Opinnäytetyö (AMK)

Energia- ja ympäristötekniikka (Insinööri)

2022

Mikael Haapakorva

LAIVAN ENERGIANVALVONTAJÄRJESTELMÄN KYBERTURVALLISUUS

TURKU AMK
TURKU UNIVERSITY OF APPLIED SCIENCES

Opinnäytetyö (AMK) | Tiivistelmä

Turun ammattikorkeakoulu

Energia,- ja ympäristötekniikka

Opinnäytetyön valmistumisajankohta kevät 2022 | 41 sivua

Mikael Haapakorva

Laivan energiavalvontajärjestelmän kyberturvallisuus

Tässä työssä tutkittiin kyberturvallisuuden kattavuutta laivan energianvalvontajärjestelmässä. Työssä käytettiin toimeksiantajan case järjestelmää, jonka kyberturvallisuuden määrittämiseen käytettiin meriteollisuuden standardeja, kattojärjestöjen suosituksia ja kyberturvallisuus alan työkaluja. Lisäksi työssä pohdittiin case-järjestelmän haavoittuvuuksia sen rajapinta-analyysin avulla, jossa käytiin läpi järjestelmän yhteyksien turvallisuustoimet. Työn teoriapohja luotiin kirjallisuuskatselmuksena vertaisarvioitujen tutkimusten ja artikkelien pohjalta.

Kyberturvallisuuden katsauksen tuloksena saatiin analysoitua järjestelmän kyberturvallisuuden kattavuus. Taustateorian avulla pääteltiin, että täydellistä kybersuojausta ei ole mahdollista toteuttaa, mutta järjestelmään tunkeutuminen voidaan tehdä erittäin haastavaksi. Tuloksena todettiin järjestelmän olevan toimeksiantajan käytössä olevien standardien mukainen, sekä järjestelmän yhteyksien suojauksien olevan tarvittavalla tasolla, jotta kyberhyökkäyksen mahdollisuus on alhainen.

Asiasanat:

Kyberturvallisuus, energianvalvontajärjestelmä, energia, energiansäästö, standardit, laiva, meriteollisuus

Bachelor’s Abstract

Turku University of Applied Sciences

Energy and environmental engineering

Completion year of the thesis spring 2022 | 41 pages

Mikael Haapakorva

Cybersecurity of a ship energy supervisory system

In this thesis, the goal was to assess and explore the cybersecurity coverage of a ship energy supervisory system. A case system was utilized where marine industry standards, umbrella organization recommendations, -and cybersecurity industry tools were used to determine the system’s cybersecurity coverage. In addition, the study considered the cybersecurity vulnerabilities of the case system through an interface drawing that was used to go through the security measures of the system’s connections.

The theoretical basis of the thesis was established through a literature review based on peer-reviewed studies and articles.

As a result of the system’s cybersecurity review, it was found that the system’s cybersecurity measures are in order with the standards in use in the system. In addition, with the theoretical basis it was concluded in the study that it is impossible to make an impenetrable system instead, it is possible to make it difficult enough to ensure a reduced chance of a cyber-attack.

Keywords:

Cybersecurity, Energy Control System, Energy, Energy Saving, Standards, Ship, Marine Industry.

Sisältö

1 Johdanto **6**
1.1 Tutkimuskysymys ja menetelmät 7

2 Kyberturvallisuus **8**
2.1 Kyberturvallisuuden määrittäminen 8
2.2 Kyberturvallisuus merenkulussa 11
2.2.1 International Maritime Organization 12
2.2.2 Kyberturvallisuuskeskus 14
2.2.3 DNV GL 14
2.3 Kyberuhat 15
2.3.1 Sisäinen uhka 17
2.3.2 Ulkoiset uhat 18
2.4 Kyberturvallisuuden standardeja ja ohjeistuksia 19

3 Case study: Energianvalvontajärjestelmä **22**
3.1 Järjestelmän rakenne 22
3.2 Laivan automaatio 23
3.3 Käytönvalvonta 25
3.4 Käyttöliittymä 25
3.5 Case järjestelmän kyberturvallisuus 27
3.5.1 Käänteinen SSH-tunneli 28
3.5.2 Navigointi NMEA 28
3.5.3 HTTPS 30
3.5.4 Modbus RTU yhteydet 30
3.5.5 Käyttöliittymä 31
3.6 CIA-triad 32

4 Yhteenveto **34**

5 Pohdinta **35**

Lähteet **37**

Taulukot

Taulukko 1 Kyberturvallisuuden tasot. Mukaillen (Lehto, 2019)

Kuvat

Kuva 1. Riskien hallinta-askeleet. 13
Kuva 2. Laivan järjestelmät ja niiden mahdolliset uhat Huoltovarmuuskeskus (2021) mukaillen. 16
Kuva 3 case järjestelmä. 23
Kuva 4 Modbus RTU protokollan toiminnan esimerkki. (William, L. & Mostia, Jr 2019 mukaillen.) 24
Kuva 5 case järjestelmän käyttöliittymä pääsivu. 26
Kuva 6 Case järjestelmän historiafunktio. 26
Kuva 7 Case järjestelmä rajapintapiirros. 28
Kuva 8 Hyökkäykselle altistunut järjestelmä. Jakaboczki & Adamko (2015) Mukaillen. 31

1 Johdanto

Tässä opinnäytetyössä selvitetään mitä kyberturvallisuus tarkoittaa erityisesti merenkulussa, lisäksi opinnäytetyössä selvitetään case järjestelmän avulla toimeksiantajan energianvalvontajärjestelmän kyberturvallisuutta ja sitä, miten kyberturvallisuus on toteutettu järjestelmässä ja vastaako se valikoituja standardeja. Case study on toteutettu toimeksiantajan antamien tietojen pohjalta, sekä myös järjestelmän testauksen ja tarkastelun avulla. Opinnäytetyössä kyberturvallisuutta arvioidaan merenkulun kyberturvallisuuden standardien avulla, sekä lisäksi hyödynnetään alan työkaluja kyberturvallisuuden kattavuuden määrittelemiseksi. Työkalujen avulla voidaan arvioida kybertuvallisuuden kattavuutta tarkastelemalla järjestelmän eri osa-alueita ja niiden rajapintoja ulkoisiin järjestelmiin. Kyberturvallisuuden selvittämiseksi työssä käydään läpi yleisimpiä kyberuhkia. Lisäksi työssä esitellään lyhyesti serveriympäristö, energianvalvontajärjestelmä, sekä kyberturvastandardeja. Lopuksi työssä käydään läpi case studyn tulokset, sekä arvioidaan tulosten perusteella järjestelmän kyberturvallisuutta tutkitun teorian pohjalta.

Kyberuhat ja kyberturvallisuus muuttuvat ajan kuluessa jatkuvasti ja niitä ymmärretään eritavoin riippuen tulkitsijan näkökulmasta. Vaikka kyberturvallisuus on mainittu jo vuosia sitten 80-luvulla, edelleen ala vaatii enemmän tutkimista ja ymmärrystä. Kyberturvallisuus ja sen uhat monesti määritellään tekniseksi vaikkakin sen uhat ovat monialaisia. Sen takia kyberturvallisuus vaatisi enemmän objektiivista ja monialaista näkemystä organisaatioiden sisällä, sillä monet organisaatiot saattavat kohdella kyberturvallisuutta subjektiivisesti ja yksiulotteisesti. Laajojen tutkimusten puutteen, sekä alan jatkuvasti muuttuva laajuus vaikeuttaa dynaamisten kyberturvallisuus raamien kehittämistä.

1.1 Tutkimuskysymys ja menetelmät

Työn tutkimuksella halutaan selvittää toimeksiantajan energiavalvontajärjestelmän kyberturvallisuuden kattavuutta ja sitä, että vastaako se eri kattojärjestöjen, valvovien viranomaisten, sekä luokituslaitosten standardeja.

Työ on toteutettu niin, että kyberturvallisuuden teoriapohja on luotu kirjallisuustutkielmana eri vertaisarvioitujen tietokantojen pohjalta. Lisäksi opinnäytetyön aikana case järjestelmä pilottiasennetaan toimeksiantajan tiloihin. Case järjestelmään asennetaan tarvittavat suojausasetukset, sekä tarkastetaan järjestelmän toiminta. Työn tuloksena saadaan arvio tutkittavan järjestelmän kyberturvallisuuden kattavuudesta.

2 Kyberturvallisuus

Kyberturvallisuus on erittäin laaja käsite, joka sisältää niin fyysistä maailmaa kuin myös kybermaailmaa. Tämän tutkimuksen aihepiirissä käsite kyber- tarkoittaa digitaalista kokonaisuutta ja vaikka tutkimukseen voi liittyä fyysisiä toimijoita niin valtaosa kokonaisuutta on digitaalista (Sähkötekniikan ja energiatehokkuuden edistämiskeskus ry, 2020). Digitaalisella kokonaisuudella tarkoitetaan sähköisiä järjestelmiä, jotka ovat kytkettyjä yhteen joko langallisesti tai langattomasti. (Boyes, H & Isbell, R. 2017) Tämän tutkimuksen puitteissa sähköiset järjestelmät koostuvat energianjakelusta, tietoverkoista sekä fyysisistä järjestelmistä. Näissä järjestelmissä hyödynnetään sekä langattomia että langallisia järjestelmiä, kuten energianjakelu-, anturi-, tutka- ja tietoverkkojärjestelmiä.

2.1 Kyberturvallisuuden määrittäminen

Kyberturvallisuuden voi määritellä työkaluiksi ja käytännöiksi, joiden avulla suojataan jotain digitaalista kokonaisuutta sekä henkilön tai henkilöiden identiteettiä. Digitaalista kokonaisuutta voidaan suojata esimerkiksi digitaalisilla tietoturvaohjelmilla, tarkoilla työohjeilla tai käytännöillä, esimerkiksi työpaikalla käytetään vain työnantajan hyväksymiä tietokoneita ja järjestelmiä. (Boyes, H & Isbell, R. 2017) Suojauksen lisäämiseksi organisaatioissa tulisi olla erilliset ohjeet ja toimintatavat yrityksen tietoturvapolitiikasta, johon on pääsy yrityksen työntekijöillä, yhteistyökumppaneilla ja asiakkailla. Ohjeilla pyritään varmistamaan tiedon luottamuksellisuus, eheys ja käytettävyys. (McAfee 2022)

Jotta voi ymmärtää kyberturvallisuutta, on syytä tarkastella kokonaiskuvaa. Kokonaisuuden määrittämistä vaikeuttaa se, että riippuen toimialasta ja arvioijan näkökulmasta, kyberturvallisuuteen voidaan sisällyttää monia eri tekijöitä.

Kyberturvallisuus voidaan jakaa viiteen eri tasoon, mikä helpottaa kokonaisuuden määrittelyä. Tasot muodostavat kybermaailman ja

kyberturvallisuuden tasot, joiden avulla voidaan tarkastella eri järjestelmiä kyberturvallisuuden laajuuden määrittelemiseksi. Taulukossa 1 nähdään, että tasoja ovat kognitiivinen, palvelu, semanttinen, syntaktinen ja fyysinen taso. Kun jonkin järjestelmän kyberturvallisuutta halutaan määritellä, on helppo ensin tarkastella mille tasoille järjestelmä ulottuu kybermaailmassa. Tämän jälkeen järjestelmään on suoraviivaisempaa määrittää tarvittavat suojaustoimenpiteet. (Lehto 2021)

Taulukko 1 Kyberturvallisuuden tasot. Mukaillen (Lehto 2019)

Kognitiivinen taso	Kognitiivisella tasolla tarkoitetaan inhimillistä ongelmanratkaisua- ja tulkintaympäristöä. Esimerkiksi valvontahuoneen operaattori toimii kognitiivisella tasolla järjestelmän kanssa. Operaattori vastaanottaa x järjestelmästä tietoa, jonka tulkitsee ja ymmärtää oman kokemuksen ja koulutuksen pohjalta omalla tavalla.
Palvelutaso	Palvelutaso on erittäin laaja, joka sisältää monia eri palveluja kuten: julkiset ja kaupalliset verkkopalvelut, sekä kansalaisen palvelut, sosiaalisenmedian palvelut ja tietoliikennepalvelut.
Semanttinen taso	Käyttäjän hallitsema informaatio- ja tietosisältö, sekä käyttäjän hallinnassa oleva järjestelmän toimintojenohjaus sisällytetään semanttiseen tasoon. Esimerkiksi tallennetut salasanat, metadata, sekä mainos algoritmit ovat semanttisella tasolla.
Syntaktinen taso	Syntaktinen taso sisältää järjestelmän ohjaus- ja hallintaohjelmat, sekä verkkoprotokollat, virheenkorjaukset ja verkkokättelyn. Esimerkiksi kahden palvelimen välistä tiedon jakamista tapahtuu syntaktisella tasolla.
Fyysinen taso	Fyysisellä tasolla on verkkolaitteet, kytkimet, reitittimet, lankayhteydet, sekä langattomat yhteydet.

Kansainvälinen luokituslaitos DNV GL on julkaissut kattavan artikkelin tietoturvan määrittämisestä kolmen pääperiaatteen avulla: Luottamuksellisuus, eheys ja saatavuus. Tätä kutsutaan nimellä CIA- triadi. Kolme kyberturvallisuuden pääpiirrettä luo käsityksen siitä mitä organisaation tulee suojata, sillä nämä pääperiaatteet on toteuduttava, jotta yrityksen kyberturvallisuus toimii. (DNV 2020)

CIA-triadi on määritetty seuraavasti (DNV 2020):

1. Luottamuksellisuudella tarkoitetaan tilannetta, jossa tiedon jakoa rajoitetaan henkilöille, jotka ovat siihen valtuutettuja. Luottamuksellisuuden toteutumiseen vaaditaan, että organisaation sisällä aktiivisesti estetään luvattomien pääsy dataan käsiksi.
2. Eheydellä tarkoitetaan nimensä mukaisesti, että jaettu tieto on ehjää eikä sitä ole peukaloitu. Tiedon eheyttä voidaan organisaatioissa suojata salaamalla, auditoimalla, sertifikaateilla, tunkeutumisen esto järjestelmillä, sekä todennusjärjestelmillä. Näiden askeleiden avulla siirretty tieto voidaan todeta oikeaksi, aidoksi ja luotettavaksi.
3. Saatavuudella tarkoitetaan tiedon laadukasta saatavuutta, eli data on saatavilla nopeasti ja luotettavasti valtuutetuille henkilöille. Luotettavuus taataan toimintamenetelmillä, sekä tietoverkkojärjestelmillä. Yksi kyberhyökkäyksen kohteista organisaatiossa voisi olla tietoverkkojärjestelmä. Palvelunesto hyökkäyksillä tai paremmin tunnettuna DDoS- hyökkäyksillä voidaan estää tietoverkkojärjestelmän luotettavan toimivuuden.

On argumentoitu, että CIA-triadi ei välttämättä ole riittävän dynaaminen nykyajan alati muuttuvan kyberturvallisuuden tarpeen takia. CIA-triadia voidaan laajentaa Parkerian Hexad-lisäelementeillä. Lisäelementit tuovat enemmän dynaamista arviointia kyberturvallisuuteen, joka auttaa määrittämään entistä paremmin kyberturvan laajuuden. Parkerian Hexad sisältää kolme lisäelementtiä seuraavasti: (Andress 2014)

1. Aitous/luotettavuus – Aitoudella tarkoitetaan sitä, että esimerkiksi viesti, liiketapatuma tai muu tieto on alkuperältään oikealta lähettäjältä. Aitouden todentamisessa vaaditaan tunnistautumista.
2. Kontrolli/hallussapito – Kontrollilla tai hallussapidolla tarkoitetaan sitä, että ulkopuolinen taho tai henkilö ei saa haltuunsa luottamuksellista tietoa ja pysty kontrolloimaan sitä. Eli yritysten tulee pyrkiä suojelemaan tieto-omaisuuttansa salauksilla tai tekijänoikeuksilla kontrollin lisäksi. Esimerkiksi kirjojen sisältö on julkista tietoa, mutta tekijänoikeuksilla suojattua.
3. Hyödyllisyys – Tieto-omaisuutta tulee pyrkiä suojelemaan esimerkiksi salaamalla se. Mallissa hyödyllisyydellä tarkoitetaan, että vuotanut tieto on hyödytöntä. Yrityksen salaiset tiedot voidaan salata, jolloin tieto olisi hyödytöntä ulkopuolisen käsissä.

2.2 Kyberturvallisuus merenkulussa

Nykyään merenkulun aluksissa on yhä enemmän digitalisaatioon, integraatioon ja automaatioon perustuvia järjestelmiä, jotka ovat alttiita kyberhyökkäyksille. Kyberhyökkäyksillä kyseisiin järjestelmiin voisi olla suuria haittoja esimerkiksi navigoinnille, miehistölle, matkustajille sekä kohteena olevien yrityksien maineelle. (Tuulaniemi 2020)

Risteilyaluksien elinkaari on keskimäärin 25–30 vuotta, joten aluksilla on käytössä jo elinkaaren puolessa välissä vanhaa teknologiaa. Ongelmana on se, että laivojen varustamot ja omistajat ovat laitevalmistajien armoilla laitteistojen päivityksistä ja huollettavuuksista, eikä laitevalmistajien markkinoilla välttämättä ole parempaa ratkaisua teknologian nopean kehittymisen vuoksi. Lisäksi laitteissa ei välttämättä ole itsessään sisäänrakennettua tietoturvaa, vaan kyberturvallisuus on rakennettava laitteisiin lisäosamaisesti, joka voi tarkoittaa taloudellisesti suurta kuluerää. Tämän tyyppiseen kyberturvallisuus uhkaan on syytä kiinnittää enemmän huomiota. (Traficom 2020)

Järjestelmät ovat nykyään niin monimutkaisia, että merenkulun kyberturvalle on määritelty ohjenuoria standardisoimaan suojausta. Kyberturvallisuutta määrittelee ja ohjeistaa monet tahot kuten IMO (International maritime organisation), TRAFICOM (Liikenne- ja viestintävirasto) ja luokituslaitokset.

Merenkuluntoimijat käyttävät kyberturvallisuudessa esimerkiksi ISO, IEC ja DNV standardeja, joita käydään tutkimuksessa myöhemmin läpi kappaleessa 2.4.

2.2.1 International Maritime Organization

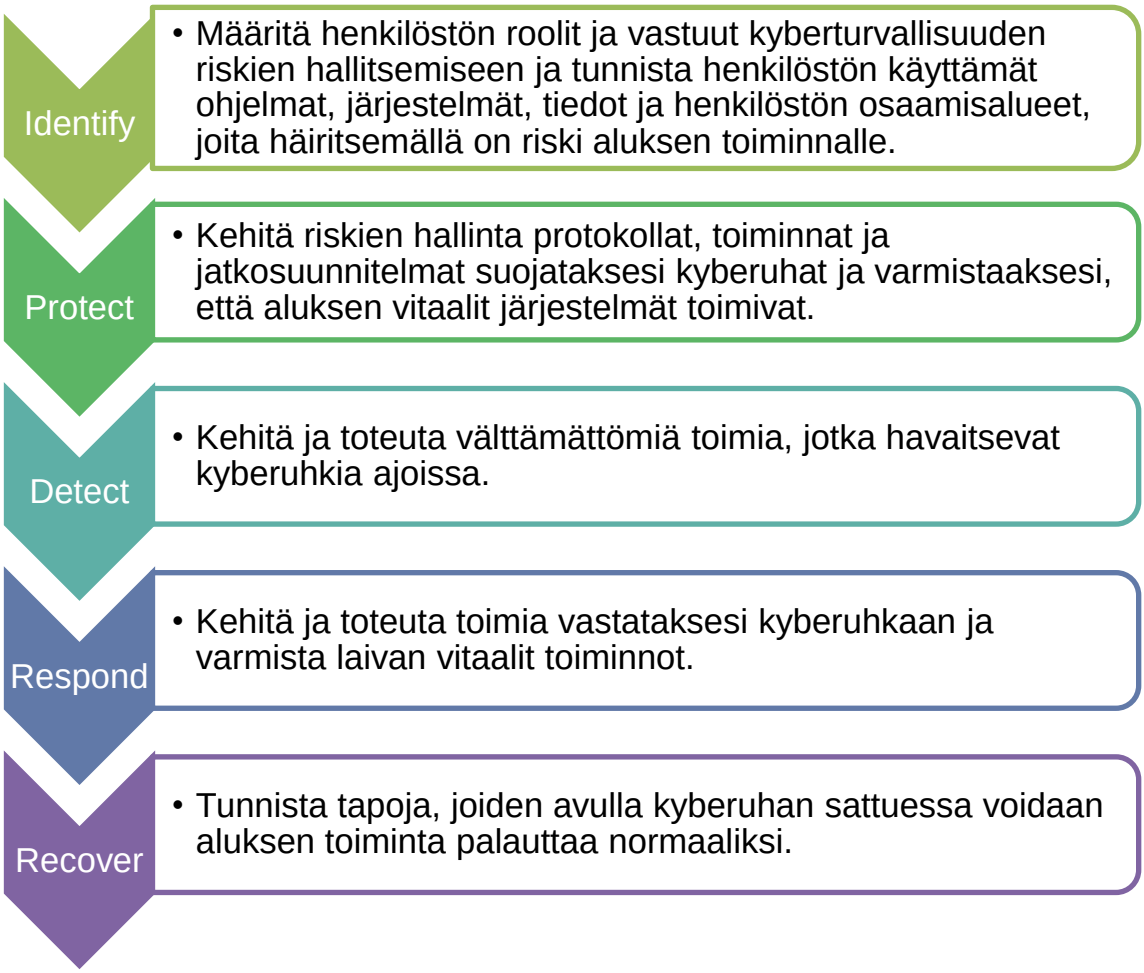
IMO on perustettu vuonna 1948 jonka tehtävänä on luoda ympäristöystävälliset, kestävät, sekä turvalliset vaatimukset merenkululle. IMO käyttää hyödyksi tehtävässään merenkulun turvallisuuden, navigointi ja ympäristöystävällisyys standardeja, sekä ottamalla huomioon merenkulkuun liittyvät oikeudelliset asiat ja toteuttamalla IMO:n välineiden tehokas käytäntöönpano. (IMO 2021)

Merenkulun kyberturvallisuuden perustana toimii IMO:n MSC:n (Maritime Safety Committee) päätöslauselma MSC.428(98). Jotta kyberturvallisuus saataisiin mahdollisimman laajaksi, päätöslauselmassa todetaan, että jokaisen merenkuluntoimijan tulisi nopeuttaa ja kehittää toimia kyberturvallisuutta varten sekä hyödyntää IMO:n ohjenuoraa ylätason kyberturvallisuuden riskien hallintaan. Lisäksi MSC:n päätöslauselmassa todetaan, että varustamoiden tulee huomioida kyberturvallisuus riippumatta alusten käyttöönottovuodesta tai toiminta-alueesta. Tästä johtuen varustamoiden tulee huomioida kyberturvallisuus jo suunnittelun aikaisessa vaiheessa, jotta järjestelmät kestäisivät teknologian edistystä koko laivan eliniän ajan. Päätöslauselma velvoittaa huomioimaan kyberturvallisuuden turvallisuusjohtamisjärjestelmä 1.1.2021 lähtien. (IMO 2017)

Iso osa kyberturvallisuudesta on riskien hallintaa. Riskien hallinnalla tarkoitetaan prosessia, jossa tunnistetaan, analysoidaan, arvioidaan ja kommunikoidaan kyberuhista ja hyväksytään, vältetään, siirretään tai hallitaan riski hyväksyttävälle tasolle, huomioiden kustannukselliset haitat. (IMO 2017)

IMO:n MSC-FAL.1 ohjenuorassa kyberturvallisuuden riskien hallintaa toteutetaan kuvassa 1 seuraavin askelin: Tunnista (Identify), Suojaa (protect), Havaitse (detect), Vastaa (respond) ja Toivu (recover). (IMO 2017)

Riskien hallinta-askeleet seuraavasti:



Kuva 1. Riskien hallinta-askeleet.

Mainitun ohjenuoran lisäksi IMO mainitsee päätöslauselmassaan, että ISO, IEC ja luokituslaitosten standardeja, tulisi hyödyntää IMO:n ohjenuoran toteutuksessa. Esimerkiksi päätöslauselmassa mainitaan ISO/IEC 27001, jossa määritellään vaatimukset tietoturvallisuuden hallintajärjestelmän luomista, toteuttamista, ylläpitämistä ja kehittämistä varten. (ISO/IEC 27000:2016) Lisäksi mainitaan monia merenkulun toimijoita, kuten varustamoita ja luokituslaitoksia,

joilla on omia suosituksia ja ohjeita kyberturvallisuutta varten. Standardeista, ohjeista ja suosituksista kerrotaan lisää kappaleessa 2.4.

2.2.2 Kyberturvallisuuskeskus

Kyberturvallisuuskeskus on Traficom:in alainen viranomainen, jonka vastuulla on kaikki CERT (Computer Emergency Response Team) -toiminnot. CERT toimintojen tehtävänä on ennaltaehkäistä tietoturvaloukkauksia ja tiedottaa tietoturva-asioista. Kyberturvallisuuskeskuksen tavoitteena on yleisten viestintäverkkojen ja viestintäpalveluiden turvallisen ja häiriöttömän toiminnan varmistaminen sekä turvata elintärkeitä yhteiskunnan toimintoja. (Traficom 2021) Traficom puolestaan on Suomen valtion liikenne- ja viestintävirasto, joka edistää liikennejärjestelmien toimivuutta ja turvallisuutta sekä varmistaa laadukkaat ja turvalliset viestintäyhteydet ja -palvelut. (Traficom 2019)

Kyberturvallisuuskeskus pitää merenkulun kyberturvallisuutta tärkeänä turvana tulevaisuuden merenkululle. Kybertuvallisuuskeskus ohjeistaa merenkuluntoimijoita, kuten varustamoita noudattamaan IMO:n ohjeistuksia, mutta ei kuitenkaan itse laadi sääntöjä tai vaadi toimia kybertuvallisuudelle. (Traficom 2020)

2.2.3 DNV GL

DNV GL on yksityinen kansainvälinen akkreditoitu luokituslaitos, joka tarjoaa palveluitaan lukuisille teollisuuksille kuten öljy-, kaasu-, energia-, elintarvike-, sekä meriteollisuudelle. Yrityksessä eri teollisuusalat on jaettu omille liiketoimisektoreille. Meriteollisuussektori toimii nimellä DNV Maritime, jolla on 12 000 alusta ja offshore-yksikköä luokituksen alaisena varmistaa, että heidän luokitetut aluksensa maailmalla ovat turvallisia, kestäviä sekä tehokkaita. (DNV 2022)

Lisäksi DNV GL on ottanut vahvan otteen kybertuvallisuuteen vaatimalla ja ohjeistamalla meriteollisuuden toimijoita kyberturvalliseen toimintaan ja ajatteluun. DNV näkee kybertuvallisuuden erittäin tärkeänä muun turvallisuuden lisäksi, sillä alusten operointi halutaan optimaaliseksi, joka saavutetaan vain digitalisaation avulla. Uudet lait, säännöt, sekä ohjeistukset yhdessä IMO:N kanssa auttavat DNV:tä parantamaan kybertuvallisuutta merellä. DNV:lla on standardeja, luokkamerkintöjä ja ohjeistuksia meriteollisuuden toimijoille, joista lisää kappaleessa 2.4. (DNV 2022)

2.3 Kyberuhat

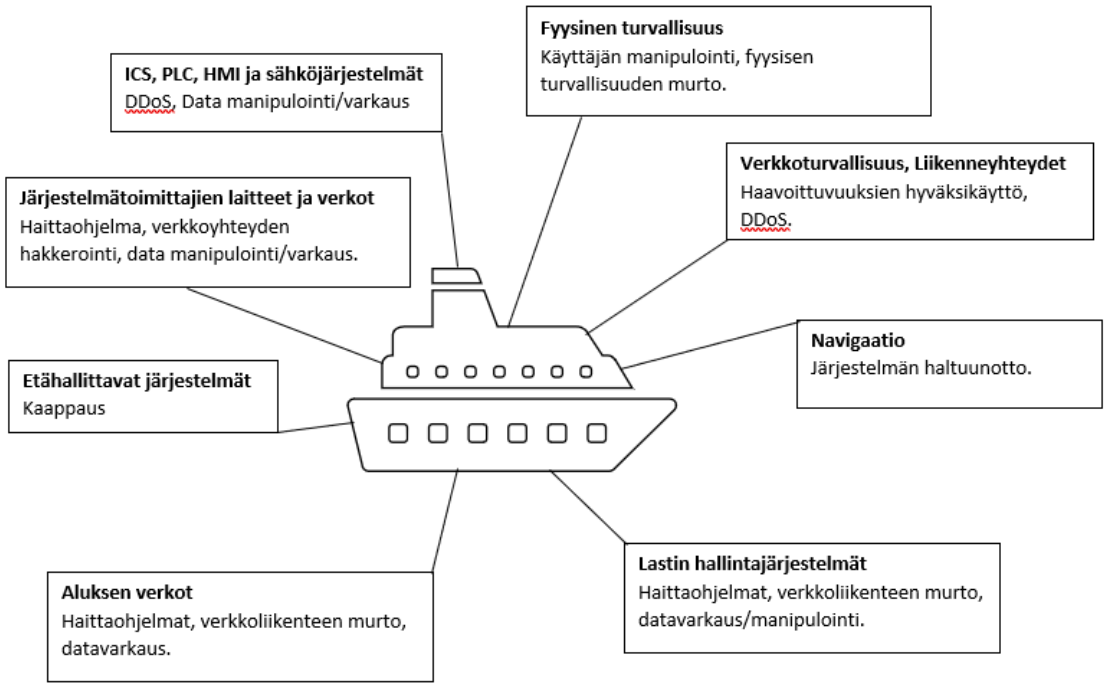
Perinteisesti ajatellaan, että kyberturvallisuudella vain yritetään suojautua kyberuhilta, mutta kyberturvallisuudella pyritään suojaamisen lisäksi myös vastaamaan hyökkäyksiin ja toipumaan hyökkäyksistä. Kyberuhkia voi siis olla niin digitaalisia kuin fyysisiä. Aikaisemmin tutkimuksessa on kerrottu, että kyberuhat ovat monialaisia ja jatkuvasti muuttuvia, tämä tarkoittaa sitä, ettei kyberuhilta ole mahdollista suojautua täysin. Kyberuhilla on aina mahdollisuus päästä organisaatioihin ja järjestelmiin sisälle, joten organisaatioiden ja laitevalmistajien tulisi varmistaa kyky vastata hyökkäyksiin ja toipua niistä, sillä ennakoimalla voidaan välttyä vakavilta ja taloudellisilta vahingoilta. (Trafi 2019)

Kyberuhkien vakavuutta voidaan määritellä erilaisten tarkastusmallien avulla. Microsoft kehitti 1999 vuonna mallin, jota käytettiin tietokonejärjestelmissä kyberuhkien selvitykseen. Malli on edelleen käytössä ja mallista eri versioita on paljon. STRIDE tulee sanoista Spoofing, Tampering, Repudiation, Information disclosure, Denial of service ja Elevation of privilege. Suomeksi käännettynä: Väärentäminen, peukalointi, kieltäminen, datan haavoittuvuus, palvelunesto ja käyttäjäoikeuksien korottaminen. STRIDE mallia käytetään niin, että haluttu järjestelmä puretaan pienempiin osiin mallin avulla. Jokaista mallin vaihetta käytetään järjestelmään, jonka avulla selvitetään järjestelmän haavoittuvuus, sekä uhkien vakavuus. Mallin avulla voidaan vastata, miten hyökkääjä ohittaisi todentamisprosessin, millainen vaikutus olisi, mikäli hyökkääjä pääsisi

käyttäjätietoihin käsiksi ja mitä tapahtuisi, mikäli hyökkääjä pystyisi estämään järjestelmän palveluja. (Microsoft 2009)

Tätä mallia ja muita uhanselvitysmalleja käytetään uhkien selvittämiseen nykyään laajasti tietoturva-alalla. Niillä selvitetään pääasiassa, että mikä käsiteltävässä järjestelmässä voisi mennä pieleen.

Kuvassa 1 on visuaalisesti kuvailtuna laivan kyberuhat ja mahdolliset hyökkäyskohdejärjestelmät.



Kuva 2. Laivan järjestelmät ja niiden mahdolliset uhat Huoltovarmuuskeskus (2021) mukaillen.

ICS (Industrial control system), PLC (Programmable logic controller) ja HMI (Human-machine interface) järjestelmät ovat osa operatiivisia eli OT (operational technology) - järjestelmiä, joita on syytä suojata kyberhyökkäyksiltä sillä niiden kyberuhat voivat olla jopa hengenvaarallisia riippuen hyökkäyksen kohdejärjestelmästä. Toisin kuin IT (Information technology) -järjestelmät, joiden uhat kohdentuvat yleisimmin taloudellisiin tai tiedon varastamisen uhkiin. (Huoltovarmuuskeskus 2021)

2.3.1 Sisäinen uhka

Kyberuhat eivät ole pelkästään digitaalisia vaan useimmin kyberhyökkäykset tapahtuvat vaikuttamalla henkilöihin organisaatioiden sisällä. Näitä hyökkäyksiä kutsutaan low-tech hyökkäyksiksi, jotka perustuvat henkilöiden huijaamiseen tai suostuttelemalla organisaation sisäinen henkilö kyberrikollisen avuksi joko taloudellisella tai kiristämisen avulla. Organisaation sisäisen henkilön kyberuhkaa kutsutaan nimellä Insider-threat, jolla tarkoitetaan henkilöä, joka pääsee käsiksi organisaation sisäisiin tietoihin. Suurin riski tämän tyyppiselle uhalle on silloin, kun työntekijä on harkitsemassa tai vaihtamassa työpaikkaa. Organisaation sisäinen henkilö pääsee käsiksi yrityksen sisäisiin tietoihin vielä ennen työpaikanvaihtoa, jolloin motivaatio on korkea tietojen tuhoamiseen tai varastamiseen. (Bosworth et al. 2014)

Suurimmissa organisaatioissa työtehtävät jaetaan osastoihin, joissa kyberuhat ovat erityyppisiä mutta kuitenkin perustuvat tiedon varastamiseen. Organisaatioiden osastoja ovat esimerkiksi johto, IT (informaatiotekniikka), HR (henkilöstöhallinto), logistiikka. Esimerkiksi IT-osaston sisäinen uhka voisi olla organisaation järjestelmien tietovarkaus, sillä IT-henkilöstöllä on pääsy salasanoihin ja käyttäjätietoihin, joiden avulla on pääsy korkeatasoiseen tietoon. Tai esimerkiksi HR uhka voisi olla identiteettivarkaus, sillä HR:llä on pääsy organisaatioiden henkilöstön yksityisiin tietoihin. (Bosworth et al. 2014)

Low-tech kyberuhkia on myös yritysten yhteistyökumppanit, sillä myös yhteistyökumppanit voivat olla kilpailevia yrityksiä. Tällaisissa tilanteissa uhat yleisimmin perustuvat liiallisen tiedon jakamiseen eli kilpailevat kumppanit haluavat hyödyntää yhteistyökumppanin tietoa omassa toiminnassa. (Bosworth et al. 2014) Yritysten henkilökunnan asentajasta johtajiin asti tulee siis välttää liiallisen tiedon jakamista ja säilyttää kommunikointi vain yhteistyön sisällön kannalta relevanttina. (Liu et al. 2018) CyberSecurity Watch tutkimuksen mukaan jopa 24 prosenttia kyberrikoksia tapahtui sisäisen henkilöstön toimesta, 53 prosenttia ulkoisten toimijoiden toimesta ja loput 17 prosenttia tuntemattomista lähteistä. (Software engineering institute 2012) Vaikkakin lähde

on vanha, niin voidaan kuitenkin päätellä, että organisaation sisäpiirin kyberuhat ovat huomattavia ja niitä ei tule vähätellä.

Sisäpiiriuhat voidaan kategorisoida kolmeen luokkaan vahinkouhat, pahantahtoiset uhat ja ei pahantahtoiset uhat. Nimensä mukaisesti vahinkouhat koostuvat useimmiten työntekijän piittaamattomuudesta organisaation määrittelemiin toimintatapoihin, huolimattomuudesta tai työntekijän tietotaidon puuttumisesta. Pahantahtoiset uhat koostuvat tavoista, joilla pyritään vahingoittamaan yrityksen mainetta, toimintakykyä tai taloudellista tilannetta. Pahantahtoisien uhkien toteuttajat koostuvat yleensä lähtevistä tai huonosti motivoituneista työntekijöistä. Ei pahantahtoiset uhat voidaan ajatella saman samanlaisina kuin pahantahtoiset. Erona on, että ei-pahantahtoiset uhat ole tahallisia. (Bosworth et al. 2014)

Sisäisiä uhkia pyritään turvaamaan monilla eri turvallisuusjärjestelmillä ja toimintatavoilla, jotka luovat yhdessä suuren turvallisuuskehikon. Esimerkiksi organisaation työntekijöiden työtehtäviin voidaan määritellä oma henkilötunnus, jolla tunnistaudutaan. Omalla henkilötunnuksella järjestelmät osaavat estää yritykset päästä käsiksi tietoihin joihin työntekijällä ei olisi normaaleissa työolosuhteissa tarpeellista päästä. Yksi tutuimmista toimintatavoista toimii seuraavasti: tunnistaminen, todennus ja valtuutus. Tunnistautumisella käytetään aikaisemmin mainittua henkilökorttia, jonka avulla voidaan todentaa oikea henkilö. Mikäli todennus onnistuu, järjestelmä valtuuttaa henkilön. Tätä toimintatapaa voidaan käyttää monipuolisesti esimerkiksi jonkin alueen sisällepääsyvaatimuksena tai jonkin järjestelmän kirjautumisessa. (Bosworth et al. 2014)

2.3.2 Ulkoiset uhat

Organisaation ulkopuolisella uhalla tarkoitetaan uhkaa, joka ei välttämättä ole minkäänlaisessa suhteessa hyökkäyskohteena olevaan organisaatioon.

On monia tapoja varastaa dataa tai päästä sisälle järjestelmiin, mutta monesti kyberrikolliset tähtäävät suojauksessa ihmistekijöihin. Suosituimmista

hyökkäystavoista on verkkourkinta tai verkkokalastelu. Verkkourkinnassa pyritään saamaan organisaation sisällä olevan henkilön esimerkiksi painamaan linkkiä sähköpostissa tai lataamalla haitallisia liitteitä, minkä avulla organisaation sisäinen henkilö asentaisi hyökkääjän viruksen, kiristys, - tai vakoilusoftan. Verkkourkintaa voidaan myös suorittaa tekaistujen verkkosivujen avulla, jossa pyydetään käyttäjää kirjautumaan tunnuksillansa sivulle, jonka jälkeen tunnukset olisi hyökkääjän hallussa. Verkkourkintaa tehdään myös tarkkoina hyökkäyksinä yrityksien johtotasolle, eli sähköpostit tai verkkosivut eivät ole enää niin yleispiirteisiä vaan suunnattuja tietyille henkilöille. Tarkempien hyökkäyksien tuloksena hyökkääjät pyrkivät pääsemään korkeamman tason tietoihin käsiksi. (F-secure 2022a)

Lisäksi verkkorikolliset pyrkivät saamaan rahallista tulosta hyökkäyksiltään toteuttamalla ransomware hyökkäyksiä. Ransomware -hyökkäyks koostuu haittaohjelmasta, joka salaa käyttäjän tietokoneen tiedostot tai jopa kaikkien organisaatioiden tietokoneiden tiedostot, minkä jälkeen haittaohjelma kiristää käyttäjää maksamaan lunnaat vapauttaakseen tiedostot tai haittaohjelma uhkaa poistaa tiedot pysyvästi. Ransomware haittaohjelman voi työntekijä asentaa vahingossa esimerkiksi tekaistusta sähköpostista tai se voidaan saada tietokoneelle haitallisten sivustojen ja mainosten avulla. Myös suojaamattomat Wi-FI-verkot ovat alttiita hyökkäyksille. (F-secure.com 2022b)

Ulkoisia uhkia pyritään estämään tarjoamalla henkilökunnalle kattava perehdytys mahdollisista uhista ja miten tulisi toimia sellaisen kohdatessa sekä kyberturvallisuuskäytäntöjen avulla. (Banks 2021)

2.4 Kyberturvallisuuden standardeja ja ohjeistuksia

Tässä kappaleessa käsitellään seuraavia kyberturvallisuuden standardeja: ISO27001, IEC 62443, sekä valikoituja DNV-ohjeistuksia kuten: DNVGL_RP_0496, DNVGL-OS-D203.

Standardointi on kriittistä monelle eri alalle, sillä standardoinnin avulla varmistetaan yrityksen toiminnalle yhteiset toimintatavat ja ratkaisut. Lisäksi standardoinnin avulla myös kansainvälisesti osataan toimia yhteisten sääntöjen mukaisesti. Standardit koostuu järjestelmien, toimintatapojen, turvallisuuden ja muiden toimintojen ominaisuuksista ja vaatimuksista. Standardien käyttäminen organisaatioissa on yleisimmin vapaaehtoista, mutta riippuen toimialasta niitä voi viranomaiset suositella käytettäväksi. (SFS 2021) Standardien lisäksi yritykset laativat omia ohjeistuksia ja suosituksia, joita joko suositellaan tai vaaditaan käytettäväksi.

Aikaisemmin työssä mainittu akkreditoitu luokituslaitos DNV GL on tehnyt ohjeen DNVGL_RP_0496. Kyseisessä ohjeessa kyberturvallisuus varmistetaan yhteistyössä kiinteänä osana merenkulun ja offshore-toimintojen yleistä turvallisuushallintaa. Ohje sisältää muun muassa kattavan kyberuhkakartoitustyökalun, jonka avulla yritys voi selvittää omien toimintojen hyökkäyspinta-alaa. Uhan määrittely alkaa yrityksen korkeimmasta tasosta, jossa yrityksen johto voi määrittää kyberturvallisuuden kannalta tärkeimmät avainosat, minkä jälkeen tarkemmat arvioinnit tehdään toimintojen tarkemmalla tarkastelulla ja arvioidaan järjestelmän hyökkäyksen mahdollisuutta ja seurauksia. Ohje tähtää siihen, että yritykset ovat valmiita kyberhyökkäykseen ja niiden seurauksiin. (DNV 2021) Ohje kuuluu DNV GL -organisaation suositeltuihin toimintaohjeisiin. Kyseisen ohjeen avulla yritys voi hakea itselleen ISO/IEC 27001 sertifikaatin. ISO/IEC27001 standardista lisää myöhemmin. (ISO/IEC 2016)

Lisäksi DNV GL:ltä on standardi DNVGL-OS-D203, joka ei suoranaisesti ole kyberturvallisuutta varten, vaan on tehty integroiduille ohjelmistoille riippuvaisille järjestelmille (Integrated System Dependent Software, ISDS). Esimerkkinä ISDS-laitteistosta laivalla on rikkipesurijärjestelmä, joka koostuu laajasta automaatiojärjestelmästä. Pesuri koostuu muun muassa vesikiertopumpuista ja elektronisesta venttiilinsäätöjärjestelmästä, joita ohjataan keskitetysti (Sethi 2021). ISDS-standardin avulla pyritään varmistamaan järjestelmien ja ohjelmistojen laadunvarmistusprosessien kehittäminen, joiden tarkoitus on

kestää laivan koko käyttöikä. Standardi antaa raamit järjestelmälliselle työskentelylle ohjelmistosta riippuvaisten järjestelmien integroidun yksikön tarvittavan käytettävyyden ja luotettavuuden sekä ylläpidettävyyden, jotta vaaditut turvallisuusstandardit täyttyvät. (DNVGL 2017)

Kyberturvallisuuden hallitsemiselle yritykset luovat hallintajärjestelmiä, jotka on luotu yritysten tavoitteiden saavuttamiseen. Hallintajärjestelmän tehtävänä on täyttää yrityksen, asiakkaiden ja sidosryhmien tietoturvavaatimukset sekä optimoimaan yrityksen suunnitelmia ja toimintoja. Hallintajärjestelmän oikealla käytöllä varmistetaan tieto-omaisuuden hallinta organisoidulla tavalla, jolla edistetään jatkuvaa kehitystä ja mukautumista organisaation päämäärien mukaan. Kyberturvallisuuden hallintajärjestelmille on luotu standardi ISO/IEC27001, joka on tarkoitettu tietotekniikan ja liiketoiminnan kyberturvallisuuteen. Tiivistetysti kyseinen standardi tarkoittaa sitä, että yrityksen tietoturvallisuuden hallintajärjestelmä on standardoitu johtamaan tietojensa turvaamista, jolloin tieto on virheetöntä, suojattua ja helposti käytettävissä. Jotta standardia käyttävät tahot haluavat saada parhaimman mahdollisen hyödyn hallintajärjestelmästä, tulee niiden seurata ja arvioida hallintajärjestelmän toimivuutta, tunnistaa ja etsiä uusia riskejä, sekä tarpeen mukaan parantaa järjestelmää. (ISO/IEC2700 2020)

Kyberturvallisuuden hallintajärjestelmä teollisuusautomaatio- ja ohjausjärjestelmiä varten ISO/IEC2007 ei ole täysin kelvollinen sillä se on standardi kyberturvallisuuden hallintajärjestelmälle hallinnollisella tasolla. Teollisuusautomaatio- ja ohjausjärjestelmille on erillinen hallintajärjestelmä standardi IEC62443, joka rakentuu ISO/IEC2007 neuvojen varaan. Tämä standardi perustaa yhdenmukaisuuden tarvetta teollisuusautomaatio- ja ohjausjärjestelmien ja liiketoiminnan järjestelmien välillä. Tässä standardissa eritellään se, että teollisuusautomaatio- ja ohjausjärjestelmien tietoturvallisuusriskeillä voi olla terveys-, turvallisuus- ja ympäristöseurauksia. IEC62443 standardi korostaa sitä näiden järjestelmien integrointia muihin hallintajärjestelmiin. (IEC/TS 62443-1-1[1),2)] 2013)

3 Case study: Energianvalvontajärjestelmä

Tutkimuksen tarkastelun kohteena on laivan energianvalvontajärjestelmä. Valvontajärjestelmä on vielä kehitysvaiheessa, eikä sitä ole otettu vielä käyttöön. Case järjestelmä on energianvalvontajärjestelmä, jolla pääasiassa kerätään ja valvotaan tietoa laivan järjestelmistä kuten automatiikasta, navigaatiosta, sekä laivan energian-, veden-, ja polttoaineen kulutusta. Lisäksi järjestelmä kerää tietoa laivan nopeudesta, voimansiirto-, ja HVAC – järjestelmistä. Järjestelmä on suunniteltu valvonta- ja analytiikkakäyttöön. Tällä hetkellä järjestelmä antaa ohjeita operaattorille, mitä tulee tehdä, jotta laivan operointi olisi energiatehokkaampaa. Järjestelmän tarkoituksena on antaa laivan henkilökunnalle parempi käsitys ja ymmärrys laivan järjestelmien tilasta, minkä avulla laivan henkilökunta voisi tehdä tietoisia päätöksiä laivan operoinnin suhteen.

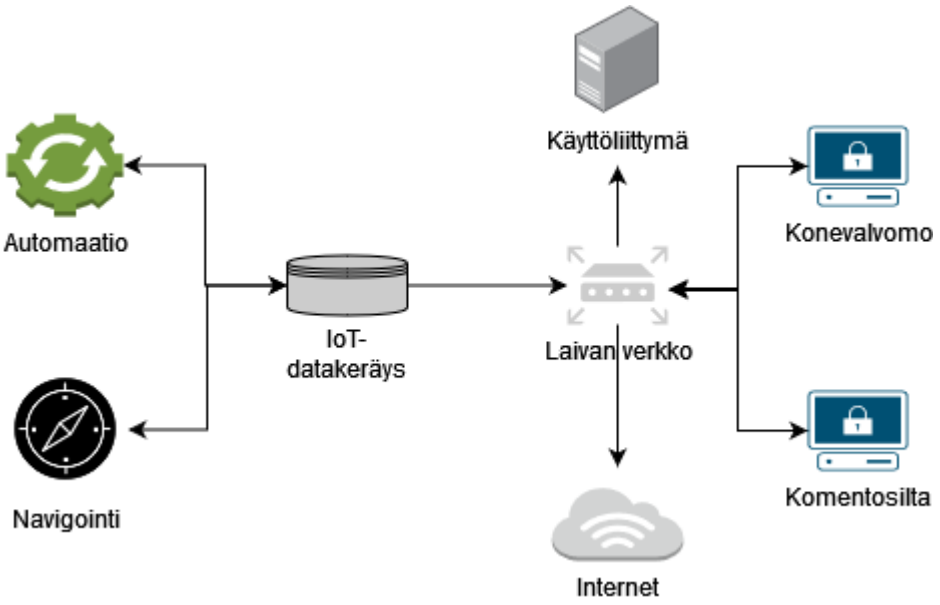
Järjestelmän ideana on joskus toimia tilaustyyppisenä palveluna, jonka käytöstä palvelun tilaaja maksaa. Kustannuksia tulee järjestelmän asennuksesta, käyttöönotosta ja tiedonhallintakuluista. Järjestelmä on tilausmaksu, joka kattaa syntyvät kulut.

Mittausdataa kerätään laivan laitteistosta IoT (Internet of things) -järjestelmän avulla, joka muuttaa datan luettavaan muotoon. Datankeräyskoneelta tiedot viedään käyttöliittymän serverille. Käyttöliittymä esittää datan pääosin graafisina kuvina, dynaamisina tavoitearvoina, sekä operoinnin kannalta relevantteina avainlukuina. Energianvalvontajärjestelmää käytetään laivan komentosillalta ja konevalvomosta.

3.1 Järjestelmän rakenne

Case järjestelmä sisältää kaksi teollisuustietokonetta datan keräystietokone ja käyttöliittymän tietokone. Tietokoneet ovat passiivijäähdytteisiä ja luotettavia teollisuuskäytössä. Lisäksi käytössä on pilvipalvelu, jonka avulla dataa voidaan

käsitellä myös laivan ulkopuolella. Alla olevasta kuvasta 2 nähdään rajapintapiirros järjestelmästä.



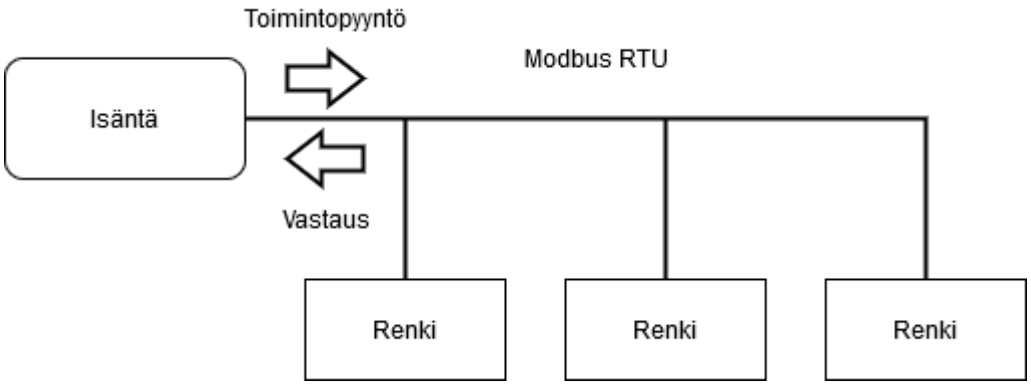
Kuva 3 case järjestelmä.

3.2 Laivan automaatio

Automaatiolla pyritään optimoimaan työprosessia tehokkaammaksi ja turvallisemmaksi korvaamalla ihmistekijä koneellisella vaihtoehdolla joko kokonaan tai osittain. Automaatiojärjestelmä voi koostua monesta eri laitteesta, kuten näyttöpaneeleista, sensoreista, hallintajärjestelmistä ja monesta muusta toimilaitteesta (Kyberturvallisuuskeskus 2021). Pääidea on kuitenkin se, että laitteet ja järjestelmät toimivat ohjelmoidusti tai itsenäisesti. Esimerkiksi kauppojen liukuovet toimivat sensoreilla ja liukuovikoneistolla automaation avulla (Kone 2022). Automaatiojärjestelmät auttavat yrityksiä ja helpottavat monia prosesseja eri teollisuuden aloilla. Lisäksi moniin eri automaatiojärjestelmiin halutaan päästä käsiksi etäältä esimerkiksi säätö tai valvonta tarkoituksien takia. Tämän takia kyberturvallisuus on tärkeää sillä, mikäli järjestelmä on liitettynä internettiin, on kyberrikollisilla mahdollisuus murtaa järjestelmä. Tämä asettaa murretun järjestelmän ja sen järjestelmät kyberuhalle alttiiksi. (Kyberturvallisuuskeskus 2020)

Laivan automaatiojärjestelmiin sisältyy esimerkiksi paloturvallisuusjärjestelmät kuten Hi-FOG, propulsio-, energia-, ja HVAC-järjestelmät. Lisäksi myös laivan turvallisuustoiminnot kuten esimerkiksi laivan varavirta-generaattorit toimivat automaatiolla, joiden avulla voidaan turvata laivan turvallinen operointi myös hätätilanteessa. Energianvalvontajärjestelmän kannalta oleelliset järjestelmät ovat HVAC-, propulsio, - energia-, navigointijärjestelmät. Automaation avulla energianvalvontajärjestelmässä voidaan seurata esimerkiksi laivan energiankulutusta ja reagoida lähes reaaliajassa. (Babicz, 2015)

Laivan automaatiojärjestelmät on kytketty case-järjestelmään Modbus RTU protokollan avulla. Modbus RTU on binäärinen isäntä – renki sarjaliikenneprotokolla, jonka avulla voidaan siirtää tietoa tai ohjata järjestelmiä. Modbus RTU protokollan toimintaperiaatetta on kuvattu alla olevassa kuvassa 4. Yksinkertaisuudessaan Isäntäpääte käskee renkipäätettä lähettämään dataa, jonka jälkeen renki toimittaa tiedon ja isäntä siirtää tiedon eteenpäin ohjelmoidusti.



Kuva 4 Modbus RTU protokollan toiminnan esimerkki. (William, L. & Mostia, Jr 2019 mukaillen.)

Modbus RTU ja NMEA protokollien avulla järjestelmään on helppoa lisätä uusia yhteyksiä, järjestelmiä ja sensoreita.

3.3 Käytönvalvonta

Laivan energiateknisiä toimintoja olisi vaikea seurata sekä optimoida, mikäli seurantaa tehtäisiin laite- tai sensorikohtaisesti. Monessa eri teollisuudessa, kuten prosessiteollisuudessa on käytössä monia eri valvontajärjestelmiä, yleisin niistä on SCADA (Supervisory control and data acquisition). Myös laivateollisuudessa on käytössä SCADA, jolla valvotaan automaatio-, ja energiajärjestelmiä. SCADA on järjestelmä, joka koostuu monesta alajärjestelmästä, jonka idea on toimia muun muassa valvontajärjestelmänä automaatiojärjestelmille, mutta voi myös toimia etäohjausjärjestelmänä valvontajärjestelmän lisäksi. Data kerätään automaatiojärjestelmistä antureiden ja muiden toimilaitteiden avulla, jonka jälkeen ne lähetetään esimerkiksi laivassa laivan konevalvomoon. Konevalvomossa voidaan datan avulla arvioida ja tehdä tietoisia päätöksiä laivan operoinnin suhteen. (Bailey & Wright, 2003) Data energianvalvontajärjestelmälle siirretään kenttäväylämoduulien avulla hyödyntämällä kenttäväyläprotokollia kuten Modbus RTU, ControlnNet ja DeviceNet. (Macaulay & Singer, 2011) Tämän opinnäytetyön aiherajauksen takia keskitytään vain Modbus RTU protokollaan. Case järjestelmä periaatteeltaan toimii vastaavanlaisesti kuin SCADA ilman ohjausmahdollisuutta. Laivan SCADA ja case järjestelmää voidaan käyttää komplementaarisesti yhdessä.

3.4 Käyttöliittymä

Tiedot laivan järjestelmistä kuten automaatio-, ja navigaatiojärjestelmistä kerätään datankeräysserverille, josta ne kootaan helposti luettavaksi laivan henkilökunnalle case järjestelmän käyttöliittymälle, joka muistuttaa nettisivua. Käyttöliittymästä voidaan nähdä reaaliajassa laivan järjestelmien datan, joka helpottaa laivan energiatehokasta käyttöä. Alla olevassa kuvassa 4 nähdään case järjestelmän dataa. Kuvassa nähdään dynaamiset lukemat joihin laivan operoijien tulisi pyrkiä, sekä prosenttimäärät paljonko kulutusta on enemmän tai vähemmän kuin normaalisti.

Kuva 5 case järjestelmän käyttöliittymä pääsivu.

Lisäksi laivan energiankäyttöä voidaan arvioida tietyn ajan jakson jälkeen järjestelmän historian avulla. Alla olevasta kuvasta 5 nähdään, että järjestelmästä voidaan valita tietty ajanjakso arvioitavaksi.

Kuva 6 Case järjestelmän historiafunktio.

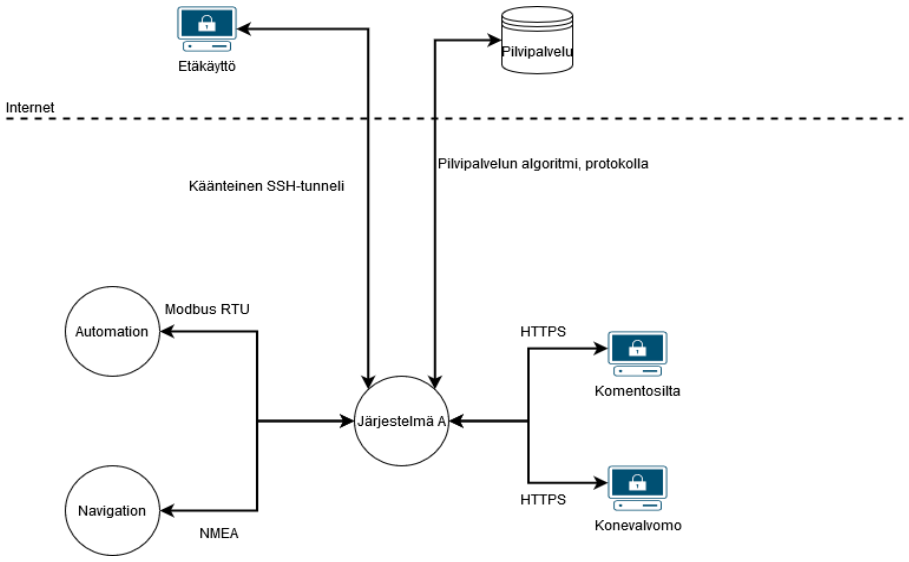
Järjestelmän toimintoa voi käyttää hyväksi esimerkiksi jonkin järjestelmän tehokkuuden arvioimiseen. Jos laivassa tehdään jokin energiatekninen ratkaisu, jonka pitäisi parantaa, esimerkiksi polttoaineen kulutusta, sen tehokkuutta ja taloudellista vaikutusta voitaisiin arvioida case järjestelmän avulla.

Käyttöliittymä muodostetaan kerätyistä tiedoista ohjelmalla, joka on luotu Linux serverille. Serverin käyttöjärjestelmä kuuluu Linux-perheeseen ja soveltuu tietoturvaltaan, laajennusmahdollisuuksiltaan sekä helppokäyttöisyydeltään serverikäyttöön.

3.5 Case järjestelmän kyberturvallisuus

Energianvalvontajärjestelmä voi koostua vain muutamista päätelaitteista, mutta dataa voidaan kerätä suuresta kokonaisuudesta monien eri toimilaitteiden avulla. Laajan järjestelmän kyberturvaa hankaloittaa se, että järjestelmät koostuvat monen eri laitevalmistajan laitteista, joka tarkoittaa sitä, että haavoittuvuuksia on voitu korjata vain osasta laitteista tai, että laitteiden tietoturvaa ei välttämättä päivitetä ollenkaan asentamisen jälkeen. Vaikka energianvalvontajärjestelmä on vain yksi osa laajaa laivan järjestelmää niin laaja järjestelmä luo suuren hyökkäyspinta-alan.

Aikaisemmin opinnäytetyössä on mainittu, että kyberturvallisuuden selvittäminen on helpointa aloittaa hyökkäyspinta-alan selvittämisellä. Ensin koostetaan rajapintapiirros järjestelmästä, johon piirretään järjestelmästä ulkonevat yhteydet ja se, miten yhteydet on suojattu. Alla olevasta kuvasta 7 nähdään, että järjestelmän A rajapintapiirros ei sisällä automaatiojärjestelmän sisäisiä laitteita, vain vastaanotettavat signaalit Modbus -protokollasta. Lisäksi rajapintapiirrokseen otetaan mukaan navigaatiojärjestelmän signaalit, sekä etäkäytön, -pilvipalvelun, -käyttöliittymän, -konevalvomon, - ja komentosillanpäätelaitteiden väylät. Rajapiirroksen jälkeen tarkastetaan yhteyksien suojaukset.



Kuva 7 Case järjestelmä rajapintapiirros.

Rajapintapiirroksessa keskimmäinen ympyrä on case järjestelmä, joka sisältää käyttöliittymäserverin ja IoT-koneen.

3.5.1 Käänteinen SSH-tunneli

Kun yhteys pitää olla mahdollisimman turvallinen etäjärjestelmään, käytetään käänteistä SSH (Secure Shell) -tunneliyhteyttä. Case järjestelmän tapauksessa käänteinen SSH-tunneliyhteys luodaan niin, että järjestelmästä luodaan SSH-tunneliyhteys etäjärjestelmään, jonka jälkeen etäjärjestelmältä tehdään SSH-tunneliyhteyden sisälle käänteinen SSH-tunneliyhteys. Käänteinen SSH-yhteys perustuu siihen, että case järjestelmän pääte odottaa SSH-yhteyden avauspyyntöä etäpäätteeltä, jolloin järjestelmä kääntää pyynnön itselleen ja avaa järjestelmien välille käänteisen SSH-tunneliyhteyden. (Mckay 2019)

3.5.2 Navigointi NMEA

Case järjestelmä kerää navigoinnin dataa NMEA (The national marine elctronics association) -protokollalla, jotta järjestelmän käyttäjät voivat nähdä laivan nopeuden, sijainnin, sekä liikennöintireitin. Navigoinnin dataa käytetään

muiden tietojen kanssa yhdessä, jotta voidaan laskea esimerkiksi laivan energiakulutusta suunnitellulla reitillä tai reaaliaikaisesti. Tätä tietoa voidaan käyttää energiatehokkaamman reitin tai operoinnin suunnitteluun ja toteuttamiseen.

Case järjestelmä on liitetty navigointijärjestelmään NMEA 2000 protokollalla, joka on sarjaliikenneväyläprotokolla. Häiriöiden varalta NMEA yhteydet case järjestelmään on suojattu galvaanisilla erottimilla. NMEA 2000 protokolla varmistaa datan oikean muodon, jotta eri valmistajien navigaatiolaitteet osaavat lukea dataa ja muodostaa esimerkiksi karttoja ja esittää nopeuden ja syvyyden. (Gakstatter, 2015) NMEA 2000 perustuu CANbus protokollaan, joka on laajalti käytössä meri, - ja autoteollisuudessa. CANbus viestiliikenne välitetään aina jokaiselle väylällä olevalle laitteelle, jotta voidaan yhdellä viestillä kertoa monelle laitteelle sama tieto, esimerkiksi navigoinnin datasta voidaan ilmoittaa nopeus tai sijainti monelle laitteelle samanaikaisesti. (Vanhala 2020)

Itsessään case järjestelmään liitetty NMEA protokolla ei täytä CIA-triadin turvallisuusmäärityksiä, vaan on väylään liitettyjen järjestelmien turvallisuusasetuksien varalla. (Tran et al. 2021). Kuitenkaan opinnäytetyön tarkoituksena ei ole arvioida case järjestelmän ulkopuolisten järjestelmien tai laitteiden kyberturvallisuutta. NMEA 2000 protokolla sisältää ylimääräisten viestien tarkistuksen, jonka perusteella jokainen moduuli tarkistaa viestit väylällä ja ilmoittaa virheistä. Mikäli virheitä ilmoitetaan tarpeeksi, viestin aiheuttaja poistetaan käytöstä automaattisesti. (Tran et al. 2021)

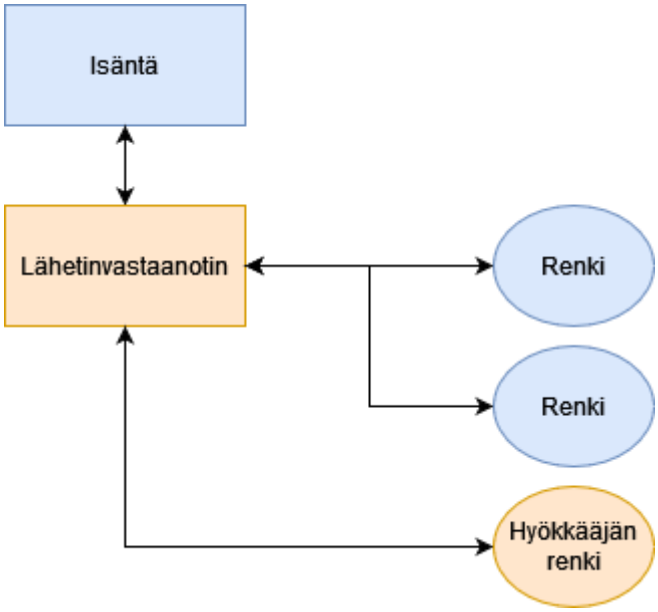
NMEA 2000 yhteys on altis palvelunestohyökkäykselle, sillä yhteyden kaistaleveys on pieni. Palvelunestohyökkäys voisi estää samassa väylässä toimivien laitteiden toiminnan. Lisäksi NMEA yhteydet on alttiita mies välissä -hyökkäykselle, jossa kahden moduulin väliin hyökkääjä tunkeutuu esittämällä olevansa väylään kuuluva moduuli. Hyökkääjä voisi moduulilla lähettää haitallista viestiä väylälle tai muuttaa, poistaa tai kuunnella viestiväylää. (Tran et al. 2021) Aikaisemmin opinnäytetyössä on mainittu NMEA 2000 protokollan tarkistusmetodi, mutta protokolla varmistaa vain virheelliset viestit, eikä tarkoituksen mukaiset.

3.5.3 HTTPS

Case järjestelmän HTTPS (Hypertext transfer protocol secure) -yhteydet on suojattu SSL (Secure sockets layer) -sertifikaatilla, mikä tarkoittaa, että tiedon siirtäminen on salattu palvelimelta ja palvelimelle. (pcmag 2022) Suojattu yhteys estää tietojen lukemista ja muokkaamista. Yhdistäminen tapahtuu päätekoneen pyynnöstä, jolloin esimerkiksi komentosillalta päätelaite lähettää sertifikaatti tunnisteen käyttöliittymäserverille, jonka jälkeen serveri avaa salatun yhteyden päätelaitteelle, mikäli sertifikaatin tunniste on oikein. Tätä tapahtumaa kutsutaan SSL-kättelyksi. Sertifikaatin tunnisteen lähettäminen tapahtuu operoijan käyttäjätunnusten avulla, jotka on ennalta asetettu sertifikaatin konfiguroinnin aikana. (SSL 2022)

3.5.4 Modbus RTU yhteydet

Modbus RTU -järjestelmät sisältävät kyberhyökkäyksen mahdollisuuden, vaikkakin hyvin epätodennäköisen. Protokollaan ei ole itsessään sisäänrakennettuja turvallisuusjärjestelmiä tai asetuksia. Järjestelmästä ei pystytä tunnistamaan ja varmistamaan erikseen renki -päätelaitteita, joka tarkoittaa sitä, että hyökkääjän on mahdollista lisätä oma laite rengiksi ja päästä sitä kautta järjestelmään sisälle. Lisäksi hyökkääjän on mahdollista asentaa lähetinvastaanotin, jonka avulla hyökkääjä voi lukea, keskeyttää tai muokata järjestelmän välisiä viestejä. Riippuen järjestelmästä se voi tarkoittaa hengenvaaraa. Alla olevasta kuvasta nähdään esimerkki, miten hyökkääjä voisi tunkeutua järjestelmään sisälle. (Jakaboczki & Adamko 2015)



Kuva 8 Hyökkäykselle altistunut järjestelmä. Jakaboczki & Adamko (2015) Mukaillen.

Case järjestelmä on liitetty automaatiojärjestelmiin Modbus RTU yhteyksillä. Tämä itsessään on turvattu yhteys siinä näkökulmassa, että fyysisten laitteiden asentaminen laivan Modbus RTU järjestelmään olisi hyvin haastavaa, sillä kaikki laivan operoinnin kannalta tärkeät järjestelmät ovat lukittujen ovien takana.

3.5.5 Käyttöliittymä

Case järjestelmän käyttöliittymä on asennettu Linux-serverille, joka on suoraan yhteydessä datankeräysserveriin, komentosillan ja konevalvomon päätelaitteisiin, sekä pilvipalveluympäristöön.

Käyttöliittymän serveri on suojattu palomuurilla ja sen lähtevät, sekä saapuvat yhteydet on suojattu tarpeiden mukaisesti, kuten aikaisemmin opinnäytetyössä on mainittu.

Linux-serverin voi suojata monella tavalla, suojaaminen tulisi aloittaa hyökkäyspinta-alan selvittämisellä ja sen pienentämisellä. Tällä tarkoitetaan

tapaa, jolla poistetaan järjestelmästä tarpeettomat reitit millä hyökkääjä voisi päästä järjestelmään sisälle, esimerkiksi turhat portit ja liitännät tulee poistaa käytöstä, sillä avoimien porttien avulla hyökkääjien on helppo tunkeutua järjestelmään sisälle. (LaCroix 2018)

3.6 CIA-triad

Järjestelmän kyberturvallisuutta arvioidessa voidaan käyttää hyödyksi aikaisemmin työssä mainittua CIA-triad mallia. Kappaleessa 2 käydään läpi CIA-triad määritelmät: luottamuksellisuus, eheys ja saatavuus.

Luottamuksellisuus toteutetaan case järjestelmässä käyttäjätunnuksien ja rajoitettujen käyttäjien avulla. Lisäksi järjestelmän päätelaitteille on pääsy vain rajoitetulla henkilökunnalla. Myös Case järjestelmän palvelun toimittajan hallussa on lista käyttäjistä sekä eri käyttäjien oikeuksista.

Järjestelmässä eheys toteutetaan varmistamalla asiakkaan osaaminen, kouluttamalla laivan henkilökunnalle järjestelmän käyttö. Lisäksi järjestelmässä on sisäänrakennettu tiedon varmuuskopiointi RAID-ominaisuudella, myös järjestelmän pilvipalvelua voidaan käyttää järjestelmän historian tarkasteluun. Pilvipalvelua voidaan myös käyttää järjestelmän eheyden ja toiminnan tarkistamiseen sekä varmistamiseen

Tiedon saatavuuden järjestelmä varmistaa edellä mainitun RAID asetuksen avulla. RAID-asetus tarkoittaa sitä, että järjestelmällä on useampi kovalevy joissa ”ylimääräiset” kovalevyt kopioivat jatkuvasti pääkovalevyn tiedot, jolloin tieto on varmuuskopioitu. Lisäksi toimeksiantajalla on käytössä toimintaohjeet kyberhyökkäyksen varalle sekä viestintäohje, joiden avulla varmistetaan järjestelmän palautuminen ennalleen mahdollisimman nopeasti. Toimintaohjeet on tehty opinnäytetyössä aikaisemmin mainittujen standardien mukaisesti, kuten ISO/IEC27001 kyberuhanriskihallinta järjestelmän mukaisesti.

Case järjestelmä kestää CIA-triad mallin ja on sen mukaisesti kyberturvallinen. Toimeksiantajalta löytyy standardit ja ohjeistukset kyberturvallisuuden

varmistamiseen sekä tarvittavat työkalut jotta tiedon luottamuksellisuus, eheys ja saatavuus on varmistettu. Laajemman kyberturvallisuuden selvittämiseksi CIA-triad mallia tulisi kokeilla jokaiseen case järjestelmän rajapintajärjestelmään.

4 Yhteenveto

Kyberturvallisuus on enemmän kuin teknistä toteuttamista ja vaatii monialaista ymmärrystä eri järjestelmistä. Täysin kyberturvallista järjestelmää on haastava toteuttaa missään järjestelmässä, eikä tässäkään tapauksessa energianvalvontajärjestelmä eroa siitä. Jokaiseen järjestelmään on mahdollista ulkopuolisen päästä sisälle, mutta tunkeutumisesta voidaan tehdä lähes mahdotonta.

Opinnäytetyössä case järjestelmä on kooltaan hyvin pieni kokonaisuus verrattuna laivan muihin järjestelmiin. Mielenkiintoinen pulma kyberturvallisuuden näkökulmasta on, että pienenkin järjestelmän kyberturvallisuus riippuu valtavan automaatiojärjestelmän kyberturvallisuudesta, sama idea toimii myös vastasuuntaisesti. Case järjestelmän yhteydet on suojattu tarvittavalla tavalla, jotta ainakaan niiden kautta ei hyökkääjällä ole pääsyä sisälle muihin järjestelmiin. Lisäksi lisäturvaa antaa käytössä olevat toimintaohjeet kyberhyökkäyksen sattuessa, jotta toiminta turvataan myös tulevaisuudessa. Kuitenkin case järjestelmä vaatii kyberturvallisuuden seuraamista ja tarvittaessa parantamista koko laivan ja järjestelmän eliniän ajan. Toimeksiantaja käyttää projekteissaan opinnäytetyössä mainittuja standardeja luvussa 2.4, joiden avulla kyberturvallisuuden hallinta on turvattu hallinnollisella tasolla, sekä projektikohtaisella tasolla.

Laivateollisuudessa on tullut vasta viimevuosina enemmän sääntöjä, miten kyberturvallisuus tulee ottaa huomioon, aiemmin sääntöjen sijasta on ollut vain ohjeistuksia. Kyberturvallisuuden säännöt tuovat alalle standardimaisen turvallisuuden, jotta jokaisen järjestelmän suoja on tarvittavalla tasolla. Kyberturvallisuudelle on tulevaisuudessa kasvava tarve, minkä takia merenkuluntoimijoiden tulee keskittyä siihen enemmän, sillä kun laitteet siirtyvät digitaalisemmiksi, se aiheuttaa suurempaa uhkaa kyberturvallisuudelle.

5 Pohdinta

Opinnäytetyönä aihe oli erinomainen laajentamaan allekirjoittaneen osaamista ja lisäämään kiinnostusta alalle. Kyberturvallisuus on erittäin laaja käsite ja jonka ammattilaiset eivät välttämättä valmistu tietystä koulutusohjelmasta, vaan ammattitaito karttuu työn ohella ja vaatii omanlaista harrastemaista kiinnostusta alaan. Lisäksi kyberturvallisuuden ymmärtämiseen ei riitä pelkästään taito tietotekniikasta vaan pitää osata ajatella myös ihmistekijöitä, jotka kuitenkin ovat suurin uhkatekijä missä järjestelmässä vain. Tämän takia aihe oli erittäin haasteellinen ja vaati laajaa opiskelua ja tutkimista.

Aiheelle riittää teoria- ja tutkimuspohjaa, joten teorian tutkiminen ei ollut haasteellista, ennemminkin teoriapohjan rajaaminen relevantteihin tietoihin oli haasteellista. Energiajärjestelmän teorian tutkiminen oli tuttua koulun kurssien taustalta. Teorian tutkimista myös täydensi se, että case järjestelmää pääsi itse asentamaan toimeksiantajan tiloihin. Myös toimeksiantajan puolesta ammattitaitoa ja opastuksen intoa löytyi, joiden avulla oli helpompaa löytää oikea suunta ja rajaus opinnäytetyölle.

Opinnäytetyön tuloksina saatiin laivan case järjestelmän kyberturvallisuuden kattavuus. Järjestelmää vertailtiin myös CIA-triad mallin vaatimuksiin, jonka se läpäisi. Lisäksi työ myös lisäsi allekirjoittaneen kykyä arvioida tulevaisuudessa kyberturvallisuutta helpommin. Jatkotutkimuksena, olisi syytä tutkia myös rajapintajärjestelmien kyberturvallisuutta, sillä jokainen case järjestelmään liitetty väylä, laite tai ihminen on mahdollinen alttius. Työ auttoi kehittämään järkevän tavan lähestyä järjestelmää kyberselvityksen näkökulmasta.

Case järjestelmää voidaan asentaa uusiin ja vanhoihin laivoihin, joka tarkoittaa sitä, että kyberturvallisuuden kattavuus vaihtelee laivojen järjestelmien välillä. Opinnäytetyössä on mainittu, että laivan elinkaari on noin 20–30-vuotta, mutta se, että päivitetäänkö laivan digitaalisten järjestelmien alttiuksia niiden ilmaantuessa vielä 15 tai 20 vuoden jälkeen, on mielenkiintoinen kysymys.

Lisäpohdintaa työn jälkeen aiheutti se, ettei Suomessa ole lakipykäliä tai valvovaa viranomaista kyberturvallisuuden tasolle. Suomessa tietoturvaa valvoo tietosuojavaltuutettu, mutta se valvoo vain henkilötietojen käsittelyjä, ei niinkään esimerkiksi automaatiojärjestelmien kyberturvallisuutta. (Tietosuoja.fi, 2020). Esimerkiksi laajalti käytössä oleva Modbus -protokollan avulla on hyökätty järjestelmiin sisälle ja aiheutettu vakavia henkilövahinkoja, sekä kuolemantapauksia. (Jakaboczki & Adamko, 2015). Pelkästään Jakaboczki & Adamko:n tutkimuksen perusteella voidaan jo päätellä, että kriittisten laitteiden suojaaminen meriteollisuudessa on aiheellista.

Lähteet

Babicz, J. 2015. *Encyclopedia of ship technology second edition.* Saatavilla www-osoitteesta: < https://www.wartsila.com/docs/default-source/marine-documents/encyclopedia/wartsila-o-marine-encyclopedia.pdf > Viitattu 23.1.2022

Bailey, D, & Wright, E 2003, Practical SCADA for Industry, Elsevier Science & Technology, Oxford. Saatavilla: ProQuest Ebook Central. Viitattu 13.1.2022

Bosworth, S, Kabay, ME, & Whyne, E (eds) 2014, Computer Security Handbook, Set, John Wiley & Sons, Incorporated, Somerset. Available from: ProQuest Ebook Central. Viitattu 1.11.2021

Boyes, H & Isbell, R 2017. *Code of practice cyber security for ships.* Institution of Engineering and Technology, London, United Kingdom. Viitattu 12.10.2021

DNV, 2020. *The three-pillar approach to cyber security: Data and information protection.* Saatavilla www-osoitteesta: < https://www.dnv.com/article/the-three-pillar-approach-to-cyber-security-data-and-information-protection-165683 > Viitattu 11.11.2021.

DNV.com, 2021. *Recommended practice: Cyber security resilience management.* Saatavilla www-osoitteesta: < https://www.dnv.com/maritime/dnvgl-rp-0496-recommended-practice-cyber-security-download.html > Viitattu 10.1.2022.

DNV.com, 2022. *Maritime cyber security.* Saatavilla www-osoitteesta: < https://www.dnv.com/maritime/insights/topics/maritime-cyber-security/index.html > Viitattu 12.1.2022

DNVGL-OS-D203, 2017. *Integrated software dependent systems.* Saatavilla www-osoitteesta:< https://rules.dnv.com/docs/pdf/DNV/os/2017-07/DNVGL-OS-D203.pdf > Viitattu 10.1.2022

F-secure.com, 2022. A. *Mitä on tietojen kalastelu?* Saatavilla www-osoitteesta: < https://www.f-secure.com/fi/home/articles/what-is-phishing > Viitattu 28.1.2022

F-secure.com, 2022. B. *Ransomware on haittaojelmista pahimpia.* Saatavilla www-osoitteesta: < https://www.f-secure.com/fi/home/articles/what-is-a-ransomware-attack > Viitattu 28.1.2022

IEC/TS 62443-1-1[1),2)], 2013. *Industrial communication networks – Network and system security – part 1-1: Terminology, concepts and models.* Viitattu 12.1.2022

International maritime organization, 2021. *Brief History of IMO.* Saatavilla www-osoitteesta: < https://www.imo.org/en/About/HistoryOfIMO/Pages/Default.aspx > Viitattu 14.10.2021

ISM & ISPS. Saatavilla www- osoitteesta: < https://www.traficom.fi/sites/default/files/media/file/1.%20Kyberturvallisuus%20ISM%20%26%20ISPS_JW.pdf > Viitattu: 19.10.2021

ISO/IEC 27000:2016. *Information technology -- Security techniques -- Information security management systems -- Overview and vocabular.* Viitattu 25.10.2021.

Jakaboczki, G. 2015. *Vulnerabilities of modbus RTU protocol – A case study.* Saatavilla www-osoitteesta: < https://imt.uoradea.ro/auo.fmte/files-2015-v1/Gabor%20JAKABOCZKI%20-%20VULNERABILITIES%20OF%20MODBUS%20RTU%20PROTOCOL%20-%20A%20CASE%20STUDY.pdf > Viitattu 24.1.2022

Jason, A. 2014. *The Basics of Information Security (Second edition) -What is information security?* Viitattu 12.1.2022

Kone.fi. 2022. *Joustavia oviratkaisuja erilaisiin kiinteistöihin.* Saatavilla www -osoitteesta: < https://www.kone.fi/Images/Automaattiliukuovet_tcm36-42980.pdf > Viitattu 13.1.2022

Kyberturvallisuuskeskus.f. 2020. *Suojaamattomia automaatiojärjestelmiä suomalaisissa verkoissa 2020.* Saatavilla www -osoitteesta: < https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Automaatiolaitekartoitus_2020.pdf > Viitattu 13.1.2022

Kyberturvallisuuskeskus.fi. 2021. *Noin 1000 automaatiolaitetta on yhä suojaamatta suomalaisissa verkoissa.* Saatavilla www -osoitteesta: < https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/noin-1000-automaatiolaitetta-yha-suojaamatta-suomalaisissa-verkoissa?toggle=Mik%C3%A4%20on%20automaatiolaite%20tai%20-j%C3%A4rjestelm%C3%A4%3F >

L. Liu, O. De Vel, Q. Han, J. Zhang and Y. Xiang, "Detecting and Preventing Cyber Insider Threats: A Survey," in IEEE Communications Surveys & Tutorials, vol. 20, no. 2, pp. 1397-1417, Secondquarter 2018, doi: 10.1109/COMST.2018.2800740.

LaCroix, J 2018, Mastering Ubuntu Server: Master the Art of Deploying, Configuring, Managing, and Troubleshooting Ubuntu Server 18. 04, 2nd Edition, Packt Publishing, Limited, Birmingham. Available from: ProQuest Ebook Central. Viitattu 15.11.2021.

Lehto, M. 2021. *Digitaalisen kybermaailman ilmiöitä ja määrittelyjä.* Jyväskylän yliopisto. Viitattu 12.10.2021

McAfee.com, 2022. *How cybersecurity policies and procedures protect against cyberattacks*. Saatavilla www-osoitteesta: < https://www.mcafee.com/enterprise/en-us/security-awareness/cybersecurity/cybersecurity-policies.html > Viitattu 28.1.2022

Mckay, D. 2019. *What is reverse SSH-tunneling? (and how to use it).* Saatavilla www-osoitteesta: < https://www.howtogeek.com/428413/what-is-reverse-ssh-tunneling-and-how-to-use-it/ > Viitattu 26.01.2022

Microsoft, 2009. *The STRID Threat Model.* Saatavilla www-osoitteesta: < https://docs.microsoft.com/en-us/previous-versions/commerce-server/ee823878(v=cs.20)?redirectedfrom=MSDN > Viitattu 29.11.2021

pcmag.fi. 2022. *HTTPS.* Saatavilla www-osoitteesta: < https://www.pcmag.com/encyclopedia/term/https > Viitattu 28.1.2022.

Sargun, S. 2021. *A guide to scrubber system on ship.* Saatavilla www-osoitteesta: < https://www.marineinsight.com/tech/scrubber-system-on-ship/ > Viitattu 12.1.2022

SFS.fi, 2021. *Mitä standardi tarkoittaa?* Saatavilla www-osoitteesta: < https://sfs.fi/standardeista/mika-on-standardi/ > Viitattu 29.11.2021

Software engineering institute, 2012. *CyberSecurity Watch Survey, How bad is the insider threat?* Saatavilla www-osoitteesta: < https://resources.sei.cmu.edu/asset_files/Presentation/2013_017_101_57766.pdf > Viitattu 10.11.2021

SSL.com, 2022. *What is HTTPS?* Saatavilla www-osoitteesta: < https://www.ssl.com/faqs/what-is-https/ > Viitattu 28.1.2022

Sähkötekniikan ja energiatehokkuuden edistämiskeskus STEK ry. 2020. *Kyberturvallisuussanasto.* Saatavilla www- osoitteesta:< https://stek.fi/perustietoa-sahkosta/termit/ > Viitattu: 11.10.2021

Tietosuoja.fi, 2020. *Tietosuojavaltuutetun toimiston toimintakertomus 2020.* Saatavilla www-osoitteesta: < https://tietosuoja.fi/documents/6927448/92481282/Tietosuojavaltuutetun+toimisto+toimintakertomus+2020.pdf > Viitattu: 31.1.2022

Traficom Liikenne- ja viestintävirasto, 2019. *Liikenne- ja viestintävirasto Traficom aloittaa 1.1.2019.* Saatavilla www- osoitteesta: < https://arkisto.trafi.fi/uutisarkisto/6673/liikenne-_ja_viestintavirasto_traficom_aloittaa_1_1_2019 > Viitattu 19.10.2021

Traficom Liikenne- ja viestintävirasto, 2020. *Kyberturvallisuus.* Viitattu 19.10.2021

Traficom Liikenne- ja viestintävirasto, 2021. *CERT.* Saatavilla www- osoitteesta: < https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/cert > Viitattu 19.10.2021

Tran, K.; Keene, S.; Fretheim, E.; Tsikerdekis, M. *Marine Network Protocols and Security Risks*. *J. Cybersecur. Priv.* **2021**, *1*, 239-251. Saatavilla www-osoitteesta: < https://doi.org/10.3390/jcp1020013 > Viitattu 27.11.2022

Tuulaniemi, V. 2020. *Katsaus merenkulun kyberuhkiin.* Traficom kyberturvallisuuskeskus.Viitattu 14.10.2021

Vanhala, M. 2020. *NMEA 2000 verkon kytkentä.* Saatavilla www-osoitteesta: < http://www.ruorimies.fi/nmea-2000-verkon-kytkenta/ > Viitattu 27.11.2022

Ylonen, T. 1996. *SSH Protocol – Secure Remote Login And File Transfer.* Saatavilla www-osoitteesta: < https://www.ssh.com/academy/ssh/protocol#how-does-the-ssh-protocol-work > Viitattu 15.11.2021

Huoltovarmuuskeskus.fi, 2021. *Merenkulun kybertuvallisuus – varustamojen parhaat käytännöt.* Saatavilla www-osoitteesta:< https://www.huoltovarmuuskeskus.fi/files/dd6e8c7f90cd8163a1e18df1aa109a6394ee608b/kyberturvallisuus-varustamojen-parhaat-kaytannot.pdf > Viitattu 7.1.2021.

William, L & Mostia, Jr. 2019. *Introduction to Modbus*. Saatavilla www-osoitteesta: < https://www.controlglobal.com/articles/2019/introduction-to-modbus/ > Viitattu 26.1.2022

Jakaboczki, G. 2015. *Vulnerabilities of modbus RTU protocol – A case study.* Saatavilla www-osoitteesta: < https://imt.uoradea.ro/auo.fmte/files-2015-v1/Gabor%20JAKABOCZKI%20-%20VULNERABILITIES%20OF%20MODBUS%20RTU%20PROTOCOL%20-%20A%20CASE%20STUDY.pdf > Viitattu 24.1.2022