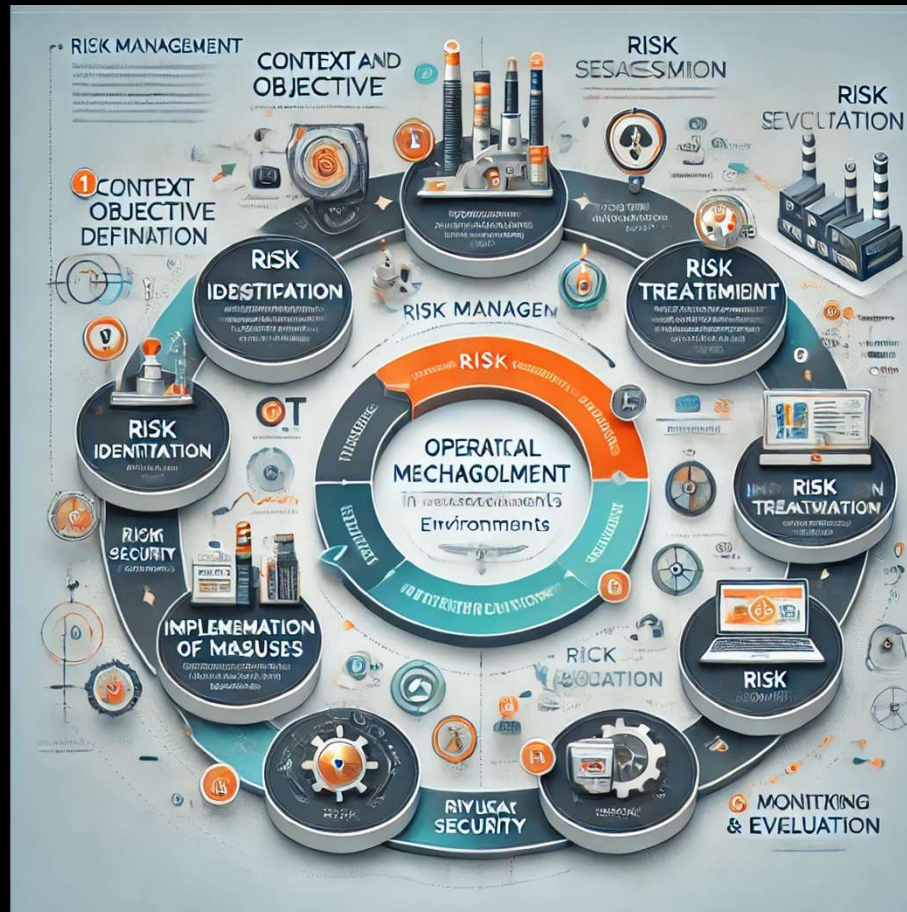


**Tunne huominen.**



Kaakkois-Suomen  
ammattikorkeakoulu

# OT-ympäristöjen Riskienhallinta



Kaakkois-Suomen ammattikorkeakoulu  
South-Eastern Finland University of Applied Sciences

[www.xamk.fi](http://www.xamk.fi)



Kaakkois-Suomen  
ammattikorkeakoulu

# OT-ympäristöjen riskienhallinta

OT-ympäristöjen riskienhallinta keskittyy teollisten ja kriittisten infrastruktuurijärjestelmien, kuten automaatiojärjestelmien, valvonta- ja hallintajärjestelmien (SCADA), prosessinohjausjärjestelmien (DCS) ja fyysisten laitteiden turvallisuuteen. Sen päätavoitteena on varmistaa toimintojen saatavuus, turvallisuus ja luotettavuus, koska häiriöt OT-ympäristöissä voivat aiheuttaa vakavia fyysisiä, taloudellisia ja ympäristöllisiä seurauksia.



Kaakkois-Suomen  
ammattikorkeakoulu

# OT-ympäristön erityispiirteet

## 1. Prioriteetit:

- Saatavuus on kriittisin tekijä – järjestelmien keskeytykset voivat johtaa tuotantopysähdyksiin tai turvallisuusriskeihin.
- Turvallisuus on keskeistä, koska OT-ympäristöt voivat aiheuttaa fyysistä vahinkoa ihmisille tai infrastruktuurille.
- Eheys on tärkeää, koska prosessien häiriöt tai manipulointi voivat vaikuttaa tuotannon laatuun.

## 2. Teknologian erityispiirteet:

- Monissa OT-järjestelmissä käytetään ikääntyneitä järjestelmiä, jotka eivät tue nykyaikaisia tietoturvamekanismeja.
- OT-ympäristöjen laitteet ovat usein jatkuvassa käytössä, mikä rajoittaa huolto- ja päivitysmahdollisuuksia.
- OT-järjestelmät on suunniteltu toimimaan fyysisessä maailmassa, mikä lisää niiden altistumista ympäristön ja ihmisten toiminnalle.

## 3. Integraatio IT-ympäristöihin:

- OT-järjestelmät ovat yhä useammin kytkettyjä IT-verkoihin, mikä altistaa ne IT-maailman kyberuhille.



Kaakkois-Suomen  
ammattikorkeakoulu

# OT-ympäristöjen riskienhallinnan prosessi

## 1. Tavoitteiden ja kontekstin määrittäminen

- Määritellään kriittiset järjestelmät ja niiden merkitys tuotannolle ja turvallisuudelle.
- Selvitetään liiketoiminnan vaatimukset, kuten laatu, tehokkuus ja turvallisuus.
- Tunnistetaan sidosryhmät, kuten operaattorit, johto, asiakkaat ja viranomaiset.



Kaakkois-Suomen  
ammattikorkeakoulu

# OT-ympäristöjen riskienhallinnan prosessi

## 2. Riskien tunnistaminen

Riskien tunnistaminen OT-ympäristössä sisältää fyysisten ja kyberuhkien sekä teknologisten haavoittuvuuksien analyysin.

### a) Uhkat:

- Fyysiset uhkat: Laitteiden vahingoittuminen, sabotaasi tai luonnonkatastrofit.
- Kyberuhkat: Haittaohjelmat, tietomurrot, kiristysohjelmat, DDoS-hyökkäykset.
- Ihmisten aiheuttamat uhkat: Tahalliset väärinkäytökset tai vahingossa tehdyt virheet.



Kaakkois-Suomen  
ammattikorkeakoulu

# OT-ympäristöjen riskienhallinnan prosessi

## b) Haavoittuvuudet:

- Vanha teknologia: Monissa OT-järjestelmissä käytetään laitteita, jotka ovat yli 20 vuotta vanhoja ja eivät tue moderneja turvamekanismeja.
- Rajoitettu päivitettävyyys: Järjestelmien jatkuva käyttö estää säännölliset päivitykset.
- Puutteellinen eristys: OT- ja IT-järjestelmät voivat olla kytkettyinä ilman riittävää segmentointia.

## c) Altistukset:

- Julkiset verkot: Jos OT-järjestelmät ovat yhteydessä internetiin, ne voivat olla alttiita ulkoisille hyökkäyksille.
- Etäkäyttö: Huonosti suojatut etäyhteydet voivat tarjota hyökkääjille pääsyn kriittisiin järjestelmiin.



Kaakkois-Suomen  
ammattikorkeakoulu

# OT-ympäristöjen riskienhallinnan prosessi

## 3. Riskiarviointi

OT-ympäristöjen riskit arvioidaan niiden todennäköisyyden ja vaikutusten perusteella.

### ➤ **Todennäköisyyden arviointi:**

- ✓ Kuinka helppoa on hyödyntää järjestelmän haavoittuvuuksia?
- ✓ Kuinka usein vastaavia uhkia on havaittu?

### ➤ **Vaikutusten arviointi:**

- ✓ Fysiset vaikutukset: Vahingot infrastruktuurille tai ympäristölle.
- ✓ Taloudelliset vaikutukset: Tuotannon menetykset ja korjauskustannukset.
- ✓ Turvallisuusvaikutukset: Henkilövahingot tai -kuolemat.



Kaakkois-Suomen  
ammattikorkeakoulu

# OT-ympäristöjen riskienhallinnan prosessi

## 4. Riskien käsittely

OT-ympäristöissä riskien käsittelystrategiat painottavat toimintojen jatkuvuutta ja turvallisuutta.

### ➤ Riskin välttäminen:

- ✓ Vältetään järjestelmien liittämistä ulkoisiin verkkoihin.
- ✓ Suunnitellaan prosessit, jotka minimoivat vaarallisten tilanteiden todennäköisyyden.

### ➤ Riskin vähentäminen:

- ✓ Segmentoidaan verkot (esim. IT- ja OT-järjestelmät erillään).
- ✓ Käytetään intrusion detection -järjestelmiä (IDS) havaitsemaan epäilyttävää liikennettä OT-verkoissa.
- ✓ Päivitetään ohjelmistot ja laitteet kriittisissä järjestelmissä.

### ➤ Riskin siirtäminen:

- ✓ Ulkoistetaan järjestelmien valvonta asiantuntijapalveluille.
- ✓ Otetaan vakuutuksia, jotka kattavat tuotannon keskeytyksestä aiheutuvat tappiot.

### ➤ Riskin hyväksyminen:

- ✓ Hyväksytään riskit, jotka ovat vähäisiä tai joiden käsittely on liian kallista suhteessa riskiin.



Kaakkois-Suomen  
ammattikorkeakoulu

# OT-ympäristöjen riskienhallinnan prosessi

## 5. Toimenpiteiden toteutus

- Asennetaan fyysisiä suojia kriittisiin kohteisiin, kuten kulunvalvonta ja valvontakamerat.
- Varmistetaan, että etäyhteydet ovat suojattuja esimerkiksi VPN:llä ja kaksivaiheisella tunnistautumisella.
- Kehitetään henkilöstön kyberturvallisuustietoisuutta ja tarjotaan koulutusta OT-järjestelmien turvalliseen käyttöön.



Kaakkois-Suomen  
ammattikorkeakoulu

# OT-ympäristöjen riskienhallinnan prosessi

## 6. Seuranta ja arviointi

- Seurataan OT-järjestelmien toimintaa reaaliajassa käyttämällä valvontajärjestelmiä.
- Analysoidaan poikkeamat ja päivitetään riskienhallintasuunnitelmia säännöllisesti.
- Tehdään säännöllisiä testauksia ja auditointeja varmistaakseen, että järjestelmät ovat suojattuja.



Kaakkois-Suomen  
ammattikorkeakoulu

# Haasteet OT-ympäristöjen riskienhallinnassa

- **Vanhat järjestelmät:** Monilla OT-laitteilla ei ole moderneja tietoturvamekanismeja.
- **Keskeytysten rajoitukset:** Päivitysten ja huoltotoimenpiteiden toteutus voi olla vaikeaa, koska järjestelmien on oltava jatkuvasti käytössä.
- **Integraatio IT-järjestelmiin:** IT- ja OT-ympäristöjen yhteyksien lisääntyminen altistaa OT-järjestelmät IT-pohjaisille uhkille.



Kaakkois-Suomen  
ammattikorkeakoulu

# OT-ympäristöjen riskienhallinnan merkitys

- **Turvallisuus:** Varmistaa, ettei ihmishenkiä tai ympäristöä vaaranneta.
- **Toimintavarmuus:** Estää tuotannon keskeytykset ja taloudelliset tappiot.
- **Regulaation noudattaminen:** OT-ympäristöissä noudatetaan usein erityisiä säädöksiä, kuten NERC CIP (energiasektori) tai IEC 62443 (teollisuusautomaatio).

Hyvin toteutettu riskienhallinta OT-ympäristöissä auttaa organisaatiota suojaamaan kriittiset toiminnot ja vähentämään vakavien häiriöiden todennäköisyyttä ja vaikutuksia.



Kaakkois-Suomen  
ammattikorkeakoulu



**Tunne huominen.**