Informaatioteknologian tiedekunnan julkaisuja
No. 57/2018

Jouni Pöyhönen

Kyberturvallisuuden hallintajärjestelmän luominen energiayhtiön lämpövoimalaitokseen

JYVÄSKYLÄN YLIOPISTO

Informaatioteknologian tiedekunnan julkaisuja
No. 57/2018

Editor: Pekka Neittaanmäki
Covers: Petri Vähäkainu ja Matti Savonen

ISBN 978-951-39-7545-6 (verkkoj.)
ISSN 2323-5004

Jyväskylä 2018

Kyberturvallisuuden hallintajärjestelmän luominen energiayhtiön lämpövoimalaitokseen

Creation of a cyber-security management system for electricity production in combined heat and power plant

Jyväskylän yliopisto
Informaatioteknologian tiedekunta
Tietotekniikan laitos

CIRP-raportti
2.painos
2016

Jouni Pöyhönen

JYVÄSKYLÄN YLIOPISTO

TIIVISTELMÄ

Modernin yhteiskunnan toiminta perustuu useiden kriittisten infrastruktuurien yhteistoimintaan. Niiden keskinäinen toimintakyky riippuu yhä enemmän luotettavista sähköisistä järjestelmistä, toimivista tiedonsiirtoverkostoista sekä tiedon luotettavuudesta, eheydestä ja käytettävyydestä toimintaympäristössä, jonka kyberturvallisuusriskejä digitaalisen maailman uhkakuvat jatkuvasti kasvattavat.

Suomen sähköntuotannosta lähes kolmannes tuotetaan sähkön ja lämmön yhteistuotantona lämpövoimalaitoksissa. Niiden tuotantoprosessien ohjaus tapahtuu pitkälle automatisoituja ja teknillisesti verkottuneita teollisuuden automaatiojärjestelmiä hyväksi käyttäen. Tämä tutkimusraportti käsittelee energiayhtiön lämpövoimalaitoksen tuotantoprosessin kyberturvallisuuden hallintaan sovellettavia menettelyjä hyödyntäen alan standardeja ja kotimaisia tutkimustuloksia.

Raportin keskeinen tulos on sähkön ja lämmöntuotannon kyberturvallisuuden riskitarkastelun ulottaminen tuotantoprosessin rakenteeseen sekä PDCA-ongelmanratkaisumenetelmän soveltamisen hyödyntäminen kehitettäessä siihen liittyviä kyberturvallisuuden hallintamenettelyjä. Toimenpiteiden jalkauttaminen edellyttää, että energiayhtiön johto pitää kyberturvallisuuden hallintaa strategisena tavoitteena ja viestittää sen toteuttamista strategiaa tukevalla toimintapolitiikalla.

Asiasanat: kriittinen infrastruktuuri, teollisuusautomaatio, kyberturvallisuuden hallinta, standardi

ABSTRACT

The modern society is based on a number of critical infrastructures that are dependent on reliable electricity, digital networks and the reliability, integrity and availability of sensitive data processing in an environment that is becoming more and more risky concerning cyber security treats.

Almost one third of Finnish electricity generation is produced by combined heat and power plants. Production process controls are fully automated by industrial control systems (ICS), which have networks between ICS-components and widely with other ICS-systems. This report comprises cyber security management guidelines that can be useful in order to increase security resilience in combined heat and power production process. The guidelines are based on cyber security standards and relevant research data.

The basic cyber security management concept associated with managing ICS-system structure related security risks is the main result of this report. The Plan-Do-Check-Act (PDCA) model has been used to improve the management process.

Implementing the system-related cyber security management guidelines requires that the top leaders of the company create a strategic vision and policies for the security goals and objectives for the organization.

Keywords: critical infrastructure, industrial control system (ICS), cyber security management, standard

TAULUKOT

TAULUKKO 1 Teollisuusautomaation kyberturvallisuuteen liittyviä standardeja..... 9
TAULUKKO 2 Lämpövoimalaitosprosessin kyberrakenne ja sen merkittävimmät riskit..... 17

KUVIOT

KUVIO 1. PDCA-ongelmanratkaisumenetelmä 6
KUVIO 2. Hajautettu ICS-järjestelmä (Industrial Control System) 9
KUVIO 3. ISO 27005: Riskien käsittelytoiminta 15
KUVIO 4. PDCA-ongelmanratkaisumenetelmä tutkimuskohteeseen sovellettuna 17

SISÄLLYS

1. Johdanto 1

2. Kyberturvallisuuden hallintajärjestelmän perusteet ja rakentaminen 3

3. Teollisuusautomaatiojärjestelmät kybertoimintaympäristössä 8

4. Kyberturvallisuuden hallintajärjestelmän laatiminen lämpövoimalaitosprosessiin 12

5. Yhteenveto 18

Lähteet 20

1. Johdanto

Sähköä tuotetaan Suomessa monipuolisesti usealla eri energialähteellä ja tuotantomuodolla. Tärkeimmät sähkön tuotannon energialähteet ovat ydinvoima, vesivoima, kivihiili, maakaasu, puupolttoaineet sekä turve. Suomessa on noin 120 sähköä tuottavaa yritystä ja noin 400 voimalaitosta, joista yli puolet on vesivoimalaitoksia. Sähköstä lähes kolmannes tuotetaan yhteistuotantona lämmöntuotannon yhteydessä. Tuotanto voidaan jaotella energialähteiden lisäksi myös sen mukaan, millaisessa voimalaitoksessa sähkö on tuotettu. Lämmöntuotannon yhteydessä toimiva sähköntuotanto tapahtuu lämpövoimalaitoksessa. (Energiateollisuus, 2016.)

Huoltovarmuuskeskuksen määritelmän mukaan sähköntuotanto on valtakunnan kriittistä infrastruktuuria, koska se on kansakunnan toiminnoille elintärkeää ja sen toimintakyvyttömyydellä tai tuhoutumisella olisi heikentävä vaikutus kansalliseen turvallisuuteen, kansantalouteen, yleiseen terveyteen ja turvallisuuteen sekä valtionhallinnon tehokkaaseen toimintaan. Maamme sähköntuotanto on moneen muuhun Euroopan maahan nähden varsin hajautettua. Monipuolinen ja hajautettu sähkön tuotantorakenne lisää sähkön kansallista toimitusvarmuutta. Kyberturvallisuuden huomioiminen sähkön tuotantoprosessissa parantaa sitä entisestään.

Viimeisten vuosikymmenten aikana tapahtunut digitaalitekniikan kehitys on mahdollistanut kybertoimintaympäristön rakentumisen tietoteknologian ja internetin muodostaman kokonaisuuden ympärille. Se on avannut tämän päivän kybermaailmalle lähes rajattoman mahdollisuuksien hyödyntämisen. Kehityskulun on arvioitu tulevaisuudessa vain kiihtyvän, koska teknologia-alueen kehitystä voidaan pitää jo deterministisenä eli kehityskulku muutoksineen määräytyy pitkälti tekniikan lähtökohdista käsin. Teknologia ja tekniikat ovat käytössä ja niitä kehitetään aktiivisesti, jolloin alan sovelluksiakin käytetään koko laajuudessaan ilman esteitä. (Airaksinen, 2003, 358 - 359.)

Kehityskulku tarjoaa yhteiskunnalle, elinkeinoelämälle ja kansalaisille lisää mahdollisuuksia toimintojen tehostamiseen, liiketoimintojen laajentamiseen ja uusien palvelujen kehittämiseen tehokkaasti ja kustannuksia alentamalla. Näitä kybermaailman mahdollisuuksia voidaan hyödyntää vain siten, että niiden toimivuuteen voidaan luottaa. Se tarkoittaa digitaalisessa muodossa olevan tiedon käytettävyyden, luotettavuuden ja eheyden varmistamista eli korkeaa kyberturvallisuutta. Kyberturvallisuutta voidaan pitää tasapainotteluna teknologian mahdollisuuksien ja siihen kohdistuvien uhkien välillä.

Kybermaailman sisältämät globaalit uhat ovat pysyneet viime vuosina korkealla tasolla kansainvälisissä World Economic Forumin laatimissa vuosittaisissa yritysmaailmaan kohdistuvissa kyselytutkimuksissa. Kyberuhat koetaan yhdeksi merkittävimmistä globaaleista uhkatekijöistä toteuman todennäköisyydellä ja sen vaikuttavuudella arvioituna. Tutkimustulosta tukee se, että kyberturvallisuuden luottamusta horjuttavia uutisia esiintyy jatkuvasti eri medioissa. (World Economic Forum.) Esimerkiksi sähköverkkojen toimintaan liittyvä laaja kyberhyökkäys katkaisi sähkönjakelun Ukrainassa joulukuussa 2015 (Helsingin Sanomat, 2016).

Kybertoimintaympäristössä tapahtuvan toiminnan luottamusta voidaan parantaa useilla toimenpiteillä, mutta erityisesti elinkeinoelämässä lähtökohtana tulee olla jokaiseen liiketoimintaan sovellettu toiminnan kehittäminen. Se merkitsee kohteena olevien organisaatioiden, prosessien ja järjestelmien turvallisuustoimien jatkuvaa parantamista, ja sitä kautta tapahtuvaa yleisen luottamuksen varmistamista ja ylläpitämistä kohteen toimintaympäristössä. Tällöin ensisijaisesti kyseeseen tulevat toimenpiteet, joilla kehitetään organisaatioiden ja niiden prosessien kyberturvallisuuden hallintamekanismeja.

DIGILE:n perustaman Cyber-trust-hankkeen (DIMECC Oy, 2017) tavoitteena on parantaa tutkimuksen avulla kansallista kyberturvallisuutta ja -luottamusta yhteistyössä tiedeyhteisöjen ja yritysmaailman toimijoiden kanssa. Hankeohjelmassa painottuvat tutkittavien uhkien lisäksi erityisesti energiajärjestelmien ja teollisuuden ohjaus- ja valvontajärjestelmien (Industrial Control System, ICS) toimivuuden ja tilannetietoisuuden kehittämistarpeet kriittisen infrastruktuurin suojaamiseksi ja häiriönsietokyvyn lisäämiseksi kyberuhkia vastaan. Hanke sisältää työpaketteja, joista yksi on kriittisen infrastruktuurin sietokyvyn ja suojaamisen parantamiseen tähtäävä työpaketti (Critical Infrastructure Resiliency and Protection, CIRP).

Tämä tutkimusraportti kuuluu osaksi Cyber Trust-hankeen CIRP-työpaketin raportointia. Sen tarkoituksena on kehittää kyberturvallisuuden hallintaa sähkön ja lämmön yhteistuotannon tuotantoprosessiin eli lämpövoimalaitosprosessiin. Raportin tavoitteena on arvioida tuotantomuodon kyberturvallisuuteen vaikuttavia tekijöitä ja saada aikaan arviointiin perustuvia kehitystoimenpiteitä, jotka ovat yleistettävissä sähköntuotannon prosessien suojaamiseen kyberuhkia vastaan kustannustehokkaasti.

2. Kyberturvallisuuden hallintajärjestelmän perusteet ja rakentaminen

Suomen kansallinen kyberturvallisuusstrategia painottaa viranomaistoimintojen tärkeyttä. Koska käytännössä kuitenkin suurin osa kansantuotteeseen vaikuttavasta tuotannosta ja palveluista tuotetaan yksityisellä sektorilla, pitää kyberturvallisuusstrategia tärkeänä julkisen sektorin ja yksityisen sektorin yhteistyötä tavoitteiden saavuttamiseksi. Lisäksi kansalaisten toiminnalla on keskeinen merkityksensä turvallisuutta kehitettäessä. Tasapainoiset toimenpiteet kaikilla näillä kolmella alueella vahvistavat tietoyhteiskunnan turvallisia toimintamahdollisuuksia, tuottavat yhteistä lisäarvoa sekä varmistavat ja lisäävät elinkeinoelämän liiketoimintaedellytyksiä. Strategia painottaa, että jokaisella toimijalla, kansalaisilla, yrityksillä ja julkishallinnolla, on vastuu omasta varautumisestaan kyberuhkia vastaan. Koulutuksella ja tutkimuksellakin on keskeinen rooli kyberturvallisuuden ylläpitäjänä, kehittäjänä ja tiedon välittäjänä laajasti läpi koko yhteiskunnan. (Turvallisuuskomitean sihteeristö, 2013, 3.)

Suomen Turvallisuuskomitean kansalliseen kyberturvallisuusstrategian jalkauttamiseen liittyvä toimeenpano-ohjelmaa pyrkii ratkaisuihin, joilla edistetään suomalaisten yritysten kyberturvallisuutta, liiketoimintamahdollisuuksia sekä viranomaisten ja yritysten välistä yhteistyötä. Se sisältää kaksi kohtaa, jotka liittyvät suoraan tämän tutkimusraportin kohteeseen: (Turvallisuuskomitean sihteeristö, 2013, 3 - 4.)

- **73. TEOLLISUUDEN KYBERTURVALLISUUDEN VAATIMUSTEN JALKAUTTAMINEN TUOTANTOON (2014-2016)**
  Sovelletaan ja jatkojalostetaan tietoturvavaatimuksia ja jalkautetaan niitä kohdeyritysten automatisoidun tuotannon prosesseihin. Sulautetaan kyberturvallisuuden ja jatkuvuudenhallinnan tarpeet ja suojauskäytännöt saumattomasti teollisuusyrityksen muihin olemassa oleviin tuotantokäytäntöihin. (Turvallisuuskomitean sihteeristö, 2013, 22.)

- **74. TUOTANTOAUTOMAATIOVERKON MONITOROINTIPALVELU (2014-2016)**
  Kehitetään ja testataan yhdessä teollisuuden kanssa tekniset monitorointipalvelut, joilla voidaan seurata tuotannon tietoverkon kyberturvallisuuden tilaa reaaliaikaisesti. Palvelu kattaa normaalista tuotannosta poikkeavien tapahtumien tunnistamisen ja raportoinnin perustuen teknologia- ja palveluyritysten, tuotantoyritysten sekä tutkimuslaitosten yhteistyöhön. (Turvallisuuskomitean sihteeristö, 2013, 22.)

Turvallisuuskomitea (2013) toteaa, että valtionhallintoa koskevien toimenpiteiden kyseessä ollen yritykset osallistuvat toimintaan lähtökohtaisesti markkinaehtoisesti sopimusosapuolina ja kumppaneina. Yhteiskunnan elintärkeiden toimintojen kannalta

välttämättömät yritykset kehittävät kyberturvallisuuttaan myös osana huoltovarmuusajatteluaan. Strategiassa todetaan myös, että tutkimus ja koulutus ovat keskeisiä toimenpiteitä kyberturvallisuuden jatkuvassa kehittämisessä ja tiedon välittämisessä läpi yhteiskunnan.

DIMECC Oy:n tutkimushankkeen lisäksi Huoltovarmuuskeskuksella on käynnissä kyberturvallisuuden tutkimushanke, jonka tavoitteena on edistää teollisuusautomaation turvallisuusratkaisuja. Se on nimeltään KYBER-TEO-hanke (2014-2016), jonka Huoltovarmuuskeskus toteuttaa yhteistyössä VTT:n, Kyberturvallisuuskeskuksen ja teollisten toimijoiden kanssa. Tutkimushanke on jatkoa useita vuosia kestäneelle tutkimusyhteistyölle osapuolten välillä. KYBER-TEO-hankekokonaisuuden valikoiduista tuloksista on laadittu julkaisu, jonka johdannossa todetaan, että liiketoimintalähtöisyys on keskeinen teema automaation turvallisuuden kehittämisessä. Siksi hankkeessa on kehitetty konkreettisissa tilanteissa ja aidoissa teollisissa liiketoimintaympäristöissä käyttökelpoisia ratkaisuja, jotka voisivat olla hyödyllisiä myös monille muille toimijoille. Hankkeessa kehitettyjen ratkaisumallien todetaan hyödyttävän alan ohjelmisto- ja järjestelmätoimittajia, palvelutarjoajia ja varsinaisia teollisia toimijoita, jotka ovat automaatiosta riippuvaisia. Hanke jatkuu yritysten kanssa turvallisuuden osa-alueilla, jotka ne keskenään arvioivat kyberturvallisuuden kannalta tärkeäksi. Näitä ovat muun muassa teollisen internetin ratkaisut ja pilvipalvelut osana automaatioratkaisuja. (Huoltovarmuuskeskus, 2015, 12)

Julkaisussa ”A survey of cyber security management in industrial control systems” (Knowlesa, Princea, Hutchisona, Ferdinand, Dissob & Jones, 2015) on käsitelty teollisuuden automaatiojärjestelmien kyberturvallisuuden kehittämiseksi laadittuja standardeja sekä niiden soveltuvuutta ja hyödyntämistä järjestelmien toimivuuden varmistamiseksi. Taulukossa 1 on lueteltu julkaisussa mainitut standardisarjat. Ne ovat yleisesti saatavilla olevia dokumentteja, joten niiden hyödyntämiselle ei ole estettä. Kansainvälistä ISO27000-standardiperhettä lukuunottamatta ne ovat myös maksuttomia.

Suomessa on käytössä lisäksi kansallinen turvallisuuden kriteeristö (Katakri), joka sisältää teknisen tietoturvaosuuden ja on siten hyödynnettävissä kyberturvallisuuden kehittämistoimenpiteissä. Kotimaan viranomaistoiminnoissa se on määräävä toiminnan auditointiohjeisto. (Puolustusministeriö, 2015, 3.)

Information security publications by industry and country.			
Industry	Country	Publication	Paid or public
Cross-industry	International	ISO/IEC27000Series	Paid
	United States	DoDDirective8500.1:InformationAssurance	Public
		DoD Instruction8500.2:InformationAssuranceImplementation	Public
		DoD Instruction8510.01:DIACAP	Public
		FIPS 199	Public
		FIPS 200	Public
		NIST 800Series	Public

TAULUKKO 1. Teollisuusautomaation kyberturvallisuuteen liittyviä standardeja (Knowlesa ym., 2015, 60)

NIST 800-standardisarja pitää sisällään kybertoimintaympäristössä toimiville organisaatioille muun muassa riskienhallinta- ja teollisuusautomaatiostandardeja. Kyberturvallisuuden hallintajärjestelmän perusrakenne puolestaan on kuvattu ISO27001-standardissa (Suomen Standardisoimisliitto SFS ry, 2012, 23). Sen lähtökohtana on kohteen riskiarviointi ja arvioinnin perusteella tehtävät toimenpideanalyysit. Yrityksen on myös tärkeää julistaa ja viestittää politiikka, jolla johto sitoutuu hallinnan kehittämisen edellyttämiin toimenpiteisiin. Varsinaiset konkreettiset käytännön toimenpiteet kohdistuvat tietoturvaratkaisujen varmistamiseen sekä lopuksi jatkuvuus- ja toipumissuunnitelmien laadintaan.

Työkaluksi hallintajärjestelmän kehittämiseen ISO27001-standardi suosittelee PDCA -ongelmanratkaisumenetelmän (Plan, Do, Check, Act) käyttöä. Se on klassinen ongelmanratkaisumalli ja organisaation toiminnan kehittämismenetelmä. Sitä kutsutaan usein myös Demingin tai Shewhartin kehittämisympyräksi tai -kehäksi. (Laatuakatemia.)

PDCA- ongelmanratkaisumenetelmä (KUVIO 1) perustuu neljän kehitysvaiheen kiertoon. Ensimmäinen vaihe koostuu suunnittelusta (Plan). Toimenpide edellyttää kohteen analysointia ja sen pohjalta laadittuja toimenpidevaihtoehtojen muodostamista. Toteutusvaiheessa (Do) pannaan toimeen valitut toimenpiteet. Tämän jälkeen tarkistetaan (Check) käytännössä, että toimenpiteet ovat toimivia, tehokaita ja tarkoituksenmukaisia. Viimeisessä ympyrämallin vaiheessa tehdään valituille toimenpiteille tarvittaessa korjaukset (Act) ja vakiinnutetaan ne käytäntöön. Yhden toteutuskierroksen jälkeen ympyrässä palataan

alkuun ja uuden tilanneanalyysin perusteella valitut kehittämistoimenpiteet aloittavat uuden kierroksen. Kehittäminen voi silloin edetä päättymättömänä prosessina, jossa jokaisen ympyrän kierroksen jälkeen ollaan uudella toiminnan tasolla. Menetelmä perustuu jatkuvan oppimisen ja toiminnan jatkuvan kehittämisen ajatukseen. (Laatuakatemia.)

PDCA-ongelmanratkaisumenetelmä on yksi merkittävimmistä ja yleisimmin käytetyistä työkaluista organisaatioiden jatkuvassa parantamisessa, laatujohtamisessa ja prosessien kehittämisessä (Laatuakatemia).

KUVIO 1. PDCA-ongelmanratkaisumenetelmä (Laatuakatemia)

Kyberturvallisuuden hallintajärjestelmä sopii hyvin osaksi yrityksen toimintajärjestelmää, jonka keskeisenä tarkoituksena on yhdessä sovittujen toimintatapojen kokoaminen yhteen ohjeistoon. Toimintajärjestelmä on menestyvässä yrityksessä jatkuvan parantamisen kohteena. Parantamistoimenpiteet perustuvat tällöin yrityksen tulostietoihin sekä eritasoisten palautteiden ja arviointien tuloksiin. Parhaimmillaan toimintajärjestelmä tukee johtamista, avustaa organisaatiota tavoitteiden saavuttamisessa ja toimii informaatiokanavana henkilöstölle. Toimintajärjestelmän perusedellytyksen on kuvattu ISO-9001-standardissa (Suomen Standardisoimisliitto ry, 2016, 9). Tarvittaessa standardit ISO-27001 ja ISO-9001 sopivat myös yrityksen toiminnan ulkopuolisen sertifioijan arviointityökaluiksi.

Tämän raportin perusteet liittyvät kansallisen kyberturvallisuusstrategian toimenpiteiden edistämiseen ja edellä mainituista tutkimushankkeista saatuihin kokemuksiin ja tietoihin, joita hyödynnetään raportissa soveltuvilta osilta. Raportin mukaisen kyberturvallisuuden

hallintajärjestelmän rakentuminen perustuu alan standardeihin, jotka ovat tarkoitettu hyödynnettäviksi organisaatioiden kehittämistoimissa, uuden toiminnan vakiinnuttamisessa ja erityisesti alan kaupallisten sopimusosapuolten yhteisenä määrittelyperustana.

3. Teollisuusautomaatiojärjestelmät kybertoimintaympäristössä

Suomen Automaatioseura luokittelee teollisuusautomaatiojärjestelmät eli ICS-järjestelmät niiden ohjausjärjestelmien ja verkkorakenteen perusteella karkeasti seuraaviin ryhmiin: (Suomen Automaatioseura ry Turvallisuusjaosto, 2010)

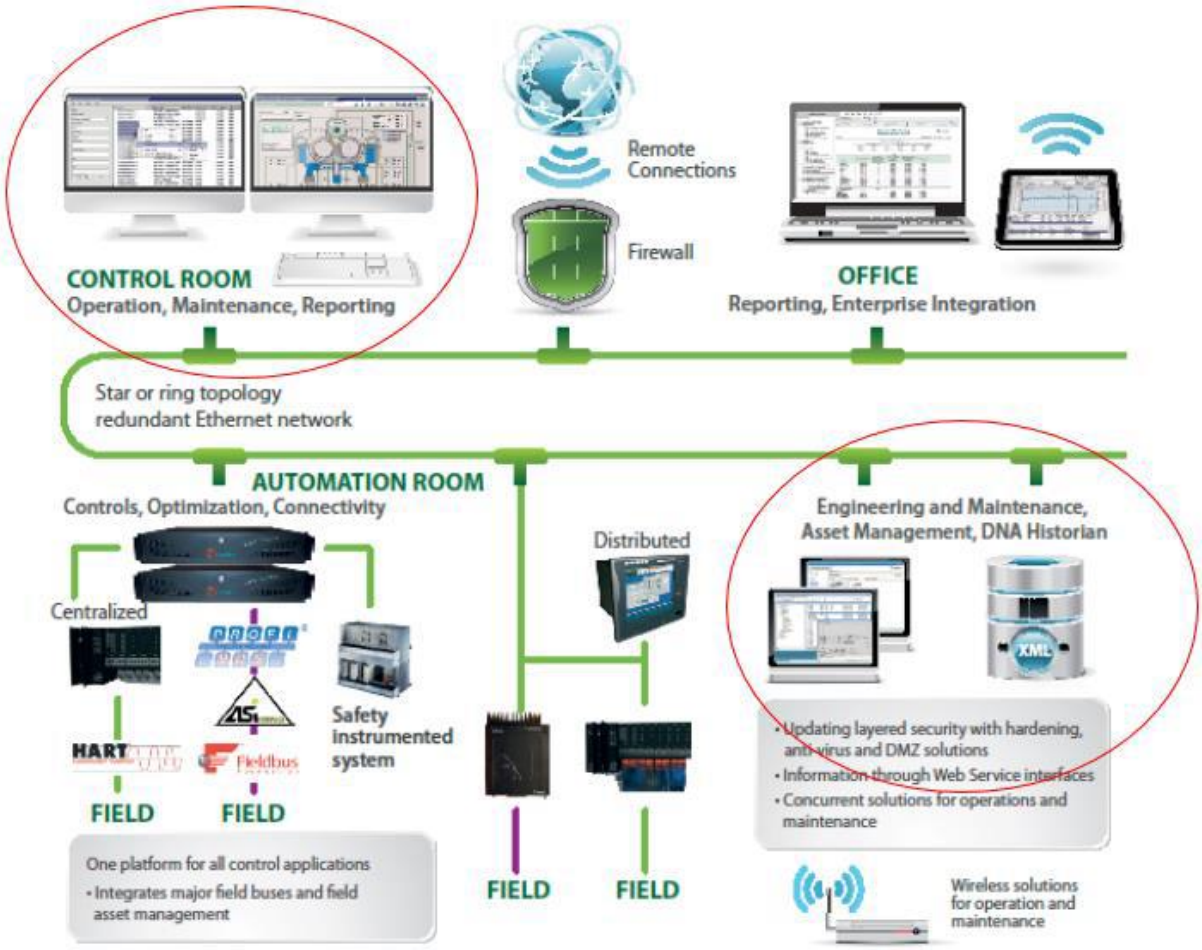
1. SCADA-käytönvalvontajärjestelmät (Supervisory Control and Data Acquisition Systems)
2. Ohjelmoitavat logiikkajärjestelmät (Programmable Logic Control, PLC)
3. Hajautetut automaatiojärjestelmät (Distributed Control Systems, DCS)

SCADA-tyyppisiä järjestelmiä käytetään pääasiassa maantieteellisesti hajautettujen järjestelmien ohjaukseen hankkimalla keskitetysti tietoja eri yksiköistä ohjaustoimintoja varten. Tyypillisiä hajautettuja toimintoja, joissa käytetään SCADA-järjestelmiä, ovat infrastruktuurijärjestelmät, kuten energianjakeluverkot, kaasulinjat, vesijärjestelmät, jätevesijärjestelmät sekä muut vastaavat yleiset verkot ja teollisuusverkot. Käytännön sovelluksissa SCADA-järjestelmien tärkein tehtävä on etäasemien ohjaus, mikä tapahtuu tavallisesti automaattisesti. SCADA-tyyppisiin järjestelmiin kuuluvat keskusvalvontayksikkö (Central Monitoring System, CMS) sekä yksi tai useampia etäasemia (Remote Terminal Unit, RTU), joihin kommunikaatio reititetään oman suojatun aliverkon kautta. Keskitetty ohjausjärjestelmä kerää ja tekee lokit tiedoista, joita saadaan etäasemista, ja tuottaa tarvittavat toimenpiteet etäasemien tekemien havaintojen ja mittausten perusteella. Tyypilliseen etäaseman kokoonpanoon kuuluu joko säätöasema ohjaus- ja toimilaitteineen tai ohjelmoitava logiikkayksikkö toimilaitteineen ja valvonta-antureineen. Yritysten liiketoimintoja varten SCADA-järjestelmistä voi olla pääsy tehtaan tietojärjestelmiin Internetverkon kautta tai joissain tapauksissa myös laajan lähiverkon (Wide Area Network, WAN) kautta. (Suomen Automaatioseura ry Turvallisuusjaosto, 2010, 54.)

Ohjelmoitavia logiikoita (PLC) käytetään ohjaamaan erillisiä prosesseja sekä hajautettujen ohjaus- ja SCADA-järjestelmien alajärjestelmiä ja erillisiä turvatoimintoja. Prosessin ohjauksessa tyypillisiä esimerkkejä löytyy kappaletavarateollisuuden valmistusjärjestelmistä. Ohjelmoitavat logiikat ovat tyypillisesti modulaarisia laitteita tai piirikortteja, joita käytetään prosessinohjaukseen, digitaalisiin binäärituloihin ja -lähtöihin sekä analogisiin tuloihin ja lähtöihin, ihminen–kone-vuorovaikutukseen sekä tietoliikenteen liitäntöihin. Turvatoimintojen esimerkkejä löytyy koneautomaatiosta, joissa turvatoimintoja tarvitaan jatkuvasti. (Suomen Automaatioseura ry Turvallisuusjaosto, 2010, 56.)

Hajautettuja automaatiojärjestelmiä (DCS) käytetään ohjaamaan laajoja ja monimutkaisia prosesseja, kuten voimalaitoksia, kemianlaitoksia ja öljynjalostuslaitoksia sekä terästeollisuuden, elintarvikealan, panimoalan, lääketeollisuuden, sellu- ja paperiteollisuuden, metalliteollisuuden ja kaivosten laitoksia, jotka sijaitsevat tavallisesti yhdellä toiminta-alueella. Hajautettu ohjausjärjestelmä käsittää ohjaustason ja yhden tai useampia hajautettuja ohjausyksiköitä samassa tehdaslaitoksessa. Valvontayksikkö toimii

ohjauspalvelimessa ja kommunikoi sen ala-asemissa oman aliverkon kautta. Ohjausyksikkö antaa asetusarvoja ja hankkii tietoja hajautetuilta ohjausyksiköiltä. Hajautetut ohjausyksiköt ohjaavat tuotantoprosessien toimintoja ohjausyksikön antamien käskyjen mukaisesti käyttämällä anturien palautetta tuotantoprosessiin sijoitetuista antureista. Nämä ohjausyksiköt käyttävät tyypillisesti paikallista kenttäväylää kommunikointiin toimilaitteiden ja anturien kanssa. Kuviossa 2 on nykyaikaisen hajautetun teollisuusautomaatiojärjestelmän perusrakenne, joka edustaan tyypillistä ohjausrakennetta kotimaisen lämpövoimalan sähköntuotantoprosessissa. Hajautettu automaatiojärjestelmä kybertoimintaympäristössä on tämän raportin tarkastelukohde.



KUVIO 2. Hajautettu ICS-järjestelmä (Industrial Control System)
(Valmet Automation Oy, 2018)

Kybermaailman rakennetta voidaan kuvata viisikerroksisella rakennemallilla, johon myös jokainen edellä mainituista teollisuuden automaatiojärjestelmistä voidaan sijoittaa. Rakenteen kerrokset ovat (Lehto, 2015, 6):

1. Kognitiivinen kerros
   - Inhimillinen ongelmanratkaisu- ja tulkintaympäristö
   - Informaation merkityssisällön ymmärtäminen ja tulkinta
2. Palvelukerros
   - Julkiset ja kaupalliset verkkopalvelut
   - Operatiiviset ja viestinnälliset palvelut
3. Semanttinen kerros
   - Käyttäjän hallitsema informaatio- ja tietosisältö
   - Käyttäjän hallitsema järjestelmän toimintojen ohjaus
4. Syntaktinen kerros
   - Järjestelmän ohjaus- ja hallintaohjelmat
   - Verkkoprotokollat, virheenkorjaus, kättelyt
5. Fyysinen kerros
   - Verkkolaitteet, kytkimet, reitittimet
   - Lankayhteydet ja langattomat yhteydet

Energiayhtiöiden kybermaailman päällimmäiset riskit liittyvät rahan, sensitiivisen tiedon ja maineen menettämiseen sekä liiketoiminnan estymiseen. Turvallisuusratkaisut ja kyky sietää häiriöitä muodostavat tällöin riskien hallinnan keskeisimmät tekijät. Riskien taustalla olevia haavoittuvuuksia voidaan puolestaan arvioida teknologian puutteena suhteessa hyökkäysteknologiaan, puutteina henkilöstön osaamisessa ja toimintatavoissa, puutteina organisaation kyberturvallisuusprosesseissa tai johtamisessa sekä puutteina toiminnan jatkuvuuden turvaamisessa tai häiriöistä toipumisessa. Teollisuusprosessien todennäköisimmät tämän päivän kyberhyökkäysmuodot voivat liittyä henkilöstön hyväksikäyttöön esimerkiksi haitta- ja vakoiluohjelmien ujuttamiseksi automaatiojärjestelmiin. Ne voivat myös kohdistua automaatiojärjestelmiin langattomien yhteyksien kautta tai internetin kautta tapahtuvina verkkohyökkäyksinä. Tällöin haitantekijöiden tavoitteet voivat liittyä verkon palvelujen estämiseen, koko toiminnan lamauttamiseen, tietovarkauksiin tai tiedon vääristämiseen tai vakoiluohjelmien perille saattamiseen. Niin sanotuilla takaporteilla saastutetut komponentit tai niiden tarkoituksellinen ohjelmointi hyökkääjän tarpeisiin on yhä enemmän esillä tämän päivän kybermaailmassa. (Lehto, 2015, 22 - 23)

Arvioitaessa teollisuusautomaatiojärjestelmien sijoittumista kybermaailmaan ja niiden kyberturvallisuuteen vaikuttavia seikkoja, on ensiarvoisen tärkeää tiedostaa järjestelmien keskeisimmät ominaisuudet. Esimerkiksi lämpövoimalaitoksissa käytössä olevia hajautettuja automaatiojärjestelmiä voidaan luonnehtia siten, että ne ovat hyvin vakiintuneita ja niiden käyttöikä on pitkä verrattuna, vaikka toimistojärjestelmiin, jotka ovat elinkaareltaan huomattavasti lyhempiä. Automaatiojärjestelmien elinkaaret voivat olla perusjärjestelmän osalta jopa useiden vuosikymmenien mittaisia. Lisäksi perusjärjestelmien konfiguraatiota

muutetaan harvoin. Muutokset toteutetaan lähinnä suurempien kunnossapito- tai muutostöiden yhteydessä järjestelmien elinkaaripäivityksinä. Automaatiojärjestelmät ovat myös resursseiltaan rajoittuneita, jolloin niissä ei ole voitu käyttää teknillisiä tietoturvaratkaisuja eikä salaustekniikoita tekniikoiden tarjoamassa täydessä laajuudessa. Järjestelmien käyttöorganisaatiot ovat hyvin tehtäviinsä koulutettuja ja tuntevat siten laitteet, laitteiden toimintaperiaatteet ja toimintaympäristöt. Automaatiojärjestelmien tietovarastot sisältävät pääosin prosessin tietoja eivätkä niinkään liiketoimintojen kannalta salassa pidettävää tietoa. Suoraa yhteyttä internet-verkkoon ei useinkaan tarvita eikä niiden tietoteknisiä laitteita käytetä muihin tarkoituksiin, vaan ne ovat hajautettuina valmistusprosessiin, sen mittaus- ja ohjaustehtäviin sekä turvatoimintoihin. Järjestelmiin tapahtuva pääsyn hallinta on useimmiten tarkasti järjestetty. Automaatiojärjestelmien toimintojen ja henkilöstön valvonta on hallittua muun muassa prosessin toiminnan käytettävyys- ja turvallisuusvaatimuksista johtuen. (Suomen Automaatioseura ry Turvallisuusjaosto, 2010.)

4. Kyberturvallisuuden hallintajärjestelmän laatiminen lämpövoimalaitosprosessiin

Energiayhtiön lämpövoimalaitoksen pääprosessina toimivan sähkön- ja lämmöntuotantoprosessin korkean käytettävyysarvon merkitys on ensisijainen liiketoiminnan tuloksen muodostuksen ja toiminnan luotettavuuden näkökulmista tarkasteltuina. Sähköntuotannon kyberturvallisuuden hallintajärjestelmän kehittämisen perustavoitteena tuleekin siten olla ensisijaisesti digitaalisessa muodossa olevan tiedon käytettävyyden varmistaminen osana tarkastelun kohteena olevan tuotantoprosessin kokonaiskäytettävyyttä. Lisäksi prosessin sisältämän ja käyttämän tiedon luotettavuus ja sisällöllinen eheys ovat tärkeitä tavoitteita. Näistä lähtökohdista tulee pyrkiä rakentamaan kokonaisluottamus, joka perustuu kohteena olevan organisaation realistiseen käsitykseen omista kyvykkyyksistään hallita kybermaailmassa toimimiseen liittyvät haasteet. Tämä raportin kappale tarkastelee ensisijaisia hallintatoimenpiteitä tuotantoprosessin kyberuhkia vastaan ISO27001-standardin periaatteiden mukaisesti. Toissijaisesti tarkastelussa on käytetty NIST 800-sarjan standardeja ja ISO9001-standardin periaatteita.

Kyberturvallisuuden kehittäminen perustuu ajatukseen, että ensiksi määritetään kohde, laaditaan kohteen uhka-arviot ja toteutetaan niitä vasten laaditut toimenpiteet. Hallintajärjestelmän rakentamisen ensimmäisenä vaiheena on riskitarkastelu, joka kohdistuu tässä tapauksessa lämpövoimalan tuotantoprosessiin. Lämpövoimalaitostuotanto tapahtuu prosessissa, jonka pääkomponentit ovat polttoaineen syöttöjärjestelmä, lämmityskattila, turbiini, generaattori ja kaukolämmönvaihdin. Erilaiset lauhdutus- ja kylmävesijärjestelmät myös kuuluvat prosessiin ja niiden merkitys on tärkeä kokonaisprosessin hallinnassa ja silloin kun kaukolämpöä ei tarvita tai sitä tarvitaan vähäisiä määriä. Koska kaikkia edellä mainittuja komponentteja tarvitaan sähkön tuotantoprosessissa, niiden keskinäinen riippuvuus, toiminnallisuuden ohjaus ja valvonta ratkaisevat tuotannon onnistumisen. Kyberturvallisuuden hallitsemiseksi koko tuotantoprosessi ja sen riskit tulee siten käsitellä samanarvoisina tarkastelukohteina. Lämpövoimalaitoksen tuotantoprosessin hajautetun automaatiojärjestelmän kybermaailman rakenne on esitetty taulukossa 2.

Tuntemalla prosessin toiminnot kerros kerrokselta viisikerroksisessa rakenteessa, voidaan niihin liittyvät merkittävimmät haavoittuvuudet, todennäköisimmin kyberhyökkäystavat ja niiden motiivit arvioida (taulukko 2). Haavoittuvuuksien analysointi mahdollisia hyökkäystapoja vastaan on järjestelmällinen apuväline prosessien toimintaan liittyvien riskien tunnistamiseen. Analyysi antaa siten nopeasti karkean kokonaiskuvan prosessin toiminnan jatkuvuuteen liittyvistä uhkista.

Sähköntuotannon kyberuhkien motiivien voidaan arvioida jakautuvan tuhovaikutusten aikaansaamiseen prosessissa, prosessihaavoittuvuuksien tiedusteluun, anarkismiin tai egoismiin. Tällöin toimijat voivat olla jopa valtiollisia toimijoita tai yleisimmin järjestäytyneitä aktivisteja tai hakkereita tai vaihtoehtoisesti yksittäisiä itsenäisiä toimijoita.

Kun on tunnistettu haavoittuvuudet, arvioitu niihin liittyvien uhkien takana olevat motiivit toimijoineen, tunnistettu mahdolliset hyökkäystavat ja tiedostettu prosessin toiminnot, voidaan suorittaa lopulliset riskiarvioinnit näiden tietojen ja arviointien pohjalta.

Riskin suuruutta puolestaan voidaan arvioida esimerkiksi vahingon seurausten ja tapahtuman todennäköisyyden tulona. Eräs seurauksia luokitteleva asteikko pitää sisällään luokat vakava, haitallinen tai vähäinen. Todennäköisyydet puolestaan voidaan luokitella asteikolla todennäköinen, mahdollinen tai epätodennäköinen. Kun seuraukset ja todennäköisyydet numeroidaan yhdestä viiteen kutakin kohtaa arvioitaessa ja muodostetaan niiden tulo, niin saadaan riskit priorisoitua tulojen suuruusjärjestyksessä. Priorisoinnissa perusteella voidaan puolestaan kohdentaa toimenpiteet tärkeysjärjestyksessä riskien hallitsemiseksi.

Raportin riskiarvio perustuu kohteen prosessin tuntemukseen, kyberturvallisuuden standardeihin, alan tutkimustietoihin sekä yleiseen käsitykseen ja kokemukseen kyberturvallisuusriskeistä. Taulukossa 2 on esitetty niistä kaikista todennäköisimmät sijoitettuna kohteen kybermaailmaa kuvaavaan viisiportaiseen rakenteeseen. Arvioitavien riskien priorisoinnin esittämisessä on käytetty seuraavaa arviointitaulukkoa ja värikoodia:

1. Merkityksetön, vihreä
2. Vähäinen, vihreä
3. Kohtalainen, keltainen
4. Merkittävä, punainen
5. Sietämätön riski, punainen

Kyberrakenne	ICS:n toiminnot	Haavoittuvuudet	Hyökkäystavat
Kognitiivinen kerros	Käyttöhenkilöstö	- kompetenssipuute - puutteellinen tilannetieto - ”sinisilmäisyys”	- tietojen kalastelu - ID-varkaudet - social engineerig
Palvelukerros	Julkiset verkkoyhteydet - internet - puhelimet - data	- riittämätön turvallisuusjohtaminen - puutteelliset turvallisuusprosessit - puutteellinen tietosuojaus	- palvelun esto - ATP - vakoiluohjelmat
Semanttinen kerros	Valvomot: - näyttöjärjestrelmät - operointilaitteet - ylläpitotiedot - raportointi - sis. verkko - data	- puutteellinen tietosuojaus - heikko varmuuskopiointijärjestel y - puutteet ohjelmistosuunnittelussa ja -tuotannossa	- tietovarkaus - tietojen tuhoaminen - tietojen vääristäminen
Syntaktinen kerros	Prosessiasemat: - ohjaus- ja säätölaitteet - vikadiagnoosit -häiriövalvonta - sis. verkko	- puutteellinen tietosuojaus	- järjestelmiin murtautuminen -haavoittuvuuksien tiedustelu
Fyysinen kerros	Kenttälaitteet: - mittaus- ja ohjauslaitteet - fyysinen kaapelointi	- puutteellinen suojaus - testaamattomat laitteet	- varkaus - vahingonteko - komponenttien saastuttaminen

HENKILÖSÖTÖN VIRHEELLISEN TOIMINNAN RISKI

VERKKOHYÖKKÄYSRISKI

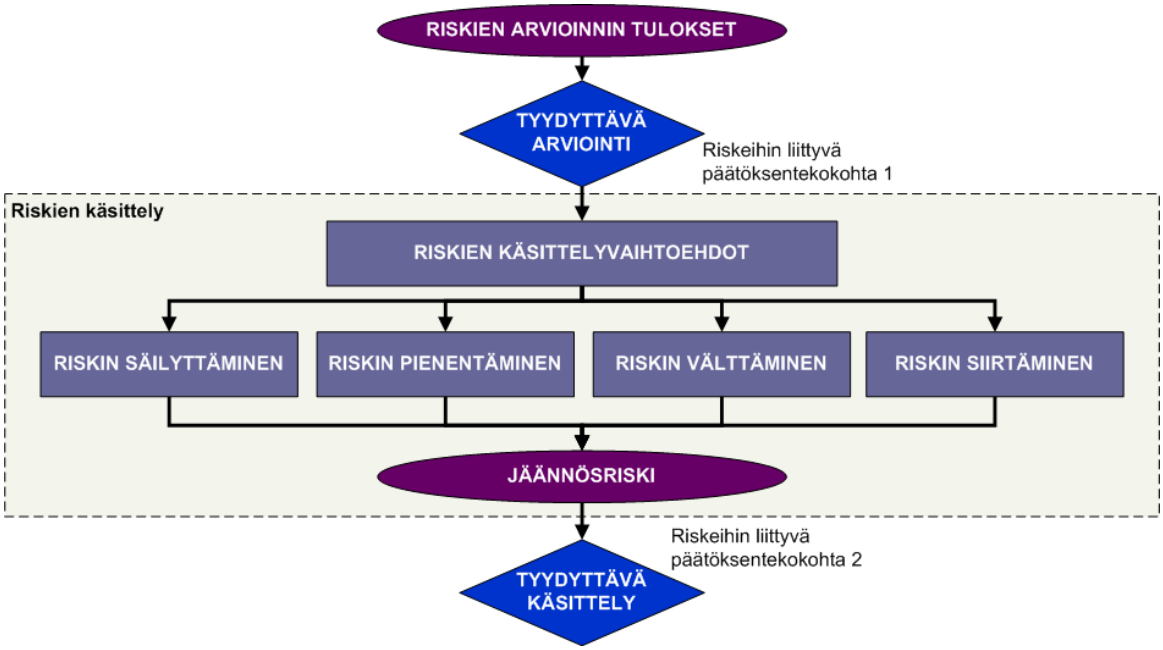
HYÖKKÄYSRISKI VALVOMO-OHJELMISTOON

HYÖKKÄYSRISKI AVOIMIIN YHTEYKSIIN

FYYSISEN HAITTAVAIKUTTAMISEN RISKI

TAULUKKO 2. Lämpövoimalaitosprosessin kyberrakenne ja sen merkittävimmät riskit (Lehto, 2015, 6)

ISO27000-sandardiperheen riskienhallintastandardi ISO27005 sisältää kuvion 3 mukaisen riskienkäsittelyprosessin. Sitä voidaan hyödyntää edellä mainittujen riskien käsittelyyn. (Lehto, 2015, 22 - 23)



KUVIO 3. ISO 27005: Riskien käsittelytoiminta (Suomen Standardisoimisliitto ry, 2015, 50)

Taulukon 2 riskien käsittelyssä liikennevalojen väreillä esitetyt riskit voidaan luokitella kuvion 3 mukaisessa käsittelyprosessissa siten, että punaisella ja keltaisella merkityt riskit joko pienennetään tai ne pyritään välttämään, kun puolestaan vihreällä merkityt riskit voidaan säilyttää. Säilytettävät riskit, jotka sijaitsevat joko kognitiivisella tai fyysisellä kierroksella, kohdistuvat henkilöstön virheelliseen toimintaan tai tuotantoprosessin kenttälaitteiden toiminnan häiritsemiseen fyysisellä vaikutuksella. Ne voidaan perustella säilytettäviksi tutkimuskohteen tuotantoprosessiin liittyvän henkilöstön hyvällä koulutuksella, tehtävien selkeällä roolituksella ja pysyvyydellä sekä tuotantolaitoksen kulkurajoitetulla luonteella. Voimalaitoksen kybermaailman palvelukerros, syntaksinen tai semanttinen kerros, sisältää joko ohjelmistoja, tietovarantoja, tiedonsiirtotekniikkaa tai teknillisiä laitteita tai niiden yhdistelmiä. Näihin rakennekerroksiin kohdistuvat riskit ovat kyberturvallisuuden kannalta joko pienennettäviä tai vältettäviä. Merkittävimmäksi riskiksi voidaan arvioida verkkohyökkäysriski palvelukerroksessa. Seuraavalla riskitasolla ovat valvontajärjestelmään kohdistuvat hyökkäysriskit semanttisessa kerroksessa ja avoimiin yhteyksiin kohdistuvat hyökkäysriskit syntaksisessa kerroksessa. Hyökkäysriski avoimiin yhteyksiin on mahdollinen uusimmissa ICS-järjestelmissä (kts. KUVIO 1), koska niiden kokoonpanoihin on voitu lisätä kenttälaitteiden testausta helpottamaan erillinen langaton valvontayhteys. Lisäksi järjestelmien rakenteisiin on voinut jäädä haavoittuvia langallisia yhteyksiä. Avoimien yhteyksien osalta riskinhallintaa tulee parantaa vähintään siten, että niiden luvaton käyttäminen estetään teknillisellä suojauksella, hallinnollisella toimintaohjeistuksella ja koulutuksella. (Lehto, 2015, 22 - 23)

Riskien välttämiseen tai pienentämiseen on käytössä kyberturvallisuuden hallinnollisia ja teknillisiä ratkaisuja, joita on esitetty kootusti KYBER-TEO-hankeen vuoden 2015 raportissa.

Oheiset ratkaisuehdotukset on poimittu raportin kyberturvallisuutta tuotantoon käsittelevästä luvusta (Huoltovarmuuskeskus, 2015, 16 - 20).

Tutkimuskohteeseen liitettynä teknillisen ratkaisut ovat seuraavat (Huoltovarmuuskeskus, 2015, 16 - 20):

1. Verkkohyökkäysriskien hallintaan liittyvät automaatioverkon monitorointijärjestelyt
- automaatioverkkoon kytkettäväksi suunniteltu palomuuri
- automaation järjestelmälokien analyysi ja raportointi
- signatuurien tunnistus
- (Verkko-IDS)
- verkkoliikenteen tietovuoseuranta ja yllättävien poikkeavuuksientunnistus
- hälytysten raportointi

2. Valvomo-ohjelmistoriskin hallintaan liittyvä automaation tietoturvatestaus
- verkkoskannerit
- fuzzerit, esimerkiksi Defensics TCF
- penetraatiotestauksen työkalut, esimerkiksi Metasploit

Kyberturvallisten teknillisten ratkaisujen lisäksi KYBER-TEO raportissa on mainittu hallinnollisia toimenpiteitä, joista ainakin seuraavat toimenpiteet ovat käyttökelpoisia tutkimuskohteessa (Huoltovarmuuskeskus, 2015, 16 - 20):

- tuotannon yhtenäinen tietoturvapolitiikka
- käytännön ohjeet tietoturvan ylläpitämiseen tuotannossa
- automaatioverkossa sallitut etäyhteyskäytännöt, tekniikat ja yhteyspisteet
- automaatio- ja verkkojärjestelmien kyberturvallisuustarkastukset ja kartoitukset
- työlupien myöntäminen ennen minkä tahansa työn aloittamista
- muutosten hallinta kaikkien automaatiojärjestelmien, automaatioverkkojen, sekä näiden kyberturvallisuuteen liittyvien asetusten ja kokoonpanon osalta

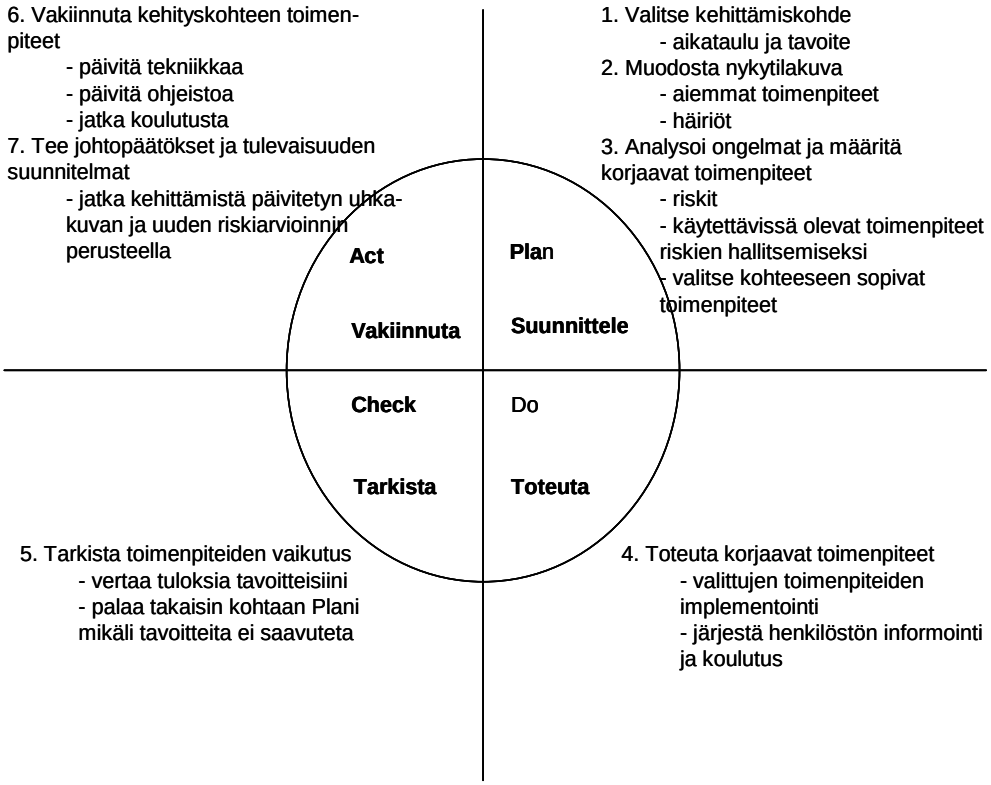
ISO27001-standardi suosittelee organisaation kyberturvallisuuden hallinnan kehittämiseen PDCA-ongelmanratkaisumenetelmää, jota on yleisesti käytetty organisaatioiden jatkuvan parantamisen työkaluna. Sen perusajatus on pitkäkestoisen organisoidun kehittämiskulttuurin aikaansaamien kehityssyklejä toistamalla. Kehittämisen osittaminen sykleihin eli ympyrän kierroksiin, perustuu jatkuvan oppimisen ajatukseen. Tällöin informaatio ja tietotaso kehityskohteesta lisääntyvät jokaisen tarkastelukierroksen aikana. Toimenpiteillä ei pyritä täydellisyyteen, vaan tarkoituksenmukaiseen, tehokkaaseen ja käytännön läheiseen laadulliseen kehittämiseen.

Ympyrän yhden kierroksen toimenpiteet ovat lähes poikkeuksetta paljon suunnittelua vaativia ja toimenpiteiden osalta aikaa vieviä, joten yleisesti ottaen kehityskierroksen toteuttamiseen on syytä varata riittävästi aikaa. Toimenpiteiden valinta on myös tärkeää suhteuttaa niiden toteuttamiseen käytettäviin resursseihin. Tutkimuskohteen ensimmäisen

vuosijakson tavoitteeksi voisi valita kyberturvallisuuden hallinnan tunnistamisen ja sen riskien käsittelyn perusteella esimerkiksi verkkohyökkäysriskien vaikutusten pienentämisen. Tällöin ympyrän toimenpiteiksi valikoituisi edellä mainituista hallinnollisista toimenpiteistä ensisijaiset käyttöönotettavat toimenpiteet, kuten yhtenäinen tietoturvapolitiikka, käytännön ohjeet tietoturvan ylläpitämiseen ja ehkä alustavat varsinaisen automaatiojärjestelmän kyberturvallisuustarkastukset. Teknillisistä toimenpiteistä luontevimmin kehityskohteiksi valikoituisivat automaatioverkon monitorointijärjestelyt.

Kuvio 4:n on hahmoteltu vaiheet edellä kuvattujen toimenpiteiden käynnistämiseksi PDCA-ongelmanratkaisumenetelmää käyttäen.

Raportin tässä kappaleessa on kuvattu kohteen tuotantoprosessin kyberturvallisuuden hallinnan hallinnolliset ja teknilliset perusratkaisut. Niiden aikaansaaminen muodostaa perustan myöhemmille toimenpiteille, kuten toiminnan jatkuvuuden hallitsemiselle ja häiriöistä toipumiselle. Niiden jalkauttamisen voisi valita seuraavaan kehityskierroksen kohteeksi.



KUVIO 4. PDCA-ongelmanratkaisumenetelmä tutkimuskohteeseen sovellettuna

5. Yhteenveto

Huoltovarmuuskeskuksen määritelmän mukaan sähköntuotanto on valtakunnan kriittistä infrastruktuuria, koska se on kansakunnan toiminnoille elintärkeää. Energiayhtiöiden sähköntuotantoprosessien käytettävyyden varmistaminen kaikissa toimintaympäristöissä on keskeinen osa kriittisen infrastruktuurin toimintakykyä. Näin ollen energiayhtiöiden toimenpiteet prosessiensa kyberturvallisuuden hallitsemiseksi muodostavat tärkeän osan tuotannon käytettävyyden varmistamista.

Lämpövoimalaitoksen tuotantoprosessin merkittävimmäksi riskiksi on tässä raportissa arvioitu verkkohyökkäysriski sen palvelukerroksessa. Seuraavalla riskitasolla ovat valvontajärjestelmään kohdistuvat hyökkäysriskit prosessin semanttisessa kerroksessa ja avoimiin yhteyksiin kohdistuvat hyökkäysriskit prosessin syntaktisessa kerroksessa. Edellä mainitut riskit tulee käsitellä osana kyberturvallisuuden hallintaa.

Energiayhtiön lämpövoimalaitoksen tuotantoprosessin riskilähtöisen kyberturvallisuuden hallinnan osalta ensimmäisen vaiheen toimenpiteet voidaan tiivistää ja priorisoida seuraavasti:

1. Varmistetaan, että yritys näkee kyberturvallisuustoimenpiteet strategisena tavoitteena ja, että valittujen toimenpiteiden toteutukseen saadaan riittävät resurssit.
2. Päivitetään yrityksen toimintapolitiikka kyberturvallisuuden edellyttämällä tavalla.
3. Valitaan ISO27001-standardi toimenpiteiden suorittamisen malliksi. Hyödynnetään muita erityisesti kyberturvallisuusalan teollisuusautomaatiospesifisiä standardeja toteutuksessa (Esimerkiksi NIST 800–82re2).
4. Suoritetaan ensimmäisessä kehitysvaiheessa kappaleessa 4 esitetyt ensisijaiset kehitystoimenpiteet (hallinnolliset toimenpiteet ja verkkohyökkäysriskin pienentäminen) sijoittamalla ne PDCA-ongelmanratkaisumenetelmään (KUVIO 4) ja toteutetaan kehityskierros.
5. Muodostetaan kehitystoimenpiteistä jatkuva prosessi valitsemalla seuraavan kehityskierroksen kohteet ja toistetaan kohdan 4 toimenpiteet.
6. Seurataan toimenpiteiden vaikuttavuutta osana yrityksen auditointi- ja johtamismenettelyjä (esimerkki osana ISO 9001-standardin menettelyjä).

Yrityksen tai jonkin sen organisaatio-osan toiminnan kehittämisen onnistumien riippuu viimekädessä johdon sitoutumisesta toimintaan ja toimenpiteiden resursoinnista. Usein joudutaankin turvautumaan yrityksen ulkopuolisiin kehittäjiin jo pelkästään siksi, että oma henkilöstö sitoutuu lähes kokonaisuudessaan päivittäiseen operatiiviseen toimintaan. Yrityksen ulkopuolisen kehitysresurssin käyttö on suositeltavaa myös tietotaidon hankinnan näkökulmasta katsottuna. Lisäksi kustannustehokkaat ratkaisut ovat poikkeuksetta tavoittelun arvoisia.

Tämä tutkimusraportti auttaa osaltaan ratkaisuissa, joilla energiayhtiöt voivat käynnistää tai edistää jo aloitettuja tuotantoprosessiensa kehittämistoimenpiteitään kyberuhkia vastaan. Toimenpiteet antavat perustan tuotantoprosessin toiminnan jatkuvuuden hallintaan ja häiriöistä toipumiseen kyberturvallisuuden ollessa uhattuna. Samalla tämän raportin jatkotoimenpiteenä edistetään myös kansallisten Turvallisuuskomitean tavoitteiden 73 ja 74 saavuttamista. (Turvallisuuskomitean sihteeristö, 2013, 22.)

Ukrainassa 23. päivänä joulukuuta 2015 tapahtuneen laajan sähkökatkon syyksi on tutkinnassa selvinnyt ulkopuolisen tahon suorittama koordinoitu kyberhyökkäys kolmen sähkönjakelusta vastaavan yrityksen ohjausjärjestelmiin ja tietovarantoihin. Erääksi mahdollisista tunkeutumiskohteita epäillään teollisuusautomaatiojärjestelmää, jonka toimintaan tunkeutujien arvioidaan päässeen käsiksi etäyhteyden kautta. Varauduttaessa teollisuuden automaatiojärjestelmiin kohdistuviin kyberhyökkäyksiin ja niiden sietokyvyn parantamiseen, organisaatioille suositellaan ensisijaiseksi toimenpiteeksi kyberturvallisuuden hallinnan parhaiden käytäntöjen käyttöönottamista. (ics-cert.us, 2016.)

Lähteet

Airaksinen, T. (2003). Tekniikan suuret kertomukset. Filosofinen raportti. Keuruu: Otavan Kirjapaino Oy.

DIMECC Oy. (2017). The finnish cyber trust program 2015–2017. The finnish cyber trust program:in loppuraportti. Saatavilla: 23.10.2015 http://cybertrust.dimecc.com/wp-content/uploads/2017/10/DIMECC717_CyberTrust.pdf

Energiateollisuus (2016). Sähköntuotanto. Energiateollisuuden internetsivusto. Saatavilla: 23.7.2018 http://energia.fi/energia-ja-ymparisto/sahkontuotanto

Helsingin Sanomat (6.1.2016). Poikkeuksellinen kyberhyökkäys onnistui sammuttamaan ukrainalaisten sähköt. Helsingin sanomien internetsivusto. Saatavilla: 23.7.2018 http://www.hs.fi/ulkomaat/a1452053903722

Huoltovarmuuskeskus (2015). Kyberturvallisuuden kehittäminen ja jalkauttaminen teollisuuteen vuonna 2014. KYBER-TEO 2014 -hankkeen tuloksia. Saatavilla: 18.7.2017 https://s3-eu-west-1.amazonaws.com/huoltovarmuuskeskus/app/uploads/2016/08/31144516/TEOSUMMARY_2015_net.pdf?AWSAccessKeyId=AKIAITCZYCPQYFESGSAQ&Expires=1532386632&Signature=%2BNGSogsw0W7sz1YmFTpomOMZ60w%3D

ics-cert.us (2016). Cyber-Attack Against Ukrainian Critical Infrastructure. Saatavilla: 20.4.2016 https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01

Knowlesa, W., Princea, D., Hutchisona, D., Ferdinand, J., Disso, P. & Jones, K. (2015). A survey of cyber security management in industrial control systems. *International journal of critical infrastructure protection 9 (2015).* Saatavilla: 25.10.2015 https://ac.els-cdn.com/S1874548215000207/1-s2.0-S1874548215000207-main.pdf?_tid=447861da-17f0-4223-8563-d7ff6013850c&acdnat=1532352262_fcc694993b2991fe9670c3615ea7a5b3

Laatuakatemia. Laatutyökaluja. Laatuakatemian internetsivusto. Saatavilla: 23.10.2015 http://www.kotiposti.net/tuurala/PDCA.htm

Lehto, M. (2015). Phenomena in the cyber world. Teoksessa Lehto, M. & Neittaanmäki, P. (toim.), *Cyber Security: Analytics, Technology and Automation* (3-29). Germany: Springer International Publishing.

Puolustusministeriö. (2015). KATAKRI – Kansallinen turvallisuusauditointikriteeristö. PowerPoint-esitys. Saatavilla: 18.7.2017 http://www.defmin.fi/files/1870/KATAKRI_versio_II.pdf

Suomen Automaatioseura ry Turvallisuusjaosto. (2010). Teollisuusautomaation tietoturva. Verkottumisen riskit ja niiden hallinta. Verkkopainos. Helsinki: Suomen Automaatioseura ry Turvallisuusjaosto. Saatavilla: 21.8.2018 https://www.viestintavirasto.fi/attachments/tietoturva/TeollisuusautomaationTietoturva.pdf

Suomen Standardisoimisliitto ry. (2016). Johdanto laadunhallinnan ISO 9000 – standardeihin. Saatavilla: 23.10.2015 www.sfsedu.fi/files/126/ISO_9000_kalvosarja_oppilaitoksille_2016.ppt

Suomen Standardisoimisliitto ry. (2012). SFS-käsikirja ISO27001. Informaatioteknologia. Turvallisuustekniikat. Tietoturvallisuuden hallintajärjestelmät. Vaatimukset.

Suomen Standardisoimisliitto SFS ry. (2015). Tietoturvallisuuden hallintajärjestelmät. ISO/IEC 27000 -standardiperhe- diasarja oppilaitoksille. Saatavilla: 18.7.2017 https://www.sfs.fi/julkaisut_ja_palvelut/tuotteet_valokeilassa/iso_iec_27000_tietoturvallisuuden_hallinta

Turvallisuuskomitea. (2014). Kansallisen kyberturvallisuusstrategian toimeenpano-ohjelma. Saatavilla: 23.7.2018 https://turvallisuuskomitea.fi/wp-content/uploads/2018/05/Kyberturvallisuusstrategian-toimeenpano-ohjelma.pdf

Turvallisuuskomitean sihteeristö. (2013). Suomen kyberturvallisuusstrategia. Suomen kyberturvallisuusstrategia - raportti. Saatavilla: 23.7.2018 https://puolustusvoimat.fi/documents/2182700/0/Kyberturvallisuusstrategia/bb56d179-9b3a-4816-806d-84c84b04da30

Valmet Automation Oy. (2018). Valmetin esittely- ja koulutusmateriaali.

World Economic Forum. The Global Risks Landscape 2015. World Economic Forumin internetsivusto. Saatavilla: 23.10.2015 http://reports.weforum.org/global-risks-2015/part-1-global-risks-2015/technological-risks-back-to-the-future/#frame/20ad6

Informaatioteknologian tiedekunnan julkaisuja
No. 57/2018

ISBN 978-951-39-7545-6 (verkkoj.)
ISSN 2323-5004

JYVÄSKYLÄN YLIOPISTO