

TALLINN UNIVERSITY OF TECHNOLOGY
School of Information Technologies

Vladyslava Shekula 245132IVCM

Improving the Security of Industrial Communication Protocols in Operational Technology (OT) Manufacturing Environments

Master's thesis

Supervisor: Aleksi Oskar Johannes
Kajander

PhD

Co-supervisor: Anastasiya Kornitska

Tallinn 2026

TALLINNA TEHNIKAÜLIKOOL
Infotehnoloogia teaduskond

Vladyslava Shekula 245132IVCM

**Tööstuslike kommunikatsiooniprotokollide
turvalisuse parandamine operatiivtehnoloogia
(OT) tootmiskeskondades**

Magistritöö

Juhendaja: Aleksi Oskar Johannes
Kajander

PhD

Kaasjuhendaja: Anastasiya Kornitska

Tallinn 2026

Author's declaration of originality

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

Author: Vladyslava Shekula

10.04.2026

Abstract

Operational Technology (OT) environments in manufacturing rely on various communication protocols to exchange data between production machines, controllers, supporting equipment, and supervisory systems. Many of these protocols were originally designed for isolated industrial networks and prioritised functionality, interoperability, and performance rather than security. As manufacturing systems become increasingly interconnected and integrated with enterprise and cloud environments, insecure deployment and configuration of protocols introduce significant risks.

Manufacturing sites commonly operate in diverse environments where legacy and modern protocols coexist. However, protocol configuration decisions are often driven by vendor defaults, compatibility constraints, or performance requirements rather than by a structured security-oriented approach. This can result in inconsistent implementations and increased exposure to vulnerabilities due to weak or insecure configurations.

This thesis evaluates the security properties, configuration approaches, and practical limitations of commonly used industrial communication protocols within a real OT manufacturing environment. Based on this analysis, it proposes a structured approach for secure protocol configuration and use.

The procedures provide practical guidance for securely configuring protocols such as Modbus TCP, OPC DA, OPC UA, and MQTT, considering their functional roles, deployment context, operational requirements, and security constraints. The goal is to support secure and consistent protocol deployment in manufacturing environments where availability, safety, and resilience are critical.

This thesis is written in English and is 96 pages long, including 7 chapters.

Lühikokkuvõte

Tööstuslike kommunikatsiooniprotokollide turvalisuse parandamine OT-tootmiskeskondades

Tootmistööstuses kasutatavad operatsioonitehnoloogia (OT) keskkonnad tuginevad mitmesugustele sideprotokollidele andmete vahetamiseks tootmismasinate, kontrolleri, tugiseadmete ja järelevalvesüsteemide vahel. Paljud neist protokollidest olid algselt loodud isoleeritud tööstusvõrkude jaoks ning seadsid esikohale funktsionaalsuse, koostalitlusvõime ja jõudluse, mitte turvalisuse. Kuna tootmissüsteemid muutuvad üha enam omavahel ühendatud ja integreeritud ettevõtte- ja pilvekeskkondadega, tekitab protokollide ebaturvaline juurutamine ja konfigureerimine olulisi riske.

Tootmiskohad tegutsevad tavaliselt erinevates keskkondades, kus eksisteerivad koos nii vanad kui ka kaasaegsed protokollid. Protokollide konfiguratsiooniotsused põhinevad aga sageli tarnija vaikesätetel, ühilduvuspiirangutel või jõudlusnõuetel, mitte struktureeritud turvalisusele orienteeritud lähenemisviisil. See võib kaasa tuua ebajärjekindlaid rakendusi ja suurenenud haavatavuste riski nõrkade või ebaturvaliste konfiguratsioonide tõttu.

Käesolev väitekiri hindab reaalses OT tootmiskeskonnas tavaliselt kasutatavate tööstuslike sideprotokollide turvaomadusi, konfiguratsioonilähenemisi ja praktilisi piiranguid. Selle analüüsi põhjal pakub käesolev väitekiri välja struktureeritud lähenemisviisi protokollide turvaliseks konfigureerimiseks ja kasutamiseks. Raamistik pakub praktilisi juhiseid selliste protokollide nagu Modbus TCP, OPC DA, OPC UA ja MQTT turvaliseks konfigureerimiseks, arvestades nende funktsionaalseid rolle, juurutamise konteksti, töökoormusi ja turvapiiranguid. Eesmärk on toetada turvalist ja järjepidevat protokollide juurutamist tootmiskeskondades, kus kättesaadavus, ohutus ja vastupidavus on kriitilise tähtsusega.

Lõputöö on kirjutatud inglise keeles ning sisaldab teksti 96 leheküljel, 7 peatükki.