jamk

Kyberturvallisuus teollisuusautomaatiossa

Teollisuusrobotiikan kyberturvallisuus

Tuukka Forssell

Opinnäytetyö, ylempi AMK
Marraskuu 2023
Robotiikka YAMK

jamk | Jyväskylän ammattikorkeakoulu
University of Applied Sciences

jamk

Kuvailulehti

Forssell, Tuukka

Kyberturvallisuus teollisuusautomaatiossa. Teollisuusrobotiikan kyberturvallisuus

Jyväskylä: Jyväskylän ammattikorkeakoulu. Marraskuu 2023, 62 sivua.

Robotiikan tutkinto-ohjelma. Opinnäytetyö YAMK.

Julkaisun kieli: suomi

Julkaisulupa avoimessa verkossa: kyllä

Tiivistelmä

Opinnäytetyön tavoitteena oli selvittää, minkälaisia suosituksia standardit asettavat automatisoiduille robotiikan järjestelmille. Toisena tavoitteena oli selvittää kyberturvallisuuden kypsyystasoa kyseisten järjestelmien osalta. Tutkimusmenetelminä käytettiin integratiivisen kirjallisuustutkimuksen menetelmää

Laitteiden toimivuus on teollisuusautomaatiojärjestelmien suunnitellussa ja rakentamisessa ohjaavia tekijöitä. Järjestelmien suojaamisessa on luotettu vahvasti fyysiseen suojaukseen, mutta kyberturvallisuus on kuitenkin noussut esiin muuttuvassa toimintaympäristössä myös teollisuusrobotiikan osalta. Teollisen tuotannon varmistaminen on myös huoltovarmuuteen liittyvä tehtävä. Yhteiskunnan toiminnan jatkuminen edellyttää myös sitä, että teollisessa toimintaympäristössä huomioidaan kyberuhkat ja niiden vaikutukset toimintaan. Teollisuusrobotiikka yhdistelee monen tekniikan alan kuten automaatio, kone, sähkö, tieto, verkko -tekniikan sekä elektroniikan, anturit, toimilaitteet ja näitä mahdollisesti ohjaava tekoälyn. Tämä haastava ja monimutkainen kokonaisuus tulisi toteuttaa huomioiden kyberturvallisuus. Kybersodankäynnin kohteena ei myöskään välttämättä ole sotilaalliset kohteet vaan vihamielinen toimija pyrkii käyttämään kaikki vaikutustavat ja myös siten että vähäisimmällä vaivalla saadaan potentiaalisesti suuri vaikutus yhteiskuntaan tai yrityksiin.

Työn tuloksena havaittiin, että teollisuusorganisaatiot kamppailevat monisyisen kyberturvallisuusongelman kanssa. Heidän tulee omaksua kypsä turvallisuusasenne tietotekniikan sekä operatiivisen teknologian ympäristöissään, samaan aikaan kun molemmat joutuvat yhä kasvavan määrän hyökkäysten kohteeksi - ja samalla kun rajat näiden kahden alueen välillä hämärtyvät päivä päivältä enemmän. Kyberturvallisuuden huomiointi tulee ottaa lähtökohdaksi jo järjestelmien suunnitteluvaiheessa ja huomioida kyberuhat käytön aikana ja hallita niitä jatkuvan riskienhallinnan avulla sekä kouluttaa ja harjoituttaa henkilöstö toimimaan oikealla tavalla kyberuhkiin varautumisessa.

Avainsanat (asiasanat)

ICS, kyber, robotiikka

jamk

Description

Forssell, Tuukka

Cyber Security in Industrial Automation, Cyber Security of the Robotics

Jyväskylä: JAMK University of Applied Sciences, October 2023, 62 pages

Degree Programme in Robotics. Master´s thesis.

Permission for open access publication: Yes

Language of publication: Finnish

Abstract

The aim of the thesis was to find out what kind of recommendations the standards set for automated robotics systems. The second goal was to find out the maturity level of cyber security with regard to the systems in question. The method of integrative literature research was used as research methods.

The functionality of the devices is a guiding factor in the design and construction of industrial automation systems. In the protection of systems, physical protection has been strongly relied on, but cyber security has nevertheless emerged in the changing operating environment also with regard to industrial robotics. Ensuring industrial supply is also a task related to security of supply. The continuation of society's activities also requires that cyber threats and their effects on operations are taken into account in the industrial operating environment. Industrial robotics combines many fields of technology such as automation, machine, electricity, information, network technology as well as electronics, sensors, actuators and the artificial intelligence that may control these. This challenging and complex entity should be implemented with cyber security in mind. The target of cyberwarfare is also not necessarily military targets, but a hostile actor tries to use all methods of influence and also in such a way that with the least effort a potentially large impact on society or companies can be achieved.

As a result of the work, it was found that industrial organizations are struggling with a multi-caused cyber security problem. They must adopt a mature security posture in their IT and operational technology environments, at a time when both are subject to an ever-increasing number of attacks - and at a time when the lines between these two areas are blurring more and more every day. Consideration of cyber security should be taken as a starting point already in the planning phase of the systems and cyber threats should be taken into account during use and managed with the help of continuous risk management, and personnel should be trained and trained to act in the right way in preparing for cyber threats.

Keywords/tags (subjects)

ICS, cyber, robotics

Sisältö

Kuviot

Taulukot

1 Johdanto

Työn toimeksiantaja on Jyväskylän ammattikorkeakoulu (JAMK) ja työssä tuli tutkia kuinka kyberturvallisuus on huomioitu teollisuusrobotiikassa. Kyberturvallisuus ja automaatio ovat keskeisiä teknologian opetusalueita Jyväskylän ammattikorkeakoulussa. Opiskelijoita Jyväskylän ammattikorkeakoulussa on noin 9500 ja henkilöstöä noin 900 vuoden 2022 vuosikertomuksen mukaan. Opetuksen lisäksi ”Robotics by JAMK” tuottaa monialaisia automaatio- ja robotiikka-alan asiantuntija-, testaus- ja tuotekehityspalveluita yrityksille ja organisaatioille sekä tarjoaa otolliset olosuhteet robottiteknologian testaamiseen tasokkaissa laboratorio- ja simulaatioympäristöissä. Automaatio ja robotiikka ovat JAMK:ssa vahvuusaloja. Robotiikkaa opetetaan pääsääntöisesti sähkö- ja tutkinto-ohjelmassa sekä robotiikan YAMK-tutkinto-ohjelmassa (www.jamk.fi).

Työssä ei käsitellä palvelurobotiikkaa tai ohjelmistorobotiikkaa, jotta työn laajuus pysyy kohtuullisena. Taustana työlle toimi koulun tarve saada tukimateriaalia tuleviin projekteihin ja erilaisiin hankkeisiin. Tämä tavoite jaettiin kahteen osaan. Ensimmäisenä tavoitteena oli selvittää, millaisia suosituksia standardit asettavat automatisoiduille robotiikan järjestelmille. Toisena oli selvittää kyberturvallisuuden kypsyystasoa kyseisten järjestelmien osalta. Tutkimusmenetelmänä käytettiin integratiivisen kirjallisuustutkimuksen menetelmää.

Alustavan tiedonhankinnan valossa teollisuusautomaatiojärjestelmien suojaamisessa ei ole kyberturvallisuus ollut päällimmäisenä vaan ajatuksellisesti laitteiden toimivuus ja turvallisuus on koneautomaation lähtökohtana teollisuusrobotiikassa. Tästä lähtökohdasta työllä voi olla vaikutusta myös siihen kansallisesti, miten kyberturvallisuus tullaan jatkossa paremmin huomioimaan työssä mahdollisesti löytyvien jatkotutkimus tai kehityskohteiden avulla. Teollisen tuotannon varmuuden varmistaminen on myös huoltovarmuuteen liittyvä tehtävä. Yhteiskunnan toiminnan jatkuminen edellyttää myös sitä, että teollisessa toimintaympäristössä huomioidaan kyberuhkat ja niiden vaikutukset toimintaan. Työn valintaperusteena oli myös omat intressit, eli oman vahvan kokemuksen kyberalalta tuominen toiseen tekniikan osa-alueeseen - automaatioon. Lisäksi teollisuusrobotiikka yhdistelee monen tekniikan alan kuten automaatio, kone, sähkö, tieto, verkko -tekniikan sekä elektroniikan, anturit, toimilaitteet ja näitä mahdollisesti ohjaava tekoälyn. Tämä haastava ja monimutkainen kokonaisuus tulisi toteuttaa huomioiden kyberturvallisuus. Kybersodankäynnin kohteena ei myöskään välttämättä ole sotilaalliset kohteet vaan vihamielinen toimija pyrkii käyttämään kaikki vaikutustavat ja myös siten että vähäisimmällä vaivalla saadaan potentiaalisesti suuri vaikutus.

Työssä käsitellään standardit IEC 62443 ICS (tehty ISA SP99 jatkotyönä), NIST SP-800-82, ISO27001-sarja tai vastaavat, sekä miten ne huomioivat kyberturvallisuutta. Verrataan olemassa oleviin arviointimenetelmiin koneturvallisuuden osalta ja huomioidaan henkilöturvallisuuden riskiarvioinnit-mitä vaaroja miten riskejä tulisi arvioida, miten arvioidaan kyberturvallisuuden riskit.

- IEC 62443-1-1 Konseptit ja malli
- IEC 62443-2-1 Tietoturvaohjelman vaatimukset omistajille
- IEC 62443-4-1 Tuotekehityksen elinkaarivaatimukset
- IEC 62443-4-2 Komponenttien tekniset vaatimukset

Teollisen automaation järjestelmät sisältävät myös toiminnallisen turvallisuuden ohjauslogiikat, joiden tarkoitus on suojata ihmisiä ja omaisuutta onnettomuuksilta. Turvallisuusohjaimet on suunniteltu tarjoamaan lisää turvallisuutta kriittisille prosesseille. Tyypillisesti turvallisuusohjaimia käytetään henkeä pelastavaan pysäytyslogiikkaan. Niihin voi sisältyä mekanismeja, jotka pysäyttävät pyörivät koneistot vaarallisen tilan havaitessaan tai pysäyttävät kaasujen virtauksen tai lämmityksen, kun vaarallinen lämpötila, paine tai muu potentiaalisesti hengenvaarallinen tilanne ilmenee. Turvallisuusohjaimet toimivat erillään normaaleista prosessinohjauslogiikoista ja niiden tarkoituksena on havaita ja estää vaarallisia fyysisiä tapahtumia. Turvallisuusohjaimet ovat usein yhteydessä toimilaitteisiin, jotka estävät normaaleja prosessinohjausjärjestelmiä jatkamasta toimintaansa. Turvallisuusohjaimien tarkoitus on pysäyttää prosessinohjausjärjestelmän toiminta turvallisesti, kun mahdollinen hengenvaarallinen tilanne on havaittu. (IEC 61508)

2 Muuttuva kybertoimintaympäristö

Turvallisuuskomitea on kuvannut seuraavasti kyberturvallisuus ja kybertoimintaympäristön käsitettä:

> ”Kyberturvallisuudella tarkoitetaan tavoitetilaa, jossa kybertoimintaympäristöön voidaan luottaa ja jossa sen toiminta turvataan”
>
> ”Kybertoimintaympäristön toiminnan häiriytyminen aiheutuu usein toteutuneesta tietoturvauhkasta, joten kyberturvallisuuteen pyrittäessä tietoturvallisuus on keskeinen tekijä. Tietoturvan lisäksi kyberturvallisuuteen pyritään muun muassa toimenpiteillä, joiden tarkoituksena on turvata häiriytyneestä kybertoimintaympäristöstä riippuvat fyysisen maailman toiminnot. Siinä missä tietoturvalla tarkoitetaan tiedon

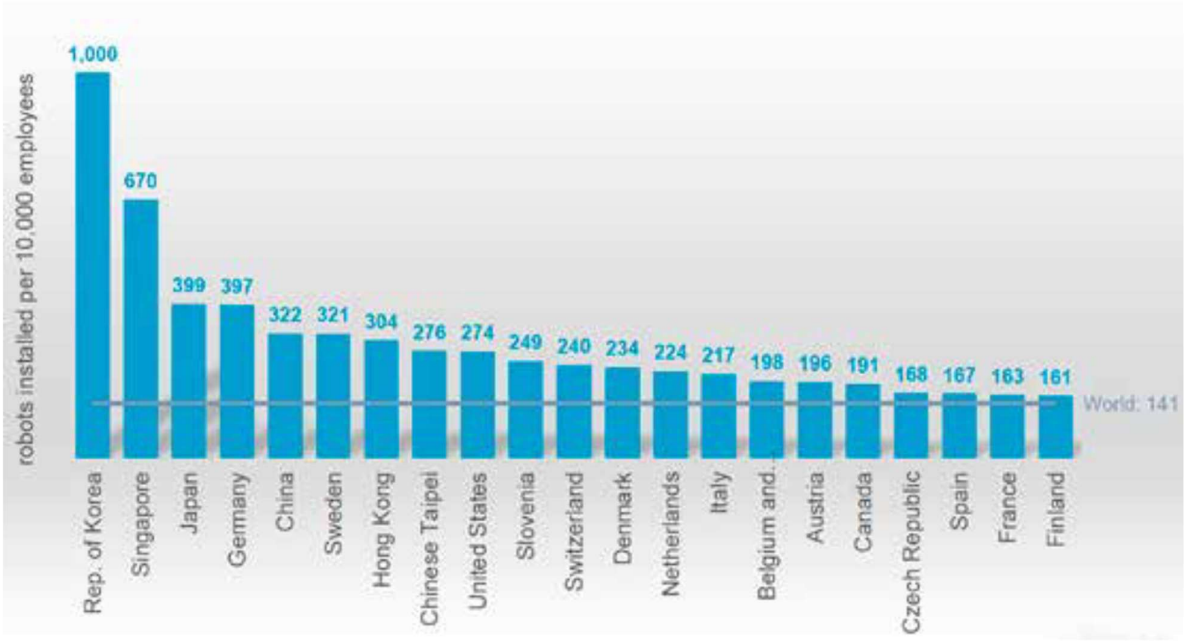
> saatavuutta, eheyttä ja luottamuksellisuutta, kyberturvallisuus tarkoittaa digitaalisen ja
> verkottuneen yhteiskunnan tai organisaation turvallisuutta ja sen vaikutusta niiden toimintoihin.” (VN, Kansallinen riskiarvio, 2018)

Tätä samaa kyberturvallisuuden käsitettä käytetään arvioitaessa teollisen robotiikan järjestelmiä. Perinteisten tuotteita valmistavien tehtaiden ja teollisten laitosten toimintaympäristö on fyysisesti rajoittunut. Tietoverkkojen ja digitalisaation myötä on kehittynyt uudenlaisia uhkakuvia teollisen automaation kybertoimintaympäristölle. Teollisessa automaatiossa ja robotiikassa tulee ottaa huomioon myös laitteita käyttävien tai niiden prosesseihin liittyvien ihmisten toiminta sekä tukifunktiot ja logistiikan järjestelyt. (Lim & al, 2010)

Ihmisen ja robotin toimintaa voi verrata miten ihminen toimii. Ihminen aistii (sensorit), toimii lihasten avulla (toimilaitteet), liikuttaa raajoja (toimilaitteet) ja kaikkea tätä ohjaa aivot (ohjelmisto, koneoppiminen ja keinoäly). Robotin synapsien tilalla on johtimia tai langattomia yhteyksiä, joita pitkin sähköinen informaatio kulkee määritellyillä protokollilla. Järjestelmiä monitoroidaan ja järjestelmissä on ihmisen ja koneen välinen rajapinta. Näistä asioista alkaa muodostua perinteisiä tietoturvauhkia robotin käytettävyydelle. (Market analysis, Robotics Sensors, 2020)

Yleisen teknisen kehityksen myötä on myös teollisen robotiikan toimintaympäristö muuttunut. Uusia uhkia ilmaantuu verkottuneen maailman osalta ja mm. kiristyshaittaohjelmien määrä kasvoi 500 % vuosien 2018–2020 välisenä aikana teollisiin ympäristöihin (Dragos). Teollisen robotiikan ympäristöt on suunniteltu toteuttamaan yleensä yhtä tehtävää, mutta ympäristö koostuu sitä tukevista järjestelmistä ja nämä ovat verkottuneet toisiinsa.

Suomen robottitiheys (161) on vaatimaton verrattuna teollistuneisiin maihin kuten Etelä-korea, jossa on yli tuhat robottia / 10 000 työntekijää. Tässä on tunnistettavissa mahdollisuus parantaa robotiikan toimintaympäristön kyberturvallisuutta laitosten robotisoinnin myötä.



Robottitiheydet teollisuusmaissa, ranking 2021, lähde World Robotics 2022.

Kuvio 1. Robottitiheys teollisuusmaissa, 2022.

Teollinen robotiikka kehittyy jatkuvasti teollisuusmaissa, ja se vaikuttaa monilla aloilla. Robotiikka tarjoaa mahdollisuuksia tehostaa tuotantoa ja parantaa tehokkuutta, mutta samalla se herättää myös kysymyksiä liittyen työvoimaan, eettisiin näkökohtiin ja turvallisuuteen.

3 ICS-järjestelmien kyberturvallisuuden kypsyystaso

Tyypillinen robotiikassa käytettävän teollisen automaation ohjausjärjestelmä ICS-järjestelmä (eng. Industrial Control Systems) sisältää lukuisia ohjaussilmukoita, ihmisrajapintoja ja etädiagnostiikka- ja ylläpitotyökaluja, jotka on rakennettu käyttämällä useita verkkoprotokollia kerroksellisissa verkkoarkkitehtuureissa. Ohjaussilmukka käyttää antureita, toimilaitteita ja logiikkaohjaimia ohjattujen prosessien manipuloimiseen. Anturi on laite, joka tuottaa mittauksen jostain fyysisestä ominaisuudesta ja lähettää sitten nämä tiedot ohjattuina muuttujina ohjaimelle. Ohjain tulkitsee saamaansa signaalit ja generoi vastaavat manipuloidut muuttujat ohjausalgoritmin ja tavoiteasetuspisteiden perusteella, jotka se välittää toimilaitteille. Prosessia ohjataan näiden komentojen perusteella, joiden toimittaminen eheänä perille on tärkeää oikean toiminnan kannalta.(Ngambeki, 2021)

3.1 Teollisuusrobotiikan suojaus

Teollisen robotin toimintaympäristöön tunnistetaan tyypillisesti suoraan robottien ohjaamiseen käytettävät järjestelmät sekä niiden oman kommunikoinnin kanavat (Ackerman, 2017). Tämän lisäksi teollisen robottiympäristön kyberturvallisuuteen liittyvät muut prosessit, jotka tukevat niiden toimintaa. Tällaisia ovat mm. logistinen kanava ja niiden suojaus. Logistisen kanavan kybersuojaamisesta on myös julkaistu standardi “Validating the integrity of computing devices” (NIST SP 800-161 rev 1). Teollisen automaation järjestelmien katkoilla voi olla myös heijastevaikutuksia toimitusketjuihin ja siten ongelmat voivat laajentua muille toimialoille. Osaltaan teollisen automaation ja robotiikan järjestelmät tulisi suunnitella siten, että niiden vaikutukset tai riippuvuudet tunnistetaan yhteiskunnan kriittisen infrastruktuurin osalta. Järjestelmien integroinnin aste on korkea ja ympäristöt sisältävät useiden toimittajien järjestelmiä, jolloin kokonaisuuden ja tietoturvan hallinnasta tulee haasteellisempaa.

3.1.1 Operatiivinen teknologia (OT)

Teollisen robotiikan OT-ympäristöissä tulee turvata toiminnallinen turvallisuus, käytettävyys ja toimintavarmuus. Robotiikan tuotannon järjestelmät kattavat laajan valikoiman ohjelmoitavia järjestelmiä ja laitteita, jotka vuorovaikuttavat fyysisen ympäristön kanssa (tai hallitsevat laitteita, jotka vuorovaikuttavat fyysisen ympäristön kanssa). Nämä järjestelmät ja laitteet havaitsevat tai aiheuttavat suoran muutoksen valvomalla ja/tai ohjaamalla laitteita, prosesseja ja tapahtumia. (IEC 62443)

3.1.2 Suojauksen toteuttaminen

Standardi SP800-82 on National Institute of Standards and Technology (NIST) julkaisema ohjeistus teollisuuden ohjausjärjestelmien (eng. ICS – Industrial Control Systems) tietoturvan parantamiseksi. Standardi ei käsittele pelkästään teollisen robotiikan järjestelmiä vaan tuotannon operatiivisten järjestelmien (OT), mutta sen suositukset ovat sovellettavissa myös robotiikan järjestelmiin. Standardi sisältää useita suosituksia tietoturvan monitoroinnista teollisuusohjausjärjestelmissä.

Suojaukseen käytetään NIST SP-800-82r2 mukaan teollisen robotiikan käyttöympäristöissä seuraavia:

- **Pääsynhallinta**, jolla tunnistetaan käyttäjät ja rajoitetaan oikeudet käyttöoikeuksien mukaisesti. Siinä suunnitellaan verkon arkkitehtuuri turvalliseksi ja toteutetaan riittävät kontrollit verkon hallinnoimiseksi ja turvallisuuden valvontaan.
- **Havainnointi**, kyetään tunnistamaan verkon tai järjestelmän valvonnalla kyberpoikkeamat järjestelmässä. Poikkeamia voi olla haittaohjelmahavainnot tai käyttäjän luvattomat toimenpiteet.
- **Tilaturvallisuus**, jolla estetään asiaton pääsy teollisen robotiikan laitteistoon. Suojaavina kontrolleina voidaan käyttää kulunvalvonnalla toteutettuja tiloja ja lukittavia laitekaappeja.
- **Haavoittuvuuksien hallinta**, jolla estetään järjestelmän haavoittuvuuksien hyväksikäyttö. Tämä tapahtuu haavoittuvuuksien hallinnalla, päivitysten toteuttamisella, testauksella ja laitteiden koventamisella.
- **Tiedonsiirron suojaus**, jolla estetään tiedon auktorisoimaton manipulointi siirrettäessä ja tallennettuna.
- **Kahdennus/varmennus**, joilla varaudutaan erilaisiin vikatilanteisiin ja toteutetaan järjestelmät siten, ettei käytettävyys vaarannu yksittäisten vikojen seurauksena.
- **Varautuminen**, jossa ytimessä on järjestelmän toipumissuunnittelu ja harjoittelu.

3.1.3 CIA-malli

CIA-mallin (eng. CIA-triad) luomisesta on hieman epäselvyyttä ja sille ei löydy varsinaista keksijä tai luojaa. Se on kehittynyt IT-ammattilaisten toimesta ajan kuluessa ja 2000-luvulla malli yleistyi tietoturvallisuuden käytännön menetelmäksi. Mallin lyhenne tulee englanninkielisistä termeistä ”*confidentiality, integrity, availability*” – suomeksi luottamuksellisuus, eheys ja saatavuus. Itse käsitteet ovat olleet pitkään käytössä, kuten luottamuksellisuus Julius Caesarin ajoista, jolloin sitä käytettiin salakirjoitukseen (ROTL #cryptolabs, 2004)

Luottamuksellisuutta pidetään IT-järjestelmissä useimmiten tärkeimpänä tekijänä. Automaatiojärjestelmissä taas saatavuuden merkitys kasvaa ja siihen kiinnitetään huomiota erilaisin teknisin ratkaisuin. Luottamuksellinen tieto on tietoa, johon luvattomilla henkilöillä, tahoilla tai prosesseilla ei saa olla pääsyä, eikä tietoja luovuteta tällaisille tahoille (ISO 27000:2023).

Saatavuus edellyttää sitä, että vain valtuutetulla taholla on tarvepohjainen pääsy- ja käyttöoikeus kohteeseen siten että resurssi myös on saatavilla. Tiedon eheys on toimintaedellytys robotiikan

järjestelmille. Käskyjen ja komentojen tulee kulkea muuttumattomina ohjausjärjestelmästä toimintalaitteeseen. Eheys on tiedon ominaisuus, johon sisältyy tiedon virheettömyys, oikeellisuus ja kattavuus (ISO 27000:2023). Jos esimerkiksi tietoliikennettä salataan kapasiteettia vaativilla ratkaisuilla saattaa tiedon saatavuus heikentyä reaaliaikajärjestelmissä. Tietoturvallisuuden CIA-malli on kuitenkin kompromissi, eli jos painotetaan luottamuksellisuutta niin jokin toinen osa-alue ei ole niin merkittävällä painoarvolla. Käytännössä tämä tarkoittaa, että jos saatavuus on tärkein prioriteetti niin luottamuksellisuus saattaa kärsiä sen seurauksena. Teollisen robotiikan järjestelmissä tiedon eheys on yleensä hyvin tärkeä, koska robotiikan ohjauksen tulee mennä täysin oikeana perille oikeana hetkenä.

3.2 ICS-järjestelmien haavoittuvuuksien määrän kehitys

ICS-järjestelmien raportoitujen haavoittuvuuksien määrä on ollut suhteellisen pieni, mutta yleinen mielenkiinto järjestelmiin ja niiden haavoittuvuuksien kartoittamiseen on lisännyt raportoitujen haavoittuvuuksien määrää. Tämän lisäksi toimintaympäristössä tulee tunnistaa myös ympäröivän ICT-infrastruktuurin haavoittuvuudet ja sen mahdolliset liitynnät teollisen tuotannon ohjausjärjestelmään.

3.2.1 Haavoittuvuustietokanta (CVE)

Internetissä on haavoittuvuustietokantoja ja yksi niistä on ”Common Vulnerabilities and Exposures” (CVE). Siihen on kerätty tietoa, joka on suunniteltu auttamaan tietoturvallisuuden parissa työskenteleviä tunnistamaan, seuraamaan ja jakamaan tietoja tietoturvariskeistä ja haavoittuvuuksista. Tämä järjestelmä tarjoaa yhtenäisen tavan haavoittuvuuksien nimeämiseen ja luokitteluun vertailukelpoisesti. Se koostuu numeerisista tunnisteista (vuosiluku ja juokseva tunniste numero), joiden avulla voidaan yksilöidä tiettyjä tietoturvaongelmia. Haavoittuvuuksia voi tarkastella internet-osoitteessa ”https://cve.mitre.org/”.

Tärkeimmät tiedot CVE-järjestelmässä ovat:

> **CVE-numero**: Jokainen haavoittuvuus saa yksilöllisen numeron. Esimerkiksi "CVE-2023-12345". Tämä numero on pysyvä ja ainutlaatuinen, ja se auttaa yksilöimään tietyn haavoittuvuuden yksiselitteisesti.

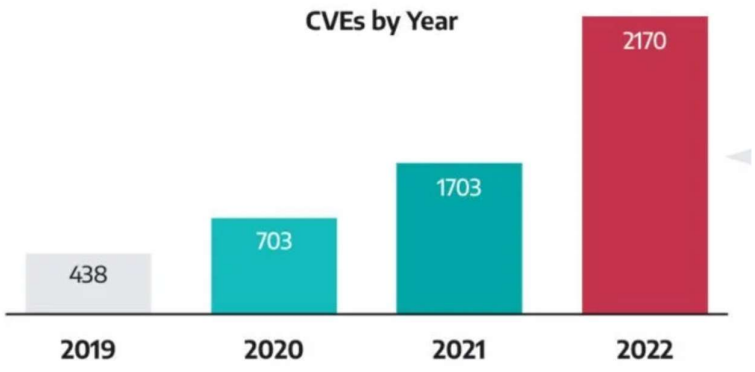
Kuvaus: Jokaiselle CVE-numerolle liittyy kuvaus kyseisestä haavoittuvuudesta. Tämä kuvaus sisältää yksityiskohtaiset tiedot siitä, miten haavoittuvuus vaikuttaa järjestelmään ja mitä riskejä se aiheuttaa.

Viittaukset: CVE-numeroita käytetään laajasti tietoturvaraporteissa, tietoturvaohjeissa ja -tietokannoissa, jotta tietoturva-asiantuntijat ja organisaatiot voivat tunnistaa ja korjata haavoittuvuudet nopeasti.

CVE-järjestelmän tarkoituksena on parantaa tietoturvallisuuden haavoittuvuuksien hallintaa ja helpottaa haavoittuvuuksien ja altistumisten jakamista ja raportointia. Se auttaa myös organisaatioita tunnistamaan omiin järjestelmiinsä liittyvät haavoittuvuudet ja ryhtymään tarvittaviin toimenpiteisiin niiden korjaamiseksi. Haavoittuvuuksien arviointiin on tarjolla yhteinen kriteeristö, Common Vulnerability Scoring System (CVSS) (FIRST – Forum of Incident Response and Security Teams, www.first.org). Kriteeristö on käytännön standardi tietoturvallisuuden arvioinnissa. Mitren haavoittuvuustietokantaan on tarjolla myös liityntä (eng. Application programming interface, API), jolloin tietokantaa voidaan hyödyntää automaattisesti tietojärjestelmissä. Rajapinta toteuttaa liityntätavan ja protokollan, millä tavalla ohjelmat voivat pyytää ja vaihtaa tietoa toisen ohjelman tai palvelun kanssa.

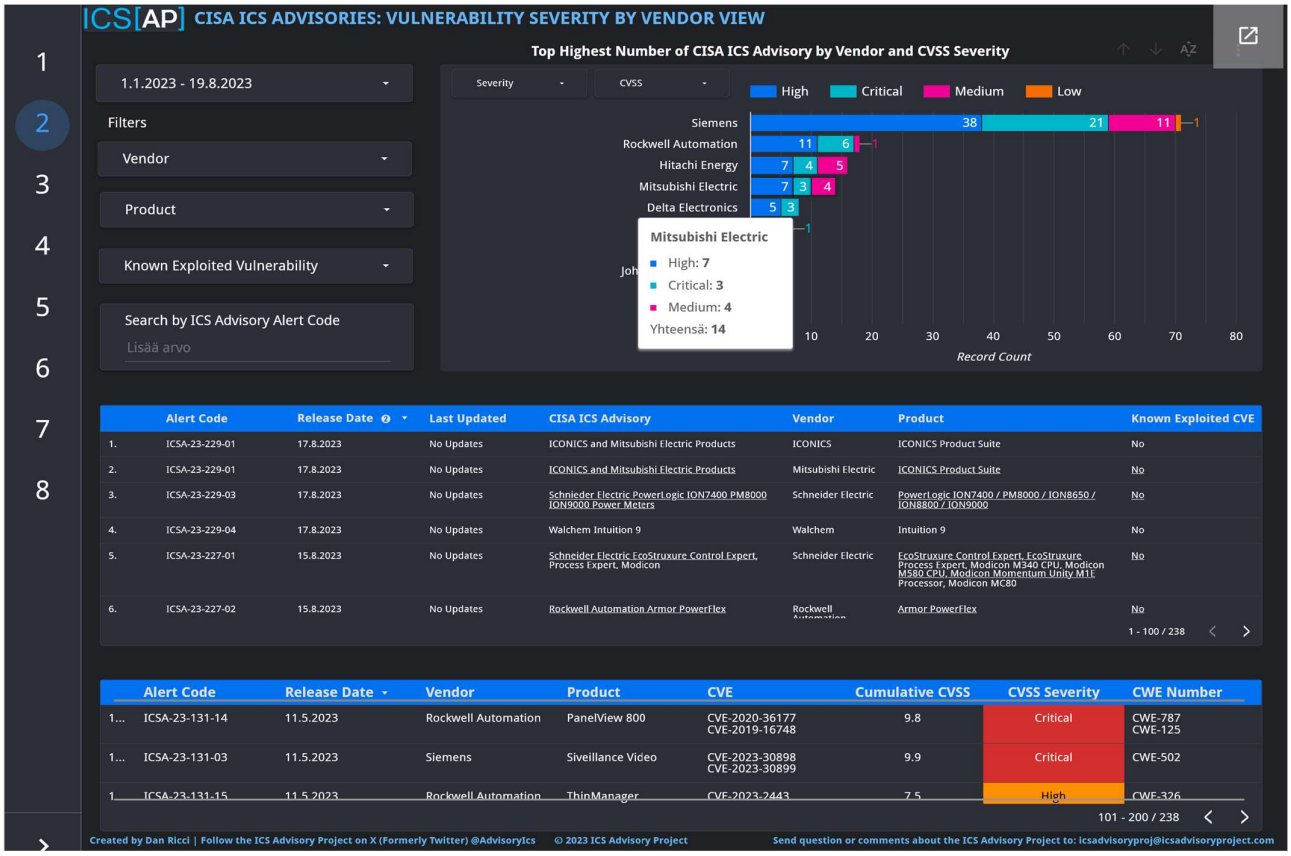
3.2.2 Haavoittuvuuksien kehittyminen ICS-järjestelmissä

Haavoittuvuuksien seurantaan on rakennettu myös sivustoja, joiden avulla voidaan laitevalmistajakohtaisesti hakea haavoittuvuuksia ja arvioida millaisia haavoittuvuuksia omaan järjestelmään kohdistuu. Kuvion kaksi mukaisesti haavoittuvuuksien määrä suurenee voimakkaasti ja sen voi olettaa aiheutuvan siitä, että haavoittuvuuksia etsitään ja raportoidaan enenevässä määrin.



Kuvio 2. Raportoidut haavoittuvuudet (Reported CVEs), Dragos 2023.

Alla olevassa kuvassa on listattu 2023 raportoituja haavoittuvuuksia ja niiden jakaumaa eri valmistajien suhteen. Sivusto päivittyy jatkuvasti ja sen tai vastaavan seuraaminen on suositeltavaa robotiikan järjestelmien turvallisuudesta vastaaville henkilöille. Haavoittuvuudet sisältävät linkityksen haavoittuvuuskuvauksiin ja niiden vaikutusten vähentämiskeinoihin Yhdysvaltojen kyberturvallisuuskeskuksen internet-sivustolla (CISA, www.cisa.gov).



Kuvio 3. Raportoidut ICS-haavoittuvuudet vuonna 2023 (Lähde, www.icsadvisoryproject.com 19.8.2023)

4 Riskienarviointi

Työssä pyrittiin löytämään ne menetelmät, jotka parhaiten sopivat teollisen robotiikan infrastruktuurin tietojärjestelmien kyberriskien hallintaan ja arviointiin. Työssä analysoitiin, miten tietojärjestelmien riskienhallintaa voidaan hyödyntää teollisen robotiikan ympäristöissä, sekä miten tietojärjestelmien riskit vaikuttavat kokonaisriskienhallinnassa ja miten kriittisen infrastruktuurin

haavoittuvuudet vaikuttavat tietojärjestelmiin ja niiden informaatioturvallisuuteen. Tarkastelemalla aiemmin tapahtuneiden onnettomuuksien tai luonnonilmiöiden vaikutuksista tietojärjestelmiin ja analysoidaan missä tapauksessa tietojärjestelmät vahvistavat onnettomuuden seurannaisvaikutuksia ja missä tapauksessa heikentävät sekä muodostaako ulkoinen riski sellaisen uhkan informaatio- tai operaatioturvallisuudelle siten, että se pitää huomioida tietojärjestelmien suunnittelussa alusta lähtien. Teollisen automaatioympäristön erottaa perinteisestä IT-ympäristöstä se tekijä, että kyberuhkat voivat vaikuttaa huomattavasti enemmän suoraan fyysiseen maailmaan ja aiheuttaa onnettomuuksia.

4.1 Toimintaympäristön analysointi

Olennaista on ymmärtää toimintaympäristö ja siihen vaikuttavat ulkoiset ja sisäiset asiat, jotka vaikuttavat kykyyn saavuttaa kyberturvallinen kokonaisuus teollisen robotiikan toimintaympäristössä ml. sidosryhmät. Tietoturvallisuuden riskejä voidaan arvioida mm. standardin ISO 27001:2022 avulla ja koneturvallisuuden osalta ISO 12100. Itse riskiarvioinnin vaiheet ovat samat, mutta yleensä esille tuodut vaarat hieman erilaisia (raajojen silpoutuminen tai tietokoneviruksen aiheuttama tehtaan pysähtyminen). Ensimmäinen askel on ymmärtää täysin järjestelmä ja sen komponentit. Toimintaympäristön analysoinnissa tulee selvittää, miten järjestelmä on rakennettu, mitkä ovat sen toiminnot ja kuinka se on liitetty muuhun infrastruktuuriin. Ohjelmistojen ja laitteistojen tyypit sekä ohjelmistoversiot ovat olennainen osa tietoa, joita tarvitaan myöhemmissä arvioinnin vaiheissa.

4.2 Analysoi potentiaaliset hyökkäystavat

Toimintaympäristön tunnistamisen jälkeen selviää mm. järjestelmän liitynnät muihin järjestelmiin, sen tietoliikenneyhteydet ml. radiorajapinnat. Siinä tunnistetaan mistä tietoa tulee järjestelmään ja miten tietoa raportoidaan. Näiden tunnistamisen avulla voidaan arvioida järjestelmän asiantuntijoiden avulla, kuinka järjestelmä saattaisi olla haavoittuva tarkoituksellisesti tai vian seurauksena. Hyökkäystapojen tunnistamiseen voidaan käyttää esimerkiksi Mitren luomaan ICS-hyökkäyskarttaa (https://attack.mitre.org/matrices/ics/).

4.3 Tunnista järjestelmän haavoittuvuudet

Toimintaympäristön tunnistamisen jälkeen voidaan laitteisto- ja ohjelmistoversiotietojen avulla rakentaa kartta haavoittuvuuksista, jotka kohdistuvat järjestelmään. Yhdistämällä se tietoon potentiaalisista järjestelmää uhkaavista hyökkäystavoista voidaan priorisoida tietoturvakontrolleja, joilla potentiaalisia ongelmia poistetaan. ICS-järjestelmien haavoittuvuuksia voidaan kartoittaa hieman helpommin https://www.icsadvisoryproject.com/ sivuston avulla. Muun IT-infrastruktuurin haavoittuvuuskantana voidaan käyttää Mitren CVE-tietokantaa, joka sisältää myös tavanomaisten käyttöjärjestelmien ja oheisohjelmien haavoittuvuudet.

4.4 Suojaustapojen arviointi

Suojauskeinoja voidaan suunnitella sekä teknisiä että toiminnallisia. Turvallisuuden prosesseja voidaan muuttaa, kouluttaa ja ohjeistaa ihmisiä toimimaan oikein. Tekniset toimenpiteet ovat yleensä suositeltuna haavoittuvuustietokantojen toimenpiteinä. Useasti toimenpidesuositus on järjestelmien päivittäminen, joka saattaa olla haasteellista tuotannon aikataulujen ja kokonaistestauksen osalta. (ISO 12100)

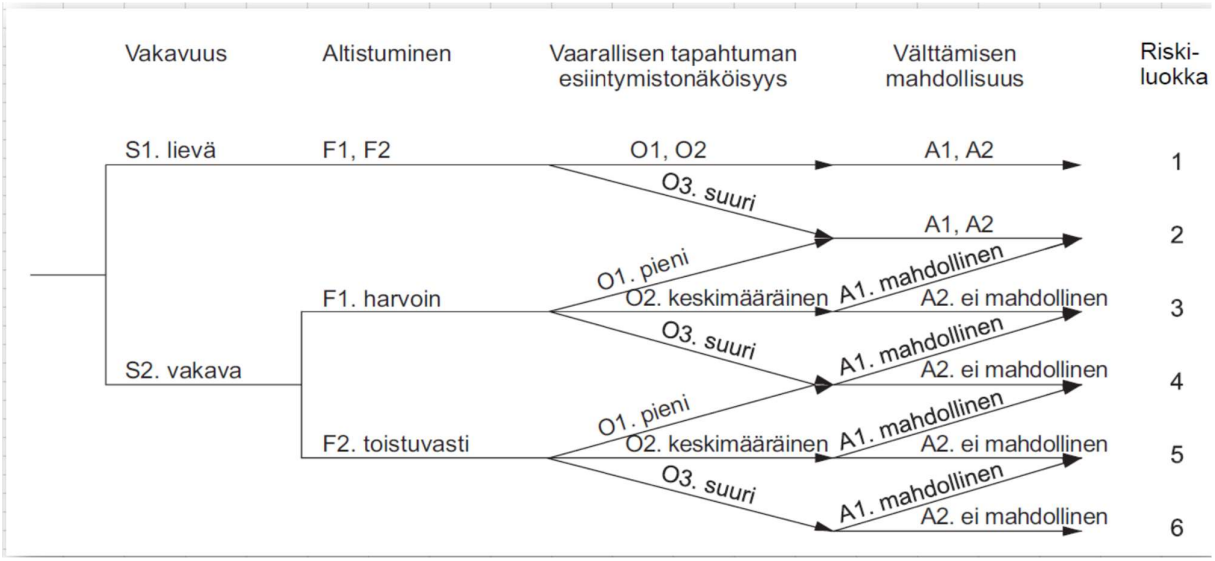
4.5 Riskienarviointi

Riskiarvioita aloitettaessa selvitetään mitä vaaroja järjestelmän käyttöön sisältyy. Konetekniikassa arvioidaan esimerkiksi sitä mitä vaaroja ihmisten loukkaantumiseen on. Samalla tavalla tulee arvioida mitä riskejä kyberuhkat aiheuttavat. Riskejä arvioidaan niiden todennäköisyyden ja vaikutuksen avulla. Yleensä näille tekijöille annetaan, joltain asteikolta arvot ja näiden tulo on arvioitu riski. (Risk Analysis, Baskerville (1991). Baskerville tuo esille riskianalyysin roolia ja merkitystä tietojärjestelmien tietoturvan perustelemisessa. Se korostaa riskianalyysin tulkinnallista ja soveltavaa luonnetta päätöksenteossa. Riskianalyysi tarjoaakin käyttökelpoisen työkalun arvioida ja perustella tietoturvatoimenpiteitä, ja sen avulla voidaan tunnistaa ja hallita uhkia sekä haavoittuvuuksia tietojärjestelmissä. Riskienhallinta ja siihen kuuluva riskianalyysi ei ole vain teknisiä toimenpiteitä vaan myös liiketoiminnallinen ja organisaatiota koskeva kysymys. Tietojärjestelmien tietoturvan parantaminen vaatii kokonaisvaltaista lähestymistapaa, ja riskianalyysi on keskeinen osa tätä prosessia arvioida ja resursoida oikein riskien vaikutusten vähentäminen (ISO 12100).

Riskienhallintaan kuuluu, että arviointikriteerit on määritetty, arviointi suoritetaan puolueettomasti ja että se dokumentoidaan sekä esitellään johdolle. Kyberturvallisuuden riskienarviointi on tärkeä osa teollisen robotiikan ICS-järjestelmän ylläpitoa. Sen avulla voidaan tunnistaa ja estää mahdolliset haavoittuvuudet ja minimoida riskit, jotka voivat johtaa tietomurtoihin tai muihin turvallisuusongelmiin (SP 800-30r1).

4.6 Jäännösriskien käsittely

Riskien analysoinnin jälkeen saattaa jäädä riskejä, joiden ottamista ei haluta tehdä. Riskienhallinnassa tuleekin laatia toimintasuunnitelma riskien vähentämiseen sekä hyväksyttää riskit liiketoiminnan johdolla. Kuvion neljä mukaisesti arvioidaan koneturvallisuuden riskejä ja sen avulla voidaan muodostaa riskiluokka.



Kuvio 4. Ote standardista SFS-ISO/TR 14121-2: Esimerkki riskin suuruuden arviointiin käytettävästä riskigraafista.

Riskienarviointia helpottamaan on tehty lomake, jolla koneturvallisuusstandardissa helpotetaan arviointien tekemistä ja niiden vertailukelpoisuutta. Riskienarvioinnin tekeminen on edelleen ihmisten tekemiseen perustuvaa, joten sen luotettavuus riippuu siitä, kuinka hyvin riskienarviointi on kyetty laatimaan. Koneturvallisuuden standardin lomake on tehty erityisesti henkilöturvallisuu-

den ja omaisuuden tuhoutumisen osalta. Vakavimpina riskeinä pidetään kuolemaan johtavia onnettomuuksia ja ne pyritään aina estämään. Kyberriskejä ei lomakkeessa anneta esimerkkeinä, mutta niiden arviointiin on hyvä käyttää myös vakioitua pohjaa. Pahimmillaan kyberuhkat voivat aiheuttaa onnettomuuksia, joissa menehtyy ihmisiä. Varsinkin kun kyberuhkiin liittyy myös se, että niiden aiheuttajalla saattaa olla pahantahtoinen motiivi (Mäntylä, J. 2014). Kyberuhkien vaikutukset saattavat myös laajentua teollista toimintaa tukevasta ympäristöstä.

Suojaustoimenpiteiden järjestys riippuu tietoturvallisuuden riskienarvioinnista ja uhkien priorisoinnista. Standardin ISO27005-2022 mukaan tietoturvallisuuden riskienhallinnassa noudatetaan usein seuraavia vaiheita:

- **Riskienarviointi:** Ennen kuin suojaustoimenpiteitä voidaan suorittaa, tietoturvallisuusriskit on ensin arvioitava. Tämä voidaan tehdä esimerkiksi riskienarvioinnilla, joka auttaa tunnistamaan järjestelmän haavoittuvuudet ja niiden mahdolliset seuraukset.
- **Priorisointi:** Kun riskit on tunnistettu, ne on arvioitava niiden vakavuusasteen mukaan ja asetettava tärkeysjärjestykseen. Tämä auttaa priorisoimaan toimenpiteet sen mukaan, mikä uhka aiheuttaa suurimman riskin järjestelmän tietoturvallisuudelle.
- **Toimenpiteiden valinta:** Kun riskit on priorisoitu, valitaan suojaustoimenpiteet, joilla niitä voidaan vähentää tai poistaa.
- **Toimenpiteiden toteuttaminen:** Suojaustoimenpiteet toteutetaan järjestyksessä sen mukaan, kuinka tärkeitä ne ovat ja kuinka suuren riskin uhka aiheuttaa.
- **Seuranta ja päivitys:** Riskienhallintatoimenpiteiden jälkeen tulee toimenpiteiden toimeenpanoa seurata ja arvioida riskit säännöllisesti uudelleen.

ISO31000 -standardissa riskien arviointi on määritelty kokonaisprosessiksi, joka sisältää riskien tunnistamisen, riskianalyysin ja riskin merkityksen arvioimisen. Riskien tunnistaminen on riskien havaitsemista ja kuvaamista. Riskianalyysi on prosessi, jonka avulla pyritään arvioimaan riskien vaikutuksia ja todennäköisyyksiä, sekä määrittämään hyväksytty riskitaso.

4.6.1 Uhka

Uhka on epätoivottu tapahtuma, joka voi johtaa jonkin menetykseen tai tuhoon Merriam-Websterin sanakirjan mukaan. Ylemmällä tasolla voidaan ajatella olevan olemassa vaaroja, joista muodostuu uhkia myös kyberturvallisuuden osa-alueella. Esimerkiksi jos tunnistetaan vaara, että teollisen automaation järjestelmän verkkoon hyökätään järjestelmän ulkopuolelta, voidaan muodostaa uhkia ja niistä aiheutuvia riskejä. Uhkamallinnus toteutetaan siten, että määritetään uhat ja suojattavat komponentit sekä immateriaalinen omaisuus, joka voi vahingoittua. Uhkamallinnuksen tavoitteena on saada vähennettyä riskejä. Riskianalyysissä arvio tehdään kokonaisuuteen kohdistuvan vaikutuksen perusteella, joka on todennäköisyyden ja luokitellun tapahtuman vakavuuden tulo. Arvioinnissa on tärkeä tunnistaa seurannaisvaikutukset ja kokonaisuuden arviointi. Teknisesti jokin pieni asia voi jäädä riskiarviossa vähälle huomiolle, mutta kumulatiivinen vaikutus monen tekijän toteutuessa voi johtaa katastrofiin. Tietoteknisen maailman riskeissä on vaara, että keskitytään vain sähköiseen maailmaan. Kuitenkin kyberturvallisuudessa tulee huomioida toimintaympäristö ja sen fyysiset ulottuvuudet sekä niihin kohdistuvat vaarat. Esimerkkinä kumulatiivisesta vaikutuksesta on Fukushiman ydinvoimalan onnettomuus, jossa tapahtui ensin maanjäristyksen seurauksena sähkökatko ja tsunami. Ydinvoimalan varavoima ei toiminut tsunamin seurauksena. Voimalan polttoaine alkoi kuumeta tämän seurauksena. Polttoaineen kuumeneminen aiheutti räjähdyksiä ja säteilyvuodon, joka vaikeutti korjaustoimenpiteitä. Ydinvoimalassa oli kuitenkin varmasti riskiarvioita laadittu, mutta silti onnettomuus tapahtui (STUK, https://stuk.fi/fukushiman-ydinvoimalaitoksen-onnettomuus). Odottamattomien ongelmien korjaamista voidaan harjoitella skenaarioajattelulla kriittisen toiminnan osalta. Kyberuhkiin varautumisen harjoittelun yhteydessä usein tunnistetaan tapoja, kuinka suojauksia voitaisiin ohittaa käyttäjien toimesta, jotka toimivat järjestelmän parissa päivittäin. Uhka-arvioita tehtäessä ei pelkästään uhkien listaaminen riitä, vaan niiltä edellytetään syvällisempää syy-seuraussuhteiden ymmärrystä (Potts, 2012).

4.6.2 Motiivi

Kyberuhkatoimijat voidaan jakaa kolmeen ryhmään: verkkorikolliset, vilpilliset työntekijät ja valtiolliset ryhmittymät. Verkkorikollisten motivaationa on taloudellisen edun tavoittelu. He hyökkäävät kohteisiinsa internetin välityksellä etsien järjestelmistä haavoittuvuuksia ja niitä hyödyntäen tunkeutuvat järjestelmiin asentaen haitallista koodia tai varastavat tietoa. Kohteet valikoituvat useimmiten satunnaisesti; mistä vain automatisoitu koputtelu sattuu löytämään aukkoja. Vilpilliset

työntekijät puolestaan ovat usein tyytymättömiä työnantajaansa ja taloudellista etua tavoitellessaan suorittavat yritykselle haitallisia toimenpiteitä. Heidän käyttämänsä menetelmät eivät välttämättä ole niin kehittyneitä kuin verkkorikollisten. On myös mahdollista, että he esimerkiksi myyvät hallussaan olevia järjestelmätietoja verkkorikollisille, jotka puolestaan hyödyntävät niitä varsinaisen tunkeutumisen yhteydessä. Valtiollisten toimijoiden vihamielisen toiminnan motivaationa voivat olla joko taloudelliset tai poliittiset syyt. Tällaisilla ryhmittymillä on tyypillisesti merkittävät resurssit käytettävissään, joten niiden toteuttamat operaatiot voivat olla hyvinkin pitkäkestoisia ja niissä käytettävät haittaohjelmat erittäin kehittyneitä. (Lehto, 2013)

4.6.3 Keinot

Mitren ATT&CK-kehikko mahdollistaa tunnistaa hyökkäystapoja, jotka kohdistuvat järjestelmään. Kehikko on erikseen myös ICS-järjestelmille ja sitä voidaan hyödyntää, kun arvioidaan OT-järjestelmiä ja sen uhkia. Ymmärrys järjestelmän haavoittuvuudesta auttaa määrittämään kontrollit, joilla epätoivotut tapahtumat voidaan estää.

Mitre esittää matriisin taktiikoista, joiden avulla hyökkääjä etenee (Mitre, 2023);

1. Verkkoon pääsy
2. Koodin suoritus
3. Jalansija
4. Oikeuksien laajentaminen
5. Sulautuminen/piiloutuminen
6. Järjestelmän kartoitus
7. Lateraalinen siirtyminen
8. Tiedon kerääminen
9. Yhteys komentopalvelimeen
10. Verkonvalvonnan kontrollien rajoittaminen
11. Prosessien kontrolliin vaikuttaminen
12. Ohjausjärjestelmän manipulointi ja vaikutusten aiheuttaminen

Hyökkäys etenee vaiheiden mukaisesti ja jokaiseen vaiheeseen liittyvät menetelmät ovat kuvattu liitteessä yksi. Vaiheiden tunnistaminen auttaa valitsemaan sopivat kontrollit ja suojaustoimenpiteet niitä vastaan sekä muodostamaan tilannetietoisuuden siitä, kuinka hyökkäys saattaisi tapahtua.

Mitren hyökkäyskartta auttaa hahmottamaan mikä motiivi on uhkatoimijalla, voiko kybervaikuttaminen olla uhkatoimijan mahdollinen ja todennäköinen toimintatapa. Sen tulisi auttaa selvittämään miten juurisyy voidaan poistaa, sen sijaan että tehdään kompensoivia kontrolleja. Teollisuuden katkot maksavat paljon, tästä syntyy motiivi syöttää kiristyshaittaohjelma. Tällöin motiivi on aiheuttaa merkittävä häiriö ja mahdollisesti suuri tuotto haittatoimijalle. Tämä johtaa siihen, että haittakoodi muokataan yksilöllisesti ja sitä ei tunnisteta automaattisesti esimerkiksi yrityksen käytössä olevalla virustorjuntaohjelmistolla. Tällöin havainnointi täytyy perustua siihen, miten hyökkääjä toimii ja sen tunnistamiseen järjestelmästä (anomalia). Hyökkääjä ei myöskään pyri toimimaan välttämättä siten, että hyökkäys toimitetaan kaikkien rakennettujen kontrollien läpi. Kontrollien ohittaminen on edullista hyökkääjälle. Tämä voidaan saavuttaa hyökkäämällä alihankintaketjun tai henkilön kautta, jolla on pääsy järjestelmään. Käyttäjän ei tarvitse olla edes tietoinen asiasta, vaan tietoja voidaan varastaa heikosti suojatusta kotikoneesta tai saastuttaa se haittakoodilla.

4.7 Riskien käsittely

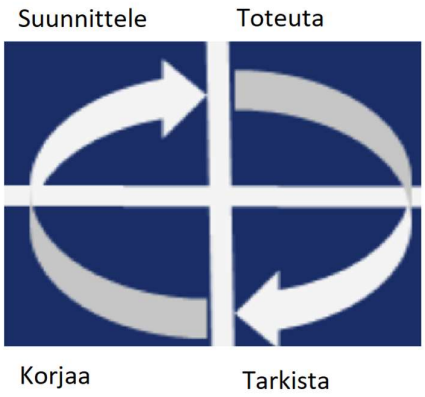
Riskienarvioinnin tuloksena saatuja riskejä käsitellään ja niiden hallitseminen voidaan toteuttaa riskejä siirtämällä, vähentämällä, välttämällä tai hyväksymisellä.

- Riskien siirtäminen, tehtävä siirretään alihankkijalle tai sitä varten otetaan vakuutus. Huomattavaa on, että menetelmä ei vaikuta välttämättä tapahtuman todennäköisyyteen.
- Riskien vähentäminen, tehdään korjaavia toimenpiteitä, joiden avulla vaikutus pienenee.
- Riskien välttäminen, jos on mahdollista jättää toimenpide suorittamatta. Esimerkkinä jos teollisuusautomaatio järjestelmä pidetään internet-verkon ulkopuolella, erotettuna se pienentää merkittävästi uhkaa julkisesta verkosta.
- Riskien hyväksymisellä tarkoitetaan sitä, että riski ollaan valmis ottamaan arvioidulla tasolla.

Riskienhallinnan vertailun kannalta kannattaa määrittää vertailukelpoiset tasot; esim. vähäinen, keskisuuri, merkittävä ja sietämätön, sekä kuvaukset tason kriteereistä helpottamaan arvioinnin toteuttamista.

Riskien hallintaa tulee toteuttaa säännöllisesti ja seuranta jatkuvasti ja pyrkiä jatkuvaan parantamiseen. Sen tekemiseksi tulee määritellä suorituskyvyn arviointiin tavoitteet, tunnistaa käytettävät mittarit, valita sopivat työkalut seurantaan, suorittaa mittaukset ja analysoida tulokset.

Suorituskyvyn arviointia voidaan toteuttaa standardin ISO27001:2022 avulla. Se voidaan toteuttaa esimerkiksi kuvion viisi mukaisen PDCA-syklin avulla (eng. plan, do, check, act).



Kuvio 5. PDCA-sykli suomeksi

Jatkuva seuranta tarkoittaa sitä, että organisaatio seuraa jatkuvasti riskejä ja niiden hallintaa. Tämä voi sisältää riskitilanteiden tunnistamista ja raportointia, riskienhallintaprosessin arviointia ja päivittämistä sekä riskienhallintatoimenpiteiden seurantaa ja arviointia. Jatkuva seuranta auttaa organisaatiota pysymään ajan tasalla riskeistä ja niiden hallinnasta. (ISO27001:2022)

Parantaminen tarkoittaa sitä, että organisaatio pyrkii jatkuvasti parantamaan toimintaa riskienhallinnan toteuttamisella. Tämä voi sisältää riskienhallintaprosessin ja riskienhallintatoimenpiteiden kehittämistä, sekä riskienhallinnan koulutusta organisaation henkilöstölle. Parantaminen auttaa organisaatiota kehittämään parempia käytäntöjä ja prosesseja riskeille alttiiden kohteiden tunnistamiseksi ja käsittelemiseksi, jolloin organisaatio on paremmin valmistautunut käsittelemään riskejä tulevaisuudessa. (ISO27001:2022)

Riskit tulee esitellä toiminnasta vastaavalle taholle – yrityksen johto, joka voi arvioida vaikutuksia myös koko liiketoiminnalle. Riskien arvioinnissa voidaan käyttää seurantaa helpottavaa lomaketta tai ohjelmistoa, jolle kirjataan toimenpide-ehdotuksen toteuttamisesta vastaava henkilö, toimenpiteen tila, toteutuksen aikataulu ja mahdolliset muut kommentit. Tällä menettelyllä arvioitua riskiä voidaan arvioida säännöllisesti ja päivittää tiedot toimenpiteiden edistyessä.

4.8 Käsittelymenetelmä

ICS-järjestelmien toimintaympäristön analysointi ja riskienarviointi voidaan toteuttaa seuraavin askelin. Kuvattu menettely yhdistää kyberuhkien arvioinnin ja riskienhallinnan menettelyä. Alla

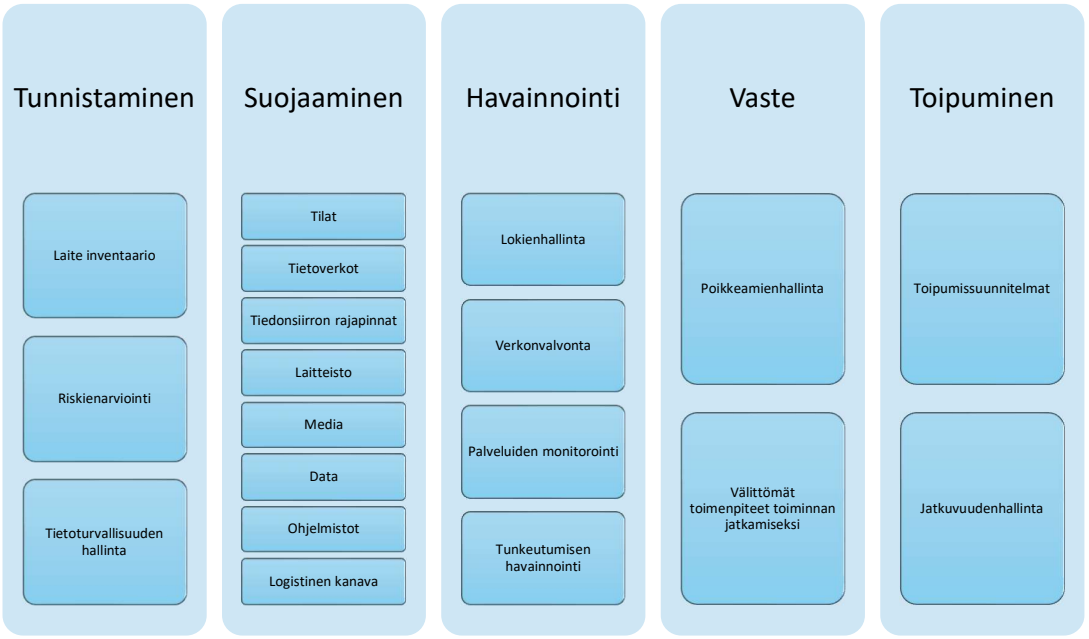
olevassa kuvassa esitetään vaiheita, joilla kyberriskien käsittely voidaan tehdä. Se on yksinkertaistettuna seuraavanlainen; toimintaympäristön tunnistaminen, ympäristöön kohdistuvat uhat, ympäristön haavoittuvuudet, suojaustoimenpiteet ja jäännösriskien käsittely. Luonnollisesti koko järjestelmän elinkaaren ajan sen riskejä hallitaan sen rakentamisen jälkeen jatkuvalla prosessilla huomioiden ympäristön muutokset.

Kuvio 6. Kyberuhkien ja riskien käsittely (kuvion kuvat Creative Content Microsoft)

Toimintaympäristön tunnistamisen tarkoituksena on rajata järjestelmä sekä tunnistaa sen ulkoisen liitynnät. Samassa yhteydessä tulee tunnistaa myös suojattavien kohteiden priorisointi. Tämän jälkeen on mahdollista arvioida järjestelmään kohdistuvia uhkatoimijoita ja mahdollisia menetelmiä. Kun uhkat on arvioitu, niin järjestelmien haavoittuvuudet tulee tunnistaa. Tämän jälkeen asetetaan turvallisuuskontrollit suojaamaan järjestelmiä hyödyntäen priorisointia. Prosessin suorittamisen jälkeen arvioidaan mitä jäännösriskejä jää jäljelle toimenpiteiden jälkeen. Tyypillisesti jos riskienhallinnassa jää merkittäviä riskejä niin niiden ottaminen jää yleensä johdon tehtäväksi, koska heillä on myös mahdollisuus resursoida riskien poistamiseen liittyviä hankintoja ja kehitystehtäviä.

5 Kyberturvallisuus teollisessa automaatioympäristössä

Teollisuuden ohjausjärjestelmien (ICS, Industrial Control Systems) elinkaari on yleensä erittäin pitkä. Järjestelmiin tehdään harvoin päivityksiä, ja elinkaaren loppuvaiheessa saattaa olla mahdollista, että tietoturvapäivityksiä ei enää ole saatavilla. Tämä lisää järjestelmien haavoittuvuutta merkittävästi. Riskiä kasvattaa myös se, että teollisuuden ohjausjärjestelmien ja laitteiden kokonaiskuvaa ei välttämättä ole selkeästi hahmotettu OT-ympäristössä. Tämä tarkoittaa tilannetiedon puutetta siitä, mitkä järjestelmät ovat verkossa, onko niihin tehty päivityksiä tai ovatko ne alttiita mahdollisille haavoittuvuuksille. Toimintaympäristön tunnistaminen on ensimmäinen askel ympäristön suojaamisessa, prosessin askelia voidaan kuvata seuraavan kaavion avulla, joka käsittää vaiheet: tunnistaminen, suojaaminen, havainnointi, vaste ja toipuminen. (Flaus, 2019)



Kuvio 7. Tietoturvallisuuden hallintaprosessi ICS-järjestelmissä

Flausin mukaan riskienhallinta sisältyy tietoturvallisuuden prosessiin ja se tehdään osana sitä. Tässä tapauksessa täytyy huomioida, että menettely sopii erittäin hyvin siihen mitä on kuvattu kappaleessa riskienarviointi. On vain kyse siitä katsotaanko asiaa kyberturvallisuuden, tietoturvallisuuden vai riskienhallinnan suunnasta. Teollisen robotiikan osalta asiaan liittyy myös koneturvallisuus ja sen riskiarvio.

5.1 Ohjelmoitava logiikkaohjain

Ohjelmoitava logiikkaohjain (eng. PLC on lyhenne sanoista Programmable Logic Controller) on laite, joka on suunniteltu teollisuusautomaation ohjaamiseen ja valvontaan. Logiikkaohjaimet ovat tärkeä osa automaatiojärjestelmiä, joissa ne keräävät tietoja antureilta ja käsittelevät niitä ohjelmoidun logiikan mukaisesti. Ne sitten ohjaavat toimilaitteita, kuten moottoreita, venttiilejä ja muita laitteita, jotka toteuttavat teollisuusprosesseja.

Logiikkaohjainten rakenne on modulaarinen, joita voidaan yhdistellä tarpeen mukaan. Moduulit sisältävät yleensä erilaisia tuloja ja lähtöjä, kuten analogisia tai digitaalisia signaaleja, joita ohjain voi käsitellä. Niiden avulla voidaan ohjelmoida monimutkaisia logiikkatoimintoja, kuten aikaperusteisia toimintoja ja loogisia ehtoja, jotka ohjaavat laitteiden toimintaa automaattisesti. (Flaus, 2019)

5.2 Etäterminaali

Etäterminaaliyksikköä (RTU – remote terminal unit) on tietokonejärjestelmä, jota käytetään usein teollisuusautomaatiossa etäohjaukseen, erityisesti automaattisissa prosessiohjausjärjestelmissä. Etäterminaaliyksiköissä on yleensä useita sisääntuloja ja lähtöjä, jotka mahdollistavat signaalien keräämisen erilaisista antureista ja ohjauslaitteista sekä ohjauskomentojen antamisen prosessilaitteille. Nämä voivat lukea anturien tuottamia analogisia tai digitaalisia signaaleja, suorittaa laskentaa ja logiikkatoimintoja signaalien perusteella ja ohjata moottoreita, venttiilejä ja muita laitteita. Teollisen robotiikan ympäristössä on itse automaatiojärjestelmän komponentit ja tiedonsiirtoyhteydet. Tämän lisäksi tulee huomioida tukevien järjestelmien vaikuttavuus toimintaan. (Flaus, 2019)

5.3 Ihmisen ja koneen välinen käyttöliittymä

Ihmisen ja koneen välissä olevaa käyttöliittymää kutsutaan englanninkielisellä lyhenteellä HMI (Human Machine Interface). HMI on yleisesti käytetty termi, joka viittaa teollisuusautomaatiossa käytettäviin laitteisiin, joilla käyttäjä voi ohjata ja valvoa automaatiojärjestelmän toimintaa.

HMI-laitteet voivat olla erilaisia, kuten kosketusnäyttöjä, näppäimistöjä, painikkeita, ohjaimia ja muita käyttöliittymiä. Ne voivat kommunikoida automaatiojärjestelmän muiden laitteiden, kuten PLC:n ja RTU:n, kanssa erilaisilla protokollilla, kuten Modbus, Profibus ja Ethernet. HMI-laitteet

näyttävät käyttäjälle tärkeitä tietoja: prosessin tilan, anturien lukemat, hälytykset ja toimintaparametrit. Niiden avulla käyttäjä voi ohjata automaatiojärjestelmän toimintaa ja tarvittaessa tehdä muutoksia. (Flaus, 2019)

HMI-laitteet ovat yleisiä teollisuusautomaatiossa ja niitä käytetään monissa eri sovelluksissa, kuten tehdasautomaatiossa, prosessiteollisuudessa, energia- ja voimalaitoksissa, liikenteessä, kemianteollisuudessa ja monissa muissa. HMI-laitteet ovat tärkeässä osassa automaatiojärjestelmissä, koska ne mahdollistavat käyttäjän vuorovaikutuksen järjestelmän kanssa ja auttavat varmistamaan, että järjestelmä toimii turvallisesti ja tehokkaasti.

5.4 Protokollat

Modbus on sarjapohjainen avoin kommunikointiprotokolla, joka on suunniteltu teollisuusautomaation käyttöön. Se mahdollistaa laitteiden, kuten anturien, ohjainten ja mittauslaitteiden, välisen kommunikoinnin. Siirtokerroksena voidaan käyttää sarjaväylää tai ethernet-verkkoa. Modbus-protokolla on erittäin suosittu teollisuusautomaation keskuudessa, koska se on helppo käyttää ja yhteensopiva monien laitteiden kanssa. Profibus on toinen yleisesti käytetty protokolla teollisuusautomaatiossa. Se on sarjaväyläprotokolla, joka mahdollistaa tiedonsiirron PLC:n ja toimilaitteiden välillä. Profibus protokolla on nopea ja luotettava, ja siitä monia eri variaatioita, kuten Profibus-DP, Profibus-PA ja ProfiNet. (Flaus, 2019)

5.5 Fyysinen turvallisuus

Teollisuusrobotiikan automaatiojärjestelmät ovat riippuvaisia fyysisestä maailmasta ja olosuhteista. Tämä kattaa laitteiden lisäksi rakennuksen, rakennelmat, siirrettävät yksiköt ja näitä tukevan fyysiset toiminnot. Fyysinen maailma on uhattuna säälle, tulipaloille tai asiattomien henkilöiden tunkeutumiseen alueelle (NIST SP800-12). Laitoksen maantieteellinen sijainti vaikuttaa merkittävästi laitokseen kohdistuvien uhkien luonteeseen. Näissä tulee huomioida sijainnin lisäksi ihmisten aiheuttamat uhat, läheisten laitosten uhat kuten kemikaalivuodot, räjähteet sekä elektromagneettiset häiriöt kuten tutkat. Rakennelmia tukeviin toimintoihin kuuluvat lämpö, vesi, ilmastointi, sähkö, automaatio (LVISA) ja näiden tuotanto.

Fyysisen maailman tapahtumat voivat helposti aiheuttaa katkoksen esimerkiksi tietoliikenteeseen. Tyypillinen esimerkki on kaivinkone, joka katkaisee yhteydet. Tällöin yhteydet tulisi olla varmennettu eri suunnista ja teollisen robotiikan tuotannon toiminta varmistettu. Tämän lisäksi laitteet

voi tuhoutua tai rikkoutua ihmisen tai luonnon toimesta. Tämän myötä voidaan menettää myös tietoa tietojärjestelmistä ja näiden palauttaminen tulee olla suunniteltu. (NIST SP800-12)

5.5.1 Kulunvalvonta

Kulunvalvonnan toteutus sisältää kulkureitit, niiden valvonnan, vyöhykkeiden määrittämisen ja niihin pääsyn tiettyjen valvontapisteiden kautta (esimerkiksi ovessa oleva kulkutunnisteen lukija). Yleensä rajoitetuilla alueilla olevat ihmiset myös tunnistavat ulkopuoliset henkilöt ja heidät on koulutettu toimimaan kyseisessä tilanteessa. Järjestelyiden toimivuus edellyttää myös henkilöstön oikeaa toimintaa ja järjestelyiden katselmointia säännöllisesti. Huomattavaa on myös se, että turvallisuussyistä tiloista pääsee ulos ilman tunnisteita. Tällainen tilanne voi syntyä, jos valtuutetun henkilön seurassa tai perässä vyöhykkeelle menee ylimääräinen henkilö. Ovien avaaminen hätäkahvoista tai fyysisillä avaimilla tulisi aiheuttaa hälytys sähköisessä kulunvalvonnassa, jolloin luvaton toiminta havaitaan. (NIST SP800-12)

5.5.2 Tukevat järjestelmät ja rakenteet

Tukevat järjestelmät ja tilat ylläpitävät teollisen robotiikan pääjärjestelmän toimintaa. Näihin liittyy sekä ihmisiä että laitteita tukevat rakenteet ja järjestelmät kuten palo-, rikos- ja LVISA- järjestelmät sekä tietoliikenneyhteydet. Myös näiden järjestelmien rikkoutuminen sään, tulipalon tai vuodon seurauksena tulee huomioida kokonaisvaltaisessa riskienhallinnassa. (NIST SP800-12). Osin fyysisen maailman toiminnot aiheuttavat vaikutuksia kybertoimintaympäristöön. Niiden täydellinen huomiointi voi olla vaikeaa, kuten Fukushiman ydinvoimalan onnettomuus osoittaa. Tukevien järjestelmien viat tai toimintakatkot voivat kuitenkin haitata teollisen robotiikan tuotantoa.

5.5.3 Tiedon saatavuuden katkot

Tiedon saatavuuden katkokset tulee tarkastella monista näkökulmista ja yksi näkökulma on sen fyysiseen maailmaan sijoittuminen. Sitä voidaan tehdä esimerkiksi standardin avulla. Se sisältää ohjeita ja vaatimuksia tietojärjestelmien suunnittelulle, käytölle ja ylläpidolle, jotta varmistetaan tietojen saatavuus myös poikkeuksellisissa tilanteissa ja häiriöissä. Tämä voi sisältää järjestelmien redundanttisuuden, varmuuskopiointiratkaisut, jatkuvan valvonnan ja reagoinnin suunnitelmat, sekä laajemman liiketoiminnan jatkuvuussuunnittelun (SP-800-12).

5.5.4 Korjaavat toimenpiteet

Fyysisen turvallisuuden osalta on olemassa kulunvalvonta ja mm. kameroihin perustuva valvonta. Edellä mainittuja ongelmia ja riskejä voidaankin hallita suhteellisen helposti. Vyöhykkeisyyttä voidaan lisätä, vähennetään kulkureittejä, ohjataan kulkua ja parannetaan niiden teknistä valvontaa (SP800-12).

5.6 Verkkoliikenteen suojaus

Teollisen robotiikan järjestelmien toiminta vaatii yleisesti myös toimivia verkkoyhteyksiä valvontaan ja käyttöön. Verkkoliikenteen suojaus voidaan toteuttaa useilla eri tavoilla, joista joitakin tärkeimpiä ovat:

- Tietoliikenteen salaaminen, (Secure Socket Layer, SSL tai Transport Layer Security, SSL/TLS). Protokolla on yleisimmin käytetty tekniikka verkkoliikenteen suojaamiseen. Siinä käytetään julkista ja yksityistä avainta, joiden avulla verkkoliikenne salataan, jotta kolmannet osapuolet eivät voi lukea tietoja.
- Palomuuri, jonka avulla voidaan estää luvattomien käyttäjien pääsy tietokoneeseen tai verkkoon. Palomuurit voivat estää haittaohjelmien, tietojenkalasteluyritysten ja muiden verkkohyökkäysten vaikutukset. Palomuurin toiminnallisuus suodattaa ja segmentoi tietoliikennettä.
- Hyökkäyksen tunnistusjärjestelmät, (Intrusion Detection System, IDS tai Intrusion Prevention System, IPS): Nämä järjestelmät ovat suunniteltu havaitsemaan ja estämään tietoturvaloukkauksia ja verkkohyökkäyksiä. Ne voivat havaita epäilyttävän liikenteen ja suorittaa ennalta määritetyn toimenpiteen – esimerkiksi estää liikenteen.
- Yksityisverkot, VPN (Virtual Private Network): VPN on salattu verkkoyhteys, joka muodostetaan kahden tietokoneen välille, jonkin verkon kautta. VPN-yhteyden avulla voidaan yhdistää tietokone etäverkkoon ja käyttää sitä turvallisesti suojattuna. VPN-yhteys on tyypillinen tapa muodostaa hallinta tai etäkäyttöyhteyksiä.
- Haittaohjelmasuojaus, joka voidaan toteuttaa ohjelmilla, joiden tehtävänä on suojata tietojärjestelmää tai tietoverkkoa erityisesti viruksilta. Suojausohjelmistoja ja niiden tunnisteita tulee päivittää säännöllisesti torjumaan uusia uhkia.

5.7 Järjestelmien ja ohjelmistojen turvallisuus

Järjestelmien ohjelmistojen turvallisuuden varmistaminen on tärkeä osa tietoturvaa, sillä ohjelmistot voivat sisältää haavoittuvuuksia, jotka voivat altistaa järjestelmän hyökkäyksille ja tietomurroille. Järjestelmien ohjelmistoturvallisuutta voidaan kohentaa seuraavin menettelyin:

- Ohjelmiston kehittämisen alkuvaiheessa on tärkeää suunnitella arkkitehtuuri ja toteutustapa turvallisesti. Sen korjaaminen on aina myöhemmissä vaiheissa kallista tai jopa mahdotonta.
- Turvallisuusstandardien, kuten ISO/IEC 27001, noudattaminen auttaa varmistamaan, että järjestelmä täyttää tietyt turvallisuusvaatimukset ja -standardit. Tämä voi auttaa kehittäjiä tunnistamaan ja korjaamaan mahdolliset turvallisuusongelmat ja auttaa järjestelmää saavuttamaan tietoturvatavoitteensa.
- Teollisen robotiikan automaatio järjestelmiä on säännöllisesti tarkasteltava mahdollisten haavoittuvuuksien varalta.

- Järjestelmien varmuuskopiointi on tärkeä osa haavoittuvuuksien hallintaa. Tämä auttaa varmistamaan, että jos järjestelmä vahingoittuu tai tuhoutuu, tärkeä tieto voidaan palauttaa.
- Järjestelmien säännöllinen päivittäminen ja korjausten asentaminen auttaa vähentämään mahdollisten hyökkääjien käyttämien haavoittuvuuksien riskiä.
- Loppukäyttäjien kouluttaminen on tärkeää haavoittuvuuksien hallinnassa. Henkilöstöä tulee kouluttaa tunnistamaan mahdolliset haavoittuvuudet ja heikkoudet (muutkin kuin teknisillä keinoilla havaittavat) ja raportoimaan niistä asianmukaisesti.

Näiden menetelmien käyttö voi auttaa vähentämään teollisuusautomaation järjestelmien haavoittuvuuksista aiheutuvia riskejä. On tärkeää toteuttaa asianmukaisia haavoittuvuuksien hallintamenetelmiä varmistaakseen, että järjestelmät ovat turvallisia ja toiminnan jatkuvuus säilyy.

Vertailu MITREN kannasta löytyvistä suurimmista valmistajista (ICS-, SCADA-, PLC-, DCS-järjestelmiä) raportoitujen haavoittuvuuksien mukaisesti: Siemens (Saksa), Schneider Electric (Ranska), ABB (Ruotsi), Honeywell (Yhdysvallat) ja General Electric (Yhdysvallat). Haavoittuvuuksien määrästä ei voi tehdä muuta päätelmää kuin että järjestelmien laajuus ja yleisyys korreloi löydettyjen haavoittuvuuksien kanssa.

5.8 Kerroksellinen suojaus

Sipulinkuoriperiaate (kerroksellinen suojaus) on tietoturvaperiaate, joka pyrkii suojamaan järjestelmiä ja tietoja useilla tasoilla, jotta yhden puolustuslinjan pettäminen ei johtaisi koko järjestelmän murtumiseen. Tämä periaate perustuu ajatukseen, että yksittäinen kontrolli, kuten palomuuri tai virustorjuntaohjelma, ei riitä suojaamaan järjestelmää, vaan tarvitaan useita erilaisia suojakerroksia.

Kerroksellinen suojauksen periaatteen noudattaminen tarkoittaa sitä että, järjestelmään rakennetaan useita eri tasoja, joilla jokaisella on oma roolinsa ja vastuunsa tietoturvan takaamisessa. Ympäristön turvallisuuden takaamiseen ei riitä, että kontrollit on rakennettu vain reuna-alueille, joihin ympäristö rajoittuu vaan suojaus tulee toteuttaa holistisesti koko järjestelmään ja eri tasoille. Teollisen robotiikan ympäristössä kerroksellinen suojaus voidaan toteuttaa esimerkiksi seuraavasti:

- Fyysinen suojaus, joka estää fyysisen pääsyn laitteisiin ja järjestelmiin. Fyysisen suojauksen keinoina voidaan käyttää esimerkiksi lukittavia kaappeja, valvontakameroita, hälytysjärjestelmiä ja muita fyysisiä esteitä.
- Pääsynhallinta, joka estää pääsyn järjestelmiin ja tietoihin verkon kautta. Verkkosuojauksen keinoina voidaan käyttää esimerkiksi palomuureja, verkon tarkkailua ja valvontaa, salattuja yhteyksiä.
- Käyttäjätunnistus ja -valvonta, joka varmistaa, että vain oikeutetut käyttäjät pääsevät järjestelmiin ja tietoihin. Käyttäjätunnistuksen ja -valvonnan keinoina voidaan käyttää esimerkiksi käyttäjätilien hallintaa, monitasoista käyttäjätunnistusta ja käyttövaltuus hallintaa.
- Sovellustason suojaus, joka estää tietoturva-aukkojen hyväksikäyttöä sovellusten kautta. Sovellussuojauksen keinoina voidaan käyttää esimerkiksi haavoittuvuuksien tunnistusta ja korjaamista, koodin auditointia ja syötteiden validointia.
- Ylin kerros on tietoturvan valvonta ja hallinta, joka koordinoi tietoturvan ylläpitoa ja varmistaa, että kaikki järjestelmän osat ovat suojattuja. Tietoturvan valvonta ja hallinta sisältää riskienhallinnan, tietoturva-auditoinnit ja kokonaisvaltaisen tietoturvallisuuden hallinan.

Yhteenvetona voidaan todeta, että SP800-82:ssa kuvataan monikerroksisen tietoturva-arkkitehtuurin käyttöä teollisuusjärjestelmissä, jossa järjestelmä suojataan useilla eri tasoilla mahdollisia uhkia vastaan.

Standardi IEC 62443 esittää mallin monikerroksisesta suojausarkkitehtuurista, joka sisältää neljä päävyöhykettä.

- Ensimmäinen vyöhyke sisältää teollisuuslaitoksen laitteiston ja järjestelmän, joka koostuu teollisuusautomaation järjestelmän sisältäen ohjaimia, antureita ja moottoreita.
- Toinen vyöhyke sisältää järjestelmän ja laitteiden välisen verkon, joka mahdollistaa tiedonkäsittelyn ja -välityksen. Tällä tasolla toteutetaan verkkoturvallisuutta, johon kuuluu verkon suojauksen, tietojen salauksen ja verkon hallinnan toteutus.
- Kolmannella vyöhykkeellä on sovelluksia, jotka ohjaavat prosesseja ja mahdollistavat eri järjestelmien välisen tiedonkulun. Tämän tason suojaus sisältää esimerkiksi sovellusten tunnistuksen ja todennuksen, tiedon salauksen, valvonnan ja hallinnan.
- Neljäs vyöhyke sisältää järjestelmän tietojärjestelmän ja siihen liittyvät liiketoimintaprosessit. Tämän tason suojaus sisältää esimerkiksi käyttäjähallinnan, tietoturvallisuuden hallinnan, riskienhallinnan, tietojen varmuuskopioinnin ja palauttamisen sekä jatkuvuuden varmistamisen.

Kerroksellinen suojaus on tärkeä periaate teollisen robotiikan ympäristössä, koska se auttaa varmistamaan, että järjestelmä on suojattu haavoittuvuuksilta ja uhilta. Kerroksellinen suojaus auttaa myös varmistamaan, että järjestelmä on suojattu kokonaisvaltaisesti usealla tasolla, eikä pelkästään yksittäisten toimenpiteiden avulla.

5.9 Valvonta ja monitorointi

"Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations" on NIST:in julkaisema ohjeistus (SP800-137) tietoturvanhallinnan hyvistä käytännöistä ICS-ympäristöissä. Julkaisun ohjeiden avulla voidaan toimeenpanna jatkuvaa tietoturvanvalvontaa.

SP800-137 sisältää ohjeita ja suosituksia jatkuvan tietoturvanvalvonnan (ISCM) käyttöönotosta, joka on tärkeä osa tietoturvan hallintaa ICS-ympäristöissä. Jatkuvalla tietoturvanvalvonnalla pyritään havaitsemaan, analysoimaan ja torjumaan tietoturvaan liittyviä riskejä ja haavoittuvuuksia reaaliajassa. Ohjeistus kattaa monia aiheita, kuten tietoturvallisuuden hallinnan suunnittelun, toteutuksen ja käytön periaatteet, tietojen keräämisen, analysoinnin ja raportoinnin prosessit, sekä erilaisia tekniikoita ja menetelmiä, joita voidaan käyttää jatkuvan tietoturvallisuuden valvonnan

toteuttamiseen. Lisäksi julkaisussa annetaan suosituksia tietoturvan hallinnan yleisistä käytännöistä, kuten riskienhallinnasta, haavoittuvuuksien hallinnasta ja tietoturvan tiedonhallinnasta.

SP800-137 on suunnattu ensisijaisesti Yhdysvaltain liittovaltion viranomaisille ja organisaatioille, mutta sen suositukset ja käytännöt ovat sovellettavissa ja hyödynnettävissä myös laajemmalle joukolle organisaatioita, jotka käyttävät ICS-järjestelmiä tuotantotoiminnassaan.

5.9.1 Lokien kerääminen, tallentaminen ja analysointi

Lokien kerääminen ja analysointi tarkoittaa järjestelmän lokitietojen keräämistä ja analysointia mahdollisten tietoturvatapahtumien havaitsemiseksi. Tähän käytetään järjestelmiä, jotka keräävät ja analysoivat lokitietoja. Lokien keräämisessä tulee huomioida ne tunnistetut uhat, joita vastaan suojaudutaan. Tämän vuoksi tulee määrittää mistä tiedosta hyökkäys voidaan tunnistaa ja että kyseinen tieto kerätään järjestelmään (SP800-30).

5.9.2 Lokien suojaaminen

Lokien suojaaminen on tärkeä tietoturva- ja tietosuoja-asia, sillä lokitiedostot sisältävät usein arkaluontoista tietoa, kuten käyttäjätunnukset, salasanat, IP-osoitteet ja muut käyttäjän toimintaan liittyvät tiedot. Lokien suojaaminen tarkoittaa näiden tietojen suojaamista luvattomalta käytöltä ja häviämiseltä.

Lokien suojaaminen voidaan toteuttaa seuraavilla tavoilla:

- Käyttöoikeuksien rajoittamisen tavoitteena on varmistaa, että vain valtuutetut käyttäjät pääsevät tarkastelemaan ja muokkaamaan lokitiedostoja. Periaatteen nimi on vähimmän käyttöoikeuden periaate. Lokitiedostot tulee tallentaa suojattuihin hakemistoihin, joihin on pääsy vain tietyillä käyttäjäryhmillä.
- Tietojen salaaminen suojaa tietoja luvattomalta käytöltä ja estää niiden lukemisen ilman oikeuksia. Lokitiedostoja voidaan salata käyttämällä salausalgoritmeja, jotka estävät tietojen lukemisen ilman asianmukaisia salausavaimia.
- Lokitiedostojen säännöllinen varmuuskopiointi estää niiden häviämisen ja varmistaa, että tärkeät tiedot ovat aina käytettävissä. Varotoimenpiteenä lokitiedostoja tulisi tallentaa useampaan paikkaan ja siirtää taltioon, josta niitä ei voida poistaa.
- Lokeihin liittyvien tietojen poistaminen ja supistaminen. Osa lokitiedostoihin tallentuvasta tiedosta kuten henkilötiedot voi olla tarpeettomia tai jopa riskialttiita säilyttää. Poistamalla

ja suodattamalla nämä tiedot pienennetään riskiä tietojen väärinkäytöltä. Lokitietojen tallennuksen kesto tulee määrittää vähintään sen mukaan, kuinka kauan tietojen tallentaminen on tarpeen lain mukaan ja yrityksen käytäntöjen mukaan.

5.9.3 ICT-maailman kybervalvonta

Kybervalvonta tarkoittaa tietoverkkojen ja sähköisten järjestelmien seurantaa ja valvontaa mahdollisten uhkien, kuten tietomurtojen, haittaohjelmien, tietovarkauksien ja muiden tietoturvarikosten varalta. Kybervalvonnalla pyritään havaitsemaan mahdolliset hyökkäykset ja torjumaan niitä mahdollisimman varhaisessa vaiheessa ennen kuin ne aiheuttavat suurempaa vahinkoa. Kybervalvonnan tavoitteena on reaktiivisen toiminnan lisäksi saada toimintaympäristö kybersietoiseksi siten, että syntyviin ongelmiin voidaan reagoida jo ennen kuin se aiheuttaa toiminnalle vaikuttavuutta.

5.9.4 Pääsynhallinta

Verkonvalvonnalla liikennettä tulisi seurata ja analysoida jatkuvasti, jotta havaitaan mahdolliset hyökkäykset ja muut poikkeamat. Verkonvalvonnan tulisi sisältää verkkolaitteiden, tunnistusjärjestelmien ja kirjautumistietojen seurannan.

Tieto- ja ohjausjärjestelmien osalta tulee valvoa myös prosessien toimivuutta kuten käyttäjäoikeuksien hallinnan, laitetilan seurannan ja tietokannan käytön. Näiden tietojen monitorointi auttaa havaitsemaan mahdolliset tietoturvaongelmat.

Fyysisen ympäristön monitorointi, kuten ovet, ikkunat ja muut pääsypisteet, auttaa estämään fyysisiä hyökkäyksiä teollisuuden ohjausjärjestelmiin. Liikennettä voidaan ohjata tiettyjen kontrollien ja kulunvalvontapisteiden kautta.

Järjestelmän tulisi sisältää hälytysjärjestelmät, jotka ilmoittavat mahdollisista tietoturvaongelmista tai muista poikkeavuuksista. Lokitietojen keskitetty kerääminen ja analysointi auttaa havaitsemaan mahdollisia tietoturvaongelmia ja mahdollistaa nopean reagoinnin niihin.

Säännöllisesti toteutettu haavoittuvuuksien etsintä auttaa löytämään tietoturva-aukot ICS-järjestelmissä. Skannaukset voivat sisältää erilaisia tekniikoita, kuten penetraatiotestauksen, jossa hyökkäystekniikoita käytetään tietoturva-aukkojen etsimiseen. Voidaan myös käyttää ns. RED

TEAMING menetelmää, jossa hyökkäyksen toteuttaa tiimi varioiden eri tapoja, joilla hyökkäys voitaisiin toteuttaa.

ICS-järjestelmissä käytettävät ohjausjärjestelmät voivat olla erittäin monimutkaisia ja sisältää useita eri laitteita ja moduuleja. Järjestelmien konfiguraation hallinta auttaa varmistamaan, että kaikki laitteet toimivat oikein ja että turvallisuuteen liittyviä asetuksia noudatetaan.

ICS-järjestelmissä käytetään usein tiettyjä turvallisuuskäytäntöjä, kuten käyttöoikeuksien hallintaa ja verkon eristämistä. Näiden käytäntöjen valvonta auttaa varmistamaan, että järjestelmät ovat suojattuja ja että vain valtuutetut käyttäjät voivat käyttää niitä.

5.9.5 Tietoturvallisuuden monitorointi

ICS-järjestelmiin liittyvät tietoturvaongelmat voivat olla hyvin monimutkaisia ja vaikeasti havaittavissa. Uhkien tunnistus- ja varoitusjärjestelmät auttavat havaitsemaan mahdollisia hyökkäyksiä ja varoittamaan niistä välittömästi. Yrityksessä tulee olla selkeät tietoturva- ja riskienhallintaprosessit, jotka sisältävät tarkat ohjeet siitä, miten tietoturvaa valvotaan ja miten havaitut ongelmat käsitellään. Prosessien tulee olla kattavia, jotta mahdollisiin tietoturvaongelmiin voidaan reagoida nopeasti ja tehokkaasti.

IEC 62443 on kansainvälinen standardi, joka käsittelee teollisuusautomaation ja ohjausjärjestelmien (ICS) tietoturvaa. Standardi sisältää useita suosituksia tietoturvan monitoroinnista, joka on yksi tärkeimmistä toimenpiteistä tietoturvallisuuden varmistamiseksi ICS-ympäristössä. Standardi korostaa tietoturvallisuuden jatkuvaa monitorointia. Siinä kuvataan miten toteuttaa jatkuva seuranta ja valvonta valvottavassa ympäristössä. Se suosittelee käyttämään automatisoituja seurantajärjestelmiä, jotka ovat kykeneviä keräämään ja analysoimaan tietoturvallisuuteen liittyviä tietoja. Standardin mukaan verkon liikennettä tulisi seurata jatkuvasti ja pyrkiä havaitsemaan poikkeamat normaalista toiminnasta. Verkon seurannan tulisi sisältää esimerkiksi palomuurit, tunnistusjärjestelmät ja kirjautumistietojen seurannan. Kerätyt tiedot tulee tallentaa lokeihin ja kerätä ne analysointia varten keskitettyyn paikkaan, jotta voidaan havaita poikkeamat ja mahdolliset tietoturvahyökkäykset. Lokien analysointi auttaa myös määrittämään, miten tietoturvallisuutta voidaan parantaa. Standardi suosittelee järjestelmien tilojen seurantaa, jotta voidaan havaita mahdolliset poikkeamat ja mahdolliset turvallisuustapahtumat. Järjestelmien tilan seurannan tulisi sisältää esimerkiksi laitetilojen seuranta, käyttäjäoikeuksien hallinta ja tietokannan käytön seuranta.

Standardi suosittelee myös ympäristön valvontaa, joka sisältää esimerkiksi pääsynvalvonnan, hälytysjärjestelmät ja valvontakamerat. Ympäristön valvonta auttaa havaitsemaan mahdolliset tietoturvaongelmat ja estämään fyysisiä hyökkäyksiä.

Yllä mainitut standardeissa olevat tekniikat ja käytännöt voivat auttaa yrityksiä varmistamaan, että niiden ICS-järjestelmät ovat turvassa ja että mahdollisiin tietoturvaongelmiin voidaan reagoida nopeasti. Kyberturvallisuus ja siihen sisältyvä tietoturvallisuuden hallinta on jatkuva prosessi. Tämä tarkoittaa, että yritysten on syytä päivittää järjestelmiään ja käytäntöjään säännöllisesti vastaamaan uusia uhkia ja haasteita. Tietoturvallisuuden tapahtumien monitorointi ICS-järjestelmissä on erityisen tärkeää, sillä tietoturvariskit voivat vaikuttaa suoraan fyysiseen ympäristöön ja vaarantaa henkilöiden turvallisuuden. Standardit auttavat yrityksiä luomaan selkeät tietoturva- ja riskienhallintaprosessit, jotka myös sisältävät riskien arvioinnin, suojaustoimenpiteiden suunnittelun ja toteutuksen, sekä jatkuvan arvioinnin ja parantamisen (SP800-82).

5.10 Standardien vertailu

Kun verrataan NIST:in standardit SP800-82 ja teollisen robotiikan standardia IEC 63443 toisiinsa, huomataan ettei perinteinen tietotekniikan standardi huomioi fyysisen toimintaympäristön aiheuttamia tekijöitä.

Toiminto	SP800-82r3	IEC 63443
Jatkuva tietoturvallisuuden monitorointi	☒	☒
Verkonvalvonta	☒	☒
Lokien kerääminen ja analysointi	☒	☒
Pääsynvalvonta	☒	☒
Kulunvalvonta	☐	☒
Ympäristön valvonta	☐	☒

Turvallisuustasot	☐	☒

Taulukko 1. Standardien vertailu

Teollisen robotiikan toimintaympäristössä tulee pystyä yhdistämään eri toiminto- ja vastuualueiden tuottamat kyberuhkat kokonaisjärjestelmälle ja liiketoiminnalle.

5.11 Varautuminen ja toipuminen

Resilienssi tarkoittaa kykyä selviytyä ja palautua häiriöistä tai ongelmista nopeasti ja tehokkaasti. Robotiikan kyberympäristössä resilienssin saavuttamiseksi tulee ottaa huomioon useita eri tekijöitä standardien, kuten IEC 62443 perusteella:

- Suojata robotiikan järjestelmät teknisillä kontrolleilla tietoturvauhkilta kuten haittaohjelmat, tietomurrot ja palvelunestohyökkäykset.
- Taata toimintavarmuus varajärjestelmien avulla, kuten varavoimajärjestelmä ja varmistusten palauttaminen.
- Järjestelmä tulee suunnitella siten, että se sietää häiriöitä ja vikatilanteita. Tämä voidaan saavuttaa esimerkiksi redundanssilla, jossa kriittiset komponentit ovat kahdennettuja ja järjestelmä voi jatkaa toimintaansa, vaikka yksi osa epäonnistuisi.
- Järjestelmää tulee valvoa jatkuvasti ja että mahdolliset häiriöt havaitaan ja käsitellään nopeasti. Valvontajärjestelmän tulisi sisältää hälytykset ja raportointi, joka kertoo järjestelmän tilan ja mahdolliset häiriöt.
- Käyttäjiä tulee kouluttaa ja tiedottaa, jotta he ovat tehtävänsä osaavia ja tietoisia järjestelmän toiminnasta, turvallisuusvaatimuksista ja mahdollisista häiriötilanteista. Hyvin koulutetut käyttäjät voivat auttaa havaitsemaan ja ratkaisemaan ongelmia nopeammin. Henkilöstö tuntee toipumismenettelyt ja on valmis toteuttamaan harjoitellut toimenpiteet.

Nämä tekijät yhdessä auttavat saavuttamaan kybersietoisuuden (resilienssin) robotiikan kyberympäristössä, jolloin järjestelmä on paremmin suojattu ja kestävämpi mahdollisia häiriötilanteita vastaan. Huomattavaa on, että mainittujen lisäksi tulee toiminnan olla jatkuvan parantamisen piirissä, jotta hallintamenettelyiden tiedetään toimivan ja vähentävän ongelmia(Vilches&al, 2018).

6 Tapaustutkimukset ICS-järjestelmien kyberuhkista

Teollisuusautomaation ja robotiikan järjestelmiä on pidetty turvasatamina kyberuhkilta tai ainakaan niitä ei tiedosteta riittävästi. Teollisen robotiikan järjestelmät ovat olleetkin perinteisessä tehdasympäristössä melko eristettyjä. Tietotekniikan verkottuneisuus ja haittaohjelmien kehittyminen on johtanut siihen, että edes fyysisesti erotetut järjestelmät eivät ole suojassa kehittyneiltä hyökkäyksiltä (APT – Advanced Persistent Threat). Tunnetuimpia esimerkkejä tällaiseen ympäristöön tunkeutumisesta on STUXNET (Baezner, 2018).

Sähköjärjestelmän katkoilla on ollut merkittäviä vaikutuksia Ukrainan sodassa. Vuonna 2015 tapahtuneet kaksi laajaa sähkökatkosta ovat esimerkkejä siitä, kuinka sähköverkkoon kohdistuvat hyökkäykset voivat vaikuttaa laajasti yhteiskunnan toimintaan. Sähköjärjestelmien ohjauksen ja järjestelmän eristyneisyys on samankaltainen kuin teollisessa robotiikassa.

Ensimmäinen laaja sähkökatkos tapahtui marraskuussa 2015, jolloin kyberhyökkäys kohdistui kolmeen sähkön jakeluverkkoon. Katkos vaikutti noin 230 000 ihmiseen ja kesti noin kuusi tuntia. Tämän seurauksena tehtaat, kaivokset ja muut yritykset joutuivat keskeyttämään toimintansa, mikä aiheutti huomattavia taloudellisia menetyksiä (CFR, 2015).

Toinen laaja sähkökatkos tapahtui joulukuussa 2015, joka kesti noin 17 tuntia ja vaikutti noin miljoonaan ihmiseen. Tämän katkoksen syynä oli myös kyberhyökkäys, joka kohdistui sähköverkon hallintajärjestelmään. Katkoksen vaikutukset olivat vakavampia kuin ensimmäisessä tapauksessa, koska se vaikutti laajemmin yhteiskunnan infrastruktuuriin, kuten veden- ja lämmönjakeluun.

Kyseiset hyökkäykset ovat merkittäviä, koska ne ovat ensimmäiset dokumentoidut tapaukset, joissa kyberhyökkäys on onnistunut aiheuttamaan laajamittaista fyysistä vahinkoa sähköverkossa. Tämä on herättänyt huolta siitä, että vastaavanlaiset hyökkäykset voivat tapahtua myös muissa maissa, ja että tällaiset hyökkäykset voivat aiheuttaa vakavia häiriöitä yhteiskunnan toiminnassa.

6.1 TRITON

TRITON-hyökkäys oli suunnattu teollisuusautomaatiojärjestelmiin, erityisesti kriittisen infrastruktuurin osiin, kuten voimalaitoksiin ja kemikaalitehtaisiin. Hyökkäyksen toimintaperiaate oli erittäin ilkeä motiiveiltaan, koska se pyrki manipuloimaan turva-automaatiotoimintoa (SIS - Safety Instru-

mented System). Sen tavoitteena oli saada aikaan fyysisiä vahinkoja tai keskeyttää näiden järjestelmien toiminta. Hyökkääjät käyttivät haittaohjelmaa, joka tunnetaan nimillä TRITON tai Trisis. (Dragos, 2017)

Tämä haittaohjelma oli suunniteltu erityisesti teollisuusautomaatiojärjestelmiin, ja se pystyi manipuloimaan turvallisuusjärjestelmiä, kuten hätäpysäytysjärjestelmää. Ohjelmiston toiminta esitellään tässä työssä, koska se sisältää kaksi robotiikkaan liittyvää ja sen uhkiin liittyvää toimintoa. Ohjelmiston hyökkäysvektori kohdistui ICT-järjestelmän kautta OT-järjestelmään manipuloiden turva-automaatiota. Järjestelmään päästiin yksinkertaisesti yrityksen Windows-työasemaverkon kautta, joka oli heikosti suojattu. Sen kautta oli pääsy OT-verkon hallintatyöasemalle.

TRITON-hyökkäys tunnistettiin ja jäljitettiin FireEyen tutkijoiden toimesta vuonna 2017. He havaitsivat TRITON-haittaohjelmiston käytön yhdessä Lähi-Idässä sijaitsevassa teollisuuslaitoksessa. Tutkijat analysoivat haittaohjelman toimintaa ja mallinsivat sen toiminnan. Ohjelman kehitys oli alkanut jo 2014 Dragosin tutkimuksen tulosten mukaan.

Ohjelmisto käytti TRISIS-haittaohjelmaa, joka on suunniteltu kohdistumaan Schneider Electricin Triconex-laitteisiin teollisuuden ohjausjärjestelmissä. TRISIS on Python-skripti, joka oli käännetty 'py2exe'-kääntäjällä mahdollistaakseen sen suorittamisen ympäristössä, jossa Pythonia ei ole asennettuna. Sen tarkoituksena on muuttaa ajonaikaisen logiikan Schneider Electricin Triconex-laitteissa, ja erityisesti Triconex 3008 -prosessorimoduuleissa.

TRISIS:in ydintoiminnallisuus perustuu neljän binäärin yhdistelmään, jotka ladataan kohteeseen. Kaksi upotettua binäärikomponenttia (inject.bin ja imain.bin), jotka sisältyvät ajettavaksi tiedostoksi käännettyyn Python-skriptiin. Skriptissä viitataan kahteen eri moduuliin, jotka sijaitsevat erillisissä tiedostoissa. Tämä antaa mahdollisuuden vaihtaa ja muokata moduuleja. (Mandiand, 2019).

Analyysin mukaan upotettuja osia (binäärit) käytetään valmistelemaan ja lataamaan ulkoisia moduuleja, jotka sisältävät korvaavan turvalogiikan hyökättävän kohteeseen. Tämä mahdollistaa sen, että TRISIS voitaisiin käyttää uudelleen vaihtoehtoisten kuormien toimittamiseen eri turvalaitteisiin. Tällöin sillä voitaisiin toimittaa muunnettuja ja kustomoituja logiikkatiedostoja täysin erilaisiin turvalaitetyyppeihin. (Dragos, 2017)

Epäilty toimija näyttää omaavan kyvyn räätälöidä omia työkaluja. Näiden työkalupakettien kehittäjät hyödynsivät olemassa olevia ohjelmistokehikoita ja muokkasivat niitä tukemaan tunkeutumista omaan kohteeseen. Kehittäjillä oli tiettyjä mieltymyksiä liittyen portteihin, protokolliin, pysyvyysmekanismeihin ja selkeitä toimintatapoja miten haittaohjelma toimi.

Vaikka todennäköisesti toimijan taktiikat, tekniikat ja menetelmät (TTM) muuttuvat ajan myötä, niiden oppiminen on edelleen hyödyllistä, jotta voidaan tunnistaa, ovatko heidän TTM sovellettavissa muihin haittaohjelman kehittäjiin ja uhkatoimijoihin. Lisäksi toimija saattoi mahdollisesti saada jalansijan muihin ympäristöihin käyttämällä samankaltaisia toimintatapoja. Tällaisissa tapauksissa retrospektiivinen etsintä auttaisi puolustajia tunnistamaan ja korjaamaan haitallisen toiminnan (Mandiand, 2019).

Koko TRISIS:in OT-ympäristöön kohdistuva haittaohjelman osuus ei hyödynnä varsinaisia haavoittuvuuksia tai hyväksikäytä mitään. Sen sijaan TRISIS:in toiminnallisuus perustuu ymmärrykseen Triconex SIS -laitteiden toiminnasta ja prosessiympäristöön liittyvistä yksityiskohdista. Näiden asioiden täyden ymmärtämisen jälkeen hyökkääjä on suunnitellut kokonaisuuteen sopivan ohjelmistopaketin.

Ohjelmistojen paketit ja dokumentaatio ovat yleisesti saatavilla ja toisaalta ne pystytään hankkimaan joka tapauksessa takaisinmallinnusta varten, kun uhkatoimijalla on resursseja. Koodin takaisinmallinnuksella on mahdollista löytää toimintalogiikan lisäksi mahdollisia haavoittuvuuksia ja kovakoodattuja tunnuksia.

Turvallisuusohjaimilla on yleisesti ottaen samanlainen suojaus kuin tavallisella ohjelmoitavalla logiikkaohjaimella. Ne olivat suojattu salasanoilla, mutta niihin sisältyi yleensä oletusarvoisesti kaksi oletustiliä, joita käyttäjä ei voi hallita. Tällaiset tilit ovat välttämättömiä varmistaakseen ylläpitotason pääsyn ja hallinnan laitteeseen hätätilanteessa. Kokenut haitallisen koodin analysoija voi paljastaa nämä tilit ja käyttää niitä saadakseen luvattoman pääsyn turvallisuusohjaimeen. Vaikka hyökkäys oli kehittynyt, se aiheutti useita hälytyksiä, joita ei huomioitu tai niihin ei reagoitu. Dokumentaation avulla voi perehtyä järjestelmän toimintaan ilman että hankkii sitä, Tritonissa hyödynnetyn ohjelmiston dokumentaatio on edelleen saatavilla Nuclear Regulatory Comission Internetsivustolla; Tristation 1131 Developer’s Workbench (NCR, 2004). Tristation ohjelmistopaketista oli mahdollista etsiä kovakoodattu tunnus, jolla järjestelmään pääsi myös luvattomasti. Schneider on poistanut uudemmista versioista ko. tunnukset (Black Hat, 2018).

Tarkastelemalla kehittäjien toimintatapoja ja abstrahoituja vastustajan metodologioita on mahdollista luoda laajempi näkymä TTM:iin erilaisilla havaitsemis- ja etsintäsäännöillä. Näiden sääntöjen kokoaminen mahdollistaa potentiaalisesti haitallisten näytteiden tunnistamisen ja luokittelemisen samalla kun rakennetaan uusia ”ansoja” toimijan etsintään (Gutmantis, 2019).

6.2 EKANS

EKANS-haittaohjelma havaittiin ensimmäisen kerran vuoden 2019 lopulla. Havainnon teki tietoturvayhtiö Dragos, joka on erikoistunut teollisuuden tietoturvan analysointiin. Dragos sai tiedon haittaohjelman olemassaolosta yhdysvaltalaisilta viranomaisilta, jonka perusteella se aloitti haittaohjelman tutkimisen.

EKANS-haittaohjelma havaittiin hyvin nopeasti sen jälkeen, kun se oli alkanut levitä. Haittaohjelman toimintatapa on poikkeuksellinen, sillä se on suunnattu erityisesti teollisuusyrityksiin ja se pyrkii haittaamaan teollisia prosesseja. Tämä herätti huomiota tietoturvayhtiöissä, ja EKANS-haittaohjelman toimintaa ryhdyttiin tutkimaan tarkemmin.

EKANS-haittaohjelman havaitsemiseen tarvittiin erittäin laaja tutkimus, jossa käytettiin erilaisia työkaluja ja menetelmiä. Haittaohjelma purettiin ja sen toiminta analysoitiin. Sen havainnoksi vahvistui että, haittaohjelma oli suunnattu erityisesti teollisuuden prosesseja hallitseviin järjestelmiin, kuten ohjausjärjestelmiin ja teollisuusautomaatioon.

EKANS-haittaohjelman havaitsemisen jälkeen tietoturvayhtiöt raportoivat tiedon haittaohjelmasta ja alkoivat työskennellä yhdessä teollisuusyritysten kanssa suojauksen parantamiseksi. Haittaohjelman leviämistä saatiin rajoitettua ja sen toimintaa vastaan kehitettiin uusia suojauksia (Hunter&al, 2020).

Yhteenvetona voidaan todeta, että EKANS-haittaohjelman havaitseminen vaati paljon resursseja ja yhteistyötä eri tietoturvayhtiöiden ja viranomaisten välillä. Haittaohjelman erikoispiirteet ja sen suunnattu toiminta teollisuusprosesseihin olivat keskeisessä roolissa sen havaitsemisessa.

Vitali Kremez oli tiettävästi ensimmäinen, joka totesi EKANS-haittaohjelman kohdistuvan teollisuuteen ja teollisuusautomaation ohjausjärjestelmiin. Alla oleva lainaus Kremezin kommentista 1.6.2020 Twitteristä / myöhemmin tunnettuna viestipalvelu X:

> *“These industrial control system machines are some of the most high-value targets,” says Kremez. “There’s lots of urgency, and data availability is at the core of the mission. So there’s a lot of incentive to pay the attackers.”*

Kun yhtälöön tuodaan raha ja se että tuotannon katkeaminen voi maksaa miljoonia, voi yritys nähdä parempana vaihtoehtona maksaa lunnaat ja palauttaa tuotanto. Jos vaihtoehtona on lähteä viranomaisten kanssa tutkimaan asiaa ja hankkimaan järjestelmien uudelleenasennusta puhtaista

lähteistä. Huomattavaa on myös se, että rikosoikeudellinen prosessi ja todisteiden tallentaminen voi olla erittäin vaikea ja hidas toteuttaa. Tässäkin tulee huomioida se, että yritysten varautuminen kyberuhkaan voi olla täysin eri tasolla. Jos tilannetta on harjoiteltu ja järjestelmiä palautettu toipumissuunnitelmien mukaan niin tilanne on paremmalla tasolla kuin jos tilanne on uusi ja odottamaton.

EKANS-haittaohjelma kohdistui useaan autoteollisuuden yritykseen ja niiden teollisuusrobotiikan järjestelmiin(Goud, 2021). Fortinetin analysoima näyte toimi kuten useimmat muut kiristyshaittaohjelmat. Haittaohjelmasta tunnistettiin seuraavat toiminnallisuudet:

- Todentaa kohdeympäristön
- Eristää saastuneen koneen (palomuuri)
- Salaukseen käytetty RSA avain dekoodataan
- Tunnistaa ja pysäyttää tiettyjä prosesseja
- Poistaa tilannevedokset (eng. shadow copy)
- Salaa tiedostot
- Poistaa palomuuri palvelun

Ohjelmiston toiminta perustui siihen, että aluksi tunnistetaan toimintaympäristö ja ollaanko oikeassa kohteessa. Ohjelmisto ei siis alkanut toimia missä tahansa, vaan kiristysohjelman luonteeseen kuuluu, että se on kohdistettu kohteeseen, josta arvioidaan saatavan suurin mahdollinen tuotto kiristyksellä (Larson, 2020). Vastaavasti jos ohjelmisto olisi levinnyt laajalti verkon kautta kotikoneisiin niin sen tunnistaminen olisi ollut nopeampaa tietoturvayritysten kannalta. Teollisuuslaitos on erittäin hyvä kohde tässä mielessä, koska käyttökatkot aiheuttavat merkittäviä taloudellisia menetyksiä. Haittaohjelmistolla oli kyky tunnistaa ja pysäyttää 64 eri prosessia ja näistä suuri osa oli sellaisia, jotka kuuluvat ICS-järjestelmiin. Toinen erikoisuus ohjelmistossa oli se, että se ei pyrkinyt leviämään verkossa toisiin työasemiin vaan massamedian kautta (USB - Universal Serial Bus). Tämä viittaa siihen, että haittaohjelma pyrittiin saamaan siirrettyä ilmavälin (eng. air gap) ylitse eristettyyn tietojärjestelmään.

6.3 Pipedream

Huhtikuussa 2022 löydettiin PIPEDREAM - ICS-hallintajärjestelmien hyökkäyskehikko, jonka on kehittänyt CHERNOVITE niminen ryhmä erikoistuen nimenomaan teollisuusinfrastruktuurin hyökkäyksiin. PIPEDREAM on tunnettu erityisesti ICS-järjestelmiin kohdistuva ja sen lisäksi se on kehitetty nimenomaan häiritsemään teollisia prosesseja. PIPEDREAM edustaa uutta kehitystä haittaohjelmien sukupolvissa. Se on ensimmäinen monialainen skaalautuva ICS-haittaohjelma, jolla on monia kyvykkyyksiä. Oikeissa toimintaolosuhteissa PIPEDREAM-haittaohjelmistoa voitaisiin käyttää tuhoaviin vaikutuksiin. Dragos tunnisti ja analysoi PIPEDREAM-haittaohjelmiston kyvykkyydet yhteistyön kautta eri viranomaisten ja yritysten kanssa alkuvuodesta 2022. PIPEDREAM:in löytäminen ennen sen laajamittaista hyödyntämistä antoi teollisuuden operaattoreille, turvallisuuspalveluntarjoajille ja teollisuuden hallintajärjestelmien tarjoajille vastata ennalta mahdolliseen hyökkäykseen. Analysoitu hyökkäyskehikko pystyttiin muuntamaan konkreettisiksi toimiksi hyökkäysten estämiseksi, havaitsemiseksi ja lieventämiseksi, jotka tulisivat käyttämään PIPEDREAM:in kaltaisia taktiikoita, tekniikoita ja menetelmiä (Dragos, 2022).

Pipedream koostuu viidestä komponentista, jonka ensimmäisenä kohteena oli Schneider Electricin järjestelmä:

1. EVILSCHOLAR: Komponentin tarkoitus on löytää, päästä käsiksi, manipuloida ja poistaa CODESYSv3-laitteita.
2. BADOMEN: Komponentin tarkoitus on tunnistaa ja kyetä toimimaan Omronin ohjelmoitavien logiikoiden (PLC) kanssa.
3. MOUSEHOLE: Työkalu OPC UA -palvelimien kanssa toimimiseen. Tämä sisältää solmujen ominaisuustietojen lukemisen ja kirjoittamisen sekä hyökkäyksen käyttäjätunnusten tiedusteluun ja murtamiseen.
4. DUSTTUNNEL: Mukautettu etäkäyttöimplanttikyvykkyys tiedusteluun ja komentokanavan luomiseen.
5. LAZYCARGO: Käyttäjätason tiedosto, joka pudottaa uuden haitallisen ajurin hyödyntäen asennuksessa haavoittuvaa ASRockin ajuria. Kyseessä on lavetti (eng. dropper), joka on tietokoneohjelma tai osa haittaohjelmasta, joka on suunniteltu toimittamaan (haittakoodi mukana) tai asentamaan muita haitallisia ohjelmia tietokoneelle tai lataamaan ne verkosta.

Lavetti voi esimerkiksi ladata haitallisen koodin etäpalvelimelta ja asentaa sen uhrin tietokoneelle. Lavetit ovat yleisiä haittaohjelmien jakelussa ja hyökkääjät voivat käyttää niitä levittämään erilaisia haittaohjelmia, kuten viruksia, troijalaisia ja kiristysohjelmia.

Haittaohjelmiston ensimmäisen moduulin kyvykkyys pystyi hyödyntämään CODESYS:in automaatio-ohjelmisto kokoelmaa IEC 61131-3. Ohjelmisto on käytössä yli viidellä sadalla valmistajilla, yli tuhannessa eri laitetyypissä ja miljoonissa laitteissa kattaen käytännössä kaikki teollisen automaation alat. Tämän lisäksi moduulissa oli toiminnallisuus hyödyntää yleisesti käytettyä Schneiderin (aiemmin Modicon) 1979 kehittämää Modbus-protokollaa logiikkaohjauksen toteuttamiseen. Toinen kyvykkyys, MOUSEHOLE toimi arkkitehtuurin mukaisesti kartoittaen ympäristöä ja tunnuksia. OPC UA (Open Platform Communications Unified Architecture) on standardi teollisuusautomaation tiedonsiirrolle, joka mahdollistaa erilaisten laitteiden ja ohjelmistojen kommunikoinnin keskenään. OPC UA:n avulla erilaiset laitteet, kuten anturit, ohjaimet ja tietokoneet, voivat lähettää ja vastaanottaa tietoa keskenään yhteisellä ja turvallisella tavalla. OPC UA:n avulla voidaan esimerkiksi valvoa tuotantoprosesseja, kerätä dataa ja ohjata laitteita. Standardi on kehitetty avoimeksi ja modulaariseksi, joten sen käyttöönotto ja ylläpito on joustavaa erilaisissa teollisuusympäristöissä.

7 Opinnäytetyön tarkoitus, tavoitteet ja tutkimuskysymykset

Opinnäytetyön tarkoituksena oli tuottaa uutta tietoa teollisen robotiikan kyberturvallisuudessa. Työ toteutettiin integratiivisena kirjallisuuskatsauksena mikä mahdollistaa eri tietolähteiden yhdistämisen. Tutkimuksen tavoitteena oli kartoittaa kyberturvallisuuden maturiteetti teollisen robotiikan ympäristöissä pääasiassa Suomessa koulutuksen osalta kohdistamalla tiedon hankinta Suomessa tehtyihin opinnäytetöihin. Kehitettävien kohteiden osalta tietopohja laajennettiin standardeihin ja kansainvälisiin tutkimuksiin.

7.1 Integratiivisen kirjallisuuskatsauksen toteuttaminen

Tutkimusmenetelmänä käytettiin integroivaa kirjallisuuskatsausta, joka mahdollistaa empiirisen ja teoreettisen kirjallisuuden tiedon yhdistämisen tutkimuksen tekoon. Holistinen tutkimus mahdollistaa yhdistää useita eri näkökulmia tutkimuksen tekemiseen. Tapaustutkimuksella on tarkoitus

löytää havaintoja yritysten toteuttamasta kyberturvallisuuden parantamistoimenpiteistä teollisen robotiikan toimialalla sekä arvioida sen kypsyystasoa.

Integratiivinen kirjallisuuskatsaus on tutkimusmenetelmä, joka pyrkii yhdistämään ja integroimaan eri tutkimusten tuloksia samasta aiheesta tai ilmiöstä. Tämän tyyppinen kirjallisuuskatsaus voi auttaa löytämään yleisiä trendejä ja mahdollisia ristiriitaisuuksia aiheesta sekä tunnistamaan tietolähteitä, jotka tarvitsevat lisätutkimusta. Tutkimus toteutettiin seuraavien vaiheiden mukaisesti:

- Tutkimuskysymyksen määrittäminen: Ensin määritettiin tutkimuskysymys ja teema, joka ohjaa integratiivista kirjallisuuskatsausta. Tutkimuskysymyksellä pyritään rajaamaan tutkimusaluetta ja selkeyttämään sitä mihin halutaan vastaus.
- Hakuprotokollan laatiminen: Tutkimuksen tietoaineiston hakuun laadittiin hakuprotokolla, joka sisältää tärkeät avainsanat ja hakutermit, jotka liittyvät tutkimuskysymykseen. Hakuprotokolla auttaa löytämään aiheeseen liittyvät artikkelit eri tietokannoista.
- Tietokantojen läpikäyminen: Tietokannoista haetaan aiheeseen liittyvät artikkelit eri tutkimus tietokannoista. Tietokantojen valinta riippuu tutkimuskysymyksestä ja siitä, missä aiheeseen liittyvät artikkelit todennäköisimmin sijaitsevat.
- Artikkelien seulonta: Artikkelit seulottiin alkuperäisten hakukriteerien perusteella. Tämä prosessi auttaa poistamaan artikkelit, jotka eivät vastaa tutkimuskysymystä.
- Artikkeleiden arviointi: Seuraava vaihe on arvioida artikkelien sisältöä ja laadukkuutta. Arvioinnin tarkoituksena on selvittää, vastaako artikkeli tutkimuskysymykseen ja onko se luotettava lähde.
- Tulosten synteesi: Viimeinen vaihe on syntetisoida tulokset, eli yhdistää ja analysoida artikkelien tulokset. Tämä voi sisältää yhtenäisten tulosten tunnistamisen, ristiriitojen selvittämisen ja mahdollisten tietolähteiden tunnistamisen, joita tarvitaan lisätutkimusta varten.

Integratiivinen kirjallisuuskatsaus on prosessi, joka vaatii huolellisuutta ja aikaa. Se auttaa kuitenkin yhdistämään eri tutkimusten tuloksia ja saamaan kokonaisvaltaisemman kuvan tutkimuskysymyksestä. (Salminen, 2011)

7.2 Tutkimusmetodi

Kirjallisuuskatsauksella voidaan havainnoida kokonaiskuvaa määritellystä tutkimusalueesta. Kirjallisuuskatsauksella pyritään tunnistamaan ongelmia asiakokonaisuudessa sekä antamaan suosituksia kehittämiseen tutkimalla olemassa olevaa aineistoa. Kirjallisuuskatsauksen metodina on se, että tehdään tutkimusta tutkimuksista. Kirjallisuustutkimuskatsaus sisältää tutkimusten asiakokonaisuuksien kriittisen arvioinnin ja tulosten analysoinnin. Integroivaa tutkimuskatsausta käytetään, kun halutaan tutkia asiaa mahdollisimman monipuolisesti. Kirjallisuuskatsauksen tarkoituksena on todellakin antaa kokonaiskuva tietystä aiheesta tai asiakokonaisuudesta. Tämä tapahtuu kokoamalla ja arvioimalla olemassa olevaa kirjallisuutta, tutkimuksia ja muita lähteitä. Kirjallisuuskatsauksella voidaan selvittää, mitä tietoa on jo olemassa tietyllä tutkimusalueella, tunnistaa tutkimuksen aukkoja ja ongelmia sekä tarjota suosituksia tulevaisuuden tutkimukselle.

Kirjallisuuskatsauksen metodina on usein "tutkimus tutkimuksista", mikä tarkoittaa, että siinä arvioidaan ja analysoidaan eri lähteitä, kuten tutkimuksia, artikkeleita ja muita julkaisuja. Tarkoituksena on tiivistää ja syntetisoida olemassa olevaa tietoa, jotta saadaan kattava ja monipuolinen käsitys tutkimusalueesta.

Kokonaisuudessaan kirjallisuuskatsauksen avulla pyritään luomaan selkeä kuva tutkimusalueesta, tunnistamaan tutkimuksen nykytila, havaitsemaan mahdolliset aukot tiedossa ja tarjoamaan suuntaviivoja tulevalle tutkimukselle. (Salminen, A 2011)

Integratiivinen kirjallisuuskatsaus on tutkimusmenetelmä, joka yhdistää ja integroi aiheeseen liittyvän kirjallisuuden eri lähteistä. Tästä syystä integroiva kirjallisuuskatsaus ei sisällä omaa empiiristä tutkimusosuutta, vaan sen sijaan se perustuu jo olemassa olevaan kirjallisuuteen. (Salminen, A 2011)

Integratiivinen kirjallisuuskatsaus on tietyn aihealueen laajaan kirjallisuuteen perustuva synteesi, joka pyrkii yhdistämään ja integroimaan erilaisia tutkimustuloksia ja -menetelmiä. Tavoitteena on tuottaa kattava ja järjestelmällinen yhteenveto aiheesta, joka tarjoaa uutta tietoa, käsitteellistä selkeyttä, teoreettista kehystä ja tutkimuksen suuntaa. Integratiivinen kirjallisuuskatsaus on erityisen hyödyllinen, kun aihealue on monitieteinen tai kun olemassa oleva tieto on hajallaan eri aloilla tai käytössä olevat menetelmät ja teoriat ovat erilaisia. Kirjallisuuskatsauksen toteuttaminen vaatii systemaattista lähestymistapaa ja tarkkaa seulontaa, jotta tutkimukset ovat laadukkaita ja luotet-

tavia (Salminen, A 2011). Valitun tutkimusmenetelmän käytön katsotaan tuottavan lisätietoa ja lisäarvoa robotiikan kyberturvallisuuden tasoa arvioitaessa ja pystyvän yhdistämään eri tutkimusalojen tietoa yhteen kokonaisuuteen.

7.3 Tutkimusongelman nimeäminen

Työn lähtökohtana oli selvittää Jyväskylän ammattikorkeakoululle kyberturvallisuuden kypsyystasoa teollisen robotiikan ympäristössä. Työssä pyrittiin myös hakemaan kehittämiskohteita ja uusia tutkimuskysymyksiä aiheen osalta.

Työ vastaa seuraaviin tutkimuskysymyksiin:

- Mikä on teollisuusautomaatiojärjestelmien kyberturvallisuuden kypsyystaso?
- Huomioiko riskienhallinta kyberturvallisuuden tällä hetkellä ICS-järjestelmissä?

7.4 Aineiston haku ja valinta

Tutkimuksessa käytettiin erilaisia hakumenetelmiä relevanttien tutkimusten ja julkaisujen löytämiseen, jotka käsittelevät kyberturvallisuutta teollisessa robotiikassa. Muutamilla testihauilla alkoi löytyä relevantit standardit sekä tutkimusten tietokannat, joihin hakuja voitiin kohdistaa.

Aineiston etsimiseen käytettiin seuraavaa menetelmää:

1. Tutkimusten hakuun käytettiin hakutermeinä ICS, kyber/cyber, sekä standardit IEC 62443 ja SP800-82.
2. Tietoa haettiin standardeista, näihin viitatuista tutkimusartikkeleista ja yleisesti internetistä. Tämän lisäksi tarkistettiin aiemmin tehdyt lopputyöt ja miten niissä asiaa on käsitelty.
3. Tulokset rajattiin siten että niiden tuli liittyä suoraan teollisen robotiikan käsittelyyn – eli epärelevantit tulokset ”cyber-sanasta” rajattiin pois, ellei viitettä teolliseen robotiikkaan löytynyt.
4. Tutkimusten lukeminen ja niiden käyttämien lähteiden tarkistaminen auttoi löytämään uusia relevantteja tutkimuksia.

5. Etsittiin myös vähemmän tunnettujen tutkimusalueiden julkaisuja ja käytettiin eksploratiivista lähestymistapaa. Tämä voi auttaa löytämään uusia näkökulmia aiheeseen ja laajentamaan aineiston kattavuutta.
6. Lopuksi edeltä mainittu hakuprosessi dokumentoitiin, jotta se voidaan toistaa ja toinen tutkija voi tarkastaa, miten aineisto on valittu.

Integroivan kirjallisuuskatsauksen hakuprosessi on systemaattinen, joten hakutulokset tulee seuloa tiukkojen kriteerien mukaan. Kun kaikki relevantit tutkimukset on löydetty, tulokset analysoidaan ja arvioidaan aineisto sekä vastataan tutkimuskysymyksiin.

7.5 Tutkimusaineiston esittely

Koska työn toimeksiantaja oli koulutusorganisaatio, niin työssä haluttiin hakea näkökulmaa myös sen suhteen, miten oppilaitoksista valmistuvat näkevät kyberturvallisuuden teollisessa robotiikassa. Theseus tietokannasta löytyi hakusanoilla ”cyber ja ics” tuloksia, hakua rajattiin siten että lyhenteen ICS tuli löytyä tutkimuksen asiasanoista tai tiivistelmästä. Muutoin cyber/kyber hakusana tuottaa liikaa vääriä tuloksia. 2010-luvulla mainintoja löytyi kaksi ja vastaavasti kaksi kuluvalta 2020-luvulta. Johtopäätös lukumääristä on se, ettei automaation tai robotiikan ohjausjärjestelmien kyberturvallisuus ole kovin suosittu lopputyön aihe. Standardin IEC 62443 ja SP800-82 käyttö hakuterminä tuottaa yhden tuloksen molemmille ajanjaksoille. Työt sisältyvät myös toiseen hakuun, hakutulos on tarkistettu syksyllä 2023.

Lopputöiden määrä on vaatimaton, mutta selkeästi kasvava. Teollisen robotiikan järjestelmien standardeja sen sijaan on useita, joita voidaan hyödyntää organisaation kybersietoisuuden kehittämisessä ja kyberuhkiin varautumisessa. Seuraavassa luetellaan relevantit standardit, joita käytettiin työn aineistona. OT-järjestelmien ja ICS-järjestelmien kyberturvallisuutta käsittelee useat standardit:

- IEC 61511 standardi käsittelee prosessiteollisuuden turvallisuutta, mutta sillä on myös merkitystä ICS-järjestelmien kyberturvallisuuden kannalta. Standardi antaa käytännön ohjeita riskienhallintaan, turvallisuuskonsepteihin ja suojaukseen.
- ISA/IEC 62443 on standardisarja, joka sisältää erilaisia vaatimuksia ja suosituksia ICS-järjestelmien kyberturvallisuuden varmistamiseksi. Standardi kattaa muun muassa ICS-laitteet, ohjelmistot ja verkot.

- ISO 27001 standardi tarjoaa yleisiä tietoturvallisuuden standardeja, jotka ovat sovellettavissa myös ICS-järjestelmiin.
- NIST SP-800-32 sisältää yleisiä periaatteita ja käytäntöjä verkkoturvallisuuden suunnitteluun, toteutukseen ja ylläpitoon. Se käsittelee muun muassa verkkoturvallisuuden peruskäsitteitä, kuten hyökkäykset, uhat, haavoittuvuudet ja riskien arviointi. Dokumentissa esitellään myös yleisiä verkkoturvallisuuden suojaustoimia, kuten käyttäjätunnistus- ja pääsynhallintajärjestelmät, palomuurit, salaus- ja varmuuskopiointitekniikat sekä tietojen hallinnointi.
- NIST SP-800-82 standardi käsittelee ICS-järjestelmien suojaamista tietoturvaloukkausten varalta.
- NIST SP-800-84 standardi käsittelee testaus-, koulutus- ja harjoitusohjelmia, jotka ovat tärkeitä ICS-järjestelmien käyttäjien harjaannuttamiseksi poikkeamiin.
- NIST SP-800-137 julkaisema kyberturvallisuuden suosituksia sisältävä standardi, joka käsittelee tietoturvan hallintaa ICS-järjestelmissä. Se sisältää käytännön ohjeita ja suosituksia ICS-ympäristöjen turvallisuuden parantamiseksi, mukaan lukien suojaustoimien suunnittelu ja toteutus, riskienhallinta, häiriötilanteiden hallinta sekä tapahtumien valvonta ja tietoturvan auditointi.
- NIST SP-800-161 standardi ohjeistaa kuinka voidaan varmistua tietotekniikan eheydestä logistisessa kanavassa.

Standardit tarjoavat hyödyllisiä suosituksia ja käytännön ohjeita, joita voidaan käyttää ICS-järjestelmien kyberturvallisuuden varmistamiseen. Huomattavaa on, ettei kyberturvallisuuden standardien noudattaminen takaa täydellistä suojaa kaikilta hyökkäyksiltä vaan ICS-järjestelmien suojaamiseen tarvitaan jatkuvaa valvontaa ja kehittämistä. Yleisesti tietoturvaa, kyberturvallisuutta ja riskienhallintaa suositellaan hallittavaksi jatkuvalla prosessilla.

7.6 Tutkimusaineiston laadunarviointi

Työssä käytettiin luotettavuuden varmennukseen hakemalla eri standardit, johon selvityksen tuloksia voitiin verrata. Työssä käytettiin vain vertaisarvioituja tutkimuksia sekä itse tutkimusalueen kartoituksessa käytiin läpi laaditut lopputyöt asiasana rajauksin. Tutkimusaineisto oli laadultaan korkea (standardit), mutta lopputöiden osuus on vaatimaton tällä hetkellä teollisen robotiikan ky-

bertoimintaympäristön osalta. Osin voidaan kuitenkin hyödyntää muiden tekniikan alojen tutkimuksia kuten informaatiotekniikka, automaatiotekniikka, sulautetut järjestelmät ja kriittinen infrastruktuuri.

7.7 Aineistolähtöisen sisällön analyysin toteutus

Aineistolähtöinen sisällön analyysi on joustava menetelmä, joka mahdollistaa tutkijan tutkimuskysymysten muuttamisen tutkimuksen aikana. Tutkimuskysymyksiä ei kuitenkaan muokattu työn aikana. Tutkimusmenetelmä mahdollisti kuitenkin eri tieteenalojen yhdistämisen ja laajan aineistokirjon käytön.

8 Pohdinta

ICS-järjestelmät ohjaavat automaatiojärjestelmiä ja siten ne ovat käytössä myös teollisuusrobotiikassa. Ne ovat suunniteltu teollisuus- ja infrastruktuuriympäristöihin ja niiden kyberturvallisuutta ohjaamaan on kirjoitettu useita standardeja. ICS-järjestelmiä käytetään yleensä valvomaan ja ohjaamaan kriittisiä prosesseja, joilla on merkittävä vaikutus teolliseen tuotantoon ja yhteiskuntaan, mikä tekee niistä houkuttelevan kohteen kyberhyökkäyksille.

Teollisen robotiikan ja sen ohjausjärjestelmien kyberturvallisuuden kypsyystaso määritellään useilla eri tekijöillä, kuten organisaation maturiteetilla, riskienhallinnan toteutuksella, ICS-järjestelmien monimutkaisuudella, käytettävillä teknologioilla ja käytännöillä. Yleisesti ottaen teollisen robotiikan järjestelmien kyberturvallisuuden kypsyystaso on suhteellisen alhainen verrattuna tietotekniikan alaan, koska ICS-järjestelmiin liittyvät turvallisuusstandardit ja -käytännöt ovat kehittyneet vasta suhteellisen hiljattain ja niiden toimeenpano kestää vuosia. Tämän lisäksi teollisen robotiikan laitteiden elinkaari on pitkä, joka hidastaa niiden päivittämistä.

Organisaatiot voivat parantaa ICS-järjestelmiensä kyberturvallisuuden kypsyystasoa noudattamalla erilaisia turvallisuuskäytäntöjä, kuten NIST:n kyberturvallisuuskehystä (Cybersecurity Framework), IEC 62443 -standardia tai NIST SP 800-82, jotka on kehitetty nimenomaan ICS-järjestelmien turvallisuuden parantamiseksi. Lisäksi organisaatioiden on tärkeää käyttää kontrolleja järjestelmien suojaamiseen, joilla voidaan pienentää kyberhyökkäysten vaikutuksia, kuten palomuureja, hyökkäyksen tunnistusjärjestelmiä, hälytysjärjestelmiä ja turvallisuusvalvontaa.

Standardien käyttö toimii usein hyvänä ohjenuorana osana organisaatioiden vaatimuksenmukaisuuden hallintaa. Vaatimuksenmukaisuuden hallinta (eng. compliance management) on prosessi, jolla varmistetaan, että organisaation toiminta noudattaa soveltuvia lakeja, asetuksia, standardeja ja niiden perusteella laadittuja ohjeita. Tämä on olennainen osa organisaation riskienhallintaa ja tietoturvallisuuden hallintaa, jolla pyritään varmistamaan organisaation toiminnan olevan edellä mainittujen periaatteiden mukaista. Vaatimustenmukaisuuden hallintaan kuuluvat vaatimusten tunnistamisen lisäksi toiminnan nykytilan arvioiminen, sen riskien tunnistaminen ja toimintaa ehkäisevien ja korjaavien toimenpiteiden prosessit. Yrityksen kannattaa asettaa vaatimuksia myös omille alihankkijoilleen sopimusten ja yhteistyökumppaneilleen teollisen robotiikan ympäristöissä sopimusten avulla (ISO 37301-2021).

Teollisuusautomaation robotiikan kyberturvallisuuden kypsyystasoa voidaan arvioida tekemällä haastatteluja organisaatioon ja varmistamaan siten tehtyjä havaintoja toimintamalleista, käytännöistä ja dokumentaatiosta. Kyberturvallisuutta voidaan todentaa teknisellä auditoinnilla, joka varmistaa laadittujen kontrollien toimivuutta määriteltyjä riskejä vähentämään. Jotta kokonaisjärjestelmä olisi turvallinen, tulee arvioinnissa kiinnittää huomiota toimintaan liittyvät sopimuskumppanit ja siihen että myös nämä huomioivat kyberturvallisuuden kokonaisvaltaisesti. Robotiikkalaitteiston hankintaa ei voida pitää pelkkänä koneena vaan sen toiminnassa tulee huomioida perinteisen tietotekniikan ongelmat ja näiden haavoittuvuuksienhallinta. Toimintamallit voivat tuoda haavoittuvuuksia järjestelmään aivan kuten ihmisten toiminta muutoinkin turvallisuuteen. Ihmisten liittyessä toimintaan on tärkeätä jalkauttaa tietoa, kouluttaa ihmisiä ja motivoida toimimaan turvallisella tavalla koska seuraukset piittaamattomuudesta voivat olla vakavia.

Kyberhyökkäykset alkavat odottamattomasti ja yllättäen. Organisaatiolla ja henkilöstöllä olisi tämän vuoksi oltava kyky vastata tapahtumiin ja ennalta estää niitä. Ei ole myöskään optimaalinen tilanne, että henkilöstö joutuu sopeutumaan toimenpiteiden toteuttamiseen ensimmäisen kyberhyökkäyksen sattuessa. Tämän vuoksi henkilöstön tietoturvatietoisuuden lisääminen auttaa ymmärtämään mahdollisia uhkia ja niistä seuraavia riskejä. Tämän lisäksi kybersuojaamisen harjoittelu on yksi tapa parantaa organisaation ja henkilöstön kykyä vastata kybertapahtumiin.

Automaation ja teollisen robotiikan ohjelmistoa suorittavat osat ovat usein suljettuja ja näiden toimintaa ei pystytä varmistamaan muuten kuin testaamalla käyttötapauksia ja simuloimalla. Kuitenkin laitteistojen sulautetut osat saattavat sisältää ohjelmistokoodia, jonka turvallisuutta ei voida tarkistaa. Kriittisiltä osin turvallisuutta voitaisiin tarkastaa takaisinmallintamalla piirien, logiikoiden

ja prosessorien toimintaa. Huomattavaa on myös, että lähes jokainen komponentti sisältää ohjelmistokoodia kuten oheispiirit, prosessorit ja massamuistit.

8.1 Takaisinmallinnus

Takaisinmallinnus tarkoittaa prosessia, jossa tuotteen, järjestelmän tai ohjelmiston rakenne ja toiminta selvitetään purkamalla se osiin ja analysoimalla sen toimintaa. Tämä tehdään usein luomalla käänteinen malli alkuperäisestä tuotteesta tai järjestelmästä.

Mallinnuksen tarkoituksena voi olla esimerkiksi selvittää tuotteen tai järjestelmän toimintaa, kehittää parannuksia tai luoda uusia versioita. Se voi myös auttaa ymmärtämään laitteiden rakennetta ja toimintaa. Samassa yhteydessä voidaan myös havaita ohjelmiston suunnitteluun ja ohjelmointiin liittyneitä virheitä tai haavoittuvuuksia.

8.2 Riskienhallinnan merkitys robotiikan järjestelmissä

Teollisen robotiikan automaatiojärjestelmissä riskienhallinta on tärkeä osa suunnittelua ja toteutusta. Suurimmat riskit liittyvät usein ihmisten ja koneiden väliseen vuorovaikutukseen, kuten esimerkiksi loukkaantumiset tai vahingot, jotka voivat aiheutua, kun ihminen joutuu kosketuksiin liikkuvan robotin kanssa. Näitä riskejä pyritään minimoimaan erilaisilla suojalaitteilla ja -järjestelmillä.

Yksi tärkeimmistä riskienhallintakeinoista on fyysinen suojelu, kuten aitaukset ja turvakaiteet, jotka estävät ihmisiä pääsemästä liikkuvien koneiden ja robottien lähelle. Tämän lisäksi robotteihin voidaan asentaa suojalaitteita, jotka tunnistavat ihmisten läsnäolon ja pysäyttävät robotin automaattisesti, jos vaaratilanne syntyy. Lisäksi robottien toimintoja ja liikkeitä voidaan rajoittaa ohjelmallisesti, jotta ne eivät pysty liikkumaan liian nopeasti tai aiheuttamaan vahinkoa, jos ne törmäävät johonkin esteeseen. Ohjelmat voivat myös sisältää tarkkoja toimintamalleja, joilla vältetään ihmisten ja robotin välinen kontakti.

Riskienhallintaan kuuluu myös koulutus, joka on välttämätöntä robotiikan käyttäjille ja ylläpitäjille. Käyttäjien on tiedettävä, miten robotti toimii ja mitä turvatoimenpiteitä on otettava käyttöön. Robotiikka laitteita käyttävien on myös oltava koulutettuja robotin ylläpitoon ja tarkistettava sen suojalaitteiden kunto säännöllisesti.

Vaarojen tunnistaminen ja riskienhallinta on tärkeä osa teollisen robotiikan automaatiojärjestelmien suunnittelua ja toteutusta, jotta voidaan varmistaa, että ihmiset voivat turvallisesti työskennellä robotin läheisyydessä ja estää vahinkojen tapahtumisen.

Teollisen automaatio robotiikan järjestelmiä hallitaan tietokoneohjelmilla, jotka ovat alttiita kyberhyökkäyksille, kuten haittaohjelmille ja tietomurroille. Kyberhyökkäys robotiikan järjestelmään voi aiheuttaa vakavia turvallisuusriskejä, kuten robottien hallinnan menettämisen tai mahdollisuuden, että ne voivat vahingoittaa ihmisiä tai ympäristöä.

Kyberturvallisuuden riskienhallintaan tulee sisällyttää useita käytäntöjä, joilla pyritään estämään tai rajoittamaan mahdollisuudet, että robotiikan järjestelmät altistuvat kyberhyökkäyksille ja että ne pystyvät rajoittamaan mahdolliset hyökkäykset tehokkaasti. Näitä standardien suosittelemia käytäntöjä ovat:

- Järjestelmän ohjelmistopäivitykset ovat tärkeitä, koska ne korjaavat turvallisuuspuutteet ja haavoittuvuudet, jotka voivat altistaa robotiikan järjestelmät hyökkäyksille.
- Verkko on suojattava asianmukaisella salauksella, palomuureilla ja muilla tietoturvakäytännöillä, joilla estetään hyökkääjän pääsy verkkoon. Verkko voi mahdollistaa myös järjestelmän haavoittuvuuden fyysisen tilaturvan ulkopuolelta.
- Käyttöoikeuksien hallinta ja myöntäminen tulee olla määritelty ja käyttäjätunnusten käytön monitorointi sen varmistamiseen, että vain valtuutetut henkilöt pääsevät järjestelmään.
- Järjestelmänvalvonta ja lokitietojen kerääminen mahdollistaa tietoturvaongelmien selvittämisen.
- Henkilöstöä tulisi kouluttaa tietoturva-asioissa, jotta he ymmärtävät turvallisuusriskejä ja pystyvät tunnistamaan potentiaaliset hyökkäykset.

Kokonaisuudessaan kyberturvallisuus on tärkeä osa robotiikan järjestelmien kokonaisuuden riskienhallintaa, ja se tulisi ottaa huomioon jo suunnitteluvaiheessa, jotta itse robotiikan järjestelmästä ei muodostu heikointa lenkkiä. Tämä auttaa varmistamaan, että robotiikan järjestelmät ovat turvallisia ja suojaavat ihmisiä ja ympäristöä kaikilta mahdollisilta turvallisuusriskeiltä, joita myös kyberhyökkäykset voivat aiheuttaa.

Operatiivisen teknologian osalta kyberturvallisuuteen liittyy erityisesti teknisten haavoittuvuuksien lisäksi se, että voidaan tarkoituksellisesti muuttaa järjestelmän toimintaa siten, että siitä aiheutuu

seuraamuksia järjestelmälle tai ympäröivälle maailmalle. Tällöin ICS-järjestelmän väärinkäyttö tulee tunnistaa myös sen osalta, että ohjelmointi näyttää toimivan kuten on suunniteltu, mutta sen toiminnassa tapahtuisi anomalioita, vaikka järjestelmä olisi päivitetty ja ajan tasalla.

9 Tutkimuksen tulosten arvionti ja johtopäätökset

Työn tutkimuskysymyksinä oli teollisuusautomaatiojärjestelmien kypsyystaso teollisessa robotiikassa ja kuinka kyberturvallisuus on huomioitu niissä. Lisäksi työltä haluttiin uusia tutkimus- ja kehittämiskohteita robotiikan kyberturvallisuuden parantamiseen. Työn tietopohjainen tausta pyrkii vastaamaan kaikkiin kysymyksiin ja kehittämiskohteet on mainittu tuloksissa.

Havaintona on se, että uusien koulutettavien insinöörien tai tekniikan alan ammattilaisten näkökulma on harvoin pelkästään teollisen robotiikan kyberturvallisuuden parantaminen. Kyberturvallisuus on osaltaan yksi osa-alue, joka vaikuttaa robotiikan toimivuuteen ja osaltaan pienentää käytettävyyteen kohdistuvien uhkien vaikutuksia. Kuitenkin turvallisuuden kokonaisvaltaiseen parantamiseen kuuluu huomioida kaikki toimintaan vaikuttavat asiat. Tällöin teollisen robotiikan järjestelmien suunnitteluperusteena täytyy käyttää myös kyberturvallisuuden parantamista ja riskien kartoittamista. Kyberturvallisuuden huomiointi alentaa käytettävien resurssien määrää verrattuna siihen, että turvallisuuden parantamista lähdetään toteuttamaan myöhemmin järjestelmän ollessa jo käytössä tai pahimmillaan vasta kun kyberhyökkäys jo kohdistuu omaan tuotantoympäristöön. Kyberturvallisuuden riskeihin varautumista pystytään parantamaan, kun esitetään yrityksen toiminnasta vastaavalle johdolle vaikutukset, joita riskien huomiotta jättäminen saattaa aiheuttaa.

9.1 Tutkimuksen luotettavuus

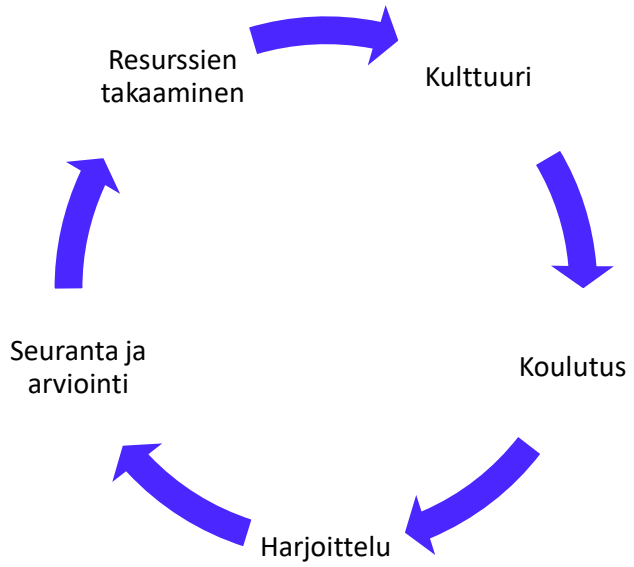
Tutkimuksen tuloksia voidaan pitää luotettavina, koska eri standardien vertailun tuloksena on saman suuntaiset havainnot ja toimenpiteet, joita esitetään toteuttavaksi. Standardeja on vertailtu kattavasti ja systemaattisesti. Standardien vertailu on helposti todennettavissa ja aineisto saatavilla, jotta voidaan varmentaa työn tulokset. Työ vastaa asetettuihin tutkimuskysymyksiin ja tutkimusmenetelmä on valittu siten että sillä on pystytty yhdistämään eri alojen tietoa. Tutkimustavan valinta lisää tutkimuksen luotettavuutta ja sitä että sillä pystytään luomaan uutta tietoa asiasta ja vahvistamaan tutkimuksen pätevyyttä. Aineistoa on standardien muodossa riittävä määrä, jotta

tuloksia voidaan pitää luotettavina. Aineisto on helposti löydettävissä ja varmennettavissa viitteiden avulla. Tulosraportointi luo uutta katsantokantaa teollisen robotiikan kyberturvallisuuden parantamiseen sekä mahdollisia uusia tutkimusaiheita. Tutkimus ja raportointi on toteutettu eettisesti oikein ja tutkimus sisältää lähdeviitteet Jyväskylän ammattikorkeakoulun käytäntöjen mukaisesti.

9.2 Johtopäätökset ja jatkotutkimusehdotukset

Työn tuloksena havaittiin, että teollisuusorganisaatiot kamppailevat monisyisen kyberturvallisuusongelman kanssa. Riskienhallinta on jopa vaativampi kuin perinteisen IT-ympäristön, koska sen lisäksi tulee OT-ympäristö hallittavaksi ja huomioitavaksi. Robotiikan ympäristöjen kehittämisessä ja operoinnissa tulee omaksua kypsä turvallisuusasenne tietotekniikan sekä operatiivisen teknologian ympäristöissä, samaan aikaan kun molemmat joutuvat yhä kasvavan määrän hyökkäysten kohteeksi - ja edelleen rajat näiden kahden alueen välillä hämärtyvät päivä päivältä enemmän. Kyberturvallisuuden huomiointi tulee ottaa lähtökohdaksi jo järjestelmien suunnitteluvaiheessa ja huomioida kyberuhat käytön aikana ja hallita niitä jatkuvan riskienhallinnan avulla sekä kouluttaa ja harjoituttaa henkilöstö toimimaan oikealla tavalla kyberuhkiin varautumisessa.

Työn tuloksena nousee esille pääteemat, joiden avulla robotiikan kyberturvallisuuden kypsyystasoa voidaan parantaa. Siihen liittyvät tekniset asiat, järjestelmien operointi ja henkilöstön kouluttaminen ja ohjeistaminen keskeisten kyberturvallisuuden uhkien torjumiseen. Kuvion yhdeksän kaaviossa kuvataan kokonaisvaltaista kyberturvallisuuden prosessia, joka lähtee kyberturvallisuuden kulttuurista, kouluttamisesta ja jalkauttamisesta. Näiden lisäksi tulee toki huomioida työssä esitellyt standardit, jotka antavat myös teknisiä keinoja kyberturvallisuuden parantamiseen. Suuri osa parantamisesta liittyy kuitenkin ihmisten toiminnan ohjaamiseen teknisten kontrollien ohella.



Kuvio 8. Kyberturvallisuuden kokonaisvaltainen parantaminen

9.2.1 Kokonaisvaltainen turvallisuuden lähestymistapa

Kyberturvallisuuden parantamisen tulisi olla kokonaisvaltainen prosessi, joka kattaa kaikki robotiikkaan vaikuttavat näkökohdat. Tämä sisältää sekä fyysisen maailman, järjestelmien käyttäjät sekä ohjelmistojen loogisen maailman. Kyberturvallisuudessa tulee huomioida kaikki muuttujat ja näiden yhteisvaikutus toimintaympäristössä. Turvallisuuden parantaminen ei saa olla pelkästään reaktiivista, vaan se tulee sisällyttää suunnitteluprosessin alkuvaiheisiin.

9.2.2 Kustannustehokas toiminta ja resurssien säästäminen

Kyberturvallisuuden huomioiminen varhaisessa vaiheessa suunnittelua voi säästää resursseja pitkällä aikavälillä. Turvallisuuspuutteiden korjaaminen järjestelmän jo ollessa käytössä voi olla huomattavasti kalliimpaa ja vaikeampaa kuin niiden ennaltaehkäisy suunnitteluvaiheessa. Tämä edellyttää koko organisaation sitoutumista ja tietoturvan integroimista liiketoimintaprosesseihin ja ohjelmistokehitykseen varhaisessa vaiheessa. Tällä voidaan varmistaa, että kyberturvallisuus on integroitu prosesseihin, toimintatapoihin ja tekniikkaan.

9.2.3 Vaikutusten viestiminen johdolle

Yrityksen toiminnasta vastaa ylin johto. He resursoivat toiminnan ja yrityksen johdon tulisi olla täysin tietoinen kyberturvallisuuden merkityksestä ja riskeistä. Selkeä viestintä vaikutuksista, joita turvallisuuden laiminlyönti voi aiheuttaa, auttaa johtoa ymmärtämään tarpeen sijoittaa resursseja turvallisuuden parantamiseen. Vaikutuksia voidaan kuvata säännönmukaisilla riskiarvioilla ja riskienhallinnan toimenpiteiden suorittamisen prosesseilla.

9.2.4 Koulutus ja tietoisuuden lisääminen

Henkilöstön tietoisuuden lisääminen kyberturvallisuudesta on tärkeää. Säännöllinen koulutus ja tietoisuuden kasvattaminen auttavat kaikkia yrityksen työntekijöitä ymmärtämään turvallisuuden merkityksen ja omaksumaan parhaat käytännöt. Vertailukohtana voitaisiin pitää lentoturvallisuutta, jossa pyritään estämään onnettomuudet sekä oppimaan niistä onnettomuuden tapahduttua, jotta samaa ei tapahdu uudelleen. Tavoitteena tietoisuuden lisäämisessä on kouluttaa ja opastaa robotin käyttäjiä, operaattoreita tai ylläpitäjiä teollisen robotiikan turvallisuuden tärkeydestä ja parhaista käytännöistä. Tämä auttaa lisäämään tietoisuutta ja estämään inhimillisiä virheitä tai laiminlyöntejä, jotka voivat vaarantaa robotin käyttäjien turvallisuuden ja kyberturvallisuuden. Yrityksien on hyvä tarjota koulutusta, opetusohjelmia tai työpajoja siitä, miten robotin käyttö, ylläpito ja vianmääritys voidaan tehdä turvallisesti ja varmasti. Tämän ohella tulee myös laatia ohjeita, menettelyjä tai sääntöjä siitä, miten robottia ja sen tietoja käsitellään, säilytetään tai hävitetään. On hyvä myös kannustaa palautteen antamiseen ja raportointiin mahdollisista kyberturvallisuusongelmista tai tapahtumista. Vain tällaisen jatkuvan kehittämisen avulla voidaan nostaa toimintaympäristön kyberturvallisuuden kypsyystaso riittävän korkeaksi.

9.2.5 Kestävä turvallisuuskulttuuri

Pitkällä aikavälillä tavoitteena tulisi olla organisaation kulttuurin muuttaminen siten, että turvallisuus ml. kyberturvallisuus on keskeinen osa jokapäiväistä toimintaa. Tämä edistää turvallisuuden tason pitkäaikaista ylläpitoa ja jatkuvaan parantamiseen pyrkimistä. Turvallista toimintaa kyberuhkien osalta olisi hyvä kouluttaa harjoituksissa tai vastaavissa demonstraatioissa, joissa saataisiin myös henkilöstön parannusehdotuksia samalla kun turvallisuuskulttuuria jalkautetaan.

9.3 Jatkotutkimusaiheita työn aihepiiriin liittyen

Teollisen robotiikan kyberturvallisuusympäristön kehittämiseksi olisi varteenotettavia tutkimusaiheita:

1. **Verkkohyökkäysten havaitseminen ja reaaliaikainen estäminen:** tutkimukset keskittyvät suojautumaan haittaohjelmilta, verkkohyökkäyksiltä ja muilta tietoturvariskeiltä. Tässä tutkimuksessa pyrittäisiin reaaliaikaiseen kykyyn havaita ja torjua verkkohyökkäyksiä teollisen automaation ja robotiikan järjestelmiin.
2. **Järjestelmän haavoittuvuusanalyysi**: tutkimuksessa pyrittäisiin löytämään toteutuksen toiminnallisia ja teknisiä heikkouksia teollisen robotiikan ympäristössä sekä tutkimaan näiden kumulatiivisia vaikutuksia.
3. **Robotiikan ohjauksen ohjelmistojen takaisinmallintaminen ja analysointi**. Rautatason ohjelmiston analysointi (eng. firmware). Tutkimuksen tavoitteena olisi löytää piileviä heikkouksia toteutustavoissa, joiden esiintyminen kuitenkin saattaa romuttaa ohjelmistolla toteutetut tietoturvallisuuskontrollit.
4. **Turvallinen ohjelmistokehitys.** Ohjelmiston lähdekoodin analyysimenetelmien käyttäminen teollisen automaatiojärjestelmien turvallisuuden parantamiseen kehityksen aikana. Tavoitteena olisi vähentää ohjelmistoissa esiintyviä virheitä ja vikatilanteita. Ohjelmistojen laadun parantamiseen käytettävien automatisointityökalujen ja testaustyökalujen käytön ohjeistaminen.
5. **Ohjelmistokoodin ja toiminnan anomalioiden etsintä koneoppimisen ja tekoälyn avulla.** Ohjelmistokoodin toteutusta ja tarkistamista on mahdollista opettaa tekoälylle ja koneoppimisen malleille, jotka voivat löytää poikkeamia toiminnasta.
6. **Robotiikan kyberfyysisten olosuhteiden kybersietoisuuden parantaminen (resilienssi).** Tavoitteena on luoda robotiikkajärjestelmiä, jotka pystyvät toimimaan turvallisesti ja luotettavasti myös kyberhyökkäysten tai fyysisten uhkien alla.

Lähteet

Ackerman, P.,2017, Industrial Cybersecurity, ISBN 978-1-78839-515-1

Baskerville, R. (1991), “Risk analysis: an interpretive feasibility tool in justifying information systems security”, European Journal of Information Systems, Vol. 1 No. 2, pp. 121-30)

Baezner, M&R, Patrice.,2018, Stuxnet,https://www.researchgate.net/publication/323199431_Stuxnet.

Counsil on Foreign Relations, 2015, https://www.cfr.org/cyber-operations/compromise-power-grid-eastern-ukraine, haettu 22.10.2023

Black Hat, 2018, How TRITON Disrupted Safety Systems & Changed the Threat Landscape of Industrial Control Systems, https://www.youtube.com/watch?v=Hw2HclZV2Kw.

Cryptolabs, 2004, ROTL, http://www.pruefziffernberechnung.de/Originaldokumente/2rot13.pdf, haettu 10/2023.

Dragos, Chernovite PIPEDREAM, 2022, https://hub.dragos.com/whitepaper/chernovite-pipedream, haettu 10/2023.

Dragos, Analysis of Safety System Targeted Malware, 2017, https://www.dragos.com/wp-content/uploads/TRISIS-01.pdf, haettu 06/2023

Flaus, J-M., 2019, Cybersecurity of Industrial Systems, https://doi.org/10.1002/9781119644538.fmatter.

Gutmantis, J., 2019, A Report from The Trenches, https://www.youtube.com/watch?v=XwSJ8hloGvY, haettu 09/2023.

Goud N., Suspected Ekans Ransomware attack on Honda - Cybersecurity Insiders (cybersecurity-insiders.com), haettu 05/2023.

Hunter & Gutierrez, 2020, EKANS Ransomware: A Malware Targeting OT ICS Systems | FortiGuard Labs (fortinet.com), haettu 2/2023.

IEC 61508, Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems (E/E/PE, or E/E/PES).

IEC 62443-1-1 Konseptit ja malli, SFS-eKirja 631-3:2013

IEC 62443-2-1 Tietoturvaohjelman vaatimukset omistajille, SFS-eKirja 631-3:2013

IEC 62443-4-1 Tuotekehityksen elinkaarivaatimukset, SFS-eKirja 631-3:2013

IEC 62443-4-2 Komponenttien tekniset vaatimukset, SFS-eKirja 631-3:2013

ISO/IEC 27001:2022, Information security, cybersecurity and privacy protection

Information security management systems Requirements, https://www.iso.org/standard/27001

ISO/IEC 27002:2022, Information security, cybersecurity and privacy protection Information security controls, https://www.iso.org/standard/27002.

Jensen, C., The Importance of Trust in Computer Security. 8th IFIP International Conference,2014, https://link.springer.com/chapter/10.1007/978-3-662-43813-8_1

Larson, S. Singleton C., 2020, Ransomware in ICS Environmnets, https://hub.dragos.com/hubfs/Whitepapers/Ransomware%20in%20ICS%20Environments%20-%20Dragos%202020.pdf?hsLang=en.

Lehto, M., (2013), The_Ways_Means_and_Ends_in_Cyber_Security_Strategies, https://www.researchgate.net/publication/338197891_Lehto_The_Ways_Means_and_Ends_in_Cyber_Security_Strategies.

Mandiand, 2019,Totally Tubular Treatise Triton and Tristation, https://www.mandiant.com/resources/blog/totally-tubular-treatise-triton-and-tristation

Mitre Att&ck matrix for ICS-systems, https://attack.mitre.org/versions/v13/matrices/ics/, haettu 10/2023.

Mäntylä, J., (2014) Kyberaseiden vaikutus kriittisen infrastruktuurin tietojärjestelmiin, http://urn.fi/URN:NBN:fi-fe2014081432832.

NIST Special Publication SP 800-30 Rev. 1, Guide for Conducting Risk Assessments, https://doi.org/10.6028/NIST.SP.800-30r1

NIST Special Publication 800-53, Security and Privacy Controls for Information Systems and Organizations, https://doi.org/10.6028/NIST.SP.800-53r5

NIST Special Publication 800-82, Guide to Industrial Control Systems (ICS) Security, https://doi.org/10.6028/NIST.SP.800-82r3.

Ngambeki, I., E. Spafford, S. Ansari, I. Alhasan, M. Basil-Camino and D. Rapp, "Creating a Concept Map for ICS Security – A Delphi Study," *2021 IEEE Frontiers in Education Conference (FIE)*, Lincoln, NE, USA, 2021, pp. 1-7, doi: 10.1109/FIE49875.2021.9637386.

Nuclear Regulatory Comission, 2004 , Tristation 1131 Developer's Workbench, https://www.nrc.gov/docs/ML0932/ML093290419.pdf.

Pöyhönen J.,2017 Informaatioteknologian tiedekunnan julkaisuja No. 55/2018

https://www.jyu.fi/it/fi/tutkimus/julkaisut/it-julkaisut/ics_standardit_verkkojulkaisu.pdf.

Salminen A. 2011, Mikä kirjallisuuskatsaus?: johdatus kirjallisuuskatsauksen tyyppeihin ja hallinto-tieteellisiin sovelluksiin, https://urn.fi/URN:ISBN:978-952-476-349-3.

Turvallisuuskomitea, Kansallinen riskiarvio, 2018,
https://julkaisut.valtioneuvosto.fi/handle/10024/161332.

Vilches V., Kirschgens L.,Calvo A, Cordero A., Rodrigo, Pisón R, Vilches D., Rosas A., Mendia G., Juan L., Ugarte I., Gil-Uriarte E., Tews E., Peter A., 2018, Introducing the Robot Security Framework (RSF), a standardized methodology to perform security assessments in robotics-Research Paper, https://arxiv.org/abs/1806.04042.

Liitteet

LIITE 1 Hyökkäyksen eteneminen

Hyökkäysvektori	Hyökkäys	Pysyvyys	Oikeuksien laajentaminen	Piiloutuminen	Luotaus	Sivuttainen siirtymä	Kerääminen	Komentokanava	Estetään turvallisuustoiminnot	Vaikutetaan prosessikontrolliin	Vaikutus
Haitallinen sivusto	Ajomoodin muutos	Kovakoodatut tunnukset	Myönnetyn oikeuden laajennus	Ajomoodin muutos	Luettelointi	Oletustunnukset	Liikenteen uudelleen ohjaus, kuuntelu	Yleiset portit	Aktivoidaan laitteiston huoltotila	Väsytyshyökkäys	Omaisuuden vahinko
Julkinen palvelu	Komentokehote	Ohjelmiston muutokset	Kirjastojen hyväksikäyttö	Ohjelman virheen hyväksikäyttö	Verkon kuuntelu	Etäpalvelu hyväksikäyttö	Automatisoitu keräys (skriptit)	Välityspalvelin	Hälytysten estäminen	Parametrimuutos	Ohjauksen estäminen
Etähallintapalvelu	Ulkoinen ohjelmarajapinta	Laitemoduuli ohjelmisto		Poistetaan haittakoodin jäljet	Verkon palveluiden tunnistaminen	Kovakoodatut tunnukset	Ohjetietokannat	Standardi ohjelmistorajapinta	Estetään komentoviestit	Alustan ohjelmiston muutos	Järjestelmän tilan monitoroinnin estäminen
Internetissä oleva laite	Graafinen käyttöliittymä	Projektitiedostot		Naamioituminen	Verkon hallintapalveluiden tunnistaminen	Työkalujen siirto verkkoresurssien kautta	Järjestelmän paikalliset tiedot		Estetään raportointi viestit	Statusviestin muutos	Saatavuuden katkos
Ulkoinen media	Dynaamiset Kirjastot	Alustaohjelmisto		Piilotettu hallintaohjelma	Langattomien verkkojen kuuntelu	Ohjelmiston lataus	Ajomoodien tunnistaminen		Estetään sarjaliikenne	Auktorisoimaton kontrollikomento	Hallinnan katkos
Valepalvelu	Suoritusjonon manipulointi	Sallitut tunnukset		Muokataan tilatietoja		Etäpalveluiden sallittu käyttö	Tulojen ja lähtöjen tietojen tallennus		Vaihdetaan salasanat		Tuotannon katkos
Kohdistettu kalastelu	Natiivit rajapinnat					Sallitut tunnukset	Prosessien tilatiedot		Datan tuhoamine		Turvallisuustoimintojen häiriö
Näkymättömät hallintalaitteet	Skriptit						Tulojen ja lähtöjen tunnistaminen		Palvelunesto		Turvallisuustoimintojen menettäminen
Langaton verkko	Käyttäjän toimet						Ohjelman lataaminen laitteistoon		Laitteen uudelleen käynnistys		Monitorointinäkyvyyden menetys
							Näytön kuvan kaappaus		Lähtöjen ja tulojen manipulointi		Ohjauksen manipulointi
									Hälytysasetusten muokkaus		Valvonnan manipulointi
											Tiedon varkaus