Tommi Lipsanen

SCADA-JÄRJESTELMIEN KYBERTURVALLISUUDEN ERITYISPIIRTEET JA PARANTAMINEN

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2019

TIIVISTELMÄ

Lipsanen, Tommi
Kyberturvallisuus SCADA-järjestelmissä
Jyväskylä: Jyväskylän yliopisto, 2018, 32 s.
Tietojärjestelmätiede, kandidaatin tutkielma
Ohjaaja(t): Takala, Arttu

Koko yhteiskunnan toiminta voi vaarautua kriittiseen infrastruktuuriin kohdistuvan kyberhyökkäyksen seurauksena. Ukrainassa tapahtui kyberhyökkäys SCADA-järjestelmään, jonka seurauksena sähköt katkesivat yli 200 000 ihmiseltä 1-6 tunnin ajaksi. Tämä kyseinen hyökkäys kohdistui SCADA-järjestelmään. SCADA-järjestelmät ovat yhdenlaisia teollisia valvonta- ja ohjausjärjestelmiä. Niitä käytetään muun muassa ohjaamassa ja valvomassa sähkön- ja vedenjakelun oikeanlaista toimintaa. Ne eroavat osittain käyttötarkoitukselta ja toiminnaltaan tavanomaisesta informaatioteknologiasta. SCADA-järjestelmään kohdistuvasta kyberhyökkäyksestä voi seurata merkityksellistä vahinkoa ihmisten terveydelle ja turvallisuudelle sekä paljon vahinkoa ympäristölle, joten kyberturvallisuuden tutkiminen tässä kontekstissa on tärkeää. Tilastot osoittavat, että SCADA-järjestelmiin kohdistuvien kyberhyökkäysten määrä on kasvanut vuosien saatossa. Tässä kirjallisuuskatsauksena tehdyssä tutkimuksessa perehdytään SCADA-järjestelmien kyberturvallisuuteen; sen erityispiirteisiin ja -vaatimuksiin tavanomaiseen informaatioteknologiaan verrattuna, järjestelmiin kohdistuviin kyberhyökkäyksiin sekä kyberturvallisuuden mahdolliseen parantamiseen. Tutkimuksessa havaittiin, että SCADA-järjestelmissä on alettu käyttämään osittain samoja teknologioita, kuin tavanomaisessa informaatioteknologiassa. Tämä altistaa SCADA-järjestelmät uudenlaisille kyberuhkille ja -hyökkäyksille. Lisäksi havaittiin, että kyberturvallisuuden parantamiseksi on monia käytäntöjä ja menetelmiä, joista keskeiseksi nousi esille erilaiset simulaatio- ja mallintamistekniikat. Näitä menetelmiä käytettäessä ja kehitettäessä täytyy ottaa huomioon SCADA-järjestelmien toiminnan erityisvaatimukset, joita ovat tosiaikaisuus, rajalliset laskentaresurssit sekä toiminnan jatkuvuus- ja turvallisuusvaatimukset.

Asiasanat: SCADA-järjestelmä, kyberturvallisuus, kyberhyökkäys, kriittinen infrastruktuuri

ABSTRACT

Lipsanen Tommi
Name of the publication
Jyväskylä: University of Jyväskylä, 2018, 32 pp.
Information Systems, Bachelor's Thesis
Supervisor(s): Takala, Arttu

The functioning of whole society can be endangered by a cyberattack on critical infrastructure. In Ukraine there was a cyberattack, which resulted blackout for 1-6 hours to over 200,000 people. This attack targeted SCADA-system. SCADA-systems are one type of industrial control system and they are used, among other things, to control and monitor the intrinsic performance of electricity and water supply. They differ in part from the purpose and function of traditional information technology. The cyberattack targeted to SCADA-system can have significant damage to human health and safety and deal great damage to the environment, so it is important to examine cyber-security in this context. Statistics show that the number of cyberattacks targeted to SCADA-systems has increased over the years. This literature review explores the cybersecurity of SCADA-systems; its special features and requirements compared to traditional information technology, cyberattacks on systems, and potential improvements in cybersecurity of SCADA-systems. It was noticed during the examination that SCADA-systems have started to use the same technologies in part as in traditional information technology. This exposes SCADA-systems to new kinds of cyber threats and attacks. In addition, it was found that there are many practices and methods for improving cybersecurity. During the examination it was noticed that pivotal methods for improving cyber security of SCADA-systems are simulation and modeling techniques. When using and developing these methods, it must be considered that there are specific requirements in SCADA-systems functioning, such as the real-time operating, the limited computing resources, and the continuity and safety requirements for functioning.

Keywords: SCADA-system, cyber security, cyberattack, critical infrastructure

KUVIOT

SISÄLLYS

1 Johdanto

SCADA-järjestelmät (engl. Supervisory Control and Data Acquisition) ovat yhdenlaisia teollisia valvonta- ja ohjausjärjestelmiä, joita käytetään muun muassa ohjaamassa ja valvomassa sähkön- ja vedenjakelun oikeanlaista toimintaa. SCADA-järjestelmiin kohdistuneet kyberhyökkäykset ovat realisoituneet viime vuosikymmenten aikana. Kyberhyökkäys on tietoverkkojen kautta tapahtuva hyökkäys, jolla voidaan tuottaa haittaa, vahinkoa tai tuhoa sekä fyysiseen, että digitaaliseen maailmaan (Limnell, Majewski & Salminen, 2014). SCADA-järjestelmät ovat useissa valtioissa osana valtion kriittistä infrastruktuuria, jolla tarkoitetaan yhteiskunnan ”alla” olevaa rakennetta, joka mahdollistaa arkipäivän sujuvuuden ja asioiden etenemisen totutusti. Kriittinen infrastruktuuri sisältää niin fyysisiä laitoksia ja rakenteita kuin sähköisiä toimintoja ja palveluja. Näihin kuuluvat muun muassa energian siirto ja jakelu, kuljetuslogistiikka, vesihuolto ja muu yhdyskuntatekniikka, raha- ja finanssijärjestelmä sekä sähköiset viestintäjärjestelmät (Limnell ym., 2014).

Monia näistä toiminnoista ja palveluista ohjaa ja valvoo SCADA-järjestelmät, joten niihin kohdistuvilla kyberhyökkäyksillä voi olla vakavat seuraukset. Tämän osoitti Ukrainassa vuonna 2015 SCADA-järjestelmään kohdistettu kyberhyökkäys, jonka seurauksena 30 sähköasemaa kytkettiin pois päältä, ja noin 230 000 ihmistä jäi ilman sähköä 1-6 tunnin ajaksi (Robert M. Lee, Michael J. Assante & Tim Conway, 2016). SCADA-järjestelmät ovat viime vuosikymmenien saatossa ottaneet käyttöön yleisiä standardisoituja laitteita, ohjelmistoja ja protokollia. Voidaan sanoa, että SCADA-järjestelmät ovat lähentyneet paljon tavanomaisen informaatioteknologian kanssa. Niihin on alkanut kohdistumaan osittain samoja kyberuhkia kuin tavanomaiseen tietotekniikkaan, joka on herättänyt paljon keskustelua SCADA-järjestelmien kyberturvallisuudesta (Hentea, 2008).

SCADA-järjestelmät kuitenkin poikkeavat toiminnaltaan ja käyttötarkoitukseltaan tavanomaisesta informaatioteknologiasta, ja niihin kohdistuvilla kyberhyökkäyksillä voi olla vakavat seuraukset, kuten esimerkiksi edellä mainittu Ukrainan tapahtuma osoitti. SCADA-järjestelmien hyvä kyberturvallisuus sekä

niiden toiminnan turvaaminen on siis hyvin merkittävää koko yhteiskunnan toimivuuden kannalta.

Aikaisempaa tutkimusta aiheesta ei olla vuosien saatossa kovinkaan paljon tehty. Aiemmat tutkimukset ja tilastot kuitenkin osoittavat, että SCADA-järjestelmiin kohdistuvat kyberuhkat ja -hyökkäykset ovat kasvaneet paljon viime vuosina, joten aiheen tutkiminen on hyvin ajankohtaista ja tärkeää. Aiemmissa tutkimuksissa myös korostetaan, että SCADA-järjestelmien kyberturvallisuuden parantamiseen olisi syytä kiinnittää enemmän huomiota ja lisätä sen tutkimusta.

Tässä tutkielmassa perehdytään SCADA-järjestelmien kyberturvallisuuteen ja sen mahdolliseen parantamiseen. Tutkielman tavoitteena on selvittää vastauksia tutkimuskysymyksiin; miten SCADA-järjestelmän kyberturvallisuus eroaa tavanomaisen informaatioteknologian kyberturvallisuudesta, millaisilla toimilla SCADA-järjestelmään voidaan tehdä onnistunut kyberhyökkäys sekä miten SCADA-järjestelmien kyberturvallisuutta voitaisiin mahdollisesti parantaa?

Tämä tutkielma suoritettiin kirjallisuuskatsauksena. Tiedonhakua tutkielmaani suoritin IEEE XPLORE:lla, Google Scholarilla ja JYKDOK-Finnalla. Hakusanoina on toiminut: ”SCADA”, ”system”, ”cyber”, ”attacks” ja ”security” sekä näiden sanojen yhdistelmiä. Lähdekirjallisuuden merkittävyyttä tutkin suomalaisen tiedeyhteisön laatiman julkaisukanavien laatuluokitus-julkaisufoorumin sivuilta.

Tutkimuksen tuloksena lähdekirjallisuuden pohjalta nousi esille, että yhtenä kyberturvallisuuteen liittyvänä merkittävänä eroavaisuutena tavanomaiseen informaatioteknologiaan verrattuna on, että kyberhyökkäys SCADA-järjestelmään voi olla vaikutuksen kohteeltaan erilainen. Ne voivat vaarantaa isonkin ihmisjoukon terveyden ja turvallisuuden sekä olla vakavana uhkana ympäristölle, kun taas tavanomaiseen informaatioteknologiaan kohdistuvalla hyökkäyksellä usein vaikutetaan tietoon tai tiedon käyttäjään. Osaltaan tämän ansiosta SCADA-järjestelmiin kohdistuvat hyökkäykset ovat yleensä luonteeltaan poliittisia (Dell, 2015).

Kyberturvallisuuteen liittyen toisena merkittävänä erona tavanomaiseen informaatioteknologiaan verrattuna lähdekirjallisuuden avulla nousi esille, että SCADA-järjestelmillä on tiukempia rajoituksia luotettavuuden, latenssin ja toimintakelpoisuusajan (uptime) suhteen. Nämä erityispiirteet voivat estää tietyt tavanomaiset kyberturvallisuustoimenpiteet SCADA-järjestelmissä ja ne tulee ottaa huomioon SCADA-järjestelmien kyberturvallisuutta käsiteltäessä.

Kyberhyökkäyksistä havaittiin, että onnistuneen hyökkäyksen SCADA-järjestelmään voi tehdä monella erilaisella toimella. Hyökkäyksen voi toteuttaa esimerkiksi estämällä tiedon liikkumista järjestelmän verkoissa tai muuttamalla hälytyskynnyksiä. Tässä tutkielmassa ei kiinnitetty kovin paljon huomiota hyökkäyksien tekniseen taustaan.

Kyberturvallisuuden mahdollisesta parantamisesta nousi kirjallisuuskatsauksen avulla esille, että erilaisten simulaatio- ja mallintamistekniikoiden kehittämisellä ja käyttöönotolla voidaan parantaa SCADA-

järjestelmien kyberturvallisuutta. Merkittävinä tekijöinä kyberturvallisuuden parantamiselle on myös tietoisuus ja yhteistyö. Kyberturvallisuustietoisuus on tärkeä vastatoimenpide ja jokainen organisaatiossa työskentelevä tulisi sisällyttää kyberturvallisuustietoisuusohjelmiin, riippumatta siitä, onko tietokoneen käyttäjä vai ei (Edwards, 2014).

Tutkielmassa esitetään aluksi SCADA-järjestelmän yleisrakennetta, protokollia, toimintaa sekä SCADA-järjestelmien historiaa ja kehittymistä. Kolmannessa luvussa esitetään aiheen kannalta olennaisia käsitteitä kyberturvallisuuteen liittyen. Tämän jälkeen siirrytään tarkastelemaan SCADA-järjestelmien kyberturvallisuutta; tarkastellaan SCADA-järjestelmien kyberturvallisuuden eroja tavanomaisen informaatioteknologian kyberturvallisuuteen. Luvussa tuon myös esille teoriaa kyberhyökkäyksistä SCADA-järjestelmiin, josta seuraa luku SCADA-järjestelmien kyberturvallisuuden parantamisesta. Tuon esille kyberturvallisuuden käytäntöjä ja -metodeja, joita SCADA-ympäristöissä hyödyntämällä voisi mahdollisesti parantaa SCADA-järjestelmien kyberturvallisuutta. Tutkielma loppuu yhteenvetoon, jossa esitellään tutkielman johtopäätöksiä ja näkemyksiä jatkotutkimusaiheista.

2 SCADA-JÄRJESTELMÄN YLEISRAKENNE

Tässä osiossa määrittelen SCADA-järjestelmän käsitettä. Otan myös käsittelyyn SCADA-järjestelmien yleistä hierarkkista rakennetta ja sen toiminnan mahdollistavia komponentteja sekä protokollia. Tämän lisäksi otan esille kyseisten järjestelmien kehittymisen historian saatossa.

2.1 SCADA-järjestelmän määritelmä ja käyttötarkoitus

SCADA muodostuu englanninkielisistä sanoista Supervisory control and data acquisition. Ala-Tala ym. (2010) suomentaa SCADA-järjestelmän olevan SCADA-käytönvalvontajärjestelmä, mutta virallisesti määriteltyä suomennosta tai lyhennettä SCADA-järjestelmästä en tutkielmaan löytänyt, joten tässä tutkielmassa käytetään termistä lyhennettä SCADA-järjestelmä.

Määrittelen SCADA-järjestelmän kahta lähdettä mukaillen. IEEE:n standardijulkaisu määrittelee SCADA-järjestelmän seuraavanlaisesti: "Järjestelmä, joka käyttää koodattuja signaaleja viestintäkanavien kautta etäpääte-laitteiden ohjaamiseksi. Valvontajärjestelmä voidaan yhdistää tiedonhankintajärjestelmään lisäämällä koodattujen signaalien käyttäminen kommunikointikanavien kautta tiedon hankkimiseksi etäpääte-laitteen tilasta monitoriin tai tallennustoimintoihin" (*IEEE std C37.1-1994*1994). Stoufferin, Falcon ja Kent (2007) määrittelevät SCADA-järjestelmien olevan erittäin hajautettuja järjestelmiä, joita käytetään hallitsemaan maantieteellisesti jopa tuhansia neliökilometrejä hajallaan olevia resursseja, joissa keskitetty tiedonhankinta ja ohjaus ovat kriittisiä järjestelmän toiminnalle (Stouffer, Falco & Kent, 2007). Otan tämän osan määrittelyyn mukaan, koska siinä tulee hyvin esille, kuinka SCADA-järjestelmät voivat olla kriittisenä osana todella isojen – pinta-alaltaan jopa tuhansien neliökilometrien alueella toimivien järjestelmäkokonaisuuksien toiminnassa.

SCADA-järjestelmällä on paljon läheisiä termejä. Teollisuuden automaatiojärjestelmä (Industrial control system) on yleinen termi, joka käsittää useita erilaisia ohjaus- ja automaatiojärjestelmiä, mukaan lukien SCADA-järjestelmiä,

hajautettuja ohjausjärjestelmiä (DCS, Distributed control system) ja muita ohjausjärjestelmäkokoonpanoja, kuten ohjelmoitavia logiikkaohjaimia (PLC, Programmable Logic Control). Ohjelmoitavia logiikkaohjaimia käytetään SCADA-järjestelmien komponentteina (Stouffer ym., 2007). Hajautetut ohjausjärjestelmät ovat ominaisuuksiltaan lähimpänä SCADA-järjestelmiä, joten on hyvä käydä läpi termien erottelua.

Yksi tärkeimmistä eroista hajautetun automaatiojärjestelmän ja SCADA-järjestelmän välillä on se, että hajautetut ohjausjärjestelmät (DCS) sijaitsevat tavallisesti enemmän rajoittuneella alueella verrattuna maantieteellisesti levittäytyneeseen SCADA-järjestelmään (Stouffer ym., 2007). Teollinen automaatiojärjestelmä on siis yläkäsite erilaisille automaatio-, ja valvontajärjestelmille, ja tässä tutkielmassa keskitytään yhdenlaiseen teolliseen automaatiojärjestelmätyyppiin eli SCADA-järjestelmiin ja niiden kyberturvallisuuteen.

Tyypillisiä hajautettuja toimintoja, joissa käytetään SCADA-järjestelmiä, ovat infrastruktuurijärjestelmät, kuten energianjakeluverkot, kaasulinjat, vesijärjestelmät, jätevesijärjestelmät sekä muut vastaavat yleiset verkot ja teollisuusverkot (Ala-Tala ym., 2010).

2.2 SCADA-järjestelmän hierarkkinen rakenne, komponentit ja protokollat

SCADA-järjestelmät koostuvat sekä laitteistosta, että ohjelmistosta (Stouffer ym., 2007), ja niiden toimintaa tarkasteltaessa sen rakenne jaetaan usein eri hierarkkisiin tasoihin. SCADA-järjestelmän hierarkkista rakennetta sekä sen komponentteja voidaan tarkastella hyvin yksinkertaistetun kuvion avulla (kuvio 1).

Nazir, S. Patel ja D. Patel (2017) kertovat SCADA-järjestelmän toiminnasta taso kerrallaan. Alimmalla tasolla ovat kenttälaitteet, jotka tarjoavat rajapinnan fyysisen prosessin ohjaamiselle ja valvomiselle. Nämä laitteet voivat keskittyä pelkkään prosessin ohjaamiseen tai valvomiseen, tai molempiin yhtä aikaa (Nazir ym., 2017). Kenttälaitteet ovat yleisesti toimilaitteita, kuten esimerkiksi venttiiliä käyttäviä laitteita tai sensoreja, jotka mittaavat jotain asiaa.

Seuraavalla, korkeammalla tasolla ovat etäasemat (RTU) ja ohjelmoitavat logiikkaohjalimet (PLC). Logiikkaohjaimet ovat tietokonejärjestelmiä, jotka ohjaavat kenttälaitteistoa. Ne toimivat ohjaavina isäntälaitteina kenttälaitteille, ja ne siirtävät komentoja sekä vastauksia viestintäverkon kautta kenttälaitteille ja SCADA-palvelimille (Nazir ym., 2017).

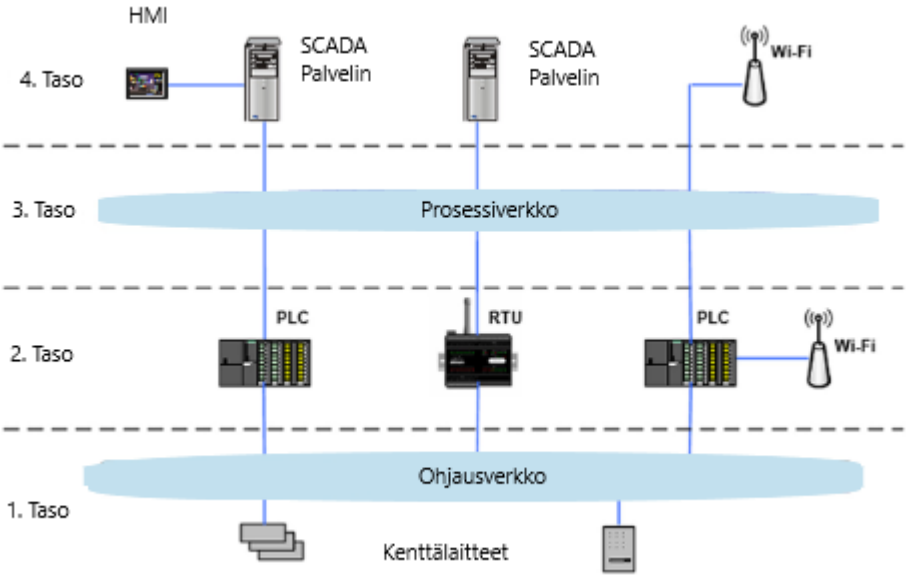
Korkeimmalla tasolla (ks. kuvio 1) SCADA-järjestelmän hierarkiassa toimii operaattori, joka näyttää prosessin tilaa ihminen-kone-rajapinnan (HMI) avulla ja kontrolloi prosessia aktivoimalla komentoja tarpeen mukaan (Nazir ym., 2017).

SCADA-järjestelmässä voi olla todella paljon laitteita liitettynä toisiinsa, ja toimiakseen niiden täytyy kommunikoida keskenään. Tyypillinen viestintä SCADA-verkossa sisältää ohjausviestejä isäntä- ja orjalaitteiden välillä (Igure,

Laughter & Williams, 2006). Protokollat ohjaavat näiden verkossa olevien laitteiden ohjausviestien yhteistä viestimuotoa, eli määrittelee sääntöjä viestintään laitteiden välillä. Näillä keinoilla viestintä saadaan toimivaksi SCADA-järjestelmässä (Bailey & Wright, 2003).

Historiallisesti SCADA-järjestelmien kommunikaatioprotokollia on kehitetty omiksi yksityisiksi protokolliksi, koska yhteisiä standardisoituja protokollia ei ollut olemassa. Yksittäisistä omista protokollista on käyttäjälle haittaa, sillä se joko lukitsee järjestelmän vain samaan omaan kehitettyyn protokollaan, tai pakottaa vaihtamaan järjestelmän merkittäviä osia vaihtaakseen toisen valmistajan protokollaan (Clarke, Reynders & Wright, 2004). Igure ym. (2006) kertovat, että American Gas Association AGA-12-standardin mukaan on olemassa noin 150-200 SCADA-protokollaa, ja näin suurta määrää pidetään ongelmana. Eri organisaatiot ovat kuitenkin pyrkineet kehittämään standardisoituja protokollia tämän ongelman ratkaisemiseksi.

Kaksi yleistä SCADA-järjestelmien käyttämää protokollaa ovat HDLC ja MODBUS. Protokollat ovat kohdanneet kuitenkin muutoksen 2000-luvulle saavuttaessa, ja niitä korvataan enemmän ja enemmän DNP3, Ethernet ja TCP/IP protokollilla (Clarke ym., 2004).



KUVIO 1 Yksinkertaistettu SCADA-järjestelmän arkkitehtuuri ja hierarkia. (Nazir, S. Patel & D. Patel, 2017, s. 437 mukaan)

2.3 SCADA-järjestelmien kehittyminen

SCADA-järjestelmät ja -ympäristöt ovat kehittyneet niiden alkuajoilta 1960-luvulta (Krutz, 2006). SCADA-järjestelmät koostuivat aikaisemmin lähes aina

tiettyyn tarkoitukseen erikseen suunnitelluista laitteista, jotka toimivat suljetuissa valmistajakohtaisissa verkoissa eikä pääsyä Internettiin tai yrityksen verkkoihin ollut (Ala-Tala ym., 2010). Tästä syystä ne olivat pääasiallisesti suojassa järjestelmän ulkopuolelta tulevilta pahanilkisiltä tunkeilijoilta tai hyökkääjiltä (Krutz, 2006).

Vuosikymmenten saatossa on kuitenkin tapahtunut paljon kehitystä. Tänä päivänä SCADA-järjestelmät käyttävät kansainvälisiä standardeja suurimpaan osaan operaatioista. Käyttöön on otettu niin standardisoituja laitteistoja, ohjelmistoja, käyttöjärjestelmiä kuin protokolliakin (Edwards, 2014). Automaatioteollisuus on siirtynyt hyväksymään yhteisiä avoimia stantardiprotokollia, mikä on SCADA-järjestelmille hyvä asia, sillä avoimien yhteisten standardien päähyötynä on se, että se tarjoaa eri valmistajien laitteiden yhteentoimivuuden (Igure ym., 2006). SCADA-järjestelmissä voi nykyään olla myös pääsy tehtaan tietojärjestelmiin Internet-verkon kautta ja joskus laajan lähiverkon (Wide Area Network WAN) kautta yritysten liiketoimintoja varten (Ala-Tala ym., 2010).

Hentea (2008) kertoo, kuinka käytettävien käyttöjärjestelmien osalta on myös tapahtunut muutosta vuosien aikana. Vaikka UNIX oli hallitseva SCADA-järjestelmissä, nyt UNIX-järjestelmät useasti syrjäytetään Linuxin ja Microsoft Windowsin -alustoilla. Nämä uudet muutokset ovat lisänneet uhkia kohdistuen SCADA-järjestelmiin sekä kasvattanut tietoisuuden tarvetta. SCADA-järjestelmät ovat viime aikoina ottaneet käyttöön Web-teknologiaa, kuten esimerkiksi ActiveX ja Java-teknologiaa. Tämän lisäksi käyttöön on otettu OPC-standardi, jota käytetään sisäiseen viestintään asiakas- ja palvelinmoduulien välillä (Hentea, 2008).

SCADA-järjestelmät ovat siis vuosikymmenien aikana muuttunut ja kehittyneet paljon. Tämän ansiosta SCADA-järjestelmät ovat lähentyneet tavanomaisen informaatioteknologian kanssa sekä ovat alttiina samoille informaatioteknologiaan liittyville uhkille, kuin lähes mikä tahansa yritysjärjestelmä (Hentea, 2008). Ala-Tala ym. (2010) kiteyttävätkin automaation viimeiset viisikymmentä vuotta siirtymänä tiettyyn tarkoitukseen erikseen suunnitelluista laitteista standardilaitteistoihin, -ohjelmistoihin ja -tiedonsiirtoteknologioilla toteutettuihin automaatioympäristöihin, joissa automaatio on toteutettu sulautetuilla ohjelmistoilla.

3 KYBERTURVALLISUUS

SCADA-järjestelmien kyberturvallisuutta käsiteltäessä, on hyvä käydä kyberturvallisuuteen liittyvät olennaiset käsitteenmäärittelyt läpi. Kyber-sanaa on ruvettu käyttämään yhä enemmän ja enemmän, mutta mitä se oikein tarkoittaa? Tässä luvussa tutustutaan kyberturvallisuuden kannalta olennaisiin käsitteisiin sekä selvitän kyberturvallisuuden ja tietoturvallisuuden käsitteiden yhtäläisyyksiä ja eroja.

3.1 Kyber

Limnell, Majewski ja Salminen (2014, s30.) määrittelevät kyberin tarkoittavan digitaalista maailmaa; kaikessa laajuudessaan sitä bittien maailmaa, joka ympärillämme on ja joka vaikuttaa päivittäiseen elämäämme. He jatkavat, että käsitteenä se usein rinnastuu kybertoimintaympäristöön tai kybermaailmaan sekä kyberiä harvemmin näkee käytettävän yksittäisenä sanana. Tarkempana määritelmänä kyber käsitteelle Limnell ym. esittävät, ja jonka määrittelyn mukaan kyber käsitettä tässä tutkielmassa käytetään: ”Etuliite, jolla viitataan tieto- ja kommunikaatioteknologian mahdollistaman digitaalisen maailman ilmiöihin, tapahtumiin, toimijoihin, toimintoihin, toimintatapoihin ja normeihin.” (Limnell ym., 2014, s239.)

3.2 Kyberturvallisuus ja tietoturvallisuus

Kyberturvallisuus ja tietoturvallisuus ovat käsitteinä läheisiä, ja niitä jopa käytetään helposti toisiaan korvaavina käsitteinä. Termiä kyberturvallisuus kuule usein osana valtioiden kriittisestä infrastruktuurista puhuttaessa, joten SCADA-järjestelmien kontekstissa näiden käsitteiden yhtäläisyyksiä ja eroja on hyvä tuoda esille.

Suomen kyberturvallisuusstrategia (2013) määrittelee tietoturvan olevan ”järjestelyjä, joilla pyritään varmistamaan tiedon käytettävyys, eheys ja luottamuksellisuus”. von Solms ja van Niekerk (2013) määrittelevät tietoturvan käsitteen ISO/IEC 27002 (2005) standardin avulla. Sen mukaan tietoturva on tietojen luottamuksellisuuden, eheyden ja saatavuuden säilyttämistä. Lisäksi siinä määritellään, että tieto voi olla niin fyysisessä, kuin digitaalisessakin muodossa (von Solms, van Niekerk, 2013). Tämä on olennainen osa näitä kahta käsitettä vertaillessa. Limnell ym. (2014) toteavat myös, että vaikka tietoturva yhdistetään yleensä vain sähköiseen tietoon ja sen käsittelyyn koskeviin asioihin, niin koskee se yhtä lailla myös fyysisessä muodossa olevaa tietoa. He jatkavat, että laajimmillaan tietoturvalla voidaan tarkoittaa minkä tahansa tiedon asianmukaista käsittelyä (Limnell ym., 2014).

Tätä voidaan tarkastella hyvin kuvion avulla (ks. kuvio 2). Tietoturvan erillään oleva ulottuvuus kuviosta kuvaa nimenomaan, että tietoturvallisuudella voidaan käsittää turvallisuutta ”tietoon pohjautuville resursseille (Assets), jotka säilytetään tai siirretään ilman viestintä- ja kommunikaatioteknologiaa”. Tämä tarkoittaa siis fyysisessä muodossa olevaa tietoa, eli esimerkiksi kansiota, missä on tietoa sisältäviä papereita. Tällaiseen tietoon suoraan kohdistuva uhka on kyberturvallisuudesta eriävä ulottuvuus.

Suomen kyberturvallisuusstrategiassa (2013) määritellään, että kyberturvallisuus käsittää yhteiskunnan elintärkeisiin toimintoihin ja kriittiseen infrastruktuuriin kohdistuvat toimenpiteet, joiden tavoitteena on saavuttaa kyky ennakoivasti hallita ja tarvittaessa sietää kyberuhkia ja niiden vaikutuksia. Kyberuhkien vaikutuksia voivat esimerkiksi olla merkittävä haitta tai vaara Suomelle tai sen väestölle. Voidaan siis sanoa kyberturvallisuuden olevan tavoitetila, jossa kybertoimintaympäristöön voidaan luottaa ja jossa sen toiminta turvataan (Suomen kyberturvallisuusstrategia, 2013).

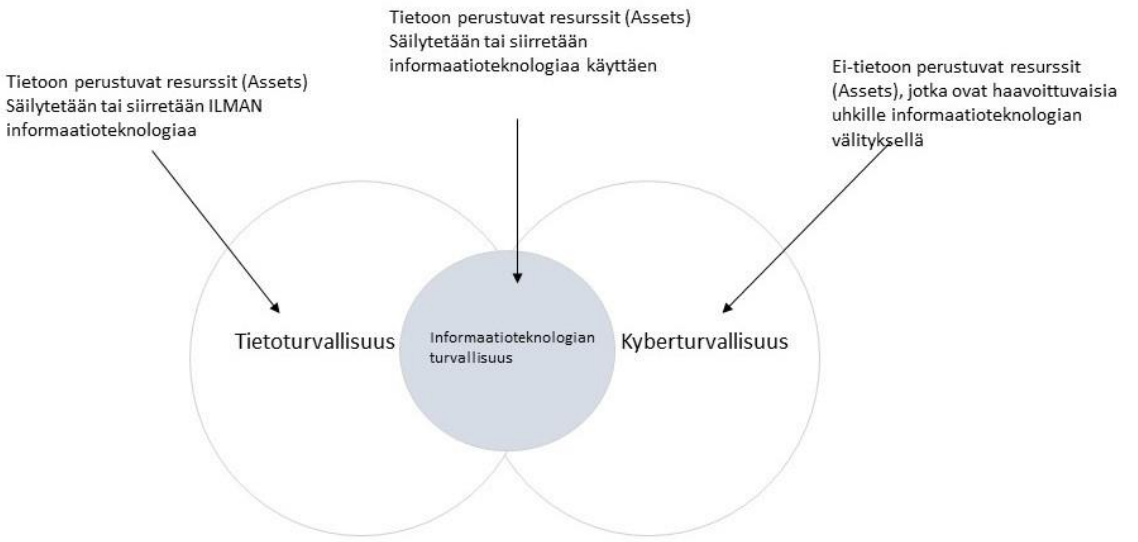
Kyberturvallisuudella on myös oma ulottuvuutensa, kuten tietoturvallisuudellakin. von Solms ja van Niekerk (2013) kuvaavat tätä kyberturvallisuuden aluetta ulottuvuudeksi, joka ulottuu tietoturvan käsittämien asioiden rajojen ulkopuolelle. Kyberturvallisuudessa omana alueena kuviossa (kuvio 2) mainitaan ”ei-tietoon perustuvat resurssit (Assets), jotka ovat haavoittuvaisia viestintä- ja kommunikaatioteknologian kautta tuleville uhkille”. Tämän ei-tietoon perustuva resurssi voi olla vaikkapa suomen kyberturvallisuusstrategiassa (2013) määritelty vaara Suomelle tai sen väestölle. Tästä voisi olla esimerkkinä palvelunestohyökkäys, jolla vaikutetaan kriittiseen infrastruktuuriin sisältyvän tietopalvelujen saatavuuteen. Tässä tapauksessa ei ole pelkästään itse tieto eikä yksittäinen tiedon käyttäjä, joka on vaarassa, vaan pikemminkin yhteiskunnan hyvinvointi kokonaisuutena. (von Solms, van Niekerk, 2013.)

Käsitteiden kyberturvallisuus ja tietoturvallisuus yhteistä ulottuvuutta on hyvä tarkastella käsitteen kybertoimintaympäristö avulla. Kybertoimintaympäristö on sähköisessä muodossa olevan informaation (tiedon) käsittelyyn tarkoitettu, yhdestä tai useammasta tietojärjestelmästä muodostuva toimintaympäristö (Suomen kyberturvallisuusstrategia, 2013). Tämän kyberympäristössä käsi-

teltävän tiedon turvallisuus on siis tietoturvallisuuden ja kyberturvallisuuden yhteinen ulottuvuus, joka on kuviossa keskellä (kuvio 2).

Tästä konkreettisena esimerkkinä voidaan pitää sähköpostia. Sähköposti voi sisältää tietoon perustuvia resursseja, ja siihen kohdistuvalla uhkalla on merkitystä niin tietoturvan, kuin kyberturvallisuudenkin kannalta. Jos esimerkiksi SCADA-järjestelmän verkkoon liitettyyn tietokoneeseen lähetettäisiin sähköposti, jossa on liitteenä haittaohjelma, voitaisiin siitä puhua tietoturvallisuuden sekä kyberturvallisuuden uhkana SCADA-järjestelmän toimintaa kohtaan. Se voisi tuhota tietoa, jota on tallennettu järjestelmän tietokoneeseen digitaalisessa muodossa, jolloin se on tietoturvallisuuden ja kyberturvallisuuden kannalta uhka, koska tuhotaan tietoon perustuvia resursseja. Toisaalta tämä haittaohjelmaa voisi myös häiritä esimerkiksi vedenjakelujärjestelmän toimintaa, jolloin sen vaikutus voisi kohdistua myös ei-tietoon perustuviin resursseihin, kuten ihmisten terveyteen, ja silloin puhutaan pelkästään kyberturvallisuuteen kohdistuvasta uhkasta.

Osassa tähän tutkielmaan valituissa lähteissä käytetään käsitettä SCADA-järjestelmien tietoturvallisuus. Korvaan kuitenkin tähän tutkielmaan valituissa lähteissä käsitteen tietoturvallisuus käsitteellä kyberturvallisuus silloin, kun tietoa käsitellään digitaalisessa muodossa kyberympäristössä.



KUVIO 2 Tietoturvallisuuden ja kyberturvallisuuden välinen suhde (von Solms & van Niekerk, 2013, s. 101 mukaan)

3.3 Kyberuhka ja -hyökkäys

On myös hyvä tehdä selväksi, mitä kyberuhkalla ja kyberhyökkäyksellä tarkoitetaan. Suomen kyberturvallisuusstrategian (2013) mukaan kyberuhka tarkoittaa ”mahdollisuutta sellaiseen kybertoimintaympäristöön vaikuttavaan tekoon

tai tapahtumaan, joka toteutuessaan vaarantaa jonkin kybertoimintaympäristöstä riippuvaisen toiminnan.” Eli esimerkiksi SCADA-järjestelmään kohdistuva kyberuhka voisi olla sellainen teko, joka tietoverkkoja pitkin saisi aikaan kommunikaatio-ongelman isäntä- ja etälaitteiston välille. Kyberturvallisuustrategiassa tarkennetaan kyberuhkien olevan uhkia, jotka toteutuessaan vaarantavat tietojärjestelmän oikeanlaisen tai tarkoitetun toiminnan (Kyberturvallisuusstrategia, 2013). Limnell ym. (2014) määrittelevät kyberuhkan olevan ”tahallisesti tai tahattomasti digitaalisessa maailmassa tapahtuva turvattavan kohteen turvallisuutta heikentävä tekijä.”

Kyberhyökkäyksen Limnell ym. (2014) määrittelevät olevan: ”Bittien maailman kautta tapahtuva hyökkäys, jolla voidaan tuottaa haittaa, vahinkoa tai tuhoa sekä fyysiseen, että bittien maailmaan. Kyberhyökkäyksen tarkoituksena voi olla myös tiedon varastaminen tai laitteiden ja järjestelmien käytön estäminen.” Nostan tästä määrittelystä keskeisenä kohdan ”Bittien maailman kautta tapahtuva hyökkäys”, kyberhyökkäys tapahtuu siis täysin elektronisia väyliä pitkin.

4 SCADA-JÄRJESTELMIEN KYBERTURVALLISUUS

Aiemmissa luvuissa käsiteltiin kyberturvallisuutta ja siihen liittyviä käsitteitä. Seuraavaksi tarkastellaan näitä SCADA-järjestelmien kontekstissa. Tarkasteltaessa SCADA-järjestelmän yleistä rakennetta ja toimintaa tuli esille, että SCADA-järjestelmät ovat teknologioiltaan - ja sitä myötä niihin kohdistuvilta uhiltaan lähentyneet tavanomaisen informaatioteknologian kanssa. SCADA-järjestelmät kuitenkin eroavat vaatimuksiltaan ja toiminnoiltaan osittain tavanomaisesta informaatioteknologiasta. Näin ollen SCADA-järjestelmien kyberturvallisuudessa on otettava huomioon erilaisia erityispiirteitä tavanomaiseen informaatioteknologiaan verrattuna.

Tässä luvussa perehdytään aluksi näihin SCADA-järjestelmien kyberturvallisuuden eroavaisuuksiin tavanomaisesta informaatioteknologiasta. Tämän jälkeen esittelen, millä toimilla onnistuneita kyberhyökkäyksiä voidaan SCADA-järjestelmiin toteuttaa ja millä tavalla ne voivat vaikuttaa järjestelmien toimintaan. Otan ohelle mukaan esimerkkejä merkittävistä kyberhyökkäyksistä SCADA-järjestelmiin. Tämän luvun jälkeen käsitellään SCADA-järjestelmien kyberturvallisuuden mahdollista parantamista.

4.1 SCADA-järjestelmien kyberturvallisuuden eroavaisuudet tavanomaisesta informaatioteknologiasta

Tietoverkkojen yleistymisen, informaation taloudellisen arvon ja laatuvaatimusten kiristymisen myötä kyberturvallisuus on noussut keskeiseksi tekijäksi teknisten järjestelmien turvallisuuden rinnalle. Teollisuusautomaatiojärjestelmät - mukaan lukien SCADA-järjestelmät, toimivat verkottuneina muihin tietojärjestelmiin. Verkottumisella saavutettavien hyötyjen ohella verkottumiseen liittyy myös kasvavia kyberturvallisuusongelmia. Kun uhkat ja haavoittuvuudet ovat lisääntyneet on myös tarve suojata tietojärjestelmiä ja niihin kuuluvia automaatiojärjestelmiä ja -verkkoja kasvanut. (Ala-Tala ym., 2010.)

Alun perin, teolliset automaatiojärjestelmät olivat lähinnä alttiina paikallisille uhkille, koska monet niiden komponentit olivat fyysisesti suojatuilla alueilla, eivätkä ne olleet yhteydessä tietoverkkoihin tai tietojärjestelmiin. Kuitenkin nykyinen trendi yhdistää teolliset automaatio/ohjausjärjestelmien (ICS) tietoverkkoihin (IT Network) vähentää huomattavasti teollisten automaatiojärjestelmien eristyneisyyttä verrattaessa aikaisempiin järjestelmiin, joka puolestaan on lisännyt tarvetta turvata järjestelmät ulkoisilta uhkilta (Stouffer ym., 2007).

Kyberhyökkäykset energiantuotanto- ja jakelujärjestelmiin mukaan lukien sähkön-, öljyn- ja kaasunjakeluverkot, jätevedenkäsittely, vedenjakelujärjestelmät sekä kemianlaitokset voivat vaarantaa yleisön terveyden ja turvallisuuden sekä olla uhkana ympäristölle. Edellä mainituissa ympäristöissä voidaan juurikin käyttää SCADA-järjestelmiä. Lisäksi näistä haitoista tulee merkittävää taloudellista tappiota vahinkojen, tuotannon menetysten, jakeluketjujen katkeamisen, salassa pidettävien tietojen leviämisen, luottamuksen menettämisen, kielteisen julkisuuden ja oikeusprosessien muodossa (Ala-Tala ym., 2010). Tämä on juurikin se, mistä monet erot tavanomaisen informaatioteknologian ja teollisten automaatiojärjestelmien kyberturvallisuuden kannalta syntyvät.

Teollisissa automaatio/ohjausjärjestelmissä suoritettu logiikka vaikuttaa suoraan fyysiseen maailmaan, ja kyberuhkista voi seurata merkityksellistä vahinkoa ihmisten terveydelle ja turvallisuudelle sekä paljon vahinkoa ympäristölle (Stouffer ym., 2007). Tämä on se kyberturvallisuuden ulottuvuus, joka poikkeaa tavanomaisesta informaatioteknologiasta. Tästä hyvänä esimerkkinä voidaan pitää Maroochyssä Australiassa tapahtunutta hyökkäystä vedenjakelu SCADA-järjestelmään, jonka seurauksena miljoona litraa käsittelemätöntä jätevettä pääsi kulkemaan paikallisiin vesiväyliin (Slay & Miller, 2007). Tällaisessa tapauksessa se ei ole itse tieto eikä yksittäinen tiedon käyttäjä, joka on vaarassa, vaan pikemminkin yhteiskunnan hyvinvointi kokonaisuutena (von Solms & van Niekerk, 2013).

Erityisvaatimuksista Ala-Tala ym. (2010) kertovat, että automaatiojärjestelmiltä vaaditaan tavallisesti korkeampaa kyberturvallisuustasoa, kuin yleisissä toimistojärjestelmien ympäristöissä. Krutz (2006) esittää, että vaikka tietyt SCADA-järjestelmien puolet ovat soveltuvia tavanomaisen informaatioteknologian järjestelmien kyberturvallisuustekniikoiden kanssa, voivat muut kriittiset osat SCADA-järjestelmissä tulla rajoitetuksi tai huonontua näiden samojen tekniikoiden käyttöönotossa. On siis tärkeää tutkia, mitkä kyberturvallisuustekniikat sekä -menetelmät sopivat SCADA-järjestelmiin.

Ala-Tala ym. (2010) kirjoittavat, kuinka tietotekniikan yleiset lähestymistavat ovat sovellettavissa myös tuotannollisiin tietojärjestelmiin sekä erilaisiin automaatio- ja ohjausjärjestelmiin. He vielä jatkavat, että näitä menettelyitä ja ratkaisuja on kuitenkin sovellettava oikealla tavalla ja ottaen huomioon automaation erityispiirteet. Erityispiirteitä ovat tosiaikaisuus, rajalliset laskentaresurssit sekä tuotannon jatkuvuus- ja turvallisuusvaatimukset.

SCADA-järjestelmien erityispiirteistä kyberturvallisuuden kannalta kertovat myös Nazir, S.Patel ja D.Patel (2017). He kertovat, että Jain ja

Tripathin (2013) mukaan SCADA-järjestelmillä on tiukempia rajoituksia luotettavuuden, latenssin/viiveen ja toimintakelpoisuusajan (uptime) suhteen, jotka on otettava huomioon kyberturvallisuusmenetelmiä sekä estävät tietyt kyberturvatoimenpiteet (Nazir, S.Patel & D.Patel, 2017).

Voidaan siis todeta, että SCADA-järjestelmissä ja niiden kyberturvallisuudessa on samanlaisia piirteitä tavanomaisen informaatioteknologian kanssa, mutta on myös erityisvaatimuksia, jotka pitää ottaa huomioon kyberturvallisuutta käsitellessä. Voidaan myös todeta, että viime vuosikymmenien aikana tapahtuneen teknologian, ohjelmistojen ja protokollien kehityksen ja käyttöönoton myötä tietoturvan – ja sitä kautta kyberturvallisuuden merkittävyys on vaihtunut hyvin paljon teollisten automaatiojärjetelmien suhteen vuosituhannen vaihtumisen myötä (Ala-Tala ym., 2010).

4.2 Kyberuhkat ja -hyökkäykset kohdistuen SCADA-järjestelmiin

Viimeaikaiset tutkimukset osoittavat, että SCADA-järjestelmiin kohdistuvien hyökkäysten määrä on kasvanut jatkuvasti vuosien varrella. Luvussa 2.3 tuli esille, että SCADA-järjestelmät ovat lähentyneet teknologioiltaan tavanomaista informaatioteknologiaa ja näin ollen niihin on alkanut kohdistumaan samoja kyberuhkia.

British Columbia Institute of Technology Kanadassa loi tietokannan (ISID) SCADA-järjestelmien turvallisuuden vaarantumistapauksista, jotta saataisiin täsmällistä kuvaa uhkista ja hyökkäyksistä teollisuusjärjestelmiin. Nykyään samainen tietokanta on nimellä RISI (Repsitory of Industrial Security Incidents).

Tietokannasta on havaittavissa huolestuttavia trendejä. Ennen vuotta 2000, lähes 70% ilmoitetuista tapahtumista johtui joko onnettomuuksista tai epätoivoisista sisäpiiriläisistä, jotka toimivat pahanilkisesti. Vuodesta 2001 vuoteen 2003, lukuun ottamatta raportoitujen tapahtumien kokonaismäärän kasvua, raportti osoittaa myös, että lähes 70% tapahtumista on peräisin SCADA-järjestelmän verkon ulkopuolelta tulevista hyökkäyksistä. (Byres Eric & Lowe Justin, 2004.) Dell näki kaksi kertaa enemmän SCADA-hyökkäyksiä vuonna 2014 kuin vuonna 2013. Maailmanlaajuisia SCADA-hyökkäyksiä Dell näki tammikuussa 2012 91 676, josta ne nousivat 163 228 tammikuuhun 2013 ja tammikuussa 2014 Dell esittää havainneensa hyökkäyksiä 675 186. (Dell, 2015.)

Kyberuhkat ja -hyökkäykset SCADA-järjestelmiin ovat siis tilastojen mukaan kasvaneet ja kuten aikaisemmassa luvussa (ks. luku 4.1) tuli selville, on SCADA-järjestelmiin kohdistuvilla kyberhyökkäyksillä tavanomaisesta informaatioteknologiasta poikkeavia vaikutuksia.

Nykyajan teollisuuden ohjaus- ja valvontajärjestelmien monimutkaisuus jättää monia haavoittuvuuksia sekä vektoreita hyökkäykseen. Hyökkäykset voivat tulla monista paikoista, kuten suoraan Internetin välityksellä tai välillisesti yritysverkon, virtuaalisen yksityisverkon (VPN), langattoman verkon tai

valintayhteysmodeemin kautta (Stouffer ym., 2007). SCADA-järjestelmiin voidaan toteuttaa monenlaisia kyberhyökkäyksiä monesta eri tahosta. Hyökkääjinä voivat toimia bottiverkkotoimijat, rikollisuusryhmät, ulkomaiset tiedustelupalvelut, sisäpiiriläiset, tietojen kalastelijat, roskapostittajat, haittaohjelmien kehittäjät, terroristit tai teollisuusvakoilijat (Stouffer ym., 2007).

Hyökkääjinä voivat siis toimia samat tekijät, kuin tavanomaiseen informaatioteknologiaan kohdistuvilla hyökkäyksillä, mutta SCADA-hyökkäykset ovat helpommin luonteeltaan poliittisia, koska ne kohdistuvat voimalaitosten, tehtaiden ja jalostamojen toimintakykyihin eikä esimerkiksi luottokorttitietoihin, kuten monissa verkkoselain tai myyntipistejärjestelmien hyökkäyksissä (Dell, 2015).

SCADA-järjestelmään kohdistuvan kyberhyökkäyksen mahdolliset vaikutukset poikkeavat tavanomaiseen informaatioteknologiaan kohdistuvan hyökkäyksen vaikutuksista. Kyberhyökkäys voi vaikuttaa SCADA-järjestelmässä suoritettavaan logiikkaan, joka vaikuttaa suoraan fyysiseen maailmaan, ja kyberuhkista voi seurata merkityksellistä vahinkoa ihmisten terveydelle ja turvallisuudelle sekä paljon vahinkoa ympäristölle (Stouffer ym., 2007).

Entiteetit tai yksilöt, joilla on haitallinen tarkoitus, voivat toteuttaa yhden tai useamman seuraavista toimista, jotta kyberhyökkäys SCADA-järjestelmään onnistuu.

Hyökkääjät voivat häiritä SCADA-järjestelmän toimintaa viivästyttämällä tai estämällä tiedon liikkumista järjestelmän verkoissa, mikä estää verkkojen saatavuuden SCADA-järjestelmän käyttäjille (GAO-04-354, 2004). Kyseinen vaikutus on mahdollista saada aikaiseksi esimerkiksi palvelunestohyökkäyksellä.

Onnistunut hyökkäys voi toteutua myös tekemällä luvattomia muutoksia ohjelmoituihin PLC tai RTU ohjaimien ohjeisiin, muuttamalla hälytyskynnyksiä tai antaa luvattomia komentoja laitteiden ohjaamiseksi, jotka voivat johtaa laitteiden vaurioitumiseen (jos toleranssit ylittyvät), myös prosessien ennenaikainen sulkeminen tai jopa ohjauslaitteiden käytöstä poistaminen on mahdollista (GAO-04-354, 2004**).**

Esimerkkinä edellämainitusta toimesta toteuttaa onnistunut kyberhyökkäys voidaan pitää Stuxnet-matoa, joka tuli ilmi syyskuussa 2010, kun “Stuxnet” niminen mato onnistui hyödyntämään Microsoft Windowsin haavoittuvuutta ja siten pystyi murtautumaan ja katkaisemaan sähköverkkoohjausjärjestelmän. Se pystyi myös lähettämään teollisuuslaitoksen tietoja - kuten kaavioita ja tietoja tuotannosta ulkoiselle verkkosivustolle (Das, Kant & Zhang, 2012).

SCADA-järjestelmiin voidaan hyökätä myös lähettämällä väärää tietoa SCADA-järjestelmän käyttäjille tarkoituksenaan joko peittää luvattomat muutokset tai käynnistää epäasianmukaisia järjestelmän toimintoja järjestelmän käyttäjiltä. Tästä hyvänä esimerkkinä voidaan pitää huijaussähköpostien lähettämistä, joiden mukana voi olla haittaohjelma liitettynä. Vuonna 2004 Kanadassa löydettiin haittaohjelma SCADA-järjestelmän tietokoneelta, joka oli mailpohjainen ja se sisälsi näppäilyn tallentajan (keylogger). Sen uskotaan tarttu-

neen, kun SCADA-järjestelmään liitetyn tietokoneen käyttäjä on selaillut järjestelmän verkosta ulkoista sähköpostisivua. (Repsitory of Industrial Security Incidents, 2015.)

Onnistunut kyberhyökkäys on myös mahdollista toteuttaa muokkaamalla SCADA-järjestelmän ohjelmistoa tuottaen ennalta arvaamattomia tuloksia ja häiritsemällä turvallisuusjärjestelmien toimintaa (GAO-04-354, 2004). Tätä toimea toteuttanut, ja sitä kautta onnistuneen kyberhyökkäyksen toi esille ”Slammer” niminen mato. Tämä merkittävä kyberhyökkäys, joka kohdistui myös SCADA-järjestelmiin, häiritsi turvallisuusjärjestelmien toimintaa. Se tapahtui vuonna 2003, kun laajasti levinnyt Slammer-mato toi esille haavoittuvuuksia myös ohjaus- ja automaatiojärjestelmissä. Das ym. (2012) kertovat, kuinka SecurityFocus (2003) oppi, että Slammer-mato tunkeutui yksityiseen tietokoneverkkoon Ohio-Davis-Besse ydinvoimalassa tammikuussa 2002 ja esti osan SCADA-järjestelmän toiminnasta. Turvallisuusseurantajärjestelmä ei toiminut lähes viiteen tuntiin huolimatta siitä, että laitoiksen henkilökunta uskoi verkon olevan täysin suojattu palomuurilla (Das ym., 2012).

Kyberhyökkäys SCADA-järjestelmään voi siis mahdollisesti sisältää yhden tai useamman edellä mainituista toimista, ja kuten näistä esimerkeistä nähdään, voivat kyberhyökkäykset häiritä SCADA-järjestelmien toimintaa ei-tarkoitetulla tavalla. Kyberhyökkäyksillä SCADA-järjestelmään voi olla erialisia vaikutuksia tavanomaiseen informaatioteknologiaan verrattuna, sillä ne voivat aiheuttaa merkittävää vahinkoa SCADA-järjestelmiin ja sitä kautta kriittiseen infrastruktuuriin sekä koko yhteiskuntaan. Näin ollen kyberuhkilta ja -hyökkäyksiltä suojautuminen on hyvin tärkeää SCADA-järjestelmiä käyttäviltä organisaatioilta.

5 SCADA-JÄRJESTELMIEN KYBERTURVALLISUUDEN PARANTAMINEN

Kyberturvallisuus ja kyberuhkilta puolustautuminen SCADA-järjestelmissä ovat nousseet isoksi huolenaiheeksi, ja kasvava määrä kyberhyökkäyksiä on herättänyt paljon huolenaiheita valtioiden, organisaatioiden ja tutkijoiden joukossa. Kun otetaan huomioon nopeasti muuttuvat kyberuhkat ja jatkuvasti kehittyvät kyberhyökkäykset, on aina tarve jatkuvalle kyberpuolustuskäytäntöjen arvioinnille ja kehittämiselle SCADA-järjestelmien kyberturvallisuuden parantamiseksi. On myös tärkeää huomata, että kyberuhkilta puolustautumisessa ja kyberturvallisuudessa SCADA-järjestelmissä esiintyy lisävaatimuksia korkean käytettävyysvaatimuksen sekä tosiaikaisessa prosessinohjausympäristössä toimimisen vuoksi**.** Tämän takia kaikki tavanomaiseen informaatioteknologiaan tarkoitetut kyberturvallisuuspolitiikat ja -periaatteet eivät sellaisenaan sovellu SCADA-järjestelmiin.

Tässä luvussa perehdytään kyberturvallisuusmenetelmiin ja -käytäntöihin, joita voitaisiin käyttää mahdollisesti SCADA-järjestelmien kyberturvallisuuden parantamiseksi. Olen jaotellut ne ei-teknisiin ja teknisiin, joista aluksi perehdytään ei-teknisiin menetelmiin ja sen jälkeen tarkastellaan teknisiä menetelmiä.

5.1 Ei-tekniset käytännöt ja menetelmät

SCADA-järjestelmän kyberturvallisuus on, kuten kyberturvallisuus yleensäkin, riskien hallintaa, jota optimoidaan korkean käytettävyyden, kyberturvallisuuden tason sekä käytettävien kustannusten kesken. Koska nykyisessä verkottuneessa maailmassa täydellistä kyberturvallisuutta ei voida saavuttaa, on kyberturvaa arvioitava nimenomaan riskien hallinnan näkökulmasta. (Ala-Tala ym., 2010.)

Riskillä tarkoitetaan normaalin olemassaolon ehtoa; se on jonkin negatiivisen tapahtuman (tai ongelman) mahdollisuutta tulevaisuudessa. Toisin kuin kyberuhkaa, kyberriskiä ei voida torjua vaan se sisältyy kaikkeen

toimintaan. (Limnell ym., 2014). Näin ollen riskeistä ja riskienhallinnasta tutkielmassa puhuttaessa, sisältyy uhka näiden käsitteiden alle. Riskienhallinta on metodi, jolla pyritään tunnistamaan ja arvioimaan riskejä sekä valitsemaan, kehittämään ja toteuttamaan vaihtoehtoja riskin käsittelemiseksi organisaatiossa (Limnell ym., 2014). Riskienhallinnan avainasia on vähentää haavoittuvuuksia ja haavoittuvuuksien syitä.

Haavoittuvuus on ongelma, jota hyökkääjä voi hyödyntää. Riskin mittaamiseen järjestelmässä on tunnistettava haavoittuvuudet, uhkat ja resurssien arvot (Hentea, 2008). Hyvä riskienhallinta on siis tärkeänä osana SCADA-järjestelmien kyberturvallisuuden parantamisen kannalta, ja se sisältää niin teknisiä kyberturvallisuusratkaisuja, kuten esimerkiksi palomuurin käyttöönottoa, kuin ei-teknisiä hallinnollisia toimia, kuten esimerkiksi päätöksentekoa.

On olemassa kaksi tärkeää ei-teknistä vastatoimenpidettä, jotka ovat tietoisuus ja yhteistyö. Tehokkain vastatoimenpide ihmisten haavoittuvuuksille on kyberturvallisuustietoisuus. Kyberturvallisuustietoisuus on tärkeä vastatoimenpide ja jokainen organisaatiossa tulisi sisällyttää kyberturvallisuustietoisuusohjelmiin, riippumatta siitä, onko tietokoneen käyttäjä vai ei (Edwards, 2014). Jokaisen organisaatioon kuuluvan yksilön tulisi tietää, millä toimilla voidaan ehkäistä kyberuhkien toteutumista. Tämä on merkittävä tekijä SCADA-järjestelmien kyberturvallisuuden parantamiseksi.

Toinen ei-tekninen toimenpide kyberturvallisuuden parantamiseksi SCADA-järjestelmissä on yhteistyö. Paremman kyberturvallisuuden varmistamiseksi on saatava aikaan yhteinen ymmärrys kyberturvallisuuteen liittyvistä asioista monien eri tahojen kesken, tavallisesti ainakin laitoksen IT-organisaation, laitoksen automaatio-osaston sekä automaatiotoimittajan kesken (Ala-Tala ym., 2010). Käytännössä tätä haastetta voi lisätä esimerkiksi se, että mukana on yrityksen konsernitason IT-organisaatio, joka voi sijaita kokonaan eri maassa kuin kyseessä oleva laitos. Yhteinen ymmärrys ei valitettavasti läheskään aina toteudu käytännön tasolla, ja usein myös IT- ja automaatiomaailman erilaiset terminologiat aiheuttavat ongelmia keskinäisessä ymmärryksessä. Lisähaasteena on usein tehtävien hoidon ulkoistaminen tehtaan ulkopuolisille tahoille, josta esimerkkinä on prosessilaitteiden jatkuvan ylläpidon ulkoistaminen (Ala-Tala ym., 2010). Tähän tulisi löytää ratkaisu SCADA-järjestelmien kyberturvallisuuden parantamiseksi.

Kyberturvallisuuden hallinnollisesta puolesta lisäksi suositellaan, että sisäverkon ja automaatioverkon kyberturvallisuusvastuut on syytä pitää erillään, koska sama taho ei tavallisesti voi vastata molemmista, mutta molempien verkkojen hallinnan on oltava mukana samassa kyberturvallisuusorganisaatiossa (Ala-Tala ym., 2010).

5.2 Tekniset käytännöt ja menetelmät

Teknisistä menetelmistä kyberturvallisuuden parantamiseen sisältyy monia asioita. SCADA-järjestelmissä valvomatonta tietoliikennettä ei saisi missään nimessä sallia, koska se on joka tapauksessa automaatiojärjestelmän kannalta kyberturvallisuusriski (Ala-Tala ym., 2010). Myös Stouffer ym. (2007) huomauttaa pääsyn rajoittamisesta verkkoon pääsystä. Tämä voidaan toteuttaa hyvin demilitarisoidun vyöhykkeen verkkoarkkitehtuurilla, johon sisältyy myös palomuurien käyttö tietoliikenteen rajoittamiseksi. Erittäin tärkeinä teknisinä toimenpiteinä voidaan pitää myös järjestelmän päivittämistä haavoittuvuuksia vastaan sekä viimeisimpien teknisten turvatoimien toteuttamista. Turvallisuustestit ja auditoinnit olisi myös suoritettava määräajoin (Edwards, 2014).

SCADA-järjestelmän kyberturvallisuutta voidaan arvioida myös käyttämällä erilaisia simulaatio- mallintamis- haavoittuvuusanalyysitekniikoita. Haavoittuvuusanalyysiä suoritetaan hyökkäämällä aktiivisesti järjestelmään, joka ei ainoastaan paljasta haavoittuvuuksia, vaan sitä voidaan myös käyttää järjestelmän virheilmoitusten määrittämiseen, mikä auttaa ymmärtämään järjestelmää ja tarjoamaan tarvittavat takeet haavoittuvuuksien korjaamiseksi. Tunkeutumistestauksia (penetration testing) ja haavoittuvuusanalyysejä voidaan katsoa loistaviksi tekniikoiksi kyberhyökkäysten ja -haavoittuvuuksien arvioinnissa SCADA-järjestelmään (Ten, Liu & Manimaran, 2008). Näitä tekniikoita voidaan käyttää koeympäristöjen avulla.

Simulaatio- ja mallintamistekniikoita käytetään hyödyllisesti SCADA-järjestelmien puolustuksen arvioimiseen sekä mittaamiseen, ja ne ovat keskeisiä tekniikoita SCADA-järjestelmien kyberturvallisuuden parantamisen kannalta. Yleensä verkkosimulaattoria, kuten OMNeT ++: aa, käytetään verkkosimulointia varten ja Simulink / MATLABia käytetään simuloimaan prosessin ohjausta (Nazir ym., 2017).

Hyvänä esimerkkinä simuloiduista hyökkäyksistä on Yilin Mo, Chabukswar & Sinopolin (2014) kehittämä menetelmä havaita SCADA-järjestelmien datan eheyteen kohdistuvia hyökkäyksiä. Mo ym. (2014) esittävät artikkelissaan keinon havaita SCADA-järjestelmien datan eheyteen kohdistuvia kyberhyökkäyksiä simuloitujen hyökkäysten avulla. He kehittivät toistohyökkäysmallin ja analysoivat hyökkäyksen kohteena olevan valvontajärjestelmän suorituskykyä.

He tekivät havainnon, että joidenkin SCADA-järjestelmien estimoinnin virheiden valvonnan havaitsemisstrategia ei ole sitkeä toistohyökkäykselle. Tällaiselle järjestelmälle pystyttiin parantamaan vian havaitsemista autentikointisignaalitekniikalla, joka kuitenkin paransi havaitsemista järjestelmän suorituskyvyn kustannuksella (Mo ym., 2014). Luvussa 4.1 tuli esille, että SCADA-järjestelmillä on vaatimuksena jatkuva toiminta, joten suorituskyvylle ei saa tapahtua suuria muutoksia.

Mo ym. (2014) esittivätkin myös, että autentikointisignaali voitaisiin viedä järjestelmään satunnaisin väliajoin jatkuvan sijaan, jolloin sen vaikutus suorituskykyyn kestäisi vain hetken aikaa. Tulevaisuudessa keskitytään laajenta-

maan näitä tekniikoita kehittyneempiin hyökkäysmalleihin ja hajautettuihin ohjausjärjestelmiin (Mo ym., 2014). Tällaisten menetelmien kehittäminen ja testaaminen on tärkeä tekijä SCADA-järjestelmien kyberturvallisuuden parantamisessa. Menetelmiä kehittäessä täytyy kuitenkin ottaa SCADA-järjestelmien erityisvaatimukset huomioon.

Myös Amin, Litrico, Sastry ja Bayen (2013) toteuttivat operatiivisen kenttätestauksen hyökkäämällä vesi SCADA-järjestelmään. He huomasivat hyökkäyskokeistaan, että vaikka SCADA-järjestelmän hyökkäysten diagnoosijärjestelmä toimii hyvin ei-samanaikaisille satunnaisotoksille, se ei ole vankka salaisille kyberhyökkäyksille, jotka harhauttavat diagnoosijärjestelmää. He esittävät jatkotutkimusaiheen, joka voisi parantaa SCADA-järjestelmien kyberturvallisuutta. Analysoimalla hyökkääjän vaatimien resurssien ja toteutuneen hyökkäyksen vaikutusten suhdetta voisi johtaa tarkkaan viitekehykseen SCADA-järjestelmien turvallisuusuhkien arviointia varten (Amin, Litrico, Sastry & Bayen, 2013).

Yhtenä menetelmänä SCADA-järjestelmien kyberhyökkäyksiltä puolustautumiseen ja kyberturvallisuuden parantamiseen on myös esitetty hyökkäyspuu (Attack tree) -menetelmä. Hyökkäyspuu-menetelmässä pohditaan, millaisilla erilaisilla tavoilla hyökkäys voi saavuttaa tavoitellun päämääränsä, ja sitä analysoimalla voidaan dokumentoida ja tunnistaa yleisesti esiintyvät hyökkäysmallit ja muuttamaan niiden perusteella hyökkäyspuita parantaakseen kyberturvallisuuden kehittämistä. (Ralston, Graham & Hieb, 2007).

Kyberturvallisuuden merkitsevyyden tietoisuuteen tuleminen on myös saanut aikaan yhden merkittävän tekijän kyberuhkilta ja -hyökkäyksiltä puolustautumiseen. SCADA-järjestelmien valmistajat ovat alkaneet korostamaan tuotteidensa turvallisuutta sekä myös varustamaan tuotteensa turvallisuutta parantavilla ominaisuuksilla. Näitä ominaisuuksia ovat mm. salaus (encryption), Kerberos ja kanavointivälityspalvelimet (multiplexing proxy) ja niitä kutsutaan sisäänrakennetuksi puolustukseksi. Näitä ominaisuuksia käyttöönottaessaan, voi tehdä SCADA-järjestelmään hyökkäämisestä vaikeampaa. SCADA-järjestelmät tarjoavat myös muita sisäänrakennettuja turvallisuusmekanismeja, kuten operatiivisia historioitsijoita sekä varaservereitä (Redundant Server) (Nazir ym., 2017).

Kyberturvallisuus sekä kyberuhkilta ja -hyökkäyksiltä puolustautuminen on jatkuva prosessi, joka ei pääty kaikkien tarvittavien kyberturvatekniikoiden käyttöönottoon. SCADA-järjestelmän verkkoa on seurattava jatkuvasti kyberturvahaavoittuvuuksien suhteen ja verkossa olevat ohjelmistot sekä laitteet on päivitettävä ja turvattava uusimpien korjaustiedostojen avulla (Igure ym., 2006).

Tiedetään, kuinka tärkeitä SCADA-järjestelmät voivat olla teollisille yrityksille tai osana valtioiden kriittistä infrastruktuuria, niin organisaatiot, kuin alan tutkijatkin ovat ruvenneet toimiin kyberturvallisuuden parantamiseksi ja kyberhyökkäyksiltä puolustautumisen suhteen. Erilaisten kyberturvallisuustekniikoiden ja -menetelmien kehittämistyö on käynnissä jatkuvasti ja niiden avulla voidaan parantaa hyvin SCADA-järjestelmien kyberturvallisuutta. Myös monet ammattijärjestöt ovat aloittaneet kehittämään standardeja parantaakseen

SCADA-järjestelmien kyberturvallisuutta (Igure ym., 2006). Se on hyvä suunta SCADA-järjestelmien kyberturvallisuuden kannalta, ja siten myös kaikkien turvallisuudelle.

6 YHTEENVETO

Tilastot osoittavat kasvua SCADA-järjestelmiin kohdistuvien hyökkäyksien osalta, joka on herättänyt paljon keskustelua SCADA-järjestelmien kyberturvallisuudesta. Selvitin lähdekirjallisuuden avulla vastauksia tutkimuskysymyksiini, jotka olivat: miten SCADA-järjestelmän kyberturvallisuus eroaa tavanomaisen informaatioteknologian kyberturvallisuudesta, millaisilla toimilla SCADA-järjestelmään voidaan tehdä onnistunut kyberhyökkäys sekä miten SCADA-järjestelmien kyberturvallisuutta voitaisiin mahdollisesti parantaa?

Tutkielmassa tuli esille, että SCADA-järjestelmät ovat kehittyneet paljon viime vuosikymmenten aikana. SCADA-järjestelmiin on alettu ottamaan käyttöön yleisiä standardisoituja laitteistoja, ohjelmistoja sekä protokollia. Näin ollen SCADA-järjestelmät ovat lähentyneet tavanomaisen informaatioteknologian kanssa, jonka seurauksena myös SCADA-järjestelmiin kohdistuvat kyberuhkat ovat muuttuneet uusien teknologioiden käyttöönoton mukana. SCADA-järjestelmät poikkeavat kuitenkin toiminnoiltaan ja vaatimuksiltaan tavanomaisesta informaatioteknologiasta, joka tulee huomioida niihin kohdistuvien kyberuhkien osalta ja kyberturvallisuutta käsiteltäessä.

SCADA-järjestelmiin kohdistuvilla kyberhyökkäyksillä voi olla tavanomaiseen informaatioteknologiaan verrattuna poikkeavia seurauksia. Hyökkäys vaikuttaa SCADA-järjestelmässä suoritettavaan logiikkaan, joka vaikuttaa suoraan fyysiseen maailmaan, ja kyberuhkista voi seurata merkityksellistä vahinkoa ihmisten terveydelle ja turvallisuudelle sekä paljon vahinkoa ympäristölle (Stouffer ym., 2007). Kyberhyökkäyksillä SCADA-järjestelmiin voidaan vaikuttaa koko yhteiskunnan toimintaan.

SCADA-järjestelmiin kohdistuvat hyökkäykset ovat helpommin luonteeltaan poliittisia, koska ne kohdistuvat voimalaitosten, tehtaiden ja jalostamojen toimintakykyihin eikä esimerkiksi luottokorttitietoihin, kuten monissa verkkoselain tai myyntipistejärjestelmien hyökkäyksissä (Dell, 2015).

SCADA-järjestelmät ovat lähentyneet tavanomaisen informaatioteknologian kanssa sekä ovat alttiina samoille informaatioteknologiaan liittyville uhkille, kuin lähes mikä tahansa yritysjärjestelmä (Hentea, 2008). Hyökkäykset voivat tulla monista paikoista, kuten suoraan Internetin välityksellä tai välillisesti

yritysverkon, virtuaalisen yksityisverkon (VPN), langattoman verkon tai valintayhteysmodeemin kautta (Stouffer ym., 2007).

Onnistuneen kyberhyökkäyksen SCADA-järjestelmään voi tehdä monella erilaisella toimella. Hyökkäyksen voi toteuttaa tekemällä luvattomia muutoksia ohjelmoituihin PLC tai RTU ohjaimen ohjeisiin, peittää luvattomat muutokset, käynnistää epäasianmukaisia järjestelmän toimintoja järjestelmän käyttäjiltä tai muokata SCADA-järjestelmän ohjelmistoa tuottaen ennalta arvaamattomia tuloksia ja häiritsemällä turvallisuusjärjestelmien toimintaa. Onnistunut kyberhyökkäys voi tehdä yhden tai useamman edellä mainituista toimista. Tutkielmassa ei perehdytty kovinkaan paljoa hyökkäysten tekniseen toteutukseen.

Lähdekirjallisuuden avulla tuli esille tutkielmassa, että SCADA-järjestelmien kyberturvallisuutta voidaan parantaa monien eri kyberpuolustusmenetelmien ja -teknologioiden avulla. Kyberpuolustusmenetelmiä on teknisiä sekä ei-teknisiä. Merkittävinä ei-teknisinä tekijöinä kyberturvallisuuden parantamiselle on tietoisuus ja yhteistyö. Kyberturvallisuustietoisuus on tärkeä vastatoimenpide ja jokainen organisaatiossa tulisi sisällyttää kyberturvallisuustietoisuusohjelmiin, riippumatta siitä, onko tietokoneen käyttäjä vai ei (Edwards, 2014).

Lisäksi lähdekirjallisuutta tutkittaessa simulaatio- ja mallintamistekniikoiden hyödyllisyys SCADA-järjestelmien kyberturvallisuuden parantamisessa nousi esille. Voinkin todeta lähdekirjallisuuden pohjalta, että simulointi- ja mallintamistekniikoita voisi kehittää ja ottaa käyttöön mahdollisimman paljon SCADA-järjestelmien yhteydessä parantaakseen niiden turvallisuutta. Tärkeänä asiana voidaan myös sanoa, että kyberturvallisuus on jatkuva prosessi, joka ei pääty kaikkien tarvittavien kyberturvatekniikoiden käyttöönottoon. Kyberturvallisuuden käsittely tulisi olla siis jatkuvasti mukana SCADA-järjestelmää käyttävän organisaation toiminnassa niin teknisellä, kuin ei-teknisellä puolella.

Aikaisemmista tutkimuksista tuli niin ikään selville, että erilaisten kyberturvallisuustekniikoiden ja menetelmien kehittämistyö on käynnissä jatkuvasti ja niiden avulla voidaan parantaa hyvin SCADA-järjestelmien kyberturvallisuutta. Tätä kehittämistyötä tulee jatkaa, ja hyvänä jatkotutkimuskohteena on SCADA-järjestelmien erilaisten kyberturvallisuusmenetelmien ja -tekniikoiden kehittäminen ja tutkiminen. Olisi tärkeää löytää mahdollisimman tehokkaita kyberturvallisuusmenetelmiä, jolla voitaisiin parantaa SCADA-järjestelmien kyberturvallisuutta ympäri maailman. SCADA-järjestelmien kyberturvallisuusmenetelmiä kehitettäessä tulee kuitenkin ottaa huomioon niiden erityisvaatimukset tavanomaisesta informaatioteknologiasta, joita ovat muun muassa tosiaikaisuus, rajalliset laskentaresurssit sekä tuotannon jatkuvuus- ja turvallisuus-vaatimukset.

Toisena mielenkiintoisena mahdollisena jatkotutkimusaiheena nousi lähdekirjallisuudessakin esiintynyt viitekehyksen kehittäminen. Analysoimalla hyökkääjän vaatimien resurssien ja toteutuneen hyökkäyksen vaikutusten suhdetta voisi johtaa tarkkaan viitekehykseen SCADA-järjestelmien kyberturvallisuusuhkien arviointia varten (Amin ym., 2013). Hyvänä jatkotutkimuskohteena

olisi tällaisen viitekehyksen kehittäminen, jonka seurauksena voitaisiin mahdollisesti parantaa SCADA-järjestelmien kyberturvallisuutta.

Edellä mainitut jatkotutkimuskohteet ovat mielenkiintoisia, sillä niihin liittyvä tutkimus on vähäistä. Kriittisen infrastruktuurin kyberturvallisuuden tutkiminen on myös hyvin ajankohtaista sekä tärkeää ihmisten turvallisuuden kannalta.

LÄHTEET

Ala-Tala, A., Havaste, A., Heimbürger H., Helenius, M., Henttu, M., Hänninen, P., Kajava, J., Koponen, P., Kyrölä, T., Riipinen, T., Savola, R., Seppälä, J., Sundquist, M., Taskinen, V., Tuovinen E., Tyynelä, M., (2010). *Teollisuusautomaation tietoturva. Helsinki: Suomen Automaatioseura ry*

Amin, S., Litrico, X., Sastry, S. & Bayen, A. M. (2013). Cyber security of water SCADA systems-part I: Analysis and experimentation of stealthy deception attacks. *IEEE Transactions on Control Systems Technology, 21*(5), 1963-1970. doi:10.1109/TCST.2012.2211873

Bailey, D. & Wright, E. (2003). *Practical SCADA for industry*. Amsterdam: Newnes. Haettu osoitteesta http://search.ebscohost.com/login.aspx?direct=true&db=nlebk&AN=104805&site=ehost-live

Byres Eric & Lowe Justin. (2004). *The myths and facts behind cyber security risks for industrial control systems*

Chee-Wooi Ten, Chen-Ching Liu & Manimaran, G. (2008). Vulnerability assessment of cybersecurity for SCADA systems. *IEEE Transactions on Power Systems, 23*(4), 1836-1846. doi:10.1109/TPWRS.2008.2002298

Clarke, G. R., Reynders, D. & Wright, E. (2004). *Practical modern SCADA protocols : DNP3, 60870.5 and related systems*. London: Newnes. Haettu osoitteesta http://search.ebscohost.com/login.aspx?direct=true&db=nlebk&AN=104779&site=ehost-live

Das, S. K., Kant, K. & Zhang, N. (toim.). (2012). *Handbook on securing cyber-physical critical infrastructure*. Waltham, MA: Morgan Kaufmann. Haettu osoitteesta http://search.ebscohost.com/login.aspx?direct=true&scope=site&db=nlebk&AN=453871

Dell. (2015). *Dell security annual threat report 2015*

Edwards, M. (toim.). (2014). *Critical infrastructure protection*. Amsterdam: IOS Press. Haettu osoitteesta http://search.ebscohost.com/login.aspx?direct=true&scope=site&db=nlebk&AN=709732

Hentea, M. (2008). Improving security for SCADA control systems. *Interdisciplinary Journal of Information, Knowledge, and Management, 3*, 73-86. doi:10.28945/91

IEEE std C37.1-1994 (1994). IEEE. doi:10.1109/IEEESTD.1994.79185

Igure, V. M., Laughter, S. A. & Williams, R. D. (2006). Security issues in SCADA networks. *Computers & Security, 25*(7), 498-506. doi:10.1016/j.cose.2006.03.001

Krutz, R. L. (2006). *Securing SCADA systems*. Indianapolis, IN: Wiley. Haettu osoitteesta http://search.ebscohost.com/login.aspx?direct=true&db=nlebk&AN=142804&site=ehost-live

Limnell, J., Majewski, K. & Salminen, M. (2014). *Kyberturvallisuus*. Jyväskylä: Docendo. Haettu osoitteesta https://jyu.finna.fi/Record/jykdok.1308608

Nazir, S., Patel, D. & Patel, S. (2017). Assessing and augmenting SCADA cyber security: A survey of techniques. *Computers & Security, 70*, 436-454. doi:10.1016/j.cose.2017.06.010

Ralston, P. A. S., Graham, J. H. & Hieb, J. L. (2007). Cyber security risk assessment for SCADA and DCS networks. *ISA Transactions, 46*(4), 583-594. doi:10.1016/j.isatra.2007.04.003

Robert M. Lee, Michael J. Assante & Tim Conway. (2016). *Analysis of the cyber attack on the ukrainian power grid* E-ISAC.

Slay, J. & Miller, M. (2007). Lessons learned from the maroochy water breach. *Critical infrastructure protection* (s. 73-82). Boston, MA: Springer US. doi:10.1007/978-0-387-75462-8_6

Stouffer, K., Falco, J. & Kent, K. (2007). *Guide to industrial control systems (ICS) security* (2nd public draft.). Gaithersburg, MD: U.S. Dept. of Commerce, National Institute of Standards and Technology. Haettu osoitteesta http://purl.access.gpo.gov/GPO/LPS97148

U.S Government Accountability Office. (2004). *Critical Infrastructure Protection: Challenges and Efforts to Secure Control Systems (GAO-04-354)*. Washington, D.C.

von Solms, R. & van Niekerk, J. (2013). From information security to cyber security. *Computers & Security, 38*, 97-102. doi:10.1016/j.cose.2013.04.004

Yilin Mo, Chabukswar, R. & Sinopoli, B. (2014). Detecting integrity attacks on SCADA systems. *IEEE Transactions on Control Systems Technology, 22*(4), 1396-1407. doi:10.1109/TCST.2013.2280899

The Repsitory of Industrial Security Incidents-Database (2015). [sähköinen tietoaineisto]. Haettu osoitteesta https://www.risidata.com/