Tampereen yliopisto

Jesse Saarnio

SÄHKÖENERGIAJÄRJESTELMIEN HAAVOITTUVUUS

Informaatioteknologian ja viestinnän tiedekunta
Kandidaatintyö
05/2019

TIIVISTELMÄ

Jesse Saarnio: Sähköenergiajärjestelmien haavoittuvuus
Engl: Vulnerability of Electric Power Systems
Kandidaatintyö
Tampereen yliopisto
Sähkötekniikan kandidaatti
04/2019

Tässä työssä tarkastellaan sähköenergiajärjestelmän haavoittuvuuksia. Sähköenergiajärjestelmän laajuuden ja hajautetun maantieteellisen sijainnin vuoksi siihen ja sen toimintaan kohdistuu moninaisia uhkia. Tässä työssä keskitytään uhkiin, jotka kohdistuvat sähköenergiajärjestelmään sen ulkopuolelta

Yhteiskunnan toimintojen riippuvuus sähköstä on lisääntynyt. Tämän vuoksi sähköenergiajärjestelmästä on tullut kriittinen infrastruktuuri yhteiskunnan toiminnan kannalta. Onkin tärkeää tuntea sähköenergiajärjestelmän haavoittuvuudet ja sitä uhkaavat tekijät, jotta järjestelmän toimintavarmuutta voidaan kehittää ja siten turvata yhteiskunnan toiminta.

Työn alussa tarkastellaan sähköenergiajärjestelmää ja sen toimintaa. Tämän jälkeen käsitellään sääilmiöiden sähköenergiajärjestelmille aiheuttamaa uhkaa ja miten sääilmiöt ovat vaikuttaneet sen toimintaa. Lopuksi tarkastellaan vahingontekojen aiheuttamaa uhkaa fyysisen vahingonteon sekä kyberturvallisuuden kannalta.

Avainsanat: sähköenergiajärjestelmä, haavoittuvuus, myrsky, vahingonteko, kyber

SISÄLLYSLUETTELO

1. JOHDANTO

Sähköenergiajärjestelmä on yksi yhteiskunnan tärkeimmistä infrastruktuureista, koska sen avulla huolehditaan ihmisten perustarpeiden tyydyttämisestä. Sähköä tarvitaan veden pumppaamisesta asuntojen lämmittämiseen sekä ruoan säilyttämiseen, mikä asettaa kovat vaatimukset sähköenergiajärjestelmän toimintavarmuudelle. Kuitenkaan sähköenergiajärjestelmän ei voida rakentaa sellaiseksi, että se kestäisi kaikki riskit ja toimisi joka tilanteessa, koska tämä nostaisi sähköntuotannon ja -siirron hintaa liian paljon. On siis löydettävä sopiva riskitaso, jossa saavutetaan riittävä toimintavarmuus hyväksyttävään hintaan.

Tässä työssä tarkastellaan sähköenergiajärjestelmän toimintaa uhkaavia ulkopuolisia riskitekijöitä ja sitä, millaisia vaikutuksia niillä on ollut sähköenergiajärjestelmään ja sen toimintaan. Työssä käsitellään pääasiassa Suomen sähköenergiajärjestelmää ja siihen kohdistuvia riskitekijöitä, mutta esimerkkeinä tuodaan esille tapauksia myös muista sähköenergiajärjestelmistä. Työssä ei käsitellä onnettomuuksia, koska niiden tapahtuminen on satunnaista ja riippuu monista muuttujista. Työn tavoitteena on tutkia kirjallisuuden avulla, millaisia riskejä sähköenergiajärjestelmään kohdistuu ja millaisia niiden vaikutukset ovat. Lisäksi tarkastellaan, ovatko nämä riskit aiheuttaneet suurempia toimia yhteiskunnan tasolla.

Toisessa luvussa esitellään sähköenergiajärjestelmä tarkemmin ja perehdytään hieman sen toimintaan, jonka ymmärtäminen on tärkeää riskien vaikutusten ymmärtämiseksi. Kolmannessa luvussa käsitellään sääilmiöitä ja neljännessä luvussa käsitellään toimia, joilla pyritään vahingoittamaan sähköenergiajärjestelmää tai häiritsemään sen toimintaa. Tässä työssä tarkasteltavia sähköenergiajärjestelmän vahingoittamisen keinoja ovat fyysinen vahingoittamien sekä kyberhyökkäykset. Lopuksi viidennessä luvussa kootaan yhteen työn tärkeimmät havainnot ja johtopäätökset.

2. SÄHKÖENERGIAJÄRJESTELMÄT

Sähköenergiajärjestelmä voidaan jakaa kolmeen osaan, jotka ovat tuotanto, siirto ja kulutus. Sähköntuotantoon kuuluvat perinteisten voimalaitosten lisäksi teollisuuden tuottama sähkö sekä hajautettu sähköntuotanto. Sähkönsiirtoon kuuluvat siirto- ja jakeluverkot sekä verkon eri osien välillä sijaitsevat sähköasemat sekä muuntajat. Sähkönkulutukseen lukeutuvat kaikki sähköä kuluttavat tahot, kuten teollisuus ja yksityiset kuluttajat. [1] Suomessa on käytössä 3-vaiheinen vaihtosähköjärjestelmä, jossa vaihtosähkön taajuus on 50 Hz.

Sähköenergiajärjestelmän tehtävä on toimittaa laadukasta sähköä sähkön tuottajilta sen kuluttajille. Sähkön laatuun vaikuttavia tekijöitä ovat jännitteen laatu ja sähköntoimitusvarmuus [1]. Sähköenergiajärjestelmässä on vallittava tehotasapaino, jotta järjestelmä toimisi. Tehotasapaino tarkoittaa, että sähköä tuotetaan joka hetki yhtä paljon kuin sitä kulutetaan. Suomessa sähköenergiajärjestelmän järjestelmävastaavana toimii kantaverkkoyhtiö Fingrid, jonka tehtävä on huolehtia Suomen sähköenergiajärjestelmän teknisestä toimivuudesta ja käyttövarmuudesta. Fingrid vastaa myös järjestelmän tehotasapainon säilymisestä eli tasehallinnasta. [2]

2.1 Sähköntuotanto ja -kulutus

Sähköntuotanto voidaan karkeasti jakaa keskitettyyn tuotantoon, johon kuuluvat peruskuormalaitokset ja huippukuormalaitokset, sekä hajautettuun tuotantoon. Keskitetty tuotanto on nimensä mukaisesti keskittynyt jollekin alueelle eli sinne, missä voimalaitokset sijaitsevat. Peruskuormalaitokset on suunniteltu tuottamaan sama kiinteä määrä sähköä koko ajan. Niiden tuottaman sähkön määrän muuttaminen on usein vaikeaa tai hidasta, joten ne eivät vastaa kulutuksen suuriin muutoksiin vaan ne vastaavat lähinnä sähkönkulutuksen muuttumattoman osuuden tuottamisesta. Esimerkiksi lauhdevoimalaitokset voidaan suunnitella peruskuormalaitoksiksi. Ydinvoimalaitokset, jotka ovat lauhdevoimalaitoksia, ovat hyvä esimerkki peruskuormalaitoksista, koska niiden tuottaman sähkön määrä ei juurikaan vaihtele. [1,3]

Huippukuormalaitokset eivät tuota sähköä koko ajan, vaan niiden avulla pyritään vastaamaan sähkönkulutuksen vaihteluihin. Niiden tuottaman sähkön määrää voidaan muuttaa nopeasti ja helposti. Huippukuormalaitosten sähköntuotannon hyötysuhde ei ole kovin korkea, minkä vuoksi niitä ei ole suunniteltu tuottamaan sähköä jatkuvasti. Esimerkiksi kaasuturpiinilaitokset ovat tyypillisiä huippukuormalaitoksia. [1,3]

Hajautetussa tuotannossa sähköä tuotetaan pienemmässä mittakaavassa kuin keskitetyssä tuotannossa, ja siinä tuotanto sijaitsee hajautetusti sähköenergiajärjestelmässä. Tällä tavalla tuotettua sähköä voidaan käyttää laitoksen omistajan omiin tarpeisiin tai sitä voidaan syöttää verkkoon, jos laitos täyttää verkkoon liittymiselle asetetut tekniset ehdot. Yleisimpiä hajautetun tuotannon muotoja ovat aurinkovoima ja tuulivoima. [1,4,5] Useista tuulivoimalaitoksista rakennetun kokonaisuuden, tuulipuiston, teho voi olla useita satoja megawatteja. Tällöin ei voida enää puhua hajautetusta tuotannosta ja sama koskee suuren kokoluokan aurinkovoimaloita.

Sähkönkulutukselle on tyypillistä sen vaihtelu vuorokaudenajan sekä vuodenajan mukaan. Suomessa sähkönkulutusta tilastoidaan tarkasti, mikä mahdollistaa hyvän kulutuksen ennustamisen. Tämä on tärkeää, koska sähköä ei voida varastoida suuria määriä, joten sähköä on tuotettava silloin kun sitä kulutetaan. Sähköntuotannon kapasiteetin on myös riitettävä kattamaan huippukulutuksen aikana tarvittava energia yhdessä tuontisähkön kanssa, koska muuten seurauksena on tehopula. [1]

Osa Suomessa käytettävästä sähköstä tuodaan ulkomailta, yleensä Ruotsista, Norjasta sekä Venäjältä. Vuonna 2018 Suomessa käytettiin sähköä 87 TWh ja siitä tuontisähköä oli noin 20 TWh [6].

2.2 Sähkönsiirtojärjestelmä

Sähkönsiirtojärjestelmän tehtävänä on siirtää sähköenergiajärjestelmään tuleva tai siihen liitettyjen voimalaitosten tuottama sähkö sen loppukäyttäjille. Sähkönsiirtojärjestelmä rakentuu sähköverkoista, joissa on useita eri jännitetasoja, ja jännitetasojen välissä olevista sähköasemista ja muuntajista, joiden tehtävä on muuttaa ja säätää jännitteitä ja virtoja. Suomessa yleisimmät jännitetasot ovat 400 kV, 220 kV, 110 kV, 20 kV ja 0,4 kV. Sähkönsiirto voidaan jakaa kahteen osaan, jotka ovat siirto- ja jakeluverkko. [1,5,7]

Sähköasema on kohta siirto- tai jakeluverkossa, jossa voidaan tehdä kytkentöjä, muuttaa jännitettä ja jakaa sekä keskittää sähkön siirtoa eri johdoille. Sähköasemien tärkeimpiä laitteita ovat muuntajat, katkaisijat, erottimet sekä mittamuuntajat. [7]

2.2.1 Siirtoverkko

Siirtoverkon tehtävä on palvella sähkön tuottajia ja kuluttajia mahdollistamalla osapuolten välinen kaupankäynti koko Suomen tasolla sekä Suomen rajat ylittävä kaupankäynti. Siirtoverkko siirtää siihen tulevan tai siihen liitettyjen voimalaitosten tuottaman sähkön jakeluverkkoon tai suoraan siirtoverkkoon kytketyille suurille sähkön kuluttajille, kuten

teollisuuslaitoksille. Suomessa siirtoverkon omistaa Fingrid ja siihen kuuluu 400 kV:n ja 220 kV:n jännitteiset johdot ja sellainen osa 110 kV:n verkosta, joka pystyy toimimaan 400 kV:n siirtoverkon korvaajana 400 kV:n johdon vikaantuessa tai muodostaa silmukkaverkon, sekä sähköasemia. Siirtoverkko on rakennettu kokonaan ilmajohdoilla. Lisäksi Fingrid omistaa suurimman osan Suomesta ulkomaille menevistä rajajohdoista. [1,2]

Siirtoverkot rakennetaan silmukoiduiksi verkoiksi, koska se pienentää verkon häviöitä ja parantaa käyttövarmuutta. Käyttövarmuus on silmukoidussa verkossa parempi, koska syöttöasemat voivat saada sähköä useampien eri teiden kautta. Näin ollen sähkölle on aina olemassa vaihtoehtoinen siirtymisreitti, jos joku siirtoreitin varrella oleva komponentti vikaantuu. Siirtoverkon käyttöperiaate on N – 1 -periaate, joka tarkoittaa että, järjestelmä on suunniteltu ja sitä käytetään siten, että se kestää aina yhden komponentin vikaantumisen ja irtoamisen järjestelmästä. [1]

2.2.2 Jakeluverkko

Jakeluverkon tehtävä on siirtää siirtoverkon kautta tuleva tai jakeluverkkoon liitettyjen voimalaitosten tuottama sähkö sen loppukäyttäjille. Suomessa jakeluverkkoon kuuluu osa 110 kV:n alueverkoista, 1-70 kV:n keskijänniteverkko ja 0,4 kV:n pienjänniteverkko sekä sähköasemia (110/20 kV) ja jakelumuuntamoita (20/0,4 kV). [1,5] Näiden primäärikomponenttien lisäksi jakeluverkkoon kuuluu paljo sekundäärilaitteita ja -järjestelmiä, joita ovat ”sähköasemilla olevat suojareleet ja apujännitejärjestelmät, käyttökeskuksissa käytössä olevat käytönvalvonta- ja käytöntukijärjestelmät, tiedonsiirto- ja radiopuhelinjärjestelmät sekä useat muut laajat tietojärjestelmät (verkkotietojärjestelmä, asiakastietojärjestelmä, materiaalin hallintajärjestelmä, jne.)” [5].

Jakeluverkko voidaan rakentaa säteittäiseksi tai silmukoiduksi verkoksi, mutta sitä käytetään yleensä säteittäisenä. Tämä johtuu siitä, että säteittäisessä verkossa häiriöiden rajoittaminen, jännitteensäätö ja suojausten toteuttaminen on helpompaa sekä oikosulkuvirrat ovat pienempiä kuin silmukoidussa verkossa. Säteittäinen jakeluverkko toimii kuitenkin oikein vain yksisuuntaisessa sähkönsiirrossa ja hajautetun tuotannon kytkeminen jakeluverkkoon edellyttää usein järjestelmätason muutoksia. Tämä johtuu jakeluverkon vanhoista suojauksista, jotka ovat suunniteltu vain yhteen suuntaan käytettävään sähkönsiirtoon, joten ne eivät toimi, jos vikavirta voi tulla kummasta suunnasta tahansa. [1,5]

Suomessa jakeluverkkoja käytetään erilaisissa toimintaympäristöissä eri puolilla maata. Osa jakeluverkoista sijaitsee taajamissa ja kaupungeissa ja osa harvaan asutuilla alueilla. Toimintaympäristö vaikuttaa jakeluverkon rakennustapaan, onko jakeluverkko tehty

ilmajohdoilla vai maakaapeleilla. Maakaapeleita käytettäessä saavutetaan yleensä parempi käyttövarmuus verrattuna ilmajohtoihin. Myös ilmajohtojen kesken on eroja niiden käyttövarmuudella ja siihen vaikuttaa esimerkiksi ilmajohdon rakennuspaikka, onko ilmajohto tien varressa vai metsän keskellä. [5,7] Vuoden 2018 loppuun mennessä Suomen jakeluverkon keskijänniteverkosta maakaapelia oli 27 % ja pienjänniteverkosta 47 % [8].

2.2.3 Sähkönsiirtojärjestelmän viat

Yleisimpiä vikoja sähkönsiirtojärjestelmässä ovat oikosulut ja maasulut. Vikoja voivat aiheuttaa esimerkiksi ylijännitteet, laitteiden toimintahäiriöt, johdon katkeaminen tai verkkokomponentin eristyskyvyn aleneminen. Vika voi johtaa häiriöön, josta voi seurata sähkönjakelun osittainen tai täydellinen katkeaminen. Säteittäisessä verkossa täydellinen sähkönjakelun katkos on mahdollinen, mutta silmukoidussa verkossa sähkönjakelu ei katkea hetkeksikään, koska silmukoidussa verkossa sähkölle on aina vaihtoehtoinen kulkureitti. [1,7]

Oikosulku on vaiheiden välinen vika ilman maakosketusta. Kolmivaiheinen oikosulku on symmetrinen vika eli vika vaikuttaa kaikkiin vaiheisiin samalla tavalla. Oikosulku voi olla myös kaksivaiheinen, jolloin vikavirtapiirissä on kaksi vaihetta. Tällöin vika on epäsymmetrinen. Oikosulku voi syntyä esimerkiksi salaman lyödessä johtoon ja valokaaren yhdistäessä johtoja tai tuulen heilauttaessa johdot yhteen. Jos vikavirtapiiriin kuuluu myös maa, on kyseessä maasulku. Maasulku syntyy, kun eristysvian tai muun vian vaikutuksesta virtapiirin johdin joutuu johtavaan yhteyteen maan tai maahan johtavassa yhteydessä olevan laitteiston osan kanssa. Maasulku voi olla 1- tai 2-vaiheinen ja maasulut voivat syntyä esimerkiksi puun kaatuessa johdolle. [1,7]

2.2.4 Sähkönsiirtojärjestelmän suojaus

Sähkönsiirtojärjestelmän laitteiden suojauksesta huolehtii katkaisijoiden, suojareleiden sekä mittamuuntajien muodostama kokonaisuus. Suojauksen tehtävä on havaita viat ja epänormaalit olosuhteet järjestelmässä, jotta viat pystytään selvittämään ja epänormaalit olosuhteet saadaan loppumaan. Oiko- tai maasulkutilanteissa suojaus erottaa vikaantuneen verkon osan muusta järjestelmästä, jotta siitä ei aiheudu vaaraa eikä oikosulkuvirta vahingoita järjestelmän laitteita. [7]

Hyvä relesuojausjärjestelmä on selektiivinen, nopea, luotettava, herkkä ja se toimii myös poikkeuksellisissa käyttötilanteissa. Suojauksen selektiivisyys tarkoittaa, että suojaus erottaa verkosta vain vikaantuneen komponentin ja että kaikki verkon osat ovat suojattu

jollain suojareleellä. Suojauksen nopeus on tärkeää, koska mitä nopeammin vika saadaan erotettua, sitä pienemmät ovat vikavirran aiheuttamat vahingot. Suojauksen luotettavuudella on kaksi puolta: toimintavarmuus ja käyttövarmuus. Toimintavarmuus tarkoittaa, että suojarele ei toimi turhaan, jos vika ei ole sen suojausalueella. Käyttövarmuus tarkoittaa, että suojarele varmasti toimii, jos sen suojausalueella on vika. Suojauksen herkkyys tarkoittaa, että suojauksen on pystyttävä toimimaan myös tilanteissa, joissa vikavirrat ovat pienentyneet käyttötilanteen muutoksen vuoksi. [7]

2.3 Sähkön laatu

Kokonaisuutena sähköntoimituksen laatu käsittää itse sähkön laadun sekä sähköntoimittamiseen liittyvien palveluiden laadun. Sähkön laadun osatekijöinä ovat jännitteen taso verkon nimellisjännitteeseen verrattuna, jännitteen hitaat vaihtelut ja jännite-epäsymmetriat, jännitehäiriöt eli jännitteen nopeat vaihtelut, jännitteen käyrämuodon vääristymät, taajuuden poikkeamat nimellisarvosta, sähköntoimituksen keskeytykset ja sähkönkäyttöoikeuden rajoitukset. Sähkön laadun ei kuitenkaan pidä olla mahdollisimman hyvää, koska se lisäisi kustannuksia merkittävästi sähköntuotannossa, -siirrossa ja -jakelussa. [1]

Verkon jännitteen tulisi olla ±10 % nimellisjännitteestä normaalitilanteessa eli tilanteessa, jossa verkossa ei ole vikaa tai jännitekatkoa. Yleensä hitaat jännitteen vaihtelut aiheutuvat tehonsiirron vaihteluista. Nopeita muutoksia jännitteen tasossa aiheuttavat nopeat ja suuret muutokset kuormituksessa. Myös salamat voivat aiheuttaa nopeita jännitteen muutoksia. Jännitekuoppa tarkoittaa lyhyen ajan kestävää alijännitetilannetta, jossa jännite on 1-90 % nimellisjännitteestä. Siinä jännite laskee nopeasti ja palautuu lyhyen ajan kuluttua. Jännitekuopat aiheutuvat yleensä oiko- tai maasuluista sähköenergiajärjestelmässä. Jännitteensäätölaitteilla jännite pidetään normaalitilanteissa halutuissa rajoissa. Näitä laitteita ovat muuntajien käämikytkimet, väliottokytkimet, kondensaattorit, reaktorit ja tehoelektroniikkaa sisältävät nopeat jännitteensäätäjät. [1,9]

Sähköenergiajärjestelmässä käytettävään kolmivaihejärjestelmään voi syntyä epäsymmetriaa, jos yksi- tai kaksivaiheiset kuormat on jaettu epätasaisesti vaiheiden välille. Epäsymmetria ei usein kehity ongelmaksi, koska vinokuormitus aiheuttaa huonon jännitteen laadun yksittäisissä vaiheissa. [1]

Taajuuden vaihtelut sähköenergiajärjestelmässä liittyvät yleensä tuotannon ja kulutuksen väliseen epätasapainoon. Ylituotanto aiheuttaa taajuuden kasvamista ja alituotanto aiheuttaa taajuuden laskua. Taajuuden vaihtelu pyritään pitämään normaalitilanteessa alle 0,1 Hz:n suuruisena nimellistaajuudesta 50 Hz. [10]

Standardissa SFS-EN 50160 (Yleisestä jakeluverkosta syötetyn sähkön jänniteominaisuudet) käyttökeskeytykseksi määritellään tilanne, jossa jännite on alle 5 % nimellisjännitteestä. Keskeytykset voidaan jakaa suunniteltuihin keskeytyksiin, joista sähkönkäyttäjille ilmoitetaan, ja häiriökeskeytyksiin, jotka aiheutuvat pysyvistä tai ohimenevistä vioista. Häiriökeskeytykset voidaan edelleen jakaa pitkiin keskeytyksiin, joiden kesto on yli 3 minuuttia, ja lyhyisiin keskeytyksiin, joiden kesto on enintään 3 minuuttia. [9] Sähköntoimitusvarmuutta voidaan arvioida erilaisten keskeytysindeksien avulla. Yleisimmin käytettyjä indeksejä ovat SAIFI-, SAIDI- ja CAIDI-indeksit. Pitkien keskeytysten lukumäärää kuvaa indeksi SAIFI (system average interruption frequency index). Keskeytystaajuus f_{SAIFI} kertoo, kuinka monta kertaa asiakkaan sähköntoimitus keskimäärin katkeaa. Keskeytysten keskimääräistä pituutta kuvaa indeksi SAIDI (system average interruption duration index). Tämä indeksi kertoo, kuinka pitkän ajan sähköntoimitus asiakkaalle on keskimäärin keskeytyneenä. Tapahtuneiden keskeytysten keskimääräistä kestoa kuvaa indeksi CAIDI (customer average interruption duration index). Näitä indeksejä käytetään verkkoyhtiöiden laadun mittaamisessa. [1]

2.4 Tehotaspaino

Suomen sähköenergiajärjestelmä on osa pohjoismaista sähköjärjestelmää, joka on yhdistetty siirtoverkon kautta yhdeksi kokonaisuudeksi. Siihen kuuluvat Suomi, Ruotsi, Norja ja Itä-Tanska. Jotta sähköenergiajärjestelmä toimii hyvin, on siinä vallittava tehotasapaino. Tehotasapainon vaihtelu ilmenee järjestelmän taajuuden vaihteluna. Suomessa järjestelmävastaava Fingrid huolehtii Suomen tasehallinnasta eli sähköntuotannon ja -kulutuksen hetkellisen tehotasapainon ylläpidosta. Sähköenergiajärjestelmä pyritään pitämään koko ajan tasapainossa, mutta kulutuksen ja tuotannon välillä on usein pieni ero. Tämä johtuu kulutuksen vaihtelevuudesta ja siitä, että kulutusta ei voida tarkasti ennustaa. Tämän vuoksi tarvitaan reservejä tehotasapainon ylläpitämiseen. Sähköenergiajärjestelmässä on kahdenlaisia reservejä, käyttö- ja häiriöreservejä. Nämä voidaan vielä jakaa aktivointiajan perusteella taajuusohjattuihin ja manuaalisesti käynnistettäviin reserveihin. [11]

Taajuuden sallitaan normaalitilanteessa vaihdella 49,9 Hz:n ja 50,1 Hz:n välillä. Järjestelmän taajuuden ollessa yli 50 Hz, on tuotanto suurempaa kuin kulutus ja taajuuden ollessa alle 50 Hz, on kulutus suurempaa kuin tuotanto. Tämä johtuu siitä, että pätötehon kulutuksen kasvaessa suuremmaksi kuin sen tuotanto, kuormitus ottaa tarvitsemansa tehon tahtigeneraattoreiden akselistojen pyörivien massojen liike-energiasta. Tämä hidastaa generaattoreita ja järjestelmässä se näkyy taajuuden pienemisenä. Päinvastoin

käy tuotannon ollessa kulutusta suurempi, jolloin tahtigeneraattoreiden liike-energia kasvaa ja ne alkavat pyöriä nopeammin, mistä seuraa järjestelmän taajuuden kasvu. [1,10]

Taajuusohjatut reservit aktivoituvat nopeasti, sekunti- ja minuuttitasolla, ja automaattisesti taajuuden muuttuessa. Taajuuden ylläpitämiseksi sähköenergiajärjestelmässä on ylläpidettävä riittävä määrä pyörivää reserviä, joka reagoi automaattisesti taajuuden muutoksiin. Suomessa taajuusohjattuna käyttöreservinä käytetään voimalaitosten pätötehoreservejä sekä tasavirtalinkkejä Venäjän ja Viron suuntaan. Taajuusohjattu häiriöreservi koostuu sovituista voimalaitoksista ja irtikytkettävistä teollisuuden kuormista. Taajuusohjattua häiriöreserviä ei käytetä normaalitilanteessa tehotasapainon ylläpitoon. [11]

Manuaalisesti käynnistettäviä reservejä käytetään, jos taajuutta ei pystytä pitämään sallituissa rajoissa taajuusohjattujen reservien avulla. Manuaalisesti käynnistettäviin reserveihin kuuluvat korkeintaan 15 minuutissa aktivoitavat säädöt säätösähkömarkkinoilla sekä nopea häiriöreservi. Säätösähkömarkkinat on Fingridin ylläpitämä ja siellä sähköntuotannon ja -kulutuksen haltijat voivat antaa säätötarjouksia säätökykyisistä resursseistaan, jotka kykenevät 10 MW:n tehonmuutokseen 15 minuutissa. Fingrid ylläpitää säätösähkömarkkinoita, koska sillä ei ole omaa säätökapasiteettia tehotasapainon ylläpitämiseksi. Nopea häiriöreservi on manuaalisesti aktivoitavaa tehoa, jota saadaan varavoimalaitoksista, sopimusvoimalaitoksista sekä sopimuksellisista teollisuuden irtikytkettävistä kuormista. [10,11]

3. SÄHKÖENERGIAJÄRJESTELMÄ JA SÄÄRISKIT

Sähköenergiajärjestelmässä erityisesti sähkönsiirrossa sekä -jakelussa on paljon osia, jotka ovat haavoittuvaisia säästä johtuville ilmiöille. Suomessa yleisimpiä sähköverkossa häiriöitä aiheuttaneita sääilmiöitä ovat kovat tuulet, rajuilmat ja myrskyt sekä lumen ja jään kertyminen. Näiden seurauksena on syntynyt pitkäkestoisia ja laaja-alaisia häiriöitä sähkönjakelussa. Myös salamointi aiheuttaa häiriöitä, mutta ne ovat yleensä lyhytkestoisempia. Sähköasemat ovat haavoittuvaisia runsaiden sateiden aiheuttamille vesistö- ja hulevesitulville. Sääilmiöt vaikuttavat myös sähköntuotantoon, esimerkiksi tuuli- ja vesivoimalat ovat riippuvaisia ilmaston olosuhteista. [12] Vuosittain säähän liittyvien ilmiöiden aiheuttamat häiriöt sähköverkossa aiheuttavat noin 60-80 % kaikkien häiriöiden keskeytysajoista [13].

Suomessa vallitsee väli-ilmasto, jossa on piirteitä sekä merellisestä että mantereisesta ilmastosta. Tämä johtuu Suomen sijainnista korkeilla leveysasteilla, suuren mantereen reunalla ja lähellä merialueita lämmittävää Golf-virtaa. [14]

3.1 Sähköverkkoihin kohdistuvat sääriskit

Sähkön siirto- ja jakeluverkko eroavat paljon toisistaan niiden rakenteen ja rakennusympäristön osalta. Siirtoverkko on rakennettu kokonaan ilmajohdoista. Niitä ympäröi leveä johtoalue, joka on yhdistelmä johtoaukeasta, joka on leveydeltään 26-42 metriä, sekä johtoaukean molemmilla puolilla olevista reunavyöhykkeistä. Reunavyöhykkeillä puiden kasvukorkeutta on rajoitettu, jotta ne eivät kaatuessaan yllä osumaan johtoihin eli siirtoverkot ovat puuvarmoja. [15]

Jakeluverkot rakentuvat sekä ilmassa olevista johtimista että maakaapeleista riippuen rakennusympäristöstä. Jakeluverkon keskijänniteverkosta 83 % on ilmassa olevia johtimia ja pienjänniteverkosta 58 %. Noin 40 % keskijänniteverkon ilmassa olevista johtimista kulkee metsässä ja 19 % sijaitsee teiden varsilla, jolloin toisella puolella johtoa kasvaa puita. Pienjänniteverkossa metsässä kulkee noin 27 % ilmassa olevista johtimista ja teiden varsilla sitä kulkee 17 %. [8] Keskijänniteverkosta noin 80 % on päällystämätöntä avojohtoa, kun taas pienjänniteverkosta päällystämätöntä avojohtoa on vain 3 %. Pienjänniteverkosta yli 50 % on ilmakaapelia, kuten AMKA-riippukierrejohtoa. [5] Avojohto on paljon haavoittuvaisempaa ja vikaherkempää kuin ilmakaapelit, koska avojohtoa ei ole päällystetty. Päällyste suojaa johtimia vioilta esimerkiksi puun koskettaessa

niitä tai puun kaatuessa johtimille. Keski- ja pienjänniteverkoissa ilmassa olevien johtimien ympärillä olevat johtokadut ovat selvästi kapeampia kuin siirtoverkon tapauksessa, jolloin puut tai niiden oksat voivat yltää johdoille, ja tämän vuoksi sääilmiöiden kaatamat ja taivuttamat puut aiheuttavat ongelma keski- ja pienjänniteverkoille.

3.1.1 Tuulet ja myrskyt

Tuulet ja myrskyt aiheuttavat sähköverkolle ongelmia usein siksi, että ne kaatavat puita tai katkovat oksia sähköjohdoille, jolloin syntyy oikosulku tai maasulku. Siirtoverkon kannalta tuulet ja myrskyt eivät yleensä aiheuta ongelmia, koska siirtoverkkojen johtokadut ovat niin leveitä, että puut tai oksat eivät yllä johtoihin. Jakeluverkossa tilanne on kuitenkin toinen, koska johtokadut ovat pienempiä. Erityisen alttiita tuulten ja myrskyjen aiheuttamille ongelmille ovat metsissä sijaitsevat jakeluverkkojen osuudet. Vuosina 2015, 2016 ja 2017 tuulet ja myrskyt ovat aiheuttaneet keskimäärin 32,5 % sähkönjakelun keskeytyksistä ja 42,5 % keskeytysajoista [13].

Suomen ilmastosta johtuen tuulen suunta ja nopeus vaihtelevat paljon päivän aikana. Kuitenkaan kovia tuulia tai myrskyjä ei esiinny Suomessa kovin usein. Taulukossa 1 on esitelty tuulen eri nopeuksien vaikutuksia maalla. Puuskissa tuulen nopeus voi olla noin 1,5-2 kertainen 10 minuutin keskituuleen nähden [16]

Taulukko 1. Tuulen vaikutuksia maalla, muokattu lähteestä [16]

Tuulen nopeus (m/s)	Tuulen nimitys	Tuulen vaikutus	Tuulen nopeus (m/s)	Tuulen nimitys	Tuulen vaikutus
0	Tyyntä	Savu nousee pystysuoraan	14-16	Kovaa	Puut heiluvat. Tuulta vasten kulkeminen vaikeaa.
1-2	Heikkoa	Tuulen suunnan näkee savun liikkeestä	17-20	Kovaa	Katkoo puiden oksia. Ulkona liikkuminen vaikeaa.
2-3	Heikkoa	Tuulen tuntee iholla. Puiden lehdet kahisevat.	21-24	Myrskyä	Katkoo puiden oksia. Ulkona liikkuminen vaikeaa.
4-5	Kohtalaista	Puiden lehdet ja lehvät liikkuvat. Kevyt lippu suoristuu.	25-28	Kovaa myrskyä	Kiskoo puita juurineen. Aiheuttaa huomattavaa vahinkoa rakennuksille. Sattuu harvoin sisämaassa.
6-7	Kohtalaista	Pienet oksat heiluvat. Nostaa maasta pölyä ja irtonaisia paperin palasia	29-32	Ankaraa myrskyä	Kaataa metsää. Siirtää rakennuksia. Sattuu erittäin harvoin sisämaassa.
8-10	Navakkaa	Pienehköt lehtipuut heiluvat. Järvenselällä vaahtopäitä	≥ 33	Hirmumyrskyä	Tuhoaa perin pohjin rakennukset ym.
11-13	Navakkaa	Suuret oksat heiluvat. Tuuli suhisee sattuessaan taloihin ja kiinteisiin esineisiin.			

Syöksyvirtauksissa tuulen nopeus voi olla jopa 30-50 m/s ja usein ne syntyvät ukkospilvien vaikutuksesta. Ne aiheuttavat paljon vahinkoa, esimerkiksi kaatavat suuria alueita metsää, koska syöksyvirtauksissa tuuli etenee maanpinnalla suoraan tai loivasti kaartuen. [17]

Sähköverkkojen kannalta tuulet alkavat vaikuttamaan, kun niiden nopeus on noin 6-10 m/s. Silloin taulukon 1 mukaisesti puiden oksat ja nuoret lehtipuut alkavat heilumaan ja ne voivat osua ilmassa oleviin johtimiin. Tällöin syntyy hetkittäisiä maasulkuja puiden ja niiden oksien osuessa johtoihin. Oksien tai puiden osuminen ei yleensä vaikuta verkon toimintaan. Mikäli puu painuu johtoon kiinni hieman pidemmäksi aikaa, voi se aiheuttaa verkossa suojauksen toiminnan ja pikajälleenkytkennän, mutta yleensä sähkönjakelu ei keskeydy pitkäksi aikaa. [18]

Kun tuulen nopeus on 11-20 m/s, lisääntyvät sähköverkolle aiheutuvat ongelmat. Kun tuuli saa liikuteltua suuria oksia, myös johtimet pylväiden välillä alkavat heilua. Tällöin myös leveämmillä johtokaduilla olevat johtimet saattavat osua puihin tai niiden oksiin.

Johtimien päälle voi myös pudota katkenneita oksia, jotka aiheuttavat oikosulkuja ja häiriöitä sähkönjakeluun. [18]

Tuulen nopeuden ylittäessä myrskyrajan 21 m/s, puita alkaa katkeilla ja kaatua juurineen. Tämä tietää isoja ongelmia sähköverkoille, erityisesti metsissä sijaitseville keski- ja pienjänniteverkoille, koska puun kaatuessa johdolle syntyy ainakin maasulku ja mahdollisesti oikosulku. Pahimmassa tapauksessa johto tai jopa tukipylväs katkeaa. Kuvassa 1 on myrsky kaatanut puita sähköjohdolle. Tämä tarkoittaa, että verkon suojaus ei pysty poistamaan aiheutunutta häiriötä, vaan häiriöpaikalle on lähetettävä korjauspartio poistamaan puu johdolta tai korjaamaan verkon vahingoittuneita osia. [18]

Kuva 1. Myrskyn sähköjohdoille kaatamia puita [19]

Myrskyjen puuskat ja syöksyvirtaukset aiheuttavat merkittäviä tuhoja. Ne voivat kaataa kokonaisia metsiä. Jos alueella on sähköverkkoa, puiden kaatuessa johdot katkeilevat ja tukipylväät kaatuvat. Tämän seurauksena kyseinen osa sähköverkosta joudutaan todennäköisesti rakentamaan kokonaan uudestaan.

Vuoden 2010 loppukesällä neljä myrskyä aiheuttivat vahinkoja yhteensä 33 verkonhaltijalle. Myrskyjen tuhoja sähköverkolle lisäsi se, että ne osuivat osin samoille alueille, mutta ne kuitenkin tulivat eri ilmansuunnista. Myrskyjen tulo eri ilmansuunnista aiheutti sähköjohtoja ympäröiviin metsiin suurta rasitusta ja sen seurauksena puita kaatui paljon myös sähköjohdoille. Myrskyt aiheuttivat katkoksia sähkönjakelussa yhteensä 481 000 asiakkaalle. 84,4 % katkoksista kesti alle 12 tuntia, mutta pisin katkos kesti noin 1 000

tuntia. Myrskyjen aiheuttamat tuhot maksoivat verkonhaltijoille yhteensä yli 30 miljoonaa euroa vianselvitys- ja korjauskustannuksina. Lisäksi asiakkaille maksettiin yli 10 miljoonaa euroa vakiokorvauksina yli 12 tuntia kestäneistä sähkönjakelun keskeytyksistä johtuen. [20]

3.1.2 Lumi ja jää

Lumi ja jää aiheuttavat ongelmia yleensä metsissä sijaitseville jakeluverkon osille. Kun sähköjohtojen lähellä on puita, voi niihin kertynyt lumi ja jää painaa ne kiinni sähköjohtoihin. Myös lumen ja jään kertyminen johdoille ja tukipylväisiin voi aiheuttaa ongelmia, jos tukipylväät ovat liian heikkoja tai niiden rakenne on vaurioitunut ja sen seurauksena niiden kestävyys on heikentynyt. Vuonna 2017 lumi- ja jääkuorma aiheutti 16 % sähkönjakelun keskeytyksistä ja 26 % keskeytysajoista [13].

Lumikuorma aiheutuu tykkylumesta. Sitä syntyy, kun ilmassa on suuri määrä kosteutta, kuten sumua tai sumupilveä, jolloin ylempänä maastossa oleviin puihin ja johtoihin voi kertyä tykkylunta. Lisäksi tykkylumen syntyminen vaatii fysikaalisen tarttumismekanismin, joka kiinnittää veden puustoon. Myös tuuli vaikuttaa tykkylumen kertymiseen. Kohtalainen 3-6 m/s puhaltava tuuli edesauttaa tykkylumen kertymistä, mutta tuulen yltyessä, se alkaa pudottaa tykkylunta puista. Lisäksi lämpötilan nouseminen pudottaa tykkylunta puista. [21]

Puihin kertyessään tykkylumi painaa niitä alaspäin. Tällöin puu tai sen oksat voivat painua kiinni sähköjohtoihin, jolloin seurauksena on maa- tai oikosulku. Jos puun painumisen seurauksena ei ole pysyvää vikaa, voi tilanne uusiutua puun painuessa uudestaan johdolle. Kuvassa 2 nähdään tykkylumen taivuttamia puita, jotka osuvat sähköjohtoon. Toisaalta ongelmia voi aiheutua myös tykkylumen pudotessa puusta ja puun noustessa. Jos puu on tykkylumen painosta taipunut sähköjohdon alle, voi se nousta kiinni sähköjohtoon sen alapuolelta.

Kuva 2. Tykkylumi painanut puita kiinni sähköjohtoon [22]

Myös johtimiin ja sähköverkon tukipylväisiin kertyvät lumi ja jää voivat aiheuttaa ongelmia. Jos tukipylväiden rakenne on liian heikko, voi lumen ja jään paino rikkoa sen liitoksia, aiheuttaa vääntymisiä sen rakenteisiin tai tukipylväs voi kaatua. Johdot saattavat painua myös niiden alla kasvavaan kasvillisuuteen kiinni tukipylvään vääntyessä. Sähköverkon rakenteisiin kertyvä tykkylumi voi siis aiheuttaa fyysistä vahinkoa verkolle sekä maa- tai oikosulkuja. [18]

3.1.3 Ukkonen ja salamat

Ukkonen ja salamat aiheuttavat häiriöitä niin siirto- kuin jakeluverkossa. Salamaniskut aiheuttavat jyrkkiä transienttiylijännitteitä. Salamaniskun osuessa sähköverkon maadoitettuun tai jännitteiseen osaan, sen aiheuttama jänniterasitus syntyy salamavirran kulkiessa verkon erilaisten impedanssien kautta. Avojohdolle osuvista salamaniskuista noin 75-80 % osuu pylväälle tai sen läheisyyteen. Siirtoverkon avojohtoja pyritään suojaamaan suorilta salamaniskuilta vaihejohtimen yläpuolelle sijoitettavilla ukkosjohtimilla. Niiden tehtävänä on vetää puoleensa johtoon suuntautuvat salamaniskut ja niillä voi olla myös muita tehtäviä, jotka liittyvät relesuojaukseen sekä vaara- ja häiriöjännitteiden pienentämiseen. Keskijänniteverkossa käytetään ylijännitesuojia, venttiilisuojia ja kipinävälejä. Suomessa ylijännitesuojat on sijoitettu sähköasemille ja yleisesti niillä suojataan vain tärkeimpiä laitteita, kuten tehomuuntajia. [23] Vuonna 2017 ukkonen aiheutti 4 % sähkönjakelun keskeytyksistä ja 2 % keskeytysajoista [13].

Salamaniskut aiheuttavat ylijännitteitä sähköverkkoon kolmella eri tavalla: suoralla osumalla jännitteiseen johtimeen, takaiskulla ja induktiolla. Salamaniskun osuessa suoraan vaihejohtimeen salamavirta jakautuu johdon molempiin suuntiin eteneviin ylijänniteaaltoihin. Suorien iskujen aiheuttamat ylijännitteet ovat yleensä suuruudeltaan useita megavoltteja. Salaman iskiessä sähköverkon maadoitettuun osaan voi syntyä ylilyönti maadoitetusta osasta vaihejohtimeen. Kyseessä on takaisku eli takaperoinen ylilyönti. Takaisku tapahtuu todennäköisesti silloin, kun salamavirta on suuri tai maadoitusolosuhteet ovat vaikeat. Takaiskun suuruuteen vaikuttavat monet seikat, kuten avojohdon jännitelujuus sekä tukipylvään maadoitusresistanssi. Kun salama iskee johdon tai sähkölaitteen välittömään läheisyyteen, ylijännite aiheutuu pääpurkausvirran sähkömagneettisesta induktiosta. Induktiolla syntyneet ylijännitteet ovat yleensä suuruusluokaltaan 200-300 kV. Indusoituneet ylijännitteet ovat yleisimpiä ukkosen aiheuttamia ylijännitteitä jakeluverkossa. Siirtoverkossa suorat salamaniskut ja takaiskut ovat merkittävimpiä ylijännitteiden aiheuttajia. [23]

Ukkosen ja salamoiden synnyttämät ylijännitteet aiheuttavat oiko- ja maasulkuja sähköverkossa. Viat johtuvat ylijännitteiden aiheuttamista valokaarista. Yleensä verkon suojaus pystyy poistamaan valokaarien aiheuttamat viat. Ylijännitteet voivat kuitenkin rikkoa sähköverkon komponentteja, kuten muuntajia, ja ylijännitteen päästessä kulkeutumaan maakaapeliverkkoon, voi maakaapeli vioittua. Tällöin seurauksena on pidempiä häiriöitä sähkönjakelussa, koska syntyneet viat vaativat korjaamista. Salamaniskun osuessa siirtoverkkoon se aiheuttaa vian epäsuorasti myös jakeluverkkoon. Salamaniskusta johtuva magneettikenttä aiheuttaa induktion kautta jakeluverkon ilmassa oleviin johtimiin jännitetransientin. Tämä jännitetransientti purkautuu ylilyöntinä eristimissä tai läpilyöntinä kipinäväleissä, mistä seurauksena on maasulku. [18]

3.2 Sähköntuotantoon kohdistuvat sääriskit

Sääilmiöt eivät vaikuta kovin paljoa itse sähköntuotantolaitoksiin. Alavilla mailla sijaitsevat laitokset voivat altistua rannikko-, vesistö- ja rankkasadetulville. Nämä eivät välttämättä aiheuta vahinkoa itse laitokselle, mutta esimerkiksi lauhdeveden kierrätys saattaa vaikeutua. Ilmaston pidemmät sääolot voivat vaikuttaa sähköntuotannossa käytettävien polttoaineiden saatavuuteen. Esimerkiksi sateiset kesät vähentävät turpeen tuotantoa ja leudot talvet vaikeuttavat biomassan hankintaa. Sää- ja ilmastoilmiöt aiheuttavat enemmän ongelmia uusiutuvista energianlähteistä tuotetun sähkön kanssa. [12,24]

Pitkään jatkuvat kuivat kaudet vaikuttavat vesivoiman tuotantoon. Riippuen vähäsateisen jakson pituudesta ja sen laajuudesta, sillä voi olla vaikutuksia yksittäisiin voimalaitoksiin tai koko pohjoismaiseen sähkömarkkinaan. Tuulivoiman tuotanto on vähäistä tai loppuu kokonaan vähätuulisissa olosuhteissa. Myös liian kova tuuli aiheuttaa tuulivoiman tuotannon pysähtymisen. Tämä johtuu siitä, että liian kovat tuulet aiheuttavat kasvavaa mekaanista rasitusta, joka voi vaurioittaa tuulivoimalaitosta. Sääolosuhteet vaikuttavat merkittävästi aurinkosähkön tuotantoon. Luonnollisesti pilvisellä säällä tuotanto jää pienemmäksi kuin auringon paistaessa kirkkaalta taivaalta. [12,25]

3.3 Sääriskien aiheuttamien häiriöiden vaikutukset

Vuoden 2013 syyskuussa voimaan tulleen uuden sähkömarkkinalain tavoite oli parantaa sähköverkkojen toimitusvarmuutta ja siten pyrkiä pienentämään sään aiheuttamia katkoja sähkönjakelussa. Uudistetun sähkömarkkinalain momentissa 51 määrätään: ”Sähkönjakeluverkko on suunniteltava, rakennettava ja ylläpidettävä siten, että jakeluverkon vioittuminen myrskyn tai lumikuorman seurauksena ei aiheuta asemakaava-alueella asiakkaille yli 6 tuntia kestävää sähkönjakelun keskeytystä eikä muulla alueella yli 36 tuntia kestävää keskeytystä.” Uuteen tavoitteeseen on määrä päästä portaittain 15 vuoden kuluessa. Lisäksi asiakkaille sähkökatkoista maksettavia vakiokorvauksia korotettiin. [26]

Sähkömarkkinalain uudistus on lisännyt merkittävästi jakeluverkkojen maakaapelointiastetta. Vuodesta 2009 vuoteen 2013 mennessä keskijänniteverkossa maakaapelointiaste kasvoi vain 3,6 % ja vuodesta 2013 vuoteen 2017 mennessä keskijänniteverkossa maakaapelointiaste kasvoi 8 % eli maakaapelointiasteen kasvunopeus tuplaantui. Pienjänniteverkossa kasvunopeus ei ole ollut yhtä suuri, mutta kasvunopeus on silti lisääntynyt. Vuoteen 2028 mennessä keskijänniteverkon maakaapelointiasteen on arvioitu olevan 47 % ja pienjänniteverkon 65 %. Maakaapelointi ei kuitenkaan ole kustannustehokkain tapa toimitusvarmuuden parantamiseen kaikissa olosuhteissa. Esimerkiksi maaseutumaisten verkonhaltijoiden keskijänniteverkon maakaapelointiaste nousee keskimäärin vain 26 prosenttiin kehittämissuunnitelmien mukaan. Maaseutumaisessa ympäristössä toimivat verkonhaltijat katsovat saavuttavansa laatuvaatimukset muilla keinoilla, esimerkiksi siirtämällä ilmassa olevia johtimia teiden varsiin. [8]

4. SÄHKÖENERGIAJÄRJESTELMÄ JA IHMISEN TOIMINNASTA AIHEUTUVAT RISKIT

Ihminen voi omalla toiminnallaan aiheuttaa monenlaista vahinkoa sähköenergiajärjestelmille. Tässä työssä tarkastellaan miten ihminen voi toiminnallaan vahingoittaa järjestelmää fyysisesti tai kybertoiminnan avulla. Järjestelmän suuren koon ja maantieteellisesti hajautetun sijainnin vuoksi siinä on myös paljon haavoittuvuuksia. Sen osien, kuten sähköasemien, sähköjohtojen sekä voimalaitosten, fyysinen vahingoittaminen tai tuhoaminen on yksi mahdollisista keinoista järjestelmän vahingoittamiseen. Kyberiskuilla voidaan vahingoittaa ja tuhota järjestelmän fyysisiä osia tai häiritä järjestelmän toimintaa. Fyysisen vahingoittamisen ja kyberiskun yhdistelmä on myös mahdollinen keino järjestelmän vahingoittamiseen. Yhteiskunnan kriittisenä infrastruktuurina sähköenergiajärjestelmä on mahdollinen kohde myös terrorismille. Sen vahingoittaminen voi lamaannuttaa yhteiskunnan toiminnan pitkäksikin aikaa. [27,28]

Yleensä vahingoittaminen on tahallista ja tahallisen vahingoittamisen takana on aina motiivi, halu vahingoittaa jotain tai aiheuttaa vaikeuksia joillekin tahoille. Tämän vuoksi sähköenergiajärjestelmän täydellinen suojaaminen on mahdotonta. Järjestelmää ja sen suojauksia voidaan parantaa, jotta vahingoittamisyrityksillä ei olisi niin suuret seuraukset ja niistä palautuminen olisi helpompaa.

4.1 Sähköenergiajärjestelmä ja fyysinen vahingonteko

Sähköenergiajärjestelmän kaikki osat ovat alttiita niiden fyysiselle vahingoittamiselle. Sähköntuotantolaitokset eivät ole helppoja kohteita vahingontekijöille, koska usein voimalaitoksen sähköä tuottava generaattori sijaitsee laitoksen sisällä ja siellä työskentelee henkilökuntaa, jotka tarjoavat sille suojaa. Lisäksi laitos voi olla suoja-aidan sisäpuolella ja sen ympärillä voi olla turvalaitteita. Kuitenkaan useimpia laitoksia ei ole suojattu turvalaitteistoilla, poikkeuksena ydinvoimalaitokset. [28] Mahdollinen vahingonteko sähköntuotantolaitokseen voi vahingoittaa sitä ja irrottaa sen verkosta. Koska sähköenergiajärjestelmä ja siirtoverkko on rakennettu N – 1 -periaatteella, kestää järjestelmä isoimmankin voimalaitoksen irtoamisen verkosta [1]. Tämän vuoksi vahingonteoilla pitäisi vahingoittaa useampaa isoa voimalaitosta, jotta järjestelmän toiminta kärsisi siitä.

Sähkönsiirtojärjestelmä on haavoittuvaisempi, koska se sijaitsee hajautetusti ympäri maata, jotta kaikki kuluttajat saavat sähköä. Siihen kuuluu tuhansia kilometrejä siirto-

verkkoja sekä jakeluverkkoja ja satoja sähköasemia, jotka eivät ole vartioituja. Järjestelmää ei ole suunniteltu kestämään tai palautumaan nopeasti vahingoista, jotka kohdistuvat samanaikaisesti moniin järjestelmän komponentteihin. Yhdysvaltalaisen raportin mukaan pieni määrä asiansa osaavia henkilöitä pystyy vahingoittamaan sähköenergiajärjestelmää vakavasti. Yhteiskunnan kriittisenä infrastruktuurina se on houkutteleva kohde vahingonteolle sekä terrorismille. Sähkönsiirtojärjestelmän monien osien sijainti syrjäisillä seuduilla takaa pienen riskin vahingontekijän kiinni jäämiselle. [28] Järjestelmän osien, kuten siirtoverkon johtojen ja sähköasemien, löytäminen on helppoa. Esimerkiksi Suomessa Fingridillä on internetissä kartta kantaverkon komponenttien sijainneista. [29] Lisäksi kaikkien saatavilla olevien satelliittikuvien avulla voi paikantaa järjestelmän eri komponenttien sijainteja. [28]

Siirtojärjestelmää voidaan vahingoittaa monin tavoin. Fyysiset laitokset ja komponentit ovat alttiina mekaanisille sekä erilaisten ammusten ja räjähdysten aiheuttamille vahingoille. Siirtoverkon sähköasemat ovat suhteellisen helppo kohde vahingonteolle, koska ne sijaitsevat yleensä syrjässä ja niiden suojana on usein vain aita. Niitä voidaan vahingoittaa tunkeutumalla sinne tai iskemällä ulkopuolelta esimerkiksi ammuksilla tai räjähteillä. Suurten sähköasemien komponenttien korvaavia osia on vaikea saada, koska ne on usein rakennettu tilaustyönä. Tämän vuoksi vahinkojen korjaaminen voi kestää pitkään. Myös siirtoverkon johdot ja pylväät sijaitsevat usein syrjäisellä seudulla ja niitäkin on helppo vahingoittaa. Esimerkiksi eristimien ampuminen aiheuttaa oikosulun yhteen vaiheeseen ja pylvään rakenteen heikentäminen voi aiheuttaa sen kaatumisen. Tällöin seurauksena on kolmivaiheinen oikosulku ja yhden pylvään kaatuminen voi aiheuttaa dominoefektin, jolloin useita pylväitä kaatuu. Siirtoverkon johtojen ja pylväiden viat on kuitenkin helpompi korjata. Ne voidaan korjata niin nopeasti kuin uusia pylväitä on saatavilla. Siirtoverkon komponenttien vahingoittamisen seurauksena koko järjestelmä voi kaatua, jos samaan aikaan toteutetaan iskuja useampaan kohtaan verkkoa, esimerkiksi useamman sähköaseman muuntajiin ja siirtoverkon suurimpiin johtoihin. Siirtojärjestelmän valvonta- ja hallintakeskukseen hyökkääminen heikentäisi merkittävästi järjestelmän toiminta- sekä korjauskykyä siksi, että se eliminoisi tärkeitä hallinta-, ohjaus- ja viestintäjärjestelmiä. Tällainen isku on kuitenkin vaikeampi toteuttaa, koska ohjauskeskukset sijaitsevat usein keskeisimmillä paikoilla ja niissä työskentelee henkilökuntaa koko ajan. Jakeluverkko ei ole yhtä houkutteleva kohde kuin siirtoverkko. Tämä johtuu siitä, että jakeluverkon komponenttien vahingoittaminen aiheuttaa yleensä vain paikallisia katkoja sähkönjakelussa eikä vaikuta koko järjestelmän toimintaan. Lisäksi jakeluverkon vahinkojen korjaaminen on helpompaa, koska sen komponenttien varaosia on hyvin saatavilla. [28,29]

Sähkönkuluttajiin kohdistuvalla vahingoittamisella ei ole kovin suuria vaikutuksia itse järjestelmän toimintaan tai yhteiskuntaan. Yleensä hyökkäyksen vaikutuksen kokisi vain se sähkönkuluttaja, jota vastaan hyökkäys kohdistui. Poikkeuksena ovat tilanteet, joissa hyökkäykset kohdistuisivat koordinoidusti esimerkiksi kemianlaitoksiin tai kohteisiin, jotka tarjoavat yhteiskunnan toiminnan kannalta keskeisiä palveluita. Tehokkaampi tapa vaikuttaa sähkönkuluttajiin onkin hyökätä siirtoa tai tuotantoa vastaan, koska silloin vaikutuksen kokee useampi kuluttaja kuin vain se tai ne, joihin hyökkäys kohdistuu. [28]

Sähköenergiajärjestelmän vahingoittaminen on esimerkiksi terroristien sekä alueellisten ryhmittymien keino pyrkiä horjuttamaan hallitsijoiden auktoriteettia sekä valtaa ja vaikeuttaa päivittäistä elämää. Esimerkiksi Kolumbiassa FARC (Fuerzas Armadas Recolucionarias de Colombia) on tehnyt satoja hyökkäyksiä maan sähkönsiirtojärjestelmään tavoitteenaan heikentää hallituksen valtaa. [28] Venezuela on kärsinyt alkuvuodesta 2019 monista pahoista sähkökatkoista. Maan hallitus on väittänyt, että katkot ovat aiheutuneet hallituksen vastustajien iskuista sähkönsiirtojärjestelmään sekä maan suurimpaan sähköntuotantolaitokseen. Hallituksen vastustajat taas väittävät, että hallitus on itse vahingoittanut järjestelmää. Ongelmat ovat voineet johtua myös Venezuelan sähköenergiajärjestelmän huonosta kunnosta, koska sen ylläpitoa ja kunnostusta on laiminlyöty vuosien ajan. Mahdollisilla iskuilla on kuitenkin pyritty vaikuttamaan maassa vallitseviin valtasuhteisiin. [28,30,31]

4.2 Sähköenergiajärjestelmä ja kyberriskit

Sähköenergiajärjestelmän fyysisiä osia ovat esimerkiksi voimalaitokset, sähköasemat ja sähköjohdot. Näiden rinnalla, sähköenergiajärjestelmän toiminnan taustalla, toimii digitaalinen ulottuvuus, jota kuvaa sana kyber. Tässä digitaalisessa ulottuvuudessa kulkee tietoa eri järjestelmien, laitteiden sekä tahojen välillä, sen avulla ohjataan laitteiden ja prosessien toimintaa sekä valvotaan järjestelmän kuntoa ja toimintaa. Nykyinen yhteiskunta ei toimi ilman kybermaailmaa. Kyberturvallisuudella pyritään turvaamaan sähköistettyjen ja verkkoon liitettyjen toimintojen turvallisuus sekä toiminta kyberuhkia ja -hyökkäyksiä vastaan.

Kyberuhkia on monenlaisia, osaa käytetään vakoiluun, toisia rikollisuuteen ja joitakin sodassa. Kyberuhkia eivät ole pelkästään erilaiset haittaohjelmat. Jo järjestelmän suunnitteluvaiheessa tehdyt ratkaisut vaikuttavat sen kyberturvallisuuteen, esimerkiksi valitut tietoturvaratkaisut ja niiden ylläpito sekä järjestelmien riittävä fyysinen suojaus. Myös henkilöstön osaaminen ja koulutus on tärkeää, jotta he eivät toiminnallaan vaaranna kybertuvallisuutta. [32,33]

Suurimpia kyberuhkia ovat esimerkiksi haittaohjelmat, kuten vakoiluohjelmat ja madot/troijalaiset, palvelunestohyökkäykset ja bottiverkot, verkkourkinta sekä kohdistetut hyökkäykset. Haittaohjelmien tarkoituksena on aiheuttaa ongelmia ja häiriöitä tietokoneohjelmissa. Vakoiluohjelma on haittaohjelma, joka kerää tietoja tietokoneesta ja sen käyttäjästä ja voi aiheuttaa tietokoneen hidastumista. Madot ovat vahinkoa aiheuttavia ohjelmia, ne voivat esimerkiksi tuhota tiedostoja, estää käyttöä tai aiheuttaa internetin toimintahäiriöitä. Ne voivat monistua ja jakaa itseään eteenpäin kohdejärjestelmän haavoittuvuuksien avulla. Troijalaiset ovat huomaamattomasti kohdejärjestelmään vietäviä ohjelmia, jotka on naamioitu hyödylliseksi ohjelmaksi. Ne voivat esimerkiksi avata takaportin järjestelmään tai varastaa dataa. Osa haittaohjelmista voi levitä verkkojen kautta järjestelmiin ja osa voi päästä järjestelmään sen käyttäjien huolimattoman toiminnan seurauksena, esimerkiksi muistitikkujen tai sähköpostien liitteiden kautta. [32,33]

Palvelunestohyökkäyksillä pyritään tekemään resurssista tai palvelusta tavoittamaton sen oikeille käyttäjille jumittamalla se. Bottiverkot ovat yhteen kytkettyjen kaapattujen tietokoneiden verkkoja, joiden avulla bottiverkon käyttäjä voi toteuttaa esimerkiksi palvelunestohyökkäyksen. Verkkourkinnassa pyritään jäljittelemään oikeita sähköposteja ja kirjautumissivuja ja niiden avulla saamaan käyttövaltuuksiin liittyviä tietoja. Kohdistetut hyökkäykset ovat yleensä pitkän ajan kuluessa toteutettuja ja ne kohdistuvat tiettyä organisaatiota vastaan. Kohdistettu hyökkäys koostuu tiedonkeruuvaiheesta ja hyökkäysvaiheesta, jossa voidaan käyttää todella edistyneitä hyökkäystekniikoita. [33]

4.2.1 Kyberturvallisuus

Kyberturvallisuus on laajempi kokonaisuus kuin tietoturvallisuus. Kyberturvallisuuden tavoitteena on turvata kybermaailman ja fyysisen maailman luoma kokonaisuus. ”Tietoturvalla pyritään estämään tiedon tuhoutuminen, leviäminen väärille tahoille sekä asiasisällön muutokset” [32]. Kybermaailmassa toimii monia eri organisaatioita, kuten valtioita, yrityksiä sekä yksilöitä, minkä vuoksi kyberturvallisuus onkin monien osatekijöiden summa. Kybermaailman kehittyessä nopeasti on siellä toimivien tahojen oltava ketteriä ja dynaamisia, koska hyökkääjät kehittävät koko ajan uusia ja parempia keinoja hyökkäyksiinsä. Tämän seurauksena on puolustautuvien tahojenkin kehitettävä omia puolustusmekanismejaan koko ajan. [33]

Internetin, IP-protokollan sekä Ethernet-pohjaisten lähiverkkojen lisääntyminen teollisuusautomaatiolaitteiden rakennusosina on lisännyt sähköenergiajärjestelmän kyberriskejä. Kyberturvallisen toimintaympäristön rakentaminen ja ylläpito on jatkuva ja kokonaisvaltainen prosessi. Kyberuhkiin varauduttaessa on tärkeää pystyä ennaltaehkäise-

mään sekä ennakoimaan tulevia uhkia. Myös ajankohtaisen ja oikean tilannekuvan ylläpito ja nopea palautumiskyky ovat tärkeitä. Kybermaailmassa on oltava kerroksittainen suojaus, koska mikään kerros ei yksinään voi antaa sataprosenttista suojaa. Kerroksittainen suojaus lisää mahdollisuuksia havaita ja pysäyttää tunkeutuja ennen kuin vahinkoa ehtii syntymään. Esimerkiksi yrityksen palomuurijärjestelmä, tunkeutumisenestojärjestelmä ja www-palvelimen virustorjunta kuuluvat kerroksittaiseen suojaukseen. [33,34]

4.2.2 Sähkönsiirtoon kohdistuvat kyberriskit

Koska sähköä ei voida varastoida suuria määriä, on sähköä tuotettava juuri kulutuksen suuruinen määrä ja tuotettu sähkö siirrettävä oikeaan paikkaan sähköverkon avulla. Verkostoautomaatiojärjestelmä tarkoittaa tietojärjestelmää tai automaatiolaitetta, jolla säädetään sähköverkon suureita, ohjataan sen kytkentätilaa tai suojataan verkon toimilaitteita. Verkostoautomaatiojärjestelmän tärkeitä osia ovat tietoliikenneyhteydet ja tietokannat, joiden avulla järjestelmät toimivat halutulla tavalla. [34]

Järjestelmien käyttäjät ovat yleisin uhka tietoturvalle, he voivat osaamattomuuttaan tai huolimattomuuttaan tuhota tai pilata tietoja. Myös järjestelmien laite- ja ohjelmistoviat ovat yleinen tietoturvauhka, koska niiden viat voivat paljastua vasta käyttöönoton jälkeen tuotannollisessa käytössä. Kyberriskien osalta sähköverkon haavoittuvuus voidaan jakaa kolmeen osaan, jotka ovat hallinnon haavoittuvuus, verkostoautomaatiojärjestelmän haavoittuvuus ja tietoliikenneverkon haavoittuvuus. [34]

Hallinnon haavoittuvuus johtuu huonosta ohjeistuksesta ja dokumentaatiosta, henkilöstön koulutuksen riittämättömyydestä sekä puutteellisesta johtamisesta. Taulukossa 2 on esitelty ja kuvattu hallintoon liittyviä haavoittuvuuksia. [34]

Taulukko 2. Hallinnon haavoittuvuuksia [34]

Haavoittuvuus	Kuvaus
Tietoturvapolitiikan ja johtamisen puutteet	Verkostoautomaatiojärjestelmien erityispiirteitä ei ole huomioitu tietoturvapolitiikkaa ja –ohjeistusta laadittaessa. Verkostoautomaatiojärjestelmien tietoturvan johtamista ei ole vastuutettu. Tietoturvan systemaattista seurantaa ja säännöllistä raportointia ei ole järjestetty tai vastuutettu.
Riskikartoituksen puutteet	Toiminnan jatkuvuutta uhkaavia riskejä ei ole tunnistettu riittävästi tai ennalta ehkäiseviin toimenpiteisiin riskien vaikutusten vähentämiseksi tai eliminoimiseksi ei ole ryhdytty
Henkilöstön tietoturvaosaaminen ja tietous puutteellista	Henkilöstön koulutus ja informointi on puutteellista. Ilman ajantasaista tietoturvapolitiikkaa ja –ohjeistusta, joihin henkilöstö on perehdytetty, ei todennäköisesti rakenneta ja ylläpidetä tietoturvallista verkostoautomaatioympäristöä
Haavoittuva tietojärjestelmäarkkitehtuuri	Verkostoautomaatiojärjestelmä on rakenteellisesti puutteellinen eikä sitä ole varustettu tietoturvauhkia estävällä, tunnistavilla ja eliminoivilla laitteilla ja ohjelmistoilla. Tietoliikenneverkkoa ei ole segmentoitu ja verkostoautomaatiojärjestelmien käyttöoikeuksien hallinta on leväperäistä tai muuten riittämätöntä. Ulkoisia tietoliikenneyhteyksiä ei ole suojattu riittävästi
Järjestelmien ja laitteiden rakentamisen ja häiriöpalauttamisen ohjeistus puutteellista	Järjestelmien suunnittelussa ja rakentamisessa käytettävää ohjeistusta tietoturvan huomioimisesta ei ole tai se on puutteellista. Jatkuvuussuunnittelun tuloksena syntyviä toipumissuunnitelmia ei ole tai ne ovat puutteellisia. Järjestelmien toipumissuunnitelman laadintaa ei ole vastuutettu.
Verkostoautomaatiojärjestelmän ja sitä tukevan tietoliikenneverkon konfiguraation hallinta puuttuu tai on riittämätön	Toimiva tietoturva edellyttää jatkuvaa ja ajantasaista järjestelmien ominaisuuksien ja parametroinnin hallintaa erityisesti tehtäessä järjestelmiin muutoksia. Parametroinnit ovat puutteellisia tai virheellisiä ja käytetään järjestelmien oletusasetuksia (tehdasasetuksia)
Puuttuvat auditoinnit tai katsastukset	Ulkopuolisten riippumattomien asiantuntijoiden on auditoitava säännöllisesti verkostoautomaatio- ja tietoliikennejärjestelmien rakenne, dokumentaatio, tietoturvapolitiikka/ohjeistus sekä käytön ja ylläpidon toimintatavat ja prosessit. Auditoijien on raportoitava vakavat löydökset ja tehtävä ehdotus niiden korjaamiseksi
Puutteellinen käyttöoikeuksien hallinta	Puutteet käyttöoikeuksien hallinnoinnissa ja autentikoinnin päivityksissä (esimerkiksi salasanojen vaihtaminen) lisäävät tunkeutumisriskiä tai antavat käyttäville liian laajoja oikeuksia tehdä järjestelmään haitallisia muutoksia

Verkostoautomaatiojärjestelmä koostuu laitteista ja varusohjelmista, kuten käyttöjärjestelmästä. Järjestelmäalustassa ajetaan sovellusohjelmia, jotka tuottavat toiminnallisuuden, sekä mahdollisesti suojausohjelmia. Verkostoautomaatiojärjestelmän haavoittuvuus voidaan jakaa kolmeen osaan, jotka ovat alustan rakenteen haavoittuvuus, fyysiset haavoittuvuudet sekä varus- ja sovellusohjelmistojen haavoittuvuudet. Alustan rakenteen haavoittuvuuksiin liittyvät muun muassa salasanojen paljastuminen ja ohjelmistojen päivitysten puutokset. Fyysisiin haavoittuvuuksiin kuuluvat muun muassa turvattomat ulkoiset yhteydet ja fyysisen suojauksen riittämättömyys. Varus- ja sovellusohjelmistojen

haavoittuvuuksia ovat muun muassa palvelunestohyökkäykset ja tarpeettomien prosessien ajaminen. Verkostoautomaatiojärjestelmän haavoittuvuuksia on esitelty ja kuvailtu taulukoissa 3, 4 ja 5. [34]

Taulukko 3. Verkostoautomaatiojärjestelmän alustan rakenteen haavoittuvuuksia [34]

Haavoittuvuus	Kuvaus
Varus- ja sovellusohjelmistojen korjauspäivitykset puutteellisia	Automaatiojärjestelmiin tehtävät ohjelmistokorjaukset ja päivitykset ovat työläitä ja vaativat perusteellista testausta ennen tuotantoympäristöön asentamista. Tämä mahdollistaa haittaohjelmille laajan aikaikkunan tehdä hyökkäyksiä
Varus- ja sovellusohjelmistot vanhentuneita ja poistuneet ylläpidon piiristä	Ohjelmistot voivat olla niin iäkkäitä, että niitä ei enää ylläpidetä eikä korjauspäivityksiä ole saatavana, vaikka uusia haavoittuvuuksia löydettäisiin
Järjestelmän käyttöönotto ilman perusteellista testausta	Järjestelmän testaus voi olla puutteellista niin toimittajan kuin tilaajankin puolelta. Varsinkin tietojärjestelmissä voi olla paljon puutteita ja virheitä käytön alkaessa. Nämä voivat sisältää hyvin moninaisia uhkia tietoturvalle
Ohjelmistojen päivityksiä on toteutettu puutteellisin testauksin	Tietoturvapäivitysten puutteellisista testauksista johtuen järjestelmässä voi esiintyä toimintahäiriöitä tai se voi kaatua kokonaan. Ohjelmistopäivitysten ohjeistus tulisi laatia ja dokumentoida
Käytetään oletusparametrointia	Oletusparametrien käyttäminen varus- ja tietoliikenneohjelmistoissa jättää auki olevia tietoliikenneportteja sekä mahdollistaa haitallisten sovellusten ajamisen palvelimissa ja työasemissa
Kriittisistä järjestelmä-konfiguraatioista ja –parametreista ei ole varmuuskopioita	Järjestelmän haavoittuessa, kaatuessa tai toimiessa muutoin puutteellisesti järjestelmä palautetaan puutteellisilla tai vanhentuneilla asetuksilla ja tietomalleilla. Järjestelmä ei toimi oikein
Suojaamattomat kannettavat laiteet ja massamuistit	Luottamuksellinen aineisto tai muutoin sensitiivinen data voi joutua sopimattomalle taholle, mikäli niitä säilytetään huolimattomasti esimerkiksi salaamattomilla laitteilla tai muistivälineillä
Salasanat eivät ole käytössä	Verkostoautomaatiojärjestelmien osajärjestelmät ja työasemat tulee olla varustettu pääsyn ja käyttöoikeuksien hallinnalla asiattoman käytön estämiseksi
Salasanan paljastuminen	Salasanojen huolimattoman säilytyksen tai muun käsittelyn takia ne päätyvät asiattomiin käsiin aiheuttaen hyökkäysriskin
Salasanan riittämätön vahvuus	Hyökkääjä murtaa liian lyhyet, yksinkertaiset tai muutoin helposti johdettavat salasanat

Taulukko 4. Verkostoautomaatiojärjestelmän fyysisiä haavoittuvuuksia [34]

Uhka / Haavoittuvuus	Kuvaus
Järjestelmälaitteiden riittämätön fyysinen suojaus	Valvomo- ja laitetilojen sekä sähköasemien fyysinen suojaus ja kulunvalvonta ovat riittämättömiä, mikä voi mahdollistaa asiattoman pääsyn laitetiloihin ja laitteisiin. Miehittämättömillä asemilla ei ole sähköistä video- tms. valvontaa. Riski laajalle kirjolle erilaisia haitallisia toimenpiteitä sekä uhka luonnononnettomuuksien ja poikkeuksellisten sääilmiöiden aiheuttamille vaurioille
Turvattomat ulkoiset yhteydet	Verkostoautomaatiojärjestelmien tietoverkkoon tulevat, huonosti suojatut ulkoiset yhteydet mahdollistavat asiattoman pääsyn laitteisiin/järjestelmiin. Palomuurit, DMZ-alueen välityspalvelimet etäkäytön RAS-palvelimet tms. ja IDS/IPS-järjestelmät ovat välttämättömiä turvallisen tietoverkon yhdysliikennekäytävissä. Suorat yhteydet julkiseen verkkoon automaatioverkosta eivät ole suositeltavia. Jos niitä on rakennettava pakottavista syistä, on niissä käytettävä lisäksi vahvaa salausta ja käyttäjien vahvaa autentikointia
Runsaasti järjestelmäliitäntöjä	Suuri määrä järjestelmistä lähteviä liityntöjä muihin järjestelmiin vaikeuttaa dataliikenteen hallinnointia ja se voi mahdollistaa asiattoman tiedonvälityksen järjestelmästä tai tietoverkosta toiseen
Dokumentoimattomat laite- ja ohjelmistokokoonpanot	Puutteellisesti dokumentoidut laite- ja ohjelmistokokoonpanot mahdollistavat asiattomien osien liittämisen järjestelmään sekä vaikeuttavat palauttamistoimenpiteitä kriisitilanteissa
EMC-häiriöt ja EMP-suojaus	Puutteellinen suojaus sähkömagneettisilta häiriöiltä voi aiheuttaa laitteiden toimintahäiriöitä ja virhetoimintoja erityisesti sähköasemilla kytkentätilanteissa ja ylivirtojen tai ylijännitteiden esiintyessä (esimerkiksi salamointi). Puutteellinen EMP-suojaus (Elektromagneettinen pulssi) altistaa elektroniset laiteet sähkömagneettiselle pulssille elektronisessa sodankäynnissä, seurauksena laitteiden tuhoutuminen
Varmentamaton tehonsyöttö	Kriittisten laitteiden varmentamaton tehonsyöttö tai riittämätön varakäyntiaika voi johtaa järjestelmän kaatumiseen tehonsyötön vikatilanteessa. Jotkin laitteet saattavat parametroitua virheellisesti tehonsyötön palauduttua tai laitteen elektroniset komponentit saattavat vioittua katkoksen yhteydessä
Puutteellinen ilmastointi ja kosteuden säätö	Elektroniset laiteet vanhenevat ja vikaantuvat ennen aikaisesti liian kuumassa ja/tai kosteassa käyttöympäristössä. Modernit prosessoripohjaiset laitteet voivat suojatoimenpiteenä sammuttaa itsensä tai siirtyä alennetun suorituskyvyn tilaan
Varmennusten puuttuminen	Kriittisten laitteiden tai tietoliikenneyhteyksien varmennusten puuttuminen voi johtaa järjestelmän toimimattomuuteen vikatilanteessa

Taulukko 5. Varus- ja sovellusohjelmistojen haavoittuvuuksia [34]

Uhka / Haavoittuvuus	Kuvaus
Puskurin ylivuoto	Ohjelmistoissa voi olla puskureiden ylivuotohaavoittuvuuksia, joita hyökkääjät voivat hyödyntää, mikäli ne ovat tiedossa
Ohjelmistojen turvaominaisuudet eivät ole oletusarvoisesti päällä	Turvaominaisuudet voivat olla oletusarvoisesti pois päältä tai ne on voitu sulkea, kaikki tietoliikenneportit auki jne. Turvaominaisuuksista ei ole hyötyä, mikäli ne eivät ole käytössä
Palvelunestohyökkäykset (DoS)	Huonosti suojattuun verkostoautomaatiojärjestelmään voi kohdistua järjestelmäresursseja voimakkaasti kuormittava hyökkäys, joka estää tai hidastaa normaalia palvelutuotantoa. Tämä ei ole ongelma asianmukaisesti rakennetussa järjestelmäarkkitehtuurissa oleville verkostoautomaatiojärjestelmille, mutta hyökkäys voi kaataa esimerkiksi verkkoyhtiön nettisivut
Tietopakettien virheellinen käsittely	Joissain verkostoautomaatiojärjestelmissä voi esiintyä virhetoimintoja, mikäli ne vastaanottavat korruptoituneita tai tahallisesti virheellisenä lähetettyjä tietopaketteja sisältäen esimerkiksi ei sallittuja muuttujien arvoja
Turvattomien tietoliikenne-protokollien käyttäminen	Käytönvalvontajärjestelmissä yleisesti käytetyt protokollat (esimerkiksi IEC 60870-5-101 ja -104, DNP3 vanhemmat versiot ja Modbus) eivät rakenteellisesti sisällä tietoturvaominaisuuksia ja ovat siten hyvin haavoittuvia
Tarpeettomien prosessien ajaminen	Monissa yleisiä käyttöjärjestelmiä käyttävissä verkosto-automaatiojärjestelmissä tietoliikennepalvelut ovat päällä oletusarvoisesti ja aiheuttavat haavoittuvuusriskin
Avoimesti saatava järjestelmätietous	Yleisimpien järjestelmien järjestelmäspesifikaatiot ja ylläpitokäsikirjat ovat julkisesti saatavissa ja helpottavat hyökkäysten suunnittelua
Järjestelmävalvojan käyttöoikeuksien huolimaton hallinta ja käsittely	Järjestelmävalvojan ja –ylläpitäjän käyttöoikeuksien päätyminen asiattomiin käsiin altistaa järjestelmän väärinkäytöksille ja hyökkäyksille
IDS/IPS-hyökkäyksen-estojärjestelmää ei käytetä	Palomuurien lisäksi IDS/IPS-järjestelmät ovat tehokas keino suojata verkostoautomaatiojärjestelmien tietoverkkoja ei toivotulta liikenteeltä
Lokeja ei hyödynnetä tai seurata reaaliaikaisesti	Ilman ajantasaisia ja tarkkoja lokitietoja ei usein ole mahdollista selvittää tietoturvapoikkeaman aiheuttajaa. Sama koskee muita turvallisuusindikaattoreita
Virustorjunta- ja muita suojausohjelmistoja ei ole käytössä	Monet verkostoautomaatiojärjestelmät eivät toimi virheettömästi, mikäli virustorjuntaohjelmia otetaan käyttöön. Tästä aiheutuu merkittävä riski haittaohjelmien tunnistamiselle ja eristämiselle

Tietoliikenneverkon haavoittuvuus voidaan jakaa fyysiseen haavoittuvuuteen sekä konfiguraation haavoittuvuuteen. Tietoliikenneverkon fyysisiä haavoittuvuuksia ovat esimerkiksi varmentamattomat tietoliikenneyhteydet ja palomuurien puuttuminen. Konfiguraa-

tion haavoittuvuuksia ovat esimerkiksi laitteiden oletusparametrien käyttäminen ja tietoliikenneverkon hallintajärjestelmän puuttuminen. Taulukoissa 6 ja 7 on esitelty ja kuvattu tietoliikenneverkon haavoittuvuuksia. [34]

Taulukko 6. Tietoliikenneverkon fyysisiä haavoittuvuuksia [34]

Haavoittuvuus	Kuvaus
Turvaton tietoliikeverkon rakenne ja siirtomedia	Tietoliikenneverkon rakenne on suunniteltu yleistä yritysteletoimintaa varten, eikä siinä ole huomioitu toimintakriittisten verkostoautomaatiojärjestelmien tietoliikenteen erityisiä turvallisuus-, luotettavuus ja laitevaatimuksia. Esimerkiksi valokaapeleiden avulla toteutetut siirtomediat ovat yleensä luotettavampia ja tietoturvallisempia kuin langattomat yhteydet
Tietoliikenneverkon ja sen laitteiden riittämätön fyysinen suojaus, esimerkiksi laitetilojen suojausluokitus ei ole riittävä, kuluvalvonta tai lukitus puutteellisia tai laitteita ei ole sijoitettu lukittuihin laitekaappeihin. Laitteiden portit ja liitännät fyysisesti ja loogisesti suojaamattomia	Telelaitetilojen, sähköasemien ja telelaitteiden riittämätön tai puuttuva fyysinen suojaus ja kulunvalvonta voi mahdollistaa huomaamattoman tunkeutumisen laitetiloihin ja laitteisiin. Miehittämättömillä asemilla ei ole esimerkiksi etävideo- tai sähköistä kulunvalvontaa. Riski kohdistuu laajalle kirjolle erilaisia haitallisia ja vihamielisiä toimenpiteitä. Uhka luonnononnettomuuksien ja poikkeuksellisten sääilmiöiden aiheuttamille vaurioille
Tietoliikenneyhteydet ovat varmentamattomia	Verkostoautomaatioyhteyksiltä edellytetään yleensä hyvin korkeaa käytettävyyttä, mikä vaati yhteyksien riippumatonta reitti- ja laitevarmennusta (esim. kahdennus). Myös tehonsyötöt ja kriittisten laitetilojen ilmastointijärjestelmät tulee kahdentaa tai niiden toimintaa tulee valvoa reaaliaikaisesti
Ulkoiset yhteydet ovat huonosti suojattuja	Ulkoiset yhteydet salaamattomia; ei käytetä VPN-tunnelointia tai vahvaa autentikointia
Puutteellinen tai tarkkuudeltaan riittämätön tietoliikenneverkon synkronointi	Puutteellisesti toimiva synkronointi voi aiheuttaa tiedonsiirtovirheitä tai kaataa tietoliikenneverkon tai sen solmuja erityisesti piirikytkentäisissä tietoliikenneverkoissa (esim. SDH- tai PDH-verkot). Myös paketti-kytkentäisissä verkoissa (mm. IP-verkot) synkronointi ja aikaleimojen siirto on toteutettava luotettavasti verkostoautomaatiojärjestelmän asettamien vaatimusten mukaisesti
Palomuureja, välityspalvelimia (proxy) tai IDS/IPS-järjestelmiä ei käytetä	Palomuurit sekä välityspalvelimet ja IDS/IPS- järjestelmät ovat oleellinen osa tietoliikenteen suojausta ja mahdollistavat liikenteen rajoittamisen sekä DMZ-alueiden rakentamisen
Tietoliikenneverkon salaus- ja suojausominaisuudet (laitteet ja ohjelmistot) puuttuvat kokonaan tai ovat puutteellisia	Tietoliikenneverkko ei mahdollista liikenteen salausta tai VPN-tunnelontia, jolloin turvallisuuskriittinen data, esimerkiksi salasanat, voivat joutua asiattomien käsiin

Taulukko 7. Tietoliikenneverkon konfiguraation haavoittuvuuksia [34]

Haavoittuvuus	Kuvaus
Puutteellinen tietoliikenteen reititys- ja access-parametrien hallinta sekä monimutkainen tai sekava verkkorakenne	Puutteellinen tietoliikenneverkon liikenteen hallinta mahdollistaa ei toivottujen järjestelmien/laitteiden kytkeytymisen verkostoautomaatiojärjestelmän laitteisiin, esim. puutteellisesti määritellyt palomuurisäännöt. Rakenteellisesti monimutkaisessa tai sekavassa verkossa ei aina hallita kaikkia tietoliikenteen mahdollisia reittejä
Laitteiden oletusparametrien käyttäminen	Asiattomat tahot pääsevät tunkeutumaan helposti tietoliikenneverkkoon tai sen laitteisiin käytettäessä käyttöoikeuksiin tai porttien aktivointiin yms. liittyvien tunnusten tai parametrien oletusarvoja
Tietoliikenneverkon konfiguraatioparametrien varmuuskopioinnin puuttuminen tai puutteet	Puuttuvat tai puutteelliset (esim. vanhentuneet) laite- ja järjestelmäparametrien varmuuskopiot voivat estää tietoliikenneverkon tai sen osan palauttamisen kriisitilanteessa
Tietoliikenneverkolla ei ole hallintajärjestelmää tai se on rakenteeltaan ja ominaisuuksiltaan puutteellinen	Tietoliikenneverkon hallintajärjestelmä mahdollistaa verkon keskitetyn ja reaaliaikaisen vikojen paikannuksen, verkon konfiguroinnin, siirronlaadun ja turvallisuus-parametrien seurannan sekä hallinnan
Tietoliikenneverkon hallintajärjestelmä tai verkon laitteiden hallintaliittymien käyttöoikeuksien riittämätön tai puuttuva hallinta	Tietoliikenneverkon hallintajärjestelmien tai –liittymien puutteellinen hallinta mahdollista asiattomien henkilöiden tai järjestelmien pääsyn tietoliikenneverkkoon ja voi johtaa tietoliikenneverkon rikolliseen haltuunottoon. Käyttöoikeuksiin liittyviä tunnuksia ja salasanoja ei vaihdeta säännöllisesti tai niiden rakenne on liian yksinkertainen
Hallintajärjestelmän ja/tai verkkolaitteiden lokeja ei hyödynnetä tai seurata systemaattisesti	Ilman ajantasaisia ja tarkkoja lokitietoja ei usein ole mahdollista selvittää laitteiden luvatonta käyttöä tai tietoturvapoikkeaman aiheuttajaa. Sama koskee muita turvallisuusindikaattoreita
Automaatiojärjestelmien vaatimaa turvallista verkkoa ei ole määritelty tai rajattu	Turvallisen verkon määrittely ja dokumentointi on edellytys verkon tehokkaalle suojaukselle
Turvallisessa verkossa siirretään turvatonta tai väärää liikennettä	Turvallista verkkoa käytetään myös muiden kuin verkostoautomaatiojärjestelmien tiedonsiirtoon, josta aiheutuu teknisiä ja turvallisuusriskejä
Avoimesti saatava järjestelmätietous	Suosittujen verkkolaitteiden rakennedata ja ylläpitokäsikirjat ovat julkisesti saatavissa ja helpottavat hyökkäysten suunnittelua

Monet fyysiset heikkoudet ja haavoittuvuudet aiheuttavat ongelmia myös kyberturvallisuuden kannalta, kuten taulukoista 2, 3, 4, 5, 6 ja 7 nähdään. Kyberturvallisuus onkin hyvin kokonaisvaltainen asia, joka ei esiinny pelkästään tietokoneilla haittaohjelmina.

Esimerkkitapauksena tarkastellaan kyberhyökkäystä, joka katkaisi sähköt 225 000 ihmiseltä Länsi-Ukrainassa joulukuussa 2015. Tämä oli tiettävästi ensimmäinen kyberhyökkäys sähköjärjestelmään, joka on onnistunut katkaisemaan sähköt sadoilta tuhansilta ihmisiltä, ja se osoitti kuinka haavoittuvaisia sähköenergiajärjestelmät ovat kyberiskuille.

Kyberhyökkäyksen jälkeen sähköjen palautus onnistui manuaalisesti noin 1-6 tunnin kuluttua. [35,36]

Hyökkäys kohdistui kolmea sähköyhtiötä vastaan. Hyökkääjät aloittivat hyökkäyksensä Kyivoblenergo-yhtiöstä, jonka omassa SCADA-ohjausjärjestelmässä hyökkääjät lähettivät seitsemälle 110 kV:n ja 23 pienemmälle 35 kV:n muuntoasemalle komennot irtautua verkosta. Myös Chernivtsioblenergo-yhtiöön kohdistui samanlainen isku. Prykarpattyaoblenergo-yhtiössä työntekijä katseli vierestä, kun hyökkääjä käytti järjestelmää etäyhteydellä ja sammutti 30 muuntoasemaa. Työntekijä ei voinut tehdä mitään, koska hyökkääjät olivat vaihtaneet hänen salasanansa, joten hän ei päässyt kirjautumaan järjestelmään. Hyökkääjät katkaisivat myös kahden valvomon katkeamattoman tehonsyötön (UPS), jolloin myös valvomot jäivät ilman sähköä. [35,36]

Hyökkäyksen valmistelu oli alkanut jo puoli vuotta ennen varsinaista hyökkäystä tietojenkalastelulla (engl. phishing), jossa työntekijöille lähetettiin sähköposteja. Avatessaan tietojenkalasteluun liittyvän sähköpostin liitteen, työntekijät latasivat tietämättään koneilleen BlackEnergy3-vakoiluohjelman. Vakoiluohjelma avasi hyökkääjille takaportin yhtiöiden järjestelmiin ja sen avulla he pystyivät salakuuntelemaan yhtiöiden verkkoliikennettä, selvittämään salasanoja ja etenemään työasemilta Windows-verkon palvelimille. Sieltä he saivat urkittua salasanat VPN:iin (virtual private network), joiden kautta he pääsivät tunkeutumaan SCADA-verkkoihin, joilla ohjattiin sähköjärjestelmää. [35,36]

Varsinaisen hyökkäyksen aluksi hyökkääjät uudelleen konfiguroivat UPS:n, joka tarjosi varavirtaa kahdelle valvomolle, jotta se ei voisi vikatilanteessa syöttää sähköä valvomoihin. Hyökkääjät tunkeutuivat lähes samanaikaisesti kolmen yhtiön SCADA-verkkoihin selvittämiensä VPN-salasanojen avulla ja tekivät UPS:n toimintakyvyttömäksi. Ennen kuin he aloittivat muuntoasemien verkosta irrottamisen, hyökkääjät laukaisivat palvelunestohyökkäyksen yhtiöiden asiakaspalveluita vastaan. Tämän avulla hyökkääjät saivat lisää aikaa operaatiolleen. Työntekijän huomatessa tilanteen, olivat hyökkääjät ehtineet irrottaa jo useita muuntoasemia verkosta. Hyökkääjät eivät vain irrottaneet muuntoasemia verkosta, vaan ennen verkosta irrottamista he korvasivat niiden firmware-koodit omilla firmware-koodeillaan, jotka rikkoivat muuntimet. Hyökkääjät viimeistelivät iskunsa KillDisk-ohjelmalla, joka poisti tiedostoja työasemilta ja korruptoi kiintolevyt, minkä seurauksena koneet eivät enää käynnistyneet. [35–37]

Vaikka sähköt eivät olleet kauaa poikki Ukrainassa, olivat iskun vaikutukset suuret. Edes kaksi kuukautta hyökkäyksen jälkeen valvomot eivät ole täysin toiminnassa. Hyökkääjät

korvasivat tärkeiden laitteiden firmware-koodia 16 muuntoasemalla. Tämän seurauksena ne eivät reagoi yhtiöiden kauko-ohjaukseen, vaan niitä on ohjattava manuaalisesti. [35,37]

4.2.3 Sähköntuotantoon kohdistuvat kyberriskit

Sähköntuotantolaitoksia ohjataan pitkälti teollisuusautomaatiojärjestelmien avulla. Teollisuusautomaatiojärjestelmät tarkoittavat tuotantolaitosten tuotannonohjausjärjestelmiä. Kyberuhkien lisääntyessä on myös tuotantoympäristön tietoliikennettä, dataa ja laskentaa erottelevien aliverkkojen, suoja-alueiden sekä virtuaaliympäristön seurantaa vahvistettava ja pidettävä huoli niiden turvallisesta toteuttamisesta. [38] Teollisuudenautomaatiojärjestelmien haavoittuvuudet ovat hyvin samanlaisia kuin luvussa 4.1.2 ja taulukoissa 2-7 esitellyt verkostoautomaatiojärjestelmien haavoittuvuudet.

Tarkastellaan esimerkkitapauksena kyberhyökkäystä Iranin Natanzin ydinlaitokseen. Vaikka kohteena ei ollut sähköntuotantolaitos, käy tapauksesta hyvin ilmi, miten teollisuuslaitokseen voidaan toteuttaa kyberisku.

Vuonna 2006 Yhdysvaltojen presidentti George W. Bush teki päätöksen kyberaseen käytöstä, jonka tavoitteena oli viivästyttää Iranin ydinaseen valmistumista. CIA, NSA ja Israel kehittivät yhteistyössä haittaohjelman, Stuxnetin. Sen oli määrä tuhota Iranin Natanzissa sijaitsevassa ydinlaitoksessa uraanin rikastamiseen käytetyt sentrifugit. [36]

Stuxnet oli hyvin kehittynyt haittaohjelma, jolla on monia ominaisuuksia. Se esimerkiksi käytti hyväkseen monia Windowsin nollapäivähaavoittuvuuksia, joiden avulla se sai täydet ylläpitäjän oikeudet järjestelmään. Lisäksi se käytti laiteajureiden omia varmenteita, modifioi järjestelmien kirjastoja ja hyökkäsi step7-asennuksiin, joihin SCADA-järjestelmä liittyy. Stuxnet levisi monin tavoin, mutta se sisälsi myös suojausmekanismeja, jotka rajoittivat sen leviämistä. Lisäksi se pystyi päivittämään itseään sekä kommunikoimaan servereiden kanssa ja siten lähettämään tietoja levinneisyydestään. [36,39]

Todennäköisesti Stuxnet pääsi Iranin Natanzin ydinlaitokseen muistitikun välityksellä, koska laitoksen koneet eivät ole yhteydessä internettiin. Joku laittoi muistitikun laitoksen verkkoon yhdistettyyn tietokoneeseen, jolloin Stuxnet pääsi laitoksen verkkoon. Siellä Stuxnet levisi ja etsi kohde ohjelmistoaan, SCADA-tuotannonohjausjärjestelmää. Päästyään tuotannonohjausjärjestelmään, Stuxnet kuunteli ja tallensi SCADA-tietoliikennettä. Kerättyään tarpeeksi dataa se alkoi ohjata sentrifugeja. Stuxnet toteutti kaksi hyökkäystä. Ensimmäisessä se kasvatti sentrifugien pyörimisnopeutta noin 15 minuutin

ajaksi. Noin kuukauden päästä toisessa hyökkäyksessä se hidasti sentrifugien pyörimisnopeutta noin 50 minuutiksi. Tätä toistui useiden kuukausien ajan. Stuxnet tuhosi noin 10-20 % Natanzin sentrifugeista, joita oli yhteensä 8 700. [36,40]

4.2.4 Sähkönkulutukseen kohdistuvat kyberriskit

Yleensä tarkastellaan sähköntuotantoon tai -siirtoon kohdistuvia uhkia. Mutta sähköenergiajärjestelmää voidaan vahingoittaa myös kulutuksen kautta. Tehopula on tilanne, jossa sähköntuotanto ja tuontisähkö eivät riitä kattamaan sähkön kulutusta. Suomessa tehopula voi syntyä huippukulutuksen aikaan, jos Suomen oma tuotanto ei riitä kattamaan kulutusta ja tuontisähköä ei ole saatavilla tarpeeksi. Vakavassa tehopulassa sähkön käyttöä voidaan joutua rajoittamaan ja sen aikana tapahtuvat viat voivat kaataa koko sähköjärjestelmän. [27]

Älylaitteiden määrä ja laitteet, joissa on IoT (Internet of Things), ovat lisääntyneet merkittävästi viime vuosina. Vaikka ne helpottavat arkea, voidaan niitä käyttää myös ongelmien tuottamiseen. Älylaitteista voi muodostaa bottiverkon, jota voi ohjailla etänä. Sillä voi vahingoittaa sähköenergiajärjestelmää kulutuksen kautta. Tällainen hyökkäys on nimetty kysynnän manipuloinniksi IoT:n kautta, MadIoT (Manipulation of Demand via IoT). Princetonin yliopiston tutkijoiden mukaan MadIoT-hyökkäyksellä voi aiheuttaa sähkökatkoja, jotka pimentäisivät jopa valtioiden sähköenergiajärjestelmiä. [41]

Tutkimuksessa mainitaan kolme erilaista MadIoT-hyökkäystä. Yhden hyökkäyksen seurauksena on sähköenergiajärjestelmän taajuuden epästabiilius. Siinä älylaitteiden bottiverkko kytketään synkronoidusti päälle tai pois päältä, joka johtaa epätasapainoon tuotannon ja kulutuksen välillä. Jos laitteet kytkettiin päälle ja kulutus kasvoi paljon, on seurauksena järjestelmän taajuuden nopea lasku. Mikäli järjestelmän taajuus laskee liian paljon, seurauksena voi olla generaattoreiden irtoaminen järjestelmästä niiden oman suojauksen vuoksi ja mahdollisesti suuri sähkökatko. Toisen hyökkäyksen seurauksena on sähkölinjojen vikoja, joiden seurauksena voi olla vyörynomainen vian eteneminen, jossa edellinen vika aiheuttaa aina uuden vian. Tämän hyökkäyksen tavoitteena on nostaa järjestelmän kulutuksen määrää nopeasti, jolloin johdot ylikuormittuvat ja vioittuvat. Esimerkiksi huippukulutuksen aikana tapahtuva kulutuksen lisääminen älylaitteiden bottiverkon avulla voi johtaa merkittäviin vahinkoihin ja sähkökatkoihin. Kolmannen hyökkäyksen tavoitteena on kasvattaa järjestelmän käyttökustannuksia. Kun kulutus nousee arvioitua kulutusta ylemmäs ja se ei aiheuta taajuuden epästabiiliutta tai johtovikoja, on sähkönjakelijoiden ostettava lisää sähköä kattamaan kulutuksen kasvu. Lisäksi järjestelmävastaava, Suomessa Fingrid, voi joutua käyttämään reservivoimalaitoksia. Tämän

seurauksena sähkönjakelijoiden kustannukset kasvavat, koska he joutuvat ostamaan lisää sähköä, ja sähköä myyvät tahot tekevät voittoa, koska sähköä voi myydä sitä kalliimmalla mitä lähempänä käyttöhetkeä ollaan. [41]

4.2.5 Suomen tilanne

”Suomen kantaverkkoon kohdistuu kymmeniä kertoja viikossa internetistä eri puolilta maailmaa tulevia tunkeutumisyrityksiä” sanoo Fingridin ICT-johtaja Kari Suominen. Hänen mukaansa kantaverkkoon kohdistuvia kyberhyökkäysyrityksiä on koko ajan, joskus enemmän ja joskus vähemmän. Nämä hyökkäykset eivät kuitenkaan ole kovin suuria vaan lähinnä verkon rajojen, kuten palomuurien ja muiden suojausten, testaamista. Hyökkääjät ovat Suomisen mukaan todennäköisesti yksityishenkilöitä, mutta toisinaan valtiotkin kokeilevat löytyykö suojauksesta aukkoja. [42]

Joulukuussa 2015 hakkerit iskivät kolmeen sähkönjakelukeskukseen Länsi-Ukrainassa ja katkaisivat sähköt yli 200 000 ihmiseltä. Aalto-yliopiston kyberturvallisuuden professori Jarno Limnéllin mukaan kyseinen hyökkäys näytti, mitä kyberympäristön kautta voi saada aikaan. Suomi on riippuvainen sähköstä ja Limnéllin mukaan laajemman Suomeen kohdistuvan hyökkäyksen toteutuminen riippuu siitä, onko jollakin taholla jostain syystä halua testata Suomen kriisinsietokykyä tai vaikeuttaa suomalaisen yhteiskunnan toimintaa. [42]

Kyberuhkien lisääntyessä ja niiden mahdollisten vaikutusten ollessa hyvin merkittäviä yhteiskunnan toiminnan kannalta, on Suomi luonut oman kyberturvallisuusstrategiansa, koska tietoyhteiskuntana Suomi on riippuvainen tietoverkkojen ja -järjestelmien toiminnasta. Valtioneuvoston 24.1.2013 julkaisemassa kyberturvallisuusstrategiassa on esitetty visio, toimintamalli sekä strategiset linjaukset kyberturvallisuudelle. Julkaisussa kyberturvallisuus on määritelty tavoitetilaksi, jossa kybertoimintaympäristöön voi luottaa ja sen toiminta on turvattu. [43]

Kyberturvallisuusstrategian visiossa Suomi on kykenevä suojaamaan yhteiskunnan tärkeimmät toiminnot kyberuhkia vastaan ja kolmen vuoden kuluessa Suomi nähdään edelläkävijänä kyberturvallisuudessa, kyberuhkiin varautumisessa ja niiden aiheuttamien häiriötilanteiden hallinnassa maana, jossa kybertoimintaympäristöä hyödynnetään tehokkaasti ja turvallisesti. [43]

Suomen kyberturvallisuuden toimintamalli perustuu kahdeksaan periaatteeseen, joiden avulla yhteiskunta pystyy varautumaan kyberuhkia vastaan ja ennakoimaan niitä. Valtioneuvosto on kyberturvallisuuden johtamisen ylin taso, jonka tehtäviä ovat kyberturvallisuuden poliittinen ohjaus ja strategiset linjaukset sekä kyberturvallisuuden voimavaroista

ja toimintaedellytyksistä päättäminen. Jotta valtioneuvosto pystyy johtamaan kyberturvallisuutta ja hallitsemaan häiriötilanteita, on sillä ja eri toimijoilla oltava käytössään luotettava ja ajantasainen tilannekuva yhteiskunnan elintärkeiden toimintojen tilasta kyberturvallisuuden kannalta. Kybertoimintaympäristö ja siellä vaikuttavien kyberuhkien luonne korostavat yhteistyötä, sen tehokkuutta ja joustavuutta, uhkiin varauduttaessa. Tunnistettujen kyberuhkien analysointi ja niistä syntyneiden häiriötilanteiden hallinta liittyvät kyberturvallisuuden strategisiin tehtäviin. [43]

Suomen kyberturvallisuutta kehitetään strategisten linjausten mukaisesti, joilla pyritään luomaan edellytykset vision toteutumiselle. Sähköenergiajärjestelmän kannalta strategisista linjauksista ensimmäinen, toinen ja kolmas ovat merkittävä. Niissä todetaan: ”Luodaan kansallisen kyberturvallisuuden ja kyberuhkien torjunnan edistämiseksi viranomaisten ja muiden toimijoiden välinen tehokas yhteistoimintamalli. Parannetaan yhteiskunnan elintärkeiden toimintojen turvaamiseen osallistuvien keskeisten toimijoiden kokonaisvaltaista kyberturvallisuuden tilannetietoisuutta ja tilanneymmärrystä. Ylläpidetään ja kehitetään yhteiskunnan elintärkeiden toimintojen turvaamisen kannalta tärkeiden yritysten ja organisaatioiden kykyä havaita ja torjua elintärkeää toimintoa vaarantavat kyberuhkat ja -häiriötilanteet sekä toipua niistä osana elinkeinoelämän jatkuvuuden hallintaa.” [43] Sähköenergiajärjestelmän toiminta voidaan katsoa yhteiskunnan elintärkeäksi toiminnoksi ja näin ollen sen kyberturvallisuutta on pyrittävä kehittämään ja luomaan yhteistoimintaa siinä toimivien osapuolten ja viranomaisten välille, minkä avulla edistetään kyberturvallisuutta.

Kyberturvallisuusstrategiallaan Suomi pyrkii turvaamaan oman yhteiskuntansa toimintaa. Siinä tärkeä osa on sähköenergiajärjestelmä ja sen toiminta, myös mahdollisissa häiriötilanteissa.

5. YHTEENVETO

Sähkön toimitusvarmuuteen on alettu kiinnittämään enemmän huomiota yhä useampien yhteiskunnan toimintojen muuttuessa riippuvaiseksi sähköstä. Sähköenergiajärjestelmän tehtävä on toimittaa sähköä sen tuottajilta kuluttajille ja se koostuu kolmesta eri osasta. Jotta järjestelmä pystyy suorittamaan tehtävänsä, on tarkasteltava, mitkä seikat vaikuttavat sen toimintaan. Tämän perusteella järjestelmää osataan kehittää ja parantaa, jotta se pääsee paremmin tavoitteisiinsa. Sähköenergiajärjestelmän keskeytymätöntä toimintaa ei ole kannattavaa tavoitella, koska se vaatisi todella suuria investointeja järjestelmän jokaiseen osaan. Tämän seurauksena sähkön ja sen siirron hinnat nousisivat merkittävästi.

Kokonaisuutena sähköenergiajärjestelmä on melko haavoittuvainen ulkopuolisia uhkia vastaan. Sähköenergiajärjestelmän eri osien haavoittuvuudet eroavat toisistaan kuitenkin paljon. Sähköntuotantoon ja -kulutukseen sääilmiöt eivät juurikaan vaikuta ja vahingonteot, kuten kyberhyökkäykset, vaikuttavat lähinnä vahingonteon kohteena olevan tuotantolaitoksen tai kulutuskohteen toimintaan. Mutta yleensä tuotantoon tai kulutukseen kohdistuvat vahingonteot eivät vaikuta koko järjestelmän toimintaan. Selvästi sähköenergiajärjestelmän haavoittuvaisin osa on sähkönsiirtojärjestelmä. Tämä johtuu järjestelmän suuresta koosta ja maantieteellisesti hajanaisesta sijainnista. Lisäksi osa sähköverkoista on rakennettu useita vuosikymmeniä sitten, jolloin esimerkiksi sähkön toimitusvarmuuteen ei kiinnitetty yhtä paljoa huomiota. Sääilmiöt voivat vaikuttaa merkittävästi erityisesti jakeluverkon toimintaan ja vahingoittaa sitä pahoin. Siirtojärjestelmä on myös houkutteleva kohde erilaisille vahingonteoille, koska sen vahingoittamisella voidaan häiritä yhteiskunnan toimintaa merkittävästi. Sääilmiöt vaikuttavat sähköntoimitukseen yleensä paikallisesti, mutta koordinoidut hyökkäykset siirtoverkkoon voivat lamauttaa koko sähköenergiajärjestelmän toiminnan.

Tulevaisuudessa sähköenergiajärjestelmän haavoittuvuudet tulevat muuttumaan järjestelmän muuttuessa. Sääriskeistä johtuvien haavoittuvuuksien määrä tulee pienenemään tulevaisuudessa. Esimerkiksi jakeluverkon maakaapelointiasteen kasvaminen tulee vähentämään sääilmiöistä aiheutuvia katkoja sähkönjakelussa ja sähköverkkoyhtiöt lisäävät myös muita keinoja sähköntoimitusvarmuuden parantamiseksi. Maakaapelointi tuo kuitenkin mukanaan omat ongelmansa ja olosuhteiden sekä kustannusten vuoksi sitä ei kannata tehdä kaikille jakeluverkon osille. Myös kyberturvallisuus ja kyberuhkien torjunta tulee olemaan isossa roolissa, kun verkkoon yhteydessä olevien laitteiden määrä järjestelmässä kasvaa. Myös kyberhyökkäysten tekijöiden osaaminen ja kyvyt kasvavat koko

ajan, mikä pakottaa myös sähköenergiajärjestelmässä toimivien tahojen panostamaan kyberturvallisuuteen ja lisäämään omaa osaamistaan. Täysin haavoittumatonta sähköenergiajärjestelmästä ei siis saada tulevaisuudessakaan vaikka haavoittuvuuksien määrä todennäköisesti vähenee.

LÄHTEET

[1] J. Elovaara, L. Haarla, Sähköverkot 1: järjestelmätekniikka ja sähköverkon laskenta, Otatieto, Helsinki, 2011, 520 s.

[2] Suomen sähköjärjestelmä, Fingrid. Saatavissa: https://www.fingrid.fi/kantaverkko/suomen-sahkojarjestelma/ (Viitattu: 27.02.2019)

[3] M. A. El-Sharkawi, Electric energy: an introduction, CRC Press, Boca Raton Florida, USA, 2nd ed., 2008, 455 p.

[4] T. Ylinen, Hajautettu energiantuotanto, Sähköala.fi, 2009. Saatavissa: http://www.sahkoala.fi/ammattilaiset/artikkelit/verkonrakennus/fi_FI/hajautettu_energiantuotanto/ (Viitattu: 27.02.2019)

[5] E. Lakervi, J. Partanen, Sähkönjakelutekniikka, Otatieto, Helsinki, 2009, 295 s.

[6] Energiavuosi 2018 - Sähkö, Energiateollisuus, 2019, s. 21. Saatavissa: https://energia.fi/ajankohtaista_ja_materiaalipankki/materiaalipankki/energiavuosi_2018_-_sahko.html#material-view (Viitattu: 02.03.2019)

[7] J. Elovaara, L. Haarla, Sähköverkot 2: verkon suunnittelu, järjestelmät ja laitteet, Otatieto, Helsinki, 2011, 551 s.

[8] Sähköverkkoliiketoiminnan kehitys, sähköverkon toimitusvarmuus ja valvonnan vaikuttavuus 2018, Energiavirasto, 2019. Saatavissa: https://www.energiavirasto.fi/documents/10191/0/Vaikuttavuusraportti_2018.pdf/48ac2585-b3cd-4d6d-ab1c-14764d68e2f8 (Viitattu: 18.03.2019)

[9] Standardi SFS-EN 50160: yleisestä jakeluverkosta syötetyn sähkön jänniteominaisuudet, Suomen standardisoimisliitto, Helsinki, 2010, 65 s.

[10] Kulutuksen ja tuotannon tasapainon ylläpito, Fingrid. Saatavissa: https://www.fingrid.fi/kantaverkko/suomen-sahkojarjestelma/kulutuksen-ja-tuotannon-tasapainon-yllapito/ (Viitattu: 27.02.2019)

[11] J. Sederlund, Taajuuden ylläpito sähköjärjestelmässä, Fingrid (verkkolehti), Nro. 3, 2008, s. 30-31. Saatavissa: https://www.fingrid.fi/globalassets/dokumentit/fi/julkaisut/asiakaslehdet/fingrid_3_08.pdf (Viitattu: 02.03.2019)

[12] H. Tuomenvirta, R. Haavisto, M. Hildén, T. Lanki, S. Luhtala, P. Meriläinen, K. Mäkinen, A. Parjanne, P. Peltonen-Sainio, K. Pilli-Sihvola, J. Sorvali, N. Veijalainen, Sää- ja ilmastoriskit Suomessa - Kansallinen arvio, Valtioneuvosto, 2018. Saatavissa: http://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/161015/43-2018-Saa%20ja%20ilmastoriskit%20Suomessa.pdf?sequence=1&isAllowed=y (Viitattu: 15.03.2019)

[13] Sähkön keskeytystilastot 2010-2017, Energiateollisuus, 2017. Saatavissa: https://energia.fi/ajankohtaista_ja_materiaalipankki/materiaalipankki/sahkon_keskeytystilastot_2010-2017.html#material-view (Viitattu: 15.03.2019)

[14] Ilmatieteen laitos, Suomen nykyilmasto, ilmasto-opas.fi. Saatavissa: http://ilmasto-opas.fi/fi/ilmastonmuutos/suomen-muuttuva-ilmasto/-/artikkeli/1c8d317b-5e65-4146-acda-f7171a0304e1/nykyinen-ilmasto-30-vuoden-keskiarvot.html (Viitattu: 19.03.2019)

[15] Johtoalue, Fingrid. Saatavissa: https://www.fingrid.fi/kantaverkko/kunnossapito/voimajohdot/johtoalue/ (Viitattu: 17.03.2019)

[16] Tuulet ja myrskyt, Ilmatieteen laitos, 2019. Saatavissa: https://ilmatieteenlaitos.fi/tuulet (Viitattu: 19.03.2019)

[17] Syöksyvirtaukset, Ilmatieteen laitos. Saatavissa: https://ilmatieteenlaitos.fi/syoksyvirtaukset (Viitattu: 19.03.2019)

[18] M. Uusi-Rasi, Säävarmuuden parantaminen Vatajankosken Sähkön keskijänniteverkossa, Tampereen Ammattikorkeakoulu, 2013, 73 s. Saatavissa: https://www.theseus.fi/bitstream/handle/10024/58125/Uusi-Rasi_Markku.pdf?sequence=1&isAllowed=y

[19] A. Nieminen, Myrskytuhot ja haja-asutusalueiden sähköverkon laadun varmistaminen, 2010. Saatavissa: http://www.siemens.fi/pool/cc/events/energiapaiva_2010/Arto%20Nieminen.pdf (Viitattu: 21.03.2019)

[20] Kesän 2010 myrskyt sähköverkon kannalta, Energiamarkkinavirasto, 2011. Saatavissa: https://www.energiavirasto.fi/documents/10179/0/Kes%C3%A4n+2010+myrsky+raportti_lopullinen+_2_.pdf/8b69b8d1-c89d-428c-a3c2-4e2ab5321ddf (Viitattu: 21.03.2019)

[21] Tykky eli tykkylumi, Ilmatieteen laitos. Saatavissa: https://ilmatieteenlaitos.fi/tykky-eli-tykkylumi (Viitattu: 23.03.2019)

[22] P. Mattila, Tulisitko toimeen päiviä ilman sähköä?, Keskisuomalainen, 2018. Saatavissa: https://www.ksml.fi/kotimaa/Tulisitko-toimeen-p%C3%A4ivi%C3%A4-ilman-s%C3%A4hk%C3%B6%C3%A4/1091797 (Viitattu: 23.03.2019)

[23] M. Aro, J. Elovaara, M. Karttunen, K. Nousiainen, V. Palva, Suurjännitetekniikka (4. korj. ja täydennetty p.), Otatieto, Helsinki, 2015, 537 s.

[24] A. Harjanne et al., Sää- ja ilmastoriskien hallinta ja tietolähteet Suomessa, Ilmatieteen laitos, 2016, 111 s. Saatavissa: https://helda.helsinki.fi/bitstream/handle/10138/168693/ilmastoriskitsuomessa.pdf?sequence=1&isAllowed=y (Viitattu: 28.03.2019)

[25] J. Luukkonen, Myrskyjen vaikutus tuulivoimatuotantoon Suomessa, Aalto-yliopisto, 2012, 57 s. Saatavissa: https://aaltodoc.aalto.fi/bitstream/handle/123456789/5220/master_luukkonen_juho-tuomas_2012.pdf?sequence=1&isAllowed=y

[26] Sähkömarkkinalaki 9.8.2013/588, 2013. Saatavissa: https://www.finlex.fi/fi/laki/alkup/2013/20130588

[27] Sähköriippuvuus modernissa yhteiskunnassa, Turvallisuuskomitea, 2015, 102 s.

[28] Terrorism and the Electric Power Delivery System, National Research Council of the National Academies, The National Academies Press, Washington, D.C, USA, 164 p. Saatavissa: https://www.nap.edu/catalog/12050/terrorism-and-the-electric-power-delivery-system

[29] H. Sokala, Suomi polvilleen 15 minuutissa: käsikirjoitus, MOT, Yle, 2013. Saatavissa: https://yle.fi/aihe/artikkeli/2013/03/08/suomi-polvilleen-15-minuutissa-kasikirjoitus (Viitattu: 15.04.2019)

[30] T. Phillips, Venezuela: huge power outage leaves much of country in the dark, The Guardian, 2019. Saatavissa: https://www.theguardian.com/world/2019/mar/07/venezuela-hit-by-major-power-outage (Viitattu: 17.04.2019)

[31] T. Phillips, P. Torres, 'No more hope': fresh blackout leaves half of Venezuela without power, The Guardian, 2019. Saatavissa: https://www.theguardian.com/world/2019/mar/25/venezuela-new-blackout-half-country-no-power-maduro (Viitattu: 17.04.2019)

[32] T. Myllylä, Sähköverkkojen kyberturvallisuus, Aalto-yliopisto, 2014, 62 s. Saatavissa: https://aaltodoc.aalto.fi/bitstream/handle/123456789/12894/master_Myllyl%C3%A4_Tony_2014.pdf?sequence=1&isAllowed=y

[33] J. Limnéll, K. Majewski, M. Salminen, Kyberturvallisuus, Docendo, Jyväskylä, 2014, 246 s.

[34] J. Tervo, Verkostoautomaatiojärjestelmien tietoturva, Reneco, 2013, 70 s. Saatavissa: https://energia.fi/files/1015/Verkostoautomaatiojarjestelmien_tietoturva_pakattu.pdf (Viitattu: 09.03.2019)

[35] P. Järvinen, Kyberuhkia ja somesotaa, Docendo, Jyväskylä, 2018, 380 s.

[36] K. Zetter, Inside the cunning, unprecented hack of Ukraine's power grid, wired, 2016. Saatavissa: https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/

[37] The Cybersecurity and Infrastructure Agency (CISA), Cyber-Attack Against Ukrainian Critical Infrastructure, The Department of Homeland Security, 2016. Saatavissa: https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01 (Viitattu: 11.03.2019)

[38] P. Ahonen et al., KYBER-TEO - tuloksia 2014-2016, Teknologian tutkimuskeskus VTT oy, Juvenes Print, Tampere, 2017, 145 s. Saatavissa: http://www.vtt.fi/inf/pdf/technology/2017/T298.pdf (Viitattu: 09.04.2019)

[39] P. Mueller, B. Yadegari, The Stuxnet Worm, 12 s. Saatavissa: https://www2.cs.arizona.edu/~collberg/Teaching/466-566/2013/Resources/presentations/2012/topic9-final/report.pdf (Viitattu: 02.04.2019)

[40] Timeline: How Stuxnet attacked a nuclear plant, BBC. Saatavissa: https://www.bbc.com/timelines/zc6fbk7 (Viitattu: 02.04.2019)

[41] P. Mittal, S. Soltan, H. Vincent Poor, BlackIoT: IoT Botnet Of High Wattage Devices Can Disrupt the Power Grid, 27th USENIX Security Symposium, Baltimore, USA, 2018. Saatavissa: https://www.usenix.org/system/files/conference/usenixsecurity18/sec18-soltan.pdf (Viitattu: 03.04.2019)

[42] T. Muhonen, J. Oksanen, Suomen sähköverkkoon hyökätään jatkuvasti - myös suurvallat aktiivisia, Ilta-Sanomat, 2017. Saatavissa: https://www.is.fi/taloussanomat/art-2000005101603.html (Viitattu: 10.03.2019)

[43] Suomen kyberturvallisuusstrategia, Turvallisuuskomitea, 2013, 40 s. Saatavissa: https://turvallisuuskomitea.fi/wp-content/uploads/2018/05/Suomen-kyberturvallisuusstrategia-ja-taustamuistio.pdf (Viitattu: 14.03.2019)