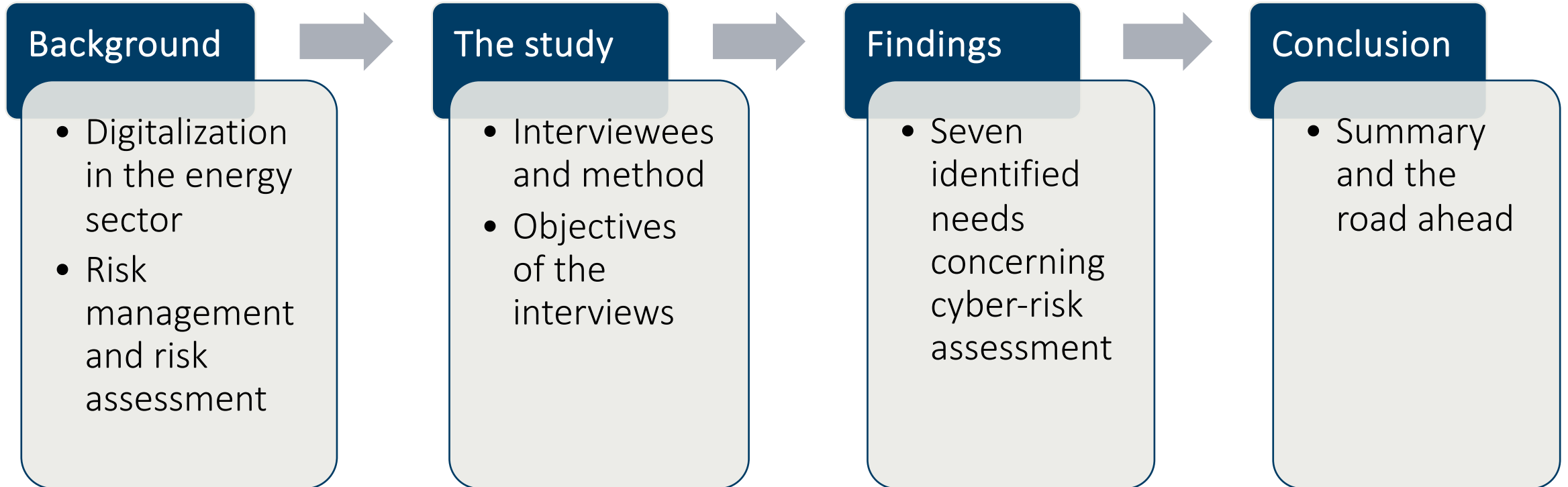
- There is an apparent discrepancy between the levels of awareness and knowledge claimed by individuals.
- People tend to trust that security is dealt with in other parts of the company. Lack of individual responsibility taking.
- The training offered is limited to the basics of security and privacy, and there is a lack of appropriate training material and courses.
- Although 45 of the 141 respondents (32%) confirm that their SME have positions dedicated to cybersecurity, there is a lack of supportive low-threshold tools to assess vulnerabilities and cybersecurity risks.
- SMEs need to increase focus on security processes, training, dedicated security positions, and awareness of attacks to better protect themselves from cybersecurity risks.



Needs and Challenges Concerning Cyber-risk Assessment in the Cyber-physical Smart Grid (interviews with domain experts)

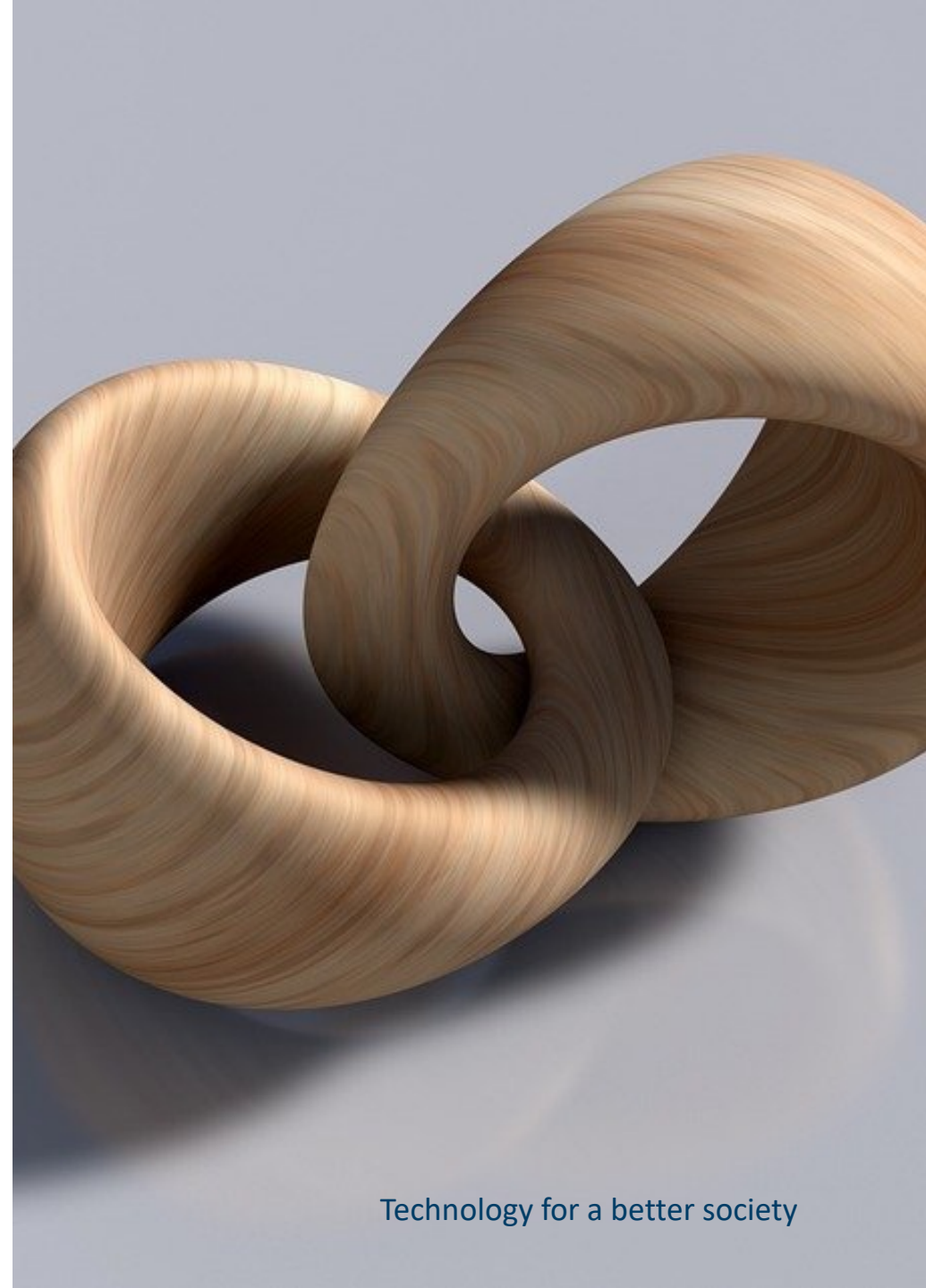


Outline



Digitalization introduces a strong coupling between the electric power domain and ICT

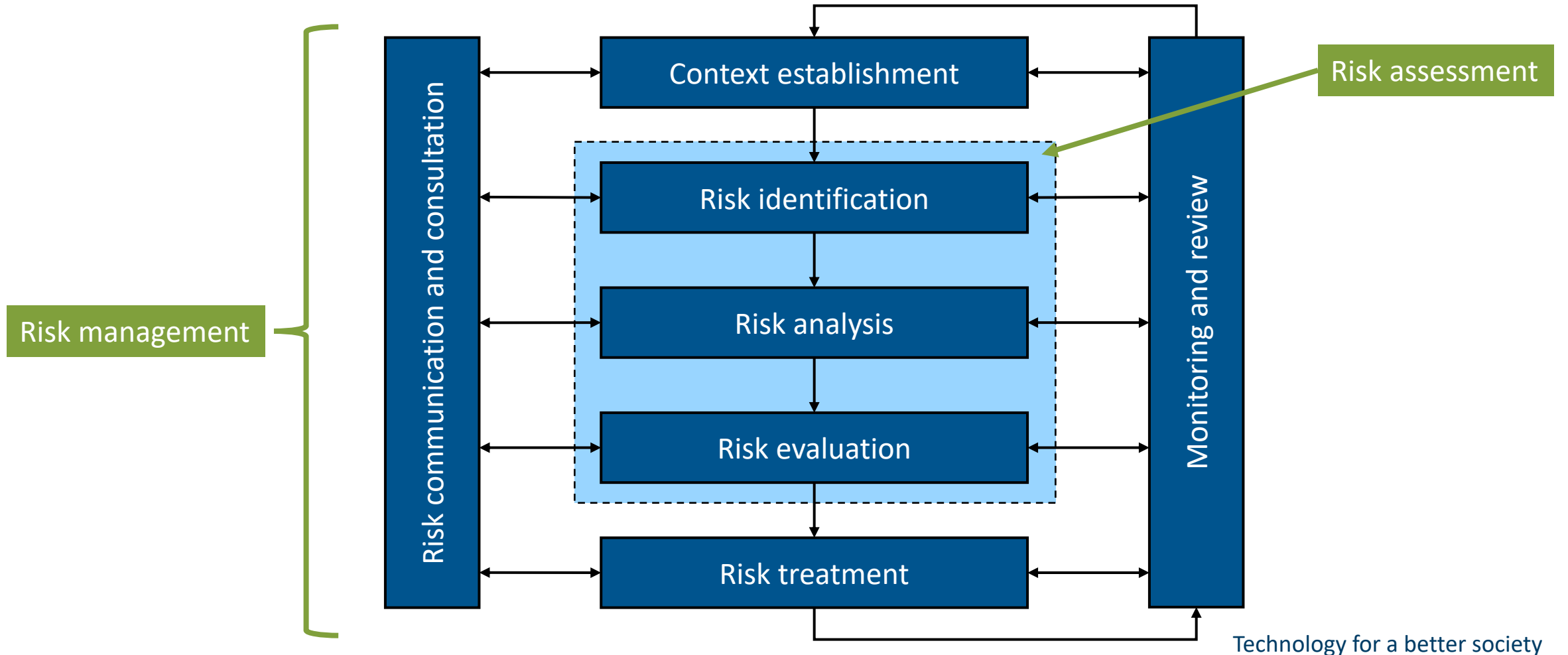
- We can no longer perceive the electric power domain isolated from the ICT domain
- These two domains are tightly integrated
- This integration introduces a new risk picture not considered earlier
 - "Connected with the rest of the world"
 - Huge attack surface
 - Almost any cybersecurity risk applies
 - Safety risk caused by security risk
- How to deal with this?





SINTEF

Risk management and risk assessment





Interviewees, method and objectives

No.	Interviewee	Organization
1	1 Cybersecurity expert	KraftCERT ¹
2	1 CISO	Energy company (LE)
3	1 CISO	Energy company (LE)
4	1 CISO 1 Senior PM	Energy company (SME)
5	1 CISO	Energy company (SME)
6	1 Cybersecurity expert	NVE ²

¹The Norwegian Computer Emergency Response Team for the electric power sector (KraftCERT).

²The Norwegian Water Resources and Energy Directorate (NVE).

Semi-structured interview with open-ended questions:

- Industry practice within cybersecurity and cyber-risk assessment
- Approaches to risk assessment that work in the industry
- Shortcomings and needs within cybersecurity and cyber-risk assessment in the energy sector

1 – Methods need to be easy to understand and use also for non cyber-risk experts

- Cybersecurity experts are becoming a bottleneck in large organizations
- Push towards system owners to take more responsibility for assessing risks
- People with little or no competence in cybersecurity have to assess cyber risk
- More than 50% of DSOs¹ are SMEs with little or no capacity within cybersecurity
- *"More important that the methods are easy to use than the quality of the results"*

¹DSO = Distribution System Operator

N O B O D Y

S A I D

I T

W A S

E A S Y



SINTEF

2 – Need for support to determine whether a method is a good match for a given context

- A large variety in current practice and ability to assess risks (detailed vs simple)
- Limited competence: difficult to know how to start assessing cyber risks
- Depending on the context of assessment
 - Which method?
 - What questions?
 - Who should be involved?
- "Need simple methods" \leftrightarrow "need to capture the full complexity"





SINTEF

3 – Need for support to prepare participants for an assessment

- Cybersecurity is often considered as one abstract scenario (lack of preparation)
- Little or no training of people that are expected in risk assessments
- People from IT and OT are involved but they "talk different languages"
- To contribute in a meaningful way, there is a need for
 - Domain specific cyber-risk scenario examples
 - Training
 - Conceptual clarifications



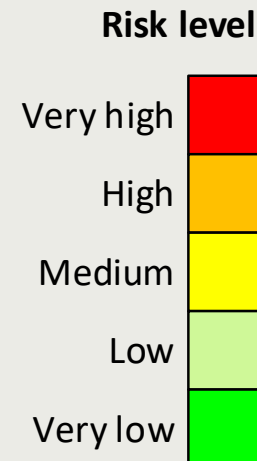
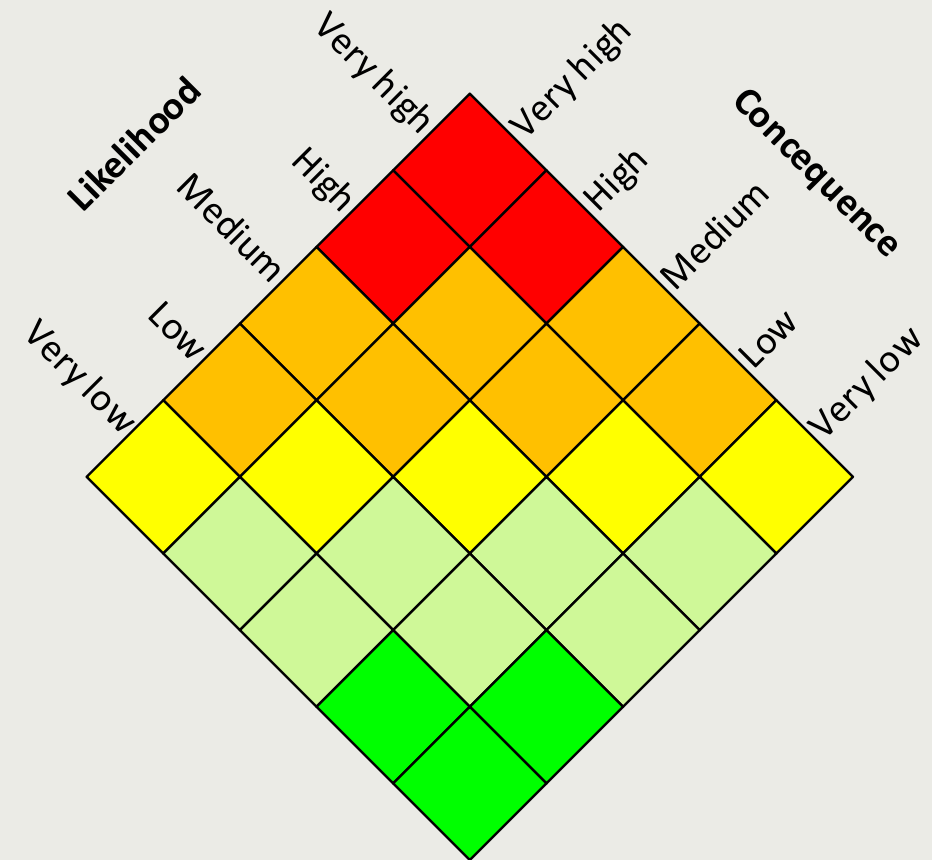
4 – Need for support to manage complexity

- The target of analysis is becoming more complex over time due to digitalization
- Difficult to carry out good/thorough risk assessments
- Difficult to capture important changes over time as part of the assessment
- Challenging to merge several assessments
- *"Pen-testing is used as an alternative to assess risks and manage complexity"*



5 – Need for support to estimate cyber-risks

- The scales used for likelihood and consequence at organizational level are not always applicable for cyber-risk
- Likelihood and consequence are understood differently (IT/OT) – disagreements happen
- Difficult to estimate the likelihood of malicious threats
- Lack of data to support estimation
 - How to deal with very-low likelihood/very-high consequence?
- *"How can we reuse likelihood estimates?"*





6 – Need for support to increase trust in the risk assessment results

- Risk assessments are often subjective
- Need to express uncertainty in order to increase trust in the results
- Uncertainty needs to be expressed together with risk estimates
- Increased trust is important to obtain better decision support for security investments
- *"Pen-testing is used as an alternative to validate the risk picture"*





SINTEF

7 – Support risk management: documentation, maintenance, and identifying treatments

- Risk assessments are not well documented in practice (lack of culture for documenting results)
- It is important to maintain the risk assessments over time (updated)
- Need guidelines to identify risk treatments and how to implement them
- Need to communicate risks and treatments to the management in a pedagogical manner





SINTEF

We identified 7 needs for cyber-risk assessment in the electric power domain

Easy to use

Good match

Preparation

Complexity

Risk
estimation

Trust

Maintenance



SINTEF

Agenda

09:00 – 10:30 Part 1

- Background
- Cybersecurity Awareness and Capacities of SMEs (based on a survey of 141 SMEs)
- Needs and Challenges Concerning Cyber-risk Assessment in the Cyber-physical Smart Grid (based on interviews with domain experts)

10:30 – 11:00 Coffee break

11:00 – 12:30 Part 2

- Introduction to the Customer Journey Modelling language and tool
- Play a puzzle game to learn Customer Journey Modelling (you need a laptop)

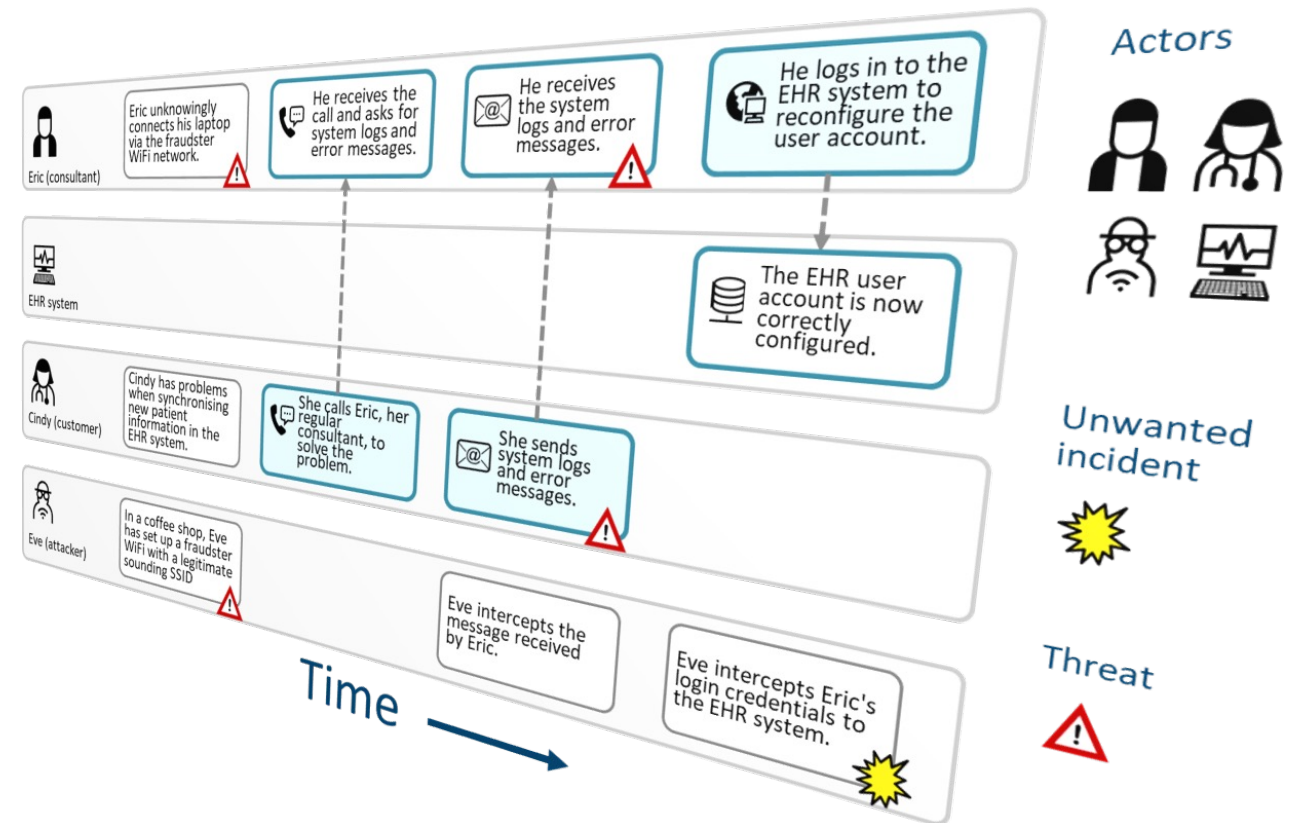


SINTEF

CJML - Customer Journey Modelling Language



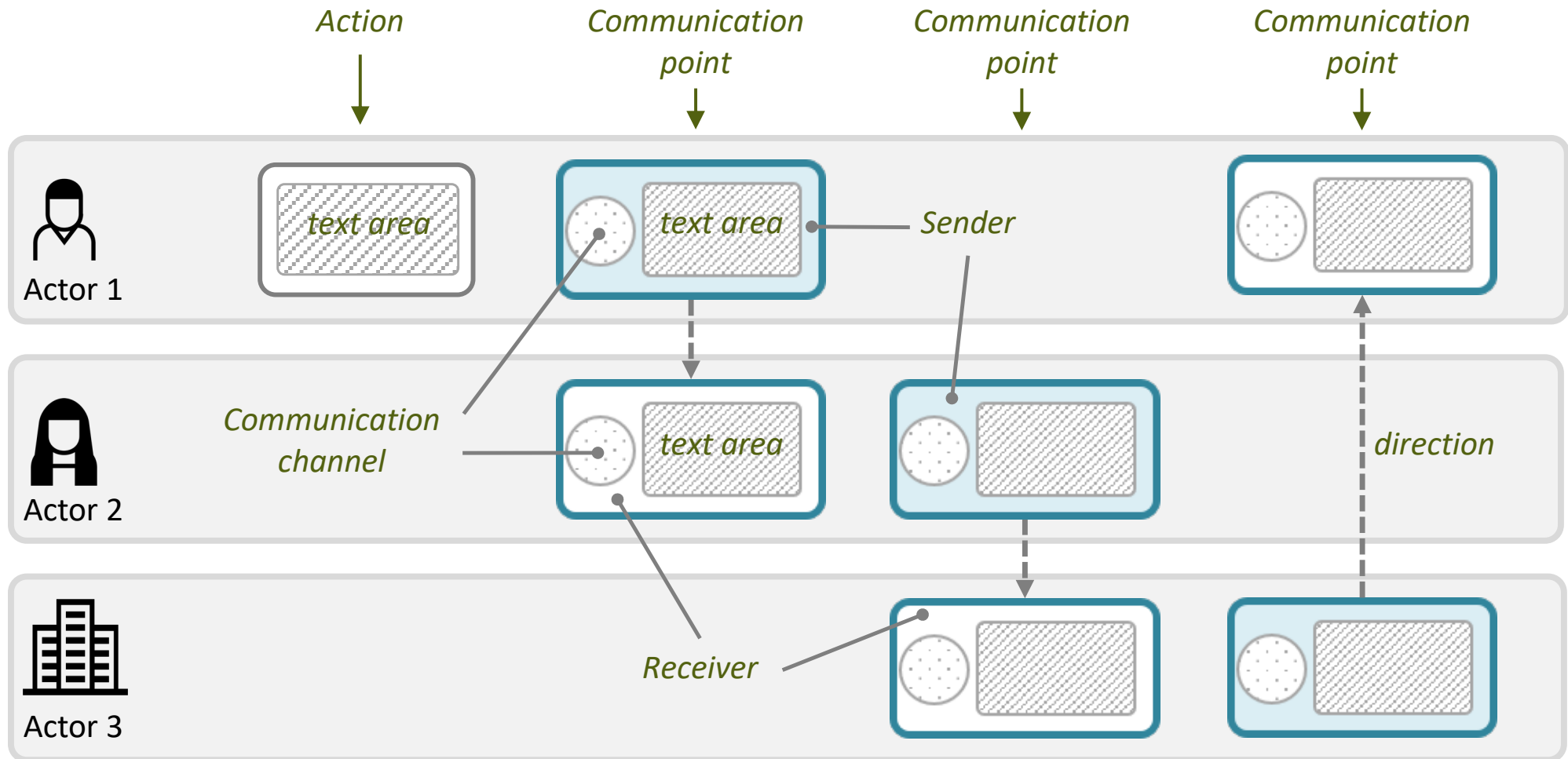
- CJML is a visual language dedicated to modelling of human journeys, regardless of whether the human has the role of customer, user, patient, or citizen
- Easy to use and understand
- Free and open source
- <https://cjml.no/horm/>





SINTEF

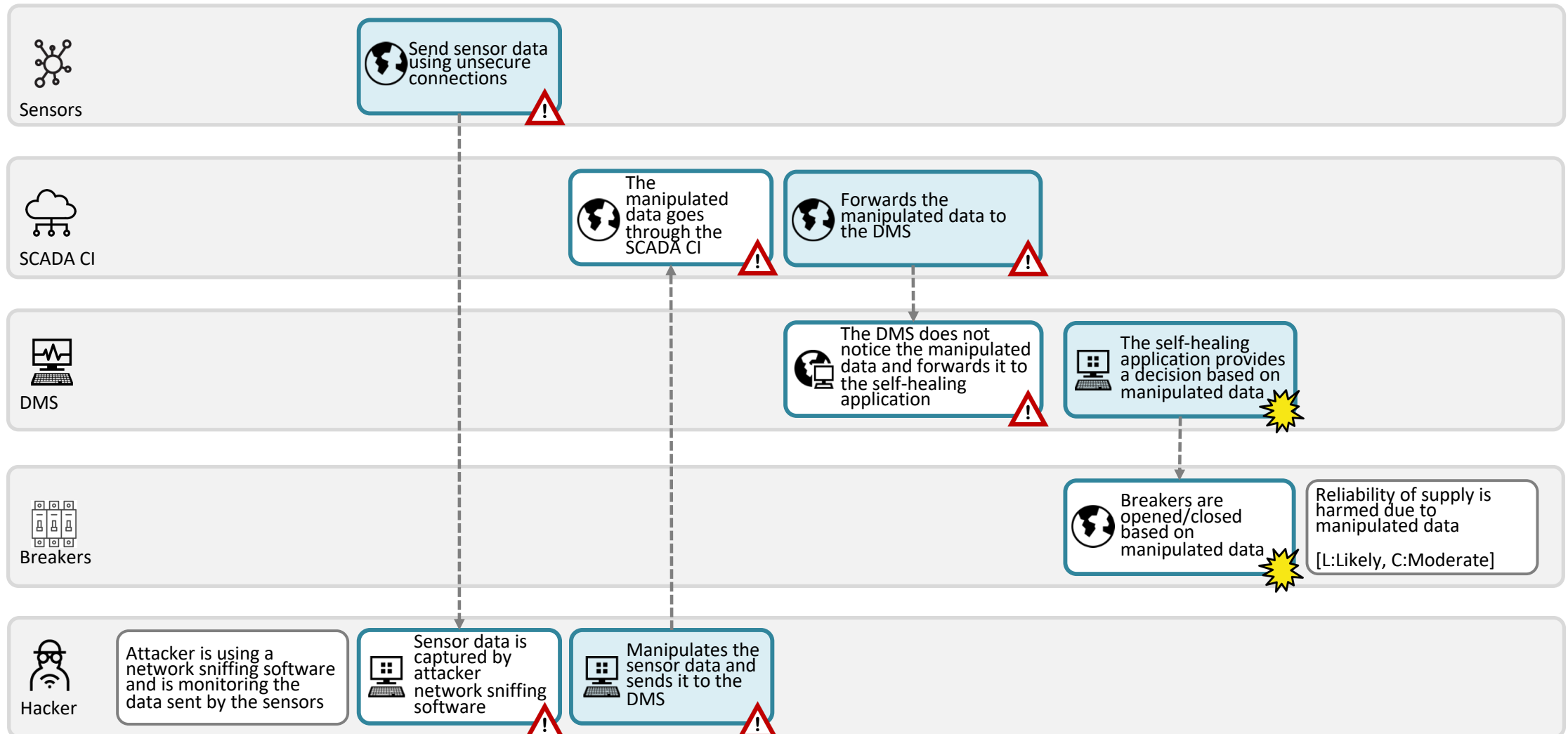
Definitions – Journey Network Diagram





SINTEF

Hacker manipulates sensor data and thereby harms reliability of electricity supply





SINTEF

References

1. Gencer Erdogan, Inger Anne Tøndel, Shukun Tokas, Michele Garau, Martin Gilje Jaatun. Needs and Challenges Concerning Cyber-Risk Assessment in the Cyber-Physical Smart Grid. In Proc. 17th International Conference on Software Technologies (ICSOFT'22), pages 21-32, SCITEPRESS, 2022. DOI: <https://doi.org/10.5220/0011137100003266>
2. Stephen C. Phillips, Nicholas Fair, Gencer Erdogan, Simeon Tverdal. Information Security and Risk Management: Trustworthiness and Human Interaction. In Proc. 16th International Conference on Research Challenges in Information Science (RCIS'22), LNBIP 446, pages 821-822, Springer, 2022. DOI: <https://doi.org/10.1007/978-3-031-05760-1>
3. Gencer Erdogan, Ragnhild Halvorsrud, Costas Boletis, Simeon Tverdal, John Brian Pickering. Cybersecurity Awareness and Capacities of SMEs. In Proc. 9th International Conference on Information Systems Security and Privacy (ICISSP'23), pages 296-304, SCITEPRESS, 2023. DOI: <https://doi.org/10.5220/0011609600003405>
4. Brian Pickering, Stephen C. Phillips, Gencer Erdogan. I Just Want to Help: SMEs Engaging with Cybersecurity Technology. In Proc. HCI for Cybersecurity, Privacy and Trust (HCII'23). Lecture Notes in Computer Science, vol 14045, pages 338-352. Springer, Cham, 2023. DOI: https://doi.org/10.1007/978-3-031-35822-7_23



SINTEF

References

5. Gencer Erdogan, Iver Bakken Sperstad, Michele Garau, Oddbjørn Gjerde, Inger Anne Tøndel, Shukun Tokas, Martin Gilje Jaatun. Adapting Cyber-Risk Assessment for the Planning of Cyber-Physical Smart Grids Based on Industrial Needs. In book titled Software Technologies. Communications in Computer and Information Science, vol 1859, pages 98-121. Springer, Cham, 2023. DOI: https://doi.org/10.1007/978-3-031-37231-5_5
6. R. Halvorsrud, C. Boletsis and E. Garcia-Ceja, "Designing a Modeling Language for Customer Journeys: Lessons Learned from User Involvement," 2021 ACM/IEEE 24th International Conference on Model Driven Engineering Languages and Systems (MODELS), Fukuoka, Japan, 2021, pp. 239-249. DOI: <https://doi.org/10.1109/models50736.2021.00032>
7. Customer Journey Modeling Language. Tools, method, language, training materials. <https://cjml.no/>
8. Human and organisational risk modelling. Tools, method, language, training materials. <https://cjml.no/horm/>
9. Lund, M. S., Solhaug, B., & Stølen, K. (2011). Model-driven risk analysis - The CORAS Approach. Springer Berlin Heidelberg. DOI: <https://doi.org/10.1007/978-3-642-12323-8>
10. The CORAS risk assessment approach. Tools, method, language, training materials. <https://coras.tools/>



SINTEF

References

11. ISO/IEC 27032:2023 Cybersecurity — Guidelines for Internet security. <https://www.iso.org/standard/76070.html>
12. ISO/IEC 27000:2018 Information technology — Security techniques — Information security management systems — Overview and vocabulary. <https://www.iso.org/standard/73906.html>
13. ISO/IEC 27005:2022 Information security, cybersecurity and privacy protection — Guidance on managing information security risks. <https://www.iso.org/standard/80585.html>
14. ISO 31000:2018 Risk management — Guidelines. <https://www.iso.org/standard/65694.html>
15. European Commission SME definition. https://single-market-economy.ec.europa.eu/smes/sme-fundamentals/sme-definition_en
16. Atle Refsdal, Bjørnar Solhaug, Ketil Stølen. Cyber-Risk Management. Springer Cham, 2015. DOI: <https://doi.org/10.1007/978-3-319-23570-7>



SINTEF

Technology for a better society