Timo Saarinen

Teollisuus 4.0: OPC UA ja tietoturvallisuus

Metropolia Ammattikorkeakoulu

Insinööri (AMK)

Sähkö- ja automaatiotekniikka

Insinöörityö

23.4.2023

Tiivistelmä

Tekijä:	Timo Saarinen
Otsikko:	Teollisuus 4.0: OPC UA ja tietoturvallisuus
Sivumäärä:	23 sivua
Aika:	23.4.2023
Tutkinto:	Insinööri (AMK)
Tutkinto-ohjelma:	Sähkö- ja automaatiotekniikka
Ammatillinen pääaine:	Automaatiotekniikka
Ohjaajat:	Lehtori Matti Välikylä

Teknologian kehitys on tuonut uusia mahdollisuuksia ja haasteita teollisuudelle ja yrityksille. Toiminta on entistä riippuvaisempaa digitaaliteknologiasta ja palveluista, mikä tuo uusia haasteita tietoturvassa, varsinkin automaatioverkoissa. Vertikaalisen integraation myötä kyseeseen tulevat myös yritysten muut verkot.

Tässä työssä käydään läpi teollisuuden kehitystä nykyhetkeen saakka, käydään läpi OPC UA -standardin kehitystä, ominaisuuksia ja roolia teollisuudessa sekä siihen sisällytettyä tietoturvaa. Tietoturvaa tarkastellaan myös hyökkääjän näkökulmasta ja avataan hyökkäyksen kulkua ja tavoitteita eri vaiheissa sekä vastatoimia.

Käymme läpi myös suosituksia ja hyviä tapoja yritysten tietoturvallisuuden toteuttamiseksi. Näihin kuuluvat myös vastatoimet, joita yritys voi käyttää hyökkäyksen toteuttamisen vaikeuttamiseen tai estämiseen.

Avainsanat: Teollisuus 4.0, Kyberturvallisuus, Tietoturvallisuus, OPC, OPC UA, IIoT

Abstract

Author:	Timo Saarinen
Title:	Industry 4.0: OPC UA and Information security
Number of Pages:	23 pages
Date:	23 April 2023
Degree:	Bachelor of Engineering
Degree Programme:	Electrical and automation engineering
Professional Major:	Automation engineering
Supervisors:	Matti Välikylä, Senior Lecturer

The purpose of this work was to explore the new opportunities and challenges that the development of technology has provided for industry and companies. Companies and industrial processes are more dependent on digital technology and services, which brings new challenges for information security especially for automation networks, but vertical integration other networks in industry have also come into question.

In this thesis, the development of industry up to the present day and the role, significance, and features of the OPC UA standard, as well as its built-in security features are reviewed. Information security is also examined from the attacker's point of view and the different stages, course and objectives of an attack are discussed, as well as countermeasures against these attacks.

The result is a review of vectors of attack against companies and systems, and the measures companies can deploy to counter or mitigate the effect of these attacks. Recommendations and good practices for proper implementation of information security for companies are also proposed.

Keywords: Industry 4.0, InfoSec, Cyber security, OPC, OPC UA, IIoT

Sisällys

Lyhenteet

OPC UA: *Open Platform Communications Unified Architecture*. Avoimen lähdekoodin IEC62541-standardi tiedonsiirtoon teollisuuden antureiden, laitteiden ja pilvisovellusten väliseen kommunikaatioon.

DMZ: Demilitarisoitu alue. Tietoturvassa tarkoittaa fyysistä tai loogista aliverkkoa, joka erottaa lähiverkon muista ei-luotettavista verkoista.

IoT: *Internet of Things.* Esineiden internet, fyysisten laitteiden väliset datayhteydet.

IIoT: *Industrial Internet of Things.* Teollinen esineiden internet, sama kuin IoT mutta teollisessa valmistuksessa.

ERP: *Enterprise Resource Planning.* ”Liiketoimintaprosessin hallintatyökaluja, joita voidaan käyttää hallitsemaan informaatiota koko organisaation laajuudella”.

SCADA: *Supervisory Control and Data Acquisition.* Tietokoneella toteutettu graafinen valvomo-ohjelmisto.

COM: *Component Object Model.* Microsoftin binääriliitäntästandardi ohjelmistokomponenteille. Mahdollistaa prosessien välisten viestintäobjektien luomisen useilla ohjelmointikielillä.

DCOM: *Distributed Component Object Model.* COM-standardin laajennus verkkoon kytkettyjen tietokoneiden ohjelmistokomponenttien väliseen viestintään.

SOA: *Service-oriented Architecture.* Ohjelmistotekniikan suunnittelutapa, jossa eri prosessit ja toiminnot toimivat itsenäisinä palveluina.

SaaS: *Software as a Service.* Ohjelmiston jakelumalli, jossa ohjelmistoa ylläpidetään pilvipalveluna.

XML: *Extensible Markup Language.* XML on merkintäkielien standardi, joka määrittää tietojen merkintämuodon loogisella rakenteella.

OSINT: *Open-Source Intelligence.* Tiedustelu avoimista lähteistä.

1 Johdanto

Tämä työ käsittelee teollisuuden viimeisintä vallankumousta, sen keskiössä olevaa OPC UA -tiedonsiirtostandardia ja teollisuuden tietoturvallisuuden merkitystä siirryttäessä yhä enemmän verkostoituneeseen toimintaympäristöön, jossa IIoT -ratkaisujen avulla saatavien massiivisten datamäärien analysoimiseen tarvitaan pilvipalveluiden tarjoamaa kapasiteettia. Tämä avaa uusia haasteita kyberturvallisuuden saralta, koska aiemmin teollisuus on toiminut lähinnä suljetuilla sisäverkoilla, jotka on suojattu suorasta kontaktista yritysverkosta ja yleisesti internetistä DMZ-vyöhykkeen avulla. Nyt teollisuuden siirtyessä yhä enemmän verkkoon tarvitaan myös uudenlaista näkökulmaa tietoturvallisuusratkaisuihin. [1.]

2 Teollisuus 4.0

2.1 Teollisuuden kehitys

Teollistuminen alkoi 1700- ja 1800-lukujen vaihteessa Isossa-Britanniassa[2]. Merkittävänä uutena ajatuksena oli fossiilisen energian käyttö, jonka avulla ensimmäiset höyrytoimiset koneet korvasivat käsityön ensisijaisena tuotannon menetelmänä. Hyödykkeitä pystyttiin valmistamaan suuria määriä kerralla. Tämä aiheutti suuren yhteiskunnallisen ja taloudellisen muutoksen. [3.]

Toinen teollinen vallankumous alkoi 1800-luvun loppupuolella. Merkittävimpiä kehityksiä tässä aallossa olivat teräksen massatuotanto, kemianteollisuus, polttomoottorit ja sähköntuotanto. Autoteollisuus liittyi mukaan 1900-luvun jälkeen mikä tuo mukanaan tuotantolinjan. Tiede oli ensimmäistä kertaa tärkeänä osana teollisuuden kehitystä. [3.]

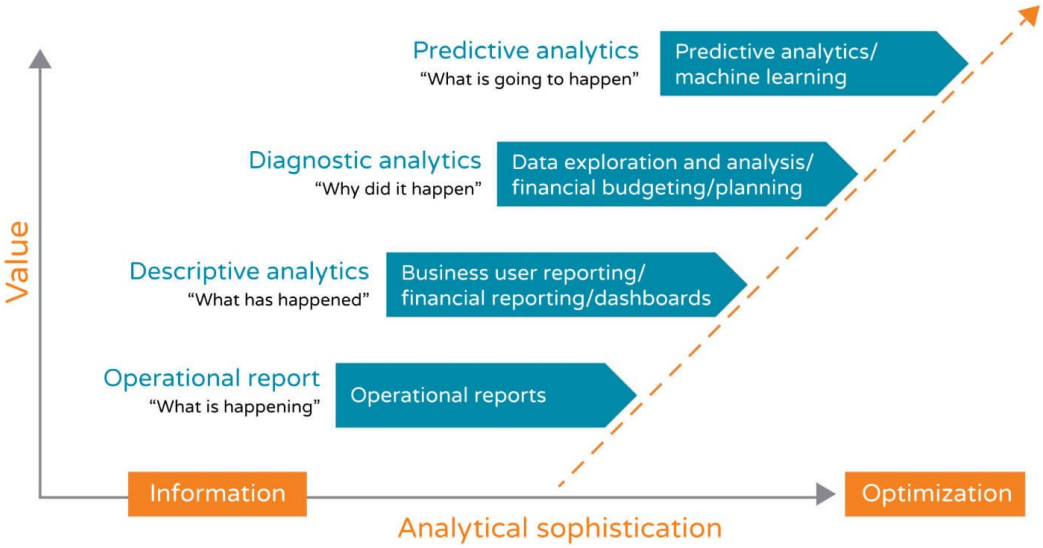
Kolmas vallankumous tapahtui 1900-luvun lopulla, mikä laajensi teollisuuden toimintaa Aasiaan lähinnä elektroniikan kehityksen myötä. Tärkeimpänä innovaationa voidaan pitää mikroelektroniikkaa ja tietokoneita. Valmistajat alkoivat

siirtymään analogisesta ja mekaanisesta teknologiasta digitaaliseen. Kolmannesta vallankumouksesta käytetään myös nimeä digitaalinen vallankumous. [4; 5.]

2.2 Neljäs teollinen vallankumous

Viime vuosikymmenien aikana syntynyttä neljättä teollisuuden vallankumousta kutsutaan nykyään nimellä Teollisuus 4.0. Siinä missä kolmannessa vallankumouksessa keskiössä olivat tietokoneet, niin neljännessä tärkeimmässä asemassa on Internet. IoT:n ja IIoT:n kehitys mahdollistaa digitalisaation viemisen uudelle tasolle avaten paljon uusia mahdollisuuksia datan hyödyntämiseen jokaisessa tehtaan toiminnossa. Digitaalisen ja fyysisen maailman yhdistäminen tuo ihmiset, datan ja koneet yhteen, mikä mahdollistaa tiiviimmän yhteistyön eri osastojen, kumppanien ja tuotteiden välillä. Tämänlaisia järjestelmiä kutsutaan kyberfyysisiksi järjestelmiksi ja niiden käyttöympäristöä älytehtaassa kybervalmistukseksi, jossa reaaliaikainen tietojenkeräys, -käsittely ja -analysointi tarjoavat läpinäkyvyyttä koko valmistustoiminnan alueelta. [5; 6.]

Suurena osana teollisuuden kehitystä ovat myös pilvipalvelut, joissa älykkään tehtaan tuottamaa massadataa voidaan analysoida eri tarkoitusperiä varten. Tätä analytiikkaa voidaan käyttää monella eri tavalla hyödyntämään yrityksen toimintaa ennakoimalla tulevaa mahdollistaen proaktiivisen toiminnan reaktiivisen sijaan, kuten kuvasta 1 voidaan nähdä. Teollisuus 4.0 -ratkaisujen ohjaama ERP auttaa optimoimaan tuotantoa ja pitää yrityksen ajan tasalla koko toimitusketjusta. [5; 6.]



Kuva 1. Ennakoivan analytiikan arvo yritykselle.[7]

3 Open Platform Communications

3.1 OPC Classic

OPC on standardi, joka kehitettiin yhteistyössä teollisuudenalan toimijoiden kanssa tarjoamaan spesifikaatiot luotettavaan ja turvalliseen tiedonvaihtoon teollisuuden eri aloilla. Standardi julkaistiin ensimmäisen kerran vuonna 1996 ja sen tarkoituksena oli abstraktoida PLC-spesifiset protokollat standardoiduksi rajapinnaksi, johon SCADA-järjestelmät saadaan liitettyä välittäjän kautta, jossa laitekohtaiset pyynnöt voidaan muuttaa yleisiksi OPC-pyynnöiksi ja päinvastoin. Tuloksena syntyi suuri tuotekirjo, josta loppukäyttäjä voi valita itselleen parhaiten soveltuvat tuotteet, jotka toimivat saumattomasti keskenään OPC:n kautta.

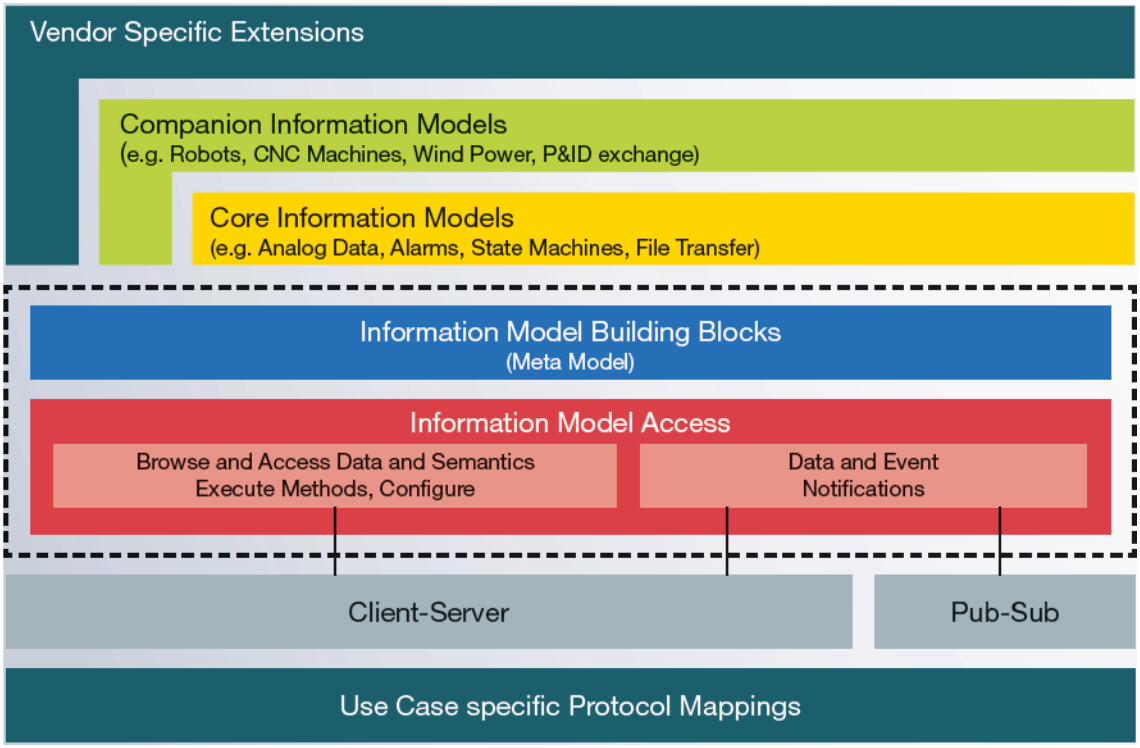
Tähän aikaan standardi oli vielä rajoitettu vain Microsoftin Windows-käyttöjärjestelmään ja toimi Windowsin COM/DCOM-mallilla. Tämä alkuperäinen versio tunnetaan nykyään nimellä OPC Classic. Classic -versioon sisältyy kolme eri spesifikaatiota: OPC Data Access, OPC Alarms & Events ja OPC Historical

Data Access. [8; 9.] OPC Classicin menestystä voidaan pitää lähtölaukaisuna teollisuuden neljännelle vallankumoukselle.

3.2 OPC UA

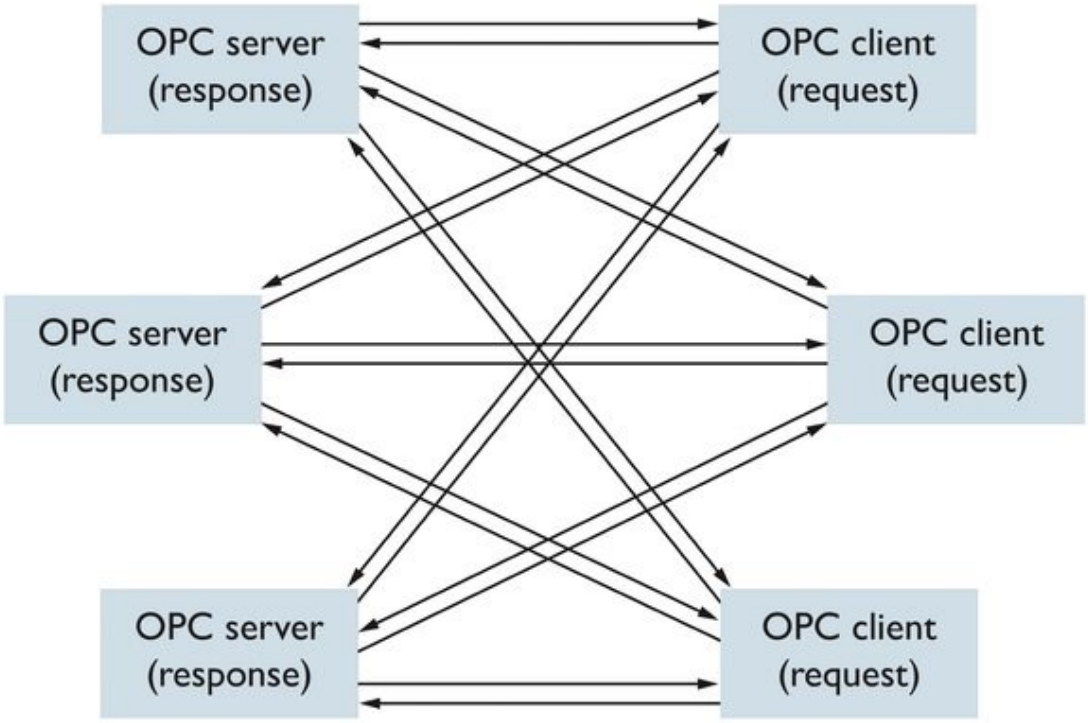
OPC Classicin menestyksen pohjalta kehitettiin toiminnallisesti vastaava OPC UA, joka julkaistiin vuonna 2008. UA on suunniteltu sisältämään Classicin toiminnallisuudet ja ominaisuuksiltaan paremmin vastaamaan teollisuuden kehityksen tuomiin haasteisiin tiedon määrässä ja sen mallintamisessa. Tähän suurena syynä oli Microsoftin siirtyminen pois COM/DCOM -malleista kohti monialustaista SOA-mallia (Service-Oriented Architecture). Toisin kuin Classic, UA on alustariippumaton ja tarjoaa yhteensopivan infrastruktuurin aina mikro-ohjaimista pilvipalveluihin saakka. UA on suunniteltu skaalautuvaksi ja laajennettavaksi. Uusia tiedonsiirtoprotokollia, sovelluspalveluita ja suojausalgoritmeja voidaan lisätä ilman yhteensopivuuden rikkomista. Tämän hetken UA-tuotteet toimivat myös tulevaisuuden tuotteiden kanssa. [10.]

UA:n informaationmallinnuskehys on sen vahvimpia ominaisuuksia, sillä dataa voi muuttaa käyttökelpoiseksi informaatioksi ja sen täydet olio-ominaisuudet mahdollistavat monitasoisten ja monimutkaisten rakenteiden mallintamisen ja laajentamisen. Kuvassa 2 näkyy, miten OPC UA:n monitasoinen informaatiokehys muodostuu. [10.]

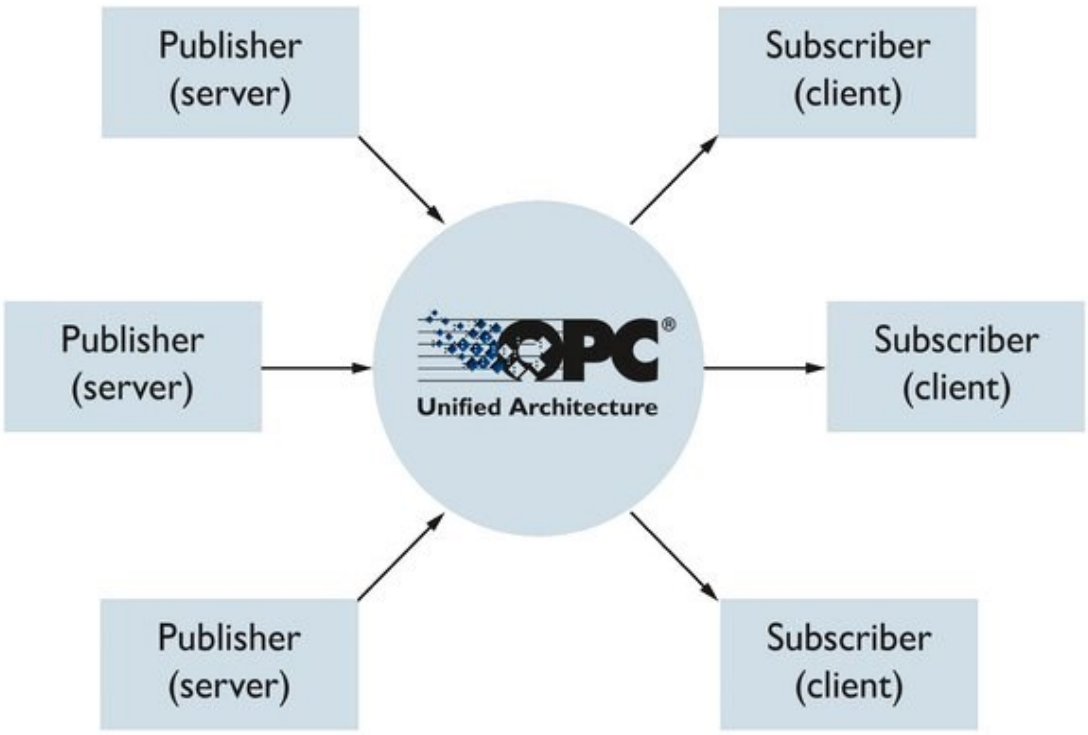


Kuva 2. OPC UA:n tietokehys.[10]

Rajoittavana tekijänä OPC UA:n kehityksessä olivat laajat asiakas-palvelinjärjestelmät, joissa jokainen laite lähettää kyselyjä palvelimille kuvan 3 mukaisesti. Tämä aiheuttaa paljon turhan datan liikkumista, hidastaa tiedonsiirtoa ja rasittaa datayhteyksiä huomattavasti ja siksi soveltuu huonosti järjestelmiin, joissa vaaditaan nopeita vasteaikoja, tai suuriin järjestelmäkokonaisuuksiin. Tämän mallin heikkouksiin OPC-säätiö vastasi vuonna 2016 julkaistulla julkaisija-tilaaja-laajennuksella (Publish/Subscribe, PubSub), jossa UA-palvelin lähettää tiedot välitysohjelmistolle (esim. pilvipalvelu) ilman tietoa siitä, mitkä asiakasohjelmat kyseistä tietoa haluavat. Tämä selkeyttää järjestelmää huomattavasti vähentämällä tarvittavia yhteyksiä, kuten kuvasta 4 voidaan huomata. Liikutettavan datan määrä vähenee huomattavasti ja säästyneitä resursseja voidaan käyttää muihin toimintoihin esimerkiksi SaaS-ratkaisuiden integroinnin toimintaan OPC UA:n toimiessa tiedonvälityskäytävänä. [11.]



Kuva 3. OPC UA:n asiakas-palvelinjärjestelmä.[12]



Kuva 4. OPC UA:n julkaisija/tilaaja-malli.[12]

4 Tietoturva

Nykyään yritykset ovat enemmän ja enemmän riippuvaisia digitaalisista palveluista ja järjestelmistä. Perinteisesti teollisuuden järjestelmät ovat toimineet suljetuissa verkoissa, jonka takia tietoturvallisuus ei ole ollut erityisen suuressa asemassa. Teknologian kehitys on siirtänyt toimintaa pois kokonaan suljetuista ympäristöistä avoimempiin ympäristöihin, ja samalla yrityksiin kohdistuvat kyberuhat ovat lisääntyneet huomattavasti. Vertikaalisen integraation vuoksi teollisuuden automaatioverkko on yhteydessä koko yrityksen verkkoon. Tietoturvaan laiminlyönti millä tahansa yrityksen verkon tasolla asettaa koko verkon haavoittuvaiseksi. Teollisuus 4.0 kehityksen tuoma reaaliaikainen yhteys kentältä pilvipalveluihin kasvattaa tietoturvariskejä entisestään. Huolellisesti suunniteltu ja oikein toteutettu tietoturva auttaa estämään tai vähentämään tietoturvauhkien muodostamia ongelmia.

4.1 Tietoturvan määrittely

Tietoturva on laaja käsite, johon sisältyy useita eri osa-alueita, joiden määrittelemiseen käytetään kansainvälisiä standardeja ja yleiseksi muodostuneita käytäntöjä. Keskeisimmät osa-alueet ovat luottamuksellisuus, eheys ja saatavuus. Näistä kolmesta käytetään yleisesti lyhennettä CIA Triad (Confidentiality, Integrity, Availability). Luottamuksellisuuden tavoitteena on taata tiedon saatavuus vain oikeutetuille käyttäjille ja estää tietojen päätyminen vääriin käsiin. Tärkein luottamuksellisuuden edistämisen työkalu on salaus. Eheyden tavoite on tiedon luotettavuuden, oikeuden ja muuttumattomuuden säilyttäminen; tieto ei saa muuttua tai tuhoutua tietomurron tai laitteisto- ja ohjelmistovikojen seurauksena. Eheyttä voidaan seurata erilaisilla tarkistussummilla, -koodeilla ja digitaalisilla allekirjoituksilla. Saatavuudella tarkoitetaan tiedon ja järjestelmien palveluvarmuutta; tietojen ja järjestelmien tulee olla oikeutettujen käyttäjien käytettävissä tietyn ajan sisällä. [13, s.11, 27-28.]

CIA Triadia täydennetään käytönhallinnan AAA-periaatteella (Authentication, Authorization, Accountability). Siihen sisältyvät tunnistus, todennus ja

kiistämättömyys. Tunnistus tarkoittaa järjestelmää käyttävän henkilön liittämistä käyttäjätiliin. Todennuksella varmistetaan käyttäjän valtuutukset lukea, kirjoittaa ja selata järjestelmän tietoja tai pääsyä järjestelmän eri osiin. Kiistämättömyys vaatii kaikkien tapahtumien kirjaamista muistiin, jotta tapahtumat ja niiden tekijät ovat paikkaansa pitäviä eikä niitä voida kiistää. [13, s.11, 87; 14.]

Tietoturvan toimivuuden kannalta on myös tärkeää muistaa johtajien, henkilöstön, asiantuntijoiden ja järjestelmän käyttäjien kouluttaminen. Henkilöstön tulee ymmärtää tietoturvan ja tietoturvariskien merkitys sekä huolehtia että vaaditut toimenpiteet suoritetaan. Kouluttamaton henkilöstö tai heikko tietoturvakulttuuri yrityksessä ovat vakavia riskejä, vaikka yrityksen järjestelmät olisi suunniteltu tietoturvaperiaatteiden mukaisesti. Mikään järjestelmä ei ole turvallinen, jos sitä käytetään väärin tai tietoturvaa laiminlyödään muualla yrityksessä. Myös ulkoisia palveluita käytettäessä on tärkeää ymmärtää, kenelle tietoa antaa ja millä tasolla palveluntarjoajan oma tietoturva on. [13, s. 64-87; 14.]

4.2 Teollisuusverkon tietoturvallisuus

Teollisuusverkkojen suurimpana tietoturvaongelmana voidaan pitää toimintaan käytettävien palveluiden integraatio verkkoon, joka on avannut perinteisesti suljettuja ja vain yrityksen hallussa olleita verkkoja avoimemmiksi. Datan pitää pystyä kulkemaan monen kerroksen läpi aina sensoreista pilvipalveluihin saakka. Tästä johtuen tietoturvallisuuden ja varsinkin kyberturvallisuuden merkitys on kasvanut huomattavasti, sillä teollisuuden automaatio- ja tietojärjestelmät ovat haluttuja hyökkäyksen kohteita. Yrityksen sisäverkot tulisi segmentoida ja suojata palomuureilla, mikä jättää mahdollisimman vähän segmenttien ja kerroksien välisiä yhdyskäytäviä. Tätä mallia kutsutaan syvyyssuuntaiseksi suojaukseksi. Nykyaikaisilta teollisuusautomaatiojärjestelmiltä vaadittava korkea käytettävyys ja reaaliaikainen prosessienohjaus tuovat omat lisävaatimuksensa

tietoturvallisuudelle. Täydellistä tietoturvaa on mahdotonta saavuttaa, joten sitä tulisi lähestyä riskienhallinnan näkökulmasta ja pyrkiä minimoimaan uhkien toteutuminen ja niiden toteutuessa pyrkiä minimoimaan sekä rajaamaan vahingot mahdollisimman pienelle alueelle. [13, s. 51-66, 67-88.]

4.2.1 Toimistoverkon tietoturvallisuus

Toimistoverkot ovat aina olleet haavoittuvaisia tietoturvauhille, sillä ne toimivat lähempänä avointa internetiä. Toimistoverkon vaatimukset käytettävyyden saralta ovat matalammat, mikä mahdollistaa yleisten salaus- ja autentikointimetodien käytön ilman huolta käyttöviiveistä. Myös perinteisiä virustorjuntaohjelmistoja tulisi käyttää ja huolehtia käytössä olevien ohjelmistojen ja laitteiden päivittämisestä jatkuvasti. Työasemat ja palvelimet tulisi myös koventaa, eli poistaa kaikki turhat ominaisuudet tai osat käytöstä. Näillä askelilla pyritään minimoimaan verkon laitteiden ja järjestelmien näkyvyys hyökkääjille. Käytönhallinnan ja tilaturvallisuuden tulee myös olla kunnossa, jotta kukaan sivullinen ei pääse fyysisesti käsiksi työasemiin ja sitä kautta sisään järjestelmään. Henkilöstön koulutukseen on myös syytä panostaa, sillä yleisimpiä tapoja, joilla hyökkääjät pyrkivät pääsemään järjestelmään, ovat tietojenkalastelusähköpostit tai muilla haittaohjelmilla saastutetut sähköpostit. [13, s. 51-66.]

4.2.2 Automaatioverkon tietoturvallisuus

Automaatioverkkojen tietoturvassa suurin muutos on IP-pohjaisten verkkoteknologioiden yleistyminen. Nämä teknologiat tuovat mukanaan tarpeen paremmalle tietoturvalle, sillä IP-protokollien heikko puoli on näkyvyys kenttäväylien ulkopuolelle. Automaatiojärjestelmien lisääntynyt tarve reaaliaikaiselle datansiirrolle tuo omat haasteensa turvallisuuden kannalta, sillä monet yleiset salaus- ja varmennustekniikat ovat resurssienkäytön puolesta raskaita aiheuttaen viivettä tiedon tulkitsemisessa. Viiveen minimointiin käytettävät nopeammin toimivat laitteet ovat heikommin suojattuja kuin normaalimmat ratkaisut. Tämä lisää järjestelmän muiden tasojen tietoturvan painoarvoa. Tästä syystä automaatioverkkojen tietoturvassa tärkeimpiä asioita ovat segmentoinnin ja liikenteen

rajoittamisen lisäksi verkon topologian ja laiteryhmien huolellinen suunnittelu. Verkkojen tulisi myös olla redundantteja ja palautua virhetilanteista nopeasti. [13, s.42, 44.]

4.3 OPC UA:n tietoturvallisuusuhat

OPC UA toimii jokaisella teollisuusverkon tasolla aina antureista pilvipalveluihin saakka, mikä tekee siitä alttiin julkisissa verkoissa liikkuville haittaohjelmille ja houkuttelevan kohteen teollisuusvakoilulle tai sabotaasille. Tämä otettiin huomioon jo suunnitteluvaiheessa painottamalla tietoturvan merkitystä ja integroimalla se osaksi järjestelmää. Tietoturvamekanismeja on suunniteltu jokaiselle CIA Triadin ja AAA-periaatteen määrittämälle osa-alueelle tunnistamalla järjestelmään kohdistuvat uhat ja määrittämällä uhille vastatoimia, jotka pyrkivät torjumaan uhkista koituvia vahinkoja. [15.] Kuvassa 5 on määritelty yleisimmät uhat ja se, mitä tietoturvallisuuden osa-aluetta ne koskevat.

	Todennus	Pääsynvalvonta	Luottamuksellisuus	Eheys	Varmennettavuus	Saatavuus	Kiistämättömyys
Palvelunesto-hyökkäys						✓	
Salakuuntelu	✓	✓	✓				
Viestihuijaus		✓					
Viestin muuntaminen	✓	✓		✓	✓		✓
Viestin toisto	✓	✓					
Epämuodostuneet viestit						✓	
Palvelimen profilointi	✓	✓	✓	✓	✓	✓	✓
Järjestelmän kaappaus	✓	✓	✓	✓	✓	✓	✓
Väärennetty palvelin	✓	✓	✓		✓	✓	
Käyttäjätietojen kaappaaminen	✓	✓	✓				
Kiistäminen							✓

Kuva 5. Yleisimmät tietoturvauhat ja niiden vaikutus tietoturvan osa-alueisiin.[16]

4.4 Turvallisuusuhat

4.4.1 Palvelunestohyökkäykset

Palvelunestohyökkäykset (Denial of Service) ovat nykymaailmassa yleisiä, sillä ne eivät vaadi hyökkääjältä merkittävää teknologista osaamista. Ne voidaan jakaa kolmeen kategoriaan: kuormitushyökkäyksiin, resurssien kuluttamiseen ja sovelluksen kaatamiseen. Hyökkääjä voi käyttää apunaan saastunutta bottiverkkoa lähettääkseen kohteeseen suuren määrän viestijä, kyselyitä tai useita pyyntöjä sisältäviä viestejä. Tarkoituksena on kuluttaa kohteen resursseja ja tukkia verkkoliikennettä. Palvelunestohyökkäykseen ei välttämättä tarvita

viestien tulvaa, jos hyökkääjä on onnistunut tiedustelemaan esimerkiksi kohdepalvelimen käyttämän käyttöjärjestelmän version, jossa on tietoturva-aukko. Yksikin viesti tietyllä rakenteella voi riittää jumittamaan tai kaatamaan palvelimen. [15.]

4.4.2 Salakuuntelu

Salaamaton verkkoliikenne mahdollistaa liikenteen salakuuntelun (Eavesdropping). Viestien ja yhteyden salaamattomuus liitettynä heikkoon tunnistettavuuteen altistavat väliintulohyökkäyksille (Man-in-the-Middle, MitM). Hyökkääjä voi käyttää salakuuntelua päästäkseen sisälle järjestelmään varastamalla käyttäjätunnuksia tai muuta arkaluontoista informaatiota. Jos hyökkääjä on onnistunut murtautumaan sisälle järjestelmään, kaikki salaamaton informaatio järjestelmässä on hyökkääjän saatavilla. [15.]

4.4.3 Viestihuijaus

Hyökkääjä voi käyttää luomaansa viestiä tai aiemmin kaappaamaansa muutettua viestiä väärentääkseen identiteettinsä (Message spoofing, message alteration). Viestissä pyritään näyttämään sen olevan peräisin joltain luotettavalta toimijalta tai sovellukselta. Huijauksen onnistuessa hyökkääjän on mahdollista saada lisää informaatiota kohteesta tai pahimmassa tapauksessa suorittaa luvattomia toimintoja ja saada pääsy suojattuun informaatioon. Väärennettyjä viestejä voi myös käyttää luvattoman toiminnan jälkien peittämiseen. [15.]

4.4.4 Viestin toisto

Tässä hyökkäyksessä kaapattua viestiä ei muuteta vaan se lähetetään myöhemmin uudelleen (Message replay). Tämä voi antaa järjestelmien käyttäjille väärän kuvan tilanteesta ja sekoittaa järjestelmää. Hyökkääjä voi myös yrittää käyttää viestiä päästäkseen sisälle järjestelmään tallennettujen istuntojen kautta. [15.]

4.4.5 Epämuodostunut viesti

Hyökkääjä voi luoda virheellisesti muodostettuja viestejä (Malformed message), joissa voi olla vääriä binääriarvoja, parametreja, data-arvoja tai väärin muotoiltua XML-koodia. Voi aiheuttaa kohteen suorittamaan luvattomia toimintoja tai käsittelemään turhia tietoja. Hyökkäys voi pahimmassa tapauksessa aiheuttaa sovellusten kaatumisen ja mahdollistaa hyökkääjän pääsyn järjestelmään. [15.]

4.4.6 Palvelimen profilointi

Hyökkääjä pyrkii tiedustelemaan palvelimen tyyppiä (Server profiling), ohjelmistoversioita, internetprotokollia tai valmistajaa saadakseen tietoa kohteen mahdollista tietoturva-aukoista ja muista haavoittuvuuksista kohteen vastausten perusteella. Hyökkäys on helppo toteuttaa, sillä internetistä löytyy useita hakukoneita, joilla profilointia on mahdollista suorittaa. Profilointi ei välttämättä rajoitu vain palvelimiin, vaan kaikki verkossa olevat laitteet on mahdollista profiloida ja niiden haavoittuvaisuuksia voidaan käyttää muiden hyökkäyksien suorittamiseen. [15.]

4.4.7 Istunnon kaappaus

Hyökkääjä pyrkii kaappaamaan istunnon (Session hijacking) valtuutetulta käyttäjältä käyttämällä kaappaamiaan, muilla hyökkäyksillä saamillaan tai arvaamillaan tiedoilla. Istunnon kaapattuaan hyökkääjä voi esiintyä käyttäjänä ja päästä luvattomasti käsiksi tietoihin tai toimintoihin. Tällaisen hyökkäyksen jäljittäminen ja tunnistaminen voi olla haastavaa, koska hyökkääjä toimii järjestelmän omana käyttäjänä. [15.]

4.4.8 Väärennetty palvelin

Hyökkääjä rakentaa oman palvelimensa (Rogue server), joka pyrkii esiintymään aitona järjestelmän palvelimena tai näyttäytyy järjestelmälle uutena palvelimena. OPC UA -järjestelmissä hyökkääjä voi myös esiintyä UA:n

julkaisijapalvelimena (Rogue publisher). Onnistuessaan hyökkäys on valtava tietoturvariski, koska hyökkääjällä on täysi pääsy kaikkeen palvelimelle tulevaan liikenteeseen ja väärennettyä palvelinta voidaan käyttää laukaisualustana aggressiivisemmille tietoturvahyökkäyksille. [15.]

4.4.9 Käyttäjätietojen kaappaaminen

Hyökkääjä käyttää muilla hyökkäyksillään hankkimiaan käyttäjätunnuksia ja salasanoja päästäkseen käsiksi järjestelmään (Compromising user credentials). Salasanoja ei välttämättä tarvitse hankkia, vaan ne voidaan myös murtaa arvaamalla tai käyttämällä salasanojen murtamiseen suunniteltuja ohjelmia. Tietoteknisten ratkaisujen lisäksi hyökkääjä voi saada käyttäjätietoja haltuunsa varastamalla dokumentteja tai muuten pääsemällä yrityksen tiloihin fyysisesti. [15.]

4.4.10 Kieltäminen

Kieltämisessä (Repudiation) ei ole suoranaisesti kysymys hyökkäyksestä, koska kyseessä ei ole kommunikaatio tai informaatio vaan viestintää seuraava luottamus. Molemmat osapuolet pystyvät normaalisti vahvistamaan mitä viestejä on lähetetty ja vastaanotettu. Järjestelmissä, joissa kieltäminen on mahdollista tämä ei toteudu. Tämä johtaa luottamusongelmiin lähettäjien tai vastaanottajien kanssa. Hyökkääjät voivat käyttää kieltämistä viestien kaappaamiseen tai luvattomien toimiensa jälkien peittelyyn. [15.]

4.5 Tietoturvahyökkäyksen vaiheet

4.5.1 Tiedustelu

Yleisimmät tietoturvahyökkäykset ovat avoimessa internetissä kulkevia haittaohjelmia ja viruksia, jotka voivat lymyillä verkkosivuilla saastuneissa elementeissä tai linkeissä. Tavallisimpia näistä ovat kiristysohjelmat, jotka salaavat kohteen tietoja omalla salausavaimellaan ja vaativat maksua salauksen purkamiseksi rikollisorganisaatiolle tai yksittäiselle toimijalle.

Tiedonkalastelusähköpostit ovat myös todella yleisiä ja hyvin toteutettuna voivat olla todella vakuuttavia ja onnistua huijaamaan ihmisiä. Nämä aiheuttavat huolenaihetta yritykselle, mutta ovat suhteellisen helppoja estää perinteisillä tietoturvaohjelmilla ja henkilöstön kouluttamisella. Huomattavasti suuremman riskin aiheuttavat harvinaisemmat kohdennetut hyökkäykset. [17.]

Kohdennetun hyökkäyksen voi jakaa kahteen vaiheeseen. Vaiheessa yksi hyökkääjä pyrkii tiedustelemaan kohteesta mahdollisimmat paljon informaatiota kohdejärjestelmästä. Tiedustelua yleensä suoritetaan internetissä avoimesti löydettävistä lähteistä (OSINT, Open-Source Intelligence), joista saatavista tiedonmurusista pyritään saamaan kasattua kohdejärjestelmästä tilannekuva, jonka pohjalta hyökkäystä lähdetään suorittamaan. Yrityksen hyökkäyspinta-ala voi olla yllättävän suuri sillä pienetkin asiat voivat antaa hyökkääjälle kriittistä tietoa hyökkäyksen kannalta. Yrityksen lehdistötiedotteista voidaan saada järjestelmätoimittajien nimiä tai kuvista voidaan mahdollisesti nähdä valvomonäyttöjä ja muuta arkaluontoista informaatiota, jos yritys ei ole huolellisesti näitä sensuroinut. Myös yritykselle tehdyissä opinnäytetöissä voidaan paljastaa osia yrityksen järjestelmän toiminnasta esimerkiksi verkon rakennetta ja osoiteavaruutta. [17.]

Myös internetin hakukoneilla voidaan saada tietoja yrityksen sisäänkirjautumissivustoista, verkkoon liitetyistä haavoittuvaisista laitteista ja automaatiolaitteistojen hallintaan käytettävistä web-palvelimista. IoT-laitteiden yleistyminen on tuonut huomattavasti lisää haasteita tietoturvallisuudelle juuri niiden verkkoon liitännän takia. Vain yksi laite haavoittuvalla päivitysversiolla voi riittää hyökkääjälle. Lähes kaikki internetiin kytketyt laitteet käyttävät myös sertifikaatteja identiteetin varmistamiseen ja, näistä voidaan myös saada tietoja yritysten aliverkoista ja sisäisistä järjestelmistä. [17.]

4.5.2 Hyökkäys ja sen tavoitteet

Päästyään sisälle järjestelmään hyökkääjä pyrkii varmistamaan, että yhteys järjestelmään on pysyvä ja se voidaan mahdollisesti ottaa uudestaan asentamalla jonkinlaisia takaportteja järjestelmään. Tämän vaiheen jälkeen tavoitteena on

saada mahdollisimman suuri osa järjestelmästä hyökkääjän haltuun keräämällä käyttäjätunnuksia tai muita haavoittuvaisuuksia käyttämällä. Kun hyökkääjä on saavuttanut tarpeeksi laajan pääsyn kohdejärjestelmään, voidaan aloittaa hyökkäyksen toinen vaihe. [17.]

Toisessa vaiheessa hyökkääjä on saanut pääsyn yrityksen syvimpiin verkkoihin esimerkiksi automaatioverkkoon. Tässä kohtaa hyökkääjän eteneminen riippuu siitä, mikä hyökkäyksen tavoitteena on. Tavoitteena voi olla maksimaalinen tuho nopeasti levittämällä haittaohjelmia tuhoamaan yrityksen tietoverkon järjestelmiä kuten tuotannonohjausjärjestelmiin. Tuhoava hyökkäys ei vaadi hyökkääjältä suurta tietotaitoa tai resursseja. Kohdennetumpi hyökkäys johonkin automaatiojärjestelmän prosessiin vaatii hyökkääjältä paljon enemmän tietoa käytössä olevista laitteista ja järjestelmistä sekä ymmärrystä kyseisen alan prosessitekniikasta. Hyökkääjän tavoitteena ei myöskään välttämättä tarvitse olla järjestelmän tuhoaminen vaan hyökkääjä voi myös pyrkiä olla mahdollisimman huomaamattomasti järjestelmässä ja vakoilla yrityksen toimintoja. Hyökkääjää, joka on onnistunut laajalti saastuttamaan järjestelmän, on lähes mahdotonta saada ulos järjestelmästä ilman koko järjestelmän ja laitteiston resetointia. [17.]

4.5.3 Vastatoimet

Yritysten tulisi kartoittaa omaa julkista hyökkäyspinta-alaansa samoilla avoimien lähteiden metodeilla kuin hyökkääjätkin. Internetin hakukoneilla on hyvä tehdä hakuja omasta yrityksestä ja katsoa, minkälaista informaatiota on avoimesti saatavilla. Kaikki yrityksen omat dokumentit ja yritykselle tehdyt opinnäyte- tai muut työt tulisi tarkastaa arkaluontoisen informaation poistamiseksi. Yrityksen sisäverkkojen ja testiympäristöjen näkyvyyttä verkkoon tulisi rajoittaa tai mahdollisuuksien mukaan estää kokonaan. Shodan-hakukone on hyvä työkalu yrityksen julkiselle internetille avoimien porttien tarkastamiseen. Myös kaikki tarpeettomat fyysiset liitännät laitteisiin tulisi poistaa käytöstä. Kaikkia vastatoimia ei välttämättä kannata tehdä itse, sillä monet tietoturvallisuuteen erikoistuneet yritykset tarjoavat palveluja yrityksen tietoturvan parantamiseen ja validointiin. Tietoturvallisuuden hallinnan standardi ISO/IEC 27001 tarjoaa hyviä

vaatimuksia, jotka yritysten tulisi täyttää. Erilaisia fyysisiä ja tietoteknisiä penetraatiotestejä olisi hyvä suorittaa, jotta mahdolliset haavoittuvaisuudet järjestelmissä ja käytännöissä löydetään. [17.]

4.6 OPC UA:n tietoturvallisuus

OPC UA on suunniteltu tietoturva huomioon ottaen ja, siitä löytyvätkin kattavat integroidut tietoturvaominaisuudet. Järjestelmään on määritetty useita tietoturvapolitiikoita ja profiileja, joiden avulla turvallinen kommunikaatio palvelimien ja asiakkaiden välillä voidaan järjestää. OPC UA -palvelimeen määriteltävä tietoturvapolitiikka vaatii asiakasohjelmilta määritystä vastaavaa tietoturvamoodia. UA:n SecurityMode kattaa kolme vaihtoehtoa, jotka ovat None, Sign ja SignAndEncrypt. Nimensä mukaan None-tila ei tarjoa minkäänlaista suojaa ja sitä tulisi käyttää vain kommunikaatioon, jossa ei vaihdeta mitään tärkeää tai arkaluontoista informaatiota. Sign-tilassa kaikki viestintä allekirjoitetaan digitaalisesti tunnistusta ja eheyden tarkistusta varten. Tämä lisää turvallisuutta huomattavasti, sillä se estää useimmat yleisimmät hyökkäykset, sillä allekirjoituksesta voidaan nähdä, onko viestin sisältö muuttunut matkan varrella. Pelkkä allekirjoittaminen ei välttämättä ole riittävää kaikissa tilanteissa. SignAndEncrypt-tilassa viesti allekirjoittamisen lisäksi myös salataan symmetrisesti tai asymmetrisesti riippuen tilanteesta. Tämä estää salakuuntelun ja muut hyökkäykset tehokkaasti sillä salauksien murtamiseen vaaditaan kryptografisia menetelmiä ja resursseja, joita tähän vaaditaan, ei löydy kaikilta. Kuvassa 6 on Saksan liittovaltion tietoturvaviraston tekemän analyysin tulokset liittyen UA:n kolmeen SecurityMode-tilaan. [15.]

5 Analysis of the protection mechanism at the parameter level

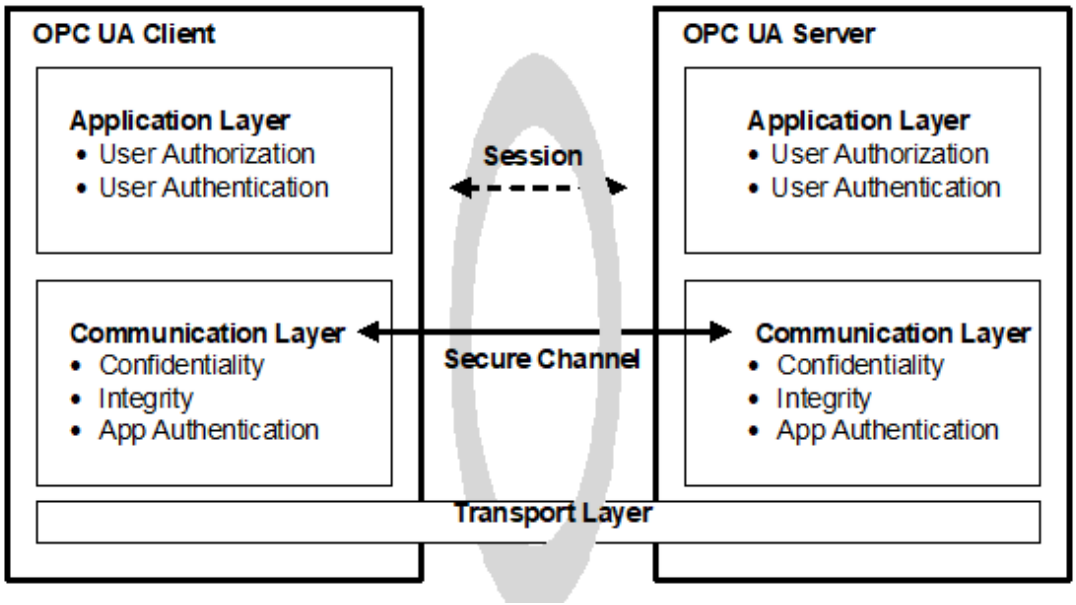
Table 9 Effectiveness of the OPC UA measure

Security-Mode	*Layer or Service*	*Denial of Service*	*Eaves-dropping*	*Message Spoofing*	*Message Alteration*	*Message Replay*	*Malformed Messages*	*Server Profiling*	*Session Hijacking*	*Rogue Server*	*Compromising User credentials*	*Repudiation*
		low prot.	no prot.	no prot.	no prot.	no prot.	low prot.	no prot.	no prot.	no prot.	no prot.	no prot.
	UACP	8	0	0	0	0	8	0	0	0	0	0
None		restricted	no prot.	no prot.	no prot.	no prot.	low prot.	low prot.	effective	low prot.	effective	restricted
	Secure-Channel	10	0	0	0	16	1	0	15	0	0	0
	Session	14	0	2	0	26	3	4	23	0	2	2
	Discovery	20	0	4	4	35	9	8	30	6	0	6
Sign		restricted	no prot.	effective	effective	effective	effective	restric-ted	effective	effective	effective	effective
	Secure-Channel	10	8	10	10	21	11	15	26	7	10	12
	Session	14	0	12	8	31	12	14	28	6	4	18
	Discovery	21	0	5	5	36	9	20	31	7	1	10
Sig-nAndEn-crypt		restricted	effective	effective	effective	effective	effective	re-stricted	effective	effective	effective	effective
	Secure-Channel	10	14	10	10	21	11	15	29	7	14	12
	Session	14	18	12	8	31	12	14	46	6	22	18
	Discovery	21	13	5	5	36	9	20	43	7	13	10

Restricted protection (prot.) - the possibilities of an attacker are restricted, but this type of attack is not prevented.
Effective protection - attacks of this type require cryptographic attacks.

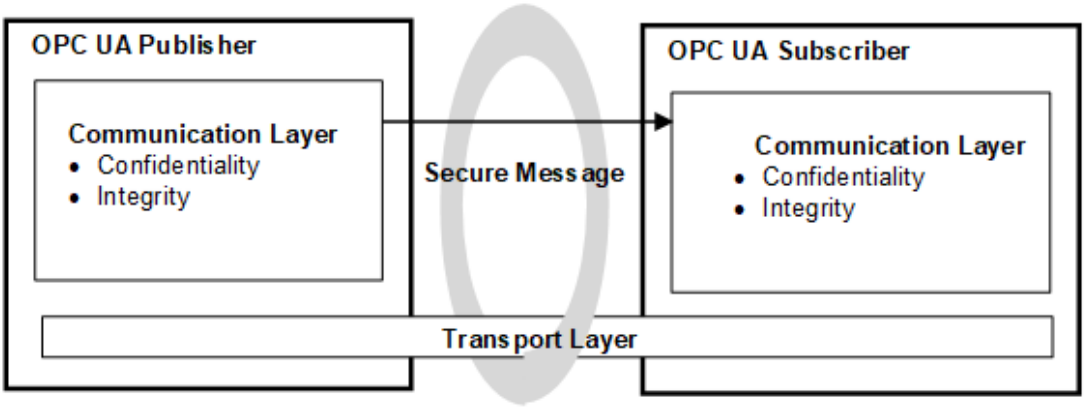
Kuva 6. Saksan liittovaltion tietoturvaviraston teettämän tietoturva-analyysin tulokset. [18, s. 24.]

OPC UA:n asiakaspalvelinkommunikaatiossa sovellukset muodostavat aina istunnon, ja SecureChannel-toiminolla avataan luotettava yhteys. Yhteyden avaamisen jälkeen palvelin tarkastaa asiakkaan oikeudet, jonka jälkeen toimintoja voidaan suorittaa. Kaikki tämä tapahtuu useassa kerroksessa samaan aikaan kuvan 6 mukaisella tavalla. Välitystason päälle on kasattu kommunikaatiotaso, jossa täytetään tietoturvallisuuden vaatimuksia luottamuksellisuuden ja eheyden osalta sekä varmistetaan sovelluksen oikeus. Sovellustasolla varmistetaan käyttäjien valtuutus ja todennus.



Kuva 7. OPC UA:n asiakaspalvelin tietoturva-arkkitehtuuri. [15, 4.5]

Julkaisija-tilaajamallissa voidaan toimia joko ilman välittäjää tai välittäjän kanssa. Välittäjättömässä versiossa sovellukset käyttävät Secure Key Server -palvelimen (SKS) jakamia symmetrisiä salausavaimia tiedonsiirron turvaamiseen. SKS toimii asiakaspalvelinmallin mukaisilla menetelmillä turvallisuudessa. Julkaisija-tilaajamallissa julkaisijat ja tilaajat voidaan jakaa SecurityGroup-ryhmiin, joissa sovellukset voivat jakaa informaatiota. Tämä malli perustuu sovellusten väliseen luottamukseen, sillä kaikilla sovelluksilla on samat oikeudet. Sovellusten välillä tapahtuu vähemmän toimintoja, kuten kuvasta 7 on havaittavissa, mikä parantaa mallin suorituskykyä ja soveltuvuutta tiettyihin prosesseihin teollisuudessa, joissa tarvitaan nopeaa tiedonvälitystä. Tästä syystä SecurityGroup-ryhmiä tulisi luoda useita ja erotella ne muista, jotta yksi kaapattu laite ei voi vaikuttaa koko järjestelmän toimintaan. [15.]



Kuva 8. OPC UA:n julkaisija-tilaaja tietoturva-arkkitehtuuri. [15, 4.5]

5 Yhteenveto

Teknologian kehitys on tuonut lisää mahdollisuuksia teollisuuden kehittämiseen, mutta samalla myös tietoturvallisuuden rooli on kasvanut merkittävästi. Samaan aikaan resurssivaatimukset hyökkäyksen suorittamiseen ovat heikentyneet. Varsinkin tiedusteluun käytettäviä sovelluksia on internetissä vapaasti käytettävissä. Tämä aiheuttaa uusia haasteita yrityksille ja yrityskulttuurille niiden sopeutuessa yhä enemmän vertikaalisesti ja horisontaalisesti integroituvaan ympäristöön. Hyvin toteutettu tietoturva on ja tulee olemaan kriittinen osa yritysten toiminnassa ja sitä tulisi lähestyä enemmän myös hyökkääjän silmin.

OPC UA on tärkeä osa tulevaisuuden teollisuutta ja on siksi myös houkutteleva kohde hyökkääjille. Sen sisältämät tietoturvatoiminnot ovat tehokkaita mutta vain oikein määriteltyinä ja yhteistyössä yleisen tietoturvan kanssa, sillä jokainen järjestelmä on yhtä vahva kuin sen heikoin osa. Varsinkin nykyaikaisten reaaliaikaista tiedonvälitystä vaativien prosessien tietoturva on haastavaa, koska yleisimpiä tietoturvan menetelmiä ei ole mahdollista käyttää. Tämä vaatii tarkempaa otetta järjestelmien rakentamiseen ja suunnitteluun, jotta riittävä turva saadaan muodostettua muilla tavoin näille prosesseille. Myös OPC UA:n laaja-

alaisuus aiheuttaa huolta, sillä esimerkiksi ohjelmointivirheen takia ilmenevällä haavoittuvuudella voi olla katastrofaalisia seurauksia toiminnan kannalta, jos sitä ei huomata ja korjata riittävän nopeasti. Kaikki tietoturvan huolet eivät myöskään ole vain teknisiä vaan henkilöstön koulutukseen, yrityksen sisäiseen tietoturvakulttuuriin ja penetraatiotestaukseen tulisi myös kiinnittää enemmän huomiota kuin ennen.

.

Lähteet

1 CISA. 2015. Layering Network Security Through Segmentation Infographic. Verkkoaineisto. < https://www.cisa.gov/sites/default/files/publications/layering-network-security-segmentation_infographic_508_0.pdf>. Luettu 1.4.2023.

2 Rinta-aho, Harri. 2004. Historian tuulet 7, s. 45. Otava. ISBN 951-1-17967-5. Luettu 3.4.2023.

3 Schön, Lennart. 2013. Maailman taloushistoria. Teollinen aika. s. 48. Tampere: Vastapaino. ISBN 978-951-768-380-7. Luettu 3.4.2023.

4 Schön, Lennart. 2013. Maailman taloushistoria. Teollinen aika. s. 278. Tampere: Osuuskunta Vastapaino. ISBN 978-951-768-380-7. Luettu 3.4.2023.

5 Mikä on Teollisuus 4.0 – Teollinen esineiden Internet (IIoT, Industrial Internet of Things). Verkkoaineisto. <https://www.epicor.com/fi-fi/resources/articles/what-is-industry-4-0/>. Luettu 6.4.2023.

6 BMWK: What is Industrie 4.0? 25.2.2019. Verkkoaineisto. <https://www.plattform-i40.de/IP/Navigation/EN/Industrie40/WhatIsIndustrie40/what-is-industrie40.html>. Luettu 6.4.2023.

7 Kuva 1. <https://www.epicor.com/globalassets/uploadedimages/us/images/articles/img-article-predictive-analytics.jpg>.

8 OPC Foundation: What is OPC? Verkkoaineisto. <https://opcfoundation.org/about/what-is-opc/>. Luettu 10.4.2023.

9 OPC Foundation: Classic. Verkkoaineisto. <https://opcfoundation.org/about/opc-technologies/opc-classic/>. Luettu 10.4.2023.

10 Kuva 2. <https://opcfoundation.org/about/opc-technologies/opc-ua/>.

11 OPC Connect: OPC UA is Enhanced for Publish-Subscribe (Pub/sub). 2016. Verkkoaineisto. <https://opcconnect.opcfoundation.org/2016/03/opc-ua-is-enhanced-for-publish-subscribe-pubsub/>. Luettu 11.4.2023.

12 Kuvat 3 ja 4. <https://www.phoenixcontact.com/en-us/technologies/communication-technologies/opc-ua>. 2023.

13 Suomen Automaatioseura. 2010. Teollisuusautomaation tietoturva. Verkkoaineisto. <https://www.automaatioseura.fi/site/assets/files/2157/sas29_teollisuusautomaation_tietoturva.pdf>. Luettu 12.4.2023.

14 OPC Foundation. 2018. Practical Security Recommendations for building OPC UA Applications. Verkkoaineisto. <https://opcfoundation.org/wp-content/uploads/2017/11/OPC-UA-Security-Advise-EN.pdf>. Luettu 12.4.2023.

15 OPC Foundation. 1.11.2022. OPC 10000-2: UA Part 2: Security. Verkkoaineisto. <https://reference.opcfoundation.org/Core/Part2/v105/docs/>. Luettu 14.4.2023.

16 Sipilä, Kari. 2019. Tulevaisuuden automaatiojärjestelmät: OPC UA:n tietoturva ja pilvipalvelut. Opinnäytetyö. s. 25 <https://www.theseus.fi/handle/10024/166396>. 2019. Luettu 13.4.2023.

17 Taponen, Janne. 2021. OSINT ja sen merkitys automaatioverkkoja vastaan tehtävissä hyökkäyksissä. Verkkoaineisto. <https://www.automaatioseura.fi/julkaisut-kirjakauppa/automaation-tietoturva-julkaisut/liitteet/>. Luettu 17.4.2023.

18 BSI. 24.4.2022. Open Platform Communications Unified Architecture Security Analysis 2021. Verkkoaineisto. <https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Studies/OPCUA/OPCUA_2022_EN.html>. Luettu 20.4.2023.