

# NORCICS

SFI Norwegian Centre for  
Cybersecurity in Critical  
Sectors



## ANNUAL REPORT 2021

#### **FUNDING AGENCY**

Norges Forskningsråd

#### **RESEARCH PARTNERS**

SINTEF Energi  
SINTEF Digital  
SINTEF Manufacturing  
Norsk Regnesentral  
Universitetet i Agder

#### **INDUSTRY PARTNERS**

Elvia  
Equinor  
Helgeland Kraft  
Norsk Hydro  
Kongsberg Gruppen  
Lnett  
Mnemonic  
NC-Spectrum  
Siemens  
Yara International

#### **PUBLIC AND GOVERNMENT PARTNERS**

Oslo Politidistrikt  
Sykehuset Innlandet  
NorSIS

#### **HOST**

Norges Teknisk-Naturvitenskapelige Universitet (NTNU)

CONTENTS

Vision. . . . . 6

Objectives . . . . . 7

Reflections from the centre director . . . . . 9

Key numbers 2021 . . . . . 10

The impact of SFI NORCICS . . . . . 12

Organization. . . . . 13

    Reflections from the chair of the board . . . . . 15

    Members of the SFI NORCICS Board. . . . . 16

    NORCICS Executive Board. . . . . 17

    NORCICS General Assembly . . . . . 17

    NORCICS Scientific Management Team . . . . . 18

    Work packages . . . . . 19

        Work Package 2, Foundations. . . . . 20

        Work Package 3, Technologies, applications, and services. . . . . 21

        Work Package 4, Demonstration environments. . . . . 22

Focus areas in NORCICS . . . . . 23

Partners . . . . . 24

    Reflections from our industry partners . . . . . 25

    NORCICS research partners . . . . . 28

Cooperation in 2021 . . . . . 31

    How to bridge the valley of death?. . . . . 32

Activities and results . . . . . 33

    Tasks in NORCICS during 2021 . . . . . 33

    Spin off projects . . . . . 34

    Cooperation with other centers . . . . . 35

    Cooperation with clusters . . . . . 35

    Cooperation with catapults . . . . . 36

    Education . . . . . 36

International cooperation . . . . . 37

    The SFI NORCICS External Advisory Board (EAB) . . . . . 37

    International collaborators . . . . . 38

    International conferences. . . . . 40

    International projects . . . . . 40

Recruitment 2021. . . . . 41

    SFI NORCICS funded PhDs and PostDocs: . . . . . 41

    SFI NORCICS associate PhDs . . . . . 42

    Presentation of PhD projects . . . . . 43

Communication and dissemination. . . . . 47

Attachments. . . . . 51

    Personnel . . . . . 51

    Publications. . . . . 54

    Annual Accounts for 2021 . . . . . 57



# VISION

*Norway is among the most digitalized countries in the world. NORCICS's vision is to contribute to making Norway the most securely digitalized country in the world by improving the cybersecurity and resilience of its Critical Sectors, through research-based innovation.*

# OBJECTIVES

- NORCICS's primary objective is to enhance the capability of private and public sector stakeholders to respond to the current and future cybersecurity risks by developing, validating, and operationalizing innovative technologies within a cyber-physical security ecosystem that includes highly trained research personnel.
- The following secondary objectives will lead to the achievement of the primary objective:
  - To create new knowledge that will improve our understanding of the dynamics and interdependencies among Critical Sectors; and of cyberattacks against Cyber Physical Systems.
  - To develop, test and validate in an industrially relevant environment novel, advanced and innovative methods for preventing cyberattacks against industrial control systems in Critical Sectors.
  - To demonstrate in an industrially relevant environment efficient cybersecurity solutions for industrial control systems in Critical Sectors;
  - To develop novel methods and tools for cybersecurity training and awareness improvement.
  - To effectively transfer the knowledge created within NORCICS among its user partners and other Norwegian businesses and stakeholders.





Sokratis Katsikas

CENTRE DIRECTOR

*NORCICS will continue to strive towards contributing to making Norway the most securely digitalized country in the world by improving the cybersecurity and resilience of its Critical Sectors, through research-based innovation.*

# REFLECTIONS FROM THE CENTRE DIRECTOR

The year 2021 has been a challenging one worldwide, due to the global pandemic. Under these unprecedented conditions and continuing uncertainty, NORCICS established itself and started conducting cutting-edge research and innovation in cybersecurity, to produce new knowledge and develop solutions to real-life societal and technological problems.

During the period covered in this report, NORCICS mapped the research needs and interests of its user partners to areas which the research in the center will focus on in the coming years. Research in a number of research projects was initiated and new PhD students and postdoctoral research fellows were recruited. Moreover, NORCICS researchers started publishing their research work in high impact journals and international conference proceedings. NORCICS reached out and established or initiated collaboration with other research centers, clusters, and catapults, as well as with international collaborators. A number of national and international R&D projects and proposals resulted directly or indirectly from the work and research collaboration within the center. Additionally, NORCICS co-organized international workshops and had invited presence in a number of international scientific events.

All this would not have been achieved without the hard work and dedication of all those who are contributing to the work in NORCICS, and without the continuing encouragement and support of the NORCICS Board, the NORCICS External Advisory Board, and the leadership of the Department of Information Security and Communication Technology and of the Faculty of Information Technology and Electrical Engineering at NTNU. I am grateful and appreciative to all for adding value to the Center and for contributing decisively to its success.

Looking into the future, NORCICS will continue to strive towards contributing to making Norway the most securely digitalized country in the world by improving the cybersecurity and resilience of its Critical Sectors, through research-based innovation.

# KEY NUMBERS 2021



NORCICS PARTNERS

**19**



TOTAL FUNDING

**215 643 000  
NOK**



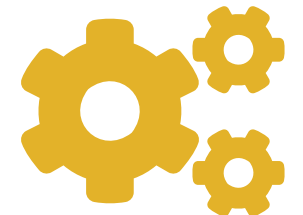
INTERNATIONAL  
PROJECTS

**10**



NEW PHDS  
AND POSTDOCS

**6**



NORCICS  
SPIN-OFF PROJECTS

**8**

# THE IMPACT OF SFI NORCICS

**The National Cybersecurity Strategy for Norway acknowledges the need to “address the (cybersecurity) challenges that will inevitably arise in conjunction with the rapid and far-reaching digitalization of Norwegian society”. Additionally, in Digital21 -Norway’s national strategy on digitalization- cybersecurity is one of the six prioritized areas.**

NORCICS contributes to all five strategic goals of the National Cybersecurity Strategy for Norway, which are 1) secure the digitalization of Norwegian companies and protect them against cyber incidents; 2) support critical societal functions with robust and reliable digital infrastructures; 3) improve cyber security competence in line with societal demands; 4) advance the ability to detect and handle cyber-attacks; and 5) strengthen the police in their ability to prevent and combat cybercrime.

NORCICS focuses on the need of organizations within Critical Sectors to engage securely with the digital transformation process. Critical Sectors are those which are critical to the nation and whose incapacity or destruction will have a debilitating impact on national security, economy, public health or safety.

The integration of operational technology (OT) with information technology (IT) and their connection to the Internet has resulted in a number of cyber vulnerabilities. Moreover, new technological advances and evolving business practices, introduce new vulnerabilities; and the increased interdependency and interconnection of cyber systems across sectors, jurisdictions, and even national borders introduces new risks. These risks affect not only the economy and the society, but also the national digital sovereignty and autonomy; therefore, they need to be mitigated for the benefit of both the economy and the society.

On the other hand, cybersecurity is an enabler of digital innovation. It supports business agility, as digital transformation requires strong cybersecurity posture; it facilitates business productivity, by diminishing the disruptive impact of cyberattacks; and it develops customer loyalty, by supporting the development and maintenance of a business’s trusted track record.

The expected long-term impact of the work within NORCICS and of its results is a safer Norwegian society with improved cybersecurity, reliability, and resilience of Critical Sectors, and with enhanced capability to combat cybercrime; these in turn increase the trust of citizens towards digitally transformed services.

# ORGANIZATION

NORCICS is hosted by the Norwegian University of Science and Technology (NTNU), under the department of Information Security and Communication Technology. The centre’s work is closely connected to the department’s Center for Cybersecurity and Information Security – a public-private and civilian-military cooperation with over 60 partners. NORCICS builds upon these relationships to provide a centre focused on innovation-driven research in cybersecurity of critical sectors.

The management of NORCICS is organized as shown below:





**Ingrid Schjøberg**  
NTNU

DEAN, FACULTY OF INFORMATION TECHNOLOGY AND ELECTRICAL ENGINEERING

*NORCICS addresses security in health systems, in energy supply, in food and materials.*

## REFLECTIONS FROM THE CHAIR OF THE BOARD

Digital technologies are necessary for efficient use of the world's resources and for implementing the UN sustainability goals. Digitalisation in both private and public sectors calls for more secure digital solutions. NORCICS addresses security in health systems, in energy supply, in food and materials. There is a strong focus on security in digital systems and towards several public sectors. NORCICS is an important centre supplying critical competence, innovations and cooperation across disciplines and sectors.

NORCICS has had a flying start with a large commitment from all partners. We really appreciate this as it is fundamental for the success of the centre. NORCICS will educate people with unique competence within cyber security applied to a number of sectors. The overall goal is that research will be taken into use among our partners.

Thank you to all our dedicated researchers and to our partners for the cooperation in 2021. We are looking forward to the continuation in 2022.

# MEMBERS OF THE SFI NORCICS BOARD



**Ingrid Schjølberg**  
NTNU  
CHAIR OF THE BOARD

SUBSTITUTE  
**Nils Kalstad**  
HEAD OF DEPARTMENT, IIK NTNU



**Erik Alexander Løkken**  
Mnemonic AS

SUBSTITUTE  
**Siri Bromander**



**Sindre Skjønsberg**  
Equinor ASA

SUBSTITUTE  
**Ove Aasen**



**Torstein Gimnes Are**  
Norsk Hydro ASA



**Arne Roar Nygård**  
Elvia AS



**Trond Austad**  
Oslo Politidistrikt

SUBSTITUTE  
**Egil Jørgen Brekke**



**Audun Solås**  
Kongsberggruppen ASA

SUBSTITUTE  
**Øystein Lintvedt**



**Dag Eirik Nordgård**  
SINTEF Energi

SUBSTITUTE  
**Oddbjørn Gjerde**

## NORCICS Executive Board

**The Board is the formal decision-making body of NORCICS. The Board is chaired by Professor Ingrid Schjølberg, the Dean of the NTNU Faculty of Information Technology and Electrical Engineering.**

Representatives of the following partners, selected according to their extent of participation to the project and on sector representativeness, make up the Board: Elvia AS, Norsk Hydro ASA, Equinor ASA, Mnemonic AS, Oslo Police District, NTNU, SINTEF Energi. In February 2021, the Board was enlarged to include a representative of Kongsberg Gruppen ASA. The Board is responsible for the overall management of the project. Board members are delegated the necessary authority to make decisions binding the partner they represent.

The Board meets every four months to monitor and direct the progress of the project.

**The tasks of the Board include:**

- 1. Ensure that the progress is maintained according to the project plan;
- 2. Review and approve financial status;
- 3. Review and approve the regular project risk assessment;
- 4. Approve and follow up the Quality Assurance Plan;
- 5. Approve and follow up the effective Innovation Management Plan;
- 6. Review the project technical results; and
- 7. Provide guidance related to a) Innovation and Exploitation potential, b) Intellectual property management, c) Dissemination and communication activities, d) Resolve potential and actual disputes between participants which cannot be resolved at lower decision levels, e) Reallocate budgets if necessary, and f) Assess ethical issues.

## NORCICS General Assembly

The General Assembly consists of one delegate from each partner. The General Assembly is responsible for setting the strategic directions of the centre; for approving the plans to implement the strategy; and for assessing the results. It meets once a year.

NORCICS Scientific Management Team

The coordination, planning, and monitoring of the research and development work in the project is performed by the NORCICS Scientific Management Team, which includes the WP leaders and is chaired by the Director. The Scientific Management Team meets weekly. The responsibility for the planning, execution, and monitoring of the work within the research activities lies with the WP Leaders.



Sokratis Katsikas

CENTRE DIRECTOR AND  
LEADER, WORK PACKAGE 6



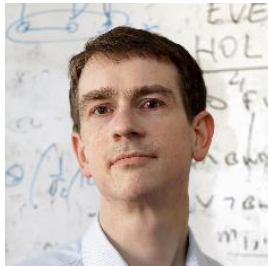
Katrin Franke

ASSOCIATE DIRECTOR AND  
LEADER, WORK PACKAGE 3



Ottar Henriksen

LEADER, WORK PACKAGE 1



Stephen Wolthusen

LEADER, WORK PACKAGE 2



Gerd Kjølle

LEADER, WORK PACKAGE 4



Vasileios Gkioulos

LEADER WORK PACKAGE 5



Hanne S. Djupdal

CENTRE COORDINATOR



Bjarne Emil Helvik

WP3, WORK PACKAGE LEADER  
(UNTIL 1 NOVEMBER 2021)

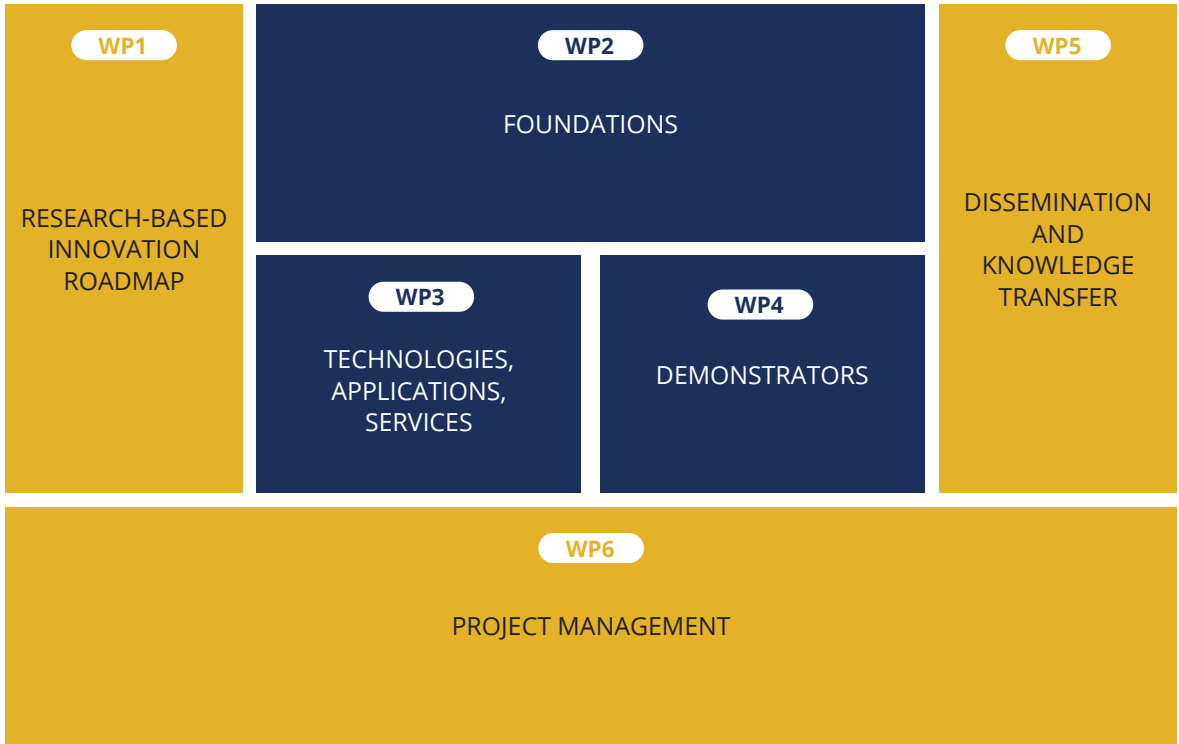
WORK PACKAGES

The work within NORCICS is organized in 6 work packages. Research is being performed within three of these (WP2, WP3, and WP4), whilst the other three (WP1, WP5, and WP6) support the research work.

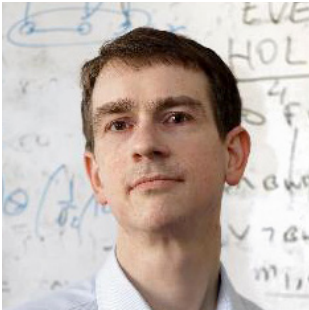
The research in each of the three research workpackages is at different Technology Readiness Levels (TRL) and is broken further down into Tasks. Specifically, research in WP2 (titled “Foundations”) is at TRL 1-3, research in WP3 (titled “Technologies, applications, services”) is at TRL 3-5, and research in WP4 (titled “Demonstration

environments”) is at TRL 5-7. WP1 is dedicated to the creation and maintenance of a dynamic research-based innovation roadmap.

The dissemination workpackage (WP5), guides all the dissemination and communication activities in NORCICS, and the project management workpackage (WP6) completes the structure of the work. All WPs span the lifetime of the project (2020-2028), whereas Tasks have durations ranging from 2 years to the project’s lifetime (in the case of demonstrators).







**Stephen Wolthusen**  
NTNU

WP2, WORK PACKAGE LEADER

DEPUTY

Vasileios Gkioulos

Work Package 2, Foundations

Attacks on critical national infrastructure could result in unacceptable damage, hence it is highly desirable to anticipate both novel attacks and their effects in an effort to enhance resilience.

Security interdependency and topology modeling are critical tools for planning, maintenance and emergency response to this effect. Within NORCICS, we will advance the state-of -the-art in this research area by developing dynamic graph models to capture infrastructure network changes in topology and the resulting impact on static and dynamic dependencies and interdependencies among inter-connected infrastructures. When modeling cyber-attacks, there is a lack of formal models for adversary placement and interaction in distributed cyber-physical systems. Existing models focus either on capturing a wide breadth of components, actors, and parameters but at a high abstraction level, or provide detailed technical mapping but in a narrow slice of a CPS. Within NORCICS, we will advance the state-of -the-art in this research area by developing formal models for adversary placement and interaction in distributed cyber-physical systems and their effects.

While a considerable amount of research activities is focused on the development and deployment of digital twins, with primary drivers within the process industries and manufacturing, there remain unexplored areas surrounding their security and resilience. These include (i) protecting digital twin configurations as these become integrated within the security/safety monitoring processes, (ii) protecting information and control flows to and from the digital twin, and (iii) exploring new attack vectors through processes that integrate digital twins and human/operators decision making during incident management. Within NORCICS, we will advance the state-of -the-art in this research area by developing mechanisms to monitor and protect Digital Twin configurations of cyber-physical systems.

Security measures must be anchored in organisations and deployed, and evidence shows that framing security using utopian and dystopian views can be counter-productive. Putting the message into stories (or frames) helps the audience to understand the potential gains (positive framing) or potential losses (negative framing). Integrating the framing process with action research or learning can provide mechanisms that help organisations and their staff to gain deep and comprehensive understanding of cyber security, integrating it into design and operational decisions. Tapping into the business model and combining it with reflection processes from action research will provide the basis for double-loop learning and continuous improvements. Within NORCICS, we will advance the state-of -the-art in this research area by developing a new methodology for organizational research based on laboratories, small experimental production lines, and simulation tools.

Tasks in work package 2:

- T2.1 Dynamic Interdependency Models for Critical Infrastructures
- T2.2 Modelling distributed subversion attacks in cyber physical systems
- T2.3 Digital Twin Security Models and Mechanisms
- T2.4 Human side of secure Industry 4.0
- T2.5 Awareness training with serious games - testing human weaknesses



**Katrin Franke**  
NTNU

WP3, WORK PACKAGE LEADER

DEPUTY

Poul Heegard



**Bjarne Helvik**  
NTNU

WP3, WORK PACKAGE LEADER (UNTIL 1 NOVEMBER 2021)

Work Package 3, Technologies, applications, and services

WP3 aims at defining and executing research, development and innovation with respect to the next generation of cybersecurity technologies, applications and services. It will provide a selection of horizontal cybersecurity technologies and solutions applicable to a range of Critical Sectors, such as novel cybersecurity monitoring, protection, intelligence and resilience. The provision shall extend the state-of-the-art, enabling innovative systems, mechanisms, and services.

**Potential innovation and outcomes: Provide novel planning, design, and validation methodologies for ensuring cybersecurity and resilience of critical sectors, e.g.:**

- Enable the secure, resilient and survivable usage of 5G, and deliver generic 5G embedded security and resilience services (virtual functions),
- Develop new analysis, planning and orchestration tools for security management in the socio-technical domain, using resilience principles,
- Deliver novel means for experimental security evaluation via the Norwegian Cyber Range and interconnected cyber-physical simulators,
- Study security anomaly “prediction”, detection and analysis to design methods for advanced machine-assisted (human) intelligence operations,
- Develop efficient mechanisms for protecting, detecting and recovery of those tens of petabytes of data used in critical sector.

Tasks in work package 3:

- T3.1 Assessing 5G and beyond as an element of critical services
- T3.2 Building cyber resilience into the critical sectors digital ecosystem
- T3.3 Cyber-physical range
- T3.4 Humanised deep Learning & Big-data Analytics
- T3.5 Codes for sub-millisecond latencies in 5G and beyond
- T3.6 Autonomous Adaptive Security for 5G-enabled IoT
- T3.7 Reverse engineering lab
- T3.8 Secure broadcasting in wireless critical systems
- T3.9 Assurance aware ontology-based scenario management framework for cyber range



**Gerd Kjølle**  
Sintef Energi

WP4, WORK PACKAGE LEADER

DEPUTY

Jørn Foros

Work Package 4, Demonstration environments

The objective of WP4 is to test and demonstrate the solutions developed within WP3 (and foundations from WP2) in laboratory and realistic environments at user partners for validation and verification. We will also define demonstration cases and use cases for identifying the needs for joint research, development, and innovation concepts to be developed in WP2 and WP3.

We will test and demonstrate the technologies from WP3 and models from WP2. The work is split into tasks addressing four critical sectors: Cyber-physical electricity system, Industry 4.0, Distributed Healthcare, and Smart districts. This will give useful knowledge about which cybersecurity technologies and solutions will work for different applications and sectors. The feedback gained through tests will be used to improve the developed technologies (WP3) and models (WP2).

The results from the demonstration and test activities will be the basis for finding the “best practice” for cybersecurity solutions. In addition to the horizontal technologies applicable to several sectors, these may need to be adapted and adjusted to the practicalities in the specific sectors.

The combination of testing and demonstration of the horizontal technologies, together with specific sector adjustments, will allow us to formulate guidelines and make recommendations for cybersecurity solutions in a variety of sectors. The first part of the activity in this WP is to develop use cases describing the tests and demonstrators at the user partners within each task.

Potential innovation and outcomes:

- Increased understanding of vulnerabilities and interdependencies in cyber-physical systems
- Improved operating procedures and under cyberattack
- Emergency preparedness, training, and handling cybersecurity in operation
- New models, tools, knowledge, input to handling cybersecurity
- Demonstrator for cybersecurity scenario testing
- Predictive analytics, real-word scenarios and relevant data sets
- Algorithms for behaviour monitoring and event detection
- New courses for broadening the awareness on security threats
- 

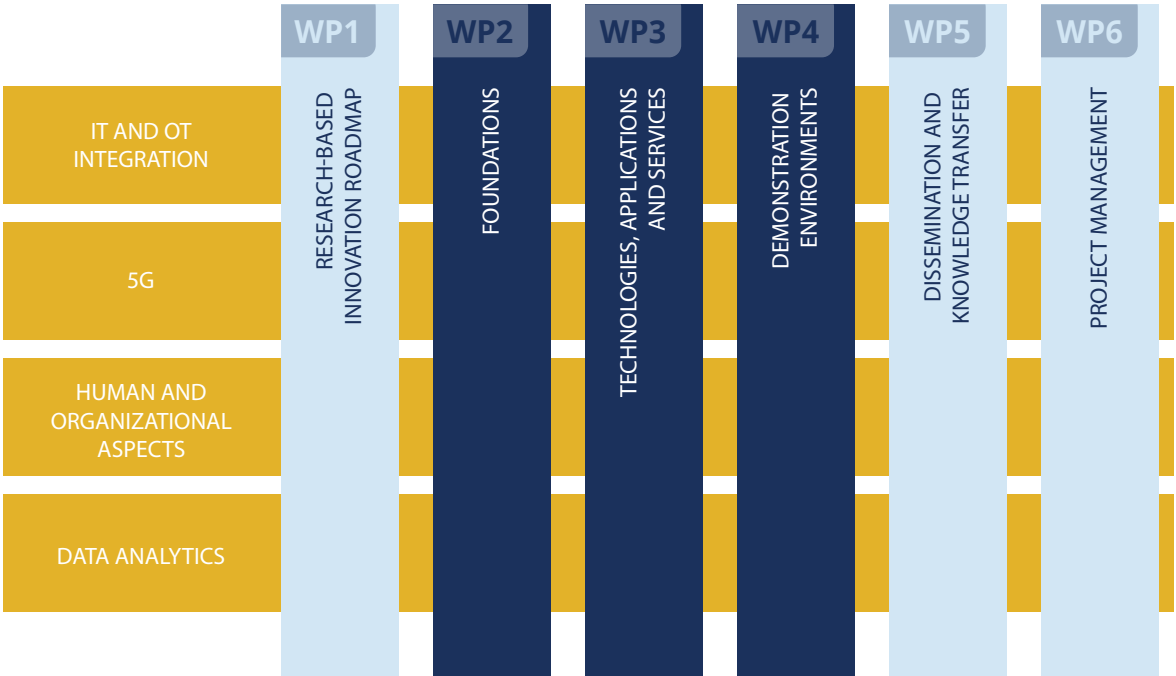
Tasks in work package 4:

- T4.1 Secure cyber-physical electricity system
- T4.2 Secure industry 4.0
- T4.3 Cybersecurity models for remote medical and care services delivery
- T4.4 Secure smart districts

FOCUS AREAS IN NORCICS

In addition to the structural organization of the research work in the workpackages as described above, research within NORCICS, guided by the user partners’ strategic innovation priorities, is organized into four cross-thematic focus areas (FAs), as shown in the figure below. Each FA addresses a range of cybersecurity challenges that arise in the process of digital transformation in critical sectors. Specifically, research in FA1 (titled “IT&OT integration”) addresses such challenges arising because of the integration of Information Technology (IT) and Operational Technology (OT) systems. Research

in FA2 (titled “5G”) addresses challenges with the secure exploitation, usage, and security of 5G and other communication technologies; cryptographic approaches are also included here. Research in FA3 (titled “Human and organizational aspects”) addresses non-technological challenges, to ensure the holistic approach to cybersecurity that NORCICS follows. Research in FA4 (titled “Data analytics”) is concerned with the efficient leveraging of data analytics to address cybersecurity challenges in the digital transformation process.







PARTNERS

The NORCICS consortium consists of 18 partners in addition to NTNU as the host institution. 5 of these are research partners – SINTEF Energi, SINTEF Digital, SINTEF Manufacturing, Norsk Regnesentral and Universitetet i Agder. 13 of them are industry partners, in both public and private sectors. SFI NORCICS also cooperates closely with NTNU CCIS, Center for Cyber and Information Security at the host institution NTNU.

The consortium members have complementary expertise that collectively covers the research areas that are relevant to NORCICS.

The NORCICS user partners can broadly be classified in three groups:

- A group of businesses/organizations with activity in diverse critical sectors - Group 1 (Elvia, Norsk Hydro, Kongsberg Gruppen, Yara International, Sykehuset Innlandet HF, Equinor, Lnett, Helgeland Kraft)
- A group of cybersecurity and/or operational technology providers – Group 2 (Mnemonic, NC-Spectrum, Siemens)
- A group of organizations dedicated to striving towards a safer society, to rising awareness and to providing advice to Norwegian citizens and enterprises concerning cyber threats, vulnerabilities and information security – Group 3 (Oslo Police District, NorSIS).

REFLECTIONS FROM OUR INDUSTRY PARTNERS

NC-Spectrum AS

**NC-Spectrum specializes in the field of cyber-security and computer networking within the Norwegian broadband and critical infrastructure sectors.**

Our main costumers are owners of critical infrastructure within electrical energy, manufacturing industry and fiber-network. Within this sector there is an ongoing rapid digitalization and convergence of IT and OT. In simpler words - critical systems are being interconnected and connected to the internet at a fast pace. This presents a wide range of exciting possibilities within Industry 4.0, smart services and efficient control and maintenance of systems.

On the other hand, this development introduces serious new vulnerabilities. Interconnected systems introduce a complex network of inter-dependencies and value-chains. It also introduces new and rapidly changing potential attack surfaces between critical infrastructure and the cyber-domain.

The owners and service providers within critical infrastructure must ensure that this development does not introduce unacceptable risks from adverse actors or system malfunction. They are rightly bound to this by law to ensure the safety of critical infrastructure like electrical energy supply for public services, businesses and everyday consumers.

How can security be ensured when the direction and impact of rapid development is unknown? There are two possible answers: Halt the technological development, or meet the need for new knowledge head on. As a partner in SFI-NORCICS we have chosen to accept the challenge by joining forces with academic, governmental and industry partners. The collaboration is necessary, not only because of the daunting challenge of bridging an ever-growing knowledge gap, but also the simple fact that the critical infrastructures we are securing is already interdependent on the security of our partners. Collaboration is the only way to achieve real cyber-security within critical infrastructure, and being an active part of R&D within the field ensures us being able to offer state-of-the art services to our customers, now and in the future.



Svein Foldøy  
BUSINESS DEVELOPMENT MANAGER



Håvard Ofte  
RESEARCH MANAGER





**Geir Kristian Lund**  
Sykehuset Innlandet HF  
PHD CANDIDATE FABL. INNOVATION  
ADVISOR, DEPARTMENT OF RESEARCH  
AND DEVELOPMENT



**Inge Harald Bolme**  
Sykehuset Innlandet HF  
CHIEF INFORMATION SECURITY OFFICER

Sykehuset Innlandet HF

**Sykehuset Innlandet HF (Innlandet Hospital Trust) operates in a sector where innovations and digitization processes meet conventional operations, old-school practice communities and many generations of organizational models.**

Over the next few years, Sykehuset Innlandet HF will adopt a multitude of new technology, implement an extensive digital platform for analyzing enormous amounts of data, and standardize existing technological solutions. Priority areas are solutions for mobility, digital solutions for home care, and technology related to the realization of a new organizational and physical structure. Information security and privacy run through all aspects of the system, and have to be integrated assets of the organization, the knowledge systems, practice and treatment. We consider our participation in NORCICS to be a very important contributor to research activities in the field of cybersecurity, resilience and infrastructure. We hope this will result in the establishing of new practices, culture and awareness for these topics, both in the existing organization and the planned, new hospital for the Innlandet area.

According to NORCICS revised proposal (2020.11.09), the centers’ primary objective is to “enhance the capability of private and public sectors stakeholders to the current and future cybersecurity risks by developing, validating and operationalizing innovative socio-technical solutions”. Sykehuset Innlandet HF is a highly complex organization operating in a highly critical sector, and thus a target for a wide range of cyberattacks. Due to this, we participate in a series of work packages and tasks in NORCICS, to participate in the research, innovation, development and demonstration of methods and tools for detection, prevention and mitigation of cyberattacks. It has also been important for our organization to involve Sykehuspartner HF, who operates as a supplier and operational managing organization for ICT programs, systems, platforms and cybersecurity on a regional level (HSØ – Health South-East).

Cybersecurity in health care is a cognitive challenge as well as a technical, and we therefore need to focus on both cultural, organizational and ICT issues in in daily operations, projects, systems and development of new organizational models. Through partnership and cooperation with the other participants in NORCICS, we hope for synergies and collaborations which will lead to the exchange and creation of knowledge, and new strategic alliances. Our hospital trust is a massive socio-technical system involving humans, machines and society, producing a great variety of tasks, operations and treatments; through NORCICS we have a unique opportunity to establish a platform for research and secure management of this complexity, and for active participation in the development of methods and tools for cybersecurity training and awareness.



**Tormod Danielsen**  
Siemens Digital Industry –  
Process Automation  
BUSINESS MANAGER



Siemens AS

Digitalization and the growing networking of machines and industrial systems also mean an increase in the risk of cyberattacks. Appropriate protective measures are imperative, especially for critical infrastructure facilities. An approach that covers all levels simultaneously – from the operational to the field level – is essential for comprehensively protecting industrial facilities against internal and external cyberattacks.

To keep pace with continuous increasing threats, companies, institutes and governments must join forces and take decisive action. This means making every effort to protect the data and assets of both individuals and businesses, prevent damage to people, businesses, and infrastructures and build a reliable basis for trust in a connected and digital world.

Siemens believes that collaboration is the best model to solve the future cyber security challenges. That’s why we are happy to be a partner in NORCICS, which brings different stakeholders together with the goal of finding solutions to common challenges, and also to be a strong voice and advocate for the importance of Industrial Cyber Security in the Norwegian Industry.



**Audun Solås**  
DIRECTOR, PROJECTS KDA BUSINESS  
SUPPORT

Kongsberg Gruppen ASA

**The Cyber threat landscape is continuously changing, new technologies and new attack vectors challenge our analysts to continuously educate and improve themselves in order to secure our business and secure our license to operate.**

In such circumstances it is very valuable for us to participate in NORCICS workshops and collaborate with the partners to exchange ideas and experiences and to find a way forward together.

To stay one step ahead of the opposition.



KONGBERG

# NORCICS RESEARCH PARTNERS

## SINTEF Energy Research



SINTEF Energy Research is an institute for applied research dedicated to creating innovative energy solutions. Security of electricity supply and smart grids (with integrated electric vehicles) are strategic areas of high priority. To enable the transition to a secure cyber-physical electricity system, cybersecurity threats, vulnerabilities and solutions need to be understood and dealt with.

SINTEF Energy Research is contributing to NORCICS with input on and competences related to power system operation as well as domain knowledge from the electric power sector, in general for activities in the SFI. They also actively participate in the scientific work according to the project description, contributing with internationally leading expertise within the power system domain, power system components, risk, vulnerability, and reliability analysis.

SINTEF Energy Research's relevant laboratory facilities at the National Smart Grid Laboratory and the SINTEF Energy Lab are made available for the demonstrators in NORCICS WP4 when relevant. Key-personnel working within NORCICS is Chief Scientist (PhD) and Centre Director of FME CINELDI Gerd Kjølle as leader of WP4,

Research Scientist (PhD) Jørn Foros as leader of task 4.1, Research Scientist (PhD) Tesfaye Amare Zerihun, Research Scientist (PhD) Santiago Sanchez Acevedo and several other highly qualified research scientists are involved. Researchers participate in WP3 and WP4, cooperating with researchers from NTNU and SINTEF Digital, and user partners in the electric power sector.

## SINTEF Digital

In NORCICS, SINTEF Digital is contributing with key resources on cyber security disciplines and resilience approaches to create a scientific and practical cyber resilience foundation that is needed to deal with the complexity of future cyber-physical infrastructures. The contribution will reflect overall strategy of integrating technical and social science perspectives and disciplines.

The key personnel participating in NORCICS from SINTEF Digital is from the department of Software Engineering, Safety and Security, belonging to the Cyber Security research group, and the Safety and Reliability research group. They bring expertise in development, testing and assessment of applied security and solutions, as well as sociotechnical approaches to cyber resilience, across the relevant critical infrastructures into this project.

Senior researcher Tor Olav Grøtan, from the department of Software Engineering, Safety and Security, is the leader of NORCICS WP 3 task 3.2 "Building cyber resilience into the critical sectors digital ecosystem".

The Safety and Reliability research group is leading and participating in many national and international research projects related to critical infrastructures and industrial safety and reliability and their digital transformations, with core competence areas in safety management, sociotechnical approaches to situated practice, resilience measurement and development, as well as emerging digital vulnerabilities of critical infrastructures. The Cyber Security research group is leading and participating in many national and international research projects, with core competency areas in secure software development, cyber-physical security solutions, cyber risk management, and cyber security incident response.

## SINTEF Manufacturing

SINTEF Manufacturing's contribution in NORCICS is facilitating the use of Norwegian Manufacturing Technology Catapult (MTNC). The plan is to use the MTNC specifically for simulation and testing within task 4.2, Secure industry 4.0. As NORCICS is still in an early phase, with 2021 only being the first full year of operation, the use of MTNC has not fully started yet and the cooperation with SINTEF Manufacturing has in 2021 been through the participation in workshops and meetings. It is expected that the cooperation and use of MTNC will intensify going forward.

## Norsk regnesentral



NR's strategic contributions and priorities are: (i) making information systems smart and trustable, adapting them to new devices and increasing their intelligence and mobility, (ii) developing advanced adaptable technologies that ensure appropriate and reliable security properties in a wide range of application areas, services linked to IoT, BigData/AI and cybersecurity, and (iii) developing and testing methods and tools for risk-based predictive analytics.

NR contributes to the following research activities in NORCICS: research-based innovation roadmap, theoretical foundations, network, and distributed systems (technologies, applications, and services), human aspects, and data security and privacy. More specifically NR leads the following tasks T2.5 (Awareness training with serious games - testing human weaknesses), T3.6 (Autonomous Adaptive Security for 5G-enabled IoT), and T3.8 (Secure broadcasting in wireless critical systems) and participates in T4.3 Cybersecurity models for remote medical and care services.

NR collaborates with NORCICS partners on organizing several international workshops in conjunction with highly reputed security conferences such as ESORICS (European Symposium on Research in Computer Security) and ARES (International Conference on Availability, Reliability and Security). These include SecHealth (Workshop on Cybersecurity in Healthcare 4.0 - 2021 & 2022),





SecIndustry Workshop on Cybersecurity in Industry 4.0 - 2022), CPS4CIP (Cyber-Physical Security for Critical Infrastructures Protection - 2021 & 2022), SecAssure 2022 (System Security Assurance).

NR also collaborates with NORCICS partners on several national and EU proposals. These include CODDECC (Cognitive Data Driven Edge-Cloud Continuum), DORIAN (Deep learning fOr cybeRsecurity In smArt environmeNts), EnvAIHealth (ENVironment meets AI towards a HEALTHier living), EU-CIP (European Knowledge Hub and Policy Testbed for Critical Infrastructure Protection), THEMIS (A European Lighthouse Community for Safe and Secure AI), ANDES (Cognitive Cloud: AI-enabled computing continuum from Cloud to Edge), DATA4SWARMS (Programming tools for decentralized intelligence and swarms), iSMART (Internet of Sustainable waste MAnagement and sorting), CybAlliance (International Alliance for Strengthening Cybersecurity and Privacy in Healthcare), ROSAIoT (Real-Time Optimal Adaptive Security Assurance For IoT), and HelDiSec (Collaborative Project on Digital Security for the Healthcare Sector).

Universitetet i Agder



Rapid urbanization makes smart city technologies more important than ever; they optimize among others the use of energy, water, transportation systems, and critical incidence and emergency services not merely as a means to achieve efficiency, but to improve the citizens' quality of life as well as to increase society's resilience.

As part of NORCICS's objectives of the development of technologies, applications, and services for improved resilience, UiA's contribution focuses on big data analytics of multi-modal information. The purpose is to improve safety and security in smart districts with a particular emphasis on content analysis in the absence of meta-data for the detection and reconstruction of abnormal activities with preventative, operational or intelligence objectives.

Our current research focuses on descriptive object identification and tracking in urban traffic. We have obtained a dataset from the 2022 AI City Challenge with contains traffic monitoring videos along with their corresponding natural language description. The technical challenge is to bridge the significant semantic gap between multi-modal vision and language models for event detection and retrieval. They have different statistical properties and aligning these different modalities is difficult. We aim to overcome this challenge by using methods such as attention mechanisms that simultaneously learn and align features in joint vision and language embedding spaces.

While video retrieval assumes that similarities in the problem space implies similarity in embedding space and vice versa, this is by no means guaranteed. We will thus probe this assumption for various feature alignment methods. Finally, we will investigate the use of mappings between visual and language embeddings which may sidestep some of the challenges of feature space alignment. The search of such mappings thru learning departs from the common practice which views video analytics and synthesis as separate pursuits: it views video retrieval and generation from descriptions as essentially equivalent tasks. We will participate in the 2022 AI Big City Challenge to evaluate our method against the state-of-the-art.

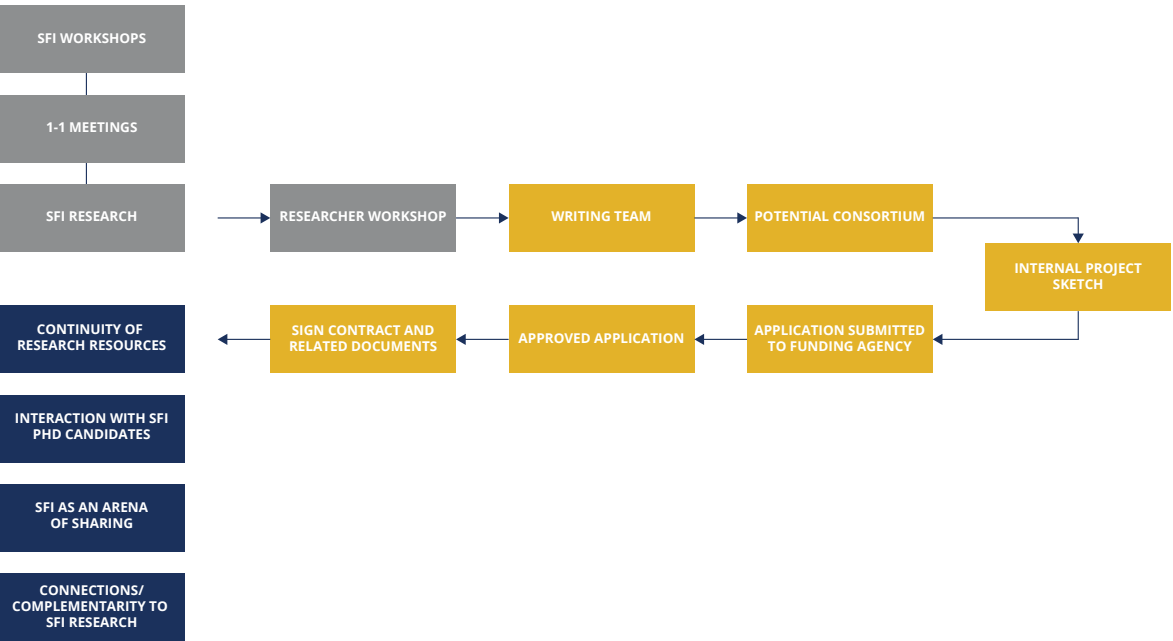
Although we are using traffic surveillance in smart cities as a use case, the methods developed in and insights gained from our research are generic and can be applied to monitoring any assets of a critical infrastructure where information with multiple modalities is available some of which may be human understandable. The NORCICS partners' ambitions and challenges are thus essential in informing our research contributions.

COOPERATION IN 2021

**SFI NORCICS has a dedicated work package for handling innovation (WP 1). The center has a large spectrum of user partners from both the private and public sector that all work actively and systematically with innovation related to the center's central research topics. In the first full year of operation it has thus been important to gain insight into the partners' innovation focus and align the center's research focus with that.**

further develop these ideas and create suggestions for concrete projects that could lead to new proposals for innovation projects to be submitted to the Norwegian Research Council or to European funding schemes.

The second workshop for all partners was conducted on December 9, 2021. The work to develop a cross-sectoral understanding between industry partners and research partners continued, to define innovation needs and understand what the current gap between the research focus and the user partners' innovation needs are. The aim has been to understand where there is need for further research on a higher technology readiness level (TRL) than what the center can contribute to through its core activities. The process to this end is shown in the figure below.

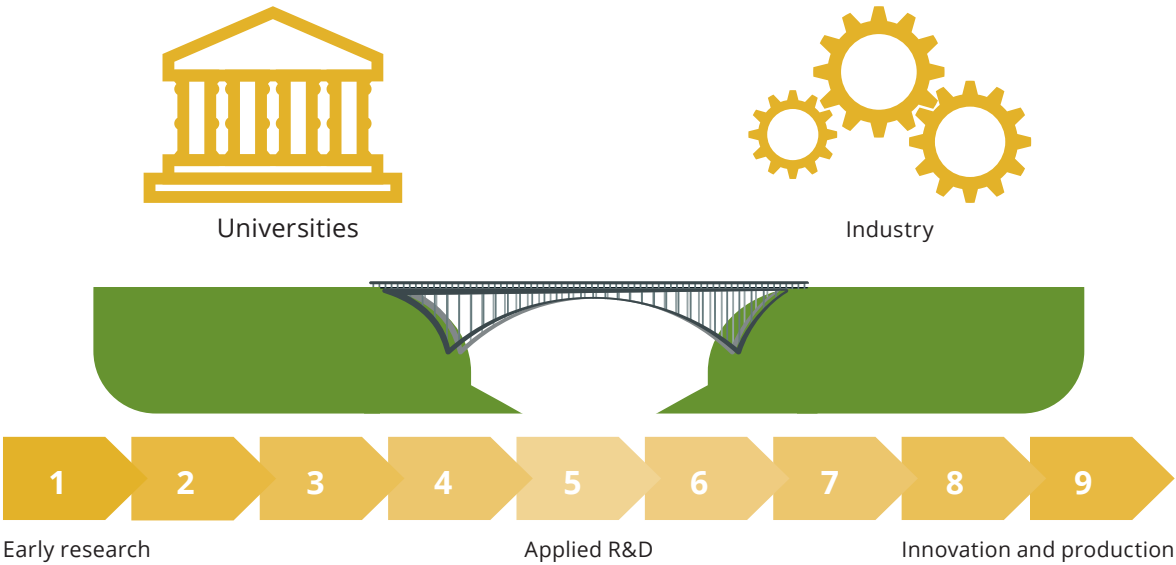


How to bridge the valley of death?

The main challenge in the cooperation between academia and industry is to bridge what we call the valley of death. The industry partners and the research partners normally have different focus on the technology readiness level (TRL) scale. The industry needs to achieve innovation and wish to utilize good academic research on TRL from 7 to 9, while the research partners have their main focus on research from TRL 1 to 4.

To bridge the valley of death, we are developing structured communication channels between all the partners to achieve common strategic views on the industrial challenges and the need for research on TRL from 1 to 7.

The different communication channels, with milestones and deliverables, are developed in our yearly work plan. One of the key deliverables is to increase the project portfolio on more applied research and development on TRL 5 to 7 between the industry partners and research partners.



ACTIVITIES AND RESULTS

Tasks in NORCICS during 2021

Task/WP#	Title	Task leader	Start - End
WP1	Research-based innovation roadmap	Ottar Henriksen (NTNU)	10.2020 – 09.2028
WP2 - T2.2	Modelling distributed subversion attacks in cyber physical systems	Stephen Wolthusen (NTNU)	01.2021(22) – 06.2025
WP2 - T2.3	Digital Twin Security Models and Mechanisms	Vasileios Gkioulos (NTNU)	02.2021(22) – 01.2025
WP2 - T2.4	Human side of secure Industry 4.0	Halvor Holtskog (NTNU)	01.2021 – 12.2023
WP2 – T2.5	Awareness training with serious games - testing human weaknesses	Ingvar Tjøstheim (NR)	01.2021 – 12.2022
WP3 – T3.1	Assessing 5G and beyond as an element of critical services	Poul E. Heegaard (NTNU)	04.2021 – 12.2025
WP3 – T3.4	Humanised deep Learning & Big-data Analytics	Katrin Franke	01.2021 – 12.2023
WP3 - T3.5	Codes for sub-millisecond latencies in 5G and beyond	Danilo Gligoroski (NTNU)	01.2021 – 12.2024
WP3 - T3.6	Autonomous Adaptive Security for 5G-enabled IoT	Habtamu Abie (NR)	01.2021 – 01.2024
WP3 - T3.7	Reverse engineering lab	Katrin Franke (NTNU)	01.2021 – 10.2023
WP3 - T3.8	Secure broadcasting in wireless critical systems	Sigurd Eskeland (NR)	01.2021 – 12.2023
WP4 – T4.1	Secure cyber-physical electricity system	Jørn Foros (SINTEF Energi)	01.2021 – 09.2028
WP4 – T4.2	Secure industry 4.0	Halvor Holtskog (NTNU)	01.2021 – 09.2028
WP4 - T4.3	Cybersecurity models for remote medical and care services delivery	Bian Yang (NTNU)	01.2021 – 09.2028
WP4 - T4.4	Secure smart districts	Katrin Franke (NTNU)	01.2021 – 09.2028
WP5	Dissemination and knowledge transfer	Vasileios Gkioulos (NTNU)	10.2020 – 09.2028
WP6	Project management	Sokratis Katsikas (NTNU)	10.2020 – 09.2028

Through 2021, NORCICS first operational year, the SFI has focused on itself; integrating the consortium and bringing the partners, which come from a variety of sectors, together; understanding the industry partners individual innovation strategies and needs; and on hiring the necessary personnel to initiate the research activities. In addition, the research partners have started the work in projects where existing personnel are involved,

and dissemination and promotion of the center and its activities has been conducted.

The close cooperation with partners and the cross sectorial focus at NORCICS have led to a number of activities and projects fully or partially developed from the work at the center already in 2021.

## Spin off projects

**The following projects and proposals have fully or partially resulted from work in SFI NORCICS in 2021:**

**Cybersecurity Barrier Management** (Secure Safety). The project will develop new knowledge, methods and guidance to secure industrial control and safety systems against cyberattacks. With several threat actor activity groups targeting the petroleum sector, the number of publicly known cyberattacks is increasing, revealing a larger threat landscape (<https://www.sintef.no/en/projects/2021/cybersecurity-barrier-management/>). The proposal was sent in to the Research Councils Petromax 2 call. The project has been approved and is receiving funding. The project partners are SINTEF Digital, NTNU IIK, Lundin Energy. The project leader is Lars Bodsberg, SINTEF Digital, and the project participants are Poul Heegaard (NTNU IIK, SFI NORCICS), PhD student, Maria Bartnes (IIK/SINTEF).

**ISMArt** (Internet of Sustainable waste Management and sorting). The Norwegian Computing center, research partner in NORCICS, is contributing in cybersecurity for ISMArt – TEKNOKONVERGENS. It is a Collaborative and Knowledge-building Collaborative Project coordinated by NTNU. The main goal is to provide an AI-powered IoT platform for sustainable waste management through boosting of sorting behavior of end-users. The objective is to increase awareness, participation, and involvement of individuals/citizens in recycling, boost recycling at the source through incentive strategy, provide optimized waste collection planning based on real-time information, and develop cybersecurity appropriate for information exchange in real-time.

**ROSAIoT** (Real-time Optimal Adaptive Security Assurance for IoT), under consortium building coordinated by NTNU and to be submitted to IKTPluss open-end call. The main goal is to develop a real-time optimal adaptive security assurance framework that provides the set of processes and practices to identify potential risks and plan to address them while reducing the operational cost of security assurance. The proposed approach will be automated, dynamic, cost-efficient and time efficient. The results will be verified and validated the use cases in the Healthcare, Smart Cities, and Smart Transportation application domains.

**HeDiSec** (Collaborative Project on Digital Security for the Healthcare Sector), under consortium building coordinated by NTNU and to be submitted as to be submitted to IKTPluss as Collaborative and Knowledge-building Project. HeDiSec will bridge the gaps between healthcare laboratories in the digital security domain by developing and validating innovative methods to provide coordinated services focus on knowledge and capacity building for Norwegian healthcare.

**Cybersecurity Academy** – Samarbeidsarena for kapasitetsløft i digital sikkerhet. The proposal was submitted to the Norwegian Research Council's call within Collaborative and Knowledge-building projects in September 2021. The project's main goal is to develop and improve the use of knowledge, competence, and research within digital security, to increase the speed and sustainability in digital innovation and through this strengthen the ICT companies, and private and public sectors in Innlandet. The initiative will also strengthen the research capacity at NTNU. Project partners are NTNU (SFI NORCICS and CCIS), Innlandet Fylkeskommune, Digital Innlandet, Manufacturing Technology Norwegian Catapult AS, Mnemonic AS, Center for Defence, Space and Security, North European Cybersecurity Cluster (NECC), KPMG AS, Total Defence Group AS, IDT Solutions AS, Thune Produkter Holding AS, Sykehuset Innlandet HF, Cyberforsvaret, Isiflo AS, NAMMO Raufoss AS, Forsvars- og sikkerhetsindustriens forening (FSI), Telenor Norge AS, Cisco Systems Norway AS. Project leader is Katrin Franke (associate director in SFI NORCICS). The proposal unfortunately did not receive funding through the Norwegian Research Council in the given round, but a process to still develop the project has been started.

**AluGreen** (Grønn plattform). The project is about going from a linear value chain to a circular value chain with verified effect by increased scrap-aluminum in the materials, processes, applications and design, to be able to develop new solutions with scrap-aluminium in large infrastructure projects, subsea cables and electric transportation. The project has a budget of 124 MNOK over 3 years. The main partners are Nexans, Statnett, Benteler, and Norsk Hydro. The project has received full financing of a postdoc position.

**Two industry PhD projects directly connected to SFI NORCICS were approved in 2021 and are receiving funding from the Norwegian Research Council:**

1. Arne Roar Nygård, Elvia AS – Reverse Engineering for verification of security in digital value chain in a critical infrastructure.
2. Kristian Andreas Kannelønning, Siemens AS - Lowering Cyber Security entry barriers for Industry 4.0 companies.

## Cooperation with other centers

**NORCICS has established a cooperation with FME Cineldi. Gerd Kjølle, leader of work package 4 in NORCICS, is the center director at FME Cineldi, and task 4.1 in NORCICS (energy demonstrator) is led by personnel also central in FME Cineldi (Jørn Foros).**

Cooperation has also been established with SFI Manufacturing. Ottar Henriksen, leader of work package 1 in NORCICS, has a close cooperation with SFI Manufacturing. Best practices from SFI Manufacturing regarding administration of innovation is being shared with NORCICS.

Cooperation with SFI NorwAI has been initiated through joint participation in the Horizon project THEMIS (A European Lighthouse Community for Safe and Secure AI). The THEMIS project was initiated by NTNU Digital and NORCICS' center director Sokratis Katsikas is leading a work package on cyber security.

Cooperation between NORCICS and SFI Autoship had already existed before both SFIs officially started operating, including through a PhD project jointly supervised by NORCICS center director Sokratis Katsikas and SFI Autoship center director Mary Ann Lundteigen.

Contact has been established and discussions on cooperation are in process with SFI C3.

The administrative coordinators and project economists at the four SFIs at NTNU's faculty of information technology and electrical engineering (IE), SFI NORCICS, SFI Autoship, SFI NorwAI and SFI CGF, cooperate closely.

The Faculty of information technology and electrical engineering (IE) at NTNU has its own innovation forum, where all leaders of innovation processes in the four new SFIs at the faculty participate. This contributes to valuable sharing of experiences across thematic areas in these SFIs. A similar forum has been established at NTNU level.

## Cooperation with clusters

**The SFI NORCICS has in many ways come out of NTNU CCIS (Center for Cyber and Information Security), <https://www.ntnu.edu/ccis/center-for-cyber-and-information-security> hosted in the same department at NTNU, and cooperates closely with this national and international cluster, which in addition to NTNU's information security environment consists of more than 50 organizations in both the private and the public sector.**

In addition, NORCICS cooperates with NCE Manufacturing/Norsk Industri, and has, among other things, contributed to the Cyber security week – Industry 4.0 in August and September 2021. Within the health sector NORCICS cooperates closely with the initiative HelselInn, which in October 2021 became a part of two national clusters appointed as test pilots within HUB-Node together with Norway Health Tech and Norwegian Smart Care Cluster (NSCC). In the region around Mjøsa, the center works with Cyberland, a regional cluster established by the Statsforvalter in Innlandet, Innlandet Fylkeskommune, the Cyber Defence, Gjøvikregionen Utvikling and Lillehammer Regionen.

Cooperation with catapults

NORCICS has initiated a cooperation with the Norwegian Manufacturing Technology Catapult (MTNC), which is closely connected to NCE Manufacturing. The plan is to use the MTNC specifically for simulation and testing within task 4.2, Secure industry 4.0.

The HelseInn Verksted for integrated health services at the NTNU Campus in Gjøvik is built on the same philosophy as the Norwegian Catapult and the plan is to be used for both simulation and testing within task 4.3, Secure Distributed Healthcare.

The Norwegian Cyber Range is also a type of catapult for testing and teaching personnel, organizations and management, and the plan is to be used for testing in task 2.4, Human and Organizational aspects of secure industry 4.0, and in task 4.1, 4.2, 4.3 and 4.4.

Education

The faculty of Economics and Management at NTNU is hosting a new master program in close collaboration with the Faculty of Information Technology and Electrical Engineering, which is the host faculty of SFI NORCICS.

The Master of Industrial Innovation and Digital Security contains three main focus areas: management and innovation, digital economy and sustainability, and digital security. The program results in 120 ETCS. The master program is a result of the collaboration in the Centre for Research-based Innovation (SFI) Norwegian Centre for Cybersecurity in Critical Sectors (SFI NORCICS).

Students with a bachelor from economics and management, logistic or informatic are qualified to apply for the program. Important challenges like sustainability, digital transformation, and cyber security at the level of society as well as company, are well covered. Management and logistic students get new insight into information security and informatic students get new insight into innovation processes and management. Both student groups will develop knowledge about circular economy, digital business models, Lean, industry 4.0/5.0, and upscaling of innovations. The combination of interdisciplinary topics is valuable for companies.

INTERNATIONAL COOPERATION

The SFI NORCICS External Advisory Board (EAB)

The research and development work in the project is supported by an international External Advisory Board (EAB), consisting of leading scientists in the fields of interest to the project, representatives of the Norwegian industry, and policy makers. The EAB provides external quality assurance to NORCICS; it convenes once every year, during the annual NORCICS workshop.

Members of the EAB

**Bente Hoff,**  
NSM, Norway

**Prof. Bruce Mork,**  
Michigan Technological University, USA

**Prof. Carmen Mas Machuca,**  
Technical University of Munich, Germany

**Em. Prof. Davydd Greenwood,**  
Cornell University, USA

**Prof. Elias Carayannis,**  
George Washington University School of Business, USA


**Janne Merete Hagen,**  
NVE, Norway


**Prof. Kai Rannenberg,**  
Goethe University, Germany


**Prof. Mauro Conti,**  
University of Padua, Italy





International collaborators


- 


**George Washington University, USA**  
Elias Carayannis
- 


**US Military Academy, USA**  
John James
- 


**University of Florida, USA**  
My Thai
- 


**Technische Universität München, Germany**  
Carmen Mas Machuca
- 


**University of Passau, Germany**  
Hermann de Meer
- 


**Telecom SudParis, France**  
Joaquin Garcia-Alfaro
- 


**DTU, Denmark**  
Weizhi Meng
- 


**Singapore University of Technology and Design**  
Jianying Zhou
- 


**New York University Abu Dhabi, UAE**  
Michail (Mihalis) Maniatakos
- 


**Polytechnique Montreal, Canada**  
Frédéric Cuppens
- 

**University of Guelph, Canada**  
Ali Deghantanha
- 

**Michigan Technological University, USA**  
Bruce Mork
- 

**University of Cagliari, Italy**  
Fabrizio Pilo
- 

**TU Hamburg, Germany**  
Dieter Gollmann
- 

**Indian Institute of Technology Kanpur, India**  
Sandeep Shukla
- 

**University of Malaga, Spain**  
Javier Lopez





International conferences

Through 2021, NORCICS was the co-organizer of three international conferences:

- 1. 7th Workshop on The Security of Industrial Control Systems & of Cyber-Physical Systems (CyberICPS 2021) In Conjunction With ESORICS 2021 (<https://www.ds.unipi.gr/cybericps2021/>)
- 2. The 2nd International Workshop on Cyber-Physical Security for Critical Infrastructures Protection (CPS4CIP 2021) Co-located with ESORICS 2021 (<https://st.fbk.eu/events/CPS4CIP2021/>)
- 3. The 1st Workshop on Cybersecurity in Healthcare 4.0 (SecHealth 2021) (<https://2021.ares-conference.eu/workshops/sechealth-2021/index.html>)

International projects

Through 2021 the following proposals were submitted to the EU HORIZON program as a result of research conducted in NORCICS:

- 1. A Systemic Approach to Collaborative Regulatory Risk Management in a Cross-Sector and Cross-Border Context (SYSTEMIC)
- 2. AI assisted buSineSs continUity and Resilience relying on AugmeNted Cybersecurity mEchanisms (ASSURANCE)
- 3. A citizens privacy enabling framework towards a fairer and more sustainable world wide web (INSPIRE)
- 4. A European Lighthouse Community for Safe and Secure AI (THEMIS)
- 5. cyBeR rESilience framework for SmarT mAnufactur-ing iNfrastrucTures (RESISTANT).
- 6. Cognitive Data Driven Edge-Cloud Continuum (COD-DECC)
- 7. Deep learning fOr cybeRsecurity In smArt environ-meNts (DORIAN)
- 8. EVNironment meets AI towards a HEALTHier living (EnAIHealth)
- 9. European Knowledge Hub and Policy Testbed for Critical Infrastructure Protection (EU-CIP)

NORCICS has also participated in the INTPART project CIRMAN.

RECRUITMENT 2021

The majority of NORCICS position announcements in 2020 and 2021 has been successful and resulted in the recruitment of several new PhD candidates and postdoctoral research fellows who started their work in NORCICS during 2021. In addition to NORCICS' funded PhDs and postdoctoral researchers, several PhDs either hired in other positions at NTNU or as public or industry PhDs have also started their work in 2021 and cooperate closely with NORCICS.

SFI NORCICS funded PhDs and PostDocs:



Arvind Sharma

Task 3.7, Reverse engineering lab



Sahana Sridhar

Task 3.5, Sub-millisecond control layer codes for 5G and beyond



Arnstein Vestad

Task 4.3, Cybersecurity models for remote medical and care services delivery



Julie Langedahl Leirmo

Task 2.4, Human side of secure industry 4.0



Karoline Anna Benum Engh

Task 4.2, Secure industry 4.0



Touseef Sadiq

Task 3.4, Humanized Deep learning & Big data analytics



SFI NORCICS associate PhDs

Alvhild Skjelvik	NTNU (CCIS)	Cybersecurity models and mechanisms for remote medical and care services
Andre Jung Waltoft-Olsen	Statnett, Norges Forskningsråd	Hardware Reverse Engineering
An Thi Nguyen	Norges Forskningsråd, NTNU	Scalable and robust instance search
Are Fjermeros	Sykehuset Innlandet	Hvilke mekanismer fremmer kontinuerlig forbedring av arbeidsprosesser i en sykehusenhet?
Arne Roar Nygård	Elvia AS, Norges Forskningsråd	Reverse Engineering for verification of security in digital value chain in a critical infrastructure
Geir Kristian Lund	Sykehuset Innlandet, Norges Forskningsråd	Faster Assembly by Learning (FABL)
Kristian Kannelønning	Siemens AS, Norges Forskningsråd	Lowering Cyber Security entry barriers for Industry 4.0 companies
Håvard Ofte	NC-Spectrum, Norges Forskningsråd	Situation Awareness in Security Operations Centers

PRESENTATION OF PHD PROJECTS

PhD in task 2.4, Human side of secure industry 4.0



**Julie Leirmo**  
Department of Industrial Economics and Technology Management, NTNU  
DOCTORAL STUDENT

**Julie started her PhD in March 2021, and her PhD-project will be for four years with 25% duty work. Her position is at the Department of Industrial Economics and Technology Management at NTNU in Gjøvik, and the PhD is a part of NORCICS Task 2.4, Human Side of Secure Industry 4.0.**

Cybersecurity is often seen as something purely technical, and therefore a lot of efforts towards defence against cyberthreats has been on technical solutions. However, Julie looks at cybersecurity with a socio-technical view, with the weight on the social and human side of cybersecurity. When humans have been considered in cybersecurity, they have often been seen as a liability and the ‘weakest link’. However, we might be better off shifting this view where humans are seen as an asset where we utilise the human side of cybersecurity in the fight against cybercriminals.

In her PhD project, she is interested in how cybersecurity may influence innovation performance in organisations when the human side of security is considered to a larger degree. She wants to investigate how the inclusion of humans in cybersecurity may affect innovation performance when some of the cybersecurity responsibility is spread throughout the organisations and with people in different parts and levels in the organisation. However, when using the words ‘human aspect’ in this project, it is important to note that it does not refer to an individual level, but the human aspect on an organisational- and value chain level.

Her study aims to provide a better understanding of how the human aspect plays a role in cybersecurity and to provide knowledge on how cybersecurity influences innovation performance with respect to how the organisation view cybersecurity. To investigate this, she plans to collect data through in-depth interviews with relevant organisations, as well as surveys. The next phase of her PhD project will therefore be to get in contact with potential organisations and to plan the data collection in more detail, such as to develop the interview guide. The collected data will be analysed to see how different views of the human side of cybersecurity within the organisations may affect innovation performance.



**Sahana Sridhar**  
Department of Information  
Security and Communication  
Technology, NTNU  
DOCTORAL STUDENT

**PhD in task 3.5, Sub-millisecond control layer codes for 5G and beyond**

**Sahana started her PhD in September 2021, and her PhD-project will be for four years with 25% duty work. Her position is at the Department of Information Security and Communication Technology at NTNU in Trondheim, and the PhD is a part of NORCICS Task 3.5, Codes for sub-millisecond latencies in 5G and beyond.**

Communication is an extremely essential aspect of our lives, more so, with the rapid advancements made in each generation of the wireless networks. With 5G and beyond networks, we see newer human-centric business value creation and use cases. These ‘SMART’ networks aim to provide or support use cases such as telemedicine, remote surgery, disaster management and so on. At the heart of these promises, are the crucial aspects of high throughput and high reliability. In order to be able to realize these promises, one of the solutions would be to explore newer families of codes or improve existing codes to reduce the structural and processing delays in communication. Thus, Sahana looks at the algorithmic side of improving the throughput and reliability requirements of future networks.

In her PhD project, she is interested in how the existing capacity-achieving coding schemes can be improved by using the fundamentals of Information Theory. She also wants to come up with newer methods of channel coding and possibly newer families of codes that can help achieve the goals. There are a few such interesting and promising codes that achieve rates close to capacity, such as LDPC codes, Polar codes and BCH codes. For Beyond 5G (B5G) networks, the control layer needs to have short codes  $\approx 40$ -128 bits, to be able to provide latencies below 1 ms. The challenge is to accomplish similar error-correction performance at short to moderate block lengths owing to Shannon’s Coding Theorem (1948) applicable to sufficiently longer block lengths.

Her research project aims to provide innovative solutions to fulfil the requirements of B5G networks and contribute to the development of next generation networks happening every decade. In the next phase of her project, she aims to explore and possibly incorporate machine learning tools for optimization of the decoding algorithms. Additionally, owing to her background in information security, her project will also focus on the security and privacy aspects of encoding/decoding in future networks.



**Touseef Sadiq**  
Department of Information and  
communication technology, UiA  
DOCTORAL STUDENT

**Task 3.4, Humanized Deep learning & Big data analytics**

**Touseef started his PhD position with NORCICS in September 2021. His position is with the NORCICS research partner University of Agder.**

As part of NORCICS’s objectives of the development of technologies, applications, and services for improved resilience, UiA’s contribution focuses on big data analytics of multi-modal information. The purpose is to improve safety and security in smart districts with a particular emphasis on content analysis in the absence of metadata for the detection and reconstruction of abnormal activities with preventative, operational or intelligence objectives.

Rapid urbanization makes smart city technologies more important than ever; they optimize among others the use of energy, water, transportation systems, and critical incidence and emergency services not merely to achieve efficiency, but to improve the citizens’ quality of life as well as to increase society’s resilience. Integration of multi modal data sources in urban environment advantages rooted in multimodal perception and information retrieval from the surrounding environments. The purpose of his PhD project is to investigate deep multimodalities for descriptive object identification and tracking in urban environments.

The research aims to investigate deep multimodal techniques for descriptive object identification and retrieval in urban environment. They have obtained a dataset from AI City Challenge 2022 which contains traffic monitoring videos along corresponding natural language description. The goal is to bridge the significant semantic gap between these two modalities (vision/language) as they have different statistical properties i.e., language has symbolic representation while video concepts are represented by signals. For the purpose of this research the following three research findings are most relevant:

- To determine the relationships and correspondences between vision and language modalities by aligning them into a common embedding space.
- To investigate and observe the underlying assumption of distance consistency should be maintained both in input and corresponding latent embedded space.
- Learning of mappings between visual and language embeddings heterogeneous data for their correspondences and semantic relationships.

We are aiming to honing a well-tuned attention mechanism which enables to perceive and focus on relevant semantics to correlate visual context and language content in joint embedding spaces. Considering the assumption, the distance between the original and transformed space implies similar; we will investigate how often this assumption is true in our feature alignment methods. Finally, we will investigate the use of mappings between visual and language embeddings which may sidestep some of the challenges of feature space alignment. At the end we will select our cross-modal tasks involving visual and text to test the generality of our claims. We solicit our contribution towards AI City Challenge 2022 to push our research and development in the intelligent traffic system.



Arne Roar Nygård  
Elvia AS

INDUSTRY PHD

Cyber Security Expertise in Reverse Engineering

– An initiative to Strengthen the Norwegian Power Grid Industry

**Arne Roar Nygård** from **Elvia**, one of the major electrical grid companies in Norway, is contributing to this work by doing an industrial PhD with funding from the National Research Council. Elvia is also a partner in NORCICS and the PhD work is related to the NORCICS work plan.

The PhD project of Arne Roar Nygård with the title **“Reverse Engineering for verification of security in digital value chains in a critical infrastructure”** focuses on security in the digital value chain from digital sensors in the power infrastructure to the HMI of the operating control system (SCADA). Specifically, it examines how cyber security can be ensured in a digital value chain with equipment from different vendors, and how it can be ensured that “maps and terrain always match.” This includes a focus on implementation (people), process and technology. Long supply chains with components from different manufacturers require a new approach and methods to ensure the security required in critical infrastructure. These issues are well described in Olav Lysne’s book “The Huawei and Snowden Questions” [ISBN: 978-3-319-74949-5].

The PhD project will help Elvia, the power industry and other Norwegian critical infrastructure as well as authorities to verify the security of products currently being used without us knowing the vulnerabilities. This is a competence that is lacking in Norway today.

The first year of the PhD project is now fulfilled and the plan for the next three years is to contribute to active research in the area of cybersecurity in digital supply chains. The primary objective of the research project is to develop a framework for systematically using tools, techniques, methods, and procedures to secure the digital value chain from supply and throughout the component’s lifetime in the power infrastructure. In parallel with the PhD program, the plan is to build up a reverse engineering laboratory and capacity at NTNU Gjøvik in close collaboration with NORCICS, national agencies and other stakeholders. The PhD-program and the laboratory infrastructure will form the basis for developing a sustainable capacity within reverse engineering in Norway.

COMMUNICATION AND DISSEMINATION

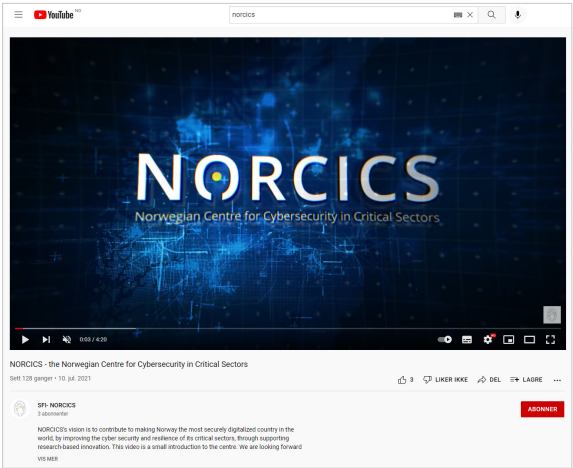
NORCICS have made efforts in 2021 to build up plans and routines for communication and dissemination work. During the year, the centre has been able to set up and start social media channels, a newsletter, and been part of articles in the media on topics relevant to digital security. NORCICS also hosted the centre’s first annual conference, in addition to being co-hosts of several international conferences and workshops.

Further details of NORCICS’ communication and dissemination work is described in an annual Communication Plan and Communication Report.

NORCICS video

The production of a video giving a introductory view into the NORCICS project has been completed and published on the center’s social media channels in 2021.

Videos giving short insight into each work package and task are being produced and will be released in 2022.



Blog posts

A plan for monthly blog posts focusing on selected topics across the project focus areas, or alternatively on recent incidents was established. We have published the blog posts on the project’s social media and for the first months they focused on communicating the project objectives. Blog posts describing the general project narrative were published, as well as posts describing activities and goals of work packages 2 and 3.

### About the SFI-NORCICS - The Norwegian Centre for Cybersecurity in Critical Sectors

Published on May 13, 2021

SFI Norwegian Centre for Cybersecurity in Critical Sectors

SFI-NORCICS .  
Our vision is to contribute to making Norway the most securely digitalized country in the world by improving the cybersecurity and resilience of her CI.

4 articles

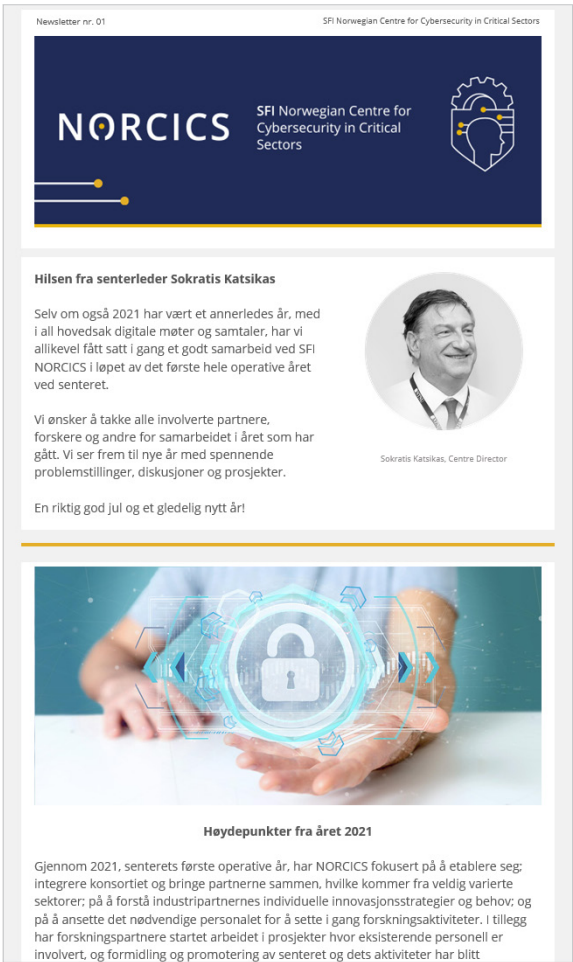
[Following](#)

Research and development in the area of security and resilience of Critical Sectors (CRISec) is paramount to enhancing the country’s cyber security posture and the Norwegian businesses’ capability to innovate. NORCICS is the Norwegian centre for research-based innovation with the overarching objective to develop innovative cybersecurity solutions at varying technology readiness levels within a dynamically evolving cyber-physical security ecosystem. We achieve this by focusing on long-term research and close alliances between research-intensive enterprises and prominent research groups in academia.



Newsletter

The first NORCICS newsletter was sent out in December 2021. The plan is to publish a quarterly newsletter to update partners, and anyone who wishes to subscribe, about the activities going on in NORCICS.



First annual conference

The first SFI NORCICS annual conference was conducted on December 8th 2021. The conference was open to invited guests, consisting of partners, partners of partners, and other relevant stakeholders.

The conference unfortunately had to be fully digital, due to the covid restrictions at the time. It was conducted in Zoom.

The feedback from the event was generally very positive. At most there were about 120 attendees present in the Zoom meeting at the same time, and at least 156 different people were at some point in the Zoom meeting.

Internal partner workshops

Two internal partner workshops were conducted during 2021. One in June and one in December. Unfortunately, both had to be fully digital. The plan for the coming years is to arrange three partner workshops through the year, where some may be hosted by alternating partner organizations to create more ownership and cooperation.

In the media

Mentions of SFI NORCICS in the media during 2021:

Article at Næringsliv Norge, [“NTNU er ledende på informasjonssikkerhet”](#)



Article at Næringsliv Norge and in Aftenposten print version, [«Verdensledende på digital sikkerhet»](#)



Other events NORCICS was a part of

Co-host of the conference “Policing in Smart Cities”, Oslo.

Co-host of the conference “7th Workshop on The Security of Industrial Control Systems & of Cyber-Physical Systems”.

Co-host of the conference “The 1st Workshop on Cybersecurity in Healthcare 4.0 (SecHealth 2021).

Co-host of the conference “The 2nd International Workshop on Cyber-Physical Security for Critical Infrastructures Protection (CPS4CIP 2021)”



# ATTACHMENTS

## Personnel

### Key Researchers

Name	Institution	Main research area
Sokratis Katsikas	NTNU	Critical Infrastructure Security and Resilience
Katrin Franke	NTNU	Digital Forensics; Computational Intelligence; AI in Forensics
Vasileios Gkioulos	NTNU	Critical Infrastructure Security and Resilience
Stephen Wolthusen	NTNU	Critical Infrastructure Security and Resilience
Bjarne Emil Helvik	NTNU	Dependability of ICT services
Ottar Henriksen	NTNU	Industrial economics and technology management
Halvor Holtskog	NTNU	Industrial economics and technology management
Bian Yang	NTNU	Health informatics and security; Privacy enhancing technologies and biometrics
Poul E. Heegaard	NTNU	Security, Robustness, and Performance in Communication Systems
Lasse Øverlier	NTNU	Information security and privacy, Content-based multimedia analytics
Danilo Gligoroski	NTNU	Information Security and Cryptography
Basel Katt	NTNU	Security assurance and evaluation, Cyber Ranges and Security edu. and training
Geir Olav Dyrkolbotn	NTNU	Cyber Intelligence, Cyber tactics, and Reverse engineering
Gerd Kjølle	SINTEF Energi	Security of electricity supply
Jørn Foros	SINTEF Energi	Security of electricity supply
Tesfaye Zerihun	SINTEF Energi	Security of electricity supply
Tor Olav Grøtan	SINTEF Digital	Critical Infrastructure Security and Resilience

Stefan Lindskog	SINTEF Digital	Security in Industrial Control Systems
Ravishankar Borgaonkar	SINTEF Digital	Security in critical com.infrastructure (mobile communication 4G/5G/Nødnett)
Gaute Knutstad	SINTEF Manufacturing	
Habtamu Abie	Norsk Regnesentral	Adaptive Security, Trust, Privacy, Risk Management, Distributed Object Computing
Svetlana Boudko	Norsk Regnesentral	Privacy-preserving AI for Cybersecurity
Ingvar Tjøstheim	Norsk Regnesentral	Risk and risk assessment. Privacy. Serious games technology. Test-methods
Sigurd Eskeland	Norsk Regnesentral	Information security and Cryptographic protocols
Thor Kristoffersen	Norsk Regnesentral	Visual systems, Distribution systems
Christian Omlin	UiA	Artificial Intelligence and Machine learning

Postdoctoral researchers with financial support from the Centre budget

Name	Nationality	Period	Sex M/F	Topic
Arvind Sharma	Indian	01.10.21 – 30.09.23	M	Task 3.7, Reverse engi- neering lab

PhD students with financial support from the Centre budget

Name	Nationality	Period	Sex M/F	Topic
Sahana Sridhar	Indian	15.09.21 – 14.09.24	F	Task 3.5, Sub-millisecond control layer codes for 5G and beyond
Arnstein Vestad	Norwegian	01.09.21 – 30.08.24	M	Task 4.3, Cybersecurity models for remote medical and care services delivery
Julie Langedahl Leirmo	Norwegian	15.03.21 – 14.03.24	F	Task 2.4, Human side of secure industry 4.0
Karoline Anna Benum Engh	Norwegian	06.04.21 – 05.04.24	F	Task 4.2, Secure industry 4.0
Touseef Sadiq	Indian	15.09.21 – 14.09.24	M	Task 3.4, Humanized Deep learning & Big data analytics

PhD students working on projects in the center with financial support from other sources

Name	Funding	Nationality	Period	Sex M/F	Topic
Alvhild Skjelvik	NTNU (CCIS)	Norwegian	10.08.2021 – 09.08.2024	F	Cybersecurity models and mechanisms for remote medical and care services
Andre Jung Waltoft-Olsen	Statnett, Norges Forskningsråd	Norwegian	01.12.2020 – 01.01.2025	M	Hardware Reverse Engineering
An Thi Nguyen	NTNU, Norges Forskningsråd	Norwegian	16.08.2021 – 16.08.2025	F	Scalable and robust instance search
Are Fjermeros	Sykehuset Innlandet	Norwegian	01.02.2020 – 31.01.2024	M	Hvilke mekanismer fremmer kontinuerlig forbedring av arbeidsprosesser i en sykehusenhet?
Arne Roar Nygård	Elvia AS, Norges Forskningsråd	Norwegian	01.01.2021 – 31.12.2024	M	Reverse Engineering for verification of security in digital value chain in a critical infrastructure
Geir Kristian Lund	Sykehuset Innlandet, Norges Forskningsråd	Norwegian	01.01.2021 – 31.12.2024	M	Faster Assembly by Learning (FAbL)

Kristian Kannelønning	Siemens AS, Norges Forskningsråd	Norwegian	01.04.2021 – 31.07.2025	M	Lowering Cyber Security entry barriers for Industry 4.0 companies
-----------------------	----------------------------------	-----------	-------------------------	---	---

# PUBLICATIONS

## Academic literature review:

1. **Pirbhulal, Sandeep; Gkioulos, Vasileios; Katsikas, Sokratis.** A Systematic Literature Review on RAMS analysis for critical infrastructures protection. International Journal of Critical Infrastructure Protection 2021 ;VAVis.L\_Volum 33. NTNU

## Academic chapters/articles/Conference papers:

1. **Boudko, Svetlana; Abie, Habtamu; Nigussie, Ethiopia; Savola, Reijo.** Towards Federated Learning-based Collaborative Adaptive Cybersecurity for Multi-microgrids. I: Proceedings of the 18th International Conference on Wireless Networks and Mobile Systems. SciTePress 2021 VAVis.L\_Isbn 978-989-758-529-6. VAVis.T\_SideForkortelse83-90. NR

## Academic articles:

1. **Radoglou-Grammatikis, Panagiotis; Sargiannidis, Panagiotis; Dalamagkas, Christos; Spyridis, Yannis; Lagkas, Thomas; Efstathopoulos, Georgios; Sesis, Achilleas; Labrador Pavon, Ignacio; Trapero Burgos, Ruben; Diaz, Rodrigo; Sargiannidis, Antonios; Papamartzivanos, Dimitris; Menesidou, Sofia Anna; Ledakis, Giannis; Pasias, Achilleas; Kotsiopoulos, Thanasis; Drosou, Anastasios; Mavropoulos, Orestis; Colet Subirachs, Alba; Paradell Sola, Pol; Domínguez-García, Jose Luis; Escalante, Marisa; Martin Alberto, Molinuevo; Caracuel, Benito; Ramos, Francisco; Gkioulos, Vasileios; Katsikas, Sokratis; Bolstad, Hans Christian; Archer, Dan-Eric; Paunovic, Nikola; Gallart, Ramon; Rokkas, Theodoros; Arce, Alicia.** SDN-Based Resilient Smart Grid: The SDN-micro-SENSE Architecture. Digital 2021 ;VAVis.L\_Volum 1.(4) VAVis.T\_SideForkortelse173-187. ENERGISINT NTNU
2. **Pirbhulal, Sandeep; Gkioulos, Vasileios; Katsikas, Sokratis.** Towards Integration of Security and Safety Measures for Critical Infrastructures Based on Bayesian Networks and Graph Theory: A Systematic Literature Review. Signals 2021 ;VAVis.L\_Volum 2.(4) VAVis.T\_SideForkortelse771-802. NTNU, NR

3. **Kavallieratos, Georgios; Spathoulas, Georgios; Katsikas, Sokratis.** Cyber Risk Propagation and Optimal Selection of Cybersecurity Controls for Complex Cyberphysical Systems. Sensors 2021 ;VAVis.L\_Volum 21.(5).NTNU
4. **Goudosis, Athanasios; Katsikas, Sokratis. Aribc:** Online reporting based on identity-based cryptography. Future Internet 2021 ;VAVis.L\_Volum 13.(2) VAVis.T\_SideForkortelse1-17. NTNU
5. **Chowdhury, Nabin; Katsikas, Sokratis; Gkioulos, Vasileios.** Modeling Effective Cybersecurity Training Frameworks: a Delphi Method-based Study. Computers & Security 2021 ;VAVis.L\_Volum 113. NTNU
6. **Amro, Ahmed Walid; Gkioulos, Vasileios; Katsikas, Sokratis.** Communication architecture for autonomous passenger ship. Proceedings of the Institution of Mechanical Engineers. Part O, Journal of risk and reliability 2021. NTNU
7. **Akbarzadeh, Aida; Katsikas, Sokratis.** Identifying and Analyzing Dependencies in and among Complex Cyber Physical Systems. Sensors 2021 ;VAVis.L\_Volum 21.(5).NTNU
8. **Pandey, Pankaj; Katsikas, Sokratis.** The Future of Money: Central Bank Issued Electronic Money. I: Advances in Core Computer Science-Based Technologies. Springer 2021 VAVis.L\_Isbn 9783030411985. NTNU
9. **Eskeland, Sigurd.** Broadcast encryption. Oslo: Norsk Regnesentral 2021 13 VAVis.T\_SideForkortelse NR-notat (DART/07/21). NR

## Publications in media:

1. **Katsikas, Sokratis.** NTNU er ledende på informasjonssikkerhet. Magazine article 2021
2. **Katsikas, Sokratis.** Verdensledende på digital sikkerhet. Magazine article 2021.



## Presentations:

1. **Henriksen, Ottar.** SFI NORCICS- orientering om prosjektet. Styremøte i Helsetjenestens Driftsorganisasjon (HDO); 2021-09-30. NTNU
2. **Henriksen, Ottar.** SFI Norcics rolle i digitalisering av helsetjenestene. HelseInn; 2021-10-01. NTNU
3. **Henriksen, Ottar.** SFI NORCICS rolle i Helseinn klynga-og mulig samarbeid med SFI C3. Drøfting av samarbeid; 2021-11-12. NTNU
4. **Henriksen, Ottar.** SFI NORCICS rolle i innovasjonsøkosystemet. RSHU workshop; 2021-11-04. NTNU
5. **Henriksen, Ottar.** SFI NORCICS rolle i utvikling av nytt innovasjonsprosjekt. Utvikling av forskningsrådssøknad i pilot helse; 2021-05-02 - 2021-09-15. NTNU
6. **Katsikas, Sokratis.** Addressing the cybersecurity needs of critical sectors through research-based innovation. Norsk-tysk fagarrangement om samfunnssikkerhet: Digital sikkerhet | Forebygging og beredskap ved naturhendelser; 2021-11-30 - 2021-11-30. NTNU
7. **Katsikas, Sokratis.** Cross-sectoral and Industry-research Collaboration and Partnerships to Improve InfoSec in the Critical Sectors. 90 Minutes CISO Episode 3: Sustainable Cyber Trust: CISOs Creating Trust with Data & Collaboration; 2021-10-13 - 2021-10-13. NTNU
8. **Katsikas, Sokratis.** Cyber-physical systems for smart cities: cybersecurity and privacy challenges. Policing in smart cities; 2021-11-18 - 2021-11-19. NTNU
9. **Katsikas, Sokratis.** Cyber-physical systems for smart cities: cybersecurity and privacy challenges of the digital government. International Conference on Theory and Practice of Electronic Governance; 2021-10-05 - 2021-10-08. NTNU
10. **Katsikas, Sokratis.** Cyber-physical systems for smart cities: cybersecurity and privacy challenges of the digital government. International Conference on Theory and Practice of Electronic Governance; 2021-10-05 - 2021-10-08. NTNU
11. **Katsikas, Sokratis.** Industry-Academia-Research collaboration for innovation. 1st Athens Space & Satellite Industry Summit; 2021-07-07 - 2021-07-08. NTNU
12. **Katsikas, Sokratis.** Industry-research collaboration and partnerships to improve infosec in the critical sectors. CYNET CSIRT Conference 2021; 2021-12-07 - 2021- 12-07. NTNU
13. **Katsikas, Sokratis.** (In)Secure digital transformation of the industry. 1st Digital Enterprise Transformation Conference; 2021-06-01 - 2021-06-02. NTNU
14. **Katsikas, Sokratis.** Integrating IT and OT: Security challenges in Industry 4.0. CriM 2021 Cyber Security Seminar and Workshops; 2021-11-09 - 2021-11-11. NTNU
15. **Katsikas, Sokratis.** International trends / Roadmap for cybersecurity and Industri 4.0. Cybersikkerhetsuka - Industri 4.0; 2021-08-30 - 2021-09-02. NTNU
16. **Katsikas, Sokratis.** Norsk senter for cybersikkerhet i kritiske sektorer – NORCICS. NOKIOS 2021 – Norsk konferanse for IKT i offentlig sektor; 2021-10-26 - 2021-10-28. NTNU
17. **Katsikas, Sokratis.** Oh! We have been attacked. What now?. Cybersikkerhetsuka - Industri 4.0; 2021-08-30 - 2021-09-02. NTNU
18. **Katsikas, Sokratis.** Research challenges in cybersecurity. Forskningsdagene på NTNU i Gjøvik; 2021-09-22 - 2021-10-03. NTNU
19. **Katsikas, Sokratis.** Securing critical infrastructure in the age of digitization. 2nd Middle East Cybersecurity Forum; 2021-09-13 - 2021-09-14. NTNU
20. **Katsikas, Sokratis.** Security of Cyber Physical Systems: Trends and Challenges. EESTech Challenge Patras; 2021-03-27 - 2021-03-27. NTNU
21. **Katsikas, Sokratis.** Security of Cyber Physical Systems: Trends and Challenges. University of Patras Computer Engineering & Informatics Department Lecture series; 2021-03-05 - 2021-03-05. NTNU
22. **Katsikas, Sokratis.** SFI NORCICS: Addressing cybersecurity challenges when integrating IT and OT. NEK Cybersikkerhetskonferanse 2021; 2021-10-21 - 2021-10-21. NTNU
23. **Katsikas, Sokratis.** SFI: Norwegian Centre for Cybersecurity in Critical Sectors. The 1st Workshop on Cybersecurity in Healthcare 4.0 (SecHealth 2021); 2021-08-18- 2021-08-18. NTNU
24. **Katsikas, Sokratis.** SFI Norwegian Centre for Cybersecurity in Critical Sectors (NORCICS). NTNU CCIS Partnerkonferansen; 2021-11-25 - 2021-11-25. NTNU
25. **Katsikas, Sokratis.** SFI: Norwegian Centre for Cybersecurity in Critical Sectors (Norsk senter for cybersikkerhet i kritiske samfunnsfunksjoner). NCSC partnere foredrag; 2021-06-15 - 2021-06-15. NTNU
26. **Katsikas, Sokratis; Gkioulos, Vasileios.** Cybersecurity research as an instrument for value creation. Challenges and opportunities for the Norwegian industry.. Cybersecurity: En dramatisk voksende trussel, og verre vil det bli - eller?; 2021-11-18 - 2021-



- 11-18. NTNU
27. **Kjølle, Gerd Hovin.** Utfordringer framover og forskningsbehov for kraftbransjen innen cybersikkerhet. Fagseminar om cybersikkerhet i kraftsektoren; 2021-11-03 -2021-11-03. ENERGISINT
28. **Nygård, Arne Roar.** Hvordan kan forskning bidra til verdiskapning. Sikkerhet i digitale verdikjeder. Fagdag om cybersecurity i kraftsektoren; 2021-11-03. NTNU
29. **Nygård, Arne Roar.** Reverse Engineering for verification of security in digital value chains in a critical infrastructure. ECODIS Workshop; 2021-03-12. NTNU
30. **Nygård, Arne Roar.** Sikkerhet i Digitale Verdikjeder. KOTE årsmøte; 2021-11-11 - 2021-11-11. NTNU
31. **Nygård, Arne Roar.** Sikkerhet i Digitale Verdikjeder. Sikring av IKT- og driftssystemer i kraftsektoren; 2021-11-15 - 2021-11-16. NTNU

Conferences and workshops:

1. NORCICS Workshop 17 June 2021. NORCICS Partner Workshop.
2. NORCICS Workshop 09 December 2021. NORCICS Partner Workshop.
3. NORCICS Conference 08 December 2021. NORCICS Annual Conference.
4. Franke, Katrin. Policing in Smart Cities Conference 18 – 19 November 2021. NORCICS Co-host of conference.
5. Katsikas, Sokratis. The 2nd International Workshop on Cyber-Physical Security for Critical Infrastructures Protection (CPS4CIP 2021). NORCICS Co-host of conference.
6. Katsikas, Sokratis. The 1st Workshop on Cybersecurity in Healthcare 4.0 (SecHealth 2021). NORCICS Co-host of conference.
7. Katsikas, Sokratis. 7th Workshop on The Security of Industrial Control Systems & of Cyber-Physical Systems. NORCICS Co-host of conference.

# ANNUAL ACCOUNTS FOR 2021



Funding	Amount	Costs	Amount
The Research Council	6112	The Host Institution NTNU	7105
The Host Institution (NTNU)	5412	Research Partners	4335
Research Partners		Enterprise partners	1005
Enterprise partners*	2400	Public partners	1479
Public partners		Equipment	
* Enterprise partners			
Kongsberg Gruppen ASA**	400		
Equinor ASA**	500		
NC-Spectrum AS**	100		
Norsk Hydro ASA**	600		
Helgeland kraft AS	200		
Lnett AS	200		
Elvia AS	250		
Yara International ASA	150		

\*\* Kongsberg Gruppen ASA, Equinor ASA, NC-Spectrum AS, and Norsk Hydro ASA also includes the amount of funding from the year 2020.