VAASAN YLIOPISTO

TEKNILLINEN TIEDEKUNTA

SÄHKÖTEKNIIKKA

Jere Mäki

KAUKOKÄYTTÖJÄRJESTELMÄN TIETOTURVALLINEN OPEROINTI JA YLLÄPITO

Diplomityö, joka on jätetty tarkastettavaksi diplomi-insinöörin tutkintoa varten Vaasassa 26.10.2016

Työn valvoja	Professori Kimmo Kauhaniemi
Työn ohjaaja	Diplomi-insinööri Lasse Autio
Työn tarkastaja	Professori Timo Mantere

SISÄLLYSLUETTELO

LYHENNELUETTELO

AGA	American Gas Association, Amerikan kaasuyhdistys
ANSI	American National Standards Institute, Amerikan kansallinen standardointijärjestö
API	American Petroleum Institute, Amerikan öljyjärjestö
BYOD	Bring your own device, omat laitteet käytössä
CERT	Computer Emergency Response Team, tietoturvaloukkauksiin ja niiden ennaltaehkäisyyn keskittyvä ryhmä
CIP	Critical Infrastructure Protection, kriittisen infrastruktuurin suojaus
CSIRT	Computer Security Incident Response Team, tietoturvaloukkauksiin ja niiden ennaltaehkäisyyn keskittyvä ryhmä
CSSP	Control System Security Program, Yhdysvaltain Home Security -hallinnon tietoturvaohjelma
DMS	Distribution Management System, käytöntukijärjestelmä
EAL	Evaluation Assurance Level, ISO/IEC 15408 -standardin vaatimustaso
ENISA	The European Network and Information Security Agency, EU:n tietoturvatoimija
EU	Euroopan unioni
HAVARO	Tietoturvaloukkausten havainnointi- ja varoitusjärjestelmä
ICS	Industrial Control Systems, teollisuusautomaatio
ICS-CERT	Industrial Control Systems Cyber Emergency Response Team, teollisuusautomaation tietoturvaloukkauksiin ja niiden ennaltaehkäisyyn keskittyvä ryhmä
IEC	International Electrotechnical Commission, kansainvälinen sähköalan standardointiorganisaatio
IED	Intelligent Electronic Device, älykäs sähköinen laite
IoT	Internet of Things, esineiden internet

ISA	Instrumentation, Systems and Automation Society, yhdysvaltalainen globaali automaatioteollisuuden asiantuntijoiden organisaatio
ISA99	Industrial Automation and Control Systems Security Standards, ISA:n automaatiojärjestelmän tietoturvastandardit
ISMS	Information Security Management System, tietoturvan hallintajärjestelmä
ISO	International Organization for Standardization, Kansainvälinen standardisointiorganisaatio
IT	Informaatioteknologia, tietotekniikka
Katakri	Kansallinen turvallisuusauditointikriteeristö
MITM	Man-in-the-middle, mies välissä -hyökkäys
NCSA	National Communications Security Authority, kansallinen tietoturvaviestintävastaava
NERC	North American Electric Reliability Corporation, Pohjois-Amerikan sähköalan luotettavuus yhteisö
NIST	National Institute of Standards and Technology, kansallinen standardi ja teknologia-instituutti
NTP	Network Time Protocol, aikasynkronointi protokolla
PDCA	Plan-Do-Check-Act, suunnittele-toteuta-arvioi-toimi -malli
SCADA	Supervisory Control And Data Acquisition, kaukokäyttöjärjestelmä
Tekes	Teknologian ja innovaatioiden kehittämiskeskus
TITAN	Tietoturvaa teollisuusautomaatioon
VPN	Virtual Private Network, erillisverkko
VTT	Valtion teknillinen tutkimuskeskus

VAASAN YLIOPISTO
Teknillinen tiedekunta
Tekijä: Jere Mäki
Diplomityön nimi: Kaukokäyttöjärjestelmän tietoturvallinen operointi ja ylläpito
Valvojan nimi: Professori Kimmo Kauhaniemi
Ohjaajan nimi: Diplomi-insinööri Lasse Autio
Tarkastajan nimi: Professori Timo Mantere
Tutkinto: Diplomi-insinööri
Oppiaine: Sähkötekniikka
Opintojen aloitusvuosi: 2007
Diplomityön valmistumisvuosi: 2016 **Sivumäärä:** 75

TIIVISTELMÄ

Tietoturva on noussut viime vuosien aikana esille mediassa. Stuxnet-haittaohjelma hyökkäsi muutama vuosi sitten automaatiojärjestelmään tehden suurta tuhoa. Vuoden vaihteessa julkaistiin uutinen, jonka mukaan hakkerit olivat päässeet murtautumaan USA:n energiaverkkoon. Samoihin aikoihin Ukrainassa hakkerit olivat onnistuneet katkaisemaan sähkönjakelun. Tällaiset tapahtumat ovat johtaneet siihen, että kansalliset tahot, kuten Huoltovarmuuskeskus ja kansainväliset tahot, kuten ENISA ovat luoneet ohjeistuksia kriittisten järjestelmien turvaamiseksi. Sisäministeriön tuoreimpaan riskinarvioon kuuluu myös kybertoimintaympäristön riskit, jotka voivat äärimmilleen mennessä johtaa hyökkäyksiin myös yhteiskunnallisesti tärkeää sähkönjakelua vastaan. Tämä diplomityö pyrkii määrittämään sähköverkon kaukokäyttöjärjestelmän tietoturvallisia toimia, joilla pyritään pienentämään murtautumisriskiä.

Teorian alussa esiteltiin sähköverkko ja sen hallintaan käytettävä kaukokäyttöjärjestelmä. Sähköverkon luonne yhteiskunnallisesti kriittisenä infrastruktuurina johtaa siihen, että tietoturvaa tulee parantaa jatkuvasti. Työssä avattiin tietoturva käsitteenä ja esitettiin tietoturvan yleinen jako osa-alueisiin. Tietoturvan toteuttamiseen ja hallintaan liittyen käytiin läpi kaukokäyttöjärjestelmään soveltuvia kansallisia ja kansainvälisiä vaatimuksia, standardeja ja ohjeistuksia.

Kaukokäyttöjärjestelmän tietoturvan heikkoja kohtia etsittiin vertailemalla energia-alalle tehtyjä aiempia tutkimuksia sekä kohdennetun sähköpostikyselyn avulla. Havaittuihin ongelmiin pyrittiin muodostamaan kaukokäyttöjärjestelmän tietoturvallisen operoinnin ja ylläpidon kannalta olennaisia toimia vertailemalla Katakri-auditointikriteeristön ja ISO/IEC 27000 -standardiperheen asettamia vaatimuksia.

Työn tuloksena kaukokäyttöjärjestelmän tietoturvaa tulisi viedä eteenpäin tietoturvapolitiikan paremmalla tiedottamisella ja vastuiden selkeyttämisellä. Kaukokäyttöjärjestelmän operointia tulisi parantaa ohjeistamisella niin normaali- kuin poikkeustilanteissa. Järjestelmän ylläpitäjällä tulee olla riittävä osaaminen tietoturvalliseen ylläpitämiseen ja hallintaan.

AVAINSANAT: Kaukokäyttö, tietoturva, sähköverkko

UNIVERSITY OF VAASA
Faculty of technology
Author: Jere Mäki
Topic of the Thesis: Cyber secure operating and maintenance of the SCADA system
Supervisor: Professor Kimmo Kauhaniemi
Instructor: Master of Science in Technology Lasse Autio
Evaluator: Professor Timo Mantere
Degree: Master of Science in Technology
Major of Subject: Electrical Technology
Year of Entering the University: 2007
Year of Completing the Thesis: 2016 **Pages:** 75

ABSTRACT

Cyber security has under the last few years been a major subject of discussion in media. Couple of years ago a Stuxnet-malware attacked and damaged an automation system. At the turn of the year a presumably successful hacking into the USAs power grid made the headlines. In the meanwhile in Ukraine hackers had managed to shut off the power supply. Events like this have led to that national actors like National Emergency Supply Agency and international actors like ENISA have created instructions about how to secure critical systems. Even the risks of cyber environment, which can at their most extreme lead to attacks against socially important power supply, are included in the latest risk assessment of the Ministry of the Interior. This M.Sc. thesis has as objective to define cyber secure actions that can minimize the chances of a potential cyber-attack.

In the beginning of the theory chapter the power grid and SCADA, which is used to control the power grid, are presented. The nature of the power grid as a socially critical infrastructure leads to the need to develop cyber security constantly. In this thesis the concept of cyber security and the general division of it into subsections are presented. Concerning the implementation and control of cyber security are the national and international requirements, standards and directives, which are applicable into SCADA, scrutinized. The weaknesses of cyber security in SCADA were searched for with a comparison of previous research in the field of energy as well as with a help of allocated email questionnary. Essential actions for cyber secure control and maintenance of SCADA were developed for the detected problems by comparing the criteria set by the Katakri-auditing criteria and the ISO/IEC 27000 -standards.

The results of this study show that the cyber security of SCADA should be developed by means of better information about cyber security policy and by means of clarifying the responsibilities. The operation of the SCADA should be improved by better briefing for both normal and exceptional situations. The operator of the system should be competent enough both to maintain and to control the system.

KEYWORDS: SCADA, cyber security, power gird

1 JOHDANTO

Elämme murroksessa, jossa digitalisaatio lisääntyy huimaa vauhtia lähes kaikilla aloilla. Samalla kun kaikki laitteet liitetään osaksi julkista internetiä, herää kysymys pystytäänkö tämä toteuttamaan tietoturvallisesti. Tietoturva onkin noussut viime vuosien aikana usein esille mediassa tietoturvamurtojen ja -hyökkäysten vuoksi, koska teknisten mahdollisuuksien nopeassa kehityksessä tietoturva ei aina ole pysynyt mukana. Tietoturvamurrot ovat kohdentuneet kahvinkeitinten ja pesukoneiden lisäksi myös erilaisiin logiikkoihin ja automaatiojärjestelmiin. Näistä esimerkkinä muutaman vuoden takainen mediatapaus Stuxnet-haittaohjelmasta, joka kylvi tuhoa automaatiojärjestelmissä.

Kun kohteeksi valikoituu kahvinkeittimen sijaan sähköverkon kaukokäyttöjärjestelmä, ja sen komponentit, voidaan olettaa, että asialla ei ole tavallinen hakkeri vaan erilaisilla intresseillä liikkeellä olevat näkymättömät toimijat ja tahot. Tämän vuoksi erilaiset kansalliset ja kansainväliset tahot ovat alkaneet vaatia ja ohjeistaa yhteiskunnallisesti tärkeiden toimijoiden tietoturvan toteuttamista. Tämän hetken esimerkkinä toimivat joulu-na 2015 Ukrainassa useita asuntoja pimentänyt hyökkäys ja useat uutisoinnit mm. USA:n energiaverkkoa kohtaan tehdyistä murroista.

Aihe diplomityölle löytyi edellä mainittujen tapahtumien ja lukuisten muiden tietoturvamurtojen virittämästä keskustelusta työympäristössä, mikä on johtanut järjestelmien tietoturvan tarkasteluun. Tarkastelen miten tietoturva toteutuu yhteiskunnalle kriittisen infrastruktuurin operoinnin ja ylläpidon osalta, kun järjestelmä on teknisen kehityksen myötä ohjauspaikasta riippumaton. Diplomityössä on tarkoitus syventyä yhteiskunnallisesti kriittisen sähkönjakelun tietoturvallisen operoinnin ja ylläpidon toteuttamiseksi vaadittaviin toimiin. Sähköverkon hallinnan osalta tärkeä kohde on keskitetty valvomo. Tästä johtuen diplomityö keskittyy kaukokäyttövalvomossa tapahtuvaan kaukokäyttöjärjestelmän operointiin ja ylläpitoon, ottaen huomioon kuitenkin nykypäivän etäkäytettävyysvaatimukset.

Vallitsevan tietoturvatilanteen selvittämiseksi työssä tarkastellaan myös aiempia aiheeseen liittyviä tutkimuksia, kuten Renecon 2013 tekemää tutkimusta verkostoautomaatiojärjestelmän tietoturvasta sekä XCure Solutions Oy:n 2015 tekemää raporttia kyberturvallisuuden tilannekuvasta energia-alalla. Aiemmissa tutkimuksissa havaittuja ongelmakohtia pyritään selvittämään vertailemalla tietoturvalle asetettuja kansallisia ja kansainvälisiä vaatimuksia ja ohjeistuksia.

Johdannon jälkeen luvussa 2 lähdetään liikkeelle sähköverkon piirteiden ja kokonaisuuden määrittelyllä. Tämän jälkeen syvennytään myös kaukokäyttöjärjestelmään ja sen liittymiseen osaksi sähköverkkoa. Tämän jälkeen luku 3 esittelee tietoturvan ja yleisen tavan jakaa se osa-alueisiin. Osa-alueiden esittelyn jälkeen esitellään yleisiä tietoturvavaatimuksia sekä sähkönjakeluun suunnattuja vaatimuksia. Kappaleessa 3.3 esitellään kansalliset ja kansainväliset tietoturvaohjeistukset ja -standardit, joita voidaan soveltaa sähköverkon kaukokäyttöjärjestelmään. Kappaleessa 3.4 puolestaan esitellään yleisimmät tietoturvauhat sekä tietoturvahyökkäyksiä operoivat toimijat. Kappaleessa käydään läpi myös Ukrainan sähköverkkoa kohtaan tehty hyökkäys ja sähköverkon kaukokäyttöjärjestelmään kohdistuvia uhkia. Luvussa 4 analysoidaan kaukokäyttöjärjestelmän tietoturvallista operointia ja ylläpitoa sähköpostikyselystä ja aiemmista tutkimuksista muodostettavan yleiskuvan perusteella. Luvun alussa käydään läpi myös tutkielman menetelmällinen näkökulma, joka nojautuu luvussa 3 esitettävien tietoturvavaatimuksien ja -ohjeistuksien kvalitatiiviseen vertailuun. Luvun 4 lopussa kootaan johtopäätökset ja luku 5 on työn yhteenveto.

2 SÄHKÖVERKON KAUKOKÄYTTÖJÄRJESTELMÄ

Kaukokäyttö- eli käytönvalvontajärjestelmä SCADA (Supervisory Control And Data Acquisition) on sähkönjakeluverkon reaaliaikainen valvontajärjestelmä. Kaukokäyttöjärjestelmän avulla verkon valvonta ja ohjaukset voidaan keskittää valvomoihin, mutta keskitetyn valvonnan lisäksi on mahdollista rakentaa myös paikallisia SCADA-järjestelmiä sähköasemille. (Lakervi & Partanen 2008: 234–235.)

Suomen kansallisen riskiarvion (2015) mukaan sähkön jatkuva saanti on tärkeää, jotta yhteiskunnan elintärkeät toiminnot voidaan turvata. Lyhyetkin, alle 10 sekunnin mittaiset, katkokset voivat aiheuttaa teollisuusprosesseille ongelmia ja pitkittyessään katko voi pysäyttää yhteiskunnan toiminnot. Sähkönjakeluverkossa tapahtuvat viat johtavat useimmiten myös sähkönjakelun häiriintymiseen. (Sisäministeriö 2016: 14–13.) Tämän vuoksi sähköverkon kaukokäyttöjärjestelmän on vastattava erityisiin luotettavuusvaatimuksiin.

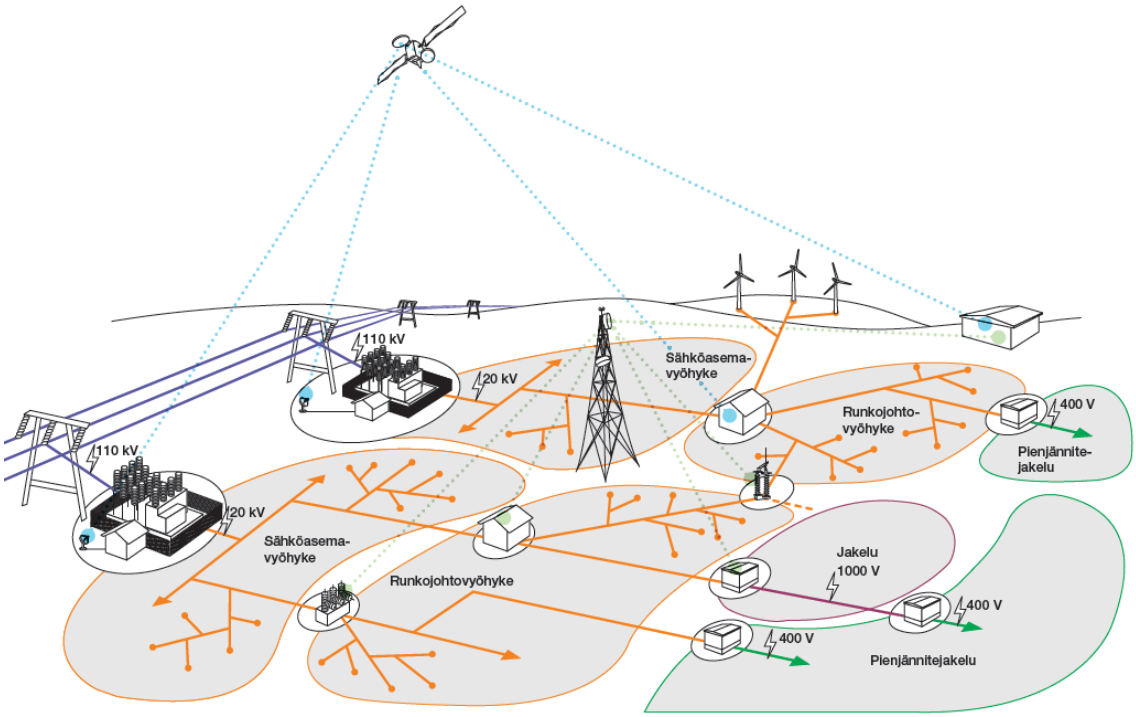
2.1 Sähköverkon piirteet

Suomessa sähkönjakelu on tarkasti säädeltyä monopolitoimintaa, jota valvoo Energiamarkkinavirasto (Lakervi & Partanen 2008: 19–21). Energiamarkkinaviraston valvonnan lisäksi kuluttajia suojaamaan on säädetty sähkömarkkinalaki 588/2013, joka velvoittaa sähköverkon haltijoita kehittämään verkon käyttövarmuutta. Laki määrittelee sähkökatkoksen enimmäispituudeksi asemakaava-alueella kuusi tuntia ja muualla 36 tuntia. Tämän lisäksi laissa on velvoite varautumissuunnitelman teosta häiriötilanteiden varalle ja suunnitelman hyväksyy Huoltovarmuuskeskus. Siirtymäaikaa lain täytäntöönpanoon on annettu porrastetusti joulukuun 2028 loppuun, jota ennen yhtiöiden tulee asteittain kehittää verkkoaan. Verkon tulee vastata täysin vaatimuksiin siirtymäajan päättyessä. (Sähkömarkkinalaki: 588/2013.)

Sähköverkko koostuu kanta-, alue-, keskijännite- ja pienjänniteverkosta, joilla kaikilla on käytössä omat jännitetasonsa (Lakervi & Partanen 2008: 11). Kantaverkosta vastaa valtion enemmistöomistuksessa oleva Fingrid, jonka lisäksi vastuu sähkönjakeluverkosta jakautuu monelle eri sähköverkon haltijalle. Syksyllä 2016 Suomessa oli Energiaviraston mukaan 93 verkon haltijaa. Näistä suurimmilla yhtiöillä, kuten Caruna Oy:llä ja Elenia Oy:llä asiakasmäärät ovat olleet 2014 vuoden raportin mukaan yli 400 000 verkkopalveluasiakasta ja jakeluverkon pituutta on kertynyt yli 65 000 kilometriä. Vastaavasti pienin yhtiö vuonna 2014 oli Karhu Voima, jolla palveltavia asiakkaita oli vain 79 kappaletta ja verkkoa 38,9 kilometriä. (Energiateollisuus 2015a; Energiavirasto 2016a; Energiavirasto 2016b.)

Sähköverkot muodostuvat säteittäisistä-, rengas- ja silmukkaverkoista. Säteittäiset verkot ovat yleisiä pienjänniteverkoissa taajaman ulkopuolella, koska ne ovat edullisia ja niille on helppo toteuttaa suojausasettelut. Rengasmalli on käytössä puolestaan taajamassa, mikä takaa paremman varmuuden ja jännitevakavuuden. Rengasmallia hyödynnetään myös 110 kilovoltin verkossa, mutta normaalitilanteessa rengasta ei pidetä suljettuna. Silmukkarakennetta käytetään kantaverkossa suurilla jännitteillä, kuten 400 ja 220 kilovolttia. Näin saavutetaan hyvä jännitevakavuus ja pienet siirtohäviöt. (ABB Oy 2000: 341; Elovaara & Haarla 2011: 57.)

Sähköverkon solmukohdissa sijaitsevat sähköasemat, jotka ovat monipuolisia jakelukeskuksia. Sähköasemat sisältävät verkkoa suojaavia suojareleitä, automaatiota, eri jännitetasojen kytkinlaitoksia ja muuntajia. Pienjänniteverkon rajalla käytetään sähköasemien sijasta puisto-, kellari- ja pylväsmuuntamoita, jotka sisältävät pienjännitepuolen ylivirtasuojauksia. Sähköasemien ja muuntamoiden lisäksi verkossa on myös paljon kauko-ohjattavia kytkinlaitteita, kuten erottimia, kuormaerottimia ja pylväskatkaisijoita. Näillä voidaan rajata vikaantunut alue nopeasti ja palauttaa sähköt toimivaan osaan verkkoa. Erottimet sijoitetaan yleensä verkon risteyskohtiin tai paikkoihin, jotka sijaitsevat kaukana valvomosta. (Lakervi & Partanen 2008: 119–121, 151–152, 157–158; Korpinen 2015: 4.) Kuva 1 esittää perinteistä sähköverkon rakennetta 110 kilovoltin siirtolinjasta pienjännitejakeluun.



Kuva 1. Sähköverkko (Salin 2015: 11).

Tulevaisuuden älyverkot puolestaan tulevat toimimaan kaksisuuntaisesti kahdessa tasossa. Tietoliikenne kulkee omassa tasossaan ja sähköenergia omassa tasossaan. Verkkorakenne tulee koostumaan suurilta osin hajautetuista energialähteistä sekä energian tuottajakuluttaja-asiakkaista (prosumers). Uudenlainen verkkorakenne kuvassa 2 pyrkii sähkön laadun ja luotettavuuden parantamiseen lisäten samalla kuluttajan mahdollisuuksia vaikuttaa sähkön käyttöön. (Delgado-Gomes, Martins, Lima & Nicolae Borza 2015: 534–535.) Suomessa tällaisia älyverkkopilotteja on rakennettu mm. Helsingin Kalasatamaan, Vaasan Sundomiin ja Oulun Hailuotoon (Jaspers 2014).

Kuva 2. Älyverkon rakennemalli (ABB Oy 2016: 4).

2.2 Kaukokäyttöjärjestelmä

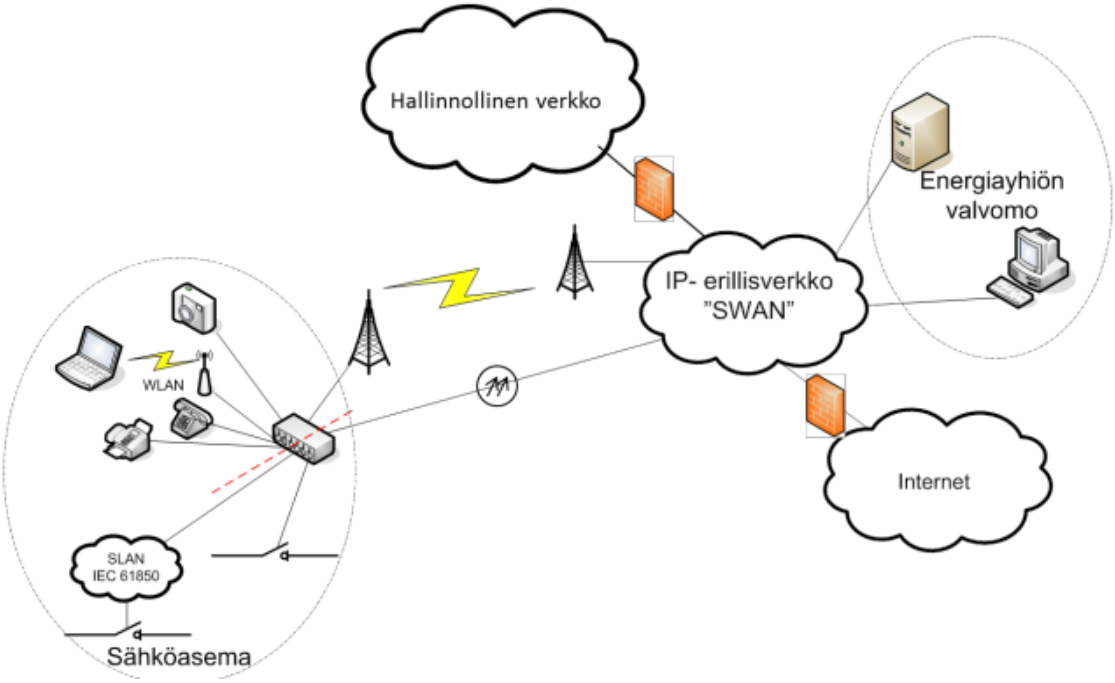
Kaukokäyttöjärjestelmät ovat olleet merkittävä askel sähköverkkojen automatisoitumisen historiassa. Kaukokäyttöjärjestelmien yleistyminen Suomessa tapahtui 1970-luvulla. Myöhemmin kaukokäyttöjärjestelmän ovat kehittyneet ja laajentuneet mikroprosessori- ja tietojenkäsittelytekniikan myötä. Laajempia kaukokäyttöjärjestelmä-kokonaisuuksia kutsutaan käytönvalvontajärjestelmiksi. (Korpinen 2015: 1.) Käytönvalvontajärjestelmään kuuluvat ala-asemat, älykkäät releet, tietoliikenneyhteydet, tiedonkeruu- ja sovelluspalvelimet, tietokanta ja käyttöliittymä (ABB Oy 2000: 408–409; Martikainen 2005: 23; Lakervi & Partanen 2008: 235).

Sähköverkon mittalaitteet ja älykkäät suojarele- ja ohjausyksiköt keräävät kaukokäyttöön tarvittavaa reaaliaikaista tietoa, jonka ne välittävät edelleen kaukokäyttöjärjestelmään itsenäisesti tai sitten ala-aseman avulla. Tiedonsiirto ala-asema ja ohjauslaitteiden välillä toimii myös toiseen suuntaan, jolloin kaukokäytöstä voidaan lähettää esimerkiksi ohjauskomentoja, aikasynkronointisanomia tai laitteiden asetteluja ala-asemalle. (ABB

Oy 2000: 409–410; Martikainen 2005: 23.) IEC 61850 -standardin myötä on tullut myös mahdolliseksi toteuttaa sähköaseman suojauksien keskittämistä asema-automaatio-tietokoneelle (Valtari 2013: 48–49).

Ala-asemat sekä suojarele- ja ohjausyksiköt sijaitsevat mm. sähköasemilla, puistomuuntamoissa, kauko-ohjattavissa maastoerottimissa ja katkaisijoissa, joista on tietoliikenneyhteydet kaukokäyttöjärjestelmään. Tiedonsiirrolla on valvonta- ja ohjauspaikasta riippuen erilaisia vaatimuksia, kuten tiedon aikakriittisyys ja luotettavuus. Yhteys sähköasemalta valvomoon tulee olla nopea ja luotettava, kun puolestaan maastoerottimen yhteys voi vähäisemmän käytön vuoksi olla vähemmän aikakriittinen. Kaukokäyttöyhteyksien tiedonsiirrossa käytettyjä tekniikoita ovat radiolinkkiyhteys, valokuitu, kiinteä kaapeli, radiopuhelinverkko, lankapuhelinverkko, matkapuhelinverkkodata, sähköverkkotiedonsiirto ja pakettiradioverkko. (Lakervi & Partanen 2008: 245.) Sähköaseman ja valvomon välisissä yhteyksissä on nykyisin laajalti käytössä valokuitu, kun taas erotinasemien langattomissa yhteyksissä suositaan matkapuhelinverkkodataa (Tervo 2012).

Sähkönjakelun yhteiskunnallisen tarpeellisuuden vuoksi tärkeissä sähköverkon ohjauspisteissä tulee varmistaa kaukokäyttöjärjestelmän tietoliikenne kahdella toisistaan riippumattomalla yhteydellä, joiden avulla voidaan taata korkea käytettävyys ja luotettavuus (Sisäministeriö 2016: 14–13; Tervo 2012). Kuva 3 on periaatteellinen kuvaus kaukokäyttöjärjestelmän kahdennetusta tietoliikenneyhteydestä sähköasemalle, jossa ensisijaisena yhteytenä toimii valokuitu ja varayhteytenä käytetään langatonta linkkiä. Julkiset matkapuhelinverkot eivät välttämättä ole oikea ratkaisu varayhteydeksi, koska tukiasemien varavirta saattaa riittää vain noin kolmen tunnin ajaksi (Tervo 2012).

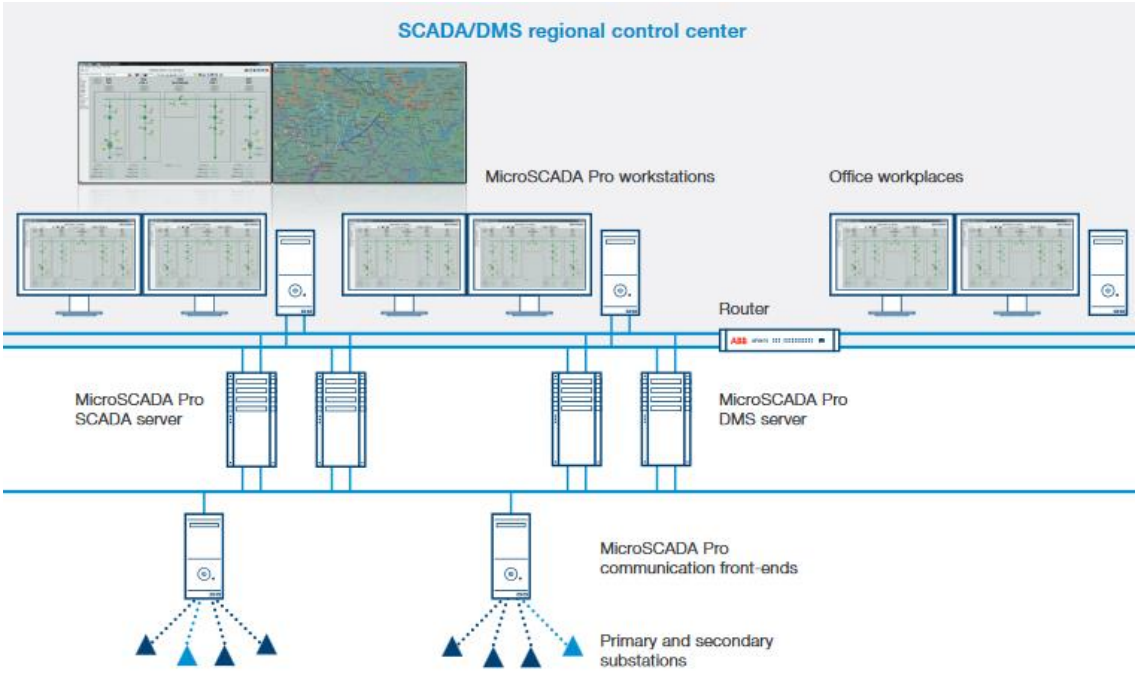


Kuva 3. Kaukokäytön ja sähköaseman välinen tietoliikennerakenne (Tervo 2012).

Kaukokäyttöjärjestelmä SCADA:n ydin koostuu varmennetuista tietokoneista, tiedonsiirtojärjestelmäliitynnästä ja tietojärjestelmäsovelluksesta, jota ohjataan korkeatasoisen käyttöliittymän kautta. Järjestelmä hallitsee verkon tapahtumatietoja, verkon kytkentätilannetta, kaukomittauksia, raportointia ja sillä pystytään tarvittaessa ohjaamaan verkon toimilaitteita. Tämän lisäksi SCADA voi jakaa verkon reaaliaikaisia tietoja myös muille tukiohjelmistoille, kuten käytöntukijärjestelmä DMS:lle (Distribution Management System). (Lakervi & Partanen 2008: 235–236.)

MicroSCADA Pro on ABB Oy:n kaukokäyttöjärjestelmätuote, jolla voidaan valvoa ja ohjata sähkönjakelujärjestelmää. Sähkön lisäksi tuotteen sovellusalueita ovat kaasu-, öljy-, vesi- ja lämpösovellukset. Kaukokäyttöjärjestelmä voidaan rakentaa kuvan 4 mukaisesti, jolloin käytetään kahdennettuja toisensa peilaavia sovellus-servereitä. Tällöin toinen servereistä on kuumana ja ajaa pääsovellusta ja toinen servereistä varjostaa kuumana olevaa pääsovellusta. Kuuman serverin vikaantuessa lähtee varjostavan serverin pääsovellus välittömästi käyntiin. Tietoliikenteen kahdennus voidaan toteuttaa IEC 80870-5-101 ja -104 ja IEC 62429/PRP protokollilla. Kuvassa 4 kaukokäytön rinnalla on myös DMS, joka helpottaa vian paikannusta sähköverkossa. MicroSCADA Pro so-

vellus pystyy toimimaan sekä kaukokäyttöjärjestelmänä että tietoliikennekoneena. (ABB Oy 2014: 8–12.)



Kuva 4. Käytönvalvonta- ja käytöntukijärjestelmä rinnakkain (ABB Oy 2014: 8).

Sähköverkon kaukokäyttöjärjestelmää operoi käytönvalvoja, jonka työpiste on valvomossa. Valvomossa käytönvalvojalla on pääsy kaikkiin kaukokäyttöjärjestelmän tila-, tapahtuma- ja mittaustietoihin. Tämän lisäksi käytönvalvojalla on mahdollisuus ohjata sähköverkkoa ja muuttaa näin sen tilaa tarvittaessa. (Martikainen 2005: 23.) Kaukokäyttöjärjestelmän ylläpidosta vastaavat sähköyhtiön tehtävään kouluttamat henkilöt, mutta on myös mahdollista, että yhtiö ostaa tarvittavat ylläpitotoimenpiteet kaukokäyttöjärjestelmän toimittajalta. Kaukokäyttöjärjestelmän ylläpitovastuita voidaan jakaa osa-alueisiin, kuten SCADA-sovellus, tietoliikenne ja ala-asemat. (Isomäki 2016.)

MicroSCADA Pro tarjoaa käytönvalvojalle dynaamisen nopeasti päivittyvän näkymän verkon tilasta, havainnolliset hälytykset prosessikuvassa sekä laitteiden lukitusten ja suojausten osoittamisen. Järjestelmä sisältää myös kattavat hälytys- ja tapahtumalistaukset, joiden suodatusominaisuudet ovat monimuotoiset. Mittaustiedoista voidaan piirtää selkeää trendikäyrä, ja teho- ja häviöraportit puolestaan ohjaavat verkon energia-

ja kustannustehokkaaseen hallintaan. Kaukokäyttöjärjestelmän ylläpitäjille MicroSCADA:sta löytyy rakennustyökalut sekä valmiit kirjastot ohjausdialogeille ja prosessikohdesymboleille. Kaukokäyttöjärjestelmän tietoliikennettä voidaan diagnosoida työkalulla ja sen voi myös salata. Ylläpitäjälle turvallisuuden kannalta tärkeitä ominaisuuksia ovat myös käyttäjien tunnistus sekä oikeutukset, jotka jäävät myös tapahtumalistalle. MicroSCADA vastaa IEC 62351, IEEE 1686 ja NERC CIP tietoturvavaatimuksiin. (ABB Oy 2014: 8–12.)

3 TIETOTURVA

Andreassonin ja Koiviston (2013: 29) mukaan tietoturvallisuudella tarkoitetaan ”tietojen, palveluiden, järjestelmien ja tietoliikenteen suojaamista ja niihin kohdistuvien riskien hallitsemista sekä normaali- että poikkeusoloissa hallinnollisilla, teknisillä ja muilla toimenpiteillä.” Tietoturva voidaan jaotella osiin monin eri tavoin, mutta yleisesti organisaatioissa on käytössä seuraavanlainen jaottelu: hallinnollinen turvallisuus, henkilöstöturvallisuus, fyysinen turvallisuus, tietoliikenneturvallisuus, laitteistoturvallisuus, ohjelmistoturvallisuus, tietoaineistoturvallisuus ja käyttöturvallisuus (Andreasson & Koivisto 2013: 52).

Tietoturvalle voidaan sovelluskohteesta riippuen asettaa erilaisia vaatimuksia ja tietoturvaa voidaan toteuttaa yrityksissä ja järjestelmissä erilaisia ohjeistoja ja standardeja mukaillen. Tietoturva on olennainen osa nykyhetkeä ja tulevaisuutta, minkä vuoksi tietoturvan saralla on eritasoisia ohjeistajia, vaatimusten asettajia sekä säännöstön laatijoita. Suomessa on 1.1.2014 alkaen toiminut Kyberturvallisuuskeskus, jonka tietoturvapalveluihin kuuluvat mm. CERT (Computer Emergency Response Team) ja NCSA (National Communications Security Authority) -tehtävät. Kyberturvallisuuskeskus on Suomen valvova viranomainen, joka pyrkii toiminnallaan varmistamaan häiriöttömät ja turvalliset viestintäverkot sekä -palvelut. Kyberturvallisuuskeskus tähtää myös jokapäiväisten yhteiskunnallisesti elintärkeiden toimintojen turvaamiseen. (Viestintävirasto 2016a.) Euroopan unionin tasolla tietoturvaohjeistuksesta, -sääntelystä ja -suosituksista vastaa ENISA (The European Network and Information Security Agency), joka on perustettu 2004 Kreikkaan (ENISA 2016a).

3.1 Tietoturvan osa-alueet

Hallinnollinen turvallisuus on avainasemassa tietoturvan määrittelyssä, suuntausten valinnassa ja seurantatyökalujen valitsemisessa. Organisaation tulee määrittää ja toteuttaa tietoturvaa siinä määrin, kun se tukee organisaation perustehtävän ja strategian saavut-

tamiseen tarvittavia panostuksia. Ihannetilanteessa tulisi pyrkiä siihen, että tietoturva on luonnollinen osa toimintaa ja organisaation riskienhallintaa. Organisaation täytyy kansalaisten yksityisyydensuojan ja yrityssalaisuuksien vuoksi huolehtia tietojen salassapidosta. Yhtiönjohto ja esimiehet vastaavat, että hallinnollinen turvallisuus toteutuu muillakin tietoturvallisuuden osa-alueilla. Halutun tietoturvatason saavuttamiseksi laaditaan organisaatiossa kirjallinen tietoturvapolitiikka, joka sisältää tavoitteet, tietoturvaan ohjaavat tekijät, tietoriskien hallinnan määrittelyn, tietoturvallisuuden merkityksen organisaatiolle, toimintojen priorisoinnin, tietoturvallisuuden hallintajärjestelmän, tietoturvavastuut, tietoturvakoulutuksen ja perehdytyksen, tietoturvallisuuden tiedottamisen, toteutumisen valvonnan ja toimintamallin poikkeustilanteissa. (Andreasson & Koivisto 2013: 32–36.)

Henkilöstöturvallisuus on osa-alue, joka paneutuu henkilöstön salassapito- ja käytettävyysriskienhallintaan tietoja ja tietojärjestelmiä käytettäessä. Tätä tietoturvan osa-aluetta pidetään keskeisenä, mutta haasteen tietoturvalle aiheuttaa toimija, ihminen. Henkilöstöturvallisuuteen kuuluu erityisesti tiedon käyttäjien ja muokkaajien määrittely. Näin ollen vain tietoihin oikeutetut ja riittävän turvatason omaavat henkilöt pääsevät käyttämää organisaation arkaluonteista tai yksityisyydensuojan alaista tietoa. Suojaukseen käytettävät estomenetelmät kuuluvat myös henkilöstöturvallisuuden alueeseen. (Valtiovarainministeriö 2008a: 11–14.)

Valtiovarainministeriön (2008b: 30) mukaan fyysinen turvallisuus sisältää muun muassa ”kulun- ja tilojenvalvonnan, vartioinnin, palo-, vesi-, sähkö-, ilmastointi- ja murtovahinkojen torjunnan sekä kuriirien ja tietoaineistoja sisältävien lähetysten turvallisuuden”. Näiden alueiden vuoksi fyysiseen turvallisuuteen kuuluu säännöksiä, jotka ovat työturvallisuus-, pelastus- ja arkistolaissa sekä laissa yksityisyydensuojasta työelämässä. Fyysiseen turvallisuuteen kuuluu olennaisesti myös tilaturvallisuus, jolla tarkoitetaan henkilöstön, tietojen ja materiaalien suojausta. Fyysisen suojauksen kokonaisuus on laaja ja monitasoinen. Sen avulla luodaan valmiit toimintamallit erilaisten ongelma- ja häiriötilanteiden osalle. Kohteen määrittelyssä huomioidaan kokonaisuus rakenteellisista ratkaisuista, kuten vahvistetuista seinistä, ovista ja ikkunoista, lähtien. Kohteen valvontaan voidaan käyttää tarpeiden mukaan video-, kulku- tai tunkeutumisvalvontaa, jotka

voivat olla yhteydessä kiinteistöautomaatiojärjestelmään. Äärimmäisissä suojausvaatimuksissa varavoima-vaatimuksen lisäksi saatetaan vaatia sähkömagneettisen pulssin tai suuritehoisen mikroaallon kestoa. (Andreasson & Koivisto 2013: 52–56.)

Tietoliikenneturvallisuus on ”tiedonsiirtoyhteyksien käytettävyyden, tiedonsiirron turvaamisen, suojaamisen ja salaamisen, käyttäjän tunnistamisen ja verkon varmistamisen turvallisuustoimenpiteet sekä lainsäädäntö, normit ja toimet, joilla pyritään aikaansaamaan tietoliikenteen turvallisuus” (Valtiovarainministeriö 2008b: 103). Tietoliikenneturvallisuus sisältää siis tietoliikennelaitteiden valvontaa, verkon hallintaa, ongelmatilanteiden selvittelyä ja kirjaamista, viestinnän salauksen hallintaa ja myös tietoliikenneohjelmien testausta. Tietoliikenneturvallisuuteen liittyen säädettyjä lakeja ovat viestintämarkkinalaki ja sähköisen viestinnän tietosuojalaki. Tietoliikenneturvallisuutta toteutetaan verkon suunnittelussa, jossa määritellään verkkoon liitettävät laitteet ja niiden toiminta-alueet. Fyysiset ja virtuaaliset alueet voidaan erotella toisistaan palomuurein, joilla pystytään myös tarkkailemaan ja säännöstelemään tarkasti liikennettä alueiden ja laitteiden välillä. Kriittisten laitteiden kanssa tulee ottaa huomioon kahdennetut tiedonsiirtoväylät. Ulospäin olevat yhteydet puolestaan tulee varmistaa varayhteyksien avulla siten, että ne vikatilanteessa takaavat riittävän palvelutason. Aktiivisten verkkolaitteiden fyysinen sijoittelu ja asettelu tulee toteuttaa minimoiden tunkeutumisriski. Verkon liityntärajapintaa tulee pohtia, sillä langattomien verkkojen osalta tietoturvan ja yhteyden salauksen kanssa tulee olla huomattavasti tarkempi, kuin lähiverkkojen kanssa. Langatonta verkkoa voidaan häiritä esimerkiksi tehokkaalla radiosignaalilla. (Andreasson & Koivisto 2013: 69–74.)

Laitteistoturvallisuudella tarkoitetaan toimenpiteitä, joilla pyritään turvaamaan laitteiston käytettävyys, toiminta ja ylläpito. Tämän saavuttamiseksi turvataan laitteiston elinkaarta takuun lisäksi erilaisilla tukipalveluilla. (Valtiovarainministeriö 2008b: 57.) Organisaatioille tämä on pyritty tekemään helpoksi erilaisten palvelusopimusten kautta, mutta tärkeiden laitteiden osalta täytyy miettiä tarkoin, onko oma välivarasto tarpeellinen. Ylläpidon tulee huolehtia järjestelmästä siten, että se pystytään tarvittavassa laajuudessa palauttamaan virhetilasta toipumisen jälkeen. Erilaiset laitekohtaiset tietoturvaominaisuudetkin on hyvä hyödyntää siinä määrin, missä ne lisäävät tietoturvallisuutta

ja estävät tietojen joutumisen vääriin käsiin. Yrityksissä 2011 jälkeen yleistynyt BYOD-käytäntö (bring your own device) aiheuttaa monia ongelmia organisaation tietohallinnolle, koska väärin asetellut tai puutteellisilla suojausohjelmilla varustetut omat laitteet tuottavat tietoturvariskin yrityksille. (Andreasson & Koivisto 2013: 65–66.)

Ohjelmistoturvallisuus pureutuu ohjelmistojen tietoturvatoimiin, kohteena ovat käyttöjärjestelmät, varus- ja työkaluohjelmistot (Valtiovarainministeriö 2008b, 68). Toteutuksena ohjelmistoturvallisuus tarkoittaa testattuja, huolellisesti valittuja ja helposti hallittavia käyttöjärjestelmiä sekä tietoliikenne- ja tietoturvaohjelmistoja. Tämän lisäksi eritavoin toteutettujen työkalu- ja varusohjelmistojen tulee olla yhteensopivia ja tietoturvallisia. Ohjelmistojen tietoturvataso määräytyy käsiteltävän tiedon turvaluokituksen mukaisesti, mikä tulee ottaa huomioon määriteltäessä tietoturvamenetelmiä, kuten käyttäjätodennusta, -tietojen hallintaa, käyttöoikeuksia, salausta, virhetilanteiden hallintaa ja auditointia. Ohjelmistoissa tulee lisäksi olla kattavat toiminnot käytönvalvontaan ja tarkkailuun, jotta mahdolliset väärinkäytökset havaitaan. (Valtiovarainministeriö 2004: 67–78.)

Tietoaineistoturvallisuus on perinteisemmin tunnettu turvallisuuden osa-alue. Osa-alue koostuu asiakirjojen, tiedostojen ja tietoaineistojen luokittelusta ja asianmukaisesta hallinnasta tiedon eheyden, käytettävyyden ja luottamuksellisuuden ylläpitämiseksi (Valtiovarainministeriö 2008b: 101). Tietojen luokitus tapahtuu omistajan toimesta, joka määrää tiedon käytöstä ja jakelusta. Mikäli aineistossa on sekä salassa pidettävää että julkista tietoa, tulee salassa pidettävyys ilmetä selvästi materiaalista. Salassapitosopimuksilla täydennetään laissa määrättyä salassapitovelvollisuutta ja sopimusrikkeestä joutuu yleensä maksamaan korvaukset. Tietoaineiston käsittelyssä, säilytyksessä ja arkistoinnissa tulee mediasta riippumatta toteuttaa vaadittu suojaus ja salaus turvaluokan mukaisesti. Yksityisyydensuojan vuoksi henkilötietojen ja -rekisterien käsittelyssä tulee olla tarkkana ja vain välttämättömät tiedot tulee tarvittaessa siirtää. (Valtiovarainministeriö 2004: 79–84.)

Käyttöturvallisuus sisältää tuki-, ylläpito-, kehittämis- ja huoltotoimenpiteet käyttöympäristöön ja laitteisiin. Se pitää sisällään ulkoistettujen toimintojen riskianalyysin ja pal-

velusopimuksien laatimisen. Osa-alueeseen kuuluvat myös käyttöympäristön laajennukseen liittyvät etäkäyttö, -työ ja -hallinta sekä niiden suunnittelu. Käyttöturvallisuuteen kuuluu myös prosessienhallinta, jolla tarkoitetaan tietojärjestelmien normaalia operointi- ja hallintatoimia sekä muutostenhallintaa, johon puolestaan kuuluvat korjauspäivitykset, tietoturvakorjaukset, järjestelmäintegroinnit ja toimittajavaihdokset. (Valtiovarainministeriö 2004: 86–93.) Käyttöturvallisuus tukee ohjelmisto-, laitteisto- ja tietoliikenneturvallisuutta.

3.2 Tietoturvavaatimukset

Tietoturvan vaatimustasot vaihtelevat sovellettavan kohteen ja alan mukaisesti. Suomessa tietoturvallisuuteen liittyy paljon sovellettavaa ja suoranaista lainsäädäntöä: mm. perustuslain perusoikeusäännökset, henkilötietolaki, laki viranomaistoiminnan julkisuudesta, rikoslaki ja laki rikoslain muuttamisesta, pakkokeinolaki ja laki huoltovarmuuden turvaamisesta (Karvi 2010: 8–9). Edeltävien lisäksi tuore 2015 voimaan tullut laki julkisen hallinnon turvallisuusverkkotoiminnasta, pyrkii varmistamaan normaali-, häiriö- ja poikkeustilanteissa valtion sekä yhteiskunnan kannalta tärkeän viestinnän häiriöttömyyden ja eheyden. (Laki julkisen hallinnon turvallisuusverkkotoiminnasta 10/2015).

Valtionvarainministeriön Vahti 2/2010-asiakirjassa esitetään yleisiä vaatimuksia viranomaisten tietojenkäsittelylle. Tietoturvallisuutta tulee toteuttaa ja ylläpitää siten, että vähintään perustaso saavutetaan. (Valtionvarainministeriö 2010: 35–36.) Perustason toteuttamisesta on määrätty 681/2010 laissa siten, että tietoturvariskit tulee huomioida ja viranomaistoimijoilla tulee olla riittävä tietoturva-asiantuntemus käytettävissä. Tietojen ja asiakirjojen osalta käsittely ja säilytys tulee toteuttaa siten, että vastuut ja tehtävät ovat tiedossa ja tarvittavat estot toteutettu asiattoman toiminnan estämiseksi. Henkilöstöä tulee ohjeistaa ja kouluttaa tietojen käsittelyyn sekä lisäksi valvoa, että ohjeita noudatetaan. Arkaluonteisia tietoja käsittelevien luotettavuus voidaan varmistaa turvallisuusselvitysmenettelyllä. (Valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa 681/2010.)

Euroopan komissio on puolestaan laittanut vuonna 2013 alulle koko EU:n aluetta koskettavan verkko- ja tietoturvadirektiivin. Direktiivi hyväksyttiin Euroopan parlamentissa 6. heinäkuuta 2016 ja se tuli voimaan elokuussa 2016. Direktiivin tarkoituksena on varmistaa yhteinen korkea tietoturvataso läpi unionin sekä parantaa jäsenmaiden kyberturvallisuuskykyä ja yhteistyötä. (European Commission 2016.) Direktiivi tulee koskemaan keskeisten palvelujen tarjoajia, jotka jäsenvaltioiden on määritettävä viimeistään 9. marraskuuta 2018. Toimialoista direktiivi sisältää energian, liikenteen, pankkialan, finanssimarkkinoiden infrastruktuurin, terveydenhuoltoalan, vedenjakelun ja digitaalisen infrastruktuurin. Energia-alaan sisältyvät sähkö, öljy ja kaasu. Verkko- ja tietoturvadirektiivi ei rajoita EU direktiivin 2008/114/EY vaatimuksia elintärkeää infrastruktuuria koskien. (Directive (EU) 2016/1148: 12, 14, 27–29.)

Keskeisten toimijoiden turvallisuusvaatimukset esitellään direktiivin artiklassa 14:

> Jäsenvaltioiden on varmistettava, että keskeisten palvelujen tarjoajat toteuttavat asianmukaiset ja oikeasuhteiset tekniset ja organisatoriset toimenpiteet hallitakseen riskejä, joita kohdistuu niiden verkko- ja tietojärjestelmien turvallisuuteen, joita nämä keskeisten palvelujen tarjoajat käyttävät toiminnoissaan. Näillä toimenpiteillä on varmistettava riskiin suhteutettu verkko- ja tietojärjestelmien turvallisuuden taso uusin tekniikka huomioon ottaen. (Directive (EU) 2016/1148: 20.)

Tämän lisäksi jäsenvaltioiden vastuulla on varmistaa, että keskeisten palvelujen tarjoajat toteuttavat ehkäisevät toimenpiteet siten, että mahdolliset poikkeamat eivät vaikuta palvelun jatkuvuuteen. Keskeisiä toimijoita sitoo myös ilmoittaminen palvelun jatkuvuutta uhkaavista poikkeuksista. Ilmoitus tulee tehdä toimivaltaiselle viranomaiselle tai CSIRT-toimijalle. Asetettuihin turvallisuusvaatimuksiin pääsemiseksi artiklassa 19 kannustetaan käyttämään merkityksellisiä eurooppalaisia tai kansainvälisesti hyväksyttyjä standardeja ja ohjeistuksia. Jäsenvaltioiden kanssa yhteistyössä toimii ENISA, joka jakaa neuvoja sekä suuntaviivoja teknisistä aloista, jotta riittävä tietoturvan taso toteutuisi. (Directive (EU) 2016/1148: 20, 23.)

EU-maista Saksa on ottanut varaslähdön verkko- ja tietoturvadirektiivin noudattamiseen ja on luonut direktiivin mukaisen lain omaan kansalliseen lainsäädäntöönsä. Saksan laki

on nimeltään kyberturvallisuuslaki ja se otettiin käyttöön syksyllä 2015. Saksassa rikkomuksista on määrätty korvaus 100 000 euroon saakka. Lakia tarkastellaan uudelleen neljän vuoden jälkeen lain voimaan astumisesta, jolloin määrittyy tarkemmin lain sovelluskohde. Ensimmäisten joukossa lainpiirin asetettiin mm. energiasektori keväällä 2016. Saksan hallituksen mukaan kriittisen infrastruktuurin sektori rajoittuu 2 000 toimijaan. Tietoturvan vähimmäisvaatimukset määrittää Saksan liittovaltion tietoturvavirasto. Toimijat ovat velvoitettuja säännöllisesti osoittamaan, että täyttävät turvallisuusvaatimukset ja sen tulee tapahtua vähintään joka toinen vuosi. Toimijalla tulee olla yhteyshenkilö tietoturvavirastoa varten ja toimija on velvollinen ilmoittamaan merkittävistä saatavuuden, eheyden, aitouden tai luottamuksellisuuden häiriöistä tietojärjestelmissään. Tietoturvaviraston tehtävä on lain perusteella toimia yhteyspisteenä ja analysoida kaikkea relevanttia tietoa. Lisäksi viraston tulee ohjeistaa, neuvoa ja varoittaa toimijoita. (Kuschewsky 2015.)

EU:n tasolla energia-ala määritellään EU direktiivin 2008/114/EY mukaan Euroopan elintärkeää infrastruktuuria käsittäväksi toimialaksi. Elintärkeällä infrastruktuurilla tarkoitetaan järjestelmiä, jotka ovat keskeisiä yhteiskunnan välttämättömien toimintojen kannalta ja joiden tuhoutuminen tai vahingoittuminen vaikuttaisi merkittävästi jäsenvaltioon. Euroopan elintärkeän infrastruktuurin tuhoutuminen tai vahingoittuminen puolestaan vaikuttaisi merkittävästi vähintään kahteen jäsenvaltioon. Muita vastaavia toimialoja, joissa käytetään kaukokäyttöjärjestelmiä, on nimetty liikenteen puolelta mm. rautatieliikenne. Euroopan elintärkeät infrastruktuurit vaativat turvallisuussuunnitelman, johon kuuluvat hyödykkeiden määrittely, riskianalyysit, vastatoimenpiteet ja pysyvät turvatoimenpiteet, kuten tietoturvan kokonaisvaltainen toteuttaminen. (Council Directive 2008/114/EC: 2-3, 6–7; ENISA 2011b: 5.) Suomi on osana pohjoismaista voimajärjestelmää yhdessä Ruotsin, Norjan ja Itä-Tanskan kanssa. Tämän lisäksi Suomesta on yhteyksiä Viroon ja Venäjälle (FINGRID 2016). Runkoverkon siirtoyhteyksien puolesta oletetaan, että Suomen sähköjärjestelmän horjuminen voisi heijastua myös naapurimaihin, mikäli energian tarve on koko Skandinavian alueella suurta.

Suomessa sähköverkkoyhtiöiden varautumissuunnitelmia sähkömarkkinalain puitteissa valvoo Huoltovarmuuskeskus (Sähkömarkkinalaki: 588/2013). Huoltovarmuuskeskus on myös jo usean vuoden ajan jakanut ohjeistusmateriaalia automaatiojärjestelmien tietoturvan toteutukseen, ylläpitämiseen sekä kehittämiseen (Huoltovarmuuskeskus 2015: 12). Ohjeistuksien käyttöönottoa ja toteutumista Huoltovarmuuskeskus seuraa mm. tilannekartoituksilla, joista viimeisimmän teki XCure Solutions Oy 2015 syksyllä. Kyberturvallisuuden tilannekuvan arvioinnissa käytettiin ISO/IEC 27001 ja 27002 -standardeja, kansallista Katakri III -turvallisuusauditointikriteeristöä ja valtionhallinnon julkaisemaa VAHTI-dokumenttisarjaa. (Immonen 2015: 1–2.) Näin ollen ISO/IEC 27001 ja 27002 -standardeja, Katakri -kriteeristöä sekä Vahti-ohjeistoja voidaan osin pitää kansallisen tason vaatimuksena tietoturvallisen automaatiojärjestelmän toteuttamiselle.

Yhdysvalloissa puolestaan on vuodesta 1968 lähtien toiminut NERC (North American Electric Reliability Corporation), jonka tehtävänä on ollut sähkönsiirtojärjestelmien luotettavuuden ja käyttövarmuuden varmistaminen. NERC ei kuulu Yhdysvaltain hallitukseen, mutta sillä on lakisääteisesti vastuu säännellä järjestelmien käyttö- ja ylläpitotoimia. Tämä toteutuu standardien määrittelyn ja valvonnan kautta, joka käytännössä tarkoittaa, että NERC antaa suunnittelusääntöjä ja toimintaohjeita, joita tulee noudattaa. (Ahonen 2010: 48.) Koska Euroopan alueella ei ole ollut yhtenäisiä vaatimuksia koskien teollisuusautomaatiojärjestelmiä, vaan lähinnä vain ”hyviä käytänteitä” (good practices), jotkut sektorit ovat alkaneet toteuttaa tietoturvaa USA:n vaatimusten NERC CIP (Critical Infrastructure Protection) -standardin pohjalta (ENISA 2011a: 18).

NERC CIP -standardit ovat kehittyneet teollisuuslähtöisesti ja ne toteutetaan ANSI-akkreditoidulla prosessilla. Kehitysprosessi on kaikille alantoimijoille avoin ja lopputuloksena luodut ja hyväksytyt standardit ovat julkisesti jaossa internetissä. (Ahonen 2010: 49.) Standardit tarjoavat kyberturvallisuuskehyksen, jonka avulla tunnistetaan ja suojataan kriittiset toiminnot sähköjärjestelmissä (ENISA 2011c: 62). Standardit määrittelevät myös erilaisia rooleja sähköjärjestelmän kokonaisuuksista, joita tulee hallita niiden kriittisyyden ja haavoittuvuuden vuoksi. Tämän lisäksi standardit kattavat kaupalliset ja operatiiviset vaatimukset ylläpitoon, hallintaan ja viestimiseen toimintojen ja or-

ganisaatioiden välillä. (ENISA 2011c: 62.) Ensimmäiset käyttövarmuusstandardit julkaistiin käyttöön 2007 ja vuodesta 2013 lähtien työn alla on ollut standardin viides versio (Ahonen 2010: 49; NERC 2016).

NERC CIP -standardit ja niiden käyttötarkoitus (Ahonen 2010: 49):

- CIP-001: sabotaasien raportointi (tätä ei normaalisti sisällytetä automaatiostandardeihin)
- CIP-002: kriittisen tietopääoman tunnistaminen
- CIP-003: turvallisuuden hallinnan kontrollit (minimikontrollit kriittisten tietopääomien suojaamiseksi)
- CIP-004: henkilöstö ja tietoturvakoulutus (henkilöstön koulutus, tietoturvatietoisuus ja mm. henkilöiden taustan tarkistaminen)
- CIP-005: suojattavien kohteiden vyöhykkeen (electronic perimeter) tunnistaminen ja suojaus (sis. liityntäpisteet)
- CIP-006: kriittisen tietopääoman fyysinen turvallisuus
- CIP-007: järjestelmien turvallisuuden hallinta (metodit, prosessit ja proseduurit järjestelmien kriittisten tietopääomien suojaamiseksi)
- CIP-008: tietoturvaloukkausten ja -tapahtumien raportointi ja reagointisuunnitelmat (sis. tapahtumien tunnistamisen ja luokittelun)
- CIP-009: toipumissuunnittelu (kriittisten tietopääomien palautussuunnitelmat, ottaen huomioon liiketoiminnan jatkuvuuden ja onnettomuuksista toipumisen tekniikat ja -käytännöt)

3.3 Tietoturvaohjeistukset ja -standardit

Tietoturvaohjeistuksia ja -standardeja on viime vuosina alettu hyödyntämään yhä enemmän. Ikävät mediahuomiota keränneet tapahtumat, kuten Stuxnet, ovat edesauttaneet ohjeistuksen määrän kasvua. Suomessa Huoltovarmuuskeskus on ollut jo useamman vuoden automaatiojärjestelmien suojaamiseen suuntaavan ohjeistuksen jakelijana ja tutkimuksen toimeksiantajana. Alun perin Tekesin ja VTT:n TITAN-projektista 2008–2010 lähtenyt ohjeiston kehittämisen ketju on jatkunut vuoteen 2016, jolloin viimeisin projekti tietoturvan jalkauttamisesta teollisuusautomaatioon saatettiin päätökseen. Ohjeistuksen kehittämisestä ja työstöstä on vastannut VTT, mutta mukana ohjeistusta kehittämässä on ollut myös valtaisa joukko suomalaisia alan yrityksiä ja osaajia. (Huoltovarmuuskeskus 2015: 12.)

VTT:n TITAN-projektin tuotoksena syntyi vuonna 2010 TITAN-käsikirja, jonka tarkoituksena on esitellä tietoturvaan liittyviä standardeja, vaatimuksia, tulevaisuuden suuntauksia. Tämän lisäksi kirjan tuli toimia ohjeistuksena suomalaiselle automaatioteollisuudelle, koska Suomessa ei ollut esitetty mitään lakiin perustuvia tietoturvavaatimuksia alalle. TITAN-käsikirjaan listattujen standardien lähtökohtana oli, että standardit sisältävät ominaisuuksia, jotka tukevat automaatioteollisuutta tai standardit ovat vakiintuneita määräyksiä ja käytäntöjä, joita vaaditaan toiminnassa. (Ahonen 2010: 3, 29.)

EU:n tasolla tietoturvaohjeistusta kriittiselle infrastruktuurille ja sen automaatiojärjestelmille on jaettu ENISA:n toimesta hieman TITAN-käsikirjan julkaisun jälkeen. ”Protecting Industrial Control Systems” -suositukset kattavine liitteineen vuonna 2011 on ENISA:n julkaisu ja sen tarkoituksena on toimia kansainvälisenä ohjeistuksena Euroopan jäsenvaltioille. Dokumentti sisältää seitsemän suositusta julkisen ja yksityisen sektorin automaatiojärjestelmän hallitsijalle. Suositukset sisältävät hyödyllisiä käytännön ohjeita, jotka parantavat nykyisiä lähtökohtia, yhteistyötä, kehitystoimenpiteitä ja käytäntöjä. Suosituksia pidetään tehokkaina, saavutettavina ja kiireisinä, koska suurin osa kohdejärjestelmistä ja toimijoista kuuluu Euroopan elintärkeän infrastruktuurin piiriin. (ENISA 2011a: 1–4.)

ENISA:n tarjoamasta ohjeistuksesta huolimatta monella EU-maalla on myös omat kansalliset ”best practices” -ohjeistuksensa, jotka ovat olleet käytössä jo ennen yhteisiä EU-tason ohjeistuksia. Iso-Britannialla on mm. “Good practice guide - Process Control and SCADA Security” -ohjeistus ja “Firewall deployment for SCADA and process control networks. A good practice guide” -ohje. Ranskalaiset luottavat puolestaan “Managing Information Security in an Electric Utility” -raporttiin. Ruotsalaisilla on ”Guide to Increased Security in Industrial Control Systems” -ohjeistus. (ENISA 2011c: 29–52.)

TITAN-käsikirjan tekijät ovat valikoineet standardeista ja käytännöistä mukaan automaatiojärjestelmän tietoturvan kannalta olennaisia, yleiskäyttöisiä ja alakohtaisia standardeja. Yleiskäyttöisesti soveltuvia standardeja ovat ISO/IEC 15408, CSSP, ISA99, NIST 800, MSISAC/SANS ja ISO/IEC 27000 -standardiperhe. Suoraan sähköalaan puolestaan liittyviä standardeja ovat NERC CIP -standardit ja IEEE 1686. Öljy- ja kaa-

sualojen standardeista mukaan on otettu AGA Standard 12 ja API Standard 1164, jotka kattavat hyvin kaukokäyttöjärjestelmän. (Ahonen 2010: 30–50.) Lähes samat standardit ja käytännöt löytyvät myös ENISA:n standardiliitteestä, mutta sähköalan standardeihin täytyy lisätä mukaan vielä IEC 62351 -sarja, koska se ottaa kantaa paljon myös kaukokäyttöjärjestelmissä käytössä olevien protokollien IEC 60870-5-101, -104 ja IEC 61850 tietoturvaan (ENISA 2011c: 2).

"ISO/IEC 15408 Common Criteria –Evaluation criteria for IT security" on laajalti käytössä oleva standardi. Standardi sisältää mallit ja peruskäsitteiden määrittelyn IT-järjestelmien tietoturvan arviointiin. Standardin ohjeistus on yleiskäytännöllistä ja tietoturvaosa-alueen kattavaa. Testattavat tuotteet voidaan evaluoida riippumattomissa, lisensoiduissa laboratorioissa ennalta teknologialle määriteltyjen kriteerien mukaisesti. Teollisuusautomaatioon kohdennettuja määrittelyjä tai ohjeistuksia ei standardi suoraan sisällä, mutta standardi tukee silti hyvin myös teollisuusautomaation tietoturvaa. (Ahonen 2010: 30–32.)

IEC 15408 -standardi koostuu kolmesta osasta, jotka ovat (Ahonen 2010: 31):

- Osa 1: Esittely ja yleinen malli
- Osa 2: Tietoturvan toiminnalliset vaatimukset
- Osa 3: Tietoturvan varmistamisen vaatimukset.

Tietoturvan toiminnalliset vaatimukset jaotellaan toisessa osassa seuraaviin luokkiin (Ahonen 2010: 31):

- FAU: Security audit
- FCO: Communication
- FCS: Cryptographic support
- FDP: User data protection
- FIA: Identification and authentication
- FMT: Security management
- FPR: Privacy
- FPT: Protection of target's security functions
- FRU: Resource utilisation
- FTA: Target of evaluation access
- FTP: Trusted path/channels.

Tietoturvan varmistamisen vaatimukset jaotellaan kolmannessa osassa seuraaviin luokkiin (Ahonen 2010: 31):

- ACM: Configuration management
- ADO: Delivery and operation
- ADV: Development
- AGD: Guidance documents
- ALC: Life cycle support
- APE: Protection profile evaluation
- ASE: Security target evaluation
- ATE: Tests
- AVA: Vulnerability assessment

Kolmas osakokonaisuus sisältää myös EAL (Evaluation Assurance Level) -vaatimustasot yhdestä seitsemään, jotka pyritään määrittämään tarpeen ja kohteen mukaan tasapainoilemalla kustannustehokkuuden ja soveltuvuuden kanssa. Vaatimukset ovat tarkkoja, periaatteellisia ja hyviä, minkä vuoksi tilaajataho voi vaatia tuotteelta EAL-tason arviointia. Standardin heikkoutena on evaluoinnin hitaus ja kustannukset. (Ahonen 2010: 32.)

CSSP (Control System Security Program) on Yhdysvaltain Home Security -hallinnon tukema “hyvä käytäntö tyyppinen” -ohjelma. CSSP-ohjelman tarkoituksena on koordinoida tietoturvariskejä ja haavoittuvuuksia vähentäviä toimenpiteitä. Ohjelman kohteena ovat kaikki Yhdysvaltojen ohjausjärjestelmät ja sen toimintaan osallistuvat useat eri tasojen toimijat. Vaikka ohjelma keskittyy Yhdysvaltojen järjestelmiin, on informaatio yleiskäyttöistä ja sitä voidaan hyödyntää myös Euroopassa. Teollisuusautomaatio on lisäksi otettu erityisesti huomioon käytäntöjen laadinnassa ja osa käytännöistä saattaa olla sidottu myös NERC-vaatimuksiin. Käytännöt lähtevät uhkien ymmärtämisestä ja ohjausjärjestelmien haavoittuvuuksien ja hyökkäystapojen kuvaamisesta, johtaen käytännön torjunta toimenpiteisiin. (Ahonen 2010: 33–34.)

Käytännöt kuvaavat seuraavia alueita, jotka löytyvät ICS-CERT (Industrial Control Systems Cyber Emergency Response Team) toimijan sivustolta (ICS-CERT 2016):

- defense-in-depth-strategiat
- tulevaisuuden ennustaminen ja suunnittelu
- automaatiojärjestelmän suunnitelman kehittäminen poikkeustilanteiden varalle
- palomuurien käyttöönotto SCADA- ja prosessiohjausverkoissa
- korjausten hallinta ohjausjärjestelmässä
- OPC-asemien kovennus ja verkkojen haavoittuvuuksien eliminointi
- ohjelmistokorjausten hallinnan käytännöt
- modeemien turvaaminen
- teollisuuden ohjausjärjestelmien etähallinta
- yleiset ohjausjärjestelmän haavoittuvuudet
- ICS turvallisuuden parantaminen (epäsuorat hyökkäykset kriittistä infrastruktuuria vastaan)
- ICS turvallisuuden parantaminen (takaovet ja aukot verkkoalueissa)

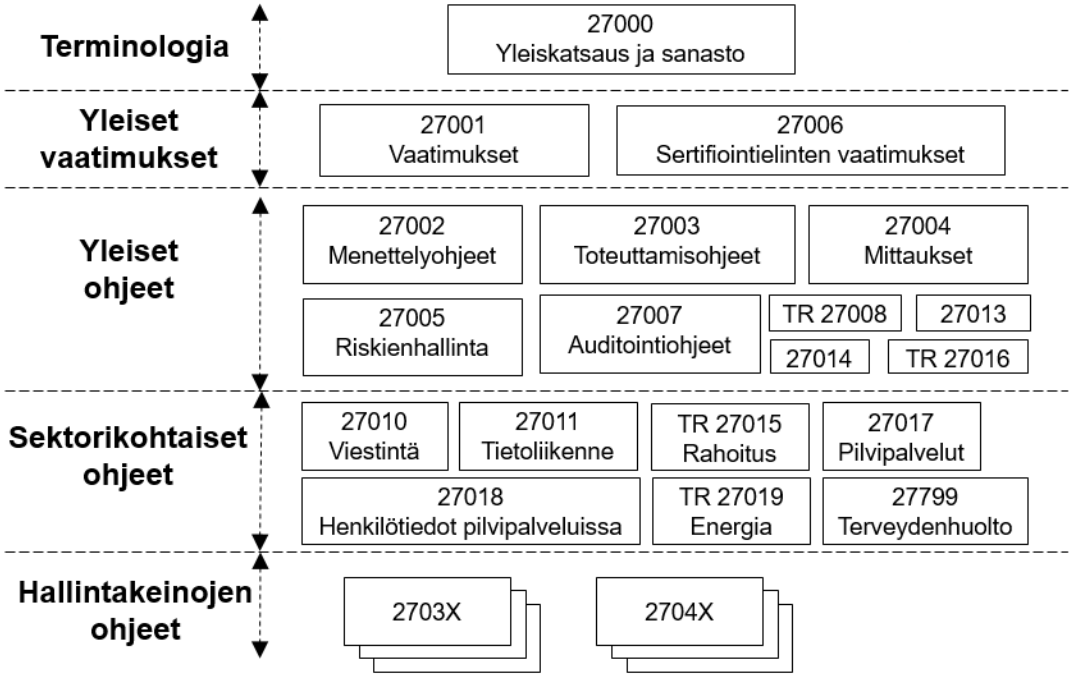
ICS-CERT toimijan tarjoamat ohjeistukset ja käytännöt ovat täsmällisesti kohdennettu ja ne käsittävät myös laajalti kaukokäyttöympäristöä teollisuusautomaation lisäksi. Erityisesti kaukokäyttöjärjestelmän näkökulmasta kriittiset ohjeet ovat palomuuriohjeistus SCADA-verkossa sekä ohjausjärjestelmän etäyhteydet, mutta myös korjauspakettien hallinta on nousemassa tärkeään rooliin järjestelmien tietoturvan kehittymisen kannalta.

“ISA99 Industrial Automation and Control Systems Security Standards” on ISA (Instrumentation, Systems and Automation Society) -asiantuntijaorganisaation standardikokoelma. ISA kehittää standardeja, kouluttaa ja julkaisee materiaalia teollisuusautomaation ympäristöä silmällä pitäen. ISA:n standardit ovat maksullisia ja ne ovat suunnattu ”järjestelmien suunnittelijoille, toteuttajille, hallinnoijille, käyttäjille, integraattoreille sekä laitevalmistajille”. Ohjeistus on käytännönläheistä, mutta jättää osin tietoturvatoteutuksen epäselväksi. Standardi sopii hyvin taustamateriaalina asioihin perehtymiseksi. (Ahonen 2010: 35–36.)

ISA:n standardit keskittyvät perustavanlaatuisiin asioihin, mutta osa standardeista on vielä keskeneräisiä (Ahonen 2010: 35; ENISA 2011c: 22–23):

- ISA 99.01.01 Konseptit, mallit ja terminologia (v. 2007 standardi)
- ISA 99.02.01 Tietoturvaohjelman alkuun saaminen organisaatiossa
- ISA 99.02.02 Tietoturvaohjelman operointi organisaatiossa (kesken)
- ISA 99.03.xx Tietoturvavaatimusten asettaminen järjestelmille (kesken)

ISO/IEC 27000 -standardiperhe tunnetaan myös ISO:n (International Organization for Standardization) ISMS (Information Security Management System) -standardeina. ISO/IEC 27000 -standardiperhe on hyvin yleiskäyttöinen, mutta kuitenkin riittävän yksityiskohtainen. Vaikka standardiperhettä ei käytetä sääntelyyn, se mahdollistaa sertifioinnin ja ISMS-standardien pohjalta voidaan asettaa vaatimuksia järjestelmille. ISO/IEC 27000 -standardiperhe suosittelee organisaatiota tunnistamaan suojausta vaativan tietosisällön ja sen mahdolliset uhat. Tietosisällön mukaisesti standardista löytyy ohjeita ja ehdotuksia tietoturvan hallintajärjestelmän rakentamiseen sekä sen kehittämiseen PDCA (Plan-Do-Check-Act) -mallilla. (Ahonen 2010: 36–38.) PDCA-malli on hyvä ja selkeä, mutta se on jätetty pois 2013 vuoden standardiversiosta (Suomen Standardisoimisliitto SFS ry 2015: 31). ISMS-standardit esitetään luokittain kuvassa 5.

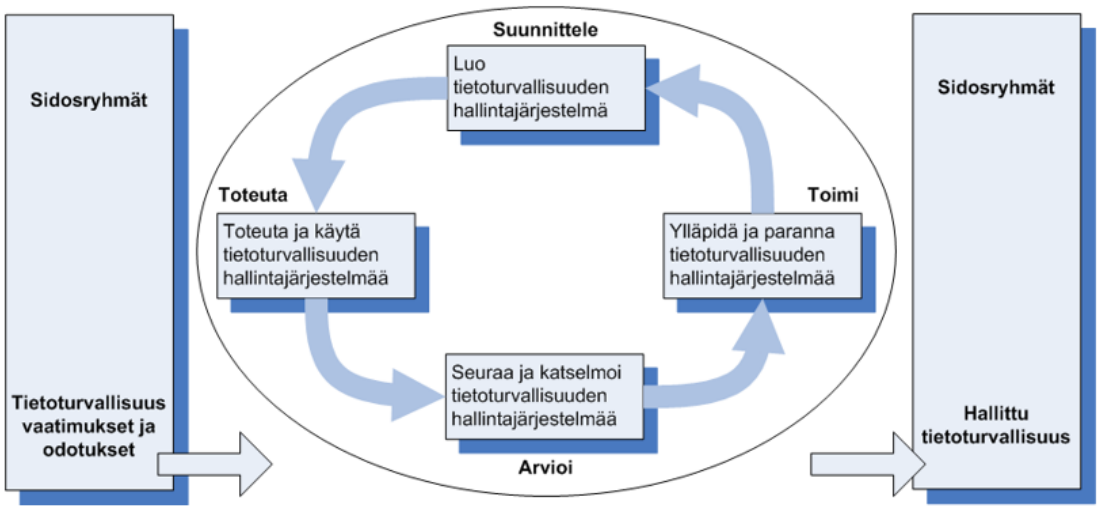


Kuva 5. ISO/IEC 27000 -standardiperheen luokittelu (Suomen Standardisoimisliitto SFS ry 2015: 21).

Ohjaus spesifiset standardit 2703x ovat (Ahonen 2010: 38):

- ISO/IEC 27031 – Guideline for ICT readiness for business continuity
- ISO/IEC 27032 – Guideline for cybersecurity
- ISO/IEC 27033 – IT network security
- ISO/IEC 27034 – Guideline for application security
- ISO/IEC 27035 – Security incident management
- ISO/IEC 27036 – Guidelines for security of outsourcing
- ISO/IEC 27037 – Guidelines for identification, collection and/or acquisition and preservation of digital evidence

ISO/IEC 27001 -standardi toimii hyvänä referenssinä tietoturvallisen järjestelmän rakentamisessa, koska se määrittelee vaatimukset tietoturvan implementointiin, operointiin, valvontaan, tarkistamiseen ja ylläpitoon. Standardia voidaan myös käyttää auditoinnissa ja sertifioinneissa. Standardi soveltuu useille eri organisaatioille, mutta erityisesti huoltovarmuuskriittistä tietoa luoville ja käyttäville toimijoille. (Ahonen 2010: 39; ENISA 2011c: 9.)



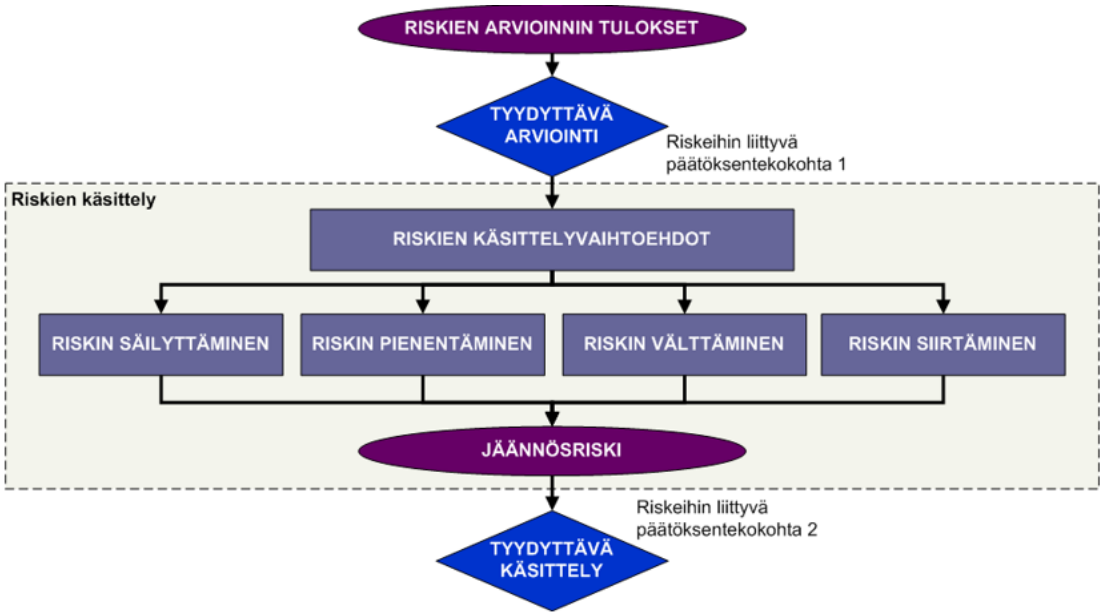
Kuva 6. PDCA-malli (Plan-Do-Check-Act) (Suomen Standardisoimisliitto SFS ry 2015: 31).

ISO/IEC 27002 -standardi määrittää tietoturvan hallitsemisen kannalta tarpeelliset ohjeet ja suositukset. Käsiteltävät asiat nähdään käytäntöinä ja hyvinä toimintatapoina.

Standardissa käsitellään seuraavat asiat (Ahonen 2010: 39–40):

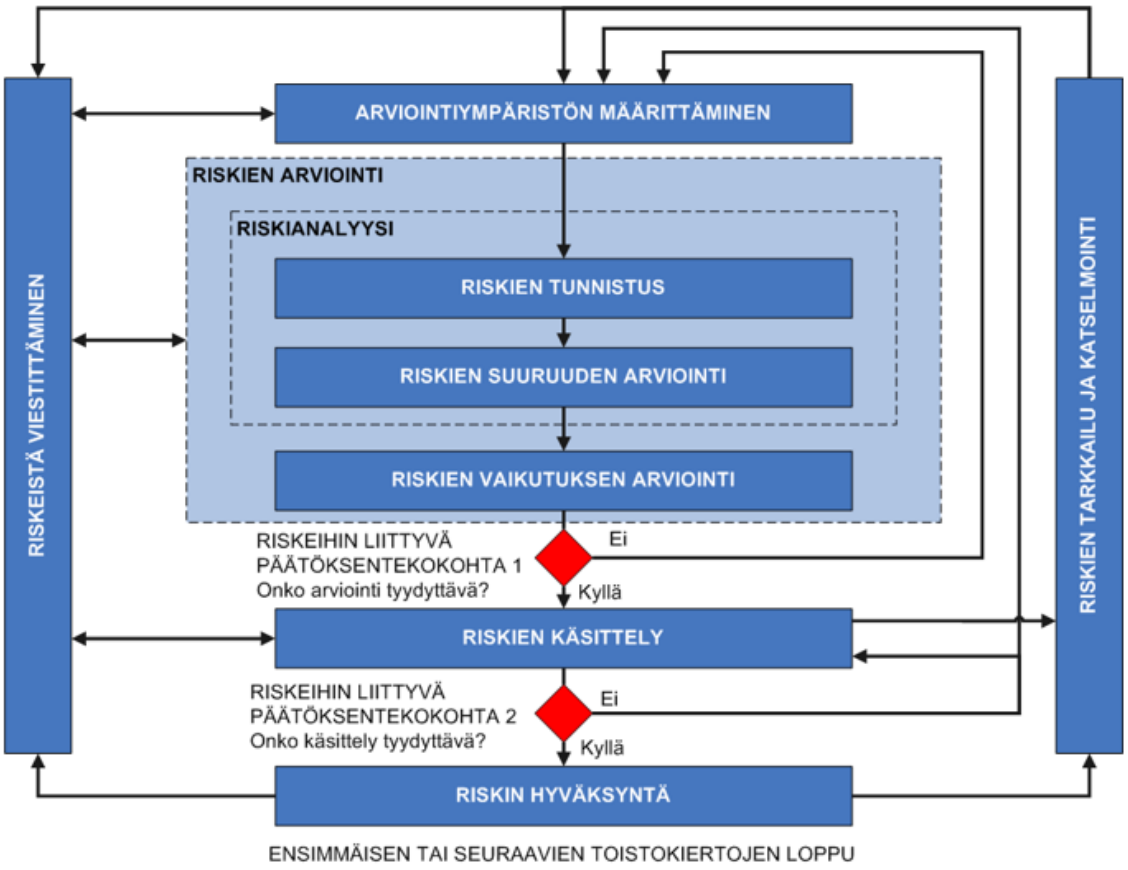
- riskien arviointi (kukin organisaatio tekee ensin arvion, johon sitten muut valinnat pohjautuvat)
- organisaation tietoturvapolitiikka
- organisaation tietoturvainfrastruktuuri
- suojattavien omaisuuksien luokittelu ja hallinta
- henkilöstöturvallisuus
- fyysinen turvallisuus ja ympäristön turvallisuus
- kommunikaation ja toimintojen hallinta
- pääsynvalvonta
- järjestelmien hankinta, kehittäminen ja ylläpito
- tietoturvatapahtumien hallinta
- liiketoiminnan jatkuvuuden hallinta
- tietoturvavaatimusten toteutuminen.

ISO/IEC 27005 -standardi määrittelee tietoturvariskien hallinnan. Standardi mukailee ISO/IEC 27001 -standardin tietoturvallisuuden hallintajärjestelmän vaatimuksia, mutta lähtee liikkeelle riskienhallinnan näkökulmasta. ISO/IEC 27005 soveltuu kaikenlaisille organisaatioille, mutta standardin viitteiksi vaaditaan ISO/IEC 27001 ja 27002 -standardit. (ENISA 2011c: 11–12; Suomen Standardisoimisliitto SFS ry 2015: 46.) ISO/IEC 27005 -standardissa kuvataan riskien käsittelyä kuvassa 7 ja riskienhallintaa kuvassa 8.



Kuva 7. Kaavio toiminnasta riskienkäsittelyssä (Suomen Standardisoimisliitto SFS ry 2015: 50).

Muita automaatiojärjestelmille hyödyllisiä ISO/IEC 27000 -standardiperheen standardeja ovat mm. ”ISO/IEC 27019 Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry”, “ISO/IEC 27032 Guidelines for cybersecurity”, “ISO/IEC 27033 Network security ja ISO/IEC 27035 Information security incident management” (Suomen Standardisoimisliitto SFS ry 2015: 15–18). ISO/IEC 27000 -standardiperhe on todella kattava ja sarjasta löytyy ohjeistusta aina fyysisestä tietoturvasta verkko- ja sovellustason tietoturvaohjeistuksiin.



Kuva 8. Kaavio tietoturvariskien hallintaan (Suomen Standardisoimisliitto SFS ry 2015: 49).

“NIST 800 Series Security Guidelines” on Yhdysvaltain National Institute of Standards and Technology (NIST) -organisaation standardikokoelma. Organisaatiossa on Computer Security -osasto, joka kehittää standardeja ja ohjeistuksia seuraaviin alueisiin: ”kryptografia, tunnistusmenetelmät, verkkoyhteyksien tietoturva, tietoturvakriteeristö ja

tietoturvan varmistaminen sekä tietoturvan hallinta ja tuki.” Teollisuusautomaatioon liittyen tärkein NIST 800 -standardi on ”SP 800-82 Guide to Industrial Control Systems (ICS) Security”, joka käy läpi “ICS-järjestelmien haavoittuvuudet, tietoturvan hallinnan organisoinnin, verkkoarkkitehtuurin, sekä spesifit tietoturvakontrollit.” (Ahonen 2010: 40.)

NIST 800 -standardit, jotka ovat yhteydessä teollisuusautomaation tietoturvaan (Ahonen 2010: 41):

- NIST SP 800-40 Creating a Patch and Vulnerability Management Program
- NIST SP 800-41 Guidelines on Firewalls and Firewall Policy
- NIST SP 800-42 Guideline on Network Security Testing
- NIST SP 800-48 Wireless Network Security: 802.11, Bluetooth, and Handheld Devices
- NIST SP 800-53 Recommended Security Controls for Federal Information Systems
- NIST SP 800-53A Guide for Assessing the Security Controls in Federal Information Systems
- NIST SP 800-61 Computer Security Incident Handling Guide
- NIST SP 800-63 Electronic Authentication Guideline
- NIST SP 800-64 Security Considerations in the Information System Development Life Cycle
- NIST SP 800-70 Security Configuration Checklists Program for IT Products – Guidance for Checklists Users and Developers
- NIST SP 800-77 Guide to IPSec VPNs
- NIST SP 800-83 Guide to Malware Incident Prevention and Handling
- NIST SP 800-86 Guide to Integrating Forensic Techniques into Incident Response
- NIST SP 800-88 Guidelines for Media Sanitization
- NIST SP 800-92 Guide to Computer Security Log Management
- NIST SP 800-94 Guide to Intrusion Detection and Prevention Systems (IDPS)
- NIST SP 880-97 Guide to IEEE 802.11i: Robust Security Networks.

”MSISAC/SANS: SCADA and Control Systems Procurement Language” on Yhdysvaltain Homeland Security -hallinnon rahoittama projekti, jossa on ollut mukana useita toimijoita. Projektin tuloksena syntynyttä Procurement Language -dokumenttia hyväksi käyttäen ohjausjärjestelmien omistajien on mahdollista määritellä yhtenäisellä tavalla tietoturvavaatimukset ICS-järjestelmän hankintaan liittyen. Dokumenttia soveltamalla toimijat voivat asettaa myös toisilleen vaatimuksia. Dokumentti on kattava ja tarkasti kohdistettu juuri ohjausjärjestelmä sektorille. (Ahonen 2010: 43.)

Dokumentista löytyy vaatimusmäärittelyt seuraaviin kokonaisuuksiin (Ahonen 2010: 43):

- järjestelmän kovennus
- ympäristön (mm. verkkojen) suojaus
- käyttäjätilien hallinta
- koodauskäytännöt
- vikojen käsittely
- haittaohjelmilta suojaaminen
- verkko-osoitteiden ja nimien toiminnallisuus
- päätelaitteet
- etäyhteydet
- fyysinen turvallisuus
- verkon segmentointi

”IEEE1686: Standard for Substation Intelligent Electronic Devices (IEDs) Cyber Security Capabilities” on sähköpuolen standardi, jonka tehtävä on määritellä tietoturvan vähittäisvaatimukset IED-laiteille. Tämä vaatimus tulee NERC CIP -standardista, jossa operaattoreille on asetettu vaatimukset, joiden toteuttaminen vaatii IEEE1686 mukaisen selvityksen tekemistä. Selvityksen ”Table of Compliances” tulee sisältää tarkka kuvaus laitteen käytössä olevista ominaisuuksista. Standardin turvallisuusominaisuudet painottuvat pääsyn valvontaan, lokiin ja reaaliaikaiseen monitorointiin. Standardi yksin ei takaa tietoturvatavoitteiden täyttymistä. (Ahonen 2010: 50–52.)

”IEC 62351: Data and communications security” -standardi luo tietoturvaa sähköjärjestelmän operaatioihin. Standardi koostuu kahdeksasta osasta, joista kaukokäytön kannalta olennaisimmat ovat 62351-5 ja -6 osat. Standardin osista ensimmäinen keskittyy IEC 60870-5-101 ja -104 tietoliikenteen turvallisuuteen ja jälkimmäinen IEC 61850 tietoliikenteen turvallisuuteen. Nämä kaksi standardin osaa määrittelevät operoinnille turvalliset viestit, proseduurit ja algoritmit toteutettaessa tiedonsiirtoa sähköjärjestelmien standardeilla. (IEC/TS 62351-6 2007: 5; IEC/TS 62351-5 2009: 8; ENISA 2011c: 2–3.)

IEC 62351 -standardin osien sisältö (IEC 2016):

- IEC/TS 62351-1: Turvallisuus asioiden esittely
- IEC/TS 62351-2: Termit ja lyhenteet
- IEC/TS 62351-3: Profiilit sisältäen TCP/IP
- IEC/TS 62351-4: Profiilit sisältäen MMS
- IEC/TS 62351-5: IEC 60870-5 ja sen johdannaisten turvallisuus
- IEC/TS 62351-6: IEC 61850 turvallisuus
- IEC/TS 62351-7: Verkkojärjestelmä hallinnan tieto-objekti mallit
- IEC/TS 62351-8: Rooli perusteinen pääsyn valvonta

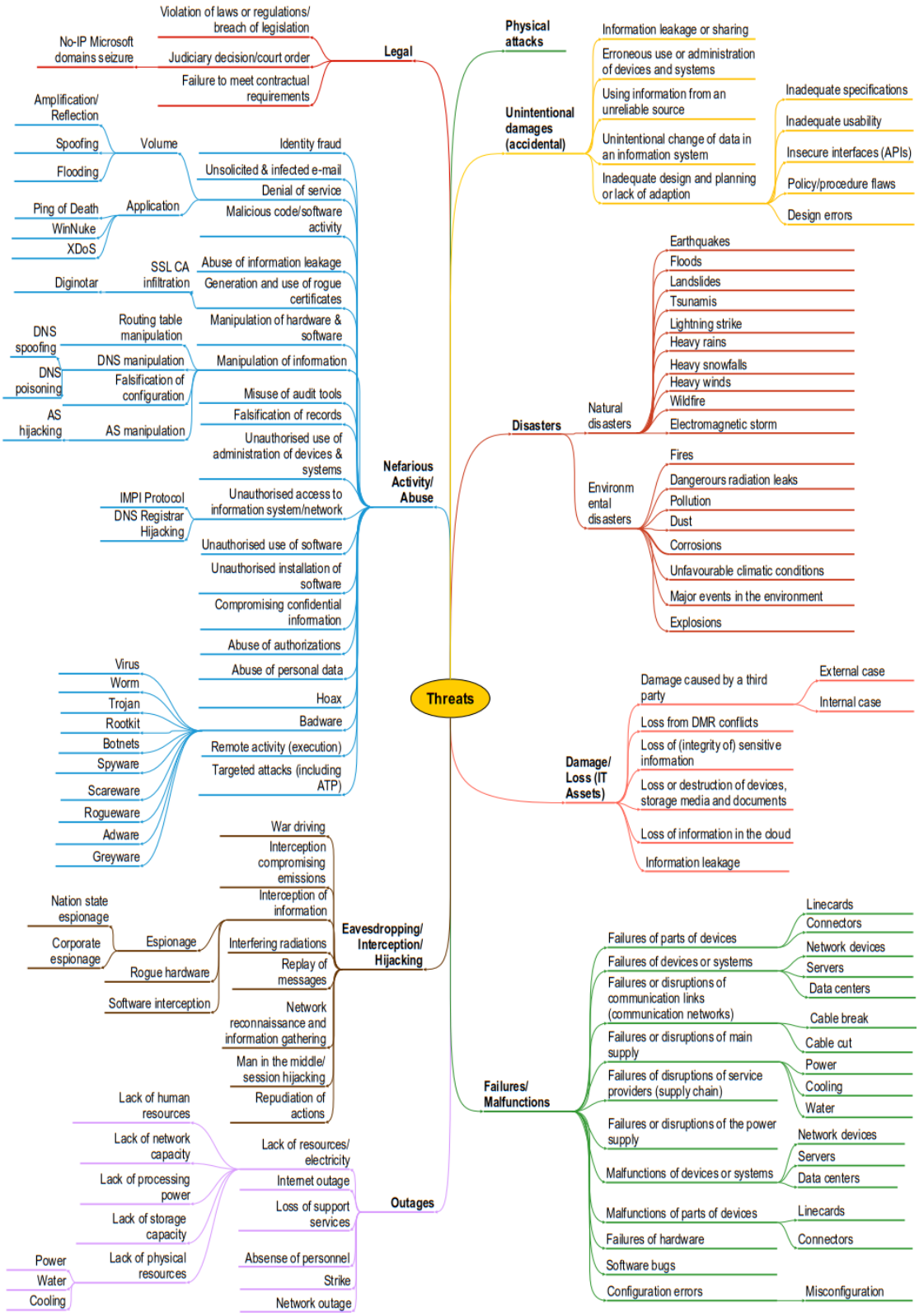
”American Gas Association (AGA) Standard 12, Cryptographic Protection of SCADA Communications” ja “American Petroleum Institute (API) Standard 1164, Pipeline SCADA Security” ovat kaasu- ja öljyalojen sovellettavat ohjeistukset. Kumpaakaan standardia ei voida suoraan soveltaa sähköverkojen kaukokäyttöjärjestelmiin, mutta koska molemmat käyttävät SCADA:a ohjaukseen löytyy myös paljon yhtäläisyyksiä. AGA on pyrkinyt tekemään standardistaan niin kattavan, että sillä säästetään SCADA-operaattorin aikaa ja työtä. API-toimijat puolestaan ovat kehittäneet ohjeistusta alusta lähtien kohdennetusti pienille ja keskisuurille toimijoille. (Ahonen 2010: 44–48.)

Kaukokäyttöön sovellettavissa olevia tietoturvastandardeja on useita. Tämän lisäksi maailmalta löytyy myös omat maa-, manner- ja liittoumakohtaiset ”best practices” -käytännöt. Tällaisessa käytäntöjen ja standardien maailmassa voi olla hankala löytää täydellisesti tarpeeseen sopivaa standardia, mutta usein paras tietoturva kaukokäyttöjärjestelmien operoinnissa ja ylläpidossa saavutetaan yhdistelemällä standardeja ja ohjeistuksia. Tietoturvan perustasoon pyrkivät lait ja direktiivit puolestaan helpottavat standardien ja ohjeistuksen valintaa. Suomessa energia-alalla kannattaisi pyrkiä toteuttamaan ISO/IEC 27000 -standardiperheen standardeja, Katakri-kriteeristöä ja myös osittain Valtionvarainministeriön Vahti-ohjeisto vaatimuksia.

3.4 Tiedostetut tietoturvauhat

Tietoturvan moninaisuudesta johtuen sillä on useita hyökkäykselle alttiita alueita. Vuonna 2015 Viestintäviraston mukaan organisaatioiden viisi yleisintä tietoturvauhkaa olivat ”päivittämättömät ohjelmistot, henkilöstön osaamattomuus, palvelunestohyökkäykset, huijausviestit ja tietojenkalastelu sekä hallitsemattomat yhteydet sisäverkkoon” (Viestintävirasto 2016b: 4). ENISA puolestaan listasi vuoden 2015 merkittävimpien uhkien listaan myös haittaohjelmat, web-pohjaiset hyökkäykset, web-ohjelmahyökkäykset, bottiverkot, fyysiset vahingot/varkaudet/katoamiset, roskapostituksen, tietomurrot, identiteetti varkaudet, tietovuodot, kiristysohjelmat ja kybervakoilun (ENISA 2016b: 7). Kuvassa 9 on ENISA:n tekemä kattava luokittelu tietoturvauhista eri alueilla. Viestintävirasto ennustaa, että vuonna 2016 henkilöstön osaamattomuutta, palvelunestohyökkäyksiä ja huijausviestejä tullaan käyttämään suuremmilla volyymeillä, kuin menneinä vuosina ja tietoja kalastellaan entistä taidokkaammin. Palvelunestohyökkäysten lisääntyvän määrän mahdollistaa IoT-laitteiden, esineiden internetin, kasvu. Uutena kohteena saatetaan nähdä myös virtuaaliympäristöt ja pilvipalvelut. (Viestintävirasto 2016b: 24).

Tietoturvaheikkouksia voidaan hyödyntää myös sähköisessä sodankäynnissä. Tällöin kohteina voivat olla yhteiskunnalle kriittinen infrastruktuuri, kuten sähkö- ja tietoliikennejärjestelmät. Nykypäivän tietoyhteiskunta on riippuvainen sähköisistä tietojärjestelmistä ja tiedonsiirrosta, jonka vuoksi tärkeät järjestelmät joutuvat huoltovarmuusvaatimusten alaisuuteen. Isku tai terroriteko tällaisiin järjestelmiin voi olla jatkumoa epäonnistuneesta politikoinnista, joka kärjistyy kyberhyökkäyksiin tai jopa hybridisodankäyntiin. Ensimmäinen tiedostettu kybersotatoimi SCADA-järjestelmään tapahtui 1982, kun haittaohjelma sai aikaan kaasuputken räjähtämisen Siperiassa. (Kostopoulos 2013: 176; Sisäministeriö 2016: 18–20.) Viimeisin kyberhyökkäys puolestaan tapahtui 23. päivä joulukuuta 2015, kun ukrainalaisen sähköverkkoyhtiön kaukokäyttöjärjestelmään tunkeuduttiin ja katkottiin sähköt yli 230 000 taloudelta (Zetter 2016).



Kuva 9. Uhkaluokittelu (ENISA 2016b: 15).

Ukrainassa tehtyä hyökkäystä edelsi tietojen kalastelu, joka alkoi työntekijöiden sähköposteista. Hakkerit lähettivät työntekijöille haittaohjelmia sähköpostitse ja pyrkivät tätä kautta saamaan pääsyn järjestelmiin. Haittaohjelmien synnyttämistä takaovista huolimatta hakkerit eivät onnistuneet luomaan suoraa yhteyttä SCADA-verkkoon, koska SCADA-verkko oli eriytetty palomuurilla toimistoverkosta. Hyökkääjät olisivat voineet yrittää murtaa SCADA-verkon palomuurin, mutta päätyivät murtautumaan käyttäjien hallintapalvelimelle (domain controller). Käyttäjien hallintapalvelimelta he etsivät käyttäjien VPN-tunnuksia SCADA-verkkoon. Varsinainen hyökkäys ajankohta ajoittui 23. joulukuuta iltapäivään ja tarkalleen vuoronvaihdon ajankohtaan. Hyökkäyksen alkuvaiheessa hakkerit sulkivat käytönvalvojat ulos järjestelmistä ja pimensivät valvomot. Valvomot pimenivät, koska hakkerit olivat sulkeneet etukäteen varavoimajärjestelmät käytöstä. Hakkerit avasivat sähköverkon katkaisijoita asema kerrallaan pimentäen sähkönjakelualueita ja samalla asuntoja. He vaikeuttivat vianhallinta- ja selvitystöitä aiheuttamalla samanaikaisesti puhelimitse palvelunestohyökkäyksen verkkoyhtiön asiakaspalveluun ja muuttamalla ala-asemien ohjelmistoja siten, että katkaisijat jouduttiin kytkemään kiinni paikallisesti käsin. Hakkerit viimeistelivät hyökkäyksen vielä tyhjentämällä hallintakoneiden kovalevyt KillDisk-haittaohjelmalla, jonka vuoksi koneet eivät enää lähteneet käyntiin. (Zetter 2016.)

Ukrainan sähköverkkoon tehty hyökkäys on hyvä esimerkki hyökkäysmenetelmien kehittymisestä. Hyökkäys kohdistui aluksi käyttäjiin, jotka mahdollistivat pääsyn järjestelmään (Zetter 2016). Näin ollen tärkeäksi muodostuu ihminen toimijana, minkä vuoksi jokaisella käyttäjällä on vastuu tietoturvan toteutumisesta. Hyökkääjät saattavat käyttää uusia ennalta arvaamattomia hyökkäystapoja, kuten Ukrainan puhelinverkon kautta tehty palvelunestohyökkäys (Zetter 2016). Jotta uudenlaisiin uhkiin voidaan varautua, täytyy tietoturvastavastaavien henkilöiden pystyä katsomaan laatikon ulkopuolelle. Epätodennäköisimmätkin hyökkäysmallit täytyy miettiä läpi tapauskohtaisesti. Mikäli hyökkäysten takana on valtio kuten Ukrainan tapauksessa, voidaan olettaa, että hyökkäykseen on mahdollisuus käyttää enemmän resursseja, kuin tavallisilla hakkeriryhmillä tai yksittäisillä henkilöillä on käytössä (Zetter 2016).

Kaukokäyttöjärjestelmien potentiaalisia hyökkääjiä valtiollisten toimijoiden lisäksi ovat mm. hakkerit, rikolliset, terroristit, bottiverkko-operaattorit, teollisuusvakoilijat ja katkeroituneet henkilöt. Ryhmät jaotellaan hyökkäystavan ja intressien mukaan. Kuvassa 10 ovat havainnollistettuna ryhmät ja käytetyt hyökkäystavat. Hakkerit käyttävät pääsääntöisesti verkosta ilmaiseksi löytyviä ohjelmia, jotka hyödyntävät tunnettuja haavoittuvuuksia. Hakkereiden tavoite on päästä urkkimalla järjestelmiin ja luoda murtojen kautta mainetta ja asemaa piireissä. Hakkerit myös levittävät yleensä murtojen yhteydessä omaa ideologiaansa sekä propagandaa. Rikollisten ja hakkereiden ero on se, että rikolliset pyrkivät hyötymään hyökkäyksestä taloudellisesti, mutta hakkerit eivät. Terroristit puolestaan pyrkivät fyysisten hyökkäysten lisäksi murtautumaan järjestelmiin, jossa voisivat aiheuttaa toimintahäiriöitä ja vaurioita. Bottiverkko-operaattorilla on puolestaan taka-ajatuksena valjastaa murrettu verkko osaksi palvelunestolaitteistoa ja hyväksikäyttää sen tietojenkäsittelykapasiteettia. Teollisuusvakoilijat etsivät luottamuksellisia tietoja kilpailijoiltaan tai tutkimuslaitoksista. He voivat käyttää apunaan tiedon saamiseksi sisäisiä myyriä, mutta verkkoyhtiöille vakoilu on kuitenkin vain pieni uhka. Pienen uhkan muodostavat myös katkeroituneet henkilöt, jotka voivat olla työsuhteessa yhtiöön tai voivat olla yhtiön aiempia työntekijöitä, jotka pyrkivät sabotoimaan yhtiön toimintaa tavoitellen taloudellista hyötyä. (Tervo 2013: 13.)

Hyökkääjä käyttää apunaan ihmisten hyväuskoisuutta sekä järjestelmän tietoturvapuutteita. Kaukokäyttöjärjestelmissä sähköverkon ohjauksen kannalta järjestelmään tulevan tiedon täytyy olla luotettavaa, eheää ja todennettua, kuten tieto on myös älykäissä sähköverkoissa. Tällöin uhiksi nousevat mm. järjestelmän salakuuntelu, liikenneanalyysi, toisto (viestin kaiutus), viestien muuttaminen, imitointi, palvelunesto ja haittaohjelmat. (Delgado-Gomes ym. 2015: 535–536.) Haittaohjelmat ovat olleet yleisesti suurin uhka ENISA:n vuonna 2015 julkaistun uhka näkymän mukaan. Haittaohjelmat ovat ohjelmia, kuten mainosohjelmia tai troijalaisia, jotka voivat luoda mm. takaovia, etätyökaluja tai keyloggereita. Haittaohjelmat pääsevät koneisiin ja järjestelmiin sähköpostin tai murrettujen ja epäilyttävien verkkosivujen kautta, mutta myös saastutettujen laitteiden avulla. Usein ne ovat vaikeasti havaittavissa, koska ne piiloutuvat järjestelmätiedostoiksi. (ENISA 2016b: 19–21.) Viime vuosien aikana kriittistä infrastruktuuria vastaan on hyö-

kätty Stuxnet, Sasser, Slammer ja Rocra nimisillä haittaohjelmilla, joiden tekijöiksi ovat osoittautuneet valtiolliset toimijat (Myllylä 2014: 56–57).

	Threat Agents								
	Cyber criminals	Insiders	Online social hackers	Nation States	Corporations	Hacktivists	Cyber Fighters	Cyber terrorists	Script kiddies
Malware	✓	✓	✓	✓	✓	✓	✓	✓	✓
Web-based attacks	✓			✓	✓	✓	✓	✓	✓
Web application attacks	✓			✓	✓	✓	✓	✓	✓
Botnets	✓			✓	✓	✓	✓	✓	✓
Denial of service	✓			✓	✓	✓	✓	✓	✓
Physical damage/ theft /loss	✓	✓		✓	✓			✓	
Insider threat	✓	✓		✓	✓			✓	
Phishing	✓	✓	✓	✓	✓	✓	✓	✓	✓
Spam	✓		✓	✓	✓	✓	✓	✓	✓
Exploit kits	✓			✓	✓	✓			✓
Data breaches	✓	✓		✓	✓	✓	✓	✓	✓
Identity theft	✓	✓		✓	✓	✓	✓	✓	✓
Information leakage	✓	✓	✓	✓	✓	✓	✓	✓	✓
Ransomware	✓		✓						✓
Cyber espionage		✓		✓	✓				

Legend:
Primary group for threat: ✓
Secondary group for threat: ✓

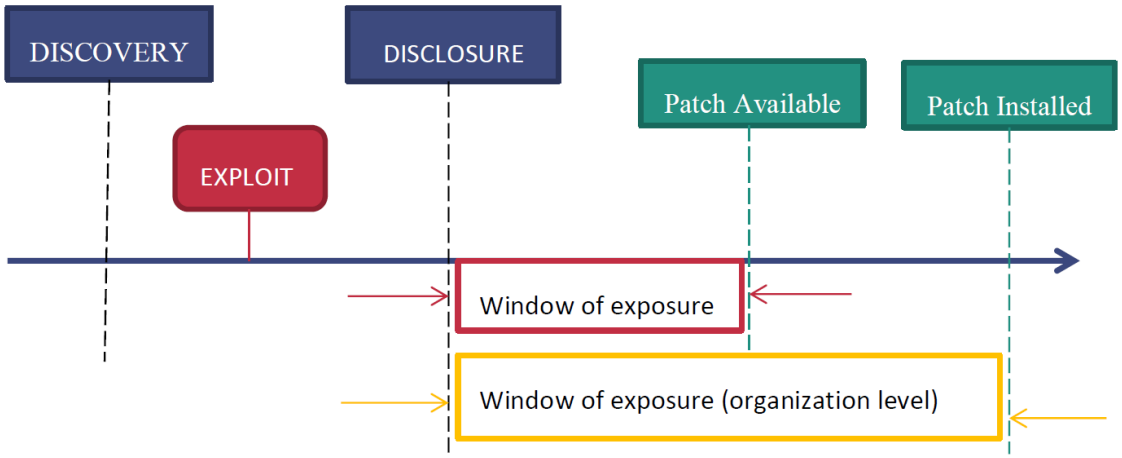
Kuva 10. Hyökkäystavat ja hyökkääjätahot esitettyinä (ENISA 2016b: 60).

Liikenneanalyysin ja salakuuntelun kautta voidaan myös päästä kiinni järjestelmään käyttäen MITM (man-in-the-middle) -hyökkäystä. Tällöin pyritään analysoimaan SCADA:lle kohdennettua liikennettä ja muuttamaan sitä matkalla. Tämä vaatii, että hyökkääjä pääsee laitteiden väliseen tietoliikenteeseen, joka on mahdollista IEC 60870-5 -protokollaperheen puutteiden vuoksi samoin kuin Modbus-protokollan heikkouksien

vuoksi. (Yang, McLaughlin, Littler, Sezer, Eul Gyu Im, Yao, Pranggono & H. F. Wang 2012: 2–3.) MITM-hyökkäys voidaan pyrkiä estämään käyttämällä suojattuja yhteyskäytäntöjä ja tiedonsiirtoväyliä. Tämä edellyttää tehokkaasti salattua liikenteen tunnelointia turvattomilla tiedonsiirtoväylillä.

Liikenneanalyysin myötä tai hakuammunnalla voidaan toteuttaa myös palvelunestohyökkäyksiä, jolloin hyökkääjä ei välttämättä pyri hallitsemaan kohteena olevaa järjestelmää vaan pyrkii vain estämään sen toiminnan. Palvelunestohyökkäysten kohteiksi ovat joutuneet viime vuosina peli- ja ohjelmistosektorin lisäksi internetpalveluiden tarjoajat. Rikolliset myyvät edullisesti rakentamiensa bottiverkostojen hyökkäyskapasiteettia ja näin siitä on tullut helposti ostettava palvelu. Pitkäkestoisella palvelunestohyökkäyksellä voidaan aiheuttaa myös suurta taloudellista vahinkoa. (ENISA 2016b: 28–29.) Vaikka SCADA-verkot käyttävät yleisesti omia eriytettyjä ja suojattu tiedonsiirtoväyliään voi tiedonsiirtopalvelun tarjoajaan kohdistettu isku johtaa suorasti tai epäsuorasti myös SCADA-verkon palveluiden jumiutumiseen ja hidasteluun. Palvelunestohyökkäyksiltä suojautuminen vaatii oman fyysisesti eriytetyn verkon SCADA-järjestelmää varten.

SCADA-järjestelmien viime vuosikymmenen kehitys täysin eristetystä järjestelmästä tilanteeseen, jossa verkko on kytköksissä yritysverkon ja internetin kanssa, on aiheuttanut lisääntyvän uhan ulkoisille hyökkäyksille (ENISA 2013: 1). Mikäli hyökkääjä pääsee suojattuun verkkoon, on hänellä mahdollisuudet päästä murtautumaan SCADA-järjestelmään käyttäen tunnettuja 0-päiväaukkoja, tai hyökkääjille suunnattuja Exploitkittejä, koska SCADA-järjestelmien haasteena ovat korjauspäivitysten aiheuttama vikaantuminen ja korjauspäivitysten puute (ENISA 2013: 1; ENISA 2016b: 37). Korjauspäivityksillä voi olla merkittävä vaikutus SCADA-järjestelmän toimintaa, minkä vuoksi testaamattomia päivityksiä ei voida hyväksyä ja näin ollen järjestelmät ovat pidempään alttiina tunnetuillekin uhille. Kuva 11 kuvaa aikaikkunaa hyökkäysaukon löydöstä paikkaavan päivityksen asentamiseen. SCADA-järjestelmien elinkaari on IT-järjestelmiä pidempi ja sen aikana korjauspäivitysten tulisi korjata turvallisuus- ja toiminnallisuusongelmat. Korjauspäivitys voi kuitenkin uusien ominaisuuksien lisäksi olla myös riski toimivan prosessin vakaudelle. (ENISA 2013: 1.)



Kuva 11. SCADA-järjestelmän haavoittuvuuden aikaikkuna (ENISA 2013: 1).

Järjestelmän käyttäjät ovat ratkaisevassa roolissa, kuten myös Ukrainan hyökkäyksessä. Käyttäjät kuuluvat sisäisiin uhkiin, joilla tarkoitetaan uhkaa, joka syntyy järjestelmän käyttäjän varomattomasta, virheellisestä tai tarkoituksen mukaisesta toiminnasta. Kybervakoilun ja käyttäjän manipuloinnin myötä sisäiset käyttäjät nähdään yhtenä monimuotoisimmista hyökkäyskanavista järjestelmiin. (ENISA 2016b: 32.) Haavoittuvuuden vakavuuteen vaikuttavat tietoturvan hallinnointi, jonka osia ovat tietoturvapolitiikka ja tietoturvan johtaminen. Tämän kautta myös henkilöstön tietoturvaosaaminen ja -tietous tulisi siis saattaa riittävälle tasolle ja käyttäjäoikeuksien hallinnan tulisi olla ajantasaista ja tarkasti säänneltyä. (Tervo 2013: 15.) Hyökkääjä voi käyttää sisäiseen käyttäjään hyvin monimuotoisia hyökkäyskeinoja, kuten haittaohjelmia, tietovuotoja, identiteetin varastamista, fyysistä varkautta tai haittaa, tietojenkalastelua tai web-pohjaisia hyökkäyksiä (ENISA 2016b: 33).

4 JÄRJESTELMÄN TIETOTURVALLINEN OPEROINTI JA YLLÄPITO

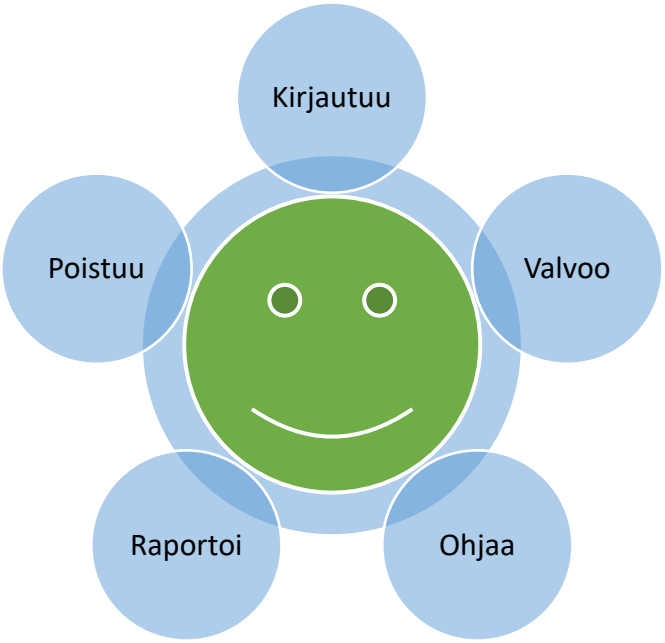
Tietoturva koostuu useista alueista ja sen heikoimmaksi lenkiksi voi muodostua ihminen. ”Suomi kyberturvallisuuden kärkimaita 2016?”, Aalto yliopiston järjestämä paneelikeskustelu keväällä 2016, avasi yleistä vallitsevaa tietoturvanäkemystä ja tilaa. Viestintäviraston pääjohtaja Kirsi Karlamaa totesi, että viime vuosina on otettu askelia eteenpäin. Näitä askelia ovat olleet Kyberturvallisuuskeskuksen ja HAVARO:n (Tietoturvaloukkausten havainnointi- ja varoitusjärjestelmä) perustaminen. Niiden myötä on pystytty tarjoamaan palveluita huoltovarmuuskriittisille toimijoille. Parannettavaa on kuitenkin esimerkiksi ihmisten asenteissa varoituksiin. Usein ihmisten asenteiden muutos vaatii jotain konkreettista näyttöä uhasta ennen kuin he ovat valmiita ryhtymään suojaustoimenpiteisiin. Huoltovarmuuskeskuksen toimitusjohtaja Raimo Luoma puolestaan kertoo, että kyberturvallisuusharjoitukset ovat lisääntyneet huoltovarmuuskriittisissä toiminnoissa, mutta kyberturvallisuus itsessään ei ole vielä energiasektorilla kaikilta osin kunnossa. Luoma viittaa 2015 syksyllä valmistuneeseen raporttiin kyberturvallisuuden tilannekuvasta energia-alalla. Lisäksi Luoman puheesta saa sen käsityksen, että välillä esiin nousee huolestuttaviakin asioita tietoturvan laiminlyönneistä, mutta vaitiolovelvollisuudesta johtuen ne eivät koskaan päädy julkisuuteen. (Paneelikeskustelu 2016.)

Verkostoautomaatiojärjestelmien tietoturvasta on viimeisten kolmen vuoden aikana tehty kaksi julkisesti internetissä saatavilla olevaa selvitystä. Ensimmäinen Renecon toimesta tehty selvitys valmistui 2013 ja se on kokonaisuudessaan julkinen. Viimeisin tutkimus on puolestaan Huoltovarmuuskeskuksen tilaama ja XCure Solutions Oy:n toteuttama tutkimus syksyllä 2015, josta on julkisesti saatavilla loppuraportti. Koska Suomessa on paljon erikokoisia sähkönjakeluyhtiöitä, tuloksissa esiintyi hajontaa. Tietoturvan toteutumisella ei kuitenkaan ollut kaikilta osin suoraa suhdetta yhtiön kokoon vaan myös pienten yhtiöidenkin joukosta löytyi jo vuonna 2013 mallisuoriutujia. Tulosten vertailun perusteella kuitenkin kehitystä on tapahtunut kahden vuoden aikana ja varsinkin teknisen tietoturvan osa-alue oli 2015 tehdyn tutkimuksen perusteella suurelta osin

erittäin hyvällä tasolla. Haasteita ja hajontaa kuitenkin löytyy edelleen hallinnollisen tietoturvan sekä tiedon elinkaaren hallinnan osalta. (Tervo 2013: 38; Immonen 2015: 5.)

Diplomityön yhteydessä tehtiin pienelle kohdennetulle ydinryhmälle sähköpostikysely syksyllä 2016, jonka perusteella pyrittiin selvittämään mahdollisia poikkeamia aiemmin saaduista tuloksista. Kysely osoittautui haastavaksi, koska tietoturvaan vedoten useat jättivät vastaamatta. Saadut vastaukset puolestaan käsitellään luottamuksellisesti, eikä niitä voida kohdentaa tarkemmin. Kyselyn tulokset huomioidaan kuitenkin luotaessa yleiskuvaa kaukokäyttöjärjestelmän tietoturvallisesta operoinnista ja ylläpidosta. Tutkielman menetelmänä hyödynnetään kvalitatiivista vertailua, sillä luvusta 3 valittuja tietoturvavaatimuksia ja -ohjeistuksia vertaillaan sähköpostikyselyn, Renecon ja XCure Solutions Oy:n tietoturvaselvitysten perusteella saatuun yleiskuvaan sekä luvussa 3 esitettyihin tietoturvauhkiin. Diplomityön tavoitteena on vertailevan tutkimuksen keinoja hyväksikäyttäen luoda ja kehittää tietoturvallisia operointi- ja ylläpitotoimia. Tutkielmassa kaukokäyttöjärjestelmän tietoturvallista operointia ja ylläpitoa lähestytään kahdesta eri näkökulmasta: käytönvalvojan ja ylläpitäjän näkökulmasta.

Kaukokäyttöjärjestelmän avulla sähköverkkoa operoi käytönvalvoja, jonka toimet kaukokäyttöjärjestelmässä ovat lähinnä järjestelmän valvomista, ohjaamista ja tarvittaessa raportointia, kuten kuvassa 12 esitetään. Yhteiskunnan jatkuvan sähkön tarpeen vuoksi operointi tulee suorittaa tietoturvallisesti ilman turhia sähkönjakelukatkoksia. Kaukokäyttöjärjestelmän ylläpitäjän toimet järjestelmässä voivat olla puolestaan nimetyistä vastuutehtävistä riippuen kuvan 13 mukaisia. Toimiin voivat kuulua käyttäjien ja järjestelmän hallinta, ylläpito ja muokkaus. Tämän lisäksi tärkeässä roolissa ovat myös päivitysten testaukset ja dokumentointi. Ylläpitäjän tulee pyrkiä toimillaan parantamaan järjestelmän tietoturvatasoa sekä taata ala-asemayhteyksien luotettava toimivuus.



Kuva 12. Käytönvalvojan toimet kaukokäyttöjärjestelmässä.

Kuva 13. Ylläpitäjän toimet kaukokäyttöjärjestelmässä.

Järjestelmän tietoturvallista operointia ja ylläpitoa lähdetään tarkastelemaan tietoturvan osa-aluejakoa hyödyntäen. Jokaisella osa-alueella määritellään aluksi yleiskuva vallitsevasta tietoturvan tilasta ja mahdolliset heikkoudet perustuen aikaisempiin tutkimustuloksiin sekä sähköpostikyselyyn. Tämän jälkeen määritellään osa-aluetta koskevat vaatimukset, jotka tulisi huomioida tietoturvallisen toiminnan toteuttamisessa. Koska viimeisessä kansallisessa XCure Solutions Oy:n tutkimuksessa 2015 on käytetty vaatimuksena Katakri III -turvallisuusauditointikriteeristöä ja ISO/IEC 27000 -standardiperheen standardeja, ovat ne myös tässä työssä vertailun kohteena. ISO/IEC 27000 -standardiperheen käyttöä puoltaa myös tuore EU-alueen verkko- ja tietoturvadirektiivi, joka velvoittaa käyttämään kansainvälisesti hyväksyttyjä standardeja.

4.1 Hallinnollinen tietoturva

Tutkimusten ja haastatteluiden perusteella hallinnollisen tietoturvan taso on kehittynyt positiivisesti viimeisten vuosien aikana, edelleen kuitenkin mukaan mahtuu poikkeuksia. Immonen (2015: 4) toteaa viimeisimmässä raportissaan, että hallinnollisessa tietoturvallisuudessa otetaan huomioon energiasektorin lainsäädäntö ja erityisvaatimukset, mutta tiedonluokittelu ja -hallinta ovat puutteellisia. Tietoturvapolitiikka saattaa olla kattavasti toteutettu, mutta on epäselvää missä määrin se jalkautetaan käytäntöön, ohjeistuksiin ja koulutuksiin. Epäselvyyttä tutkimuksissa on esiintynyt myös vastuuhenkilöiden nimeämisen suhteen. Vastuidenjakoa ei ollut joko suoritettu tai vastuiden määrittelyssä oli havaittu ongelmia. (Tervo 2013: 15; Immonen 2015: 5.)

Hallinnollisen tietoturvan toteuttamiseen on olemassa useita ohjeita ja yhtiön tuleekin muodostaa aina tarpeisiinsa ja liiketoimintastrategiaansa sopiva hallinnollinen tietoturva alkaen tietoturvapolitiikasta ja sen tavoitteista. Politiikkaa laadittaessa tulee ottaa huomioon organisaatiolle tai alalle kohdistetut erityisvaatimukset, jotka voivat olla myös laissa määrättyjä. Sähkömarkkinalaki velvoittaa sähköverkkoyhtiöitä varautumissuunnitelman tekoon ja Huoltovarmuuskeskus puolestaan vaatii yhteiskunnallisesti tärkeän sähköntuotannon ja -jakelun turvaamista. Nämä ulkoiset vaikutteet jo itsessään vaikuttavat paljon siihen, että kovin kevyellä tietoturvalla ei näissä yhtiöissä voida lähteä liik-

keelle. Tämän lisäksi EU:n vuonna 2016 voimaan tullut verkko- ja tietoturvadirektiivi tulee myös vaatimaan standardeihin ja hyviin käytöntöihin perustuvaa tietoturvaa yhteiskunnan keskeisiltä toimijoilta. Tietoturvapolitiikan laadinnassa ja ohjeiden teossa on hyvä käyttää apuna kansainvälisiä standardeja, kuten ISO/IEC 27001, -27002 ja energia-alan prosessiohjaukseen suunnattua ISO/IEC TR 27019.

Kuvassa 14 on esitetty lyhyesti Katakri 2015:ta asettamat vaatimukset hallinnolliselle tietoturvajohtamiselle. Kaukokäyttöjärjestelmän operointiin ja ylläpitoon hallinnollinen tietoturva vaikuttaa monin tavoin. Joskus yhtiöissä saattaa olla tilanne, että kaukokäyttöjärjestelmän ylläpitäjän vastuulla on myös laajamittaisesti tietoturvasta vastaaminen. Nopeat verkot ja runsaat etäkäyttömahdollisuudet mahdollistavat ylläpitotoimenpiteiden oston myös ulkopuolisilta toimittajilta, mutta lähtökohtaisesti ostajan tulisi tietää, mitä ostaa ja miten työt toteutetaan, jotta tietoturva toteutuu toiminnassa.

Vaikka ylläpitäjällä ja käytönvalvojalla on erilaiset toiminnot kaukokäyttöjärjestelmässä, joutuvat molemmat päivittäin työssään noudattamaan yhtiön tietoturvapolitiikan mukaisia toimintamalleja. Heillä on näin ollen vastuu tietoturvan ja yhtiön turvallisuusperiaatteiden toteutumisesta niille määriteltyjen asioiden ja toimintojen osalta. Tutkimustuloksissa ilmenneet epäselvyydet tieturvavastuista ja osin tietoturvapolitiikasta voivat johtua siitä, että tietoturvapolitiikka on ollut vain ylimmän johdon tiedossa, eikä sitä tai ohjeistusta ole jaettu riittävissä määrin kaukokäyttöjärjestelmän ylläpidosta ja operoinnista vastaaville toimijoille.

Kuva 14. Katakri 2015 turvallisuusjohtaminen. (Puolustusministeriö 2015: 6–12).

ISO/IEC 27001 määrittelee tietoturvallisuuden hallintajärjestelmän vaatimukset. Tämän mukaan johtamisessa ja sitouttamisessa tulisi huomioida tietoturvamääräysten integrointi organisaation prosesseihin ja varmistaa, että tietoturvalle tarvittavat resurssit ovat käytettävissä. Tietoturvasta on tärkeää viestittää, että se toteutuu. Tämän lisäksi tulee varmistaa, että asetetut tavoitteet saavutetaan ja jatkuva kehittäminen on prosessissa mukana. (ISO/IEC 27001 2013: 2.) Tietoturvan parantamiseen löytyy yksinkertainen PDCA-malli, joka on esitetty kuvassa 6 (sivulla 31). ISO/IEC 27005 mukainen riskien käsittely on kuvattu kuvassa 7 (sivulla 32) ja puolestaan tietoturvariskienhallintamalli kuvassa 8 (sivulla 33). ISO/IEC 27002 sisältämät menettelyohjeet tietoturvalle puolestaan esittävät

organisaation tietoturvakohdassa, että kaikki tietoturvavastuut tulee määritellä ja kohdentaa, ristiriitaiset velvollisuudet ja vastuualueet tulee myös erotella väärinkäytösten vuoksi. Tämän lisäksi on tärkeää määritellä myös järjestelmän etäkäyttöpolitiikka, koska sähköverkon ohjaus on mahdollinen myös etäyhteyksien kautta. (ISO/IEC 27002 2013: 4–8.) ISO/IEC TR 27019 (2013: 6) tekninen raportti on suunnattu energiateollisuudelle ja siinä korostetaan vielä lisäyksenä edeltävään yhteistyön merkitystä merkittävien viranomaisten kanssa, sillä energiateollisuus kuuluu kriittiseen infrastruktuuriin.

Standardia mukaillen kaukokäyttöjärjestelmäorganisaatioissa tulisi siis määritellä entistä paremmin henkilöt, jotka vastaavat tietoturvasta ja mitkä heidän tehtävänsä ovat. Tehtävien määrityksessä tulisi huomioida, ettei ristiriitaisia vastuualueita synny. Tietoturva tulisi jalkauttaa paremmin yhtiön prosesseihin ja koko organisaatioon. Tämä voisi tarkoittaa ylläpitäjän näkökulmasta sitä, että hänelle nimettäisiin vastuualueita liittyen teknisen turvallisuuteen ja pienemmissä yhtiöissä myös fyysisen turvallisuuden ja henkilöstöturvallisuuden osalta. Vastuiden nimeäminen kuitenkin edellyttää, että henkilöllä on riittävä asiantuntijuus tehtävän suorittamiseksi. Ylläpitäjän tulee luoda ja päivittää tarvittaessa vastuualueeseensa liittyvä poikkeustilaohjeistus, jotta se on ajantasainen ja käytettävissä.

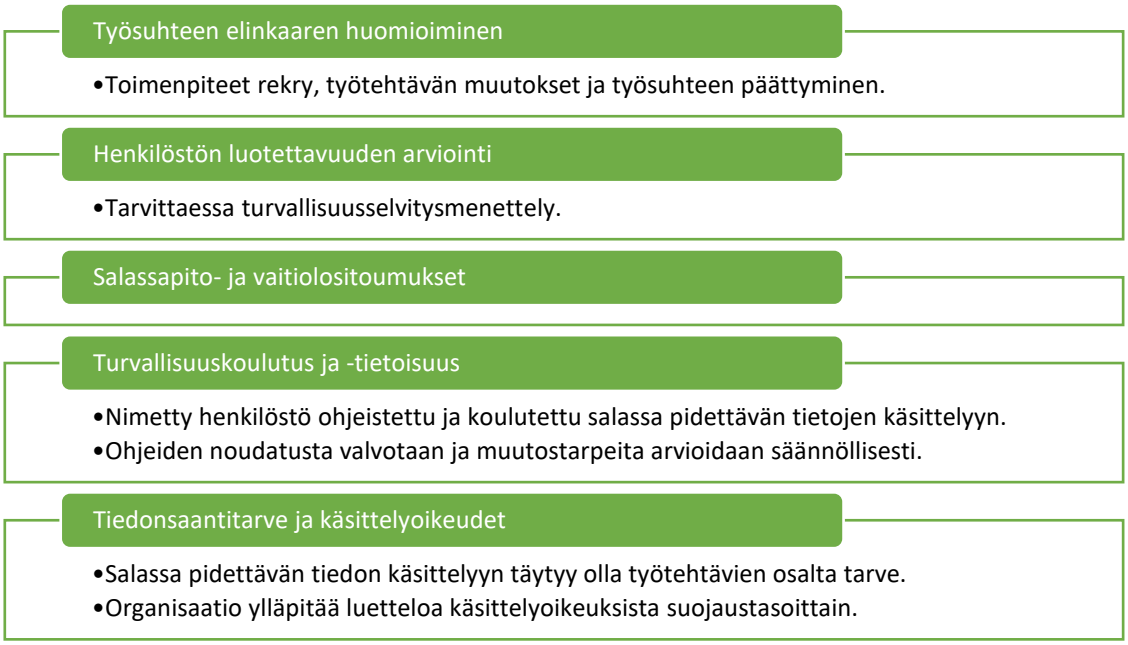
Järjestelmää operoivan käytönvalvojan osalta parannukset tarkoittaisivat lähinnä parempaa yhtiön sisäistä tietoturvakoulutusta, jossa esitetään selkeästi käytönvalvojan toimenkuvaan kuuluvat toimet ja niiden tietoturvallinen toteuttaminen. Tämän lisäksi käytönvalvojan tulisi tunnistaa mahdolliset poikkeamat järjestelmässä ja tietää miten toimia poikkeusoloissa. Käytönvalvojien tietoturvatietämyksen tasoa tulisi seurata säännöllisesti ja tietoja päivittäviä lisäkoulutuksia järjestää tarvittaessa.

4.2 Kaukokäyttöjärjestelmän henkilöstöturvallisuus

Henkilöstöturvallisuuden osa-alue oli Renecon tekemän tutkimuksen perusteella vuonna 2013 käyttöoikeuksien hallinnan osalta monimuotoinen ja osassa yhtiöistä oli käytössä yhteinen salasana käytönvalvontajärjestelmään (Tervo 2013: 30). Kehitystä tästä on kui-

tenkin tapahtunut, sillä XCure Solutions Oy:n 2015 raportissa ei ole mainintaa kyseisestä ongelmasta ja myös haastattelujen perusteella käytössä on käyttäjäkohtaiset tunnukset. XCure Solutions Oy:n mukaan puutteita puolestaan ilmeni salassapito- tai vaitiolositoumusmenettelyjen käytön suhteen. (Immonen 2015: 4; Sähköpostikysely 2016.)

Katakrin henkilöstöturvallisuudessa (kuva 15) on määritelty henkilöstöä koskevat vaatimukset, jotka ovat myös samaan tapaan esillä ISO/IEC 27002 -standardissa. 27002 ottaa myös kantaa työsuhteen aikana tapahtuvan tietoturvan toteuttamiseen, henkilön itsensä kehittämiseen ja seuraamusmenettelyyn. ISO/IEC TR 27019 määrää tarkastamaan vielä erityisen huolella kriittisen infrastruktuurin ylläpidosta vastaavat ja infrastruktuuria operoivat henkilöt. Tämän lisäksi työsopimuksissa tulee ottaa huomioon erityisesti työntekijän sitoutuminen tietoturvan toteuttamiseen ja kriittisistä toimista vastaavien henkilöiden osalta vielä erikseen rajoitteet, kuten lakko-oikeus tai hätätilanteessa enimmäistyöajan määritys. Henkilön pääsynhallintaan liittyen ISO/IEC 27002 -standardista löytyy myös vaatimuksia pääsynhallintapolitiikkaan, henkilöiden rekisteröintiin, pääsyoikeuksien jakamiseen ja tunnistautumistietojen hallintaan. (ISO/IEC 27002 2013: 9–12, 19–24; ISO/IEC TR 27019 2013: 10.)



Kuva 15. Katakri 2015 henkilöstöturvallisuus (Puolustusministeriö 2015: 13–15).

Koska yhtiön henkilöstö on usein se helpoin tie kaukokäyttöjärjestelmään, on ylläpitäjän ja käytönvalvojan osalta tärkeää sitoutua itsensä kehittämiseen ja tietoturvan toteuttamiseen työsuhteen jokaisessa vaiheessa. Käytännössä tämä tarkoittaa, että ylläpitäjä ja käytönvalvoja tiedostavat riskin, että heitä voidaan yrittää huijata arkaluontoisten tietojen saamisen toivossa. Tietoturvan vastuualueiden osalta ylläpitäjä voi vielä lisäksi joutua vastaamaan käyttäjätunnuksista ja -oikeuksista, jolloin on tärkeää, että käyttäjien oikeudet ovat ajan tasalla ja salasanat riittävän vahvoja käyttäjän oikeuksiin suhteutettuna. Ylläpitäjän vastuulla voi olla myös käyttäjätunnusten käytön valvominen, että mahdolliset väärinkäytökset voidaan eliminoida.

4.3 Valvomon fyysinen turvallisuus

XCure Solutions Oy:n raportista käy ilmi, että fyysinen turvallisuus toteutuu hieman ristiriitaisesti. Vahvuutena voidaan todeta useilla olevan jo käytössä kamera- ja kulunvalvonta, joka kuitenkin saattaa osalla toimia puutteellisesti. Vaikka tilat ovat suunniteltu riskienhallintaprosessien kautta, uuden tyyppiset riskit, kuten sabotaasi, terrorismi, tiedustelu tai rikokset ovat jääneet huomiotta. (Immonen 2015: 4.) Kyselyn perusteella kuitenkin kaikki alkaa näiltä osin olla kunnossa kaukokäyttöjärjestelmävalvomoiden osalta (Sähköpostikysely 2016).

Katakrin kuvassa 16 lyhyesti esitetyt fyysisen turvallisuuden vaatimukset ovat kattavia ja niissä otetaan huomioon hieman ehkä liiankin laajalla mittakaavalla fyysinen tietoturva kaukokäyttöjärjestelmän valvomoa ajatellen. Tässä kohdassa on hyvä lähteä miettimään tietoturvaa yhtiön tarpeista, mutta unohtamatta kriittisen infrastruktuurin asettamia korkeampia vaatimuksia mm. toiminnan jatkuvuuden varmistamiselle. ISO/IEC TR 27019 (2013: 12) puolestaan lähtee ohjeistamaan tietoturvallisen kaukokäytön rakentamispaikan valinnasta lähtien.

Kuva 16. Katakri 2015 fyysinen turvallisuus (Puolustusministeriö 2015: 18–28).

Fyysisen turvallisuuden yhteys kaukokäyttökäyttöjärjestelmän ylläpitoon ja operointiin tulee vastaan joka päivä valvomotilan kulunvalvonnan ja mahdollisen kameravalvonnan kautta. Tämä on tietoturvan toteutumisen kannalta tärkeää, ettei valvomoon pääse tunkeutumaan asiattomia henkilöitä. Valvomo ei kuitenkaan nykypäivänä ole enää se ainut paikka, josta pystytään valvomaan järjestelmää vaan mikäli käytetään etäyhteyksiä, tulisi se tehdä myös turvallisessa ympäristössä. Ylläpidollisesti tietoturvaa tulee tarkastella jatkuvuuden näkökulmasta, mikä tarkoittaa ennalta ehkäiseviä toimenpiteitä kriittisiin laitetiloihin. Samoihin laitetiloihin tulee olla pääsy vain sinne työtehtävien puolesta pääsyn tarvitsevilla henkilöillä. Järjestelmän varmuuskopiot tai luottamukselliset avaimet tulee säilyttää fyysisesti ja teknisesti suojatuissa, riittävän suojauksen omaavissa säilytysvälineissä, jolloin pystytään takaamaan tiedon koskemattomuus.

4.4 Tekninen tietoturva

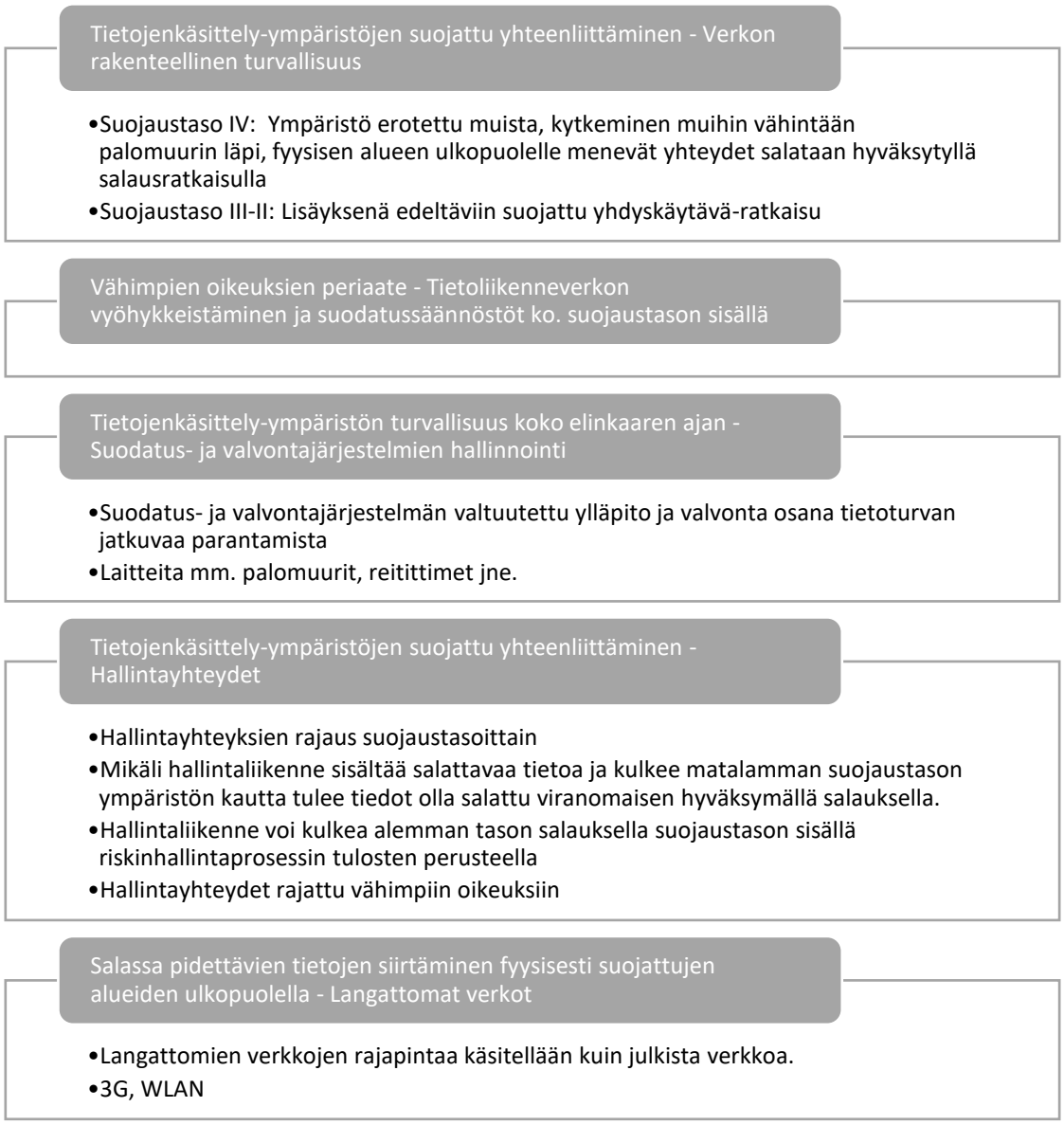
Tekninen tietoturvallisuus on osa-alueeltaan todella laaja ja vaikka sen toteutuminen suurimmalta osin tutkimusten perusteella on hyvällä tasolla, tulee siihen kiinnittää erityishuomiota. Tekninen tietoturva suojaa viime kädessä kaukokäyttöjärjestelmän sisäisiltä ja ulkoisilta uhilta ja teknisiltä väärinkäytöksiltä, kuten oikeudettomilta ohjauksilta tai kriittisen tiedon muutoksilta. Sisäisiä uhkia voivat olla mm. ylläpito- ja operointitoimijoiden inhimillisestä virheestä aiheutunut toiminta. Teknisen tietoturvan tarjoamista vaikutusmahdollisuuksista huolimatta se on kuitenkin vain yksi osakokonaisuus tietoturvaa. Näin ollen löytyy myös toimia, joita teknisellä suojauksella ei välttämättä pystytä täysin torjumaan. Tekniseen tietoturvaan kuuluvat tietoliikenneturvallisuus, laitteistoturvallisuus, ohjelmistoturvallisuus, tietoaineistoturvallisuus ja käyttöturvallisuus.

4.4.1 Tietoliikenneturvallisuus

Kaukokäyttöjärjestelmässä tiedon luotettavuus, sekä ohjattavasta kohteesta riippuen myös aikakriittisyys, ovat tärkeässä roolissa. Tärkeiden yhteyksien kahdentamisella voidaan varmistaa järjestelmän parempi vikasietoisuus. 2013 tehdyn tutkimuksen perusteella tietoliikenneturvallisuus on toteutettu käyttämällä pääosin yhtiön omia tietoliikenneverkkoja, joita on sitten tarpeiden mukaan laajennettu teleoperaattoreilta vuokratuilla yhteyksillä. Tämä mahdollistaa vahvasti eriytettyjen verkkoalueiden luomisen, mikä parantaa kaukokäyttöjärjestelmän turvallisuutta. Tekninen siirtymä sarjaliikenneyhteyksistä IP-pohjaiseen liikenteeseen vaatii verkkolaiteiden asettelijoilta vahvaa teknistä ja tietoturva-osaamista. (Tervo 2013: 30.) 2015 ja 2016 saatujen tietojen mukaan tämä alue on pääsääntöisesti hyvin turvattu.

Kuvassa 17 esitetään Katakrin asettamat kovat vaatimukset tietoliikenneturvallisuudelle. Mikäli kaukokäyttöjärjestelmien tietoliikenneturvallisuudessa pystytään toteuttamaan kokonaisuudessaan Katakrissa asetetut vaatimukset ja suojaustasot, on järjestelmän tietoturva näiltä osin varmasti riittävä. ISO/IEC 27002 -standardin tietoliikenneturvallisuudessa vaaditaan verkon valvontaa siten, että tietojärjestelmät ja sovellukset ovat suojattuja, tietoturvamekanismit, palvelutasot ja tarvittavat hallintapalvelut ovat tunnis-

tettuja ja sisällytetty verkkopalvelusopimuksiin. ISO/IEC TR 27019 vaatii puolestaan suojattua kaukokäyttöliikennettä, joka varmistaa tiedon luottamuksellisuuden, eheyden ja saatavuuden niin sisäisissä kuin ulkoisissa kaukokäyttöyhteyksissä. Aikasynkronoinnista ohjeistetaan käyttämään sisäisiä NTP-servereitä tai digitaalisesti-allekirjoitettu NTP-aikaviestejä, jotta voidaan estää mahdolliset NTP-signaalimanipulaatiot. Vanhojen järjestelmien osalta ohjeistetaan tekemään kunnolliset haavoittuvuus ja riskiarviot. (ISO/IEC 27002 2013: 49; ISO/IEC TR 27019 2013: 18–20.)



Kuva 17. Katakri 2015 tietoliikenneturvallisuus (Puolustusministeriö 2015: 30–37).

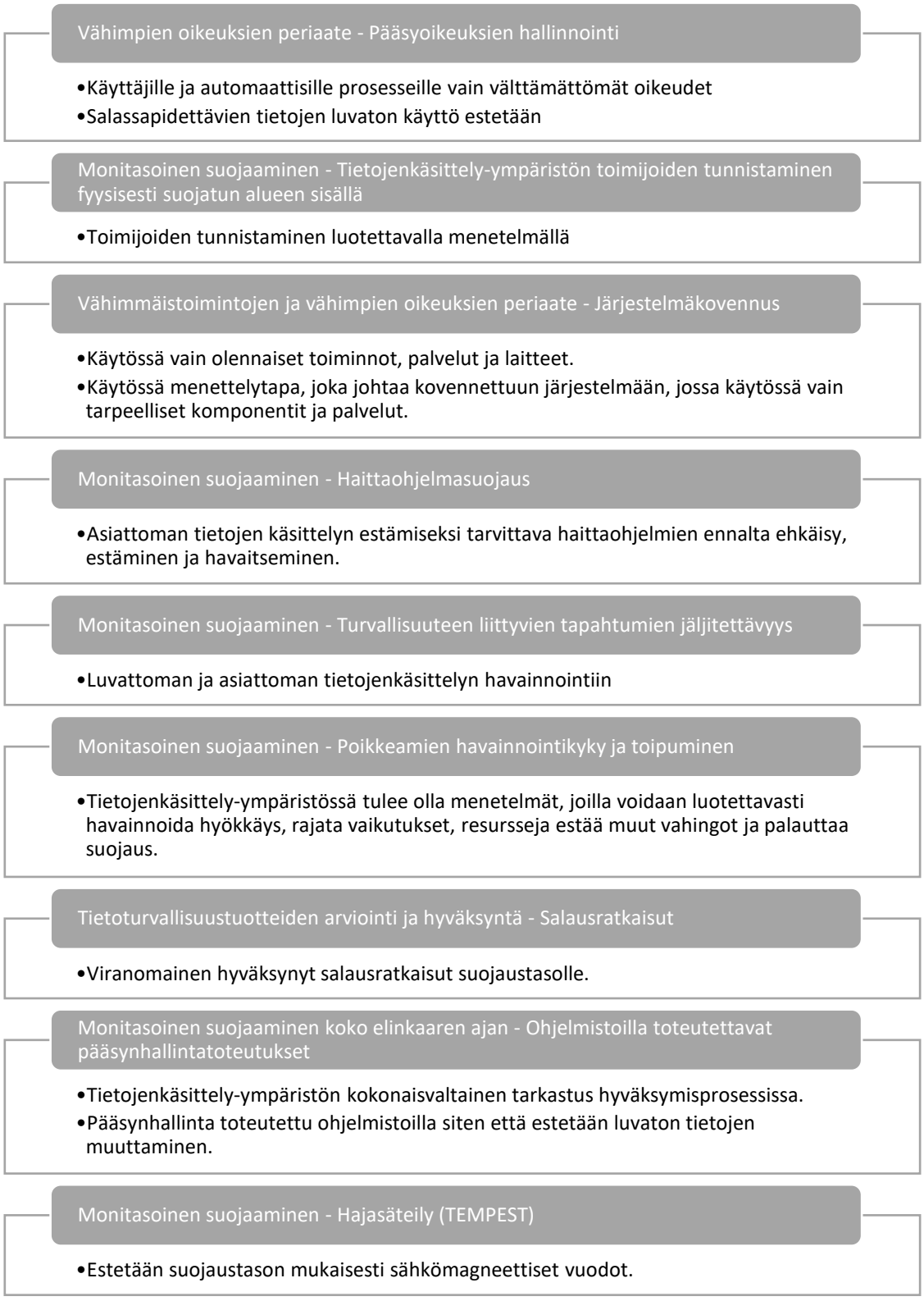
Tietoliikenneturvallisuus järjestelmän operoinnin osalta on merkittävässä roolissa, koska valvomosta on useita eritasoisia yhteyksiä sähköasemille ja erottimille. Käytönvalvojan tulee tietää ohjaushetkellä sähköverkon tila ja mahdollisissa vikatilanteissa vikaantunut tai hälyttävä laite, jotta hän pystyy palauttamaan sähköt toimivaan osaan verkkoa. Ylläpitäjä puolestaan vastaa kaukokäyttöjärjestelmän toiminnasta siten, että normaalitilanteessa yhteydet ala-asemien ja kaukokäyttöjärjestelmän välillä toimivat luotettavasti. Ylläpitäjän vastuulla voi olla tietoliikenneyhteyksien salaus, kahdentaminen ja koventaminen osana järjestelmän teknistä tietoturvavastuuta. Tällöin tulee huomioida myös yleiset uhat, kuten palvelunestohyökkäykset, MITM-hyökkäykset varsinkin käytettäessä julkisia tiedonsiirtoväyliä. Ylläpitäjällä tulee olla riittävä tietotaito ja osaaminen tietoliikenneturvallisuuden toteuttamiseen, mikä tarkoittaa ajantasaista koulutusta kyseiseen tietoturva-alueeseen. Uusien ja vanhojen laiteiden osalta on hyvä varmistaa, että kaikki tarpeettomat palvelut ja toiminnot ovat pois kytkettynä ja palomuurin asetteluissa tulisi käyttää tapahtumien kirjausta sekä tiukkoja sääntöjä, jolloin verkon tietoliikennettä voidaan valvoa ja rajoittaa tarvittavan tietoturvatason saavuttamiseksi. Yksityiskohtaista ohjeistusta salauksiin ja palomuurin asetteluihin on laajalti saatavilla useista eri lähteistä. Kaukokäyttöjärjestelmän tarpeisiin hyviä lähteitä ovat mm. ICS-CERT ja NERC CIP.

4.4.2 Laitteisto- ja ohjelmistoturvallisuus

Laitteisto- ja ohjelmistoturvallisuus nousee tärkeään osaan sähkönjakelussa, jossa toimilaitteiden elinkaari on huomattavasti tavallisia IT-järjestelmiä pidempi. Joskus voi tulla vastaan tilanteita, että vanhan tietoliikennekortin tilalle ei esimerkiksi löydy enää korvaavaa tai uuteen tietoliikennekoneeseen ei löydy yhteensopivaa korttia, joka toimisi vanhojen ala-asemien kanssa. Vastaavasti eteen voi tulla tilanteita, joissa kaukokäyttöverkossa on edelleen käytössä Windows NT-käyttöjärjestelmällä toimivia koneita, joiden virallinen ja epävirallinen tuki on päättynyt jo useita vuosia sitten. Tämän vuoksi laitteisto- ja ohjelmistoturvallisuudesta tulee huolehtia. XCure Solutions Oy:n vuonna 2015 julkaistun raportin perusteella laitteistosta pidettiin hyvin yllä varmuuskopioita, mutta uusien laitteiden käyttöönotoissa ei juurikaan suosittu koventamismenetelmiä ja järjestelmästä oli vaikea havaita mahdolliset poikkeamat (Immonen 2015: 4).

Katakrin kuvassa 18 esitetyt tietojärjestelmäturvallisuuden vaatimukset kuuluvat laitteisto- ja ohjelmistoturvallisuuden alueeseen, mutta sivuavat myös muita teknisen tietoturvan osa-alueita. Katakria vastaavia vaatimuksia asettaa myös ISO/IEC 27002 (2013: 13–14, 19–28, 33–38, 41–48), josta laitteisto- ja ohjelmistotietoturvan alueeseen kuuluvat suojattavan omaisuudenhallinnan osalta laitteiden luettelointi, pääsynhallinnasta mm. sovellusten ja prosessien oikeudet, fyysisen turvallisuuden hallinnasta laiteiden sijoittelu ja sähkönsyötön varmistus ja käyttöturvallisuuden alueesta mm. päivitys- ja ylläpitotoimia. ISO/IEC TR 27019 tarkentaa suojattavan omaisuuden käsitettä energiasektorilla. Tällöin suojattavalla omaisuudella tarkoitetaan siis koko kaukokäyttöjärjestelmäprosessia aina valvontatiedosta fyysisiin toimilaitteisiin sekä palveluihin. Pääsynhallinnasta puolestaan todetaan, että tietoturvapolitiikan tulee ottaa huomioon vanhojen järjestelmien rajoitteet, kuten mahdollisuus vain yhden salasanan käytölle ja heikoille salasanoille. Tällaisissa tapauksissa tulee pyrkiä parhaan tason saavuttamiseen mahdollisuuksien mukaan. Ongelmaksi nousevat tällöin myös säännöllinen salasanojen vaihtaminen keskittämättömissä ympäristöissä. Kolmannen osapuolen tiloissa toimittaessa tulee varmistaa laitteiden ympäristö riskien minimoinniksi, kuten luvattoman käytön estämiseksi. (ISO/IEC TR 27019 2013: 8–9, 15, 20–22.)

Kaukokäyttöjärjestelmän ylläpidon kannalta koventaminen eli vähimpien oikeuksien periaate olisi hyvä saada toteutettua mahdollisimman laaja-alaisesti. Tällä tavoin voidaan vähentää järjestelmiin murtautumisen riskiä. Laitteistojen suojaus ja tapahtumien monitorointi tulisi toteuttaa siten, että mahdolliset poikkeamat järjestelmässä havaitaan. Ylläpitäjän vastuulla on teknisesti ylläpitää käyttäjäturvallisuuden mukaisia käyttäjäoikeuksia ja sovellusten osalta puolestaan prosessi- ja ohjelmakohtaisia oikeuksia. Ylläpitäjä vastaa siitä, että laitteistosta ja ohjelmista on tarvittavat varmuuskopiot, dokumentaatiot ja ohje järjestelmän toiminnan palauttamiseen vikatilanteesta. Ylläpitäjän vastuulla on myös ohjelmistojen ja laiteohjelmistojen ajan tasalla pitäminen. Päivitykset tulee pyrkiä asentamaan järjestelmiin heti kun se on turvallista, että järjestelmän haavoittuvuuden aikaikkuna, joka on esitetty kuvassa 11 (sivulla 43), voidaan supistaa mahdollisimman pieneksi. Kaukokäyttöjärjestelmää operoivalla henkilöllä ei varsinaisesti ole vastuita tällä osa-alueella.



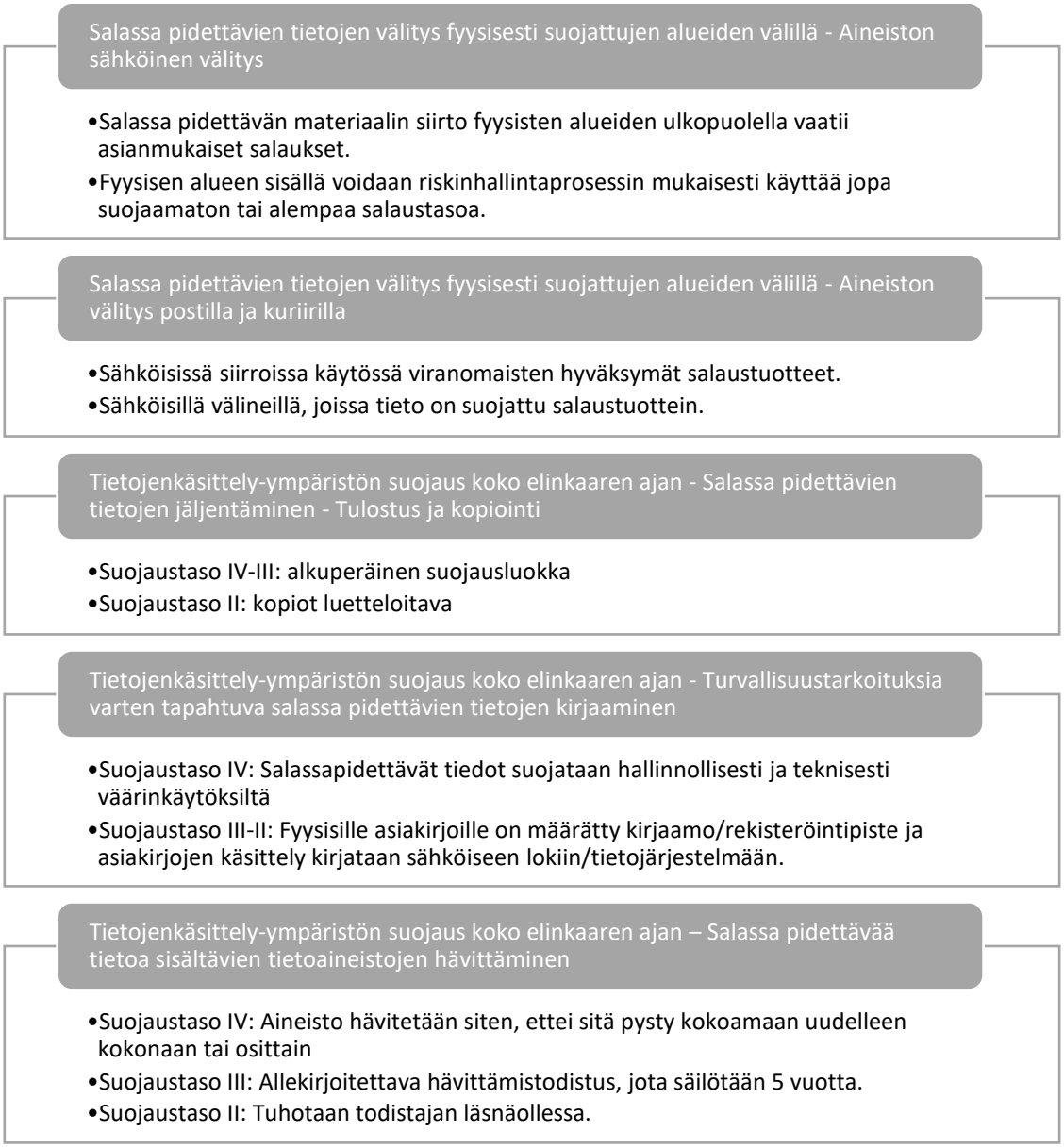
Kuva 18. Katakri 2015 tietojärjestelmäturvallisuus (Puolustusministeriö 2015: 38–52).

4.4.3 Tietoaineistoturvallisuus

Tietoaineistoturvallisuus kaukokäyttöjärjestelmässä tarkoittaa verkosta saatua tilatietoa, häiriöraportteja ja mittauksia, mutta se voi käsittää valvomossa myös muita asiakirjoja, kuten varautumissuunnitelmia, luottamuksellisia asettelutietoja tai henkilöstötietoja. Verkosta saatu tilatieto on verkonvalvonnan kannalta tärkeää ja sen tulee olla luotettavaa ja eheää. XCure Solutions Oy:n vuonna 2015 tehdystä raportissa ilmeni, että tiedon elinkaaren hallinnassa on energiasektorilla vielä tehtävää ja nimenomaan oikeuksissa kuka saa jakaa, muokata, arkistoida tai hyödyntää tietoa ja miten tiedon käytönhallintaan on parannettavaa (Immonen 2015: 4–5).

Katakrissa (kts. kuva 19) on suojaustasosta riippuen vaatimuksia tiedon elinkaarelle ja miten tiedon siirron tai siirtomedian kanssa tulee toimia. Kaikkiin Katakrin kohtiin ei löydy vastinetta ISO/IEC 27002 -standardista, mutta salatun tiedon siirtoon ja laitteiston ja tiedon turvalliseen poistamiseen liittyvät hallintakeinot ovat saatavilla. Tämän lisäksi tietoaineistoturvallisuusvaatimuksia ovat tietojen luokittelu, merkintä ja tietoihin pääsyn rajoittaminen. (ISO/IEC 27002 2013: 15–18, 25, 37, 50–53.)

Tietoaineistoturvallisuus koskettaa siis sekä ylläpitäjää että käytönvalvojaa siinä määrin kuin he käsittelevät yhtiön tietoturvapolitiikassa määriteltyjä luottamuksellisia tai arkaluonteisia tietoja. Mikäli tällaisista tiedoista tehdään kopioita, tulee niistä huolehtia asianmukaisesti ja säilyttää niitä suojatuissa tiloissa. Kaukokäyttöjärjestelmän kannalta voidaan tärkeänä tietoaineistona pitää myös etänä asetettavia suojausasetteluita tai muita vastaavia laitteiston konfigurointiasetteluita, jotka saattaisivat väärissä käsissä johtaa järjestelmän tietoturvariskin lisääntymiseen. Tällaisten asetteluiden siirtämisessä tulee käyttää riittävän salattua tai eriytettyä tiedonsiirtoväylää tai siihen soveltuvaa suojattua siirtomediaa. Ylläpitäjän vastuulla on myös tiedon elinkaaren hallinta, jossa olennaisena osana on pääsyn rajoittaminen ja siirrettävien tiedonsiirtomedioiden käytön ohjeistus ja lopuksi tiedon turvallinen tuhoaminen.



Kuva 19. Katakri 2015 tietoaineistoturvallisuus (Puolustusministeriö 2015: 53–59).

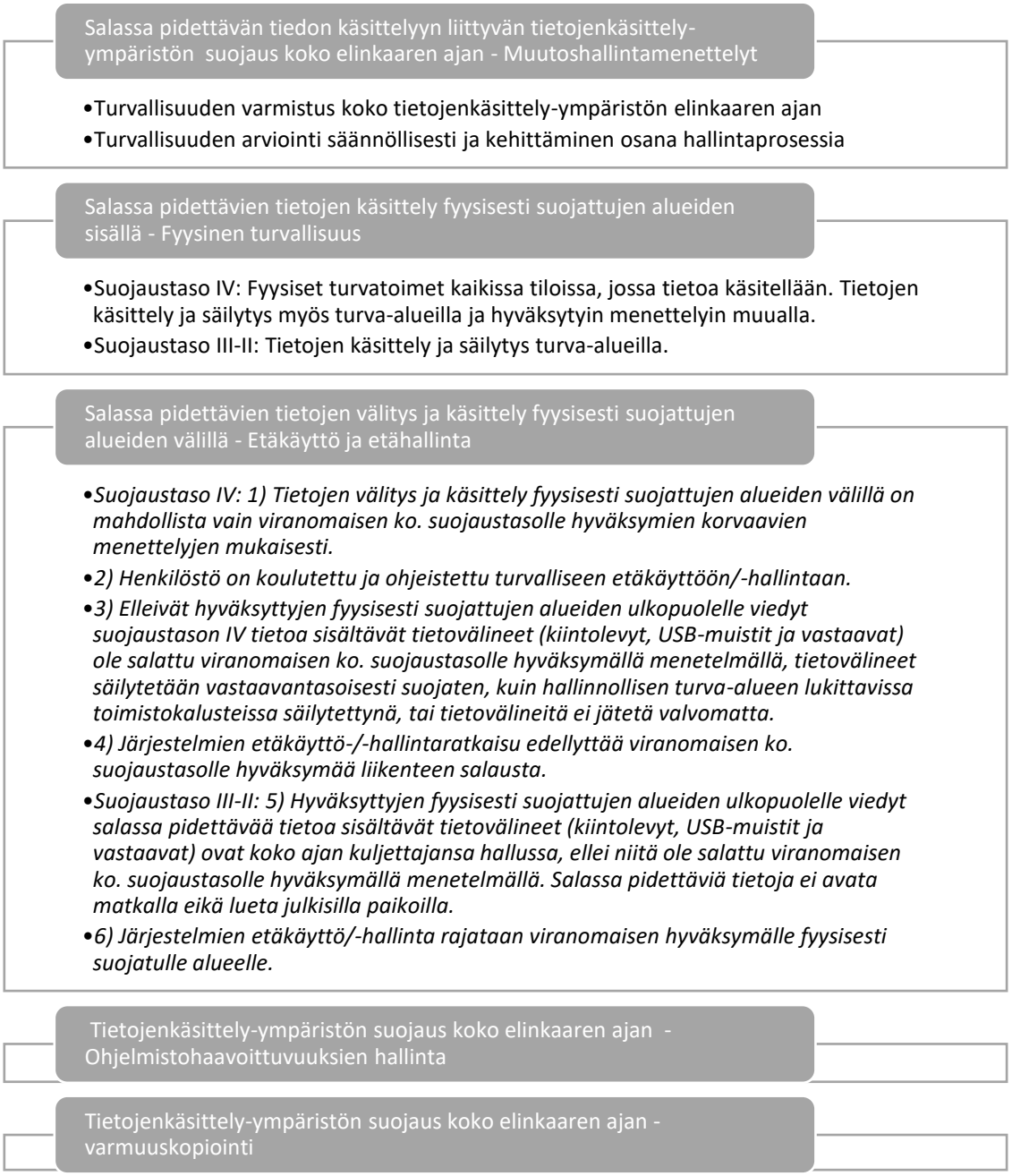
4.4.4 Käyttöturvallisuus

Kaukokäyttöjärjestelmän käyttöturvallisuudella tarkoitetaan käytön aikaista turvallisuutta ja siihen vaikutetaan tuki-, huolto- ja ylläpitotoimenpiteillä. Tämän lisäksi alueeseen kuuluvat käyttöympäristön laajennukset, kuten etäkäytöt ja prosessinhallinta. Käyttöturvallisuus tukee tietoliikenne-, laitteisto- ja ohjelmistoturvallisuutta. Renecon tutkimuksen mukaan jo lähes kaikilla yhtiöillä oli vuonna 2013 mahdollisuudet kaukokäyttöjär-

jestelmän etäkäyttöihin, mutta tutkimuksessa todettiin myös tämän lisäävän huomattavasti tietoturvariskiä (Tervo 2013: 30). Pienestä otannasta huolimatta sähköpostikyselystä, jonka suoritin syksyllä 2016, käy ilmi, että etäkäyttöjen tietoturvallisuus otetaan vakavasti, mutta jälleen laajan toimijoiden kirjon vuoksi on todettava, että kaikilla toimijoilla ei ole välttämättä rahaa tai resursseja panostaa myöskään tähän alueeseen riittävästi (Sähköpostikysely 2016).

Katakrissa (kts. kuva 20) käyttöturvallisuus painottuu pitkälti salassa pidettävien tietojen käsittelyyn, mikä voidaan rinnastaa sähköverkon operointiin. Katakrissa on myös mukana laitteiston elinkaaren kestävä haavoittuvuuksien hallinta ja varmuuskopiointi, jotka olisivat voineet olla myös laitteisto- ja ohjelmistoturvallisuuden osa-alueessa. Merkittävänä kohtana on myös Katakrissa mukana oleva etäkäyttö ja -hallinta, jolle asetetaan kovat vaatimukset suojaustasosta riippuen. ISO/IEC 27002 vastaa etätyö- ja operointivaatimuksiin tietoturvallisuuden organisoinnilla mobiililaite- ja etätyökohdassa, mikä käytännössä tarkoittaa laitteiden huomioimista tietoturvapolitiikassa ja niiden riskien tunnistamista. Operoinnin ja käytettävien tietovälineiden tietoturvan osalta henkilöstö tulee kouluttaa ja ohjeistaa. Operointiympäristön tulee olla turvallinen ja laitteistot tulee suojata haittaohjelmia ja teknisiä haavoittuvuuksia vastaan. (ISO/IEC 27002 2013: 6–8, 11–12, 17–19, 30–38.)

Ylläpitäjän osalta käyttöturvallisuus tarkoittaa järjestelmien, laitteiden ja tietoliikenneyhteyksien ylläpito-, hallinta- ja valvontatoimia, jotka ovat osaltaan myös laite- ja ohjelmistoturvallisuutta. Samaan kategoriaan kuuluu myös säännöllinen varmuuskopioiden ylläpitäminen. Ylläpitäjä toteuttaa ohjeistuksen järjestelmän tietoturvalliseen operointiin ja huolehtii, että etäyhteydet ovat riittävän vahvasti salattuja. Käytönvalvojan vastuulle jää huolehtia, että kaukokäyttöjärjestelmän operointi suoritetaan ohjeistuksen mukaisesti, tietoturvallisesti sekä turvallisessa ympäristössä. Ympäristön merkitys korostuu otettaessa yhteyksiä kaukokäyttöjärjestelmään etäältä, esimerkiksi kotoa käsin. Käytönvalvoja on myös velvollinen raportoimaan ja toimimaan ohjeiden mukaisesti, mikäli havaitsee poikkeamia järjestelmässä.



Kuva 20. Katakri 2015 käyttöturvallisuus (Puolustusministeriö 2015: 60–65).

4.5 Johtopäätökset

Verkostoautomaatiojärjestelmien tietoturvan kehittyminen on jo vuosia ollut positiivista. Jotta positiivinen kehitys jatkuisi, tulee Huoltovarmuuskeskuksen vaatimuksia,

Katakri-auditointityökalua ja kansainvälisiä standardeja, kuten ISO/IEC 27000 -standardiperhettä, käyttää apuna tietoturvan toteuttamiseen sekä jatkuvaan parantamiseen. Painetta kaukokäyttöjärjestelmän tietoturvalliseen suojaamiseen tulee kansallisella tasolla lainsäädännöstä ja EU:n tasolla tuoreen verkko- ja tietoturvadirektiivin osalta.

Kaukokäyttöjärjestelmän ja yleisesti tietoturvan osalta tärkein tietoturvan osa-alue on hallinnollinen tietoturva, jossa havaittiin puutteita tiedottamisen ja tietoturvapolitiikan suhteen. Yhtiön johto päättää yhtiössä toteutettavan tietoturvapolitiikan siten, että se vastaa alalle asetettuja vaatimuksia ja yhtiön strategiaa. Tietoturvapolitiikassa tulee huomioida erityisesti suojattavat kohteet, määrittää tietoturvavastuut ja turvallisuusdokumentit. Tietoturvan toteuttamiseen ja jatkuvan parantamisen prosessiin puolestaan tulee varata riittävät resurssit. Tietoturvan kehittämisessä on hyvä käyttää suunnittele-toteuta-arvioi-toimi -mallia ja puolestaan riskienhallintaan ISO/IEC 27005 riskienhallintakaaviota. Lisäksi kaukokäyttöjärjestelmien etäkäyttömahdollisuuksista johtuen tulee tietoturvapolitiikassa huomioida myös etäkäytön vaatimukset ja ohjeistukset. Tietoturvapolitiikan toteutuminen on mahdollista vain, jos siitä tiedotetaan kaukokäyttöjärjestelmän käytönvalvojia ja ylläpitäjiä sekä järjestetään säännöllisiä koulutustilaisuuksia.

Kaukokäyttöjärjestelmän operointiin liittyen käytönvalvojan toimet järjestelmässä ovat vähäisiä, mutta niiden tietoturvallinen toteutus on tärkeässä roolissa, että laadukas sähkönjakelu voidaan taata yhteiskunnallisesti. Käytönvalvojan tulee sitoutua noudattamaan yhtiön asettamaa tietoturvapolitiikka ja kehittää tarvittaessa itseään, että pystyy takaamaan turvallisen operoinnin. Mikäli käytönvalvoja ottaa etäyhteyksiä järjestelmään muualta kuin yhtiön suojatusta valvomosta tulee hänen varmistaa turvallinen toimintaympäristö sekä toteuttaa yhtiön etäkäyttöohjeistuksia. Järjestelmän turvalliseen operointiin tulee yhtiöllä olla selkeä ohjeistus ja toimintaohjeet poikkeustilan varalle.

Kaukokäyttöjärjestelmän ylläpitäjä puolestaan vastaa tietoturvavastuiden mukaisesti järjestelmän hallinnasta, ylläpidosta ja muokkauksesta. Ylläpitäjä on käytönvalvojan mukaisesti vastuussa osaamisensa kehittämisestä sekä yhtiön tietoturvan toteuttamisesta kaikissa toimissaan. Ylläpitäjälle tulee tarjota koulutusta, jotta yhtiön tietoturvan toteuttamiseksi tarvittava osaaminen pysyy ajan tasalla nopeasti muuttuvassa ympäristössä.

Ylläpitäjä on asetettujen tietoturvavastuiden perusteella velvollinen toteuttamaan ja kehittämään kaukokäyttöjärjestelmän tietoturvaa. Mikäli ylläpitäjä ulkoistaa järjestelmän ylläpidon osakokonaisuuksia on hänen velvollisuus tietää miten ulkopuoliset toimittajat toteuttavat yhtiön asettamat tietoturvallisuusvaatimukset.

Tekninen tietoturva on ensi sijassa ylläpitäjän vastuulla ja tärkeä osa kaukokäyttöjärjestelmän ylläpitoa. Tekniseen tietoturvaan kuuluvat kaukokäyttöjärjestelmän laitteiston, ohjelmistojen, tietoaineistojen ja tietoliikenneyhteyksien valvonta ja hallinta. Ylläpitäjä vastaa, että laitteisto ja käytettävät ohjelmistot ovat kovennettuja, varmistettuja ja suojattuja tietoturvauhkia vastaa. Tämä tarkoittaa, että laitteisto ja ohjelmistot ovat tietoturvallisesti asetellut, mahdollisuuksien mukaan ajantasaisesti päivitetyt ja niistä on saatavilla tarvittaessa ajantasaiset varmuuskopiot järjestelmän palauttamista varten. Tietoliikenneyhteydet ovat varmistettuja ja suojattuja, siten kuin tietoturvapolitiikassa käytettävän siirtotien osalta on määrätty. Ohjelmien ja palomuurin osalta olennaista on vähimpien oikeuksien periaate, joka helpottaa tärkeän liikenteen ja prosessien seurantaa. Käyttöturvallisuuden varmistamiseksi ylläpitäjän tulee huolehtia järjestelmän turvallisen operoinnin ohjeistuksesta, jossa otetaan huomioon tietoaineistoa koskevat menettelyt sekä toiminta järjestelmän poikkeustilanteissa. Erityisen tärkeä on ohjeistus järjestelmän palauttamiselle siltä varalta, että siihen päästään hyökkäämään.

Henkilöstöturvallisuus saattaa yhtiöstä riippuen kuulua myös ylläpitäjälle. Tämä tarkoittaa, että ylläpitäjän vastuulla on henkilöiden tunnukset ja niihin liittyvät oikeudet. Ylläpitäjän tulee huomioida työsuhteen elinkaari sekä turvallisuusselvitysmenettely antaessaan oikeuksia arkaluontoisen tiedon tai järjestelmäosien käyttöön.

Kun aikaisemmista tutkimuksista esiin nousseet tietoturvapuutteet korjataan tässä diplomityössä esitetyillä toimilla, voidaan kaukokäyttöjärjestelmän tietoturvallisessa operoinnissa ja ylläpidossa päästä seuraavalle tasolle. Tietoturvauhkien ja tietoturvaympäristön jatkuvasta muutoksesta johtuen tietoturva ei kuitenkaan koskaan voi saavuttaa täydellistä tasoa. Sen sijaan tietoturvassa voidaan saavuttaa riittävä tai vaadittava taso käyttäen hyväksi esiteltyjä tietoturvaohjeistuksia ja -standardeja.

5 YHTEENVETO

Diplomityön tarkoituksena oli tarkastella aiemmista tutkimustuloksista ja sähköpostikyselystä esiin tulevia tietoturvapuutteita sähköverkon kaukokäyttöjärjestelmän operoinnissa ja ylläpidossa. Näihin havaittuihin puutteisiin pyrittiin löytämään tietoturvavaatimuksien vertailun kautta tietoturvalliset toimintamallit, jotka parantavat ja mahdollistavat kaukokäyttöjärjestelmän tietoturvallisen operoinnin ja ylläpidon. Jotta voidaan ymmärtää sähköverkon kaukokäyttöjärjestelmässä tehtävät toimet, tulee ymmärtää kokonaisuus, johon kaukokäyttöjärjestelmä on kytköksissä. Tietoturvan toteutumiseksi kaukokäyttöjärjestelmässä puolestaan vaaditaan tietämystä tietoturvasta, tietoturvavaatimuksista ja -uhkista liittyen järjestelmään.

Kaukokäyttöjärjestelmällä ohjataan sähköverkkoa, joka koostuu useista erilaisista toimilaitteista ja laitteet sijoittuvat verkon eri osiin. Kaukokäyttöjärjestelmässä on useita erilaisia tiedonsiirtoyhteyksiä kaukokäytettäville laitteille. Tiedonsiirrolle on asetettu erilaisia vaatimuksia, kuten aikakriittisyys ja luotettavuus, minkä vuoksi tärkeät yhteydet tulee kahdentaa. Kaukokäyttöjärjestelmä-kokonaisuuksia voidaan kutsua myös käytönvalvontajärjestelmiksi. Käytönvalvontaohjelmisto sisältää käyttöliittymän, joka tarjoaa käytönvalvojalle verkon reaaliaikaisen tilan, hälytykset, lukitukset ja muun tarpeellisen verkkotiedon. Ylläpitäjälle ohjelmisto puolestaan tarjoaa rakennustyökalut, tietoliikenne diagnostiikan, käyttäjätunnistukset ja -oikeutukset.

Tietoturva tarkoittaa omaisuuden ja toimintojen suojaamista ja niihin kohdistuvien riskien hallintaa normaali- ja poikkeusoloissa. Tietoturva voidaan jakaa seuraavasti osiin: hallinnollinen turvallisuus, henkilöstöturvallisuus, fyysinen turvallisuus, tietoliikenneturvallisuus, laitteistoturvallisuus, ohjelmistoturvallisuus, tietoaineistoturvallisuus ja käyttöturvallisuus. Tietoturvan toteuttaminen tulee usein pakolliseksi vaatimusten kautta. Vaatimukset voivat puolestaan tulla kansallisesti lainsäädännöstä tai kansainvälisesti EU:n direktiiveistä, standardeista tai ohjeistuksista.

Sähköverkon kaukokäyttöjärjestelmää koskee kansallisesti sähkömarkkinalaki ja Huoltovarmuuskeskus valvoo, että huoltovarmuus toteutuu. Kansainvälisiä vaatimuksia ovat puolestaan EU:n uusi verkko- ja tietoturvadirektiivi ja EU:n elintärkeän infrastruktuurin suojaukseen kohdistuva direktiivi. Vaatimuksena voidaan myös nähdä kansallisesti energia-alan tietoturva-auditoinneissa käytetyt Katakri-kriteeristö, ISO/IEC 27001 ja 27002 -standardit ja Vahti-ohjeisto. Kaukokäyttöjärjestelmän tietoturvan toteuttamiseen on paljon ohjeita ja standardeja, mutta EU:n verkko- ja tietoturvadirektiivin vaatimuksia silmällä pitäen ISO/IEC 27000 -standardiperhe on näistä sopivin toteutettavaksi.

Vuoden 2015 yleisimmistä tieturvauhista useimmat sopivat myös kaukokäyttöjärjestelmän uhiksi. Näitä uhkia ovat päivittämätön ohjelmisto, tietojen kalastelu, palvelunestohyökkäys ja henkilöstön osaamattomuus. Pahimmillaan näiden uhkien kautta voidaan luoda kyberhyökkäys, joka lamaannuttaa sähkönjakelun. Toimijat hyökkäysten takana vaihtelevat, mutta laajuudesta ja toimintatavoista voidaan päätellä hyökkäyksen takana oleva taho.

Jotta sähkönjakelu pysyy vakaana ja ohjaus käytönvalvojien käsissä, tulee kaukokäyttöjärjestelmää operoida ja ylläpitää tietoturvallisesti. Tietoturvallisuudessa lähtökohtana toimii hallinnollisen tietoturvan tietoturvapolitiikka. Sen havaitut puutteet tiedottamisessa ja vastuun jaossa on äärimmäisen tärkeä korjata, jotta tietoturvapolitiikkaa toteutuu yhtiön toiminnassa. Korjausliike tehdään paremmalla koulutuksella ja tiedottamisella. Tämän lisäksi tietoturvaa tulee kehittää jatkuvan parantamisen prosessissa.

Henkilöstöturvallisuuden osa-alueella on aiempien tutkimusten mukaan käytetty yhteistä salasanaa, mutta tämä tietoturvapuute on kuitenkin jo tiedostetusti korjattu. Tietoturvan kehittäminen tällä alueella koostuu eteenpäin viedystä käyttäjien hallinnasta, jossa huomioidaan työsuhteen elinkaari. Fyysisen turvallisuuden osalta puolestaan puutteet ilmenivät uudenlaisten riskien, kuten sabotaasin, terrorismin ja tiedustelun, huomiotta jättämisellä. Fyysisessä turvallisuudessa rajoitetaan pääsyä kulunvalvonnalla ja suojataan arvokas tieto fyysisesti ja teknisesti riittävällä suojauksella.

Tekniseen tietoturvaan kuuluvat tietoliikenneturvallisuus, laitteisto- ja ohjelmistoturvallisuus, tietoaineistoturvallisuus sekä käyttöturvallisuus. Tutkimusten perusteella teknisen turvallisuuden lähtötaso oli korkea ja tämän vuoksi puutteita esiintyi lähinnä laitteisto-, ohjelmisto- ja tietoaineistoturvallisuudessa. Puutteet olivat uusien laitteiden koventamisessa ja tietojen elinkaarihallinnassa. Kehitys tarpeita ovat siis koventaminen niin uusissa kuin vanhemmissa laitteissa aina tietoliikenneyhteyksiä myöden ja samoin käyttäjä oikeuksissa ja prosesseissa vähimpien oikeuksien periaate.

Käytönvalvojan operointitoimet kaukokäyttöjärjestelmässä ovat rajoittuneet valvomiseen, ohjaamiseen ja raportointiin. Toimien toteuttaminen tulee tapahtua tietoturvallisesti ohjeiden ja tietoturvapolitiikan mukaisesti, jotta sähkönjakelu ei häiriinny. Kaukokäyttöjärjestelmän operointipaikan tulee olla turvallinen, oli se sitten valvomo tai etätyöpiste.

Kaukokäyttöjärjestelmän ylläpitäjä on tietoturvavastuiden mukaisesti velvollinen huolehtimaan järjestelmän hallinnasta, ylläpidosta ja muokkauksesta. Ylläpitäjällä tulee olla riittävä osaaminen, että hän voi toteuttaa teknistä tietoturvaa, joka kattaa laitteiden päivityksen, kovennukset, asettelut ja varmuuskopioinnin. Tämän lisäksi ylläpitäjän vastuulla on ohjeistaa käytönvalvojien toimia normaali- ja poikkeustilanteissa.

Mikäli tutkimuksissa ilmenneet puutteet korjataan esitetyillä toimilla, voidaan kaukokäyttöjärjestelmän tietoturvassa nousta seuraavalle tasolle. Tietoturvaympäristö kuitenkin muuttuu koko ajan ja sen vuoksi koskaan ei saavuteta täydellistä tasoa, mutta riittävä tai vaadittu taso voidaan saavuttaa ohjeistuksien avulla.

Työssä käsiteltiin sähköverkkoa ja kaukokäyttöjärjestelmän liittymistä osaksi sitä. Lisäksi käytiin läpi tietoturva ja kaukokäyttöjärjestelmän tietoturvaan tähtäävät vaatimukset, ohjeistukset ja standardit sekä tietoturvauhat. Tältä teoriapohjalta syvennyttiin tutkimuksissa esiin tulleisiin puutteisiin, joille haettiin vaatimuksia ja ohjeistuksia vertaillen Katakria ja ISO/IEC 27000 -standardiperheen standardeja. Vertailun kautta syntyneet tietoturvalliset toimintamallit ovat odotettu lopputulos.

LÄHDELUETTELO

ABB Oy (2000). *Teknisiä tietoja ja taulukoita*. 10. painos. Vaasa: Ykkös-Offset Oy. ISBN 951-99366-0-2.

ABB Oy (2014). *MicroSCADA Pro for network control and distribution management*. [online]. [30.4.2016]. Saatavissa: https://library.e.abb.com/public/635ed4e2b4b8fb4fc1257d65002b8970/1MRS756253_E_en_MicroSCADA_Pro_for_network_control_and_distribution_management.pdf

ABB Oy (2016). *Toward a smarter grid ABB's Vision for the Power System of the Future*. [online]. [22.3.2016]. Saatavissa: http://www02.abb.com/db/db0003/db002698.nsf/0/36cc9a21a024dc02c125761d0050b4fa/$file/Toward_a_smarter_grid_Jul+09.pdf

Ahonen, Pasi (2010). *TITAN-käsikirja*. *VTT:n päätuloksia Tekesin Turvallisuusohjelman TITAN-projektissa* [online]. [3.4.2016]. Helsinki: Edita Prima Oy. ISBN 978-951-38-7642-5. Saatavissa: http://www.vtt.fi/inf/pdf/tiedotteet/2010/t2545.pdf

Andreasson, Ari & Koivisto Juha (2013). *Tietoturvaa toteuttamassa*. Tallinna: AS Pakett. ISBN 978-951-885-334-6.

Council Directive 2008/114/EC. [online]. [22.5.2016]. Saatavissa: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32008L0114&from=EN.

Delgado-Gomes, V., J.F. Martins, C. Lima & P. Nicolae Borza (2015). Smart grid security issues. *International Conference on Compatibility and Power Electronics (CPE)*, 2015 9th, pp.534-538, 24-26 June 2015

Directive (EU) 2016/1148. [online]. [16.9.2016]. Saatavissa: http://data.europa.eu/eli/dir/2016/1148/oj.

Elovaara, Jarmo & Haarla Liisa (2011). *Sähköverkot 1. Järjestelmätekniikka ja sähköverkon laskenta*. 1. painos. Helsinki: Gaudeamus Helsinki University Press Oy Yliopistokustannus. ISBN 978-951-672-360-3.

Energiateollisuus (2015a). *Sähköverkkoyhtiöt* [online]. [30.11.2015] Saatavissa: http://energia.fi/sahkomarkkinat/sahkoverkko/sahkoverkkoyhtiot

Energiavirasto (2016a). *Sähköverkkotoiminnan tunnusluvut vuodelta 2014* [online]. [14.9.2016] Saatavissa: https://www.energiavirasto.fi/documents/10191/0/jvh+tekniset+tunnusluvut+2014.xlsx/40320fba-025f-4c87-8ad5-1f3641f72dd2

Energiavirasto (2016b). *Sähköverkon haltijat* [online]. [14.9.2016] Saatavissa: https://www.energiavirasto.fi/sahkoverkon-haltijat

ENISA (2011a). *Protecting Industrial Control Systems. Recommendations for Europe and Member States* [online]. [11.6.2016]. Saatavissa: https://www.enisa.europa.eu/publications/protecting-industrial-control-systems.-recommendations-for-europe-and-member-states

ENISA (2011b). *Protecting Industrial Control Systems. Annex I: Desktop research Result* [online]. [22.5.2016]. Saatavissa: https://www.enisa.europa.eu/publications/annex-i

ENISA (2011c). *Protecting Industrial Control Systems. Annex III: ICS Security Related Standards, Guidelines and Policy Documents* [online]. [11.6.2016]. Saatavissa: https://www.enisa.europa.eu/publications/annex-iii

ENISA (2013). *Window of exposure.. a real problem for SCADA systems?* [online]. [8.9.2016]. Saatavissa: https://www.enisa.europa.eu/publications/window-of-exposure-a-real-problem-for-scada-systems

ENISA (2016a). *About ENISA* [online]. [11.5.2016]. Saatavissa: https://www.enisa.europa.eu/about-enisa

ENISA (2016b). *ENISA Threat Landscape 2015* [online]. [27.7.2016]. Saatavissa: https://www.enisa.europa.eu/publications/etl2015

European Commission (2016). *The Directive on security of network and information systems (NIS Directive)* [online]. [16.9.2016]. Saatavissa: https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive#Article

FINGRID (2016). *Pohjoismainen voimajärjestelmä ja liitynnät muihin järjestelmiin.* [online]. [5.6.2016]. Saatavissa: http://www.fingrid.fi/fi/voimajarjestelma/voimaj%C3%A4rjestelm%C3%A4/Pohjoismainen%20voimaj%C3%A4rjestelm%C3%A4%20ja%20liitynn%C3%A4t%20muihin%20j%C3%A4rjestelmiin/Sivut/default.aspx

Huoltovarmuuskeskus (2015). *KYBERTURVALLISUUDEN KEHITTÄMINEN JA JALKAUTTAMINEN TEOLLISUUTEEN VUONNA 2014. KYBER-TEO 2014 - hankkeen tuloksia* [online]. [3.4.2016]. Oulu: Erwko. ISBN 978-952-5608-30-4. Saatavissa: http://www.huoltovarmuus.fi/static/pdf/839.pdf.

ICS-CERT (2016). *Recommended Practices* [online]. [13.6.2016]. Saatavissa: https://ics-cert.us-cert.gov/Recommended-Practices

IEC (2016). *Smart Grid. Core IEC Standards* [online]. [16.6.2016]. Saatavissa: http://www.iec.ch/smartgrid/standards/

IEC/TS 62351-5 (2009). *Power systems management and associated information exchange – Data and communications security*. Part 5: Security for IEC 60870-5 and derivatives. 1. ed. Sveitsi: International Electrotechnical Commission.

IEC/TS 62351-6 (2007). *Power systems management and associated information exchange – Data and communications security*. *Part 6: Security for IEC 61850*. 1. ed. Sveitsi: International Electrotechnical Commission.

Immonen, Aapo (2015). *Kyberturvallisuuden tilannekuva energia-alalla* [online]. [5.6.2016]. XCure Solutions Oy. Saatavissa: http://www.huoltovarmuus.fi/static/pdf/877.pdf

ISO/IEC 27001 (2013). *Information technology — Security techniques — Information security management systems — Requirements*. 2. ed. Sveitsi: International Electrotechnical Commission.

ISO/IEC 27002 (2013). *Information technology — Security techniques — Code of practice for information security controls*. 2. ed. Sveitsi: International Electrotechnical Commission.

ISO/IEC TR 27019 (2013). *Information technology — Security techniques — Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry*. 1. ed. Sveitsi: International Electrotechnical Commission.

Isomäki, Osmo (2016). Service Engineer, ABB Oy. Haastattelu, Vaasa 29.4.2016.

Jaspers, Peter (2014). *The Finnish Smart Grid. An overview of renewable energies and smart grid technologies in Finland* [online]. [28.4.2016]. Saatavissa: http://www.handelskammer.se/sites/www.handelskammer.se/files/peter_jaspers_the_finnish_smart_grid.pdf

Karvi, Timo (2010). *Tietoturvan perusteet. Luku1: Yleistä tietoturvasta* [online]. [4.6.2016]. Saatavissa: https://www.cs.helsinki.fi/u/karvi /perusteet-luku1-bea_10.pdf

Korpinen, Leena (2015). *Sähkövoimatekniikka. 5. Sähköverkon automaatio ja suojaus* [online]. [22.12.2015]. Saatavissa: http://www.leenakorpinen.fi/archive/svt_opus /5sahkoverkon_automaatio_ja_suojaus.pdf

Kostopoulos, George K. (2013). *Cyberspace and Cybersecurity*. Boca Raton: CRC Press. ISBN 978-1-4665-0133-1.

Kuschewsky, Monika (2015). *What You Need to Know About Germany's Cybersecurity Law* [online]. [12.6.2016]. Saatavissa: https://www.insideprivacy.com/data-security /what-you-need-to-know-about-germanys-cybersecurity-law/

Lakervi, Erkki & Partanen Jarmo (2008). *Sähkönjakelutekniikka*. 2. painos. Helsinki:Gaudeamus Helsinki University Press Oy Yliopistokustannus. ISBN 978-951-672-359-7.

Laki julkisen hallinnon turvallisuusverkkotoiminnasta 10/2015. [online]. [5.6.2016]. Saatavissa: http://www.finlex.fi/fi/laki/ajantasa/2015/20150010

Martikainen, Jari (2005). Käytönvalvontajärjestelmä. *Fingrid* 2005:1, 22–23.

Myllylä, T. (2014). *Sähköverkkojen kyberturvallisuus*. Aalto-yliopisto. Sähkötekniikan korkeakoulu. Diplomityö.

NERC (2016). *Project 2014-02 Critical Infrastructure Protection Standards Version 5 Revisions* [online]. [12.5.2016]. Saatavissa: http://www.nerc.com/pa/Stand/Pages /Project-2014-XX-Critical-Infrastructure-Protection-Version-5-Revisions.aspx

Paneelikeskustelu (2016). *Suomi kyberturvallisuuden kärkimaita 2016?*, Aalto yliopisto. [video]. [9.5.2016]. Saatavissa: https://www.youtube.com /watch?v=X59eoIL-KZY

Puolustusministeriö (2015). *Katakri 2015. Tietoturvallisuuden auditointityökalu viranomaisille*. [online]. [26.9.2016]. Helsinki: Puolustusministeriö. ISBN 978-951-25-2682-6. Saatavissa: http://formin-origin.finland.fi/public /download.aspx?ID=144915&GUID={A909E480-1110-4390-95F3-52E9FE7D78CE}.

Salin, Marianna (2015). Verkkoremontti fiksusti. *power* [online] 15:1, [20.3.2016], 10-13. Saatavissa: https://library.e.abb.com/public /e9ac4c7bb4f10aafc1257dd90041ce74/abb_power_1_2015.pdf

Sisäministeriö (2016). *Suomen kansallinen riskiarvio 2015*. [online]. [20.2.2016]. Helsinki: Sisäministeriö. ISBN 978-952-324-059-9. Saatavissa: http://www.intermin.fi/julkaisu/ 032016?docID=65646.

Suomen Standardisoimisliitto SFS ry (2015). *Informaatioteknologia. Turvallisuus. Tietoturvallisuuden hallintajärjestelmät. ISO/IEC 27000 -standardiperhe* [online]. [14.6.2016]. Saatavissa: http://www.sfsedu.fi/files/121/ISO-27000.ppt

Sähkömarkkinalaki 588/2013. [online]. [19.5.2016]. Saatavissa: http://www.finlex.fi /fi/laki/alkup/2013/20130588.

Sähköpostikysely (2016). Kysely tietoturvan tilasta diplomityöhön "Kaukokäyttöjärjestelmän tietoturvallinen operointi ja ylläpito”. 15.09.2016.

Tervo, Jouko (2012). *Moderni sähköverkko vaatii luotettavaa ja vikasietoista tiedonsiirtoa* [online]. [30.4.2016]. Saatavissa: https://konsulttitoimistoreneco.wordpress.com/2012/03/05 /moderni-sahkoverkko-vaatii-luotettavaa-ja-vikasietoista-tiedonsiirtoa/

Tervo, Jouko (2013). *Verkostoautomaatiojärjestelmien tietoturva* [online]. [9.2.2016]. Saatavissa: https://konsulttitoimistoreneco.files.wordpress.com/2013/10 /verkostoautomaatiojarjestelmien-tietoturva-2013-09-27.pdf

Valtari, Jani (2013). Sähköasemien automaation keskittäminen lisää luotettavuutta. *Sähköala* 2013:8, 48–49.

Valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa 681/2010. [online]. [19.5.2016]. Saatavissa: http://www.finlex.fi/fi/laki/ajantasa/2010/20100681.

Valtiovarainministeriö (2004). *Valtionhallinnon keskeisten tietojärjestelmien turvaaminen*. Helsinki: Edita Prima Oy. ISBN 951-804-468-6. Saatavissa: <URL: https://www.vahtiohje.fi/c/document_library/get_file?uuid=35e1f7af-9ecd-4787-8cbf-a685213cd4f8&groupId=10128&groupId=10229>.

Valtiovarainministeriö (2008a). *Tärkein tekijä on ihminen - henkilöstöturvallisuus osana tietoturvallisuutta*. Helsinki: Edita Prima Oy. ISBN 978-951-804-799-8. Saatavissa: <URL: https://www.vahtiohje.fi/c/document_library /get_file?uuid=af5614a4-fa44-482c-98860af9e6a13929&groupId=10128&groupId=10229>.

Valtiovarainministeriö (2008b). *Valtionhallinnon tietoturvasanasto*. Helsinki: Edita Prima Oy. ISBN 978-951-804-889-6. Saatavissa: <URL: https://www.vahtiohje.fi /c/document_library/get_file?uuid=7e2220f1-cc93-4ba6-8c70-a67869c526cc&groupId=10128&groupId=10229>.

Viestintävirasto (2016a). *Kyberturvallisuuskeskuksen tietoturvapalvelut* [online]. [11.5.2016]. Saatavissa: https://www.viestintavirasto.fi/kyberturvallisuus /viestintavirastontietoturvapalvelut.html

Viestintävirasto (2016b). *Viestintäviraston Kyberturvallisuuskeskuksen vuosiraportti 2015* [online]. [24.7.2016]. Saatavissa: https://www.viestintavirasto.fi/attachments /tietoturva/Viestintaviraston_Kyberturvallisuuskeskuksen_vuosiraportti_2015.pdf

Yang, Y, K. McLaughlin, T. Littler, S. Sezer, Eul Gyu Im, Z. Q. Yao, B. Pranggono & H. F. Wang (2012). Man-in-the-middle attack test-bed investigating cyber-security vulnerabilities in Smart Grid SCADA systems. *2012 International Conference on Sustainable Power Generation and Supply (SUPERGEN 2012)*, Hangzhou, 2012, pp. 1-8.

Zetter, Kim (2016). *Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid* [online]. [19.8.2016]. Saatavissa: https://www.wired.com/2016/03 /inside-cunning-unprecedented-hack-ukraines-power-grid/