NORCICS SFI Norwegian Centre for Cybersecurity in Critical Sectors

NESIOT

3rd NESIOT Annual Conference on Resilience by Design in Secure IT-OT Integration

Venue: Clarion Hotel The Hub, Biskop Gunnerus Gate 0155, Oslo
Date: 11 February 2026
Time: 09:00-17:00

Objectives: The 3rd NESIOT Annual Conference will bring together stakeholders from industry, academia, and government to advance "Resilience by Design" approaches for secure IT-OT integration across systems and supply chains, embedding robustness, adaptability, and rapid recovery capabilities into architectures and operations so that critical services and their dependent supply networks can withstand, absorb, and quickly recover from cyber disruptions and evolving threats. This event serves as a platform for stakeholders of the Norwegian IT-OT ecosystem to learn new knowledge and skills, share ideas and experiences, engage in debates, present research results, and expand networking opportunities. By fostering collaboration across all sectors, the conference will strengthen partnerships and promote the exchange of best practices for resilient IT-OT integration.

Program

Time	Topics Title	Chair & Speakers
09:00 – 09:15	**Welcome Coffee:** Networking opportunities	Chair: Sandeep Pirbhulal and Habtamu Abie, NR, Speakers: Wolfgang Leister, NR and Sokratis Katsikas, NTNU, NORCICS Director
09:15-09:30	**Introduction** to NESIOT and Spin-off ResCri	Chair: Sandeep Pirbhulal, NR
09:30 – 10:15	**Opening Keynote:** Resilience-by-Design: Shaping the Future of Secure IT-OT Integration (Plenary session with Q&A)	Chair : Sokratis Katsikas, NTNU, NORCICS Director Speaker: Jo De Vliegher, Client Partner, ISTARI Global Limited
10:15-11:15	**Track 1:** Foundations of Resilience-by-Design, Principles and frameworks Standards and best practices	Chair : Sokratis Katsikas, NTNU, NORCICS Director • Raymond Andre Hagen, Senior Cyber Security Advisor at the Norwegian Digitalisation Agency, Understanding

Time	Topics Title	Chair & Speakers
	(Panel discussion and Q&A)	APT Defense Through Expert Eyes: A Critical Exploration of Perceived Needs and Gaps • Kristian Andreas Kannelønning, Siemens, Deployment of Cybersecurity Controls in the Norwegian Industry 4.0 • Audun Scheide, Omny, Collective Defence by Design: Building Resilient IT-OT Security Together
11:15-11:30	**Networking Break**	
11:30 – 12:30	**Track 2:** Secure IT-OT Architectures Designing secure and resilient architectures Protocols, interoperability, and supply chain security (Case studies and Q&A)	Chair: Habtamu Abie, Norsk Regnesentral Speakers: • Krisztian Mitrik, Senior Cyber Security Continuous Improvement Manager, Norsk Hydro, From Logs to Insight: Designing for Adversary Detection • Michael Golding, Cyber Domain Architecture Lead, Yara International Enterprise IT, Supply Chain facets and managing the IT-OT risk • Inge Kampenes, CEO Naoris Consulting NOR, Collective Cyber Defence-post-quantum resilience in all infrastructures
12:30 – 13:30	**Lunch and Networking, Matchmaking Mixer**	
13:30-15:00	**Track 3:** IT-OT Case Studies & Real-World Applications Industry and government presentations Lessons learned and practical insights (Panel discussion and Q&A)	Chair: Sandeep Pirbhulal Speakers: • Runar Brekke, Cyber Security Manager - 3rd party risk, Norsk Hydro, "**TPRM - Human vs AI**" - Could we automate away humans? • Bjørn Ihler, CEO & Founder, Revontulet, Monitoring of Threats Against Civilian & Critical Infrastructure • Håvard J. Ofte, Research Manager, NC-Spectrum, Changing demands and regulations regarding physical security of IT-OT in the power sector. • Siv Hilde Houmb (PhD), Senior Cyber Security Advisor Houmb AS, Professor II Norwegian Cyber Defence Academy, OT cyber security in Practice - experiences from Renewable and Oil & Gas
15:00 – 15:20	**Networking Break**	
15:20-16:00	**Track 4:** IT-OT Supply Chain Resilience Collaborative strategies and compliance for resilient IT-OT and Open forum for stakeholder feedback and future collaboration (Interactive roundtable and Q&A)	Chair: Habtamu Abie Panellists: • Antonio.Courbassier, Norsk Hydro (TBC) • Alexander Mollan, Braekhus (TBC) • Raymond Andre Hagen, Digidir (TBC) • Christian A. Haukaas, VentureNet • Sandeep Pirbhulal, NR
16:00 – 16:05	**Closing remarks and Wrap-up** *Networking opportunity, and steps forward.*	Speakers: Habtamu Abie, NR Sokratis Katsikas, NTNU, NORCICS Director

Speakers:

Krisztián Mitrik, Norsk Hydro
Title: From Logs to Insight: Designing for Adversary Detection
Abstract: Effective cyber defense depends on collecting the right logs for the right reasons. This presentation breaks down how logging architectures are designed to detect adversary techniques, the common mistakes that lead to blind spots, and how security teams balance coverage, cost, and operational complexity to achieve measurable outcomes.

Runar Brekke, Cyber Security Manager - 3rd party risk, Norsk Hydro,
Title: "TPRM - Human vs AI" - Could we automate away humans?
Abstract: A look at how Third-Party Risk Management is evolving as IT and OT systems increasingly converge. The session highlights how human judgement and AI-driven automation should/could complement each other to strengthen supply-chain security across modern digital ecosystems.

Audun Scheide, Omny
Title: Collective Defence by Design: Building Resilient IT-OT Security Together
Abstract: This talk explores why "Resilience by Design" in IT-OT environments cannot be achieved by technology or individual organizations alone, but must emerge through deliberate cross-sector collaboration between industry, academia, vendors, and government. Drawing on the perspective of a software company working closely with anchor clients and industry groups in critical infrastructure, the presentation highlights key integration challenges and makes a call for stakeholders to lean in early to co-create secure, resilient, and sovereign IT-OT solutions in an increasingly geopolitical threat landscape.

Inge Kampenes, CEO Naoris Consulting NOR
Title: Collective Cyber Defence-post-quantum resilience in all infrastructures.
Abstract: Collective Cyber Defence reframes security from isolated controls to shared, continuously verified trust across IT-OT infrastructures. This talk explores how post quantum-resilient, decentralized architectures can embed resilience by design - enabling critical infrastructure and supply chains to withstand, adapt to, and rapidly recover from cyber disruption. Practical examples from ongoing cooperations illustrate how collective security can be operationalised at scale.

Bjørn Ihler, CEO & Founder, Revontulet
Title: Monitoring of Threats Against Civilian & Critical Infrastructure
Abstract: In an increasingly complex global threat landscape, we see escalating threats and attacks targeting critical and civilian infrastructure. This directly affects our access to electricity, clean water, transit and logistics networks, oil and gas, and other critical components of a functioning society. In tandem with increasing threats, we see growing safety and security requirements and demands placed on infrastructure providers and industry by government and regulatory bodies. This is part of a broader, more inclusive approach to the role of the civilian sector intended to increase our capacity for defense and resilience in peacetime, crisis, and conflict.
While infrastructure providers and industry face increased requirements and pressure on their security roles, they often operate with significant intelligence blind spots. This makes it challenging to take proactive and adequate measures to defend against attacks. This is not made easier by global government spending cuts, which lead to inadequate data on threats, attacks, and vulnerabilities, nor by law enforcement and national security agencies that often fail to collaborate effectively and share intelligence with the private and civilian sectors.
To fill this gap, we work with the private and civilian sectors to monitor geopolitical risks, threats posed by global terrorist networks, private military companies, and organized crime networks, which at times act as non-state actors and at times on behalf of national governments.
In this presentation, we draw on real-world intelligence data and case studies on threats facing service and infrastructure providers to frame a discussion of the security threats to civilian and critical

infrastructure providers and the steps that can be taken to identify and mitigate risks before harm occurs.

Håvard J. Ofte, Research Manager, NC-Spectrum
Title: Changing demands and regulations regarding physical security of IT-OT in the power sector.
Abstract: The physical security of IT-OT installations in the Norwegian power sector is challenged by the new geopolitical landscape. Risk assessments may soon need to include war-like scenarios and physical sabotage. How can the actors in the power sector respond to these challenges and meet the demands from coming regulations.

Siv Hilde Houmb (PhD), Senior Cyber Security Advisor Houmb AS, Professor II Norwegian Cyber Defence Academy
Title: OT cyber security in Practice - experiences from Renewable and Oil & Gas
Abstract: IEC 62443 and other international standards, EU directives and national regulation for Operational Technology (OT) systems is not necessarily straight forward to implement in practice. The presentation will provide examples from ongoing projects within renewable and oil & gas sector and shed light on how to manage OT cyber security in practice.

Raymond Andre Hagen, Senior Cyber Security Advisor, Norwegian Digitalisation Agency
Bio: Raymond Andre Hagen is a Senior Cyber Security Advisor at the Norwegian Digitalisation Agency and is working on a PHD thesis at NTNU about protection against advance cyber threat actors.
Title: Understanding APT Defense Through Expert Eyes: A Critical Exploration of Perceived Needs and Gaps
Abstract: Based on focused interviews with cyber security experts with experience with incident response and APT defence we investigate what are the perceived needs, and how the perceived need aligns with the specific need for an effective APT defence.

Kristian Andreas Kannelønning, Siemens
Title: Deployment of Cybersecurity Controls in the Norwegian Industry 4.0
Abstract: Cybersecurity threats against industry are rising, and attacks on cyber-physical systems can have severe consequences for people, the environment, and organizations. This paper presents results from a survey examining security measures implemented in Norwegian industry. Based on the NIST "Guide to Operational Technology," the survey included 70 questions assessing deployed security controls. Findings show an average implementation level of 63%, with 53% of organizations using 60% or more of the recommended controls