TUTKIMUSRAPORTTI

VTT-R-00560-22

CyberFactory#1 – Tulevaisuuden tehtaiden mahdollisuudet ja uhat

Tutkimushankkeen loppuraportti

Kirjoittajat: Jarno Salonen
Markku Kylänpää
Outi-Marja Latvala
Markku Mikkola
Mirko Sailio

Luottamuksellisuus: VTT Public

Versio: 8.7.2022

Raportin nimi CyberFactory#1 – Tulevaisuuden tehtaiden mahdollisuudet ja uhat Tutkimushankkeen loppuraportti	
Asiakkaan nimi, yhteyshenkilö ja yhteystiedot Yhteisrahoitteinen Business Finland -hanke (Dnro 5192/31/2018), Matti Säynätjoki, matti.saynatjoki@businessfinland.fi	**Asiakkaan viite** Projekti 5192/31/2018 - E7632 ITEA3 CyberFactory
Projektin nimi ITEA3 CyberFactory#1	**Projektin numero/lyhytnimi** BF_ITEA3_CyFa
Raportin laatija(t) Jarno Salonen, Markku Kylänpää, Outi-Marja Latvala, Markku Mikkola ja Mirko Sailio, Teknologian tutkimuskeskus VTT	**Sivujen/liitesivujen lukumäärä** 27/-
Avainsanat Industry 4.0, kyberturvallisuus, mallintaminen, simulointi, digital twin, cyber range, kybersietoisuus, resilienssi, liiketoimintaekosysteemi, tulevaisuuden tehdas	**Raportin numero** VTT-R-00560-22

Tiivistelmä

Tämä raportti on pääosin Business Finlandin rahoittaman julkisen CyberFactory#1 -tutkimus- ja kehityshankkeen (ITEA3 17032, 2018-2022) loppuraportti. Hankkeen koordinaattorina toimi Airbus SAS Ranskasta ja hankkeessa oli mukana yhteensä 28 partneria seitsemästä maasta. VTT:n koordinoimaan Suomen konsortioon kuului turvallisia viestintä- ja liitettävyysratkaisuita kehittävä Bittium Oyj, älykkäitä ratkaisuja ruostumattomasta teräksestä mm. elintarviketeollisuudelle valmistava High Metal Oy, edistyneitä analytiikkaratkaisuja ja -palveluja mm. tekoälyn avulla tarjoava Houston Analytics Oy, kyberturvallisilla ratkaisuilla toteutettuihin kokonaisvaltaisiin IT-palveluihin keskittyvä Netox Oy sekä luotettavaan ja turvalliseen digitaaliseen kommunikointiin ratkaisuja rakentava Rugged Tooling Oy.

Hankkeessa tutkittiin ja kehitettiin ratkaisuja tulevaisuuden tehtaiden sekä näiden järjestelmien mallintamiseen ja simulointiin, laitteiden ja prosessien tehokkaampaan optimointiin tiedon avulla sekä kyberturvallisuuden ja kyber-sietokyvyn (resilienssi) parantamiseen. Käytetyt teknologiaratkaisut liittyivät muun muassa pilvipalveluihin, robotiikkaan ja tekoälyyn. Hankkeen keskeisimmät käyttötapaukset liittyivät lentokoneteollisuuteen, kuluttajaelektroniikkaan sekä tekstiili- ja elintarviketeollisuuteen. Hankkeessa tehtiin myös mm. robotiikkaan sekä tietoturvalliseen viestintään liittyvää arkkitehtuuri- ja prosessikehitystä. VTT keskittyi hankkeessa erityisesti kyberturvallisuuteen sekä mallintamiseen ja simulointiin liittyvään tutkimukseen ja sen vetovastuulla oli tulevaisuuden tehtaan dynaamiseen riskienhallintaan ja resilienssiin (kybersietoisuus) liittyvä työpaketti. Hankkeen tuloksena syntyi erilaisia menetelmiä tulevaisuuden tehtaan liiketoimintaekosysteemin ja sen eri toimijoiden mallintamiseen sekä kyberturvallisia ratkaisuja joiden avulla pystytään lisäämään tehtaan ja sen järjestelmien resilienssiä elinkaaren eri vaiheissa. Hankkeen tuloksia on julkaistu tämän tutkimusraportin lisäksi myös hankkeen aikana kirjoitetuissa yli kymmenessä konferenssi- ja muissa tieteellisessä artikkeleissa sekä hankkeen aikana järjestetyissä webinaareissa ja muissa tilaisuuksissa.

Luottamuksellisuus	VTT Public

Tampere 8.7.2022

Laatija	**Tarkastaja**
Jarno Salonen, Senior Scientisthankkeen projektipäällikkö	Jukka Julku, Research Scientist Applied Cybersecurity

VTT:n yhteystiedot
Teknologian tutkimuskeskus VTT Oy, PL 1000, 02044 VTT

Jakelu (asiakkaat ja VTT)

Projektin osapuolet
Teknologian tutkimuskeskus VTT

Hyväksyminen

TEKNOLOGIAN TUTKIMUSKESKUS VTT OY

Päivämäärä:	8.7.2022
Allekirjoitus:	DocuSigned by: Pertti Raatikainen 9EAB53457FD743E...
Nimi:	Pertti Raatikainen
Asema:	Lead, Connectivity. Projektin vastuullinen johtaja

Alkusanat

CyberFactory#1-tutkimushankkeen lähtökohtana oli saksalaiseen terästehtaaseen kahdeksan vuotta sitten kohdistunut kyberhyökkäys, joka mainittiin ensimmäistä kertaa Saksan kansallisen tietoturvaviranomaisen (BSI, Bundesamt für Sicherheit in der Informationstechnik) julkaisemassa vuosikatsauksessa[1] joulukuussa 2014. Neljä vuotta aiemmin havaittu Iranin väitettyä ydinaseohjelmaa sabotoinut Stuxnet oli siihen mennessä ainoa tiedossa ollut haittaohjelma joka oli pystynyt aiheuttamaan fyysistä vahinkoa teollisuuden ohjausjärjestelmille. BSI:n raportin ja siihen perustuvan yhdysvaltalaisen SANS-instituutin tapaustutkimuksen[2] mukaan hyökkäyksen aiheuttamat fyysiset vahingot terästehtaalle olivat mittavia. Lisäksi hyökkäyksestä aiheutuvat menetykset tuotannossa ja mainehaitta lisäsivät hyökkäyksen vaikuttavuutta. Yksityiskohtaisia tietoja hyökkäyksen kohteesta tai hyökkääjästä ei ole tiettävästi koskaan julkaistu, mutta koska tutkimushanke keskittyi neljänteen teolliseen vallankumoukseen sekä tulevaisuuden digitalisoituviin tehtaisiin, niin kriittistä tuhoa aiheuttavat kyber-fyysiset hyökkäykset ja niiden tutkiminen kyberturvallisuuden ja kybersietoisuuden näkökulmasta vaikutti äärimmäisen houkuttelevalta. Hankkeen koordinaattorina toimiva ranskalainen Airbus CyberSecurity SAS yhdessä saksalaisen vastineensa (Airbus CyberSecurity GmbH) ja espanjalaisen Airbus Defence & Space:n kanssa muodostivat vahvan perustan hankkeelle, jonka ympärille oli hyvä rakentaa hankkeen tavoitteita tukeva yhteensä 28 partnerin konsortio. Konsortioon kuuluivat edellä jo mainittujen maiden ja Suomen lisäksi myös Kanada, Portugali ja Turkki. Hankevalmistelun aikana muodostunut kansainvälinen konsortio oli erittäin yhteistyökykyinen ja Suomesta saatiin mukaan erinomainen joukko oman alansa hyvin asiantuntevia yrityspartnereita eri toiminta-alueilta.

Tutkimushanke käynnistyi joulukuussa 2018 ja tammi-helmikuun vaihteessa 2020 projektikonsortio oli Oulussa valmistautumassa ensimmäiseen ITEA Review -tilaisuuteen, kun uutisissa mainittiin ensimmäinen Suomessa havaittu koronapandemiatapaus. Pandemian johdosta tuon konsortiokokouksen jälkeen hankkeessa siirryttiin virtuaalimoodiin sekä kotimaassa että kansainvälisesti koko projektin loppuajaksi. Toisaalta pandemia kasvatti etätyön ja virtuaalikokousten ohella erilaisten digitaalisten ratkaisujen ja palveluiden tarvetta ja siten myös projektin tutkimuksen ja tuotekehityksen merkitystä projektin kohderyhmänä olevalle teollisuudelle ja osittain myös yhteiskunnalle. Tätä kirjoitettaessa pandemia ei vaikuta olevan vielä ohi eikä paluuta entiseen pidetä edes kovin todennäköisenä. Yksi asia on kuitenkin varmaa: digitalisaatio on tullut ja pysyy.

Haluamme kiittää kaikkia projektikonsortion jäseniä ja erityisesti kotimaisia yrityspartnereita (Bittium, High Metal, Houston Analytics, Netox ja Rugged Tooling) näistä kolmesta ja puolesta vuodesta, jonka ajan teimme yhteistyötä projektin tutkimuksen ja kehityksen parissa. Lisäksi esitämme kiitokset Business Finlandille hankkeen rahoittamisesta ja siten mahdollisuudesta tehdä näin mielenkiintoista tutkimusta kansainvälisessä ITEA-hankkeessa.

Tampereella 8.7.2022

Tekijät

[1] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2014.pdf (viitattu 8.7.2022)
[2] https://assets.contentstack.io/v3/assets/blt36c2e63521272fdc/bltc79a41dbf7d1441e/607f235775873e466bcc539c/ICS-CPPE-case-Study-2-German-Steelworks_Facility.pdf (viitattu 8.7.2022)

Sisällysluettelo

Alkusanat 3
1. Johdanto 5
   1.1 Hankkeen konsortio ja rakenne 5
   1.2 Hankkeen koordinointi ja yhteistyö 7
   1.3 Rajaukset VTT:n hankkeessa suorittamaan tutkimustyöhön 8
2. Projektissa tehty tutkimus ja keskeisimmät tulokset 9
   2.1 Tulevaisuuden tehtaiden mallintaminen ja simulointi 9
      2.1.1 Kirjallisuuskatsauksen yhteenveto 9
      2.1.2 Lähestymistapa ekosysteemin liiketoiminnalliseen mallintamiseen 9
      2.1.3 Liiketoiminnan mallinnuselementit 10
      2.1.4 Mallinnusprosessi 12
      2.1.5 Yhteenveto ja johtopäätökset ekosysteemimallinnuksesta 12
   2.2 Tulevaisuuden tehtaiden resilienssi 12
      2.2.1 Etätodentaminen 13
      2.2.2 Elintarvikeprosessien kyberturvallisuuden simulointi kyberharjoitteluympäristöissä 14
      2.2.3 Tekoälyn ja visualisoinnin hyödyntäminen poikkeamien havainnoimisessa 14
      2.2.4 Organisaation kyberturvallisuuden kypsyyden mittaaminen 15
3. Projektin julkaisut ja viestintä 20
   3.1 Hankkeen aikana tuotetut julkaisut 20
   3.2 Hankkeen aikana suoritettu muu viestintä 21
4. Yhteistyö ja jatkosuunnitelmat 23
   4.1 Yhteistyö ja verkottuminen kotimaassa 23
   4.2 Yhteistyö ja verkottuminen kansainvälisesti 23
   4.3 Muu yhteistyö 24
   4.4 Hankkeessa tehdyn tutkimuksen ja tulosten hyödyntäminen projektin jälkeen 24
5. Yhteenveto 26
6. Lähdeviitteet 27

1. Johdanto

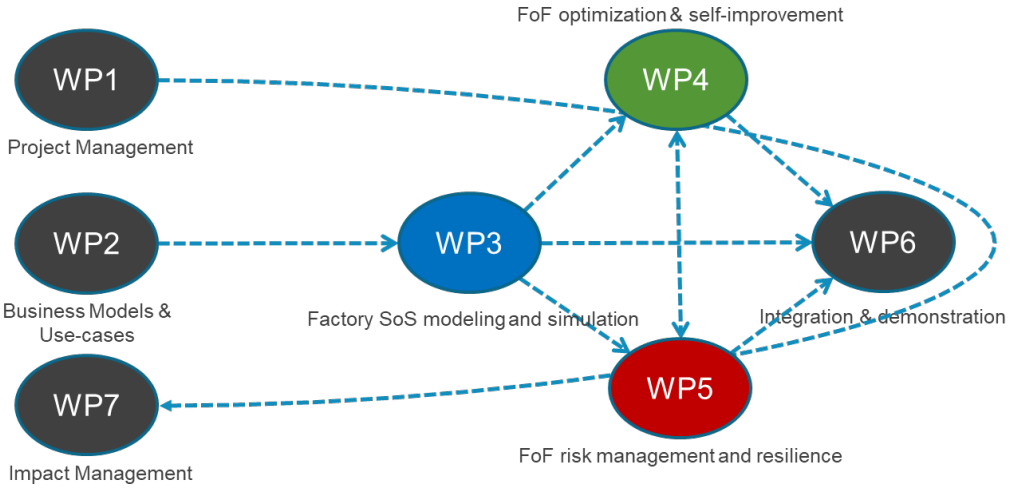
CyberFactory#1 (CF#1) -hankkeen tavoitteena oli suunnitella, kehittää, integroida ja demonstroida joukko kyvykkyyksiä, joiden avulla voidaan parantaa tulevaisuuden tehtaiden (Factory of the Future, FoF) optimointia ja toimintavarmuutta. Projekti vastasi eri teollisuudenaloilla tunnistettuihin tarpeisiin, kuten yhteisöllinen tuotekehitys, laitteiden itsenäinen asetusten uudelleenmääritys, tuotteiden jatkuva parantaminen, hajautettu valmistus sekä reaaliaikainen tilannetietoisuus. Projektissa kehitettiin myös kyvykkyyksiä, jotka suojaavat ja parantavat tulevaisuuden tehtaiden kykyä vastata sekä kyberuhkiin, että fyysisiin uhkiin, sekä myös muihin turvallisuusasioihin. Kehitetyt kyvykkyydet pyrittiin demonstroimaan realistisessa ympäristössä, joka kuvastaa erilaisia tehdastyyppejä joita tulevaisuudessa voi olla, kuten käyttäjäkeskeinen tehdas tai oppimistehdas, ottaen huomioon liiketoimintamallien muutokset, kuten tuotteiden muutos palveluiksi tai erilaisten datapalveluiden kehittäminen tuotannon päälle.

1.1 Hankkeen konsortio ja rakenne

CF#1 oli ITEA-tutkimushanke, joka käynnistyi joulukuussa 2018 ja päättyi kesäkuussa 2022. Hanketta koordinoi ranskalainen Airbus CyberSecurity SAS[3] ja siihen osallistui 28 partneria seitsemästä eri maasta (Espanja, Kanada, Portugali, Ranska, Saksa, Suomi ja Turkki). Suomesta hankkeeseen osallistui maakoordinaatorina toimivan VTT:n lisäksi Bittium, High Metal, Houston Analytics, Netox ja Rugged Tooling. Suomen konsortio sai tutkimusrahoitusta hankkeeseen Business Finlandilta aikavälillä 1.1.2019-31.12.2022 (hanketunnus: E7632 ITEA3 CyberFactory). Johtuen kansainvälisen hankkeen hitaasta käynnistymisestä, joka aiheutui muutamien maiden rahoituspäätösten viivästymisestä sekä Ranskan konsortion vetäytymisestä kokonaan hankkeesta rahoituksen puuttuessa, Suomen konsortio haki muiden maiden tavoin jatkoaikaa projektille Business Finlandilta ja se myönnettiin loppuvuonna 2021, jolloin päättymispäiväksi asetettiin 18.6.2022[4] kansainvälisen ITEA-hankkeen päättymispäivän mukaan.

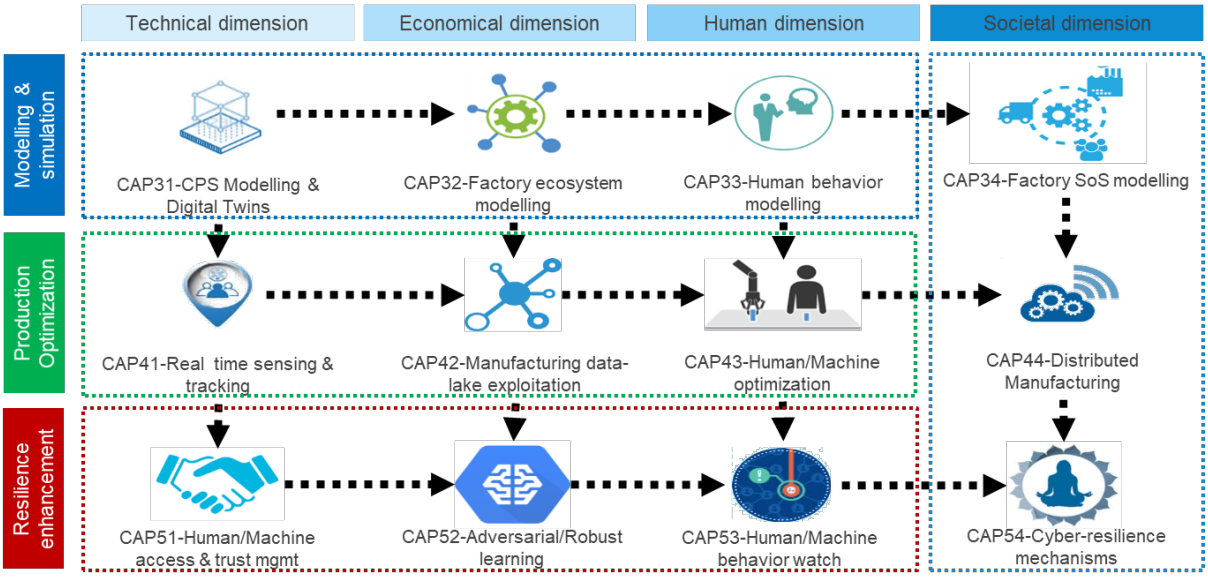
Hanke koostui kolmesta teknisestä työpaketista, joista WP3 keskittyi tulevaisuuden tehtaan järjestelmien mallintamiseen ja simulointiin, WP4:n näkökulmana oli tehtaan ja sen järjestelmien optimointi ja WP5 kehitti ratkaisuja parantamaan tehtaan riskienhallintaa ja kybersietoisuutta perinteisen tehdasturvallisuuden ja erityisesti kyberturvallisuuden näkökulmasta. Hankkeen työpaketit ja kokonaisrakenne on esitetty seuraavassa kuvassa.

[3] Airbus koordinoi hanketta omarahoituksella johtuen Ranskan rahoituspäätöksen viivästymisestä yli vuodella. Rahoituspäätös oli lopulta kielteinen, jonka vuoksi koko muu Ranskan konsortio vetäytyi hankkeesta.
[4] Muista Suomen konsortion partnereista poiketen Houston Analytics Oy ei hakenut jatkoaikaa vuodelle 2022



Kuva 1. CyberFactory#1-hankkeen rakenne

Projektin tavoitteena oli kehittää kyvykkyyksiä tulevaisuuden tehtaan simuloinnin ja mallintamisen, optimoinnin ja tehdas- ja kyberturvallisuuden tarpeisiin. Tavoitellut kyvykkyydet - yhteensä 12 kappaletta - oli jaettu neljään eri kategoriaan; tekninen, taloudellinen, inhimillinen ja yhteiskunnallinen, joista jokaiseen oli määritelty yksi kyvykkyys työpakettia kohti seuraavan kuvan mukaisesti.

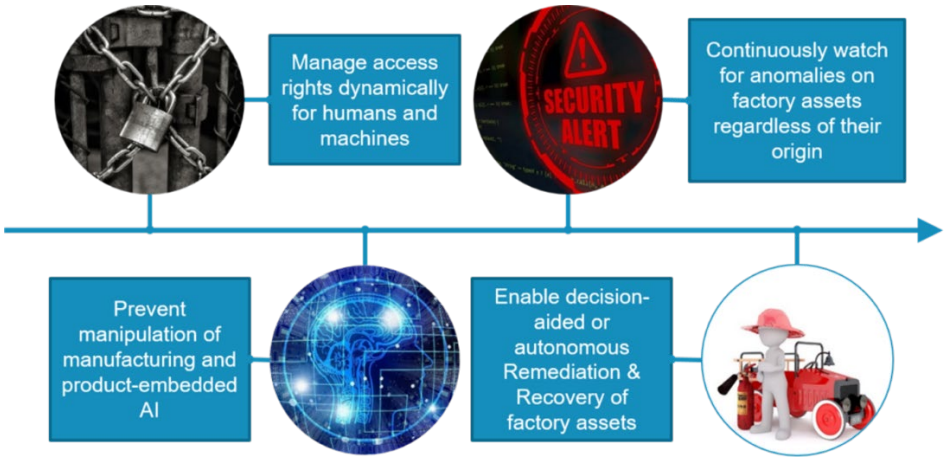


Kuva 2. Hankkeessa tavoitellut teknologiset ja muut kyvykkyydet

Edellä mainitut kyvykkyydet oli projektissa kiinnitetty suoraan työpakettien tehtäviin ja esim. VTT:n vastuulla olevan WP5 FoF (Dynamic Risk Management and) Resilience -työpaketin tehtävät oli nimetty kyvykkyyksien mukaan seuraavasti:

- T5.1 Human/Machine access & trust management
- T5.2 Robust learning ability
- T5.3 Human/Machine behavior watch
- T5.4 Cyber-resilience capabilities

Seuraavassa kuvassa esitetään edellä mainitut tehtävät hieman yksityiskohtaisemmin. Kahden vasemmanpuolimmaisen tehtävän (T5.1 ja T5.2) rooli tulevaisuuden tehtaan elinkaaren osalta oli toimia ennakoivasti ja määritellä rajat mm. tietoturvapolitiikan ja käyttöoikeushallinnan, mutta myös tehtaassa käytettävän uudenlaisen teknologian - tässä tapauksessa tekoälyn - käytölle. Kaksi oikeanpuolimmaista tehtävää (T5.3 ja T5.4) kehittivät reaktiivisia ratkaisuja, joiden avulla voidaan havaita kyberhyökkäyksiä tai muita vastaavanlaisia poikkeamia (anomalioita) tehtaissa, jotta niihin voidaan reagoida ja vastata. Reagointi käsitti käytännössä myös harjoittelemista katastrofitilanteita varten eli esim. täydellistä tehtaan tai sen yksittäisten laitteiden menettämistä kyberhyökkäyksen johdosta, jolloin tehtävänä on palauttaa tehdas takaisin hallintaan mahdollisimman tehokkaasti niin aikataulun kuin tehtävien toimenpiteidenkin näkökulmasta.



Kuva 3. VTT:n vetämän FoF Resilience -työpaketin tehtävärakenne

Myös muiden työpakettien tehtävät oli linkitetty vastaavalla tavalla toisiinsa sekä projektin tavoitteena oleviin kyvykkyyksiin.

1.2 Hankkeen koordinointi ja yhteistyö

Projektin koordinointiin liittyvää päätöksentekoa toteutettiin paitsi 12 kertaa projektin aikana järjestettävissä konsortiokokouksissa niin myös neljän viikon välein järjestetyissä WP1 Project Management -työpaketin online-kokouksissa, joihin osallistuivat kaikki partnerit. Kokouksissa käytiin yleensä eri maiden rahoitustilanne sekä operatiivinen tilanne (esim. matkustusrajoitukset koronapandemian aikana) läpi sekä erikseen työpakettien eteneminen, minkä vuoksi kokouksissa mukana oli aina myös käynnissä olevien työpakettien vetäjät yksittäisten partnerien edustajien lisäksi. Projektin käynnistyskokous järjestettiin Sevillassa, Espanjassa joulukuussa 2018 ja fyysisiä kokouksia ehdittiin pitää säännöllisesti ensimmäiseen ITEA Review -tilaisuuteen saakka tammikuun lopussa 2020, jonka jälkeen siirryttiin kokonaan virtuaalisiin ja osittain hybridimuotoisiin konsortiokokouksiin, joita järjestettiin projektin päätöskokoukseen ja ITEA Final Review-tilaisuuteen saakka toukokuussa 2022.

Edellisen lisäksi jokaisella rahoitetulla maalla oli oma ohjausryhmä tai vastaava, joka kokoontui säännöllisin väliajoin. Suomen konsortion johtoryhmä kokoontui yhteensä 12 kertaa projektin aikana pyrkien järjestämään kokoukset lähellä konsortiokokouksen ajankohtaa ja koostui jokaisen partnerin edustajasta, Business Finlandin edustajasta sekä VTT:n projektipäälliköstä, joka toimi kokouksen sihteerinä. Suomen konsortion eri partnerit toimivat kokouksen puheenjohtajana vuorotellen. Business Finlandin edustajana kokouksissa toimi Matti Säynätjoki. Myös Suomen konsortio kokoontui ensin fyysisesti Oulussa ja pääkaupunkiseudulla, mutta huhtikuusta 2020 lähtien kokoukset järjestettiin

kokonaan virtuaalisesti Teamsissa ja vasta projektin päätöskokous 7.6.2022 järjestettiin fyysisesti Oulussa, tosin muutama etäosallistuja huomioiden.

Konsortiokokousten lisäksi jokainen työpaketti järjesti säännöllisiä online-kokouksia oman elinkaarensa aikana. Näitä 45 minuutin pituisia kokouksia järjestettiin yleensä noin kahden viikon välein jokaisessa työpaketissa ja ne sijoittuivat yleisimmin torstai-iltapäivään. Kokouksissa puheenjohtajana toimi työpaketin vetäjä ja niissä käsiteltiin tutkimus- ja kehitystyön etenemistä työpaketin eri tehtävissä. Näiden säännöllisten kokousten lisäksi konsortiokokouksissa oli yleensä varattu aikaa eri työpakettien sisäisille kokouksille ja työpaketit ja/tai tehtävät saivat järjestää myös erillisiä online-työpajoja tai -kokouksia projektin aikana.

1.3 Rajaukset VTT:n hankkeessa suorittamaan tutkimustyöhön

VTT teki CF#1-hankevalmistelun aikana päätöksen keskittyä enemmän mallinnukseen ja simulointiin sekä kyberturvallisuuteen ja kybersietoisuuteen. Tämä tarkoitti sitä, että resurssit WP4 FoF optimization -työpaketissa jäivät lopulta niin vähäisiksi, että lopulta VTT jättäytyi koko työpaketista pois. VTT teki hieman yhteistyötä kotimaisten ja kansainvälisten partnerien kanssa optimointiin liittyvässä tutkimuksessa ja kehityksessä, mutta keskittyi niissä simuloinnin ja mallintamisen sekä kyberturvallisuuden ja kybersietoisuuden näkökulmaan. Vaikka VTT:n tutkijoita osallistui satunnaisesti myös WP4-työpaketin kokouksiin, niin yhteistyö ei kuitenkaan laajentunut työpaketin julkisen state-of-the-art -raportin tekemiseen tai muuhun deliverable-työhön.

2. Projektissa tehty tutkimus ja keskeisimmät tulokset

Tässä luvussa käsitellään projektissa tehtyä tutkimusta ja sen keskeisimpiä tuloksia kattaen VTT:lle keskeisten työpakettien WP3 Factory SoS Modelling and Simulation sekä WP5 FoF Dynamic Risk Management and Resilience ja niiden eri tehtävissä (task) suoritettua työtä.

2.1 Tulevaisuuden tehtaiden mallintaminen ja simulointi

Tässä kappaleessa kuvataan projektin työpaketin WP3 Factory SoS Modelling and Simulation tehtävässä T3.2 Factory ecosystem modelling tehtyä tutkimustyötä, joka kohdistui liiketoimintaekosysteemien mallintamiseen. Työ alkoi kirjallisuuskatsauksella ekosysteemien mallintamisen erilaisiin lähestymistapoihin ja jatkui lähestymistavan kehittämisellä erityisesti ekosysteemin taloudellisten ja organisatoristen yhteyksien mallintamiseen.

2.1.1 Kirjallisuuskatsauksen yhteenveto

Liiketoimintaekosysteemien tarkastelu kattaa hyvin laajasti erilaisia toimintoja ja eri toimijoiden näkökulmia. Siitä johtuen ekosysteemitarkastelujen ja -analyysien toteuttamiseksi on olemassa myös laaja valikoima lähestymistapoja ja menetelmiä. Lähestymistapojen laajuudesta huolimatta yhteisiäkin piirteitä löytyy. Organisaation näkökulmasta lähestymistavat vastaavat sellaisiin kysymyksiin, kuten ketkä ovat ekosysteemin avaintoimijoita, mitä resursseja ne tarjoavat ekosysteemille ja mitkä ovat niiden subjektiiviset tavoitteet ja kannustimet osallistua ekosysteemiin. Liiketoimintaprosessien näkökulmasta eri lähestymistavat mallintavat toimijoiden välisiä yhteyksiä, eli mitkä tapahtumat laukaisevat toimijoiden välisiä aktiviteetteja ja miten työprosessit, materiaalivirrat ja arvovirrat kulkevat kumppanien välillä. Mallintamisen yksityiskohtaisuus riippuu siitä, minkälaisia analyysejä varten niitä tehdään. Tämän suhteen on tunnistettavissa kolmen tason tarkasteluja: strateginen taso, arvonmuodostustaso ja teknologinen taso. Ne voidaan linkittää organisaatio-prosessi-näkökulmiin siten, että strateginen taso pohtii asioita enemmän organisaation näkökulmasta, arvotason tarkastelu puolestaan tutkii liiketoimintaprosesseja ja teknologiataso vie analyysit yksityiskohtaisimpiin teknisiin ratkaisuihin (Cyberfactory#1 -projektiraportti, 2020).

Yritysekosysteemien eri näkökulmien määrän ja mahdollisten analyysitasojen laajuuden vuoksi on haastavaa tunnistaa yleisiä tarpeita joiden pohjalta kehittää mallinnuslähestymistapoja tai -työkaluja. Yksityiskohtaisemmalle analyysitasolle siirtyminen ja esimerkiksi taloudellisiin simulaatiomalleihin tähtääminen tuo esiin yhden perustavanlaatuisen haasteen. Koska ekosysteemin kumppanit ovat itsenäisiä liiketoimijoita, he eivät ole kovin innokkaita jakamaan yksityiskohtaisia taloudellisia tietoja. Vastaava voi koskea myös kyberturvallisuuteen liittyvien tietojen jakamista. Kirjallisuuskatsauksen yhteenvetona voitiinkin todeta, että ekosysteemin toiminnan mallintamisen laajuus ja yksityiskohdat riippuvat kyseisen ekosysteemin erityistilanteesta ja ominaisuuksista (Cyberfactory#1 -projektiraportti, 2020).

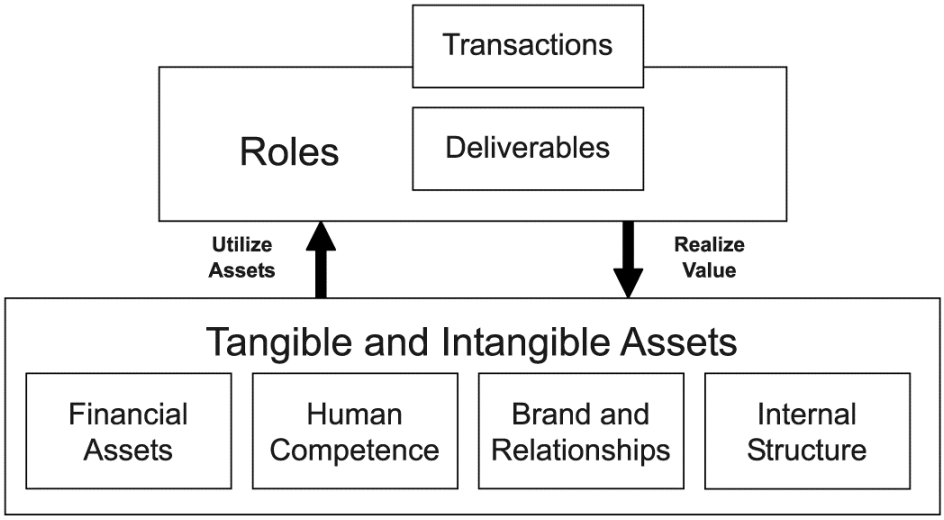
2.1.2 Lähestymistapa ekosysteemin liiketoiminnalliseen mallintamiseen

Ekosysteemimallinnuksen osalta erityisesti organisaatio- ja liiketoimintamallinäkökulmasta työ perustettiin kirjallisuuskatsausta laadittaessa tunnistettuun Value Network Analysis (VNA) -konseptiin (Allee, 2009). VNA:n tavoitteena on tuottaa kattava kuvaus siitä, missä liiketoimintaverkostossa arvo on ja miten arvoa luodaan. VNA:ssa on seuraavat perusvaiheet (Peppard & Rylanderin, 2006):

1. Määritä verkosto
2. Tunnista ja määrittele verkoston toimijat
3. Määrittele arvo, jonka kukin toimija katsoo saavansa ollessaan verkon jäsen

4. Tunnista ja kartoita verkoston toimijoiden keskinäiset vaikutukset
5. Analysoi ja muotoile verkostokuvaus

Arvoverkostoon osallistujat, joko yksin tai kollektiivisesti, hyödyntävät aineellista ja aineetonta omaisuuspohjaansa ottamalla tai luomalla rooleja, jotka muuttavat kyseiset omaisuudet siirtokelpoisemmiksi arvomuodoiksi, jotka voidaan luovuttaa muille rooleille kaupan toteuttamisen kautta. Arvoverkoston osallistujat puolestaan ymmärtävät saatujen suoritteiden arvon muuttaessaan ne aineellisten tai aineettomien hyödykkeiden hyödyiksi tai parannuksiksi itselleen. Seuraavassa kuvassa esitetty arvonmuunnon mallinnuskehikko havainnollistaa tätä toimijakohtaista arvon muuntamista.



Kuva 4. Ekosysteemitoimijan arvonmuunnon mallinnuskehikko (Allee, 2009)

Arvoverkostoa mallinnettaessa tulee ensin kartoittaa arvonvaihdot verkoston yli. Tässä kartoitusmenetelmässä on kolme yksinkertaista elementtiä – roolit, transaktiot ja toimitteet:

1. **Rooleissa (roles)** toimivat verkoston osallistujat. He tuovat verkostoon panoksia ja suorittavat tehtäviä. Osallistujilla on valta aloittaa toimintaa, osallistua vuorovaikutukseen, lisätä arvoa ja tehdä päätöksiä. He voivat olla yksilöitä; pieniä ryhmiä tai liiketoimintayksiköitä, organisaatiot; erilaisia yhteisöjä; tai jopa kansallisvaltioita.
2. **Transaktiot (transactions)** lähtevät liikkeelle yhdeltä osallistujalta ja päättyvät toiseen. Nuolet osoittavat kahden roolin välisen toiminnan suunnan. Kiinteät viivat ovat muodollista vaihdantaa tuotteiden ja tulojen suhteen, kun taas katkoviivat kuvaavat markkinainformaation ja -etujen aineettomia virtoja.
3. **Toimitteet (deliverables)** ovat todellisia "asioita", jotka siirtyvät roolista toiseen. Toimitettava asia voi olla fyysinen (esim. asiakirja tai taulukko) tai se voi olla ei-fyysinen (esim. viesti tai pyyntö, joka toimitetaan vain suullisesti). Se voi myös olla tietyntyyppistä tietoa, asiantuntemusta, neuvoja tai tietoa jostain palvelusta tai edusta, joka annetaan vastaanottajalle.

2.1.3 Liiketoiminnan mallinnuselementit

Yritysten ekosysteemejä voidaan analysoida ja mallintaa monesta eri näkökulmasta. Tässä keskitymme ekosysteemin liiketoimintamahdollisuuksien taloudelliseen analyysiin ja siihen, miten sitä voitaisiin lähestyä. Analysoidaksemme uutta liiketoimintamallimahdollisuutta tiivistimme joitakin keskeisiä elementtejä kirjallisuudessa esitetyistä malleista. Liiketoimintamallin näkökulmasta seuraavat keskeiset elementit tunnistettiin oleelliseksi huomioida ja analysoida arvioitaessa liiketoimintaekosysteemin eri konfiguraatiovaihtoehtoja.

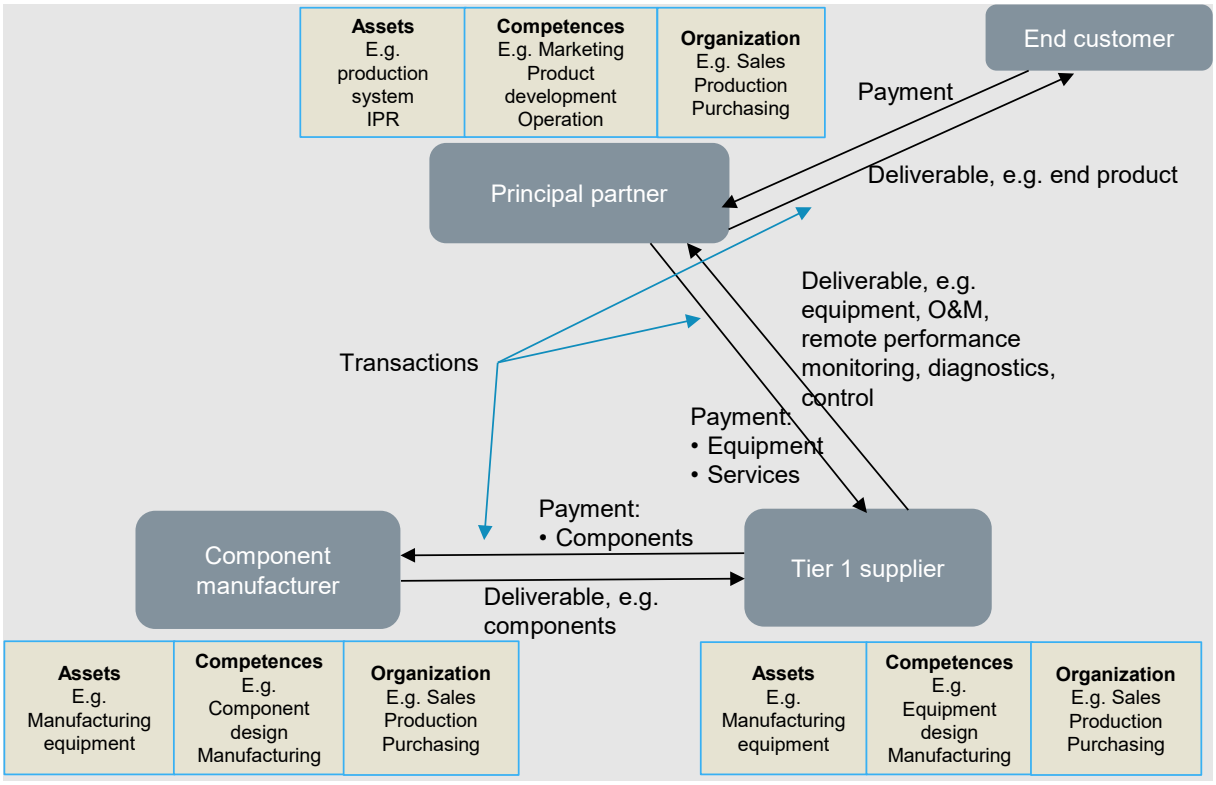
Liiketoimintaekosysteemin liikevaihto: tämä on yleensä (etenkin perinteisessä toimitusketjuekosysteemissä) pääyrityksen (tai sen liiketoimintayksikön) tuloa. Tämä tuotto jaetaan edelleen ekosysteemin muiden sidosryhmien (toimittajien) kanssa erilaisten liiketoimien kautta.

Liiketapahtumat kumppanien välillä: nämä ovat erilaisia toimintoja ja mekanismeja arvon ja tulojen vaihtamiseksi kumppanien välillä. Tyypillisesti arvo, samoin kuin hinta, kulkeutuu tuotteissa ja palveluissa, joita kumppanit tarjoavat toisilleen. Tuloihin liittyvät tapahtumat voidaan konfiguroida monella eri tavalla, esim. suoraan tuotteen/palvelun kauppaan tai pitkäaikaisena kiinteänä palvelumaksuna.

Kumppaneiden investoinnit: kumppaneiden on tehtävä investointeja palvellakseen yhteistyössä ekosysteemin tuottoa. Nämä investoinnit voidaan tehdä aineellisiin tai aineettomiin hyödykkeisiin tai molempiin. Aineellisia investointeja ovat tyypillisesti laitteet ja koneet, aineettomat hyödykkeet ovat mm. T&K-toiminnan organisaation osaaminen ja IPR. Laitteisiin ja koneisiin tehdyt investoinnit ovat yksi keskeinen toimenpide käyttökustannusten arvioinnissa.

Kumppaneiden henkilöstö: jokaisen organisaation keskeinen voimavara on henkilöstö, johon sisältyy yrityksen osaaminen ja inhimillinen pääoma. Tarvittavan henkilöstörakenteen ja eri kumppanien panostusten analysointi antaa keskeistä tietoa toimintakustannusten arvioinnille.

Arvoverkostoanalyysi (Allee, 2009) tarjoaa käyttökelpoisen viitekehyksen ekosysteemien konfiguraatioiden ja eri sidosryhmien suhteiden visualisointiin. Seuraava kuva havainnollistaa yksinkertaista liiketoimintaekosysteemiä kuvaten kolmen toimijan kaksitasoista toimitusketjua, joka koostuu pääyrityksestä (lopputuotteen valmistaja) ja sen tason 1 toimittajasta ja tason 2 komponenttitoimittajasta.



Kuva 5. Liiketoimintaekosysteemin yleiset mallinnuselementit (Lähde: CyberFactory#1 Deliverable 3.2 Factory Ecosystem Modelling)

2.1.4 Mallinnusprosessi

Ekosysteemimallinnusprosessille tunnistimme ja määritimme seuraavat avainvaiheet Alleen (2009) ja Peppard & Rylanderin (2006) arvoverkostomallinnuskonseptien perusteella:

1. Tunnista ekosysteemin sidosryhmät/kumppanit
2. Tunnista ja määrittele arvolupaus ja suoritukset, joita kumppanit tarjoavat toisilleen ekosysteemissä
3. Määrittele kunkin kumppanin keskeiset voimavarat ja osaaminen
4. Tunnista ja määrittele kumppanien väliset liiketoimet
5. Analysoi ja määrittele ekosysteemin tulot, jotka jaetaan transaktioiden kautta
6. Analysoi ja määrittele taloudelliset investoinnit (esim. tuotantoresurssit, organisaatio), jotka kunkin kumppanin on tehtävä tuottaakseen arvoa ekosysteemille
7. Määritä valinnaiset tapahtumat ja konfiguraatiot ekosysteemikumppaneiden välillä
8. Analysoi eri tapahtumamallien ja/tai ekosysteemikonfiguraatioiden vaikutus liiketoimintaan
9. Vertaa eri liiketoimintaekosysteemimalleja

2.1.5 Yhteenveto ja johtopäätökset ekosysteemimallinnuksesta

Kehitettyä lähestymistapaa on tarkoitus käyttää tulevaisuuden liiketoimintamahdollisuuksien analysoinnissa ja arvioinnissa. Mahdollisia tulevaisuuden liiketoimintakonsepteja tutkittaessa ja arvioitaessa on tehtävä tulevaisuuteen suuntautuneita oletuksia, mikä tarkoittaa, että on hyväksyttävä myös arvioituihin liiketoimintalukuihin liittyvä epävarmuus. Suurinvestoinnit ja välittömät työvoimakustannukset ovat suhteellisen helppoja arvioida, mutta esimerkiksi välillisten kustannusten tarkempi huomiointi ja analysointi voi olla haastavaa tai ainakin työlästä. Tästä arvioinnin epävarmuudesta johtuen ei ehkä ole mahdollista pyrkiä kovin yksityiskohtaiseen mallinnukseen ja simulointiin. Konseptien vertailua varten kaikkien elementtien ja tekijöiden sekä niihin liittyvien kustannusten yksityiskohtainen analysointi ei välttämättä ole edes tarpeen, koska voidaan keskittyä vain tekijöihin, joilla on merkitystä vertailtavien palvelumallien välisten erojen tunnistamisessa ja arvioinnissa. Toisin sanoen analyysit eivät välttämättä tuota absoluuttisia lukuja tietystä mallista, vaan lukuja, jotka ovat vertailukelpoisia vaihtoehtoisten mallien kanssa.

Yksi perustavanlaatuinen epävarmuutta aiheuttava tekijä ekosysteemin taloudellisissa arvioissa on se, että sidosryhmien väliset suhteet ovat usein löyhästi kytköksissä, jolloin kumppanit eivät välttämättä halua jakaa liiketoimintatietojaan muille. Tämä on tilanne varsinkin silloin, kun ekosysteemisuhteet ovat alkuvaiheessa. Jopa kypsemmissä suhteissa, joissa luottamus on rakennettu pitkällä aikavälillä, halukkuus taloudellisten tietojen jakamiseen on todennäköisesti hyvin rajallista.

Yllä kuvatuista rajoituksista huolimatta liiketoimintaekosysteemin taloudellisen analyysin lähestymistapa auttaa ymmärtämään ekosysteemin suhteita ja mahdollisia konfiguraatioita eri liiketoimintamalli-mahdollisuuksien suhteen. Vaikka lähestymistapa ei välttämättä tuota täysin analyyttisiä ja absoluuttisia tuloksia, mallinnuskehys tukee kumppaneita keskustelussa yhteisestä liiketoimintamahdollisuudesta ja yhteisen kehittämistoiminnan suunnittelussa.

2.2 Tulevaisuuden tehtaiden resilienssi

Tässä kappaleessa kuvataan projektin työpaketissa WP5 FoF Dynamic Risk Management and Resilience ja sen tehtävissä T5.1 Human/Machine Access & Trust Management, T5.3 Human/Machine Behavior Watch sekä T5.4 Cyber-resilience Capacity tehtyä tutkimus- ja kehitystyötä ja niiden tuloksia. Työn tarkempi sisältö sekä tulokset on kuvattu projektin luottamuksellisissa ITEA-deliverable -raporteissa. Tämä tutkimusraportti kertoo yhteenvedon VTT:n suorittamasta ei-luottamuksellisesta tutkimustyöstä, jota on kuvattu mm. projektin sivuilla julkaistuissa blog-artikkeleissa sekä muissa konferenssi- ja tieteellisissä artikkeleissa, joita on lueteltu erikseen luvussa 3. ”Projektin julkaisut ja viestintä”.

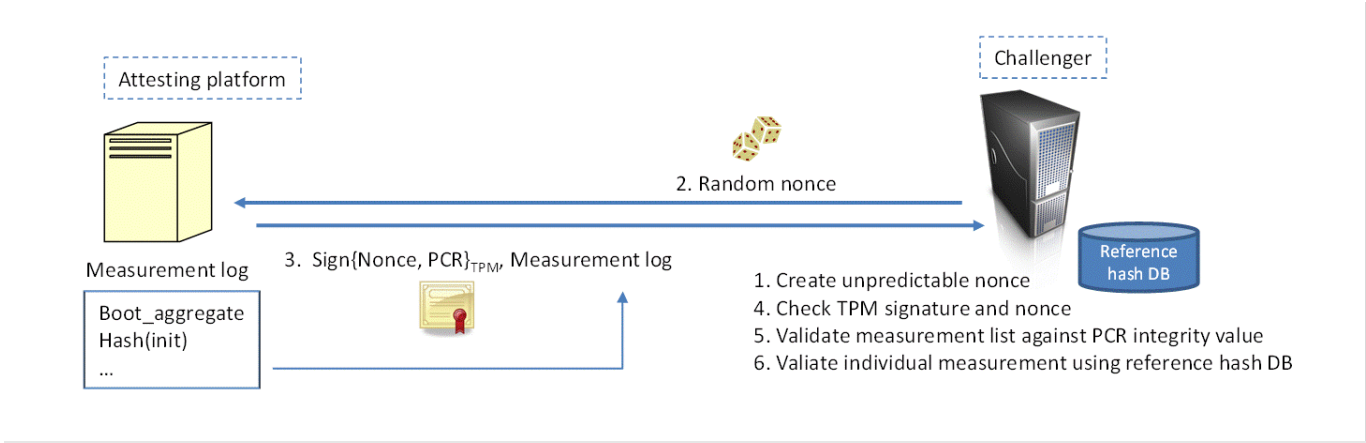
2.2.1 Etätodentaminen

Projektissa tutkittiin mekanismeja, joilla voitaisiin monitoroida tehdaslaitteiden ohjelmistojen eheyttä ja varmistaa, että ohjelmistokirjanpito todella vastaa laitteisiin asennettuja versioita ja havaita poikkeamat.

Tulevaisuuden tehdas koostuu lukuisista yhteen kytketyistä IIoT-laitteista, joiden ohjelmistoversioiden ja turvallisuuskorjausten ylläpito vaatii jatkuvaa työtä. Se on kuitenkin välttämätöntä, koska muuten vanhat ohjelmaversiot ja korjaamattomat haavoittuvuudet tarjoavat mahdollisuuden hyökkääjille tunkeutua tehdasjärjestelmiin. Hyökkääjät voivat esimerkiksi sabotoida tehtaan toimintaa, liittää tehdaslaitteita bot-verkkoon, väärinkäyttää tehtaan laskentaresursseja kryptovaluuttojen louhintaan tai lukita tehdaslaitteita ja vaatia lunnaita niiden avaamisesta. Aiemmin tehdasverkot olivat eristettyjä verkkoja, joita ei kytketty Internet-verkkoon, jolloin ne olivat suojassa verkon kautta tulevilta etähyökkäyksiltä. Tulevaisuuden tehtaassa tämä jako on kuitenkin suureksi osaksi poistunut ja tehdasjärjestelmät kommunikoivat Internetin yli joko suoraan tai jonkin välityspalvelimen kautta. Nämä yhteydet mahdollistavat myös hyökkäysyritykset. Lisäksi ei voida enää välttämättä olettaa tehdastilan fyysisen suojauksen olevan riittävällä tasolla, koska tehdastilassa voi liikkua paljon alihankkijoita ja muuta tilapäistyövoimaa sekä näiden hallinnoimia laitteita, mikä vaikeuttaa valvontaa. Tehdasverkossa voi olla asennettuna luvattomia monitorointilaitteita tai jopa osa tehdaslaitteiden ohjelmistoista voi olla korvattu muokatuilla versioilla.

Näiden syiden vuoksi on välttämätöntä, että tulevaisuuden tehtaan tietoturva tulee ottaa huomioon jo suunnitteluvaiheessa ja tietoturvaratkaisujen tulee kattaa tietokonejärjestelmien lisäksi myös mikrokontrollerityyppiset laitteet. Tietoturvaratkaisujen perustana tulee olla väärentämätön laiteidentiteetti ja siihen liitetyt salausavaimet. Tämä vaatii laitteistopohjaisia ratkaisuja, joista tunnetuin on Trusted Platform Module (TPM), joka on yleensä PC-laitteistoissa mukana. Myös muissa järjestelmissä on ominaisuuksia, jotka mahdollistavat väärentämättömän laiteidentiteetin. Eräs käyttötapaus tälle teknologialle on järjestelmän eheyden mittaus käynnistysvaiheessa. Käynnistysvaiheessa ohjelmakomponentti laskee kryptografisen tiivisteen (esimerkiksi SHA256) seuraavan vaiheen ohjelmakomponentista ennen kuin luovuttaa kontrollin sille ja tallentaa sitten mittaustuloksen eheyssuojattuun tallennustilaan. Näistä mittaustuloksista voi samalla tunnistaa laitteistossa käytetyn ohjelmistoversion.

Luotettavia eheysmittaustuloksia on myös mahdollista hyödyntää koko järjestelmän eheyden varmistamisessa. Etätodentaminen (remote attestation) välittää mittaustiedot toiseen järjestelmään, joka voi sitten verifioida tiedot ja verrata niitä esimerkiksi ohjelmistotietokantaan. TPM:ää hyödyntävä prosessi on kuvattu seuraavassa kuvassa.



Kuva 6. Etätodentamisen prosessikuva (Lähde: Kylänpää & Salonen, 2022)

Edellä olevassa kuvassa etätodennettavalle järjestelmälle lähetetään haasteviesti, joka sisältää satunnaisluvun. Etätodennettava järjestelmä allekirjoittaa (TPM:ään sidotulla sertifioidulla avaimella) datalohkon, jossa on eheysmittauksista johdettu tieto (tässä tapauksessa TPM:n PCR-rekisterit) sekä

haasteviestissä saatu satunnaisluku. Tämä allekirjoitettu datalohko välitetään sitten vasteviestinä haasteen lähettäjälle yhdessä mittauslokin kanssa. Lähettäjä voi varmistaa datalohkon allekirjoituksen ja satunnaisluvun ja sen jälkeen todentaa, että mittauslokin perusteella päädytään samoihin TPM:n PCR-rekisterin arvoihin, jotka olivat allekirjoitetussa datalohkossa ja tämän jälkeen vielä verrata näitä mittausarvoja viitearvoihin. Vastaava toiminnallisuus voidaan toteuttaa myös muulla kuin TPM-teknologialla.

Projektissa tutkittiin, miten etätodennus voitaisiin integroida perinteisiin OT-protokolliin (Operational Technology eli tuotantoympäristössä käytössä olevat teknologiat) ja miten se sopisi käytettäväksi identiteetti ja pääsynhallinta (IAM) -mekanismien kanssa. Integrointi tarjoaisi mahdollisuuden rakentaa järjestelmäkehys, jolla voitaisiin luotettavasti verifioida koko tulevaisuuden tehtaan ohjelmistojen eheys ja havaita poikkeamat kuten esimerkiksi epäonnistunut ohjelmistopäivitys. Kartoituksen perusteella löytyi eräitä tutkimusprojekteja, joissa integrointia oli tehty, mutta mekanismi ei ole laajassa käytössä, vaikka sille olisi tarvetta erityisesti kriittisen infrastruktuurin yhteydessä. Etätodennusta ei ole huomioitu edes suhteellisen uudessa OPC UA -automaatioprotokollassa. Alueen standardointi olisi tärkeää, jotta vältytään sirpaloitumista lisääviltä valmistajakohtaisilta ratkaisuilta.

2.2.2 Elintarvikeprosessien kyberturvallisuuden simulointi kyberharjoitteluympäristöissä

Tehtävä liittyy suoraan projektin työpaketissa WP5 FoF Dynamic Risk Management and Resilience ja sen tehtävässä T5.4 Cyber-resilience Capacity tehtyyn työhön. Tutkimus jakautui karkeasti neljään alueeseen:

- Teollisuuden yleisten uhkatekijöiden kartoitus (Julkaisu: Sailio et al. 2020)
- State of the art demonstraatio liikenteen monitoroinnista Bittiumin moniyhteys arkkitehtuurissa (ITEA väliarviotapahtuma 2/2020)
- Kyber ja fyysisten uhkien korrelointi anomalioiden havaitsemiseksi
- High Metal:in juustorobottiympäristön verkkoliikennesimulaattorin tekeminen, sekä sen siirtäminen Airbus CyberRange -ympäristöön. Ympäristön mallia käytettiin yhteisdemonstraatioon, jossa VTT:n ja Rugged Tooling:in työkalut suojasivat juustorobottijärjestelmää kyberhyökkäykseltä (loppudemo).

Työpaketti suoritettiin suurelta osalta Airbus CyberRange -ympäristössä, mikä osittain lisäsi teknisten haasteiden ratkaisuun kulunutta aikaa. Kaikki tukitoiminnot ympäristön käyttämiseen eivät aina olleet nopeasti saatavilla. Lisäksi kohtuullinen osa ajasta kului oman ympäristömallin sopeuttamiseen toteutusympäristön rajoitusten vuoksi. Kaiken kaikkiaan ympäristö oli kuitenkin hyvä ratkaisu yhteistoiminnan mahdollistamiseksi. Oman kyberharjoitteluympäristön (cyber-range) perustaminen (esim. Open Stack) projektia varten olisi tuonut huomattavasti haasteita ympäristön ylläpidon osalta.

Työpaketti toi hyvin ilmi tulevaisuuden tehtaiden yhteyskyvykkyyksien mukanaan tuoman haasteen tietoturvan osalta. Koska järjestelmät ovat yhteydessä järjestelmiin Internetissä, yhteyksien suojaaminen ja verkon tietoturvan paikallinen monitorointi on erittäin tärkeää, jottei järjestelmän toiminta vaarannu kyberhyökkäyksessä. Onnistuneen kyberhyökkäyksen johdosta ei vaarannu pelkästään tuotannon laatu ja tehokkuus, vaan myös käyttäjien ja kuluttajien turvallisuus.

Projektin loppudemo on julkaistu tutkimuksen taustaa ja menetelmiä kuvaavan blogitekstin kanssa 17.6.2022 projektin verkkosivuilla otsikolla ”Network monitoring for cheese? Securing the dairy manufacturing process of the future” (Sailio et al. 2022).

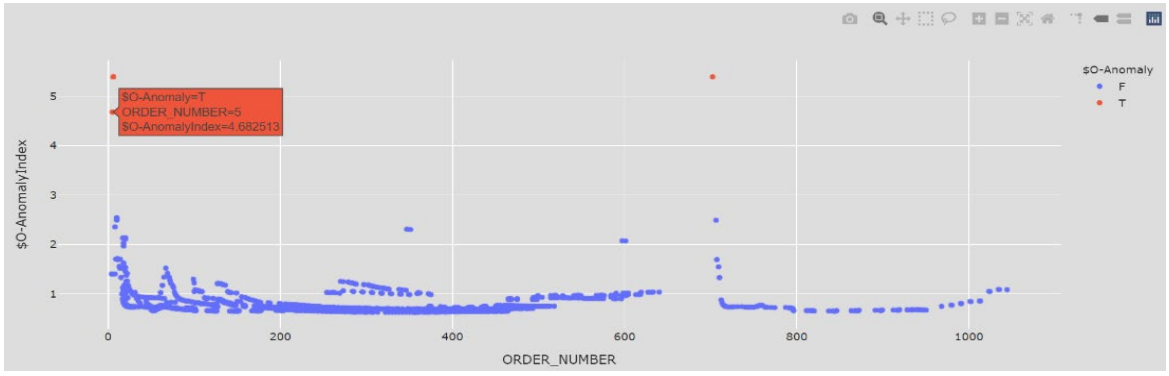
2.2.3 Tekoälyn ja visualisoinnin hyödyntäminen poikkeamien havainnoimisessa

Tämä esimerkkitoteutus liittyy projektin T5.3 Human/Machine Behaviour Watch -tehtävässä tehtyyn työhön. VTT toteutti yhteistyössä Houston Analyticsin kanssa konseptitoteutuksen, jossa yhdistettiin koneoppiminen ja visualisointi poikkeamien havaitsemiseen tulevaisuuden tehtaan tuottamasta datasta.

Toteutuksessa käytettiin Bittiumin tietokantaa, joka sisälsi tuotteiden laadunmittaustietoa kuuden kuukauden ajalta. Tietokantaa analysoitiin poikkeamien löytämiseksi Houston Analytics:in kehittämillä koneoppimisalgoritmeilla. Tavoitteena oli kehittää keinoja ja ymmärrystä parempaan poikkeamien havainnointiin, sekä mahdollistaa huoltotoimenpiteiden ennakointi, vähentää tehtaan vaatimaa seisokkiaikaa ja vähentää epäkelpojen tuotteiden esiintyvyyttä.

Analyysin jälkeen data visualisoitiin käyttäen Python-kirjastoja. Visualisointia käytetään yleensä kahteen eri tarkoitukseen: tunnetun asian esittämiseen yleisölle helposti omaksuttavassa muodossa ja uuden tiedon etsimiseen ihmisystävällisellä tavalla. Tässä visualisointityössä tarkoituksena oli tiedon löytäminen suuresta abstraktista tietomassasta. Toteutimme useita erilaisia graafeja ja kuvaajia tästä datasta, jotta poikkeuksia ensinnäkin löytyisi tehokkaasti, ja toisaalta niihin voisi saada uusia näkökulmia erilaisia parametreja visualisoimalla.

Seuraavassa esimerkkikuvassa katsoja löytää helposti poikkeamat muiden pisteiden joukosta. Lisätietoja hän saa pitämällä hiiren kursoria hetken aikaa poikkeaman päällä. Käytetyssä Python-kirjastossa (Dash) oli sisäänrakennettuna myös muita käytännöllisiä työkaluja, joilla visualisoitua dataa oli helppo tutkia.



Kuva 7: Kuvakaappaus yhdestä konseptitoteutuksen visualisoinnista (Lähde: Latvala et al., 2022)

Tehtaista kerätyt mittaustiedot ovat hyvin abstrakteja ja moniulotteisia, joten ne vaativat paljon käsittelyä ennen kuin niistä tulee käyttökelpoista ja ymmärrettävää informaatiota. Tässä projektissa tutkimme tekoälyn ja visualisoinnin yhdistelmää tehdasdatan analysoimiseen ja käyttäjän ymmärryksen tukemiseen.

2.2.4 Organisaation kyberturvallisuuden kypsyyden mittaaminen

Kybersietoisen tulevaisuuden tehtaan rakentaminen vaatii lähtökohtaisesti kattavan joukon työkaluja, dataa ja prosesseja. Ensinnäkin tarvitaan riittävä ymmärrys tehdasympäristöstä ja sen toiminnoista, mutta myös tietoa sen liitynnöistä ja rajapinnoista sekä saumaton verkon vikasietoisuus, joka mahdollistaa riittävän IT- ja OT-ympäristön valvonnan. Toiseksi turvallisuuspolitiikan (security policy) tulee olla määritelty ja toimeenpantu, mukaan lukien toteutuksen dokumentointi käsittäen mm. pääsyoikeudet tehtaan OT- ja IT-järjestelmiin (access management). Identiteetti- ja pääsynhallintakäytännöt ja -oikeudet tulee ottaa käyttöön ja niiden tulee kattaa kaikki tiloissa työskentelevät alueet sekä ihmiset, mutta myös koneet ja laitteet (esim. IoT). Uusia teknologioita, kuten tekoälyä, tulisi tutkia ja kehittää kyvykkyyksiä, jotta voidaan valmistautua mahdollisiin niihin kohdistuviin hyökkäyksiin. Lisäksi tulisi toteuttaa sekä ihmisten että koneiden reaaliaikainen seuranta, jotta voidaan havaita mahdolliset poikkeamat (anomaliat) tehtaan tiloissa, prosesseissa ja verkoissa, kattaen myös edellisiin otettavat etäyhteydet. Lopulta tulisi kehittää ja harjoitella myös riskien lieventämis- (mitigation) ja muita toimenpiteitä, jotta poikkeamiin pystytään reagoimaan oikein ja kohtuullisessa ajassa heti, kun niitä havaitaan.

Kaikki edellä mainitut tiedot tulisi sisällyttää SIEM-järjestelmään (Security Information and Event Management) riittävän tilannetietoisuuden rakentamiseksi ja perustaa SOC (Secure Operations Centre) täydentämään SIEM:ää ja tarjoamaan tarvittavat resurssit mm. tietoturvaluokkausten tutkintaa (digital forensics) sekä tapausten hallintaa (incident management) varten. Myös digitaalisia kaksosia (digital twin,

DT) ja kyber-harjoitusympäristöjä (cyber range) tulisi käyttää soveltuvien torjunta- ja vastatoimitaktiikkojen harjoittamiseen sekä henkilöstön kouluttamiseen, jotta nämä pystyvät reagoimaan hyökkäyksiin ja uhkiin mahdollisimman tehokkaasti, mutta myös testaamaan uusia turvatoimia ns. turvallisessa ympäristössä ennen muutosten toteuttamista todelliseen tuotantoympäristöön. Kun kaikki tiedot ovat saatavilla ja turvatoimenpiteet ovat käytössä, on keskityttävä katastrofien hallintaan ja liiketoiminnan jatkuvuuteen eli valmisteltava FoF pahimpaan mahdolliseen skenaarioon, siis hyökkäykseen, joka johtaa tehtaan ja sen laitteiden täydelliseen hallinnan menettämiseen. Toimenpiteet tehtaan ja sen laitteiden saamiseksi takaisin käyttöön tulee suunnitella etukäteen ja niihin kuuluu mm. päätöksenteon tukijärjestelmien käyttö, dynaaminen uudelleenkonfigurointi, korjaus- ja muut mekanismit, mutta mahdollisuuksien mukaan myös digitaalisen kaksosen tai kyber-harjoitusympäristön kautta tehtävää skenaarioiden mallinnusta ja tehdassimulaatioita.

Kuten edellä on kuvattu, tarvitaan siis kokonaisvaltaista ymmärrystä tehtaan tiloista ja sen laitteista kybersietoisen tulevaisuuden tehtaan rakentamiseksi. Mutta kuinka voimme varmistaa, että kaikki keskeiset elementit ovat jo olemassa vai tarvitaanko lisäkehittämistä joidenkin osien osalta? Yksi ratkaisu on VTT:n hanketta varten kehittämä CyberMaturity-työkalukonsepti. Konsepti koostuu kyselystä, jonka avulla voidaan arvioida organisaation tai sen yksittäisen osan kyberturvallisuuden kypsyyttä sekä tukitoimenpiteitä (palveluita), joiden avulla voidaan kehittää kyselyprosessin aikana mahdollisesti havaittuja puutteita. Työkalu ja prosessi perustuvat VTT:n jo olemassa oleviin online-kypsyysarviointityökaluihin, kuten DigiMaturity[5], AI Maturity[6] ja ManuMaturity[7], mutta kysymykset ja vastausvaihtoehdot on sovellettu kyberturvallisuusaiheeseen ja niissä hyödynnetään olemassa olevia tutkimustuloksia ja kokemuksia aikaisemmista tutkimusprojekteista. CyberMaturity-palveluprosessi on esitetty seuraavassa kuvassa ja kuvattu kappaleissa.

Kuva 8. CyberMaturity-palveluprosessi (Lähde: CyberFactory#1 D5.4 FoF Resilience)

Palveluprosessin käynnistää itsearviointipalveluun rekisteröitynyt käyttäjä. Ilmoittautuminen tapahtuu antamalla perustiedot organisaatiosta, sen toimialasta sekä vastaajan yhteystiedot. Rekisteröitymisen jälkeen käyttäjä saa käyttäjätunnuksen ja salasanan päästäkseen itsearviointityökaluun. Kaikki kyselyn tiedot ovat ehdottoman luottamuksellisia ja niitä käsitellään vain VTT:n kyberturvallisuusasiantuntijoiden toimesta. Vastauksia käytetään paitsi yksittäisen organisaation kyberkypsyyden määrittämiseen niin myös tilastollisen vertailudatan luomiseen kaikkia vastaajia varten sekä ns. kontrolliryhmien tulosten esittämiseen prosessin aikana järjestettävissä CyberMaturity-työpajoissa.

CyberMaturity-kysely (itsearviointi)

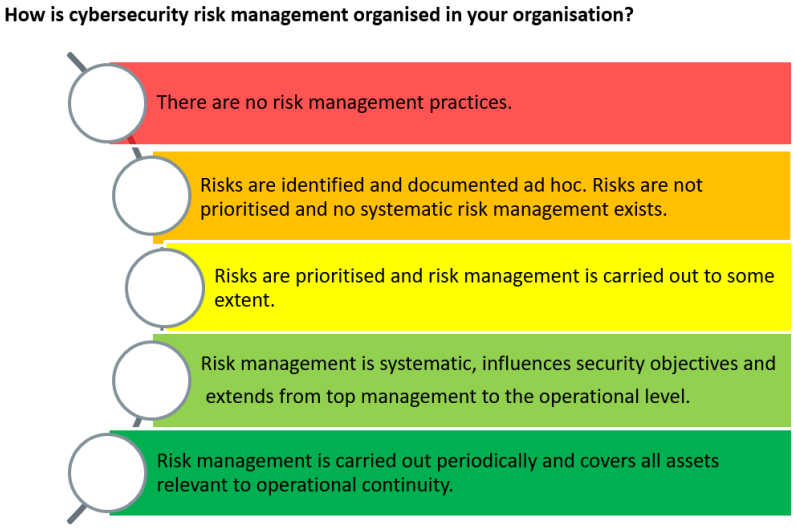
CyberMaturity-kysely koostuu noin 20 monivalintakysymyksestä kuudesta eri aihealueesta, jotka on listattu alla. Huomaa, että yksittäiset aiheet ja kysymykset eivät välttämättä ole lopullisia.

- Ensimmäinen aihealue kattaa kyberturvallisuuden hallinnan ja hallinnon. Kysymykset liittyvät kyberturvallisuusstrategiaan ja sen tavoitteisiin, kyberturvallisuuspolitiikan toimeenpanoon sekä kyberturvallisuuden johtamisen tukeen.

[5] https://digimaturity.vtt.fi/
[6] https://ai.digimaturity.vtt.fi/
[7] https://manumaturity.vtt.fi/

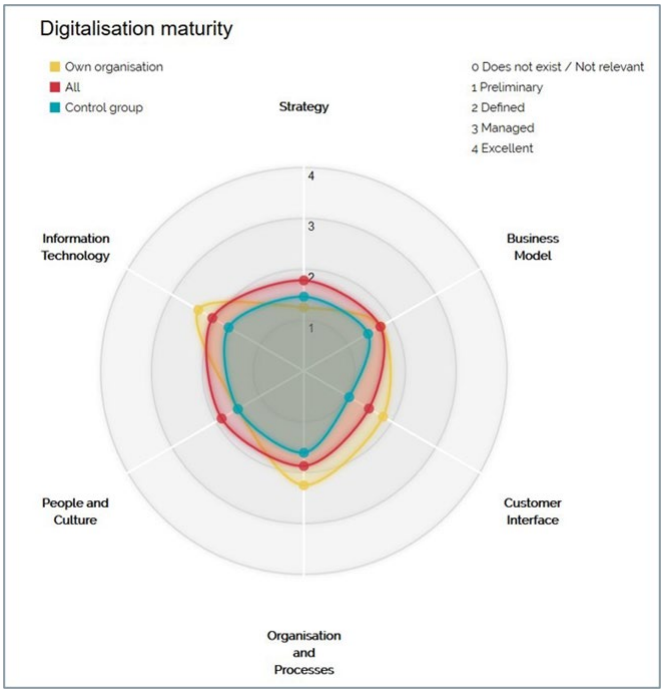
- Toinen aihealue keskittyy kyberturvallisuuden toimintamalliin ja koostuu hankintoihin ja kyberturvallisuusinvestointeihin, riskien ja yksityisyyden hallintaan sekä fyysiseen turvallisuuteen liittyvistä kysymyksistä.
- Kolmas aihealue keskittyy prosesseihin, jotka liittyvät omaisuudenhallintaan, tapausten hallintaan, tilannetietoisuuteen, identiteetinhallintaan ja kulunvalvontaan sekä uhkien ja haavoittuvuuksien hallintaan.
- Neljäs aihealue keskittyy ihmisiin ja kulttuuriin sekä käsittelee turvallisuuskulttuuriin, kyberturvallisuuden taitoihin ja kybertietoisuuteen liittyviä kysymyksiä.
- Viides aihealue keskittyy tuoteturvallisuuteen ja ulkoisiin riippuvuuksiin, jotka ovat erittäin tärkeitä varsinkin valmistavan teollisuuden kannalta. Kysymykset sisältävät asiakkaiden vaatimuksia, vaatimustenmukaisuutta sekä varmuustason ja arvoverkoston riippuvuuksia.
- Kuudes ja viimeinen aihealue keskittyy teknologioihin ja kattaa mm. järjestelmien ja verkkojen yhteenliittämiseen, laite- ja ohjelmistoturvallisuuskonfiguraatioon, virus- ja haittaohjelmatorjuntaan sekä pilven turvallisuuteen liittyviä kysymyksiä.

Kyselyn jokaisessa kysymyksessä on viisi vastausvaihtoehtoa, jotka vaihtelevat erittäin epäkypsästä tai peruskyvystä erittäin kypsään tai kehittyneeseen kykyyn. Vastaajaa neuvotaan valitsemaan esitetyistä vaihtoehdoista lähin organisaation (tai sen osan) nykyistä tilannetta ja kykyä vastaava vaihtoehto ja jokainen kysymys on pakollinen. Alla olevassa kuvassa on yksi esimerkkikysymys ja sen vastausvaihtoehdot.



Kuva 9. Esimerkki CyberMaturity-kyselyn kysymyksestä vastausvaihtoehtoineen (Lähde: CyberFactory#1 D5.4 FoF Resilience)

Itsearviointikyselyn täyttämisen jälkeen vastaajalle näytetään arvioinnin tulokset tähän tarkoitukseen soveltuvassa ns. seittikaaviossa ja kaikkien vastausten keskiarvo vertailua varten. Koska CyberMaturity-työkalu on vasta konseptivaiheessa, seuraavassa kuvassa on esitetty malliesimerkki DigiMaturity-kypsyystyökalun tulossivusta.



Kuva 10. Esimerkki VTT:n DigiMaturity-työkalun tulossivusta (Lähde: CyberFactory#1 D5.4 FoF Resilience)

Itsearvioinnin jälkeen vastaaja voi ottaa yhteyttä VTT:n henkilöstöön ja pyytää tapaamista, jossa voidaan keskustella tuloksista ja alustavista kehittämisideoista kyberkypsyyden kehittämistä varten tai VTT:n henkilöstö voi ottaa yhteyttä vastaajaan myöhemmin. Siinä tapauksessa, että itsearviointi tehdään osana projektikokousta tai muuta sopivaa tilaisuutta, tuloksista voidaan keskustella jo ko. tapahtuman aikana.

Alustavien kehitysideoiden käsittely

Tämä vaihe koostuu VTT:n asiakasorganisaation kanssa järjestämästä kokouksesta, joka kattaa CyberMaturity-prosessin sekä itsearviointikyselyn läpikäynnin sekä tulokset ja vertailun verrokkiryhmään. Kokouksen tavoitteena on keskustella alustavista ideoista organisaation kyberturvallisuusvalmiuksien kehittämiseksi. Tämän ensimmäisen kokouksen jälkeen prosessin seuraavat vaiheet riippuvat asiakkaan päätöksestä siirtyä tämän omien tarpeiden mukaan räätälöityyn kehittämiseen.

CyberMaturity-työpaja

Prosessin seuraava vaihe on CyberMaturity-työpaja, joka on räätälöity asiakkaan tarpeiden mukaan. Työpaja voi koostua erilaisista kaupallisista toiminnoista, jotka vaihtelevat yksityiskohtaisemmista kyselyistä, tutkimuksista ja henkilöstöhaastatteluista aina VTT:n asiantuntijoiden toteuttamiin tai tukemiin konkreettisiin kehittämistoimiin. Työpajan ja siihen liittyvien tukitoimintojen tuloksena asiakasorganisaatio saa kattavamman tilannekuvan oman organisaation kyberturvallisuuden kypsyystilanteesta sekä yksityiskohtaisemman kehityssuunnitelman, joka voidaan toteuttaa VTT:n tai jonkin kolmannen osapuolen toteuttamana yhtenä tai useampana tutkimus- ja kehittämishankkeena.

Kehittämisvaihe

Prosessin viimeinen vaihe käsittää yhden tai useampia T&K-hankkeita, jotka keskittyvät organisaation haluttujen kyberkyvykkyyksien kehittämiseen asetetulle tavoitetasolle. Näihin hankkeisiin voi sisältyä erilaisia kyberturvallisuustietoisuutta (awareness) lisääviä toimia, järjestelmien tai sen laitteistojen ja ohjelmistojen turvallisuus- tai tunkeutumistestausta (penetration testing), koulutusta ja muita vastaavia toimintoja, jotka auttavat organisaatiota saavuttamaan halutun kypsyystason kohtuullisessa ajassa VTT:n tai jonkin kolmannen osapuolen organisaation asiantuntemuksen avulla. Kehityshankkeet räätälöidään yhdessä asiakkaan kanssa tämän tarpeiden ja mieltymysten mukaan.

Palvelukonseptin yhteenveto ja johtopäätökset

CyberMaturity-palvelukonseptin ja -prosessin tavoitteena on tarjota helppo tapa arvioida organisaation kyberturvallisuuden kypsyyttä itsenäisesti tarjoamalla siihen tarvittavat mittarit. Tämä mahdollistaa kybersietoisen tulevaisuuden tehtaan kehittämisen ja parantaa mahdollisesti jo olemassa olevia kyberturvallisuuteen ja -sietoisuuteenliittyviä prosesseja kohdeorganisaatioissa. CyberMaturity-itsearviointi perustuu Capability Maturity Model (CMM) -kypsyysmalliin ja sen seuraajiin, Capability Maturity Model Integration (CMMI) ja Cybersecurity Capability Maturity Model (C2M2) - malleihin. Vaikka CyberMaturity-kysely on melko yksinkertainen, tukiprosessit voivat koostua yksityiskohtaisemmista tutkimuksista, joissa on esimerkiksi tarkempia alakohtaisia kysymyksiä. CyberMaturity-palvelukonsepti on kehitetty CyberFactory#1-tutkimushankkeen aikana, mutta sen mahdollinen toteutus ja julkaisu tapahtuu vasta hankkeen jälkeen. Edellisen lisäksi konseptin toteutuksesta ja siihen käytettävistä menetelmistä on tekeillä myös artikkeli tämän vuoden aikana.

3. Projektin julkaisut ja viestintä

Tässä luvussa listataan VTT:n hankkeen aikana tuottamat julkaisut sekä kuvataan muuta hankkeen aikana harjoitettua viestintää, esimerkiksi muita kuin konferenssiartikkelien julkaisemiseen liittyviä esityksiä sekä osallistumisia messu- ja vastaaviin tilaisuuksiin.

3.1 Hankkeen aikana tuotetut julkaisut

Projektisuunnitelmassa mainittu VTT:n tavoite hankkeen julkaisumääristä oli neljä konferenssiartikkelia. Tutkimustulosten hyvän laadun ja Covid-19 -pandemian myötä avautuneiden konferenssien etäosallistumismahdollisuuksien ansiosta julkaistujen konferenssiartikkelien määrä oli lopulta yli kaksinkertainen suunnitelmiin nähden. Seuraavassa taulukossa on listattu projektissa syntyneet konferenssi- (9 kpl) ja lehtiartikkelit (2 kpl). Journal-artikkeleista toinen on hyväksytty, mutta odottaa vielä julkaisua tämän raportin tekovaiheessa.

Taulukko 1. Hankkeen aikana tuotetut konferenssi- ja lehtiartikkelit

#	Konferenssi	Artikkelin otsikko	Kirjoittajat
1	9th International Conference on Operations and Supply Chain Management (OSCM 2019)	Management of Cyber Security Threats in the Factories of the Future Supply Chains	Jukka Hemilä, Markku Mikkola, Jarno Salonen
2	Multidisciplinary Digital Publishing Institute (MDPI 2020), Journal	Cyber Threat Actors for the Factory of the Future	Mirko Sailio, Outi-Marja Latvala, Alexander Szanto
3	34th annual European Simulation and Modelling Conference (ESM 2020)	Inter-Organizational Perspective to Cyber-Physical System Modelling in Industrial Production	Markku Mikkola, Markus Jähi
4	16th International Conference for Internet Technology and Secured Transactions (ICITST 2021)	Review on Cybersecurity Threats Related to Cyber Ranges	Sami Noponen, Juha Pärssinen, Jarno Salonen
5	International Conference on Industry Science and Computer Sciences Innovation (iSCSi 2022)	Device life cycle management requirements for identity and access management in the factory of future environment	Jari Partanen, Markku Kylänpää, Sanna Loukusa, Markku Korkiakoski, Jarno Salonen
6	13th ISPIM Innovation Conference (ISPIM 2022)	Supporting Industry 4.0 implementation with virtual modelling - experiences from two cases	Markku Mikkola, Patrick Eschemann, Linda Feeken, Jarno Salonen
7	10th International Symposium on Digital Forensics and Security (ISDFS 2022)	The Digital Forensics of Cyber Attacks at Electrical Power Grid Substation	Juha Pärssinen, Petra Raussi, Sami Noponen, Mikael Opas, Jarno Salonen
8	21st European Conference on Cyber Warfare and Security (ECCWS 2022)	Combining System Integrity Verification with Identity and Access Management	Markku Kylänpää, Jarno Salonen

#	Konferenssi	Artikkelin otsikko	Kirjoittajat
9	International Conference on Signal Processing, Information System and Cyber Security (SPISCS 2022)	Experimental Remote Attestation over OPC UA Protocol	Markku Kylänpää, Arto Juhola
10	International Conference on Signal Processing, Information System and Cyber Security (SPISCS 2022)	Developing the Factory of the Future Cybersecurity and Resilience	Adrian Kotelba, Jarno Salonen
11	International Journal of Innovation and Scientific Research (IJISR 2022), Journal	Cybersecurity of Cyber Ranges: Threats and Mitigations (hyväksytty 29.6.2022)	Sami Noponen, Juha Pärssinen, Jarno Salonen

Konferenssi- ja journal-artikkelien lisäksi VTT julkaisi hankkeen tuloksia myös mm. blogitekstien muodossa. Seuraavassa taulukossa on listattu hankkeen aikana tehdyt blogitekstit (3 kpl) sekä muut julkaisut (1 kpl).

Taulukko 2. Hankkeen aikana tuotetut blogitekstit ja muut julkaisut

#	Julkaisumuoto ja -kohde	Julkaisun otsikko	Kirjoittajat
1	Blogiteksti (2.11.2020), VTT:n verkkosivut	The power of data in remote work – anticipation supports success[8]	Jarno Salonen, Outi-Marja Latvala, Pia Raitio, Seppo Heikura
2	Kontribuutio kirjaan (14.4.2021), Suomen Automaatioseura ry	Automaation tietoturva – Kriittisen tuotannon turvaaminen[9]	Pia Raitio
3	Blogiteksti (18.5.2022), Hankkeen verkkosivut	Tackling anomalies in FoF networks with AI and visualization[10]	Outi-Marja Latvala, Mirko Sailio, Jarno Salonen
4	Blogiteksti (17.6.2022), Hankkeen verkkosivut	Blogiteksti + Demovideo	Mirko Sailio

Edellisten julkaisuiden lisäksi VTT osallistui myös projektin luottamuksellisten ITEA-raporttien (deliverable) sekä projektissa toteutettujen sekä myöhemmin ITEA:n sivuilla julkaistujen State-of-the-Art -raporttien kirjoittamiseen. State-of-the-Art -raporteista VTT osallistui ”Modeling and Simulation of Factories of the Future” -raportin kirjoittamiseen (CyberFactory#1 State of the Art: Modeling and Simulation, 2020) sekä vastasi ”Factory of the Future Resilience” -raportin kirjoittamisesta (CyberFactory#1 State of the Art: FoF Resilience, 2021).

3.2 Hankkeen aikana suoritettu muu viestintä

Projektin aikana suoritetun julkaisutoiminnan lisäksi VTT järjesti myös webinaareja sekä esitti hankkeen tuloksia soveltuvissa tilaisuuksissa. Seuraavassa taulukossa on listattu hankkeen aikana suoritettua muuta viestintää. Taulukossa mainittujen tilaisuuksien lisäksi VTT:n tutkijat osallistuivat myös muihin

[8] https://www.vttresearch.com/en/news-and-ideas/power-data-remote-work-anticipation-supports-success
[9] https://www.automaatioseura.fi/julkaisut-kirjakauppa/automaation-tietoturva-julkaisut/
[10] https://www.cyberfactory-1.org/blog/tackling-anomalies-in-factory-of-the-future-networks-with-ai-and-visualization/

läheisesti projektin tutkimusaiheisiin liittyviin kotimaisiin ja kansainvälisiin tilaisuuksiin, joissa tavoitteena oli joko projektiviestintä ja/tai verkottuminen.

Taulukko 3. Hankkeen aikana VTT:n suorittama projektin viestintä eri tilaisuuksissa

#	Tilaisuus, aika ja paikka	Aihe	Esittäjä/osallistuja
1	6th Basque Industry 4.0 -tilaisuus (20.-21.11.2019), Bilbao, Espanja	Hankkeen sekä VTT:n akvaario-visualisointidemon esittely	Jarno Salonen
2	Kyberturvallisuuskeskuksen ja VTT:n välinen verkostoitumistilaisuus, (29.9.2020), Online	CyberFactory#1 and FoF threat actor analysis	Pia Raitio, Mirko Sailio
3	Teknologiateollisuus ry:n työväline- ja muoviteollisuuden neuvottelupäivän webinaari[11], (28.1.2021)	Esitys: Kybernäkökulma tulevaisuuden tehtaan arvoketjuihin	Markku Mikkola
4	VTT:n sekä FoF resilience -partnerien järjestämä hankkeen webinaari: “Resilience Capabilities for the Factory of the Future”[12], (28.4.2021), Online	FoF Resilience -työpaketin sekä VTT:n cyber range tutkimustyön esittely	Jarno Salonen
5	Tampereen yliopiston Johtajuussymposium 2021, (8.9.2021), Tampere + Online	Esitys: “The concept of (almost) total cyber resilience”	Jarno Salonen
6	35th annual European Simulation and Modelling Conference (ESM 2021) (27.10.2021), Online	Keynote-esitys: “CyberFactory#1 – Increasing the FoF Resilience with Modelling and Simulation Tools”	Jarno Salonen
7	Cyber Security and Cloud Expo, (23.-24.11.2021, Amsterdam, Alankomaat	Projektin ja sen tulosten esittely projektin omalla osastolla ITEA-osastolla yhdessä muiden projektipartnerien kanssa	Jarno Salonen
8	VTT:n ja kotimaisten partnerien järjestämä hankkeen webinaari: “CyberFactory#1 Results webinar in Finland”[13], 14.2.2022, Online	Hankkeen, VTT:n vetämän FoF Resilience -työpaketin sekä VTT:n cyber range -tutkimustyön esittely	Jarno Salonen, Mirko Sailio
9	CriM – International Crisis Management workshop (9.-11.11.2021), Oulu	Esitys: Cybersecurity and critical infrastructure	Pia Raitio
10	“FIIF event: CyberFactory#1 Dissemination”[14], 9.6.2022, Helsinki + Teams (VTT toimi tilaisuuden toisena järjestäjänä)	Hankkeen yleisesittely sekä esimerkkejä kotimaisen konsortion T&K-toiminnan tuloksista.	Jarno Salonen

[11] https://teknologiateollisuus.fi/fi/ajankohtaista/tapahtumat/tyovaline-ja-muoviteollisuuden-neuvottelupaivan-webinaari-2812021, https://teknologiateollisuus.fi/en/node/27517
[12] https://www.cyberfactory-1.org/blog/webinar-resilience-capabilities/
[13] https://www.cyberfactory-1.org/blog/cyberfactory1-results-webinar-in-finland/
[14] https://fiif.fi/events/fiif-event-cyberfactory1-dissemination-event-june-9-2022-helsinki-online/

4. Yhteistyö ja jatkosuunnitelmat

Tässä luvussa käsitellään projektin aikana tehtyä yhteistyötä muiden kotimaisten ja kansainvälisten hankkeiden kanssa sekä eri projektipartnerien kanssa tehtyä hankevalmistelutyötä. Lisäksi kuvataan VTT:n suunnitelmia hankkeen tutkimuksen ja sen tulosten hyödyntämiseksi projektin jälkeen.

4.1 Yhteistyö ja verkottuminen kotimaassa

VTT valmisteli vuosien 2019-2021 aikana SecurMap -hanketta Business Finlandin Digital Trust -ohjelmaan. Hankkeen tavoitteena oli erityisesti valmistavan teollisuuden yritysten kyberturvallisuustarpeiden mittaaminen ja analysointi. Pilottikohteena oli kansainvälisiä pilottiyrityksiä ja CF#1-konsortiosta mukana oli Houston Analytics, mutta hankevalmistelu kariutui lopulta kotimaan yrityskonsortion haasteisiin Covid-19-pandemian aikana sekä kansainvälisten pilottiyritysten rahoituksen puuttumiseen. Hanke olisi toteutuessaan täydentänyt CyberFactory#1-hankkeessa tehtyä kyberturvallisuuden kypsyyden mittaamiseen liittyvää tutkimusta.

Toinen VTT:n hankevalmistelu nimellä ”CRIICI - Correlating thReats from dIfferent sources In Critical Infrastructure” (”Eri lähteistä tulevien uhkien korrelointi kriittisessä infrastruktuurissa”) käynnistyi Business Finlandin Digital Trust Challenge -tilaisuudesta ja oli käynnissä vuonna 2020-2021. CF#1-konsortiosta tässä hankevalmistelussa oli mukana Bittium ja Netox, mutta valmistelu keskeytettiin kiinnostuneiden loppukäyttäjien puuttumiseen osin pandemian aiheuttamista haasteista johtuen.

4.2 Yhteistyö ja verkottuminen kansainvälisesti

CyberFactory#1-hankkeessa on tehty hyvin paljon yhteistyötä Airbus:in koordinoiman ja vuonna 2019 käynnistyneen SeCoIIA - Secure Collaborative Intelligent Industrial Assets -hankkeen (2019-2022, GA#871967, https://secoiia.eu/) kanssa. VTT oli tässä hankkeessa mukana ainoana suomalaisena partnerina ja muutamat projektin tutkijoista olivat mukana molemmissa projekteissa. Muita molemmille projekteille yhteisiä partnereita oli Airbusin lisäksi PAL Robotics Espanjasta, ISEP ja Sistrade Portugalista sekä Fraunhofer AISEC Saksasta. SeCoIIA-hankkeessa VTT vastasi ”fine-grained access control and encryption” tehtävästä, jolla oli yhteneväisyyksiä CF#1-hankkeessa Netoxin vetämään ”Human/Machine access and trust management” tehtävään VTT:n vetämässä ”FoF Dynamic Risk Management and Resilience” -työpaketissa.

Pienimuotoista yhteistyötä tehtiin myös ”Cyber-MAR - Cyber preparedness actions for a holistic approach and awareness raising in the MARitime logistics supply chain” -hankkeen (2019-2022, GA#833389, https://www.cyber-mar.eu/) kanssa, jossa VTT oli mukana ainoana partnerina. Projektien välinen yhteistyö VTT:n sisällä liittyi enimmäkseen cyber range -tutkimukseen sekä jossain määrin myös tietoturvaluokkausten tutkintaan.

Läheistä yhteistyötä on tehty myös kesällä 2021 käynnistyneen ”Mind4Machines - Manufacturing Industry’s Novel Digitalisation Value Chains for Connecting Machines with People, Process and Technology” -hankkeen (2021-2024, GA# 101005711, https://mind4machines.eu/) kanssa ja VTT:n projektitiimin jäsenet ovat mukana myös CF#1-hankkeessa. Mind4Machines -hankkeessa ei ole VTT:n lisäksi muita yhteisiä partnereita ja yhteistyö on liittynyt valmistavan teollisuuden digitalisaatioon sekä siinä erityisesti tekoälyyn ja kyberturvallisuuteen.

VTT on CyberFactory#1 -hankkeen aikana koordinoinut tai osallistunut myös muihin H2020- ja Horizon Europe -hankevalmisteluihin sekä vuoden 2021 EIT Manufacturing -hakuun. Hankevalmisteluissa mukana on ollut kotimaisista partnereista Bittium, Houston Analytics ja Netox sekä kansainvälisistä partnereista BIGS (DE), Fraunhofer AISEC (DE), GOHM Electronics (TR) ja Vestel (TR). Suurin osa näistä valmisteluista ei ole saanut rahoitusta, mutta ainakin yksi valmisteluista on rahoitusneuvotteluissa kesällä 2022 ja toinen odottaa rahoituspäätöstä. Yhteys CF#1-hankkeeseen valmisteluissa on yleisimmin ollut

valmistavan teollisuuden tai muun soveltuvan kohdesektorin digitalisaatio ja siihen liittyvät teknologian (esim. AI) käyttöönottoon liittyvät kyberturvallisuushaasteet.

4.3 Muu yhteistyö

VTT osallistui Team Finland -delegaation vierailulle Pariisiin 16.-18.5.2022 osana Sustainable Manufacturing Finland -verkoston ryhmää. Vierailun tavoitteena oli kartoittaa projektin aikana tehdyn tutkimuksen ja sen tulosten hyödyntämismahdollisuuksia ranskalaisten loppukäyttäjäyritysten parissa, selvittää tulevia hankeyhteistyömahdollisuuksia sekä edistää projektin viestintää.

VTT osallistui CONVERGENCE NEXT[15] -tilaisuuteen Brysselissä 1.-3.6.2022. Kyseessä oli European Cyber Competence Network[16] -verkoston järjestämä tilaisuus, jossa esitettiin pilottiprojektien tuloksia sekä keskusteltiin eurooppalaisen kyberturvallisuuden tulevaisuuden haasteista mukaan lukien kyberturvallisuusosaamisen näkökulma. Verkosto käsittää neljä EU-pilottiprojektia eli Concordia, CyberSec4Europe, Echo ja Sparta, joiden tavoitteena on kehittää eurooppalaisen kyberturvallisuuden teollisia- ja teknologiakyvykkyyksiä sekä vahvistaa yleistä kyberosaamista. VTT:n tavoitteena tilaisuudessa oli selvittää Industry 4.0 liittyviä tulevaisuudennäkymiä erityisesti tulevaisuuden tehtaan IT-verkkojen osalta.

VTT on käynyt keskusteluja Bittumin kanssa cyber range -osaamisen laajentamisesta, joko jatkoprojektin tai muun toiminnan puitteissa. Sekä Bittium että VTT ovat hyödyntäneet Airbus CyberRange[17] -ympäristöä tehokkaasti CyberFactory#1-hankkeen aikana koska siihen liittyvä kyberturvallisuuden mallintamis- ja muu osaaminen on melko vahvaa niin aihe on ajankohtainen molemmille osapuolille.

4.4 Hankkeessa tehdyn tutkimuksen ja tulosten hyödyntäminen projektin jälkeen

Tässä raportissa esitetty lähestymistapa liiketoimintaekosysteemien mallintamiseen on vielä konseptitasolla. Samalla kun sitä voidaan hyödyntää tulevissa liiketoimintaekosysteemien kehityshankkeissa, sitä voidaan myös edelleen kehittää. Kehittämistä voidaan tehdä ainakin tiedon keräämisen menetelmien osalta, samoin kuin tiedon jakamisen pelisääntöjen suhteen. Useampien tapaustutkimusten pohjalta voisi olla mahdollista myös kehittää geneeristä ekosysteemin taloudellista analyysia tukevaa laskentatyökalua.

Etätodentaminen (remote attestation) on tärkeää erityisesti kriittisen infrastruktuurin hankkeissa ja kertynyttä osaamista ja näkemystä sen yhdistämisessä OT-protokolliin voidaan hyödyntää tulevissa hankevalmisteluissa. Kaupallisten hankkeiden rooli riippuu aiheen hyödyntämisestä kiinnostuneen teollisuuskumppanin löytymisestä. Alueen standardoinnin seuraaminen (esimerkiksi IETF RATS WG) on myös jatkossa tärkeää.

Kyberharjoitusympäristöt (cyber range) mahdollistavat uusia lähestymisiä erityisesti simulointiin, mallintamiseen ja koulutukseen. Ne mahdollistavat oikeanlaisten ympäristöjen testaamisen ilman todellisen ympäristön riskejä. Kriittisten verkkojen ja ympäristöjen turvaaminen simuloimalla niiden ominaisuuksia CR ympäristössä vaatii vielä tutkimusta, mutta toimiessaan sekä helpottaa organisaatioiden kyberturva osaamisvajetta, että kriittisten ympäristöjen heikkouksien korjaamista.

[15] https://cybersec4europe.eu/events/convergence-next/
[16] https://cybercompetencenetwork.eu/
[17] https://airbus-cyber-security.com/products-and-services/prevent/cyberrange/

Konseptitoteutus, jossa yhdistettiin koneoppimista ja visualisointia, mahdollisti poikkeamien havaitsemisen normaalien datapisteiden joukosta. Luonnollisena jatkumona tälle olisi löydettyjen poikkeamien parametrien analysointi erilaisten visualisointien avulla, jotka voisi edelleen koota kokonaiseksi kojelautanäkymäksi.

CyberMaturity-palvelukonseptin kehittämistä jatketaan myös hankkeen jälkeen ja se pyritään julkaisemaan osana VTT:n Maturity-palvelutarjoamaa. Konseptin ja prosessin kehityksessä tarvittavaa osaamista liittyen kyberturvallisuuden arviointiin on tarvetta jatkokehittää, mikä tapahtuu VTT:n nykyisissä ja tulevissa tutkimus- ja kehityshankkeissa.

5. Yhteenveto

Tämä tutkimusraportti kuvaa VTT:n suorittamaa tutkimusta ja tuotekehitystä kansainvälisessä ITEA3-CyberFactory#1 (CF#1) -hankkeessa, jonka tavoitteena oli suunnitella, kehittää, integroida ja demonstroida joukko kyvykkyyksiä, joiden avulla voidaan parantaa tulevaisuuden tehtaiden optimointia ja toimintavarmuutta. Hankeen lähtökohta oli neljännessä teollisessa vallankumouksessa, jonka keskiössä on kasvavan digitalisaation tuomat haasteet, aiempaa monimutkaisemmat ja verkottuneet tuotanto- ja toimitusketjut, uudenlaisten teknologioiden sekä palveluliiketoiminnan hyödyntäminen sekä erityisesti tulevaisuuden tehtaasta laitteista, prosesseista ja erilaisista sensoreista kerättävän tiedon tehokkaampi hyödyntäminen tuotannon optimointiin ja erilaisten häiriötilanteiden havaitsemiseen.

Yhteenvetona luvun 2.1 liiketoimintaekosysteemien mallinnukseen liittyvästä tutkimuksesta hankkeessa voidaan todeta, että tulevaisuuden tehdas on paljon monimutkaisempi niin tuotanto- kuin toimitusverkostojen osalta. Verkoston eri jäsenten väliset luottamussuhteet eivät ole niin kiinteitä kuin aiemmin ja esimerkiksi halukkuus taloudellisten ja muiden analysoinnin kannalta tärkeiden avaintietojen jakamiseen voi siten olla rajoittunutta. Tämä lisää mallintamisen ja erilaisten liiketoimintakonseptivaihtoehtojen arviointiin liittyvää epävarmuutta mikä puolestaan rajoittaa mahdollisuuksia hyvin yksityiskohtaiseen mallintamiseen ja simulointiin. Toisaalta kaikkien elementtien tai tekijöiden yksityiskohtainen analysointi ei ole edes tarpeen, jos arvioinnissa keskitytään vain sen kannalta merkityksellisiin tekijöihin ja käytetään esim. absoluuttisten mallikohtaisten lukujen sijasta tietoa, joka on verrattavissa muihin vaihtoehtoisiin malleihin. Hankkeessa kehitetty lähestymistapa liiketoimintaekosysteemien mallintamiseen auttaa kuitenkin ymmärtämään ekosysteemin suhteita ja mahdollisia liiketoimintamallin konfiguraatioita paremmin ja se tukee kumppaneita näiden keskustelussa yhteisistä liiketoimintamahdollisuuksista ja niiden kehittämistoiminnan suunnittelusta.

Yhteenvetona luvussa 2.2 kuvatussa hankkeen kyberturvallisuuteen ja kybersietoisuuteen liittyvästä tutkimuksesta voidaan todeta, että tulevaisuuden teollisuus perustuu toimiville verkkoyhteyksille, joilla mahdollistetaan älykäs laitteiden ja sensoreiden käyttäminen. Tämä tehostaa ja parantaa tehdasympäristön hallittavuutta, mutta toisaalta aiheuttaa myös lisääntyviä vaatimuksia kyberturvan osalta. Aiemmin käytössä ollut eristämisen strategia ei ole enää realistinen, vaan tulevaisuuden tehdasympäristöissä on aktiivisesti tarkkailtava verkkoympäristöä kyberhyökkäysten varalta. Verkkoyhteyksien hallinnan lisäksi myös niiden turvallisuuden hallinta onkin ensiarvoisen tärkeää.

Edellisen lisäksi tulevaisuuden tehtaan työkaluvalikoimaan olisi hyvä, ellei peräti välttämätöntä, sisällyttää myös digitaalisia kaksosia (digital twin) ja virtuaalisia kyber-harjoitusympäristöjä (cyber range), joiden avulla pystytään kehittämään tehtaan kyvykkyyksiä sen laitteiden ja prosessien optimointiin sekä varautumaan myös kyberhyökkäyksistä tai muista vastaavanlaisista häiriötilanteista johtuviin toiminta- ja muihin katkoksiin. Tämä on normaalia yrityksen liiketoiminnan jatkuvuuden varmistamiseen liittyvää toimintaa ja täysin verrattavissa jo olemassa oleviin käytäntöihin koskien pelastus- ja vastaavia harjoituksia, tosin sillä poikkeuksella, että tehtaan ja sen laitteiden hallinnan täydellistä menettämistä ei voi harjoitella tuotantoympäristössä aiheuttamatta kohtuutonta haittaa tehtaan normaalille toiminnalle. Virtuaaliympäristössä harjoittelu on kuitenkin mahdollista ja lisäksi ympäristössä tehdyt konkreettiset havainnot esim. yksittäisten laitteiden tai prosessien haavoittuvuuksista voidaan myöhemmin todentaa tuotantoympäristössä, mikä vähentää tehtaan tuotannolle aiheutuvaa haittaa.

Hankkeen jatkosuunnitelmia sekä sen tutkimustulosten hyödyntämistä on käsitelty erikseen luvussa 4.4. Konsortion jäsenet niin Suomessa kuin kansainvälisestikin ovat lähtökohtaisesti olleet kiinnostuneita yhteistyön jatkamisesta ja keskustelua on jo käyty mahdollisen jatkohankkeen valmistelusta. On kuitenkin varmaa, että tulevaisuuden tehdas kehittyy ja monimutkaistuu edelleen uusien teknologiaratkaisujen yleistymisen ja uusien liiketoiminnallisten tarpeiden myötä ja toisaalta mm. päästö- ja kestävän kehityksen vaatimukset vaikuttavat omalta osaltaan tehtaiden tulevaisuudennäkymiin. Työ ei siis suinkaan ole ohi vaikka tämä projekti onkin jo saatu päätökseen.

6. Lähdeviitteet

Allee, V. (2009). Value-creating networks: Organizational issues and challenges. Learning Organization, 16(6), 427–442. https://doi.org/10.1108/09696470910993918

CyberFactory#1 -projekti. (2020). State of the Art: Modeling and Simulation of Factories of the Future. Julkinen projektiraportti. https://itea4.org/project/cyberfactory-1.html (viitattu: 15.6.2022)

CyberFactory#1 -projekti. (2021). State of the Art: Factory of the Future Resilience. Julkinen projektiraportti. https://itea4.org/project/cyberfactory-1.html (viitattu: 17.6.2022)

CyberFactory#1 -projekti. (2021). Deliverable 3.2: Factory Ecosystem Modelling. Luottamuksellinen projektiraportti.

CyberFactory#1 -projekti. (2021). Deliverable 5.4: FoF Resilience. Luottamuksellinen projektiraportti.

Kylänpää, M. & Salonen, J. (2022). Combining System Integrity Verification With Identity and Access Management, Proceedings of the 21st European Conference on Cyber Warfare and Security, 16 - 17 June 2022, Chester, UK, E-Book ISBN: 978-1-914587-41-2, https://papers.academic-conferences.org/index.php/eccws/article/view/202/355

Latvala, O-M, Sailio, M & Salonen, J. (2022). Tackling Anomalies in Factory of the Future Networks with AI and Visualization. Blogiteksti. https://www.cyberfactory-1.org/blog/tackling-anomalies-in-factory-of-the-future-networks-with-ai-and-visualization/ (viitattu: 15.6.2022)

Peppard, J., & Rylander, A. (2006). From Value Chain to Value Network: Insights for Mobile Operators. European Management Journal, 24(2–3), 128–141. https://doi.org/10.1016/J.EMJ.2006.03.003

Sailio, M, Latvala, O-M, Szanto, A. 2020. Cyber Threat Actors for the Factory of the Future. Multidisciplinary Digital Publishing Institute (MDPI 2020). https://doi.org/10.3390/app10124334

Sailio, M, Salonen, J & Mikkola, M. (2022) Network monitoring for cheese? Securing the dairy manufacturing process of the future. Blogiteksti. https://www.cyberfactory-1.org/blog/network-monitoring-for-cheese/ (viitattu: 17.6.2022)

DocuSign

Certificate Of Completion

Envelope Id: 06F0EA01FC8A4D81A70E9C2F2AC45E8A
Status: Completed
Subject: Please DocuSign: VTT-R-00560-22-CyberFactoryNo1_loppuraportti.pdf
Source Envelope:
Document Pages: 28
Signatures: 1
Certificate Pages: 1
Initials: 0
AutoNav: Enabled
EnvelopeId Stamping: Enabled
Time Zone: (UTC+02:00) Helsinki, Kyiv, Riga, Sofia, Tallinn, Vilnius

Envelope Originator:
Jessica Vepsäläinen
Vuorimiehentie 3, Espoo,
., . P.O Box1000,FI-02044
Jessica.Vepsalainen@vtt.fi
IP Address: 130.188.17.16

Record Tracking

Status: Original
08 July 2022 | 15:58

Holder: Jessica Vepsäläinen
Jessica.Vepsalainen@vtt.fi

Location: DocuSign

Signer Events	Signature	Timestamp
Pertti Raatikainen Pertti.Raatikainen@vtt.fi Research Manager VTT Technical Research Centre of Finland Ltd Security Level: Email, Account Authentication (None), Authentication	DocuSigned by: Pertti Raatikainen 9EAB53457FD743E... Signature Adoption: Pre-selected Style Using IP Address: 130.188.17.16	Sent: 08 July 2022 | 15:59 Viewed: 08 July 2022 | 16:04 Signed: 08 July 2022 | 16:04

Authentication Details
SMS Auth:
Transaction: 660777A086A805049195B74CEADAA534
Result: passed
Vendor ID: TeleSign
Type: SMSAuth
Performed: 08 July 2022 | 16:03
Phone: +358 40 7224476

Electronic Record and Signature Disclosure:
Not Offered via DocuSign

In Person Signer Events	Signature	Timestamp

Editor Delivery Events	Status	Timestamp

Agent Delivery Events	Status	Timestamp

Intermediary Delivery Events	Status	Timestamp

Certified Delivery Events	Status	Timestamp

Carbon Copy Events	Status	Timestamp

Witness Events	Signature	Timestamp

Notary Events	Signature	Timestamp

Envelope Summary Events	Status	Timestamps
Envelope Sent	Hashed/Encrypted	08 July 2022 | 15:59
Certified Delivered	Security Checked	08 July 2022 | 16:04
Signing Complete	Security Checked	08 July 2022 | 16:04
Completed	Security Checked	08 July 2022 | 16:04

Payment Events	Status	Timestamps