IoT-järjestelmät (Internet of Things) yleistyvät nopeasti myös kunnallisessa automaatiossa – esimerkiksi vedenjakelussa, jäteveden käsittelyssä, energiaverkoissa ja rakennusautomaatiossa. Niiden avulla saadaan tehokkuutta, reaaliaikaista dataa ja etäohjausmahdollisuuksia. Samalla ne altistuvat kyberturvallisuusuhille.

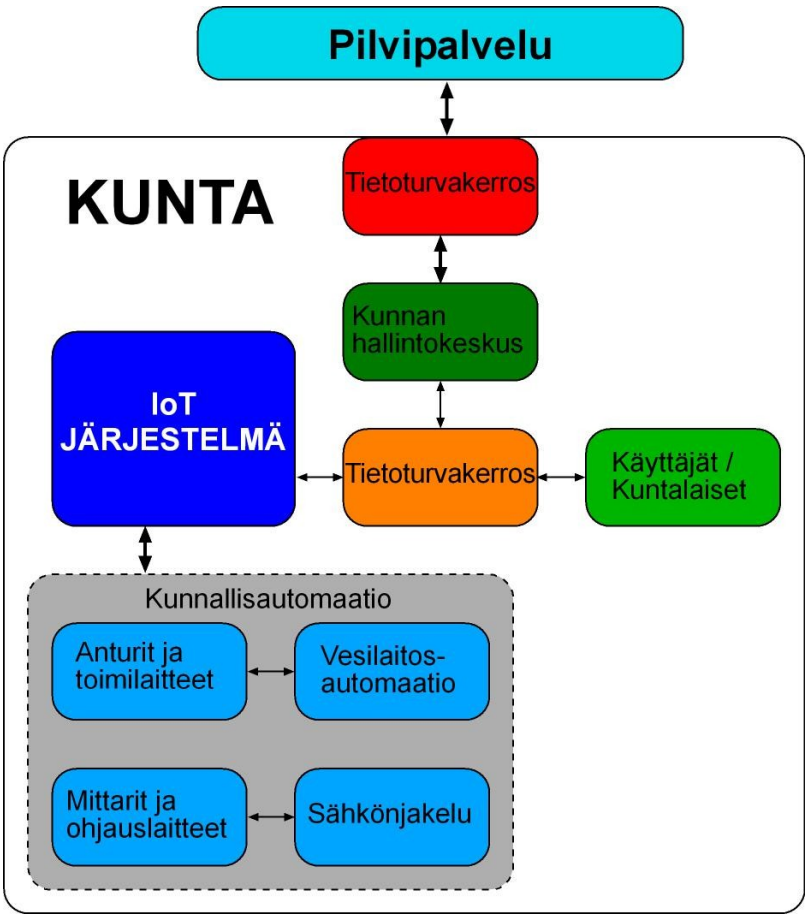
1. **Haavoittuvat laitteet**
   - Monet IoT-laitteet toimitetaan oletussalasanoilla tai vanhentuneilla ohjelmistoilla ja laitteiden valmistajat eivät aina tarjoa päivityksiä tai tukea koko käyttöiän ajan.
2. **Tietoturvattomat yhteydet**
   - Puutteellisesti salattu verkkoliikenne voi mahdollistaa salakuuntelun, ohjauskäskyjen kaappaamisen tai muuntamisen.
3. **Keskitetyt hallintajärjestelmät**
   - Jos kunnallistekniikan valvomoon päästään käsiksi, voidaan lamauttaa kokonaisia prosesseja (esim. vedenpumppaus).

Sabotointimahdollisuudet kunnallisessa automaatiossa

- **Palvelunestohyökkäykset**: IoT-laitteita voidaan kaapata bottiverkoiksi, jotka kuormittavat ohjausjärjestelmiä.
- **Tietojen väärentäminen**: Anturidatan manipulointi voi johtaa virheellisiin päätöksiin (esim. vedenlaadun mittarit näyttävät puhdasta vettä, vaikka näin ei ole).
- **Etäohjauksen kaappaaminen**: Jos hyökkääjä saa pääsyn hallintajärjestelmään, hän voi estää pumppuja tai valaistusta toimimasta.
- **Fyysinen sabotaasi**: Laitteiden irrottaminen, vahingoittaminen tai luvaton kytkentä voi häiritä koko verkkoa.
- **Kriittisen infrastruktuurin häiriö**: Pahimmillaan sabotaasi voi kohdistua vedenjakeluun ja sähköverkkoon, mikä vaarantaa turvallisuutta ja luottamusta.

Riskienhallintakeinoja

- **Tietoturvapäivitykset ja haavoittuvuuksien hallinta**.
- **Verkkosegmentointi**: erotetaan kunnallisautomaatio julkisista verkoista.
- **Vahva tunnistautuminen ja salaus**.
- **Lokien seuranta ja poikkeamien havaitseminen**.
- **Henkilöstön koulutus** ja selkeät toimintasuunnitelmat poikkeustilanteisiin.
- **Fyysinen suojaus** kenttälaitteille.



IoT:n riskit kunnallistekniikassa

Haavoittuvat laitteet (oletussalasanat, päivittämättömät järjestelmät)	Hyökkääjä saa etäyhteyden yksittäiseen laitteeseen, esim. vedenottamon pumpun ohjaimeen.
Tietoturvattomat yhteydet (salaamattomat protokollat)	Ohjauskäskyjä siepataan tai muokataan, esim. pumppuasemat reagoivat virheellisesti.
Keskitetyn hallintajärjestelmän kaappaus	Kokonainen vedenjakeluverkko tai sähköverkko lamaantuu.
Fyysinen sabotaasi kenttälaitteille	Anturi tai ohjainrikko aiheuttaa paikallisia häiriöitä (esim. pumppu sammuu).
Palvelunestohyökkäys (DDoS)	Etävalvontajärjestelmä tukkeutuu, huoltotoiminta vaikeutuu.
Anturidatan manipulointi	Esim. vedenlaadun mittaus vääristyy, viranomaiset eivät reagoi saastumiseen ajoissa.
Toimitusketju- ja ohjelmistoriski	Haittakoodi leviää päivitysten mukana useisiin kunnallisiin laitteisiin yhtä aikaa.

Palvelunestohyökkäys

- **Englanniksi DDoS (distributed denial of service)**
- **Keinotekoisesti tuotettu "digitaalinen liikenneruuhka", jossa kohdepalvelinta pommitetaan tietopyynnöillä niin intensiivisesti, että se ei ehdi vastaamaan ja vaipuu saavuttamattomiin.**
- **Toteutetaan ohjelmallisesti kaapatuista älylaitteista rakennetuilla bottiverkoilla.**
- **Bottiverkon laitteet eli ”zombit” voivat olla esimerkiksi tietokoneita, reitittimiä tai valvontakameroita – käytännössä melkein mitä vain nettiin kytkettyjä laitteita.**
- **Palvelunestohyökkäys ei vaadi teknisiä kykyjä, sillä sellaisen voi ostaa harmailta markkinoilta.**
- **Palvelunestohyökkäys ei ole tietomurto, sillä siihen ei liity järjestelmään tunkeutumista. Se rinnastuu lähinnä ilkivaltaan.**
- **Käytetään muun muassa kiristyksiin, poliittisiin voimannäyttöihin, aktivismiin ja häirintään.**
- **Palvelunestohyökkäys on rikos. Poliisi kehottaa tekemään siitä rikosilmoituksen.**