Norwegian Ecosystem for Secure IT-OT Integration (NESIOT)
NGINO Meeting, SINTEF Oslo

Habtamu Abie Norwegian Computing Center
Tuesday 29. November 2022
SFI NORCICS (Norwegian Centre for Cybersecurity in Critical Sectors) : Synopsis

- Funding: 214,519 kNOK over 8 years (2020-2028)
- Research Council of Norway under the Centres for Research-based Innovation scheme (SFI)

19 partners
- Research: NTNU, SINTEF Energy, SINTEF Digital, NR, UiA
- Technology providers: Mnemonic, Siemens, SINTEF Manufacturing
- Organizations for safer society: Oslo Police District, NorSIS (?)

- International partners: More than 15 partners
Vision

• Contribute to making Norway the most securely digitalized country in the world
  • by improving the cyber security and resilience of its critical sectors
  • through supporting research-based innovation

• Enhance the capability of private and public sector stakeholders
  • respond to the current and future cyber-security risks
  • by developing, validating, and operationalizing innovative socio-technical solutions

Objectives

➢ Create new knowledge
  • improve our understanding of the dynamics and interdependencies among CrSec, and of cyberattacks against CPS

➢ Develop, test and validate
  • novel, advanced and innovative methods for preventing cyberattacks against industrial control systems in CrSec

➢ Demonstrate
  • efficient cybersecurity solutions for industrial control systems in CrSec

➢ Develop novel methods and tools
  • cyber security training and awareness improvement

➢ Effectively transfer knowledge
  • among NORCICS user partners and other Norwegian businesses and stakeholders
Goals of Focus Areas

- Four focus areas: IT-OT Integration, 5G, Human Aspects, Data Analytics

- Ensuring coherence and complementarity
- Avoiding overlaps between tasks
- Maximizing potential to develop synergies
- Strengthening collaboration between partners
- Encouraging spinoff innovation projects
The modern technological advancement is mainly based on new paradigms such as AI, IIoT, 5G, Digital Twins, Augmented Reality, Cognitive/Cloud/Edge computing, which involve heterogeneous networks where Information Technologies (IT) merge with the Operational Technologies (OT).

This IT and OT integration allows maximization, optimization and customization of relevant tasks, and provides a wide range of functional services for better critical sectors, economy and society [1,2]. This convergence is however leading to new challenges in cybersecurity.

- Recent survey (Sophos, May 2022): 66% hit by ransomware in the last year, 61% attacks resulted in data encryption, 69% increase in volume of cyber attacks, highest across all sectors, 67% increase in complexity of cyber attacks, highest across all sectors, 59% increase in impact of cyber attacks, second-highest across all sectors.

The cybersecurity of IT-OT integration under the following 4 pillars:

- **New Research-based Innovation**
  - Identify the needs for new innovations and knowledge

- **Analysis Capability**
  - Enhance analytical capability to identify gaps in existing research and solutions with innovation potential

- **Ecosystem**
  - Build a vibrant ecosystem of stakeholders around IT-OT integration to provide sustainability, security, safety, etc.

- **Amplify**
  - Maximize the impact of IT-OT integration activities
IT-OT Integration Pillars (1/4)

Pillar I: New Research-based Innovations

- Unified modelling of IT-OT for unified visibility
- Enhanced cybersecurity decision-making automation
- Real-time automated data collection and sharing
- Secure supply chain management
- Dynamic risks, vulnerabilities and threats
IT-OT Integration Pillars (2/4)

Pillar II: Analysis Capability

- AI and Data analytics
- State-of-the-art and beyond
- Risks, vulnerabilities and threats
- Complimentary, overlaps and synergies with other tasks
IT-OT Integration Pillars (3/4)

Pillar III: Ecosystem

- Strengthening collaborative between partners and beyond

- Multiple stakeholders: sensor/device manufactures, telecoms operations, cloud and data analysis solution providers, industrial system operators, etc.

- Enabling technologies and the application of those technologies

- Collaboration between partners through secure IT-OT Integration - Forging stronger partnerships to magnify IT-OT cybersecurity knowledge
IT-OT Integration Pillars (4/4)

Pillar IV: Amplify

- Maximize the innovation, analysis and ecosystem for enhancing cybersecurity in secure IT-OT integration

- Spinoff innovation projects, synergies, exploitation and dissemination

- Magnify cybersecurity knowledge circulation and innovative ideas and products, leading to even more secure and safe IT-OT environments
Main goal
• to create synergies and foster emerging solutions for secure IT-OT Integration via cross-sectors collaboration and innovation

Objectives
• Strengthen collaboration between NORCICS partners and beyond through secure IT-OT Integration
• Achieve secure digitalization of industry through IT-OT integration
• Close the IT-OT cybersecurity vulnerability gap
• Increase unified visibility of secure IT-OT integration
• Provide matchmaking for both national and international project spin-offs
• Organize yearly national conference/workshop, involving both Norwegian policy makers, regulators, standard bodies, industry and academic, practitioners, and representatives from the research council of Norway
• Organize bi-annually meetings

NESIOT (Norwegian Ecosystem for Secure IT-OT Integration)
NESIOT Current Partners

- **NORCICS partners**
  - NTNU, NR, SINTEF, Elvia AS, Equinor ASA, Siemens AS

- **Cross-sectors**
  - Simula, IFE
  - City of Oslo
    - Agency for Improvement and Development
    - Stovner District
    - Agency for Water and Wastewater Services
    - Oslobygg
    - Department of Finance

- **Norwegian H2020 projects**
  - FINSEC (NR), CyberSec4Europe (NTNU), STOP-IT (SINTEF), CONCORDIA (OsloMet)

- **Norwegian CERTS/CSERTs**
  - KraftCERT/InfraCERT, Telenor CERT(?), Equinor CSIRT

- **Norwegian certification authorities and security evaluation facilities**
  - Nemko System Sikkerhet AS, Norconsult ITSEF

- **Norwegian Regulators, Standards and Policies**
  - Petroleumsstilsynet, NVE, NVE-RME, NEK

- **Waiting for confirmation from 20 partners**

The cybersecurity of IT-OT integration under the following 4 pillars:

- **New Research-based Innovation**
  - Identify the needs for new innovations and knowledge
  - Enhance analytical capability to identify gaps in existing research and solutions with innovation potential

- **Ecosystem (NESIOT)**
  - Build a vibrant ecosystem of stakeholders around IT-OT integration to provide sustainability, security, etc.

- **Ecosystem**
  - Maximize the impact of IT-OT integration activities

- **Amplify**
  - • Amplify

12
NESIOT for NGI: Moral

NESIOT

- forge stronger partnerships to magnify IT-OT cybersecurity knowledge circulation and innovative ideas and products, leading to even more secure and safe IT-OT environments

Contribute to NGI

- 5G, IoT, AI Analytics, Digital Twins, Automated Cybersecurity, Cognition
Thank you!

Contact: Habtamu Abie, Norwegian Computing Center
Email: abie@nr.no