AgOpenGPS-pohjaisen RTK-tukiaseman käytännön tietoturva

25.8.2025

AgOpenGPS-pohjaisen RTK-tukiaseman tietoturva nojaa neljään perusasiaan: oikein konfiguroitu ja ajantasainen GNSS-vastaanotin sekä tukiasemaohjelmisto, salattu korjausdatan siirto (esim. TLS) käyttäjätunnistuksella, verkon minimialtistus ilman anonyymikäyttöä sekä ennalta testattu toipumismalli (varmistukset ja vaihtoehtoinen korjauslähde). Fyysinen suojaus, maadoitus ja hyvä RF-ympäristö vähentävät häiriöitä. Suomessa GNSS-häirintä on realistinen riski, johon on varauduttava etukäteen määritellyllä toimintamallilla (siirtyminen varakorjaukseen tai ohjauspään automaation keskeytys).

Ympäristö, fyysinen suojaus ja RF-olosuhteet

Kenttäkäytön luotettavuus rakentuu pitkälti sijoittelusta ja rakenteista. Antennille haetaan esteetön taivasnäkymä ja elektroniikka sijoittuu tyypillisesti sääsuojattuun, lukittuun koteloon. GNSS-häiriöitä (jamming/spoofing) raportoidaan laajasti, joten käyttötavoissa varaudutaan tilanteisiin, joissa korjaus katoaa tilapäisesti. Tällöin siirrytään varakorjaukseen tai ohjauksen automaatio keskeytetään, kunnes signaali palautuu. Viranomaiset julkaisevat säännöllisesti tilannekuvaa tapahtuneista häirinnöistä ja tahallinen häirintä on useimmiten kiellettyä (Traficom 2024; Traficom 2025).

Vastaanotin ja ohjelmistot: konfigurointi ja

päivitykset

Vastaanottimen toiminta osoittautuu vakaimmaksi, kun firmware ja kokoonpanot ovat ajantasaisia ja asetukset tallennettu pysyviksi. Toistuvat häiriöt kytkeytyvät samoihin lähteisiin: sarjaliikenteen siirtonopeuden epäyhteensopivuuksiin, asetusten jäämiseen volatile-tilaan sekä käynnistyksiin ilman antennia—kaikki ilmiöitä, jotka kentällä näyttäytyvät “selittämättöminä” katkoksina (u-blox 2024; AgOpenGPS Documentation 2025).

Korjausdatan siirto ja verkkoarkkitehtuuri

NTRIP-ympäristöissä arki rakentuu käytänteille, joissa mountpoint, käyttäjäkohtaiset tilit ja salasanat muodostavat perustan, ja liikenne kulkee päästä päähän salattuna (esim. TLS/HTTPS), jolloin sekä tunnukset että data pysyvät suojattuina. Jos caster ei tarjoa salausta, käänteisproxy tai suojattu tunneli toimii tavanomaisena ratkaisuna. Verkkonäkymässä vastaanotin ja caster pysyvät palomuurin ja NATin takana, ja ulospäin näkyy vain välttämätön. NTRIPissä vakiintuneesti 2101/TCP, salatuissa toteutuksissa usein 443/TCP. Oikeuksia rajataan vähimmän etuoikeuden periaatteella, eikä anonyymejä kirjautumisia tyypillisesti käytetä. Lisäksi tapahtumien lokituksella parannetaan jäljitettävyyttä (Söhne 2016; BKG 2016; SNIP 2024).

Jatkuvuus, toipumismalli ja sääntely

Käyttökatkoja lyhennetään pitämällä saatavilla palautusmedia (esim. levykuva), versioimalla vastaanottimen ja ohjelmistojen konfiguraatiot ja pitämällä kriittiset vaihtokomponentit helposti käsillä. Ohjausohjelmistoon määritellään etukäteen varakorjauslähde, ja palautusprosessi testataan säännöllisesti, jotta toimet ovat toistettavissa myös kiireessä. Sääntely viitoittaa radiolähettimien käyttöä taajuus- ja tehorajoineen sekä lupaehtoineen. Tässä tapauksessa vaatimustenmukaisuus ja EMC kuuluvat kokonaisuuteen ja tahallinen GNSS-häirintä luokitellaan tyypillisesti lainvastaiseksi. Käytännön kompastuskivet toistuvat: salasanoitta jätetyt tai yhteistunnuksilla toimivat casterit, “varmuuden vuoksi” avatut ylimääräiset portit, vanhentunut firmware tai epäyhteensopivat konfiguraatiot, pysyvän tallennuksen puuttuminen, virheellinen sarjanopeus, käynnistykset ilman antennia sekä päivittämättömät päätelaitteet vähentävät käytetyn kokoonpanon tietoturvaa (AgOpenGPS Documentation 2025; Traficom 2024).

Agropilotti- ”Tee-se-itse” automaattiohjaus on Euroopan unionin osarahoittama hanke. Tutustu hankkeeseen: https://projektit.seamk.fi/alykkaat-teknologiat/agropilotti/.

FarmGuard – Maatilojen ja puutarhojen kyberturvallisuuden vahvistaminen käytännön keinoin on Euroopan unionin osarahoittama hanke. Tutustu hankkeeseen: https://projektit.seamk.fi/kestavat-ruokaratkaisut/farmguard-maatilojen-ja-puutarhojen-kyberturvallisuuden-vahvistaminen-kaytannon-keinoin.

Matti Saari
SEAMK

Kirjoittaja toimii SEAMKissa projektipäällikkönä. Hän sijaisti Agropilotti-hankkeen projektipäällikköä vuonna 2025 ja toimii FarmGuard-hankkeen projektipäällikkönä.

Juho Pirttilahti
SEAMK

Kirjoittaja toimii SEAMKissa TKI-asiantuntijana. Hän vetää Agropilotti-hanketta.

Lähteet

AgOpenGPS Documentation. (2025). *AgOpenGPS – RTK Setup; AgIO NTRIP Client*. Haettu 13.8.2025, https://github.com/AgOpenGPS

BKG (Bundesamt für Kartographie und Geodäsie). (2016). *Professional NtripCaster (BKG) – Dokumentaatio / Ntrip Client/Server -ohjeistus*. Haettu 13.8.2025, https://igs.bkg.bund.de

SNIP (SubCarrier Systems Corp.). 2024. *SNIP Caster Knowledge Base (TLS/HTTPS, autentikointi ja portit*). Haettu 13.8.2025, https://www.use-snip.com

Söhne, W. 2016. *NTRIP – The Protocol (Networked Transport of RTCM via Internet Protocol). BKG/RTCM-työryhmä.* Haettu 13.8.2025, https://igs.bkg.bund.de

Traficom. 2024. *GNSS-häiriötilannekuva ja häiriöiden seuranta.* Haettu 13.8.2025, https://www.traficom.fi

Traficom. 2025. *GNSS-häirinnän kielto ja radiolaitteiden vaatimustenmukaisuus.* Haettu 13.8.2025, https://www.traficom.fi

u-blox. 2024. ZED-F9P Integration Manual; u-center User Guide. Haettu 13.8.2025: https://www.u-blox.com