TALLINN UNIVERSITY OF TECHNOLOGY
School of Information Technologies

Anastasiya Kornitska IVCM177360

EXPLORING HOW TO ESTABLISH CROSS-FUNCTIONAL TEAMS FOR CYBER SECURITY OF INDUSTRIAL CONTROL SYSTEMS

Master's Thesis

Supervisor: Hayretdin Bahşi
Professor

Tallinn 2021

TALLINNA TEHNIKAÜLIKOOL
Infotehnoloogia teaduskond

Anastasiya Kornitska IVCM177360

TÖÖSTUSLIKE JUHTIMISSÜSTEEMIDE KAITSEKS LOODUD MULTIDISTSIPLINAARSETE KÜBERTURVALISUSE MEESKONDADE LOOMINE

Magistritöö

Juhendaja: Hayretdin Bahşi
Professor

Tallinn 2021

Author’s declaration of originality

I hereby certify that I am the sole author of this thesis. All the used materials, references to the literature and the work of others have been referred to. This thesis has not been presented for examination anywhere else.

Author: Anastasiya Kornitska

21.12.2020

Abstract

This thesis is written in the English language and is 88 pages long, includes five chapters, five figures and seven tables.

The digital transformation of the industrial control system environments led to the OT-responsible and the IT employees working together to ensure its cybersecurity. However, there is also a substantial deficit of qualified talents on the market to perform the work. This thesis addresses the lack of best practices available in regard to establishing ICS cybersecurity cross-functional teams. This research is a descriptive study that uses semi-structured interviews as a type of elicitation data collection methods. A qualitative data analysis method is used by keyword coding, that is performed in MaxQDA software. The interviews were done with seven experts who had different levels of experience in ICS cybersecurity-cross functional teams as managers or team members. The data gathered, reveals the perspectives of the experts in: selecting team members and the manager; the transition of employees from former responsibilities to the work in ICS cybersecurity cross-functional teams; reporting structure and accountability for risks; description of typical activities and projects, education and learning; communication; and relationship management with vendors. The research discusses the best and worst practices, by comparing the collected information with the available literature (academic articles, reports, industry recommendations and standards). It describes the common criteria and suggestions in: cybersecurity processes in ICS that should be done by a cross-functional team, governance structures, competencies, soft skills that need to be possessed by the members, education, communication management, motivations and other soft aspects. The results of this research study can be used as a reference point or manual in the decision-making processes when creating or designing such teams.

Keywords: *ICS, cybersecurity, cross-functional team, IT/OT convergence, OT, IT.*

Annotatsioon

Lõputöö on kirjutatud inglise keeles ja on 88 lehekülge pikk, sisaldades 5-te pealkirja, 6-te kirjeldavat pilti ja 7-t tabelit.

Viimase 15 aasta jooksul on tänu digitaalsetele muudatustele, tööstuslike juhtimissüsteemide keskondades toimunud paradigma muutus, kus käidutehnoloogia eest ja IT-süsteemide eest vastutavad inimesed on pidanud hakkama koos töötama, et veenduda küberturvalisuse tasemes käidutehnoloogiate (OT) puhul. Samal ajal on faktiks see, et me näeme märkmisväärset defitsiiti kvaliteetse tööjõu jaoks sellel turul, kes oskaks sellist tööd teha. See lõputöö puudutab parimate praktikate puudumist, teemal, kuidas luua tööstulike juhtimissüsteemide kaitseks multidistsiplinaarseid küberturvalisuse eest vastutavaid tiime. See uurimustöö kasutab kirjeldava uurimise metoodikaid, nimelt kvalitatiivküsitlust, andmete kogumise meetodina. Kvalitatiitvne andmeanalüüs viidi läbi, kasutades MaxQDA tarkvara koos märksõnade kodeerimisega. Kvalitatiivne küsitlus viidi läbi 7 erialaeksperdiga, kellel oli olemas varasem kogemus läbi nende seotusega, kas juhina või tiimiliikmena, erinevates tööstussüsteemidega seotud multidistsiplinaarsetes küberturvalisuse tiimides. Andmete abil annab autor edasi intervjueeritud ekspertide perspektiivid järgnevatel teemadel : tiimiliikmete ja juhtide valimine; töötajate üleminekuprotsess eelnevate tööülesannete juurest selleni, et töödata multidisplinaarses tööstussüsteemidega seotud küberturvalisuse tiimis; raporteerimisstruktuur; vastutus riskdie eest; peamised tegevused ja projektid; haridus ja õppimine; kommunikatsioon; suhted tootjatega. Uurimustöö arutleb teemadel, nagu parimad ja halvimad praktikad, võrreldes neid kogutud informatsiooniga ja olemasoleva kirjandusega (akadeemilised artiklid, raportid, valdkonna spetsialistide või asutuste soovitused ja standardid). Uurimustöö sisaldab ka kirjeldust tüüpilistest protsessidest, mis on seotud tööstusautomaatika ja juhtimisseadmetega, mida peaksid järgima eelpoolnimetatud multidisplinaarsed tiimid, IT valitsemise struktuurist (governance), vajalikest kompetentsidest, kommunikatsiooni manageerimine, motivatsioon ja teised pehmemad tahud. Lõputöö tulemusi saab kasutada võrdluspunkti(de)na / võrdlusmaterjalina sel teemal seonduvates otsustusprotsessides.

Märksõnad: *tehnojuhtimissüsteem, küberturvalisus, multidistsiplinaarne tiim, IT ja käidutehnoloogia vaheline koostöö/sulandus*

Acknowledgements

Taking this MSc Cyber Security degree has been my golden ticket in life. It provided me with an opportunity to transition from humanities to the engineering field and discover exciting disciplines and subjects. Nowadays, I do the work that I once have not dreamt of performing and live the life I have never dreamt living. Thanks to it, I can follow my aspirations and pay forward by helping other people in their endeavours. I am grateful to this program for accumulating brilliant minds that I can call my true friends who taught me curiosity, persistence, empathy and kindness. Therefore, I would like to take a chance to thank everyone who has been a part of my story since early 2017.

First and foremost, I thank my supervisor Dr Hayretdin Bahşi for the unconditional support, guidance and faith that has been there even with the most unrealistic ideas and most challenging times. It gave me the fuel and confidence to move forward, and I will always try to do my best to support others the same way as he supported me. Moreover, I would like to thank him for lecturing the Fundamentals of Cybersecurity course in the first semester of the degree that helped me to get my first job as an IT Security Analyst at MyJar in November 2017.

Thank you, Mariia Tsokol, for helping me prepare for the exercise of the admission process and get familiar with the field before the studies began.

Thank you, Dr Olaf Maennel, for believing in me and giving a chance to get into this program, for the support and feedback in extracurricular activities, and for showing broader perspectives in the cybersecurity field.

Thank you, Dr Agnes Kasper, for believing in me throughout my path, and challenging me in Cyber 9/11 in Geneve in 2019.

Thank you, Dr Raimundas Matulevicius, for helping me get one of two spots for an exchange program to KTH Royal University of Technology and move to Stockholm, Sweden.

I would like to thank Saber Yari, Maarja Heinsoo, Alberto Zorrilla, Kristine Hovhannisyan, Jorge Medina, Matis Palm, Olesia Yaremenko, Roman Müller, Heleri Aitsam, Kris Price, Alvaro Schuller, Tedel Baca, Kayla Cannon, Brady Maxwell, Jessica

Truong, Thilina Jayanath, Shaymaa Mamdouh, Krishna Vaishnav, Rohin Kumar for teaching me everything I know. You are the role models I will always look up to, and your contribution to my story cannot be underestimated. But most importantly, thank you all for letting me experience being in the closest possible friendship that genuinely was our family.

I would like to thank my employer Orange Cyberdefense Sweden, specifically Marie Engström, Milan Brodsky and Ove Tjörnhed, who supported me on my way to concluding my commitments with kinds words, professional advice and opportunities.

I also thank all experts that have taken part in the research interviews for the dedicated time, shared experience, knowledge and wisdom.

Finally, I would like to thank Alexander Kutovoy for being my brightest light and giving invaluable support during those years, and my family for having my back and cheering me up. I could not wish for more.

This master thesis is devoted to my grandparents, Ludmila and Vadim Belokur, for playing a massive role in my life and pushing me towards accomplishing this work.

List of abbreviations and terms

OT	*Operational Technology*
IT	*Information Technology*
ICS	*Industrial Control System*
SCADA	*Supervisory Control and Data Acquisition system*
PLC	*Programmable Logical Computer*
SOC	*Security Operations Centre*
ICCFT	*ICS cybersecurity cross-functional team*
NIST	*National Institute of Standards and Technology*
DCS	*Distributed Control System*

Contents

List of figures

List of tables

1 Introduction

Motivation

Operational Technology (OT) is a term for technologies and equipment in industrial environments (ICS, SCADA, else) in such industries as manufacturing, utilities, oil, gas, energy, and other. It is usually used to highlight the contrast with Information Technology. Industries' development stimulated the business needs for optimization and more productivity of the environments. Nowadays, the new generation of these changes is commonly known as a part of Industry 4.0 [1]. Cybersecurity came into play in the context of Industry 4.0 for several reasons. Firstly, with the growth of more extensive networks of equipment, there were too many devices on the network to manage each of them individually, secondly, due to the digitalization of vendors' solutions, automation of processes and remote control. Lastly, the Aurora test in 2007 [2] and Stuxnet in 2010 [3] had drawn a historical line between the times when cybersecurity was just an option, and when the possibility of cyber threats on industrial environments became internationally recognized. The OT environments require protection and detection, response and recovery plans, and similar security technologies that are available for securing IT infrastructure.

Consequently, the need for personnel that manage the ICS cybersecurity has grown dramatically. However, the talent market did not adapt that quickly [4]. Even now, there is an extreme shortage of experts specializing in both IT and electrical engineering and automation [5] – in an ICS cybersecurity competency. At the same time, the general awareness of cybersecurity is extremely low among engineers, solution architects, site managers, technicians and operators that work with industrial control systems. Hence, there is an underestimated challenge to bridge two historically distinct areas that are merging for the past decade. The solution for the companies was educating internal staff and trusting them to perform those drastic changes in the environments, being accompanied by vendor consultants. Later, the best practice of forming OT/IT cross-functional teams occurred. Nevertheless, even nowadays it is still a rare practice because

too complicated to form and maintain a cross-functional team due to lack of personnel, reorganization, new roles, processes, and high costs for the changes and best practices how to do it.

Research question

This master thesis looks at the problem of creation and best practices of ICS cybersecurity cross-functional teams' (hereinafter – ICCFT). There is not enough information available and minimal research done about them from both ICS cybersecurity side and management/organizational disciplines. The existing information mainly points to the problems but does not elaborate on how to overcome them. It is the research gap that this research addresses. Hence, the research question of this thesis is:

"What are the best practices in establishing ICS cybersecurity cross-functional teams?"

Objectives and outcomes

The goal of this thesis is to discover and accumulate best and worst practices that circulate within the industry on how to create ICS cross-functional teams based on the data collected from industry experts and literature, reports, recommendations, and standards. The study also aims to contribute to the academic literature by establishing more research landscape on ICS cross-functional team to enable researchers and practitioners to grow the topic further because, after several months of literature review, the have been very few relevant articles found. Another objective for this study is to serve as a reference point for companies in decision-making.

Scope

The scope of this research covers establishing ICCFTs in companies of any size in such industries as manufacturing, petro(chemical), and power (distribution, transmission, but not generation). However, the results may apply to industries beyond this list. The thesis mainly concentrates on cybersecurity-related activities and governance practices, but also covers soft skills, communication, and relations aspects. The language of this study aims to be understood by representatives of electrical and automation engineering, organizational management, and cybersecurity fields. The study does not dive deeply in improving any specific process within the company but discovers the best and worst practices in general.

Introduction to other sections

Chapter 2 establishes the landscape of literature available on ICS cybersecurity cross-functional teams. There are industry standards and recommendations, reports by companies on ICS cybersecurity market, scientific articles that cover ICS cybersecurity cross-functional teams and success factors of cross-functional teams. The articles from that chapter are used for creating the research methods in Chapter 3. Further, the articles are compared with the findings in the Discussions chapter 5.

Chapter 3 focuses on developing the appropriate methods for studying best practices, guides through the creation of interview questions, describes the process of experts' selection and introduces their profiles, and talks about the data collection and analysis process.

Chapter 4 presents the findings. The data from seven interviews is coded in MaxQDA software and sorted by the most common topics in experts' discussions.

Chapter 5 is dedicated to the discussions of the findings, compares them to the literature in background information and beyond, adding interesting findings.

2 Background information

This section establishes a baseline for answering the research questions. The author does the literature review of industry standards and regulations that mention cross-functional or alternative teams for cybersecurity tasks, the reports done by companies that gather statistics, and academic articles that cover cross-functional teams. Additionally, the author reviews the articles from the management field on cross-functional teams and the factors of their success and effectiveness to include the soft side perspective. These help to develop the interview questions for the experts. The chapter summarizes the findings and identifies further steps.

2.1 Industry security standards review

To investigate how does the industry requires or recommends forming cross-functional teams, it is reasonable to start with international industry standards and recommendations as these are the documents that establish an international baseline. To select standards, the author turns to the most common ones. In 2019 SANS report on industrial cybersecurity, table 8 addresses a question of what are the top 10 regulations, standards, best practices used.

Rank	Regulation	Response
1	NIST CSF (Cyber Security Framework)	38.1%
2	ISO 27000 series	32.0%
3	NIST 800-53	31.4%
4	NIST 800-82	30.9%
5	ISA/IEC 62443	30.4%
6	CIS Critical Security Controls	29.9%
7	NERC CIP	23.7%
8	GDPR	15.5%
9	C2M2 (Cybersecurity Capability Maturity Model)	10.3%
10	NIS Directive (EU)	8.3%

Table 1: Ranking of the most common regulations implemented [6]

Since these turned out to be the most commonly used ones, the review below presents the regulations that mention ICS cybersecurity cross-functional teams or similar. To find relevant information, the search for the keywords has been done throughout all of those documents: cross-functional, cross, functional, team, teams, personnel, staff, employees.

NIST 800-82 [7]

There is an article *4.2 Build and Train a Cross-Functional Team.*

Team members listed:
a member of the organization's IT staff; a control engineer; a control system operator; network and system security expert; security subject matter experts; a member of the enterprise risk management staff; a member of the physical security department; a safety expert; a control system vendor or system integrator.

Security expertise required*:*
network architecture and design; security processes and practices; secure infrastructure design and operation; "Contemporary thinking that both safety and security are emergent properties of connected systems with digital control".

Organizational structure – reporting:

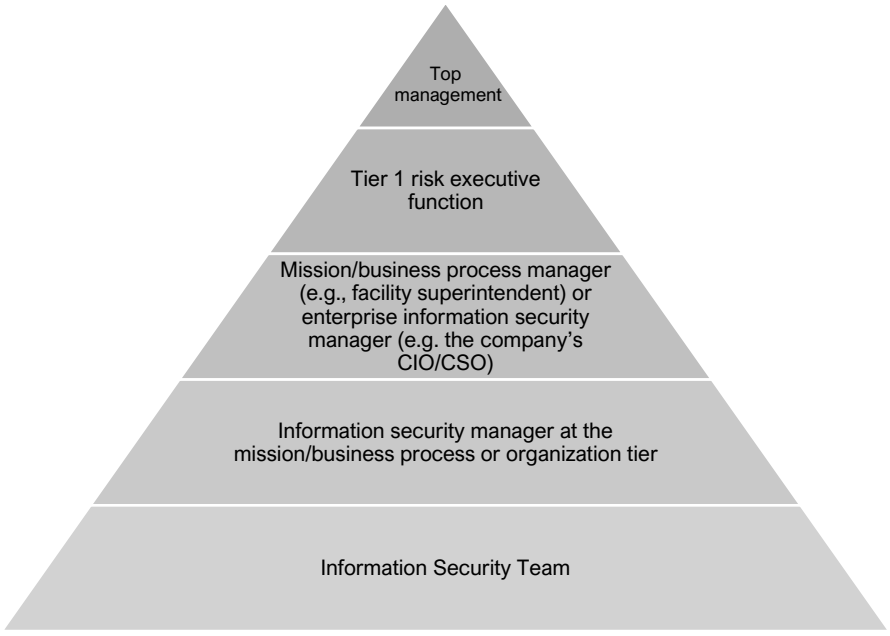

Figure 1: Reporting structure proposed in NIST 800-82 [4]

Other general principles:

- The experience of IT employees in cybersecurity field is essential and widely applicable in the OT environment, even though the central role is still on the engineers. It is crucial to establish an integration between the cultures of those

two groups of staff to achieve "*a collaborative security design and operation*" [7].

- Vendors should be involved in ICS cybersecurity decision-making process to ensure "*continuity and completeness"* [7].
- Layering security measures, so-called "defence-in-depth" should be in the core of an effective ICS cybersecurity program.
- A deep convergence and collaboration are required between the cybersecurity specialists and control system operators and engineers in order to properly install, maintain and operate security solutions in the ICS environments. Commercial off the shelf solutions are not always a proper fit. Therefore, it should be carefully discussed, and suitable security vendors should be consulted.
- Knowledge of varied domains and experience sharing are vital for the successful risk assessment, mitigation, and overall functioning of the cross-functional team.

NIST 800-53 [8]

Suggests having different teams for different functions: assessment, analysis, red or penetration testing team, threat hunting, incident response, else.

ISA/IEC 62443 [9]

The IEC 62443-2-1-2011, section A.3.2.2.2 "*Developing the CSMS scope*" talks about the cross-functional teams. The team should consist of varied competencies that are rarely found in one employee. Depending on the activity and task, different roles can be leading in a process, and that may change over time. However, it is crucial for a leader to possess needed competencies and personal skills to unite two culturally different teams to more towards a mutual goal. The roles may include: "*IACS person(s) who may be implementing and supporting the IACS devices; Operations person(s) responsible for making the product and meeting customer orders; Process safety management person(s) whose job it is to ensure that no HSE incidents occur; IT person(s) who may be responsible for network design and operation, support of desktops and servers, and the like; Security person(s) associated with physical and IT security at the site; Additional resources who may be in the legal, human resources and customer support or order fulfillment roles*" [9].

Additional information

- There should be a designated role that holds responsibility for an ICS cybersecurity in the company and being the head of the cross-functional team. The team should be the owner of relevant assets, industrial operations, and security resources.
- The ICS cybersecurity cross-functional team should receive training on incident response.
- The company should encourage assistance, communication, closer activities, knowledge and experience sharing between different business units for the sake of increased cybersecurity, holistic capabilities in response, investigation and incident evaluation".

Swedish Civil Contingencies Agency [10]
"Guide to Increased Security in Industrial Information and Control Systems", section 2 "Clarify roles and responsibilities for security in industrial information and control systems."

The guide says that due to the shortage of designated ICS cybersecurity roles and internal competency, the other point of reference is usually the vendor's consultants. Otherwise, the administration of the IT systems within the OT environment lies in the hands of process engineers that do not possess relevant cybersecurity knowledge. That, in turn, leads to an internal unawareness of certain security aspects of IT systems and lowers organizational knowledge and ability to manage the use of technologies. The solution discussed is to assign internal IT responsible for the cybersecurity aspects of IT systems within OT.

The guide provides a reference to the industry standards' chapters where these points are described in better detail. Even though those do not refer exactly to the cross-functional teams, they address the relevant points.

- NERC CIP (003-4)
- NIST 800-82 (Chapter 4.2, 6.1, 6.2)
- CPNI (GPG 4, GPG 7)
- DOE 21 Steps (No. 12, 16, 20)

- OLF (No. 1, 3)
- 27002 (Chapter 6, 8)
- IAEA (Chapter 4, 5.1)

The following regulations do not contain any information about cross-functional teams:

- CIS Critical Security Controls
- GDPR
- C2M2 (Cybersecurity Capability Maturity Model)
- NIS Directive (EU)
- NIST CSF (Cyber Security Framework)

Conclusion

There is a limited number of standards, regulations and recommendations that describe the work of cross-functional teams. The information in those available is short and basic. The reason is that kind of documents should be generalized and applicable to the whole industry because the organizations are very different.

2.2 Reports review

Reports done by such companies and institutions in the industry as SANS Institute, Kaspersky, and Ponemon Institute cover the current situation internationally and highlight the solutions and challenges that companies face.

The challenges

Kaspersky [4] says that 80% of their respondents see the interconnectedness of IT and OT challenging, 37% of those respondents say that it is due to the "*different pace of technology adoption*", and 18% said because of the "*lack of communication between two departments*". On the other hand, the barriers to a successful convergence of cybersecurity, functional safety and data privacy listed by Ponemon Institute [11] consist of 56% putting it on "*inability to overcome turf and silo issues*", 47% say that the barrier is an "*inability to control security, safety and privacy initiatives*", and in this ranking, the "*lack of in-house expertise*" was selected only by 40% and it is situated on the 4th place. Ponemon Institute also provides information on perceptions of how to achieve convergence. Respondents replied that "*convergence is not possible without the support*

of the Chief Information Officer" (73%), "*convergence is not possible without strict safeguards to protect the sharing and use of data that is critical to operations*" (65%), and "*convergence is not possible without the support of C-level executives*" (62%). The factors that prevent companies from achieving a robust convergence process are "*lack of skilled or expert personnel*" (50%), "*insufficient assessment of risks*" (50%), "*insufficient visibility of people and business processes*" (46%).

The current situation at the companies

SANS [6] shows that almost half of the respondents in 2019 did not have an OT/IT convergence strategy. At the same time, Ponemon Institute says that the majority (50%) of companies are not allocating a budget for convergence between IT and OT. Kaspersky states that in 29% of respondents, the dedicated OT/ICS security team is involved in approval on a dedicated OT/ICS security budget. It means that today, only a tiny share of companies has financial resources for ICS cybersecurity, and even if they do, the decision-makers in the budget planning are not always the group with the recommended combination of expertise. These statistics highlight that judging by the attitude towards budgets in companies, cross-functional teams are not always identified as a prioritized organizational change and practice. Hence, it also confirms the lack of specialists with experience in forming and operating cross-functional teams. Kaspersky writes that for ICS cybersecurity activities companies are forming internal teams with roles from different departments. However, "*due to the lack of in-house experts, this work is often carried out with external system integrators or service providers"* [4], although recommended by IEC 62443. Ponemon Institute provides the ratio of external and internal resources involved in these activities based on their respondents: the majority (46%) combines in-house and outsourced talents, 34% has only the in-house employees to manage the convergence, and 20% use only the services of outsourced providers. SANS asked their responders about the assessment team composition (see *Figure 2*), where the leading positions over the past 3, 4-6, and 7-12 months were shared between "external consulting firm/service provider" (11.8%, 12.9%, 11.8%, respectively), "internal IT" (13.5%, 8.4%, 9.0%), and "internal IT/OT hybrid role" (7.3%, 10.7%, 7.3%). The assessment was done by the internal OT only in (10.1%, 6.2%, 8.4%) of cases over the year.

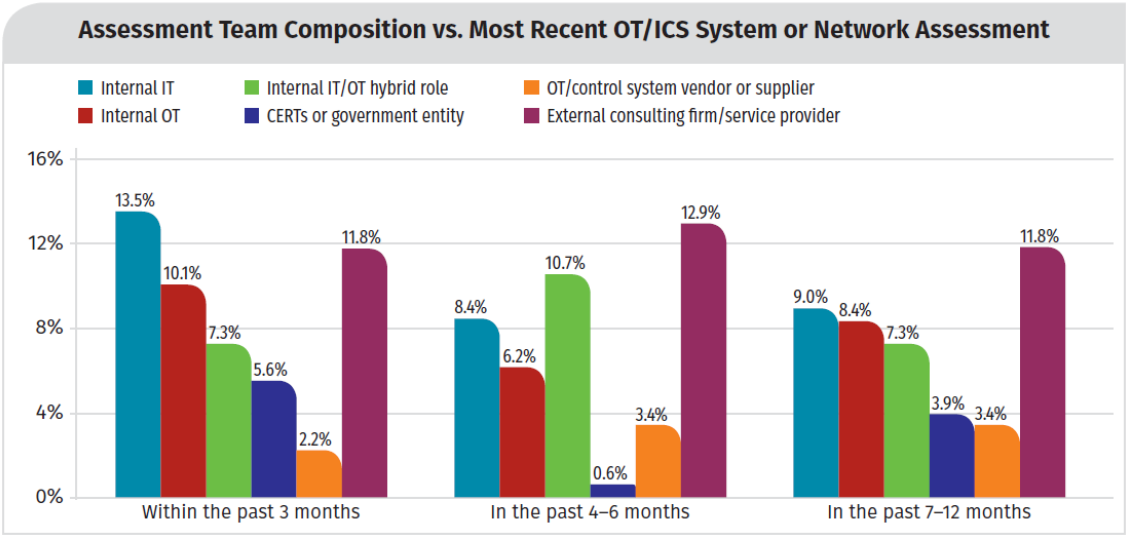

Figure 2: Assessment Team Composition for Assessments within Past 12 Months [6]

2.3 Academic articles review

The search for academic articles had two goals: to find the articles on ICS cybersecurity cross-functional teams with the focus on cybersecurity practices and teams' formation and challenges and to find articles on how to form cross-functional teams. Firstly, the author has done a keyword search for such terms as cross-functional teams, interdisciplinary teams, ICS, OT/IT, convergence, cybersecurity. Out of the found articles, the articles that cover the formation of ICCF teams were selected – article #1 and #2. In general, there is a minimal number of research explicitly devoted to ICS cybersecurity cross-functional teams and IT/OT convergence teams. The available articles mainly mention it as a side topic, not as a central one. Therefore, those were not included here. Secondly, the author has found an article on success factors for cross-functional teams that summarizes several dozens of other scientific articles on success factors. Using that article allows covering wider scope of scientific articles.

Article #1 - The future of information security incident management training: A case study of electrical power companies [5]

The authors conducted 2.5 years of fieldwork at Norwegian electric power companies in order to produce an article on cybersecurity challenges for improving practices in information security incident management. In section 5.1, they discuss "Creating cross-functional teams", mainly addressing teams for incident response purposes.

Firstly, the article says that each member of a cross-functional team has his/her goals that depend on the competency and the field they come from. Hence, the conflict of interests is inevitable. However, to make team members collaborate, they should have common superordinate goals.
Secondly, they say that some researchers previously have highlighted the mistrust between OT and IT. The authors, however, have not noticed mistrust in their study but found that both OT and IT representatives "*admitted the need for exchanging information and learning from each other to become better at both detecting and responding to incidents"* [5].
Thirdly, the authors say that it is important to consider including vendors and suppliers in the information security training, discussions, and decision-making processes. Currently, it is a rare practice in the industry, but also it is challenging to include outsourcing into the exercise.
Fourthly, the shared mental model and learning who knows what is one of the most crucial aspects of training. It is crucial to get the right people for the cross-functional team training that will provide a possibility for growing a shared understanding and knowledge.
Lastly, one of the difficulties in training a cross-functional team for incident response is not knowing who will be available if something happens. Hence, the exercise scenarios should count in different sets of people being trained for that in order to create interchangeable team members from each competence area.

Article #2 - Identification and application of security measures for petrochemical industrial control systems [12]

The paper presents discoveries of more than a hundred conducted cybersecurity assessments that were based on NIST 800-53 publication. Authors provide a systematic process checklist for the ICS organization to maintain an effective cybersecurity program.
The authors talk about cross-functional teams mainly in the context of risk assessment.
The article describes various cross-functional team practices, such as sharing domain knowledge and experience to evaluate and mitigate the risks of the ICS environment.
The article lists the same prospective team members, as the NIST 800-82. The responsibility for the cybersecurity of the operational technology of the site should be on CIO/CSO, and the team should report to that person. Lastly, the article mentions that a

multidisciplinary team should be created that consists of *"computer science, operations, security, and risk assessment"* [12] competencies in order to conduct risk assessments, identification of vulnerabilities, credible exploitation scenarios, and use a "*structured brainstorming approach*" [12] for that.

Article #3 - Critical success factors for cross-functional teamwork in new product development [13]

The topic of cross-functional team effectiveness is a well-established area, has a long history and much high-quality research performed already starting from studies on group work in the 1960s [14]. The central article in this part of the literature review is a highly cited one in the field – "Critical success factors for cross-functional teamwork in new product development" [13]. Being driven by the need of "*the evidence-based guidance*", the authors review dozens of studies related to the effectiveness of cross-functional teams. Then, the key findings of each of them are divided into six categories based on a heuristic team effectiveness model (see *Figure 3*)*: "task design, group composition, organizational context, internal processes, external processes and group psychosocial traits*" (see *Table 2*). Further, a diagnostic model of success factors is created based on the findings (see *Figure 4*). Its purpose is to be a reference point in forming, managing, and facilitating cross-functional teams.

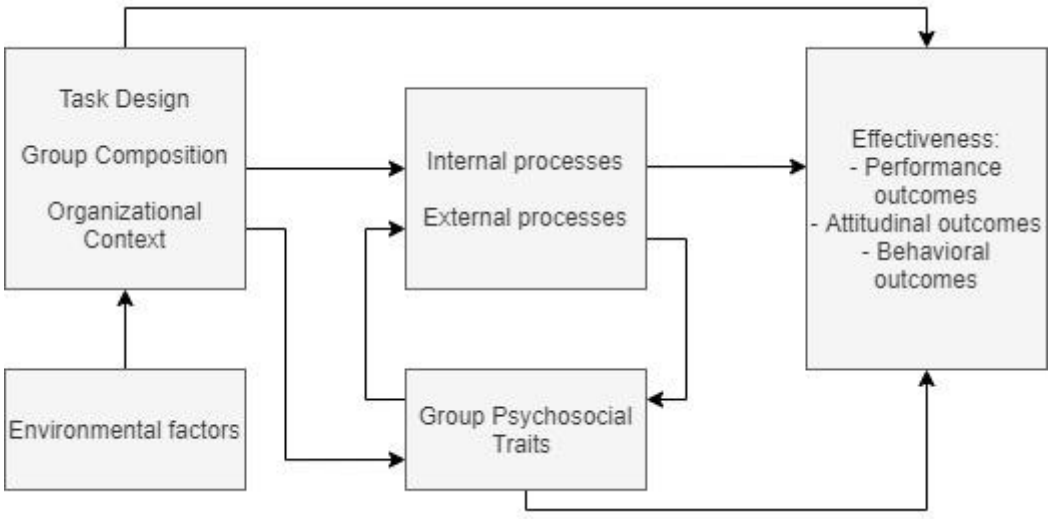

Figure 3: A Heuristic Model of Group Effectiveness [14]

Task design	Group composition	Organizational context	Internal processes	External processes	Group psychosocial traits
Team empowerment	Right functional mix	Clear mission from senior management	Overarching team goals	Boundary management	Mutual respect/trust
Formal yet flexible integrative processes	Team leader selection	Strategic alignment between functions	Team leader skills and vision		Flexibility and openness to learning/willingness to change
Customer focus	Clear roles and responsibilities	Senior managers as champions	Frequent, genuine communication		Team cohesiveness
Important, challenging task	Team tenure	Climate supportive of teams	Creative problem-solving		
		Project leader power	Sharing and use of uncertain information		
		Resources/time	Constructive conflict		
		Training in team process skills			
		Team-based accountability			
		Team-based rewards and recognition			
		Team co-location			
		Mechanisms to co-ordinate activities and share learning between teams			

Table 2: Critical success factors for cross-functional teamwork [13]

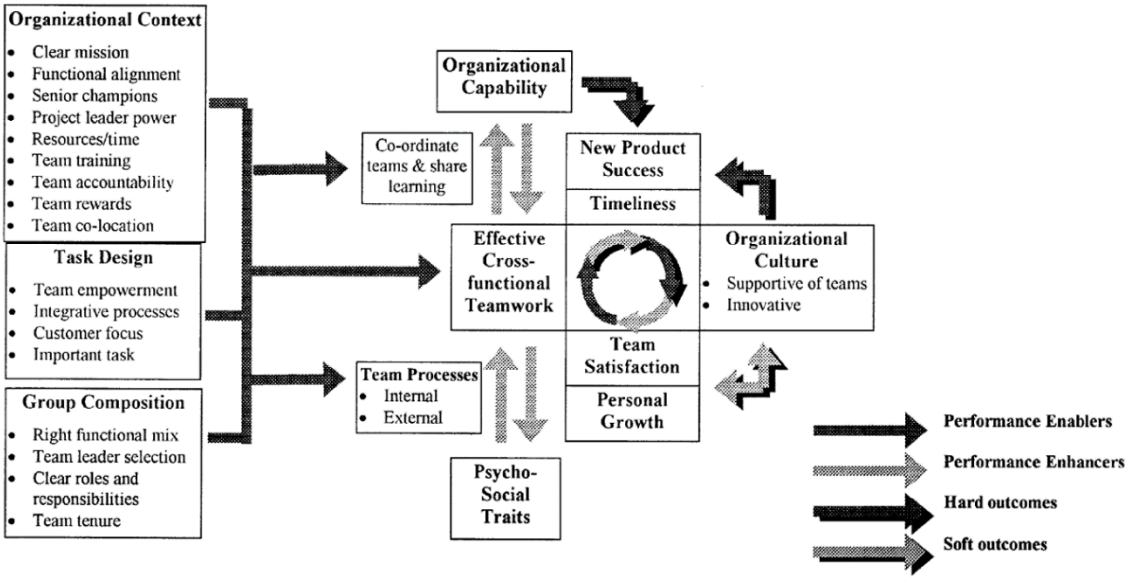

Figure 4: Integrated model of cross-functional teamwork [13]

Due to a substantial work that the authors of the article have done in the main part of the study and its academic recognition, it provides a generalized understanding of success factors for cross-functional teams, and their results can be extrapolated to cross-functional teams in any domain. However, due to the previously discussed purpose differences between product and ICS cybersecurity cross-functional teams, the model in *Figure 4* might not be directly applicable, even though the points provided in *Table 2* are universal and are the same for any team, including ICS cybersecurity-focused. Therefore, a more detailed study on specific success factors for ICCFTs is needed to see the differences and include nuances in the model.

Critical success factors for cross-functional teamwork

This section reviews the twenty-nine categories of cross-functional team effectiveness from *Table 2*. They are described in *Table 3* below.

1. Team empowerment — 'autonomy', 'authority' or 'power' 'the capability to make a difference in the attainment of the individual, team and organizational goals'.
2. Formal yet flexible integrative process — the presence of the processes that require careful planning, and those with experimental approaches, frequent iterations and testing.
3. Customer focus — meeting business needs.
4. Important, challenging task — ensuring that team members know they have tasks important to the company's mission and their department, that the tasks matter to their career. Meaningful and ambitious tasks correlate with a team's effectiveness.

5. Right functional mix — since there is a tendency for cross-functional teams to become too big, [15] and [16] recommend keeping the team size of six or seven people.
6. Team leader selection — a selected leader is preferable over an appointed one, as well as “afunctional” managers outside traditional functional hierarchy within the company are a probable solution to the leadership problems [17].
7. Clear roles and responsibilities — formalization of roles eliminate confusion and support productive relations. However, flexibility in the job description and novel routines are attributes of more effective cross-functional team performance. Managers should be dedicated to one project, not several; be there from the beginning to the end, not phase-based; should be loyal to the team and the project, not the function.
8. Team tenure — performance of the teams declines after five years due to the declined documentation within the group. Older
9. Clear mission from senior management — senior managers should have conscious aims to develop a better culture, to utilize the potential of each team member, clearly communicate aspirational goals with the team, and develop a strategy map that will allow team members to identify themselves with it.
10. Strategic alignment between functions — before forming cross-functional teams, the cross-functional team strategy should be developed in order to prevent team members isolating themselves within the group.
11. Senior managers as champions — should play a key role in motivating co-workers, maintaining their commitment, review, approve, and allocate resources, and alter mindsets of middle managers.
12. Climate supportive of teams — the organization should be supportive of teamwork, and managers should contribute to the development of this culture.
13. Project leader power — should utilize their executive power in order to protect teams from external interference and lobby for their interests.
14. Resources/time — it is proven successful to have flexible budgets in order to meet the cross-functional teams’ objectives. To empower teams and ensure their effectiveness, enough resources should be dedicated.
15. Training in team process skills — training should be provided both to the team members and managers to encourage learning, prepare them to the tasks and show who knows what.
16. Team-based accountability — accountability is a measure balance the empowerment to prevent too cosy relational norms as it harms performance. Teams should be demanding to each other.
17. Team-based rewards and recognition — have the well-balanced congruence between task and reward to prevent competition and increase motivation. The rewards should not necessarily be financial as it might be perceived as unequal treatment.
18. Team co-location — co-locating teams is crucial in their performance as it increases productive communication.
19. Mechanisms to coordinate activities and share learning between teams — have the same individual on several teams and coordination with other teams is a critical success factor.
20. Overarching team goals — having consistent goals allows teams to perform better. It is up to management to define ambitious goals.

21. Team leader skills and vision — should be a mediator between all parties within the organization and communicate a complex vision of the team.
22. Frequent, genuine communication — intense communication and one of the conditions for high awareness and effectiveness.
23. Creative, integrative problem-solving — decisions should be made with a team diversity of the team members in mind, and the output of their decisions should add a new dimension to the organization's innovations.
24. Sharing and use of uncertain information — team members should be able to articulate uncertain information with others, be ready to explain or act. It improves cooperation, trust and work results.
25. Constructive conflict — be productive in task-related conflicts and try to eliminate personal conflicts.
26. Boundary management — management of relations with external parties.
27. Mutual respect/trust — trust correlate with effective teamwork; it also creates an atmosphere of inclusion that is crucial for information sharing.
28. Flexibility and openness to learning/willingness to change — effective cross-functional team members are to adopt new attitudes, mindsets and behaviours.
29. Team cohesiveness — is an outcome of co-location and internal communication. Teams should avoid 'groupthink – over-optimism and risk-taking while the opponent is viewed as evil, weak, and stupid.

Table 3: Description of the points from the Table 2 [13]

3 Methods

3.1 Research method

The research methodology for this thesis was mainly selected with the help of the book "Research Methods for Cyber Security" [18]. Based on the research question formulated in the problem statement, this master thesis is a descriptive study [18]. Descriptive studies are a type of qualitative research that focuses more on an in-depth target subject and specific cases [18]. The literature review indicated that there is minimal information in articles, standards, recommendations, and reports. Hence, most likely, such knowledge is transferred by professionals within the industry. Since the "data holders" from the perspective of this research are the industry experts, a central priority of this descriptive study is to discover their experience. Therefore, elicitation is a suitable descriptive study method that involves data gathering from people, collecting *"the wisdom of a specific population*" [18]. However, to identify which data collection type is the right fit (e.g. interviews, questionnaires, surveys, and other), it is essential to investigate the needs of the research questions and consider the data analysis methods to prepare the dataset.

The research question of how to establish cross-functional teams requires gathering practices of experts as broadly as possible. Their views may vary significantly. Therefore, the research method should allow enough space to cover the whole picture. Hence, to prepare the needed data set, the semi-structured interview is selected as a data collection method, and the qualitative data analysis method is the selected one for the research question. Quantitative methods will not satisfy the need since surveys or questionnaires would limit the spectrum of answers, and quantitative data analysis will limit the format of answers within the analysis only to quantifiable. However, to identify the patterns, the data analysis should contain keyword mapping methodology and shed some light on how many respondents provide such answer and why. Therefore, data analysis utilizes keyword mapping as a methodology.

The open-ended questions in semi-structured interviews were selected as an elicitation research methodology. Semi-structured interviews allow the interviewer to keep track on the direction of respondents' answers and make sure that their focus is directed to fulfil the needs of the research, either digging in more detail in some topic or covering a newly-mentioned best practice.

3.2 Creating questions for the interview

Even though semi-structured interviews are selected as a qualitative research method for this elicitation study, it has some considerations before creating the interview questions. According to [18], the interview questions should be clear and short. Complex questions should be avoided in verbal interviews, and detailed answers cannot be expected to be delivered in written interviews. At the same time, the interview should not take too long, as the interviewee will get tired and lose focus. The recommended duration of the interview is from 30 min up to 2 hours [18]. Since the research question requires many aspects being covered, it is crucial to let the interviewees have enough space to express their opinions. Hence, verbal semi-structured interviews were selected over the written ones (via email or Google Forms). Since the experts are in different countries, semi-structured interviews were performed via Microsoft Teams. To have short and clear questions for the virtual interview, the author has created 13 questions to collect data. In short, the creation of questions can be described in *Figure 5*.

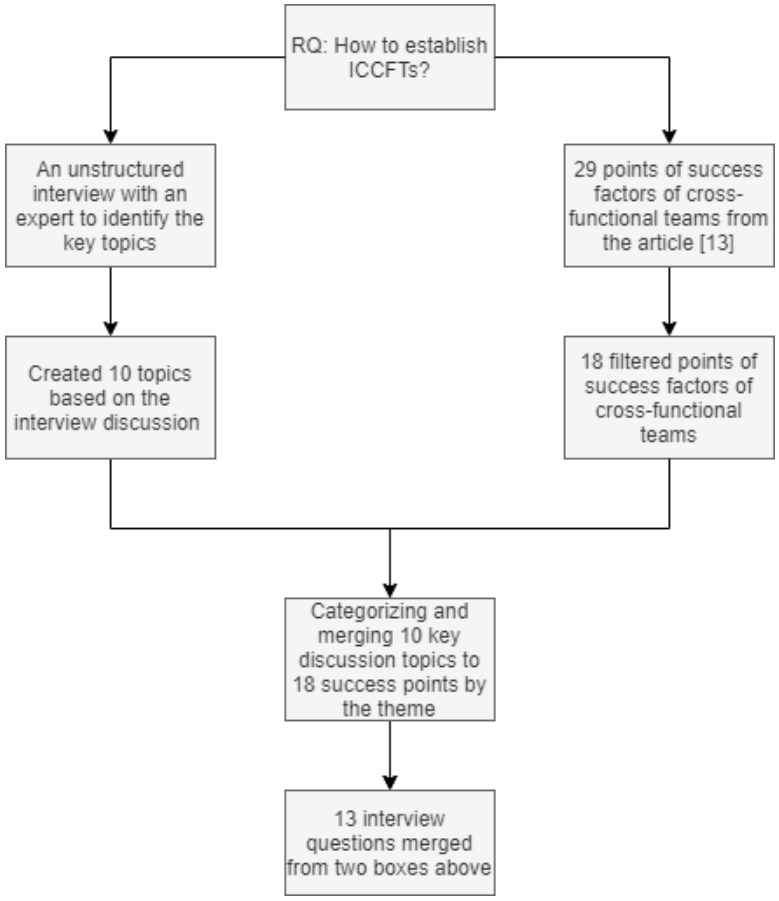

Figure 5: The process of interview questions' creation.

The process was the following. Firstly, to identify the primary topics in the interview, the author conducted an unstructured interview with the expert PhaManLa1 (name coding is in *3.5 Data collection – Profiles of experts*) discussing how to create ICS cybersecurity cross-functional teams in general. Based on the discussion points, the author was able to identify ten key discussion topics that should lie in the base of the interview questions.

The second step in questions creation was working with 29 categories of success factors from the article [13]. A big part of those points were universal factors that doubtlessly are critical for the success of any cross-functional team, regardless of the industry and purpose. They are 'Customer focus', 'Important, challenging task', 'Clear mission from senior management', 'Strategic alignment between functions', 'Climate supportive of teams', 'Resources/time', 'Training in team process skills', 'Team-based accountability', 'Mutual respect/trust', 'Clear roles and responsibilities', 'Team empowerment'. Therefore, they were removed from the list of points that will lie in the foundation of the interview questions. The author focused more on subjects which may provide more distinct remarks for the problem domain.

Thirdly, to limit the number of questions in the interview, ten discussion topics from the unstructured interview were compared to the 18 remaining points for success factors listed in *Table 2* above. If the themes matched, they were combined into one category and logged into *Table 4* below in one line. The discussion topics from the unstructured interview are labelled in *Table 4* as UIT (Unstructured Interview Topics). Success factors were also combined with other success factors by topics, even if no UIT matched them.

Each row in *Table 4* contains success factors' names and UITs, if applicable. Three questions from the unstructured interview did not match the categories from the success factors in *Table 2* because they are specific to the process of teams' creation. Therefore, they were logged as UITs at the end of the table

#	**Questions combines by themes**
1	Formal yet flexible integrative process + UIT
2	Right functional mix + Team tenure + UIT
3	Team leader selection + Team leader skills and vision + Project leader power + Senior managers as champions

4	Training in team process skills + UIT
5	Team co-location + Frequent, genuine communication + Team cohesiveness
6	Mechanisms to co-ordinate activities and share learning between teams + Flexibility and openness to learning/willingness to change + Training in team process skills + UIT
7	Overarching team goals + Clear mission from senior management + Important, challenging task
8	Sharing and use of uncertain information + UIT
9	Constructive conflict + Team-based rewards and recognition + Creative, integrative problem-solving + UIT
10	Boundary management + UIT
11	UIT: From your experience, who (which body/role) within the organization was the initiator of the need in cross-functional teams?
12	UIT: You are to form a cross-functional ICS cybersecurity team out of OT and IT business units' representatives. You have all team members selected. What are the next steps? (e.g. dividing the tasks / awareness trainings / process formation/ other).
13	UIT: What were the required knowledge / awareness / skills for members to possess before they started their new responsibilities within the cross-functional ICS cybersecurity team?

Table 4: Combination of topics to form the interview questions

The next step is to form questions based on the combined themes in *Table 4*. To do that, the author consulted the methodology of interview questions creation in the book [19] and the book section [20]. Firstly, considering the research questions asked, the interview questions type should be descriptive. The focus should be on "What should be done?" and "How something should be done?". It is important to have questions created neutrally, so they do not incline the interviewee to one or another answer. One fundamental principle in creating descriptive interview questions is to expand them in order to get a better answer. They "*not only give informants time to think, but it says, "Tell me as much as you can, in great detail""* [20]. In *Appendix 1*, there is a final version of the interview questions presented to the interviewees.

3.3 Interviewees selection, request for collaboration and ethical considerations

The requirements for the respondents' profiles are:

- Have been working with ICS cybersecurity in such fields as manufacturing, oil and gas, petrochemical/chemical, utilities, power, and other.
- Have experience with cross-functional teams that consisted of representatives from the IT and the OT business units, and their job involved cybersecurity projects and tasks.
- Had one of the following roles:
    - managers and/or creators of the cross-functional team.
    - team members of the cross-functional team.
    - external employee that facilitated cross-functional teams.
    - integrator or vendor representative that has been involved in forming or supplying a cross-functional team.

Since it is a very specific category of cybersecurity field representatives, there are not that many people in the world who have experience. Hence, to find such experts, the author has utilized two ways of searching for interviewees. Firstly, the author is a member of a Russian-speaking "RUSCADASEC Community" [21] group on Telegram that is dedicated to OT cybersecurity. At the moment of writing this thesis, there were more than 2200 chat members. The author made a publication stating that experts that match the aforementioned criteria are welcomed to participate in the master thesis research. In the end, several members of the group have agreed to take part in the interview session. Secondly, the author made the same publication on her page in LinkedIn, where she has many connections within the ICS cybersecurity field, and several connections expressed willingness to participate.

ICS cybersecurity is a highly confidential field, hence, for the compliance of each respondents' current and former employment contracts, the author of the thesis is not revealing their names, former and current employers' names, vendor names, and any other identifiable information. The information about the industry, roles, years of experience, and the experience itself was agreed to be discussed.

3.4 Developing a Plan for Data Analysis

The author identified that a suitable data analysis method for elicitation research design is thematic coding [18] [19]. The collected unstructured data is *"converted into categorical or taxonomic data"* [18]. In qualitative studies, data collection goes hand in hand with data analysis [19]. The more data is processed, the more the patterns reveal itself. Data interpretation consists of two processes: analytic and synthetic. During the analytic process, the data is being parsed and assigned a code.

The software MaxQDA is created for qualitative research and was used for coding. In turn, the analytic process kicks off a synthetic one — grouping the thematic codes into categories (*Figure 5*). The data is interpreted *"exploring thematic relationships in response to research question"* [19]. However, to control the objectiveness, it is essential to label all data from the very beginning in details in order to have a broad picture, unlike labelling only the data that the author subjectively finds relevant to the expected conclusions.

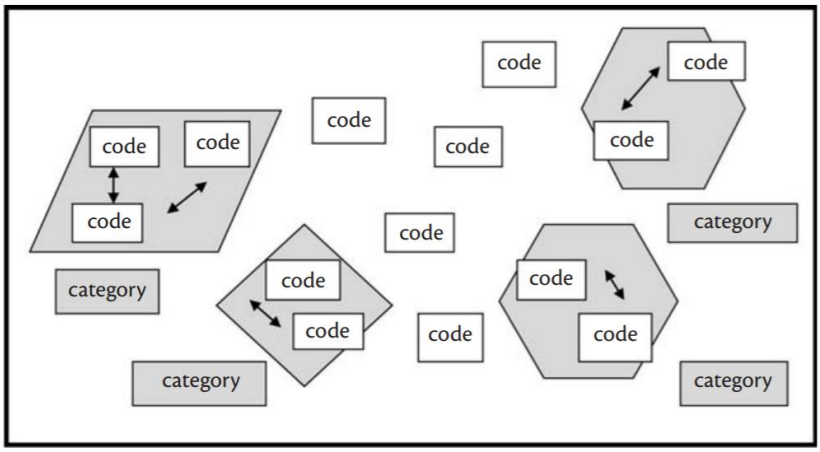

Figure 6: Thematic codes and categories [19]

3.5 Data collection

Sample size for qualitative research

It is vital to conduct enough interviews to be statistically representative. The author has consulted the research papers to identify the number of experts to be invited. The term "saturation" refers to the incoming data that no longer provides novelty in the data collection process [22]. The article [22] had a goal to identify how many new concepts

are discovered in a growing number of interviews and what is their saturation coverage. The researchers conducted "*systematic inductive thematic analysis of 60 in-depth interviews"* [23] and derived 114 new concepts based on the answers. They identified that 70% of new concepts were discovered in the first six interviews, whereas 92% (100 concepts) were discovered in the first 12. At the same time, 100 new concepts comprised 97% of the most common findings, meaning that most coverage can be done in 7-12 interviews. Same findings were confirmed by other authors that researched the saturation topic: [24] found out that 5-6 interviews provided the majority of new concepts and ten interviews provided 92% of new concepts; [25] conducted ten interviews where three did not provide any new concepts. [23]

The exact saturation can only be identified during or after data analysis. Therefore, the author initially planned to do six interviews, and in case no radically new perspectives were revealed, she will stop with the interview process and proceed to the data analysis. However, if the incoming information would bring new perspectives, the author will identify what profile of the interviewer will be the most complimentary to the dataset and will conduct more interviews. After having conducted six interviews, the author identified that there is not much diversity brought in by new responses. However, to improve the saturation provided by the sample size, the author decided to conduct one more interview. Therefore, she contacted her community in social media again to find a suitable interviewee. Finally, the author conducted one more in-depth interview to have a total of 7 interviews. Additionally, she has conducted two more follow-up interviews with the selected experts to complement the final dataset with certain topics that were not fully covered from their side during the main interviews.

Questions improvement & bias prevention

After the first interview, the author has identified several questions that were too complex to be addressed during the virtual interview. Therefore, some interview questions were rephrased to be easier understood by the interviewee. At the same time, after the first interaction, the questions were also checked for imposing any unconscious bias [18]. Also, in order to prevent interviewees answering in the manner they think the interviewer would expect them to answer, further in the interviews the author has highlighted that it is essential to be honest, constructive, logical and reminding that the interview is done in anonymity.

Profiles of experts

The table below presents the profiles of experts. The names were anonymized. Instead, each expert was given a name code to be referred to in Results and Discussions chapters. The name code consists of 3-5 first letters of their one or two industries, the size of the company, and a serial number ('Phar' – pharmaceuticals; 'Man' – manufacturing; 'Chem' – chemical; 'Petro' – petrochemical, 'Com' – communications; 'Pow' – power; 'La' – large; 'Me' – medium). The size of the organization was determined by the expert, where large enterprise usually imply international companies with several dozens of sites. Industries and the size of an enterprise were identified to be the most important information for a reader to keep in mind to get more context of experts' answers. ChemLaMe3, ManComLa5, PowManLa6, and ManMe7 have been working as consultants at vendors and integrators, meaning they worked in different other companies. There are three main industries represented: manufacturing, (petro)chemical, and power.

Expert's name code	Industry	Role	Originally OT or IT	Total years of experience	OT/ cyber security years of experience	Size of the company	Location
PharManLa1	Pharmaceuticals and Manufacturing	Team manager, team member	OT/IT	22	10	Large	Middle East
ManLa2	Manufacturing	CTO, head of cybersecurity	IT	20	10	Large	Northern Europe
ChemLaMe3	Petrochemical, chemical	Team manager, project leader, consultant	OT/IT	15	10	Large and medium	Western Europe
PetroLaMe4	Petrochemical	Team member, facilitator	IT	22	6	Large and medium	South America
ManComLa5	Industrial communications, power, industrial cybersecurity	Team lead, engineer, consultant	OT	20	8	Large	Eastern Europe / Asia
PowManLa6	Power, transmission grid, manufacturing	Team lead, team member, consultant, engineer	OT	15	12	Large	Eastern Europe / Asia
ManMe7	Manufacturing	Team member, team manager	OT/IT	24	13	Medium	Western Europe

Table 5: Profiles of experts

Interview protocol and data collection

As soon as the questions were ready, the profiles of interviewees were identified, and the announcements were made in two social networks (LinkedIn and Telegram professional group), the experts have contacted the author. She has informed them about the purpose of the interview, the anonymity conditions mentioned above, and the time it would take to conduct an interview (1.5-2 hours). The time estimate was derived from the unstructured interview conducted before. When the expert agreed for participation and suggested the suitable date and time for the interview, the author sent out the interview questions in PDF format to their email - in advance to let experts prepare if needed and be aware of the upcoming discussion.

Opening protocol of the interview session

It was planned according to the "Opening Segment of the Semi-Structured Interview" in the book [19], Figure 2-1.

1. Welcoming words and expressing gratitude for participation.
2. The research being conducted is a master thesis for MSc Cybersecurity program; the research questions; the purpose of the study.
3. How the interview will be conducted (the call recording, transcript creation, review and editing by the expert, final approval).
4. Data anonymity discussion (described above).
5. Rights of the interviewee: clarifications are provided by request; the expert may refuse to answer a question or may limit the answer to what is allowed to be discussed according to their former/current employment contracts; the interview may be conducted in two parts if we run out of time.
6. Addressing the first broad question that creates openings for experts to begin to share experience – asking about the career path, industries, roles, years of experience; cybersecurity-related experience; experience with ICS cybersecurity cross-functional teams.

Middle Segment of the Semi-Structured Interview

After the expert establishes the ground for further discussion by telling a 10-minute story of their professional experience, the author started addressing the interview questions. It is where the elicitation happens, so the interviewer aims to ensure that the topic is

appropriately explored. Apart from the main interview questions, the author asked follow-up questions that clarified the understanding or the opinion of the expert or developed the discussion further.

Concluding Segment of the Semi-Structured Interview

The author took a chance to return to points that need final comments or asked a question "To sum up, what are the success factors for ICCFTs in bullet points?" that summarizes the ideas of the expert, if they were not fully clear. Generally, the author "*worked toward a sense of wrapping up"* [19]. In the end, the interviewer expressed gratitude for their time and contribution and reminded that the transcript would be sent soon.

Data transformation

The interviews were recorded in Microsoft Teams. This method of data collection in semi-structured interviews is a preferred one over taking notes during the call because it allows the interviewer to concentrate on what the expert responds and ensure that the conversation goes to the right direction instead of taking notes in a hurry. The author has tested notes taking data collection method during the unstructured trial interview. It distracted from the conversation, not everything was noted, and it was hard to concentrate on guiding the conversation. The reason for selecting Microsoft Teams over other platforms is that it allows sharing a screen, doing the recording of the call, and downloading a transcript of the call as a text file. Thanks to that, the process of data extraction was less time-consuming.

The process of data transformation started with working with the "raw materials". In 4 cases, the interviews were done in English. In 3 other cases, the interviews were done in Russian, and it means that even though the Teams calls were recorded, the transcript was not generated in Russian. Therefore, the author had to transcribe the transcript for interviews in Russian by listening to the recording. Interviews in Russian were not translated to English because the author is a native speaker and translation takes much time. Nevertheless, individual quotes were extracted, translated to English and checked with the expert. In the case of interviews in English, the author downloaded the transcript from Microsoft Teams, listened to the interview and edited the mistakes to create a correct text. The transcript of all interviews was sent to the experts, they have reviewed it and sent the approved version to the author.

4 Results

The data from seven interviews were categorized by 653 codes, the code system extracted from MaxQDA is attached in the *Appendix 2*. Umbrella topics were created based on the research questions and interview questions. Then new codes are made on the frequency of response occurrence, or as options, dividing the respondents into two and more camps.

1. Teams

1.1 Definition of ICS cybersecurity cross-functional teams

When talking about ICS cybersecurity cross-functional teams, experts have described different formats, structures, and purposes because it highly depends on the company itself and the industry. Some of the ICCFT types are:

- Umbrella or Global Experts Group — a team of representatives from each production site that approve common security measures to have standardization across the company.
- A local team that are permanently on-site.
- A team that is responsible for everything on one or more sites (applicable to companies with unsupervised sites); it usually consists of engineers with security knowledge.
- A team of mostly IT and some OT people with knowledge of IT that are responsible for compliance.
- OT SOC team that consists of security analysts and OT engineers.
- Workgroups that combine the needed competencies to implement certain IT and IT security-related project in an ICS environment.

One or more structures from this list exist in the organisation, for example, an umbrella team with representatives of all sites, teams responsible for one or more sites, and an OT SOC. Expert ManLa2 said that having a permanent ICCF team on site is a privilege of large, mature, and strategically important sites that can afford it. Small sites sometimes run with no or minimum supervision, and for security matters, there are external parties taking care of that.

1.2 Initiation. Who should initiate the creation of ICCFTs?

There is no unity among experts' responses as they named different parties to be the initiator. ManLa2, PharManLa1, PowManLa6, ChemLaMe3 said that the initiator is the management (vice-presidents/executive directors, CISO, CTO, business, or site managers). Also, ManComLa5, PetroLaMe4, ManLa2, ManMe7 stated that it should be cybersecurity or information security team. The overlap was in one expert that was the CTO and the head of cybersecurity, meaning he covered both management and cybersecurity, and the other expert PharManLa1 argued for management and OT. PharManLa1 argued that IT could never be the initiator. It always comes from the OT side (engineers, site managers), sometimes general management that pushes all teams to collaborate more effectively and quickly. He said that it is the business that drives progress, whereas IT is a service function. PharManLa1 said, *"The business demands the OT to make processes more effective: managing 10-100 devices via the network is much more efficient instead of running around the site and manage each of them individually. […] The other misconception is to form a cross-functional team for cybersecurity only. No one allocates people to do cybersecurity alone because cybersecurity, in essence, is everything. It is a quintessence of both OT and IT".*

1.2 Transition

If the ICCF team members are not newly hired for these specific roles, and the team members are not contractors, the management can put existing employees into cross-functional teams. When it comes to the most optimal ways of how to put personnel in this transition, three experts talked about the transition highlighted that it should be gradual. ManComLa5 and PetroLaMe4 said that employees could start transitioning into a new role beginning from 20h/w (half of their work time), so they have enough time to hand over responsibilities and receive new knowledge. ChemLaMe3 said that it is more favorable to start with one day a week because for IT people, for example, OT security might look dull. "*It is a passion that one needs to develop. They still need to have enough time to work on their fun part. If IT starts gradually, they start being more comfortable. They understand more, start appreciating OT technologies more, then they can increase the amount of time they work. But I've seen quite a lot of resistance from IT guys"*. No expert said that employees' transition to full time at ICCFTs should be immediate.

However, there might be a problem in motivating the employees to change their responsibilities. ChemLaMe3 says *"The problem is that it is just something inaugurated and nobody is giving the teams on-site extra time or money to work on the new security functions. Management neither reduces the workload nor gets extra people to compensate for the absence in the former department or share the workload in a new one. Therefore, team members try to execute their role with the least effort. They don't want even to consult and talk to the global experts because they will be overwhelmed with recommendations that they don't have time to understand and execute. That is one of the reasons why security on sites is done in an ad-hoc manner instead of having a planned approach".* The recommendation for such problems of the transition period was said to be for management to incentivize employees by offering a salary raise or a bonus for starting at a new function because it requires a lot of learning efforts and management should count that in too.

1.3 Permanent/temporary teams & part-time/full-time participation

Four of seven experts think that ICCF teams should be permanent with permanent members working on projects and daily routines together. Two said that the teams should be permanent, but for certain projects and tasks, team members should be combined into smaller workgroups by required functional mix. One argues that teams should be project-based and temporary.

Three out of seven experts discussed whether selected workers should be a part of a team full-time or part-time of their employment. Two experts said that it should be full-time, but one said that in his/her experience the team members had a daily routine with ICS cybersecurity only part-time for several years. When the organization matured, some people turned to work with it full-time.

1.4 Composition of the team

1.4.1 Competencies

PhaManLa1 said that in future, the team members would be people that are educated explicitly for industrial control systems' cybersecurity, same as IT cybersecurity specialists nowadays graduate from universities and other institutions. PhaManLa1, ManComLa5, and ChemLaMe3 mentioned a significant shortage of such talents. ManComLa5 described a case at a customer when a business-critical incident was not

noticed for two or three weeks. When they started investigating, it turned out that four existing security employees did not have enough time to fulfil their responsibilities. In contrast, the company had 50 open security-related vacancies due to a "talent hunger". PhaManLa1 said, "*It is indeed a rare case when there is an existing team at the company. One of the reasons is that it is a big responsibility that requires specific qualification that is still very uncommon in the industry – for people to have a degree in either electrical, or mechanical engineering and automation, and at the same time to have experience in computer science, IT, and vice versa. These talents are in high demand. Such positions in companies can be opened for months and years, offer a competitive salary, social security, all the benefits, but still, they might not find a perfect fit".* ChemLaMe3 said that those talents barely exist. However, since there is no such kind of programs to study the field comprehensively, the competencies for the team should be collected to specifically satisfy today's needs. The named competencies are listed below. These are the competencies that should be in the cross-functional team, not necessarily possessed by each team member in depth.

- Data transmission network
- Automation and control systems
- Embedded systems and sensors
- Maintenance methods
- Ways to eliminate device and system planning errors
- IT network protocols and production protocols
- Network security and safety
- Core IT understanding
- PLC programming
- Cybersecurity governance
- ICS applications operations
- Security systems administration. To be able to configure, maintain, and service security solutions that have been implemented and operated.
- Security management competence. Prerequisite: basic cybersecurity education
    - Identification
    - Protection
    - Detection
    - Response
    - Recovery

Employees' roles that can be included in the team:

• IT – network engineer, system engineer, information security specialist (however, the last one might have hard times understanding how OT works and all nuances of it, but will be responsible for standards compliance, risk assessment, incident response plan), security analyst, network security specialist.

• OT – Electrical and Automation Engineers is the best choice because only on that level, it is possible to understand attacks, all incidents, vulnerabilities in OT. Electrical engineers understand how computer tasks are converted in the lower-level signals that are executed on OT equipment, how it works in essence. Mechanical engineers are not the right fit.

1.4.2 Functional mix

In general, all experts said that the mix should be created from OT and IT sides in approximately equal proportion. Three experts said that the functional mix should allow members to be nearly interchangeable in tasks if representatives of one group prevail. It means that all should have enough knowledge about both OT and IT areas to either take two roles or fully comprehend. Three other experts mentioned that the team (the workgroup) should change depending on the project/task' needs. However, these two team composition principles highly depend on the existing governance structure in the company.

- ***PhaManLa1***: "*Team should solely consist of OT and IT representatives with the ratio of 50/50. These are entirely two distinct areas that have very different approaches to security and technology operations. It leads to the point when they treat their work differently. […] It should be a team that acts like one brain, with almost interchangeable members*".
- ***ManComLa5***: the mix that it allows covering identification, protection, detection, response, and recovery to both corporate and industrial IT infrastructure.
- ***ChemLaMe3***: the functional mix should be created by the goals of projects or tasks, be it OT governance framework development or threat intelligence. So, the team members can differ from project to project.
- ***PowManLa6***: Instead of IT, information security specialists should be selected. Instead of operating personnel – service department. "*In my practice, there was a case when the operating personnel did not know how to work with the*

manipulator, i.e., computer mouse." The teams should not be created assuming by default that it should consist of IT and OT. People should be selected into a team based on the specific task that is to be performed.

- ***ManLa2***: on the most modern and digitalized sites, they will have their local dedicated people that are controlling everything. Some will have dual roles, working both with IT and production, others will work 100% with production. On larger sites, it can be an extensive team of people working directly with OT, where 20% of them have a focus on security within OT.
- ***ManMe7***: based on the experience, there are three types of people in ICCFTs: 1 – PLC programmers and hardcore PLC guys; 2 – operations people managing all from the hardware to the application side of the environment, 3 - the IT part.
- ***ManComLa5***: the cross-functional team should consist of two parts: those who operate and maintain systems (OT or IT and OT), and those who provide security functions and implementation of protection (OT and IT).

At the same time, in case of human resource shortage to form an ICCFT, PhaManLa1, ManComLa5, said that OT employees should be selected and educated, whereas PetroLaMe4 said that it should be cybersecurity employees selected and educated if needed to fulfil the need. The expert argued that it is easier to understand OT cybersecurity for someone that has worked with IT infrastructure, than as an operator of the equipment at a manufacturing site. In some responses above, one can also see that experts name more employees from OT side.

1.4.3 Number of team members

Summing up the experts' answers, there can be 4-6 people in a team that oversees one or more sites depending on the size of the company and the governance structure. For the umbrella teams, it depends on the size of a company, but the experts' experience shows that it is about 15-30. The exact number might not matter that much unless there are open-minded people and "translators" that can help facilitate the conversations. Here are some of the different answers from the experts:

- ***ManComLa5:*** in a corporate security center for the industrial segment (eight branches and about 40 industrial large facilities) there are five-seven people (+15

more to be hired to grow), where at least one or two people are security analysts in an umbrella SOC team that manages sites' security via remote control.

- ***PowManLa6:*** when talking about the energy sector, let us take an organization with *"300 power substations in the regions, 10 - 20 automation systems and about 20 suppliers of various equipment. An automated control system service is being created, which is responsible for automatic control systems. In such a service, there are not more than 20-30 engineers and network manager"* that work on security, and external cybersecurity contractors that provide SOC service to the umbrella team. Their representative, the head of cybersecurity, is a part of that umbrella team.
- ***PetroLaMe4***: Minimum two. Better four or five. The more team members there are, the better they will be in certain narrow specializations. If there are fewer people, they should be a master of everything, even though they can leverage the knowledge of their colleagues when needed. Most importantly, to have open-minded people with excellent soft skills. Otherwise, it does not matter if there are ten people who do not accept ideas and changes.
- ***ChemLaMe3:*** three-five people, but companies now realized that security is not just annoying compliance, but a business enabler, so they grow those teams.
- ***ManLa2:*** umbrella team is 15 members from each business unit and two facilitators. Facilitators are needed to *"be the translator between the teams - that is a successful setup. There should not be too many people that try to be the master of everything".* Six people in a workgroup per business unit on sites, plus colleagues assisting them on demand. It is not enough, but it covers the most business-critical.
- ***ManMe7***: in his/her experience, there were two people from the OT side and four or five from IT. In total, he thinks, four or five people, depending on the size of the company, is enough for ICCFT.

2. Team's activities and projects

2.1 Statistics on experts' responses

Typical projects, activities, and tasks of ICCFTs were the largest part of the discussions during the interviews. This section alone counted 144 codes out of 653 during the data analysis part. The table below represents cybersecurity-related activities and projects in

ICS environments that ICCFTs can perform. The numbers in the second column show the times the keyword occurred in all interviews. Therefore, the numbers and the order within the table do not show the weight of each keyword and should not mislead the reader: they do not reflect the importance of the activity and do not reflect each expert's contribution to the number. Nevertheless, the number shows how often each subject was a matter of conversation on cross-functional teams.

Playbooks	10
Security solutions & defence measures	10
Network administration	9
Incident response	8
SOC	8
Network monitoring & Detection	6
Enterprise software & applications	5
Compliance	5
Threat intelligence	4
Governance	4
Remote access	4
Prevention	3
Maintenance	3
Backups	3
Patching	3
SCADA management & upgrade	3
Data bases administration	2
PLC programming	2
Validation of solutions, testing	2
Recovery plans and processes	2
Risk assessments	2
Network segmentation	2
Migration projects	2
Unification and standardization	2
Network security	2
SIEM & security analytics	1
Infrastructure administration	1

Table 6: ICCFT's cybersecurity-related activities and projects in ICS environments

2.2 Experts comments on the team's activities

Some of the categories are described below, where the experts provided holistic opinions. The rest of the keywords were mention alone in the interviews, with no additional comments.

Playbooks

Firstly, not all experts were using the term “playbook” or a concept that was close to its meaning; only ManComLa5 and ChemLaMe3 did. The nearest category to this was “incident response” that is discussed below. ManComLa5 describes it in the following context:

“When a cybersecurity incident occurs, there should be policies and procedures (a playbook) in place, according to which the response to typical and most critical incidents should be scheduled. These playbooks must be communicated to the staff at facilities. A cybersecurity officer who detects an attempt of penetration, compromise, or ransomware in the network, saw it at the top - in the corporate centre. Since there are usually no people at the stations, and this may even be an unattended object, there must be a person who can turn off some network equipment using the playbook or put the system into the protected, isolated mode. This can only be done by the maintenance personnel of this system; the cybersecurity officer will never do it. Therefore, only operational personnel on duty will suffice in the part of prevention, response, rehearsal, and testing of the playbook at the facility in the system. But management will need to introduce an awareness program to the OT personnel, so that they are aware of what the ransomware is generally dangerous and what will happen to his/her ICS if the ransomware gets in.”

ManComLa5 talks about playbooks in the context of a security operations centre (SOC):

“In a nationwide technology company, the first line of SOC only does security monitoring and works on playbooks together with the administrators of security solutions”.

ManComLa5 also covers the example of how the playbooks can be changed:

“Security analysts are needed. First, they analyse the landscape, look at reports, see trends (which incidents occur most often, in which part of the infrastructure, on what equipment). Analysing the current situation, analyst should be able to influence changes in policies or changes in playbooks.”

ChemLaMe3 talks about playbooks when naming the possible projects for ICCFTs, saying that one of them can be *“creating incident response playbook for different vendors or distributed control systems (DCSs)”.* Also, ChemLaMe3 uses playbooks in the example of differences between IT and OT employees:

“IT team knows that they want to build a playbook for incident response. OT people don't know how even normal IT incident response look like, not talking about the OT incident response, so they don't know what to tell them about their work”

Incident response

In certain cases, "incident response" is used in a similar context with "playbooks", as it was mentioned before. PhaManLa1, ManComLa5, PetroLaMe4, ChemLaMe3 talked about incident response in different ways.

- Having incident response plans along with the business continuity plan. The employees responsible for incident response processes should be from the OT side.
- ***PhaManLa1:*** *"The difference between IT and OT cyberattacks is when an attack on OT environment happens, you can rarely know whether it is an attack, or something just has broken. It is almost impossible to understand what the reason was. Sometimes the only way to know is to do a forensics investigation that is costly and sometimes might not show anything. There is a lot of computerized equipment, such as sensors. The reason could be that something is stuck somewhere, or someone has a remote connection from outside. You never know, and the investigation takes a lot of time".* That is one of the reasons why incident response plans are essential: if the personnel know how to distinguish the attack, prevent, or isolate abnormal behaviour of unknown source, these steps should be documented and known by the employees.

Network administration

Network administration was mentioned by five experts (PhaManLa1, ManComLa5, ChemLaMe3, ManLa2, ManMe7). It is the highest number among all categories. Network administration also contains such sub-categories as network security, migration projects, network segmentation, but not network monitoring, as it appears separately together with detection. Experts say that network administration is not necessarily connected to the security activities – it is a routine network administration that OT people do on sites. However, personnel with cybersecurity qualifications are ensuring the security of the processes performed and changes made. It might include firewalls, putting devices on the network, maintenance, integration of OT networks, local segmentation. Migration was mentioned in the context of migrating from one networking provider to another. It was said to be a big and complex project to accomplish.

Security solutions & defence measures

Five respondents (PhaManLa1, ManComLa5, ChemLaMe3, PowManLa6, PetroLaMe4) were discussing defence measures and security solutions. Specifically, installing and administering anti-virus, but before the solution is installed, the team should know the impact and consequence of it on the system. *"When the devices are connected to the network, there is a requirement for an anti-virus. First, that should be discussed with the vendor whether they are ready to install this software on their PLC. However, there are more considerations. What will happen if the anti-virus observes malware? What next? If in an IT network with 10 000 servers one got malware on it, the anti-virus isolates and blocks this computer. But what if that all happens on the machinery in the OT, on a counter-reactor? What are the actions in that case? Should the network be blocked, should the operator be disconnected? But what if at this exact moment there is a production cycle going on? One cannot just come and install an anti-virus. There should be a set of tests performed, such as IQ (Installation Qualification), OQ, and other, as part of the validation process"* said PhaManLa1.

Administration of security solutions includes *"performance check, expert rule bases update, configuration. For example, if new hosts have changed or the settings on end nodes in the network have changed, the team member should register some routes in the firewall, open and close ports, roll the database update on anti-viruses in accordance with the regulations"* said ManComLa5.

Security Operations Centre (SOC)

Three respondents (ManComLa5, PetroLaMe4, ChemLaMe3) have talked about SOCs, all in the context of big companies having cybersecurity centres - either their customers/employers had one or planned to have one. They are big enough to afford it, and because of the size, they need better visibility into security. ManComLa5 gave an example saying "*if this is a large steel plant, but a localized one, then a full-fledged cybersecurity centre can be created on-site. However, metallurgical companies usually have several factories, so there can be different approaches. They can create centralized cybersecurity centres, where they connect the corporate segment first, then the technological one"*. ChemLaMe3 also said that usually OT SOCs are created by integrating it to the existing corporate SOC. The same expert assumes that "*the implementation of a network monitoring solution, integration of OT networks and*

integration into the corporate SOC could be roughly a two-year initiative with the roadmap. That requires building a workgroup. That work group will be built from the relevant people: some of them are consultants, some are from OT domain, relevant personnel from corporate SOC, and corporate infrastructure people".

Security solutions on-site are either managed remotely from a SOC or on-site employees are given this responsibility. At the same time, the SOC's "*work is built along the lines of support and response. Usually, the 1st, maximum 2nd line are in the regular structure of the company, the 3rd line is specialists who are engaged in investigations (threat hunting and other). Most industrial companies have neither specialists nor expertise to deal with threat hunting and full-fledged investigation of incidents. Therefore, as a rule, it is outsourced to external cybersecurity service companies, managed security service providers (MSSP). How the first and second lines are created depends on the infrastructure"* (ManComLa5). Although if it is an in-house SOC, ICCFT may consist of four people in smaller companies that have blended functions, or there might be a larger in-house SOC where team members have dedicated roles.

2.3 Impact of digitalization

The experts highlighted that digitalization is a big factor behind the need for ICCFT's service. PhaManLa1 said: *"Before, the support on-site was the following: an engineer goes to the manufacturing site, usually by the car driving for 50-200 km from the HQ. Takes the laptop, goes through the security checks and corridors and performs the support. Right now, there is a demand to do it remotely. One thing is to connect to the laptop and make some change requests in the computer network, and another thing is to connect to a bio centrifuge with 5 ton of substance. Even such a small process should be planned for a long time, all scenarios should be evaluated, and all clicks should be made consciously."*

At the same time, ManLa2 shared their experience: *"We have one of Europe's most modern industrial 4.0 manufacturing sites, and it is recognized. That is driving a lot of resources and a lot of initiatives in this area, and they need support. First, the local site built the digitalization and wanted to do everything by themselves. Now, they're coming and asking "Can you provide services from the IT team? We cannot concentrate on building IT for OT; we do not want to run production segmentation. We need to concentrate on digitalization and understanding of how we connect an old drill to do*

some processes for analytics." If to look at the sites that are at the forefront, one can see a significant shift. But if you are looking at the old ones, it is still this in a complicated situation. There it is more of "How can we run this environment not connected for as long as possible? We don't want to touch it". Later, when trying to do digitalization, there will be another complexity with 5G-enabled sensors and others. It is a hard area with a lot of work. It is both innovation and digitalization that are pushing the business leaders. At the same time, they should do more and more and more for less money. So, a conflict of interests".

3. Governance

3.1 Reporting structure and organizational hierarchy

Experts discussed several types of reporting structures. It can be noticed that all of them highly depend on the existing organizational structure and its needs, however, there are several common perspectives and clear explanations. Below each unique type of reporting structure is presented.

- Six experts said that a cross-functional team should report only to CISO, where four said that the team should be an *independent unit* that reports only to CISO.
- Four talked about a centralized ICCF umbrella team should cover management of security processes at all levels, both corporate IT and ICS that reports to CISO, and a local ICCF team that implements safety management processes at the site level that reports to the site management.
- ManLa2 said that "*OT people need to be placed close to the production manager or site manager. But not CISO. Coming in and working for a site manager or production manager provides an understanding that they have different drivers".*
- A shared view is that at every plant, at every manufacturing site there should be their own team managing ICS cybersecurity. The site manager is responsible for cybersecurity, but he/she will be governed and consulted by this cross-functional team, frequently reporting to CISO.
- ChemLaMe3 said that previously, it was unclear what should be the responsibilities of IT, what should be on OT, and now it is more or less that IT is winning. They are taking over the demilitarized zones and Level 3 shared services in the Purdue model. OT is now mostly responsible for automation system, so Level 2 and Level 1. This clear delimitation is favourable because it eliminates

conflicts. Also, the fact that IT protects DMZ and Level 3 with advanced IT security methods, creates decent in-depth perimeter protection, so, there can be fewer security controls in Level 2.

- ManLa2 said that about five years ago, their multinational organization with dozens of manufacturing sites has gone through an extensive decentralization *"pushing most of the responsibility as far down in the organization as possible*". Right now, they are introducing certain centralization again. ManComLa5 from power industry expressed a similar opinion, saying that "*It is impossible to manage the cybersecurity of 10 or 20 power plants not centrally. Therefore, there are two ways to approach it: a more costly, capacious and beyond the strength of anyone - the creation of security centres at each site. Nobody does this, because there is no money for it, and anyway, these teams will have to be managed centrally. Therefore, they create cybersecurity teams at the top, those that are the "umbrella", and they cover branches or individual plant sites with "umbrella" processes. They should already have the technical and infrastructural capabilities to manage, monitor and protect".*
- ManMe7 argued that both OT and IT teams should report to the IT operational manager. The hierarchy can be the following: the IT director is on the top of organizational structure and IT operations manager and the project IT site manager report to him. The IT and the OT teams both report to the operations manager. He added that it forces the two teams to work closely together because they both have the same manager to report to. When there are discussions, they could be resolved easier than if there are two different hierarchies to report to.
- Three out of seven experts say that right now there is a trend for a change in an organizational and reporting structure globally: from having organizational verticals to horizontal teams that are equals to each other. Sometimes new teams are created where team members remain in their original department with the same line manager but report about security work to CISO (flat organizations).

The problems come when each division has its own budget, and they need to share resources. ManComLa5 said that *"One of the main limitations, why such teams are difficult to create, is that each unit that is led by a CTO, CISO and other, has its own strictly limited budgets. In the rules of some industrial companies, it is not customary to share the budget. For example, if a security officer needs a technician in his/her team,*

and he/she needs to be taken from another unit, then the CISO must share its budget. But no one likes to do this, because the common budgeting practice for the next periods is to get a budget for your resources and not share with others. As a rule, the creation of such cross-functional teams lies in the plane of financing and budgeting, and only then in the plane of focusing individual divisions on the goals that are pursued when creating cross-functional teams. Initially, the technical unit (the OT), those who have a responsibility for industrial control systems, are solely responsible for these systems. They are not responsible for cybersecurity of OT systems. It is very strange, but over time it has developed like this all over the world. Cyber security issues are not included in OT tasks and objectives. On the other hand, CISO has a mission to ensure the security of the entire IT infrastructure, both corporate and technological (OT). Here CISO has a boundary of responsibility finishing between the cybersecurity division and the OT because ICS is a responsibility of the OT. However, the goal to protect ICS remains. That is why CISO is always the initiator, but at the same time, his/her goals are clear: protection of the IT infrastructure of the entire company, regardless of whether it is OT or IT."

ManComLa5 also provided comments on a prospective solution of such situations. If CISO needs to borrow an OT resource from a CTO for part-time or on a project basis, they need to agree on term and conditions for sharing resources. If a CISO needs to create a permanent ICCF team, the organization needs to undergo restructuring to create a separate unit that would report to either the CISO or the CIO.

However, since OT initially does not have responsibility for cybersecurity of their systems, and is accountable only for operations, who then signs off the risks for the cyber incidents at industrial control systems? The next section covers it.

3.2 Risks and accountability

Organizational structure and reporting go hand in hand with who is responsible and accountable for the risks. Four experts described the same accountability structure: ICCFT evaluates the risks, site manager signs off for the site risks and reports to CISO. CISO ensures that all sites have the right security measures and signs off the risks for the entire organization. When asked about who holds the responsibility for ICS cybersecurity incident, the site manager or the CISO, two experts said that in the first place, it depends on the service level agreement (SLA). However generally, the implementation and quality of processes are the responsibility of the site management, it is one of their KPIs. CISO

would take accountability for the overall security of a company and should place the goals or the demands on the site manager.

ManMe7 said that it is hard to say who is responsible for ICS cybersecurity, and that is one of the reasons why we need cross-functional teams. PetroLaMe4 shared that "*sometimes the site department can accept the risk. If the responsibility of cybersecurity is on the CISO, he/she says what needs to be done. But the site department can say no because they, for example, do not want to do it. Then CISO can say "No problem, you are not obliged to do that. But these responsibilities are yours". So, the site department must sign a letter of responsibility, and if something wrong happens, OT is accountable for it".*

3.3 CISO

CISO's role in ICCFTs was mentioned in the interviews very often – 100% of experts have expressed the need for CISO's participation. Five experts said that CISO should have a strong position in the company when it comes to ICS cybersecurity cross-functional team, as those should report to him/her and he/she is accountable for the risks.

Two of those experts covered the role of CISO within the relations with the top management and the OT department. ManComLa5 also said, "*As national legislation on the protection of critical infrastructure is being strengthened in all countries, the CISO now has leverage on the technological unit. He/she comes and says: "The responsibility for cyberattacks and incidents at industrial enterprises lies with the top management in accordance with the legislation. Accordingly, if we do not now take any measures with you to ensure compliance with government requirements; if we do not technically increase the level of security, you, the top management, will suffer". And no one wants top management to suffer because there will be problems for everyone".*

ChemLaMe3 highlighted that CISO could play a crucial role in creating favourable relations with OT and boosting cooperation. "*CISO would play crucial role in appreciating and understanding that IT and OT are different. In the end, CISO is the one who is signing up for all the risks. And if the CISO is a wise person, he/she is supposed to be the one who should find that champion in the OT domain and say "Hey, I'm trusting you and I'm listening to you. Please advise me. Please educate me and tell me what you need. Which tools are more practical and provide more value so that if IT is not even*

listening, then I have executive power to overwrite their opinion and decision and give more power to your decision. But you have to convince me and explain to me why this tool is better". And that is supposed to be the type of CISO you need."

However, the remaining two experts are more sceptical. ManLa2 said that "*often CISOs do not understand availability and safety concepts of the OT field. They are too concerned with protecting information, confidentiality. In the future, it would be good if all CISOs understand production, digitalization, availability, resilience of the production facility, and the different drivers. Currently, they have a minimal understanding. Top management like CISO needs to understand the OT priorities. That is a significant mindset change that needs to happen right across the field - to stop thinking about information as the only critical things within security".*

PowManLa6 from power industry said, "*The chief engineer carries the operation of the core business systems of this enterprise, and therefore the responsibility can be arbitrarily great on the CISO, but he/she will not be allowed to those systems. Therefore, in reality, it is impossible to involve CISO directly other than an advisory role, at least in the electric power industry. CISO is not in a position for recommending security measures for the power industry, scientific and technical innovations can be possible only at the level of technical centres of research institutions."*

4. Soft aspects of OT and IT

4.1 ICCF team's manager profile

All experts said that the team manager should be the person who knows both IT and OT. ManMe7 said that it does not matter whether the manager comes from the IT or the OT side unless the manager can do the work. Several respondents highlighted that it is usually the person who is *"highly competent both in IT and OT, and additionally knows everything about the production, all processes from A to Z, what does which pieces of equipment do*", "*who speaks the language of a multi-programmer, a networking guy or a security guy"* and *"can glue two different worlds together".* It was said that "*it is impossible to ensure ICS cybersecurity without the knowledge of IT infrastructure and its cybersecurity*".

As it turned out, the character traits were discussed by the experts much more often than the manager's qualifications. However, PowManLa6 said, "*A team leader should be, first of all, an expert in process automation. In this way, we reduce risks*". The table below presents the concepts that were coded during the data analysis. The number in the right column shows how many times the concept was recalled.

A technical expert	8
Willing to understand	7
Negotiable	6
Empathetic	4
Open-minded	4
Management skills	3
Sociable	3
Supports and develops employees	2
Flexible	2
Advanced soft skills	2
Respectful	1
Patient	1

Table 7: Traits of an ICCFT's manager

Below are some of the extended comments to the three points in the table.

Negotiable

To be successful, the manager must be able to explain the benefits of doing OT in the right way and how it can contribute to business values. He/she needs to be able to translate this. Otherwise, it will not be included in the correct forums or meetings. So, it is building a person that understands the complexity and the technical side of it, that can translate it to be to business leaders. I think then you will have a successful story.

Supports and develops employees

- ***PhaManLa1:*** It is a responsibility of the manager of the newly purchased security solutions and equipment to ensure the professional development of staff assigned to manage it. It is vital to keep them proactive and have the needed plans and playbooks developed, even if there is no dedicated cross-functional team yet.
- ***PowManLa6:*** Increasing efficiency, reducing costs, and increasing the competence of personnel, such a goal-setting should be in the team leader, and not goal setting for maximum security, business efficiency, a complete reduction in costs to the absence of cybersecurity.

Patient

ChemLaMe3: *"The manager should have enough patience to communicate these different concepts between teams. Even I, who has this knowledge, sometimes need to speak for five, six and seven times about the same issue and concept until this message arrives. It is important not to get frustrated. For example, I spend a lot of time in control rooms explaining them security concepts, and they start listening. In the beginning, they would not even understand. It takes a few hours until they more or less start understanding. Then you come again and again, you return and tell the stories, maybe with different words from different angles, and slowly it's coming. But it requires a lot of patience and if you might disagree or not understand each other at the beginning, but you have to understand that it is normal. I would go back, and we would continue this conversation, and again, to do it with empathy."*

4.2 Team member's personality traits

The majority of experts have commented on what personality traits should team members have. Below are some of the answers.

- When forming such a team, one needs to immediately look for super-motivated professionals who improve their skills every day, perform clear actions that are indicated in the instructions and who will work purely based on the task at hand.
- People should be open-minded and ready to cooperate.
- They should have certain soft skills, maybe one should not be that pushy.
- Sense of duty: it is not acceptable to turn everything off in the case of the incident. Most probably, the site manager will say "I take responsibility for the site running on shoulders, keep working!" because the losses can be unrecoverable.

4.3 Communication

- Five experts said that co-location is beneficial in creating better communication and relations in the team. It could be co-location on the same production site in the office, at the SOC, or in the office at headquarters – to put them as physically close together as possible. Otherwise, they will communicate on the need basis as seldom as acceptable. It is also one of the challenges in 2020 when most of the employees at industrial companies are working remotely.

- Sharing uncertain information is also confirmed to be essential. ManLa2 said that the goal is "*to create an openness and non-critical environment that is having a supportive approach and culture, to learn evaluating and using information together*". PhaManLa1 said that it should be "*an independent unit where employees are not afraid to speak up and cause tension"* and *"people should be open-minded and ready to cooperate"*. Trust has been named by four of seven experts as a critical component of the relations in the team and the progress in work.
- PetroLaMe4 said that if he does not have an in-depth knowledge of a certain subject, he is open about it with his/her team, but then he goes and learns it. He says that people respect him for being transparent. ManLa2 provided an extended reply about transparency: "*I think OT people do not want transparency on what they have done in cybersecurity. They fear the decisions they have taken and therefore want to limit the visibility as it might fall badly on them. Hence, when central IT security people try to step in, they shy away. OT does not want them to interfere. These are the worst cases of with protectionism and control. When OT and IT start to work together and are humble from both sides, they get a good joint venture of support to each other. To be less transparent is a terrible thing. I believe, to be open is always the key. If there is anything one needs to handle, rather say, rather be open with the risk of it. Colleagues will try to support. To prevent such kind of situations, I think it is best to enter it from a very humble way. If one wants to enter OT, one should have certain soft skills, maybe one should not be that pushy".*

4.4 Shared mental model

In the work of ICCFT, it is essential to nurture a shared mental model because, as ChemLaMe3 said, those are two different universes. Five experts said that the most effective way to create a shared mental model is to put IT and OT members on a mutual activity together. It can be a training or a shift at SOC. In this way, they will be not only to learn together but also learn who knows what. "Those training and the real work will not be enough even after a week or a month of working together to fully learn who knows what. Understanding the team members' competency takes months and years, and it is a process of constant learning. The team should work on it, do the lessons learned to prevent a zero-day attack".

5. Conflicts

There has been a lot of discussions on conflicts that can occur in ICCFTs and how to work with them. Below there are statistics on the reasons for conflict and experts' extended comments.

Five of seven respondents named different priorities to be the most common reason for conflicts, where risk management plays a central role – four experts covered it.

- ***ManLa2:*** Traditional enterprise IT needs to change the mindset on how they tackle OT teams because otherwise, they will have a lot of frictions. IT works with confidentiality, integrity, and availability. But when it comes to OT, availability and safety always overtake everything else, there is a different perspective. Main conflicts reside within the understanding of each other's practises and main objectives and how to align those different perspectives of overall company risks vs production unit risk and availability.
- ***ManComLa5:*** There is the problem of translation from one language to another: from industrial automation to the language of cybersecurity. There is a different technological apparatus, a different understanding of security tasks, data privacy issues at ICS are of the lowest priority.
- ***PhaManLa1:*** The organization received information from a vendor that there is a CSV in a PLC. The question is to dedicate time for maintenance to patch it. It is very complicated for OT to devote time. After all, there will be many decisions that should be approved by many parties; the stop of production time will bring lots of financial losses because it is the production unit that makes revenue. On the contrary, IT is a service function within the organization and is not equal to the OT in decision making.
- ***ManComLa5:*** Security officers do not understand the specifics of ICS cybersecurity. There might be a broadcast poll (network scan) in a segment of the ICS network. Policies in companies prohibit scanning. For a security officer, the very fact that such a scan appears is a security incident that needs to be dealt with. For a process control system, this is not an incident at all. The solution will depend on how IT and OT agree, what policies and playbooks they develop and how they process it. The solution can be the following. The OT members of the cross-functional team can convince the security officer to allow broadcast polls for

certain protocols, in a certain network segment from specific hosts, and this must be fixed. It is necessary to clearly state who, where and why has the right to do so. Here they need to agree on two things. Firstly, whether these are prioritized business or production risks, which are not about information security, but generally about company risks. Secondly, on a cybersecurity threat model that reflects and maintains a business risk registry. When the security officer says that something is an incident or is dangerous, OT has some questions. Why is it dangerous? Where is the evidence with the mapping of cyber risks to business risks? The moment of proof is very critical. It is essential to justify. The cross-functional team needs to come to the consensus on that this risk is real and important to us; there cannot be two separate perceptions of risks in ICS cybersecurity. When these two things are connected with each other, then it is not a problem for the security officers and the automated control system to come to an agreement. Everyone understands where does the raising of channels bypassing the firewall leads to."

- ***ManComLa5****:* There are different risks from different areas of IT and OT. The problem is to combine them. Luckily, everything has already been invented - ISO27000 series of standards for cybersecurity management. Cybersecurity risks need to be managed when there is a clear understanding of the business risks of the company. If cybersecurity risks do not affect business risks or operational risks or production risks, then this risk has a low priority.
- ***ChemLaMe3:*** Medium alarms might have the maximum reaction time of 15 minutes and the maximum consequences cost is 10,000,000. That is something unthinkable in IT. They don't understand that OT cannot afford a single hiccup in because a single disturbance on even on the network may result in significant losses with short recovery time. Everything must work with a high precision, high availability. They cannot afford to have extra software which might impede availability or even performance of the assets.

ManComLa5 and PowManLa6 stated that budgets and financial questions are the main cornerstones.

- The first example by ManComLa5 has been provided above in the section "Reporting structure and organizational hierarchy" on sharing a budget.

- ***PowManLa6:*** *Cybersecurity is a vast expense, and a corporate business is always a source of revenue. It is a direct contradiction between reducing costs and increasing efficiency by reducing costs. It contrasts with the size of the team and the budget of each of them. Conflicts of interest are not a common occurrence in such places, as the interests of the majority coincide. There are also conflicts based on the area of responsibility, the involvement of additional teams that are not directly subordinate to the chief engineer causes a conflict. Here diplomacy can be barely applied.*

ChemLaMe3 and ManLa2 concluded that the reason for conflicts is the inability to communicate and a low-level education about each other.

"Not all the projects are successful in ICS cybersecurity. People cannot appreciate the opinions of each other or understand the arguments of each other because they are just not educated. They need to talk to each other, hear and understand each other. This is where cross-education helps", said ChemLaMe3.

ManMe7 and ChemLaMe3 shared that external interference is also a reason for conflict.

- ***ManMe7:*** *"The conflict that I saw was also about giving up his/her autonomy. Before all the sites were just connected with phone cables and the OT Department managed that network all by itself. So, it was much smaller, and not redundant, but the OT guy knew everything how it worked. And now that everything is connected and firewalled and stuff like that, yeah, he/she loses his/her grip on his/her network and has difficult discussions sometimes".*
- ***ChemLaMe3:*** *"Typical conflicts of interest in IT/OT domain are when OT tries to minimize the amount of software, services, data streams running on OT because you want to have maximum available resources to run your control process, process control functions. In contrast, IT people now want to introduce their solutions: whitelisting, agents for network and logs collection, agents that would monitor for intrusions, to send all of those logs via the network. That all creates additional opportunities for congested networks and applications running a little bit slower. They want to have more security, but that may cause me more consequences or more troubles. The solution is to put as much IT security*

protections in those Layers of network, like DMZ, Layer 3, corporate, to make sure that the remote access, for example, is bulletproof secure".

6. Knowledge & Education

Education, training, knowledge sharing, and learning is substantial and crucial in the successful work of ICCFT. Firstly, all members have stated that training and any learning should be regular, it should be done "constantly, a lot and quickly" to be on track. Experts name several types of those activities.

- Cybersecurity awareness training and exercise for all
    - Proliferation exercise
    - Phishing campaigns
- Cybersecurity news information sharing between all members
    - New attack vectors and methods
    - APTs
    - New CVEs
    - New security technologies
    - Best practices
- Education on security methods, solutions, and products for each
    - Education from vendors and integrators
    - Cyber defence measures
    - SANS ICS410: ICS/SCADA Security Essentials
- Knowledge about industrial sites
    - The geographic location of sites
    - All processes in each enterprise (although, each site has a different way to work, so it is hard to teach the ICS cybersecurity team the in-depth knowledge of each site that your company has).
    - Technologies used in the standard operating procedure for each area of the production
    - What are the firewalls, where are they, and what do they filter
    - Technical and infrastructure capabilities of the sites
    - Site risk assessment
    - Site incident response plan

- Education for OT employees about IT and cybersecurity (e.g. advanced methods in IT Security)
- Education for IT/cybersecurity employees on OT (ICS, DCS), limitations and constraints when securing that infrastructure.

A conflict of perspectives was discovered in interviews of two experts. ManMe7 said that the training should be the same for IT and OT, and ChemLaMe3 said that each should have a separate one.

ManMe7: *"Based on the experience I had with the team I think it should be one training for both. It was more important to show them the advantage of working together and bringing the two worlds together".*

ChemLaMe3: "*Whenever management asks me "Would like to develop training?", I always ask "How do you work? Who is your audience? Is it for IT or OT team?" and I get "We cannot create different training for each, so it has to be generic enough that both could participate". Then it is a training that is useless for both".*

Two experts have elaborated a lot about education. Below there are their perspectives on it. The one from the power industry addressed trainings for the umbrella ICS cybersecurity cross-functional team:

PowManLa6: *"I believe training should be provided only for low-skilled personnel and in highly specialized courses that are difficult to find outside the workplace. It seems nonsense to me to provide training to professors and luminaries of science. On the contrary, they should share their knowledge through scientific publications and various conferences. It can only be an equal exchange of experience between an expert and a professional".*

ChemLaMe3, who has extensive experience in consulting and management roles at various petrochemical and chemical customers, has provided the following answer:

"The general education about each other with a context of each other's jobs - is not there. Therefore, OT and IT have difficulties in communicating and understanding even the information which is already given. You can share some information with the other side, but they do not really know how to interpret it and understand how it is useful. This is why I have never seen those projects being very successful sometimes. It is important to

provide the necessary information in the context, which a person can understand and appreciate. For example, to show to the OT people that structure of the SOC is very similar to the structure of the DCS and Control room. Once I took a team of IT people from IT SOC into the so-called OT security SOC, which was at that time considered to be very advanced. IT people were so disappointed: they could not relate to anything and were bored. The information needs to be explained in the language of their technologies and should be shown how it can benefit them. There is a need to explain that new information in the context which they can understand".

ChemLaMe3 highlights that there is a solution in such situations – an exchange of employees. *"To take a person from the SOC and put him into the control room and send automation people into the SOC. Then, day by day, interaction by interaction they will find the language and vocabulary, start understanding job specifics, needs, limitations, constraints, values, main objectives, and priorities. So, placing them into the roles each other, but with preliminary knowledge and education. Putting a person into the shoes of others without explanation will not make them understand or appreciate it. It is once they start understanding the specifics of each other job, then they will have more information and maybe interest to communicate with each other".*

7. Vendors

Experts have shared that vendors have to play a significant role in security decisions, especially if a company does not have responsible people or no cross-functional team. Respondents provided their comments on how to manage relations with a vendor when there is an ICCF team in place.

- Vendors of the control system's equipment have a strong say in what security solutions can be used on their environment. They often would have a list of security vendors that have tested compatibility to their equipment. If a customer wants to use a vendor outside of that list or change any configuration on the equipment, the vendor will refer to their contract, where it often says that it will violate the warranty. Some might not have it and provide more flexible conditions of use and integrity. ChemLaMe3 said that "*for asset owners, it's very inconvenient and not beneficial. But on the other hand, such system provides guarantees and support, although with less freedom. So far, there is no*

established opinion and established model how this relationship work. If I would be an asset owner, I obviously would not want that my vendor to dictate me what to use".

- ManLa2 covered risks and accountability issues: "We need to lift it from the technical perspective with the right people at the vendor, talk about who is accountable for their risk. If the vendor wants to do it in a certain way, they also need to understand that they will be accountable for the risk. That is the only way I see we can change it and I often see it stops technical people at a vendor. It is crucial to insure against a penalty for the overall group. Maybe a small company or a big vendor can take that risk, not the smaller vendor."
- On the other hand, national legislation in some countries puts a limitation on the offers that vendors can make. ManComLa5 said that *"cybersecurity of critical infrastructure is becoming a nationalized issue. When projects for automation or modernization of systems start, in many countries, enterprises are under pressure from legislation that these are issues of national security. Hence even though vendors have something to say and offer in terms of cybersecurity of their systems must comply with legal requirements".*
- When it comes to selecting the security solutions, ChemLaMe3 said that IT vendors are having a lead on the market and are more popular among customers than better solutions because the brands are familiar to the IT department that takes such decisions. "*Maybe it will be suboptimal, not delivering the needed value, but those security solutions will be adopted and applied to the OT environment just because IT people are more comfortable with them. Lobbying will be always there because the stronger party will always want to use own tools. And unfortunately, OT people will never have that strong convincing factor or messaging to convince cybersecurity people in using their tools. That I find very, very unfortunate".*

5 Discussions

The discussions chapter is divided according to the topics of the results section and aims to answer the research question on "What are the best practices in establishing ICS cybersecurity cross-functional teams"?

Governance

This section discusses the governance of ICCF team, the organizational structure, its management, the relations between the team and others, the reporting structure and accountability for the risk.

There is no unity in answers of experts on the organizational structure and reporting because those are dependent on the company itself. However, common principles match the structure stated in NIST 800-82. In general, experts do not recommend having too decentralized security because it will be highly complicated to manage them. In other words, companies should have unified cybersecurity measures implemented, the teams from different sites and business units should have a connection to each other to discuss security matters, there should be a common OT SOC covering all sites and reporting should go under one person – CISO or similar. If the company is small or has just one site, it is recommended to have one ICCFT and one local SOC there that might be executed by the same set of people. If a company has several sites in different locations, the best practice is to have "an umbrella" team that will consist of representatives of those sites. Some refer to the umbrella team as a global expert group. Together, the members of the umbrella team decide on the security measures to be implemented in all sites, create policies, and consult site management on creating local ICCFTs.

If disconnecting OT and IT personnel from their previous line manager and the department is not an option, four experts said that the organization might implement a matrix reporting structure, where an employee has a department manager and security manager who can be either regional/business unit security manager or CISO.

A question of accountability is important. The organization-wide accountability lies on the shoulders of CISO (that is discussed below), whereas each site manager signs off the risks at a specific site. If the site manager refuses to comply with the requirements from the CISO, it is a best practice to sign a letter of responsibility stating that if something happens, the risk is on them. It is also a best practice to have site manager responsible for

the site cybersecurity who reports to CISO. The article [13] states that cross-functional teams *"are held accountable by senior management for all facets of the project (not just their functions piece) and also for the entire project from beginning to end (as opposed to a single phase)."* The team manager is accountable for the performance of the team and should hold "*teams jointly accountable and discouraged finger-pointing*" [26].

CISO

Fortinet report said that only in 9% of their respondent's companies CISO was responsible for ICS cybersecurity, however, 70% of their respondents said that they plan to roll ICS cybersecurity under CISO in the next 12 months [27]. In the meanwhile, six experts from this thesis study said that the best practice for ICCFT's managers is to report to CISO. It means that among experts from different countries and industries who have experience with ICCF, it is a shared opinion on the best practice since several years ago. At the same time, they say that CISO should change his/her mindset from confidentiality- and compliance-centric to OT-centric to understand the needs of ICS in cybersecurity. For that, CISO should also be educated for ICS cybersecurity.

The profile of the team manager

The best practice in selecting an ICCF team manager is to get a person from the engineering (OT) side that knows the ICS processes and operations very well, and also has a strong understanding of cybersecurity concepts. The experts of this thesis said that the team manager should in the first place be the technical expert with hard skills, and the article [13] authors say that "in highly collaborative firms, managers '*functioned primarily as educators and coaches'* [26]." It should be someone who either worked in a cross-functional team before or someone who has working experience from both industries. Also, the manager should have strong soft skills, such as being negotiable, empathetic, open-minded, sociable, flexible, respectful, patient, be willing to understand. Several experts said that it might be the most crucial criteria and they also admitted that it is an extremely scarce type of resources. The ideas expressed by the experts match the success factors in the article [13] stating that the leader should play a key role in team empowerment, provide the team with autonomy in their decisions, protect from external interference, and to lobby for the team's interests within the organization. The team manager needs to have the trust of members from both OT and IT and actively take part

in their professional development. Industry standards [7] and [9] emphasize an essential role of the team manager is bridging two different cultures of IT and OT.

Transition

The transition of selected team members from their former responsibilities to the new ones was not a topic of discussion in any of the research papers. It might be intuitive to assume that if there has been a decision to create a cross-functional team, the team members will start their work there from the first day of the official decision. However, no expert said that it is the right way to do it. The majority of experts said that the transition should be gradual. The article on success factors also mentioned "*formal yet flexible integrative process*" with careful planning and testing [13]. For instance, first, the team members may start from 20 hours a week. ChemLaMe3 said that the transition should be done by smaller steps, starting from one day a week because working with another field is a passion one should develop. It is a valid argument because having fewer days in the beginning may help the employees feel more motivated to do the work and to learn gradually.

The team formed was said to be mainly a permanent organizational unit, not temporary. Although, the opinions have split in: three experts think that team members should work together and become so knowledgeable about each other that they can be interchangeable. Four others think that out of 5-7 people in the cross-functional team there could be workgroups for specific tasks, presumably consisting of 3-5 people, possibly also other employees for certain specific tasks and contractors.

Composition of a team

The roles named by the experts have matched to what was listed in the industry standards NIST 800-82 and ISA/IEC 62443. Experts also listed competencies that match the roles in those standards and the article [12]. These should not necessarily be possessed by each team member in high proficiency, but all should have a general understanding of each of them, and some should specialize in certain. These are data transmission network, automation and control systems, embedded systems and sensors, maintenance methods, ways to eliminate device and system planning errors, IT network protocols and production protocols, network security and safety, core IT understanding, PLC programming, cybersecurity governance, the application side of OT environment, security systems

administration, service security solutions management, cybersecurity management competence.

Therefore, before the selection of the potential team members, the manager may map their competencies to the required ones listed in this study. It will also help to identify which competencies are lacking; hence it will be easier to decide what education to provide.

The amount of people to have in the team recommended by the article on success factors of cross-functional teams [13] and the experts from any company size is from 5 to 7 members. It also matches the recommendations of the article [28] that smaller teams perform better than bigger as "teamwork quality is lost in large teams", although research cannot "provide an absolute optimal team size in terms of a specific number". Hence, these recommendations of experts improve the chances of better cooperation.

Functional mix

It is a best practice for the functional mix in ICCFTs to have an approximate ratio of 50/50 of IT and OT employees. If to combine specific recommendations of some expert, they advise having two subcategories inside the team. First is some people from IT and OT who would work towards becoming interchangeable. That will create internal resources competent in ICS cybersecurity and in turn, they can help the industry bring up more talents in the same emerging competency. The second subcategory to have is team members that specialize on certain narrow competencies, such as PLC programming, information security of IT infrastructure. Team members can also be categorized by those who operate the equipment, and those who implement protection. Interestingly, there is no consensus on whom to educate if there is a shortage of employees: IT employees in OT competencies or OT employees in IT competencies. Each of the experts had a firm opinion, therefore, the general recommendation should be to have a couple of key people in OT and in IT to decide who of the staff should be selected to be educated, so this functional mix satisfies the needs of the team.

Lack of talents on the market

All experts of this study and such articles as [4] and [5] have confirmed a lack of talents in ICS cybersecurity on the market. Companies sometimes are failing in their tasks and projects because the existing few ICS cybersecurity-related employees are overwhelmed with other responsibilities. Therefore, the companies should be certain to dedicate time

generously in the work of their employees for education as those are trying to substitute a talent that is not yet even a little spread on the market. The gap can be eliminated by cooperating with academia and by educating internal employees.

Motivation

The experts of this study, ISA/IEC 62443 document, and the articles [5] and [13] said that motivation is a critical component of the work of cross-functional teams and that some of the success factors in it are clear and ambitious goals, trust between team members, clear and frequent communication, regular education, team building activities (education, shifts, exchange). While there is a deficit of qualified professionals on the global market, existing competent employees at companies may experience a lack of motivation because of the conditions of their work. Experts said that usually during this transition, the employees do not get a salary increase. This period of their career is quite overwhelming: to learn new disciplines and start performing work there, to defend their perspective in ICS cybersecurity-related decisions, integrate into a team and get along with new people, do a handover to those who will take over the old responsibilities, in certain periods of time do the double work since yet there might be no one to do the job as good as them, but also to start doing the new tasks. Therefore, management should find incentives for them and suitable conditions, and there is no consensus between experts' opinions and research articles. The experts of the thesis suggest a bosun or raise in a salary, or at least to ensure a smooth transition to the new responsibilities. Article [13] summarizes several studies saying that according to the Deutsch's theory of cooperation in psychology [29], individual incentives provoke "*competition of appearing the brightest*", *"rivalry, secrecy, distrust, frustration, hostility and low productivity*" [13]. It is called "negative interdependence", whereas "positive interdependence" means that if a goal can be achieved via cooperation, it creates more productivity and trust. Article [30] on compensation strategies says team-based rewards are more effective in increasing performance than individual rewards, but the team manager should be very careful with distributing financial rewards. An article [31] on compensating teams' states that *"Money can create a feeling of inequity. Rewarding on results penalizes those who take unsuccessful risks. Individuals should be rewarded for behaviour, not team results."* Taking up a challenge to join an ICS cybersecurity cross-functional team is an attribute of a brave and curious employee. Hence, the manager should use incentives when creating

ICCFTs, favor team-based rewards over the individual, and if applicable, carefully distribute financial rewards, although non-financial might be fairer.

Activities

Some of the findings match certain activities named by the article [12]. It is a best practice for ICCFT to be responsible for all activities in identification, protection, detection, response and recovery in the ICS environment. The names activities were creating playbooks, security solutions & defense measures, network administration, incident response, SOC, network monitoring & detection, enterprise software & applications, compliance, threat intelligence, governance, remote access, prevention, maintenance, backups, patching, cybersecurity aspects of SCADA management & upgrade, databases administration, plc programming, validation of solutions, testing, recovery plans and processes, risk assessments, network segmentation, migration projects, unification and standardization, network security, SIEM & security analytics, infrastructure administration

The best practice of working with vendor security solutions and performing patching in ICS environment:

- Cooperate with a vendor to ensure what is allowed to install not to violate the warranty
- Run tests before the installation
- Perform backups
- If applicable, select the right timing in the production circle to perform the installation or maintenance of the security solution
- Have updated risk assessment, business continuity plan and incident response plan before performing any of the actions.

If a company is big enough and has an IT SOC, it is a best practice to integrate OT SOC there. If a company cannot afford to have SOC, they manage the detection and response themselves or outsource it. In that case, the best practice is to ensure that resources are educated enough and have the volume of responsibilities they can manage. Playbooks were identified to be an important practice in incident response. They should be created by OT employees in cooperation with cybersecurity team members for each specific scenario, security solution, vendors, DCS, be regularly updated, tested, communicated

with staff facilities on how to act in the case of an incident. In turn, it means that facility staff should receive cybersecurity awareness training too. Although it is clear for IT team members that a playbook is an essential part of incident response, it is important to explain and communicate this need correctly with OT.

Education & Knowledge

All experts concluded that education and gaining knowledge should be greatly prioritized because otherwise, employees would not be able to do their work. Employees should educate themselves, share knowledge with other colleagues, learn about the opposite department, learn together with them. Management should incorporate timeslots dedicated to learning into the schedules of the employees apart from their day-to-day job. It is also proven that learning, information and experience sharing help *"to address the economics constraints"* [32]. It was highlighted by five experts that knowing the ICS environment, the processes and equipment is crucial. At the same time, no expert said that the IT personnel should take education in fields of electrical and automation engineering. Therefore, it can be concluded that they should know the high-level information about it, but the OT staff can explain some technical specifics on-demand basis if that is needed for the project. Experts also did not provide a common answer on whether OT and IT should be educated with the same training materials or different, but some experts argued that these should be different. The main reason is to be able to explain OT how they can benefit from IT and cybersecurity measures, and to explain to IT the complexity of the ICS environments, how they work and what are their priorities. It is impossible to address both perspectives in one training. One of the working practices is to provide each side preliminary education in the other field and then place a person in the opposite environment so that they can relate the work to the gained knowledge and understand how the other division works.

Communication & Conflict resolution

It is a best practice to co-locate the team members on the same site as it increases their cooperation and improves their relations. It was mentioned both by the thesis experts and in the article [13] that referenced four other research papers. It is also one of the challenges in 2020 when most of the employees at industrial companies are working remotely, and the gap in communication between OT and IT team members can only grow. Due to the

pandemic's economic crisis, some companies (24%) are cutting costs on security, as Kaspersky says [33]. However, on the other hand, they should be increasing them as more employees started working remotely and need more security measures and training, but only 15% did so [33].

The experts of this thesis and the article [5] identified having a shared mental model as the soft goal of ICCFTs because team members aim to substitute ICS cybersecurity competency. A shared mental model is an essential part of the integration between the cultures to achieve "*a collaborative security design and operation*" [7] in ICS cybersecurity-related decisions. One of the best practices is to put pre-trained OT and IT team members into joint activities such as shifts at SOC or common education. One of the attributes of a shared mindset of ICCF team members is to be transparent to each other in what they know and do not know and share uncertain information to prevent an incident from happening. In the book [34] it is explained that *"sharing provisional information, being prepared to act upon it, and treating decisions as tentative renders teams more flexible in responding to problems"* [13]. The team manager should play a central role in creating trust and shared mental model among team members. The article [5] mentions that many other articles say that there is a huge mistrust between OT and IT, but they did not find it. In contrast, their respondents "*admitted the need for exchanging information and learning from each other*". In this master thesis, the experts did not say that there is mistrust between IT and OT, but they said that trust is one of the crucial components. ChemLaMe3 said that the reason for mistrust is a lack of understanding of each other and a lack of education.

It was identified that conflicts usually arise from financial issues, interference into responsibilities, different perspectives, and priorities: when and how to patch, what security measures to implement and when. Very often, the reason for conflicts is team members being poorly educated about each other and not being able to relate to the discussion topic. As ChemLaMe3 said, if to share information with OT in the language of IT, they will not be able to interpret it and relate to it. Therefore, it is essential to find a way how to explain and translate the information to them. A team manager must be a moderator and ensure that conflicts are task-based, not relationship-based [35]. Moderate task-based conflicts are beneficial as they give a chance to evaluate a problem critically. However, it is possible only among educated team members who can be equals in such discussions. The best practice to prevent conflicts is the education of employees in the topics of each other, team building activities, and developing a common language among

the experts. It means the preparation of such training and incorporating the developed common language into the training could be necessary.

Vendors

In this section, the discussion about vendors lies in the following context: there is a manufacturing/petrochemical/power/other company that has equipment supplier. Equipment supplier provides equipment from different ICS vendors. Each vendor may have a set of selected security vendor solutions that have passed a compatibility test.

Both the experts of this study and such papers as NIST 800-82, and [5] said that vendors should be included in decision-making processes and should provide education to the employees. Experts said that the cross-functional team has more authority and power, and the manufacturer is always interested in the satisfaction of the customer. Hence, they are always ready to find a compromise. Therefore, vendors may always suggest possible solutions, but the final word holds the team. There are a couple of scenarios when a company may decide to change the vendor. Some suppliers or ICS equipment vendors may not agree to allow the company to install the security solution of their choice because it is not tested for compatibility. In some countries, the legislation might require companies to have security solutions that comply with certain criteria. Those criteria might not match the criteria of security solutions compatible with the existing vendor equipment. Hence, the company and the vendor should come to a consensus that is either changing the vendor or the vendor approving the needed security solution. Also, if there has been a CVE found in the vendor's equipment and the vendor failed to issue a patch over a more extended period of time, the company may decide to select a new equipment vendor.

In order to select the right security solution vendor, it is essential to educate OT personnel, so they have a say in this decision. OT should be able to understand its functioning and the value of the product. Otherwise, conflicts may occur. Usually, IT employees are the one to decide on cybersecurity solutions in OT. It is a bad practice that should be changed to both participating in selection and decision-making process being equals in understanding and power. Team members should be educated in managing and using all vendors' equipment and solution and know what they are for. It is often that employees do not know how to use them or that they exist. Team members might also *"perceive the time spent away from task activities"* on vendor communication as "*unhelpful distractions*", whereas their team manager is aware of the "politics" importance [36].

Hence, “teams also need to be educated to consider boundary management as an important part of their tasks” [13].

Interesting findings

- Some experts have identified that there is no good training for IT and OT on cross-functional teams: what is their vocabulary, main goals, objectives, metrics. There is a demand from companies, but there is a low supply on the education market.
- There cannot be “one-size-fits-all” conceptual and product solutions for OT because each environment is too unique to be able to generalize. Therefore, the industry should be ready to produce solutions that can be customed. At the same time, there is a lack of such solutions. *“Therefore, the industry, in general, should take responsibility for popularizing and raising the awareness of the OT cybersecurity. […] Globalization, automation of all technological processes, remote work makes the systems and networks vulnerable. It created a need for dedicated attention, as especially now there is a popular business requirement to manage the manufacturing plant sitting at home.”*, as one expert said.
- There is no consensus on who is leading: OT or IT. Experts and the literature have strong opinions in favour and against each of the perspectives. Therefore, it might be concluded that OT has some things to learn from IT, and IT learns from OT. Four experts’ opinions can be summarized stating that OT becomes IT-centric and IT-looking in the approach to cybersecurity and the vendors used. At the same time, three other experts and [7] said that engineers have the leading role. Such symbiosis is a significant transformation in the electrical engineering and automation industry; hence, academia and the eco-system will adapt, produce new solutions, frameworks, and most importantly talents. However, IT and cybersecurity industry will also change int heir approach to OT cybersecurity to avoid frictions because confidentiality and compliance are not the central priorities in OT.

6 Summary

The main goal of the thesis was to discover how to establish the ICS cybersecurity cross-functional teams. The author reviewed the background information from all available resources such as industry standards and recommendations, reports, studies, and articles to establish a baseline of what is known and what can be further explored. The author identified that to answer the research question of this descriptive study, the data should be collected with the elicitation method. Hence, semi-structured interviews were conducted with seven experts that had experience in ICS cybersecurity cross-functional teams in manufacturing, petrochemical, and power industries. A qualitative data analysis method is used by keyword coding, that is performed in MaxQDA software. The results revealed a broad landscape of experts' perspectives on selecting team members and the manager; the transition of employees from former responsibilities to the work in ICS cybersecurity cross-functional teams; reporting structure and accountability for risks; description of typical activities and projects, education and learning; communication; and relationship management with vendors. These were further discussed together with the papers from the background information chapter to draw conclusions. The research discusses the best and worst practices, by comparing the collected information with the available literature. It describes the common criteria and suggestions in cybersecurity processes in ICS that should be done by a cross-functional team, governance structures, competencies, soft skills that need to be possessed by the members, education, communication management, motivations and other soft aspects. The results of this research study can be used as a reference point or manual in the decision-making processes when creating or designing such teams.

Limitations

The selection criteria of experts turned out to be too broad. It led to experts having too different backgrounds to be able to generalize their experience. They were from different industries, different sizes of companies, different organizational structures, different countries. On the other hand, the author had hard times looking for the experts because it is infrequent to find an experienced member of cross-functional teams. Also, at that time, the circle of connections of the author was limited, so she was not able to reach to significantly more people via her connections than she did. Also, several potential experts

did not reply to the suggestion to participate in the research. Hence, the next research can select narrower categories. For example, select experts by industry, by country, by the size of the organization (e.g. Sweden, manufacturing, up to 1000 people, with a advanced IT department). However, in that case, the search for candidates will be much longer.

Because the thesis was finalized at the end of the year, the experts were busy or not reachable for the follow-up comments on their interview. Sometimes, 5 of 7 experts would express an opinion about a matter, but two did not cover it in the interviews. The follow up was possible only with 4 of 7 experts.

Interviews with experts is not a universal truth because they are subjective. Each expert did not have the perfect experience that can be labelled as the golden standard. However, the results should reflect the patters in subjective perceptions. The set of experts is also a strength of this study because there is no other study that retrieves information from experienced people who worked in ICS cybersecurity cross-functional team.

Notable contributions

There is yet no substantial research done on ICS cybersecurity cross-functional teams. Therefore, this thesis establishes a new landscape of literature in this field. The novelty of this research lies in the application of the descriptive study methodology and qualitative data analysis method on a unique data set. No research has previously gathered information from experts that have experience in ICS cybersecurity.

Future work

Consequent studies should focus on specific industries, enterprise sizes, and regions for better accuracy. The fields of studies can be the following:

Cybersecurity:

- Compliance to industry standards performed by ICCFTs
- Asset management, risk assessment, business continuity plan creation by ICCFTs
- Protection methods used by ICCFTs and their implementation and maintenance
- Detection methods used by ICCFTs
- Incident response by ICCFTs and OT SOC
- Developing education for IT in ICS cybersecurity
- Developing education for OT in ICS cybersecurity

- Exploring the education used by ICCFTs

OT:

- Cybersecurity considerations in operations of an Industrial Control System
- Incident detection in ICS by ICCFTs
- IoT devices management by ICCFTs

Management:

- Governance structures in ICCFTs
- Risk management in ICCFTs
- CISO’s role in ICCFTs

Psychology:

- Conflict resolution in ICCFTs
- Communication in ICCFTs

Economics:

- Optimization of costs by creating ICCFTs
- Economic sustainability of ICCFTs compared to divided functions of IT and OT

References

[1] European Comission, “Digital Transformation Monitor,” *Germany: Industry 4.0,* 2017.

[2] Mark Zeller, Schweitzer Engineering Laboratories, Inc., “Common Questions and Answers Addressing the Aurora Vulnerability,” *DistribuTECH Conference,* 2011.

[3] R. Langner, “Stuxnet: Dissecting a Cyberwarfare Weapon,” *IEEE,* 2011.

[4] T. Menze, “The State of Industrial Cybersecurity,” *Kaspersky,* 2019.

[5] M. Bartnes, N. B. Moe and P. E. Heegaard, “The future of information security incident management training: A case study of electrical power companies,” *Computers & Security,* 2016.

[6] B. Filkins and D. Wylie, “SANS 2019 State of OT/ICS Cybersecurity Survey,” SANS Institute, 2019.

[7] K. Stouffer, S. Lightman, V. Pillitteri, M. Abrams and A. Hahn, “Guide to Industrial Control Systems (ICS) Security,” *NIST Special Publication 800-82,* vol. Revision 2 Initial Public Draft, 2014.

[8] National Institute of Standards and Technology, “Security and Privacy Controls for Information Systems and Organizations. NIST Special Publication 800-53,” 2020.

[9] International Electrotechnical Commission & British Standard Institute, “62443-2-1 International Standard. Industrial communication networks – Network and system security – Part 2-1: Establishing an industrial automation and control system security program,” 2020.

[10] Swedish Civil Contingencies Agency, “Guide to Increased Security in Industrial Information and Control Systems,” 2014.

[11] Ponemon Institute, “Safety, Security & Privacy in the Interconnected World of IT, OT & IIoT,” February 2019.

[12] H. Leith and J. W. Piper, “Identification and application of security measures for petrochemical industrial control systems,” *Journal of Loss Prevention in the Process Industries,* 2013.

[13] S. Holland, K. Gaston and J. Gomes, “Critical success factors for cross-functional teamwork in new product development,” *International Journal of Management Reviews,* vol. 2, no. 3, p. 231–259, 2000.

[14] B. G. Glaser and A. L. Strauss, The Discovery of Grounded Theory: Strategies for Qualitative Research, New Brunswick (U.S.A.) and London (U.K.): Aldine Transaction, 1967.

[15] R. M. Belbin, Management Teams, Why They Succeed or Fail, Oxford: Butterworth-Heinemann, 1981.

[16] J. B. Quinn, “Managing innovation: controlled chaos,” *Harvard Business Review,* vol. 63, no. 3, p. 73–84, 1985.

[17] W. E. Souder and J. D. Sherman, “Organizational design and organizational development solutions to the problem of R&D marketing integration,” *Research in Organizational Change and Development,* vol. 7, p. 181–215, 1993.

[18] T. W. Edgar and D. O. Manz, Research Methods for Cyber Security, Cambridge, USA: Elsevier, 2017.

[19] A. Galletta, Mastering the Semi-Structured Interview and Beyond: From Research Design to Analysis and Publication, New York and London: New York University Press, 2013.

[20] J. Spradley, "Asking descriptive questions," in *Qualitative Approaches to Criminal Justice*, SAGE Publications, 2002, pp. 44-61.

[21] R. Community. [Online]. Available: https://t.me/RuScadaSec.

[22] L. Johnson, A. Bunce and G. Guest, "How Many Interviews Are Enough? An Experiment with Data Saturation and Variability," *Field Methods,* vol. 18, no. 1, pp. 59-82, 2006.

[23] E. Namey, "Riddle me this: How many interviews (or focus groups) are enough?," R&E Search for Evidence, 25 April 2017. [Online]. Available: https://researchforevidence.fhi360.org/riddle-me-this-how-many-interviews-or-focus-groups-are-enough#:~:text=Since%20Guest%20et%20al.'s,interviews%20needed%20to%20reach%20saturation..

[24] M. G. Morgan , B. Fischhoff, A. Bostrom and C. J. Atman , Risk Communication: A Mental Models Approach, Cambridge University Press, 2001.

[25] J. J. Francis, M. Johnston, C. Robertson, L. Glidewell, V. Entwistle, M. P. Eccles and J. M. Grimshaw, "What is an adequate sample size? Operationalising data saturation for theory-based interview studies," *Psychology and Health Journal* , vol. 25, no. 10, pp. 1229-1245 , 2010.

[26] A. S. H. Jassawalla, "An examination of collaboration in high-technology new product development processes," *Journal of Product Innovation Management,* vol. 15, p. 237–254, 1998.

[27] Fortinet, "State of Operational Technology and Cybersecurity Report," 2019.

[28] M. Hoegl, "Smaller teams—better teamwork: How to keep project teams small," *Business Horizons,* vol. 48, no. 3, pp. 209-214, 2005.

[29] D. Tjosvold, "The dynamics of interdependence in organisations," *Human Relations,* vol. 39 (6), pp. 517-540, 1986.

[30] L. a. B. D. Gomez-Mejia, "Effectiveness of individual and aggregate compensation strategies," *Industrial Relations,* vol. 28, p. 431–445, 1989.

[31] P. Pascarella, "Compensating teams," *Across the Board,* vol. 34 (2), p. 16–22, 1997.

[32] E. J. Lerums and J. E. Dietz, "The Economics of Critical Infrastructure Controls Systems' Cyber Security," *2018 IEEE International Symposium on Technologies for Homeland Security (HST), Woburn, MA,* no. 1-9, 2018.

[33] T. Menze, "THE STATEOF INDUSTRIAL CYBERSECURITY IN THE ERA OF DIGITALIZATION," *Kaspersky,* 2020.

[34] G. a. D. J. Susman, "Development of a model for predicting design for manufacturability effectiveness," in *Integrating Design and Manufacturing for Competitive Advantage,* New York: Oxford, In Susman, G.I. (ed.), 1992.

[35] K. Jehn, “A multimethod examination of the benefits and detriments of intragroup conflict,” *Administrative Science Quarterly,* vol. 40, p. 245–282, 1995.

[36] D. a. C. D. Ancona, “Beyond boundary spanning: managing external dependence in product development teams,” *Journal of High Technology Management Research,* vol. 1 (2), p. 119–135, 1990.

[37] X. Luo, R. J. Slotegraaf and X. Pan, “Cross-Functional “Coopetition”: The Simultaneous Role of Cooperation and Competition Within Firms,” *Journal of Marketing, American Marketing Association,* vol. Vol. 70 (April 2006), no. ISSN: 0022-2429 (print), 1547-7185 (electronic), p. 67–80, 2006.

[38] S. G. Cohen and D. E. Bailey, “What Makes Teams Work: Group Effectiveness Research from the Shop FIoor to the Executive Suite,” *Journal of Management,* vol. 23, no. 3, pp. 239-290, 1997.

[39] L. E. Wood, “Semi-Structured Interviewing for User-Centered Design,” *Interactions. Association for Computing Machinery Journal,* Vols. March-April, pp. 48-61, 1997.

Appendix 1. Interview questions

#	Questions combines by topics	Questions created
1	Formal yet flexible integrative process + RQ1 question	• What are the typical projects/tasks/processes for which cross-functional teams are formed? • What are the key cybersecurity-related activities? • Should they be carefully planned or experimental?
2	Right functional mix + Clear roles and responsibilities + Team empowerment + Team tenure + RQ1 question	• What should be the functional mix / competencies? • How many people should be in the team? • How should a transition from former departments to the ICCFT look for the team members? E.g. from 20h/week to full time. • What should be the reporting structure? • How autonomous should the team be? • Is there any deadline for how long the teams should be created? Temporary/permanent?
3	Team leader selection + Team leader skills and vision + Project leader power + Senior managers as champions	• How to select an ICCFT leader? (Advised profile, skills, vision) • Project leaders are effective at lobbying for resources and protecting the team from outside interference. What could be examples of interference and lobbying? • What should be CISO's and other top management involvement for better effectiveness?
4	Training in team process skills + RQ1 question	• What kind of activities should be provided to team members, middle managers, senior managers to learn what is the experience of each of them and who knows what? • Was providing a means for growing shared understanding of the team knowledge a consideration when you formed a cross-functional team, or did you just welcome a team and gave them tasks?

5	Team co-location + Frequent, genuine communication + Team cohesiveness	• Should the team be co-located together? If yes, what are the best practices in co-location? • How often should ICCFT communicate internally? How to enable the team to communicate and prevent isolation of teams in the case of remote work? • How to ensure cohesiveness and 'groupthink in ICCFTs and how to work with it to achieve success?
6	Mechanisms to co-ordinate activities and share learning between teams + Flexibility and openness to learning/willingness to change + Training in team process skills + RQ1 question	• What education, awareness and other training should team members take? • Are there any prerequisite trainings that team members should take before starting their responsibilities?
7	Overarching team goals + Clear mission from senior management + Important, challenging task	• What is the goal of creation of cross-functional teams? • How should senior managers communicate the purpose of a cross-functional team within the organization?
8	Sharing and use of uncertain information + RQ1 question	• How to stimulate the team members to share and use uncertain information? What are the benefits for the ICCFTs? • How should teams share uncertain information?
9	Constructive conflict + Team-based rewards and recognition + Creative, integrative problem-solving + RQ1 question	• What are the typical conflicts of interest in the ICS cybersecurity cross-functional team? How are they usually resolved?
10	Boundary management	• How to make sure that the vendor relations are maintained after the creation of an ICCFT?

Appendix 2. Interview code system exported from MaxQDA

Code System	Frequency
Code System	653
Security projects, processes, activities	144
By category	108
DBs administration	2
PLC programming	2
SCADA man. upgrade	1
SIEM/security analytics	1
Prevention	3
Validation of solutions	2
Recovery	2
Enterprise soft/app	5
Risk assessments	2
Means unification	1
Remote access	3
Infrastructure	1
Anti-virus/defense	10
Threat intelligence	4
Net mon & Detection	6
SOC	8
Playbooks	10
Incident response	9
Governance	4
Maintenance	3
Compliance	5
Network administration	15
Segmentation	2
Migration	2
Network security	2
Backups	3
Processes	3
patching	3

Governance	151
Responsibility	13
Risk	2
Duties	0
Accountability	1
Reporting & Hierarchy (+)	14
Governance principles	7
Centralized	0
Decentralized	0
Umbrella	5
Local teams	1
Management people	0
CISO	29
Top management	12
Site management	7
Lead's Profile	5
Lead's tasks	1
Lobbying & Protection from interference	6
Traits	0
management skills	3
respectful	1
Improving employees	2
technical expert	8
negotiable	6
sociable	3
flexible	2
soft-skilled	2
open-minded	4
patient	1
willing to understand	7
empathetic	4
Decision-making	5
Conflicts	25
Budget	5

Common language & different priorities	7
Learning	37
Exchange knowledge	11
Site knowledge	7
Training & Education	17
Training for both or separate	2
Vendors	8
Relations	8
Changes	3
Vendor choice	4
Vulnerabilities	2
OT/IT	52
Member's traits	13
Communication	7
Co-location	7
Uncertain information	2
Shared mental model	11
Trust	7
Collaboration	5
Interesting findings	0
No right training for both	1
concepts for OT sec	1
no transparency	1
digitalization changes OT	2
decentralization	1
Not one size fit all	2
proving risks to OT	1
Lack of talents	5
when started, people are incorporated in processes	1
Cybersecurity equipment not administrated	1
Umbrella teams are needed	1
Raise industry awareness. Popularization	1
Interchangeable members	2
OT becomes IT-looking	1

OT is boring for IT	2
Success factors	0
Corp SOC for both	6
IT is winning	5
Against	3
Introduction	0
Definition	2
General experience	7
Industry	0
Power	1
Manufacturing	5
Petrochemical	2
Chemical	1
Water	2
Experience with ICCFTs	5
Management	3
Network	1
Security incidents analytics	1
Security solutions	1
Cyber defense	1
IT infrastructure	1
SOC	2
governance	2
Activities	31
People selected. Next steps.	9
Goals, purpose, strategy	18
Experimental/planned	2
Teams	103
Initiation	1
Who	0
OT (engineering)	1
Management	4
IT or IT security	4
Composition	4

Functional mix	15
Number of members	14
Competencies	16
Who to educate	4
Contractors	6
Hired to compensate	1
Transition	11
Right away	0
Gradual	3
20h/w	2
One day a week	2
Tenure	13
Perm. w/ workgroups	4
Project-based temporary	3
Permanent	6
Hourly engagement	5
Full-time	3
Part-time	2
Autonomy	4
Success factors	10
Knowledge	1
Leading role	1
Cooperation	2
Motivation	3
Bad practices	1
Ad hoc	1