



KUNNOSSAPIDON KYBERTURVALLISUUS

RAUTATEIDEN KUNNOSSAPIDON KYBERTURVALLISUUSRISKIEN
ARVIOINTI JA KÄSITTELY

Rataforumi | 26.3.2026



Agenda

01

Esityksen tausta

02

Standardipohjainen
lähestymistapa

03

Riskien arviointi- ja
käsittelyprosessi

04

Kysymykset ja kommentit

ESITYKSEN TAUSTAA



Miksi rautateiden kunnossapidon kyberturvallisuus on tärkeää?

01

Kunnossapidettävät järjestelmät ovat yhä digitalisoituneempia ja verkottuneempia

02

Kunnossapidon tietojärjestelmät ovat toiminnan kannalta kriittisiä

03

Kunnossapidon työkalut sekä diagnostiikka- ja valvontajärjestelmät ovat verkottuneita

04

Toimitusketjut ja kolmannet osapuolet ovat merkittävä riskilähde

05

OT-uhat ja haavoittuvuudet lisääntyvät koko ajan

06

Haktivistiryhmillä on kyky ja motivaatio kohdistaa hyökkäyksiä OT-ympäristöihin

07

Kunnossapito on keskeinen osa liiketoiminnan jatkuvuutta ja kriisinsietokykyä

08

EU:n NIS2- ja CER-säätely asettavat vaatimuksia kriittisille toimijoille

09

Kyberturvallisuus tukee toiminnallista turvallisuutta

STANDARDIPOHJAINEN LÄHESTYMISTAPA



Standardipohjainen, järjestelmällinen lähestymistapa riskien arviointiin

Prosessipohjainen lähestymistapa

Hyödyntämällä eri standardeista johdettuja viiteprosesseja sekä niihin liittyvää tietoa ja ohjeistusta voidaan muodostaa tehokas menetelmä riskien arviointiin prosessitasolla ja sitä alemmilla tasoilla.

Omaisuuksilähtöinen lähestymistapa

Omaisuuksilähtöinen lähestymistapa tarkoittaa, että riskit tunnistetaan ja arvioidaan tunnistamalla ensin suojattavat omaisuuserät ja tämän jälkeen tutkimalla, analysoimalla ja arvioimalla niihin liittyviä haavoittuvuuksia ja uhkia.

Yhdistetty lähestymistapa

Kokonaisvaltainen lähestymistapa yhdistää

- kunnossapidon referenssiprosesseihin liittyvän tiedon sekä
 - omaisuuksilähtöisen riskien tunnistamisen ja arvioinnin
- yhdeksi menetelmäksi, jonka avulla kunnossapitoon liittyvät kyberriskit voidaan tunnistaa ja arvioida tehokkaasti.

EN 17007 ja ISO 27005

EN 17007

- Eurooppalainen standardi SFS-EN 17007:2017
Kunnossapitoprosessi ja siihen liittyvät tunnusluvut esittää kunnossapitoprosessin yleistasoisen kuvauksen.
- EN 17007 –standardin kuvailemat prosessit
 - Johtamisprosessi
 - Toteuttamisprosessit
 - Tukiprosessit

ISO 27005

- Kansainvälinen standardi SFS-EN ISO/IEC 27005:2024
Tietoturvallisuus, kyberturvallisuus ja tietosuoja.
- Ohjeita tietoturvariskien hallintaan antaa ohjeita organisaatioiden tietoturvariskienhallinnan toteuttamiseen, erityisesti tietoturvariskien arviointiin ja käsittelyyn.
- Tukee muiden standardien periaatteiden ja vaatimusten mukaista riskienhallintaa.
- Esittelee kaksi yleisesti käytettyä toimintamallia riskien tunnistamiseen
 - Tapahtumakohtainen toimintamalli
 - Omaisuuseriin perustuva toimintamalli

RISKIEN ARVIOINTI- JA KÄSITTELYPROSESSI



Riskien tunnistamisen periaatteita

Keskeiset vaiheet ja kysymykset

- Laaditaan **omaisuusrekisteri**, joka sisältää organisaation ensisijaiset ja tukevat omaisuuserät.
- Miten rautateiden kunnossapitoprosessien pysähtyminen vaikuttaa liikenteeseen ja turvallisuuteen?
- Miten kunnossapitotoimintaan liittyvien tietojen saatavuuden, eheyden tai luottamuksellisuuden vaarantuminen vaikuttaa
 - Kunnossapitoprosesseihin (ydinliiketoimintaan)
 - Kolmannen osapuolen kanssa tehtyihin sopimuksiin
- Millä tukevilla omaisuuserillä (järjestelmät, laitteet, ihmiset, tilat tms.) on vaikutusta prosesseihin ja tietoihin?

Käytännön ohjeistusta

- Riskien tunnistaminen tapahtuu katselmoimalla järjestelmällisesti omaisuusrekisteriin kirjattuja omaisuuksia ja pohtimalla, että mitä **haavoittuvuuksia ja uhkia** niihin liittyy ja miten mahdollinen riski vaikuttaa toimintaan
- Riskien tunnistamisessa kannattaa hyödyntää myös ISO/IEC 27005:n esimerkkejä:
 - riskin lähteistä ja hyökkäysmenetelmistä
 - motivaatiotekijöistä ja
 - lopputavoitteista
- Mikäli johonkin omaisuuserään liittyy useita erilaisia haavoittuvuuksia ja uhkia, niin kannattaa kirjata useita erillisiä riskejä.

Esimerkkejä tunnistetuista riskeistä 1/2

Omaisuus (EN 17007)	Riskin kuvaus	Uhka (ISO/IEC 27005 taulukko A.10)	Haavoittuvuus (ISO/IEC 27005 taulukko A.11)
MAN-prosessi	Kunnossapidon kyberturvallisuuteen liittyviä vastuita ei ole määritelty	TO04 Lakien tai viranomaisvaatimusten rikkominen	VO14 Tietoturvavastuiden epäasiallinen osoittaminen
PRV-prosessi	Ennakoivan kunnossapidon suunnitelmat ovat kyberturvallisuuden kannalta riittämättömiä, jonka takia kunnossapidettävän kohteen kyberhaavoittuvuus jää paikkaamatta ja aiheuttaa tapahtuman	TI05 Tietoliikennelaitteiden vikaantuminen	VH02 Laitteistojen aikataulutettujen uusimissuunnitelmien riittämättömyys
BUD-prosessi	Kyberturvallisuutta ei osata huomioida riittävästi toiminnan budjetoinnissa ja seurannan ja valvonnan suorittamiseen ei varata riittävästi resursseja	TO02 Resurssivajeet	VP06 Seurantamekanismien puute tai riittämättömyys
DOC-prosessi	Kunnossapidon dokumentaatio ei ole riittävää tai ajantasaista ja kunnossapitotehtävä viivästyy tai estyy	TC01 Käyttövirhe	VS10 Dokumentaation riittämättömyys tai puuttuminen

Esimerkkejä tunnistetuista riskeistä 2/2

Omaisuus (EN 17007)	Riskin kuvaus	Uhka (ISO/IEC 27005 taulukko A.10)	Haavoittuvuus (ISO/IEC 27005 taulukko A.11)
SER-prosessi	Kunnossapitoon liittyviin sopimuksiin toisten osapuolten kanssa ei sisällytetä riittävästi kyberturvallisuuteen liittyviä vaatimuksia tai vaatimusten toteuttamista ei valvota	TO03 Palveluntarjoajan epäonnistuminen	VO09 Palvelutasosopimuksen puute tai riittämättömyys
SPP-prosessi	Purettujen komponenttien/varaosien varastointi- ja kierrätysprosessit eivät ole riittävän turvallisia ja ulkopuolinen tekijä pääsee käsiksi niihin ja niiden sisältämään tietoon	TH24 Tiedon luvaton käsittely	VH09 Huolimatonta käytöstä poistaminen
TOL-prosessi	Kunnossapidossa käytettäviä työkaluja ja laitteita (esim. mobiililaitteet, kannettavat tietokoneet, verkotetut mittalaitteet ja diagnostiikkajärjestelmät tms.) ei säilytetä turvallisesti	TH12 Laitteiston peukaloiminen	VS01 Rakennusten ja huoneiden kulunvalvonnan puutteellinen tai huolimatonta käyttö

Riskien analysointi

Riskien seurauksien arviointi

Tietojen luottamuksellisuuden, eheyden tai saatavuuden säilyttämisen epäonnistumisesta syntyvät seuraukset tunnistetaan ja arvioidaan.

Seurauksien arvioinnissa kannattaa hyödyntää EN 17007-standardin prosessikuvausten sisältöä ja ISO/IEC 27005 ohjeistuksia.

Riskien todennäköisyyksien arviointi

Mahdollisten tai todellisten skenaarioiden todennäköisyydet arvioidaan ja ilmaistaan käyttäen laadittuja todennäköisyyttä koskevia kriteereitä.

Riskitasojen määrittäminen

Riskitasot määritetään kaikkien olennaisiksi katsottujen riskiskenaarioiden arvioitujen todennäköisyyksien ja arvioitujen seurausten yhdistelmänä.

	Seuraus					
		1	2	3	4	5
Todennäköisyys	5					
	4					
	3					
	2					
	1					

Riskien merkittävyyden arviointi

Riskien merkittävyyden arviointi

Riskitasoja verrataan riskien merkityksen arviointikriteereihin, etenkin hyväksymiskriteereihin.

Arvioinnissa tehtävä priorisointi perustuu pääasiassa hyväksymiskriteereihin.

Riskien priorisointi

Riskit priorisoidaan merkittävyyden arvioinnin jälkeen käsittelyä varten.

Riskitaso	Riskin merkittävyyden arviointi	Kuvaus
Erittäin korkea	Sietämätön riski	Riskiä ei voida hyväksyä
Korkea	Korkea riski, joka voidaan hyväksyä vain poikkeuksellisissa olosuhteissa	Riskiä ei voida hyväksyä normaalioloissa. Poikkeusoloissa riskin hyväksymisestä vastaa johtoryhmä. Riskiä on seurattava jatkuvasti, vähintään kuukausittain.
Keskinkertainen	Hallittu ja valvottu riski	Riskin voidaan hyväksyä, mutta sen poistamiseen tai pienentämiseen liittyviä käsittelytoimenpiteitä on tehtävä lyhyellä aikavälillä ja riskiä on seurattava vähintään kvartaaleittain.
Matala	Hallittu riski	Riski voidaan hyväksyä. Ei tarvetta jatkuvalle seurannalle, mutta riskin pienentämiseksi olisi tehtävä toimenpiteitä osana vuosittaista jatkuvan parantamisen suunnitelmaa.
Erittäin matala	Merkityksetön riski	Riski voidaan hyväksyä ilman toimenpiteitä. Ei tarvetta seurannalle.

Riskien käsittely

Riskien käsittelyvaihtoehtojen valinta

- Monimutkaisessa toimintaympäristössä on huomioitava muut tahot (tilaaja, toimittaja, alihankkijat, muut osapuolet).
- Riskien omistajuuden määrittäminen ja käsittely tulisi myös tehdä.

Hallintakeinojen määrittäminen

- Hallintakeinojen määrittämisessä on huomioitava myös muut tahot ja niiden vaatimukset.
- Sopimukseen sisältyy yleensä tietoturva vaatimuksia, jotka liittyvät usein tunnistettuihin riskeihin.

Omaisuus (EN 17007)	Riskin kuvaus	Riskitaso	Hallintakeino(t)
SPP-prosessi	Purettujen komponenttien/varaosien varastointi- ja kierrätysprosessit eivät ole riittävän turvallisia ja ulkopuolinen tekijä pääsee käsiksi niihin ja niiden sisältämään tietoon	Korkea	Määritellään ja otetaan käyttöön turvallinen varastointi- ja kierrätysprosessi, joka sisältää pääsynhallinnan, fyysisen suojauksen sekä tietoa sisältävien komponenttien tietoturvallisen tyhjennyksen tai tuhoamisen ennen varastointia ja luovutusta. Prosessin noudattamista valvotaan sopimusehdoilla, ohjeistuksella ja säännöllisillä tarkastuksilla.

KYSYMYKSET JA VASTAUKSET

