

Fingrid Oyj

~~Reservien~~
~~käyttövarmuusvaatimukset~~Reservien
toimitusvarmuusvaatimukset

28.10.2025

1 Muutostenhallinta:

versio 1.0 (12.5.2025)

1 Muutostenhallinta:

- [versio 1.1 \(28.10.2025\)](#)
- [versio 1.0 \(12.5.2025\)](#)

2 Johdanto

Tämän dokumentin tarkoituksena on määritellä reservien ylläpitoon liittyvät ~~käyttövarmuusvaatimukset~~ toimitusvarmuusvaatimukset. Dokumentti käsittelee mm. tietoturvaan, toimintojen kahdentamiseen sekä poikkeamienhallintaan liittyviä vaatimuksia. ~~Esitettyjen vaatimusten täyttäminen tulee osoittaa reservikohteen hakemuslomakkeessa. Dokumentissa määritetyt vaatimukset tarkentavat seuraavien asiakirjojen yleisvaatimuksia keskitettyjen ohjaus- ja kaupankäyntijärjestelmien kuvauksesta sekä niiden ominaisuuksista:~~

~~Ehdot ja edellytykset nopean taajuusreservin (FFR) toimittajalle~~

~~Ehdot ja edellytykset taajuuden vakautusreservin (FCR) toimittajalle~~

~~Ehdot ja edellytykset automaattisen taajuuden palautusreservin (aFRR) toimittajalle~~

~~Ehdot ja edellytykset manuaalisen taajuuden palautusreservin (mFRR) toimittajalle~~

Yleiset tekniset vaatimukset ja tarvittavat säätökokeet on määritelty seuraavissa dokumenteissa:

- *Nopean taajuusreservin (FFR) teknisten vaatimusten todentaminen ja hyväksyttämismenettely*
- *Taajuuden vakautusreservin (FCR) teknisten vaatimusten todentaminen ja hyväksyttämismenettely*
- Automaattisen taajuuden palautusreservin (aFRR) teknisten vaatimusten todentaminen ja hyväksyttämismenettely
- -Manuaalisen taajuuden palautusreservin (mFRR) teknisten vaatimusten todentaminen ja hyväksyttämismenettely

Dokumentit ovat saatavilla Fingridin internetsivuilla, ks. liitteet tuotekohtaisilla sivuilla.

Reservitoimittaja vastaa itse omista reservikohteistaan sekä järjestelmistään. Dokumentin ehtojen noudattaminen ei siis automaattisesti takaa esimerkiksi vakuutusyhtiön fyysistä- tai kyberturvallisuutta koskevien sopimusehtojen täyttymistä.

Myöhemmin tässä dokumentissa vaaditut prosessi- sekä järjestelmäkuvaukset ovat lähtökohtaisesti reservitoimijan omaan käyttöön, ellei niitä vaadita erikseen osana reservikohteen hakemuslomaketta. Fingrid voi kuitenkin sopia toimijan kanssa erillisen auditoinnin suorittamisesta, mikäli katsoo sen tarpeelliseksi. Tapauksissa, joissa kuvaus vaaditaan osana reservikohteen hakemuslomaketta, annetut vaatimukset määrittävät kuvauksen vähimmäislaajuuden. Esimerkkinä tällaisesta tapauksesta alaluku 3.1.1, joka käsittelee keskitettyjen ohjausjärjestelmien arkkitehtuurin kuvausta.

Fingrid voi perustellusta syystä myöntää siirtymäajan tässä asiakirjassa esitettyjen

vaatimusten käyttöönotolle tai poikkeuksia yksittäisten vaatimusten osalta. Esimerkkinä tällaisesta tapauksesta siirtymäajan myöntäminen kameravalvonnan toteuttamiseen säätökokeiden uusinnan yhteydessä.

2.1 Lyhenteet ja määritelmät

Määritelmiä:

Keskitetty ohjausjärjestelmä: Järjestelmä välittää tehokomentoja sen piirissä oleville reservikohteille ja niiden alaisille reserviresursseille.

Keskitetty kaupankäyntijärjestelmä: Järjestelmä välittää tiedon ylläpidettävästä kapasiteetista paikallisesti ohjatuille reservikohteille. Voidaan soveltaa FCR-N, FCR-D ja FFR reserveillä.

Operatiivinen taho: Reservitoimittaja tai valtuutettu edustaja (esim. palveluntarjoaja), joka pystyy muokkaamaan reservikohteen tarjouksia, seuraamaan aktivointia, muuttamaan reservikohteen tilaa ja aloittamaan tarvittaessa vianselvityksen.

Reservikohde: Tarkoitetaan kokonaisuutta, joka täyttää reservin tarjoamista koskevat vaatimukset. Reservikohde voi koostua useasta tai yhdestä Reserviresurssista.

Reserviresurssi: Tarkoitetaan yksittäistä säätökykyistä resurssia; voimalaitosta, kulutuskohdetta tai energiavarastoa.

Reservitoimittaja: Fingridin sopimuskumppani, joka tarjoaa, ylläpitää ja aktivoi reserviä.

IT-tuki: IT-tuella tarkoitetaan sitä tahoaa, jolla on tarvittavase tietämys ja osaaminen koko tuotettavan palvelun ylläpitämiseksi, ongelmien rajaamiseksi, ratkaisemiseksi sekä korjaamiseksi. IT-tuki voi olla sisäistä, ulkoista tai koostua useammasta osapuolesta. Oleellista on, että palvelua tuottava taho on sopinut vastuut ja palvelutasot ja -ajat tuotettavalle palvelulle ja että ne ovat johdonmukaiset ja yhteneväiset erityisesti silloin, kun palvelussa on mukana useampia osapuolia. IT-tuen tulee kattaa koko palvelun tuottamiselle oleelliset komponentit, laitteistot, sovellukset ja lisenssit.

Monivaiheinen tunnistus: Monivaiheisella tunnistuksella tarkoitetaan MFA-määritystä (Multi-Factor Authentication), eli tunnistautuminen varmistetaan vähintään kahdella eri tunnistautumistavalla. Lisätietoja Traficomin sivuilta aiheesta "monivaiheinen tunnistautuminen".

2.2 Vaatimusten käyttöönotto

Uusille reservikohteille vaatimukset tulevat voimaan dokumentin alussa mainittuna päivänä. Ennen tämä dokumentin voimaantuloa hyväksytyille reservikohteille vaatimukset tulevat voimaan niiden säätökokeiden uusinnan yhteydessä tai viimeistään 5 vuoden kuluessa tämän dokumentin voimaantulosta. Mikäli reservikohde on riippuvainen keskitetystä kaupankäynti- tai ohjausjärjestelmästä, siirtyvät nämä järjestelmät vaatimusten piiriin kohteen säätökoeprosessin (ensimmäinen tai uusintakoe) tai markkinoille hyväksymisprosessin aikana.

2.2 1.1 Muutostenhallinta:

— versio 1.0 (12.5.2025)

3

Yleiset käyttövarmuusvaatimukset toimitusvarmuusvaatimukset

Tässä luvussa esitetyt käyttövarmuusvaatimukset toimitusvarmuusvaatimukset liittyvät yleisesti reservin ylläpitoon. Vaatimukset pätevät kaikille reservituotteille sekä kaikille reserviä ylläpitäville reservitoimittajille ja heidän palveluntoimittajilleen.

Yleisvaatimus 1: Toimija vastaa siitä, että reservikohde toimii asetettujen vaatimusten mukaisesti, kun sillä ylläpidetään reserviä.

Yleisvaatimus 2: Kohteen operatiivisen tahon tulee olla tavoitettavissa puhelimitse, kun ylläpidetään reserviä.

Yleisvaatimus 3: Yksittäisen vian takana oleva ylläpidetty reservikapasiteetti saa olla enintään:

- 50 MW FFR
- ⊖ 70 MW FCR-N tai FCR-D reserviä
-
- 70 MW aFRR reserviä
- Yhteensä 100 MW FCR-N ja FCR-D reserviä
- ⊖
- Yhteensä 200 MW FCR-N, FCR-D, FFR, aFRR ja mFRR reserviä
- Lisäksi kohteilla, jotka kuuluvat Olkiluoto 3 järjestelmäsuojaan on voimassa seuraavat rajoitus:
 - Yhteensä 70 MW FFR ja Olkiluoto 3 järjestelmäsuojaan kapasiteettia.
 - Yhteensä 200 MW FCR-N, FCR-D, FFR, aFRR, mFRR reserviä ja Olkiluoto 3 järjestelmäsuojaan kapasiteettia.

Mikäli reservin ylläpito on toteutettu siten, että siinä ei ole yksittäistä vikaa, joka voisi estää reservin ylläpidon kokonaisuudessaan, ylläpidetylle kapasiteetille ei ole rajoitusta. Tämä voidaan toteuttaa mm. järjestelmän redundanttisuudella. Huomioitavia asioita:

- Esimerkkejä yksittäisistä vioista ovat: sähkötekkinen vika, tietojärjestelmän vikaantuminen, tietojärjestelmän vikaantuminen, laiterikko tai tietoliikennekatkos.
- Reservitoimittaja on vastuussa palveluntarjoajan vikasietoisuudesta.
- Redundanssin ei tule perustua yksinomaan toimintojen kahdentamiseen saman laitteiston tietojärjestelmän sisällä, vaan erillisillä toisistaan riippumattomilla komponenteilla ja laitteilla. (esim. klusterointi HA-ratkaisuilla).

RAID-tekniikka tiedon tallennuksessa, kahdenneetut tietoliikenneyhteydet eri operaattoreilta)

- Kahdennuksen riittävyys varmistetaan käymällä toteutus erikseen läpi Fingridin kanssa ja hyväksyttämällä se Fingridillä.

○

Ohjeita kahdennusvaatimuksen tulkintaan:

- mFRR tapauksessa kahdentamisvaatimus katsotaan täyttyneeksi välillä Fingrid - Reservitoimija, mikäli Fingrid pystyy aktivoimaan säätötarjouksia puhelinsoitolla reservitoimittajan valvomoon. Puhelinsoitto katsotaan myös riittäväksi kahdennustoimeksi välillä Reservitoimijan valvomo - Reservikohde, mikäli aktivoinnit tapatuvat normaalisti toista väylää käyttäen.

Yleisvaatimus 4: Reservitoimittaja vastaa reservikohteiden kaupankäynnin ja ylläpidon suunnittelusta siten että ylläpito on teknisesti mahdollista. Reservien ylläpidossa tulee ottaa huomioon, että muille reservituotteille tai muihin käyttötarkoituksiin varattua teho- ja energiakapasiteettia ei saa tarjota markkinoille kahdesti.

3.1

Fyysinen- ja kyberturvallisuus

~~Alla olevilla vaatimuksilla pyritään luomaan IT-kontrollien kokonaisuus, jossa turvallisuus ja tietoturvallisuus ei nojaudu yksittäisen komponentin taakse, vaan tukeutuu monikerroksisuuteen, jossa yhden komponentin pettäminen ei vielä mahdollistaisi järjestelmän täydellistä murtumista.~~

32.1.1

Kyberturvallisuus

Alla olevilla vaatimuksilla pyritään luomaan IT-kontrollien kokonaisuus, jossa turvallisuus ja tietoturvallisuus ei nojaudu yksittäisen komponentin taakse, vaan tukeutuu monikerroksisuuteen, jossa yhden komponentin pettäminen ei vielä mahdollistaisi järjestelmän täydellistä murtumista.

Vaatimus 1: Käytännöt ja maantieteellinen sijainti. Fyysisen- sekä kyberturvallisuuden tulee olla alan hyvien käytänteiden mukaisella tasolla, kuten noudattaa direktiivin NIS2:ta tai jastandardin ISO27001 käytänteitä ja yleistä tietosuoja-asetusta (GDPR). Kaupankäynti- ja ohjausjärjestelmien tietojärjestelmien tulee sijaita maantieteellisesti Euroopan unionin sisämarkkina-alueella.

Vaatimus 2: Vahva tunnistus. Kaikkien käyttäjien kaksivaiheinen monivaiheinen tunnistautuminen on käytössä aina ennen ohjaus- tai kaupankäyntijärjestelmän komponentteihin pääsyä. IP-rajauksen tulee sallia vain toiminnan kannalta välttämättömät rajapintayhteydet ja se tulee ottaa käyttöön aina kun se on teknisesti mahdollista toteuttaa. Tällä rajataan turha altistuminen internetistä tulevalle haitalliselle liikenteelle, kun pääsy sinne on rajattu vain sitä tarvitseville, luotetuille IP-osoitteille, joita katselmoidaan säännöllisesti. Vahvasta tunnistautumisesta voidaan luopua ainoastaan, jos muita kompensoivia rajoituksia on otettu huomioon, kuten liikenne ei kulje internetissä.

vaan siitä täysin erillisessä liittymässä sekä käyttäjäryhmät ovat rajattu ylläpito- ja käyttäjäryhmiin RBAC:ia (Role Based Access Control), missä käyttäjäryhmillä on ainoastaan lukuoikeudet tai hyvin rajalliset muutosoikeudet.

Vaatus 3: Lokitus. Pääsynhallinnasta, hyppykoneista ja järjestelmän sovellustapahtumista tulee kerätä lokia ja säilöä erillisessä lokienhallintapalvelimessa. Lokeista tulee käydä ilmi järjestelmään liittyvät kirjautumiset, sovellusten virheet, käyttäjien tekemät toiminnot ja pääsynhallinnan tapahtumat, jotta voidaan jäljittää millä tunnuksilla on mitään toimenpiteitä tehty. Lokeja tulee säilyttää vähintään 6kk.

Vaatus 4: Käyttöoikeudet. Käyttöoikeudet rajataan henkilöiden työtehtävien mukaan ja niiden tarpeellisuutta seurataan säännöllisesti. Näin muodostuneilla rooleilla tulee olla elinkaari, jolla on selkeä alkua ja loppu ja tarvittaessa niitä jatketaan. Mikään tunnus ei tule olla ikuisesti voimassa ja suositeltava katselmointiväli tunnuksille ja rooleille on alle 1 vuosi. Poikkeuksena on ns. "emergency account" sekä valvontakäyttöön tarkoitettu vain lukuoikeudellinen/rajattu tunnus. Näiden tunnuksien voimassaoloa ei ole pakko määrittää, jonka tunnus ei vanhene päättymään ennalta. ja Emergency-tunnusta sitä ei tule käyttää kuin hätätilanteessa, kun esimerkiksi muilla tunnuksilla kirjautuminen ei onnistu järjestelmän palautuksessa tai asennuksessa. Tämän – ja kaikkien muiden – tunnuksien salasanat tulee pakottaa pitkiksi (>15 merkkiä) satunnaismerkkijonoksi, sisältäen erikoismerkkejä. Emergency-tunnuksen käytöstä on tultava hälytys ylläpitäjille. Lisäksi se ja valvonta- ja valvomokäytön tunnus saa olla ainoat tunnuks~~et~~et, jossa ei tarvitse olla vahvaa tunnistautumista. Tämän tunnuksen salana tulee olla salanas~~at~~at äilössäilössä tai kassakaapissa. Muita yhteiskäyttötunnuksia ei tule sallia, ilman osapuolen johdon hyväksyntää.

Vaatus 5: Etäkäyttö ja hallintayhteydet. Etäkäytön mahdollisuus rajataan niihin toimintoihin, joissa sitä oikeasti tarvitaan on toiminnan kannalta välttämätöntä, sekä pakotetaan vahva tunnistautuminen. Hallintayhteys ei lähtökohtaisesti tule olla internetiin avoinna. Jos se on pakko avata internetiin, se tulee se IP-rajauksella rajata vain toiminnan kannalta hyvin harvoin tarvittaviin yksittäisiin IP-osoitteisiin ja IP-rajauksella se tulee ottaa käyttöön aina kun se on teknisesti mahdollista toteuttaa. Vahvana suosituksena: hallintayhteyksiä tulisi käyttää vain hyppykone-yhteyksien kautta, joilla pyritään katkaisemaan suora yhteys käyttäjän koneelta kohteeseen ja tällä tavalla rajoitetaan luvattomien sovellusten tai toiminnallisuuksien suora hyödyntäminen etäyhteyden kautta. Tämä edellyttää, että hyppykoneella on asennettuna vain tarvittavat, luotettavat turvalliseksi todetut sovellukset sekä ajan tasalla pysyvä päätelaitesuojausohjelmisto ja jatkuvasti päivittyvät komponentit ja käyttöjärjestelmä.

Vaatus 6: Päivittäminen. Kaikkia järjestelmän komponentteja tulee säännöllisesti päivittää valmistajan sivuilta ja niiden haavoittuvuuksia tulee seurata säännöllisesti. Kaikki internetiin kytkettynä olevat komponentit tulee päivittää ensi tilassa, mikäli niissä on todettu korkean- (high)- tai kriittisen (critical) -tason haavoittuvuuksia. Komponenteista tulee pitää kirjaa, jotta tiedetään minkä tuotteen ja mitä versioita tulee erityisesti seurata ja päivittää. Hyvä "seurantavahti" on mm. Traficomien haavoittuvuustiedotteet.

Vaatus 7: Salaus. Kaikki API- tai hallintayhteydet itse järjestelmän ja sen ulkopuolisen kohteiden välillä tulee olla salattuja joko TLS1.2 tai TLS1.3 -salauksella tai AES256 tai sitä vahvemmalla AES-salauksella. Symmetrisessä salauksessa salausavaimen tulee

vaihtua vähintään kerran tunnissa, sekä salausavaimen tulee olla yli 15 merkkiä koostuen täysin satunnaisista- ja erikoismerkeistä (koskee tyypillisesti VPN-yhteyksiä).

Sertifikaatteja käytettäessä tulee heikot salausalgoritmit karsia pois (cipher suite) ja ohjeena tähän voi käyttää Traficomin suosituksia turvallisille salausalgoritmeille. Myös näihin yhteyksiin tulee asettaa IP-rajaukset. Mikäli em. salausvaatimukset ovat liian raskaita laitteelle, tulee valita erillinen laite tekemään salausta (VPN-laite) tai käyttää laitteen turvallisinta mahdollista salausalgoritmia. Myös näihin yhteyksiin tulee asettaa IP-rajaukset, jotka sallivat vain toiminnan kannalta välttämättömät yhteydet ja se tulee ottaa käyttöön aina kun se on teknisesti mahdollista toteuttaa.

Vaatus 8: Internet-yhteydet. Ohjattavista – tai muista kriittisistä laitteista – ei tule olla suoria yhteyksiä internetiin. Ainoastaan käytön kannalta pakolliset järjestelmän toiminnan kannalta välttämättömät ulospäin suuntautuvat yhteydet ovat sallittuja, eli ne pitää ns. "whitelistata" ja oletuksena muutoin estää. Whitelistauksella tarkoitetaan vain luotettuja kohteita, kuten laitevalmistajan päivitys-sivustoja ja toiminnan kannalta muut välttämättömät yhteydet ja protokollat.

Vaatus 9: Päätelaitesuojaus. Hallinta- ja etäyhteyksissä sekä hyppykoneissa tulee olla ajantasainen tietoturvapäätelaitesuojaus, joka lokittaa ja hälyttää poikkeamista kaikkina vuorokaudenaikoina. Näitä hälytyksiä tulee seurata ja niiden tulee reagoida poikkeaman mukaisella kriittisyydellä. Päätelaitesuoja tulee olla kaikissa oleellisissa komponenteissa, mitä kautta järjestelmään on pääsy. Mikäli sitä ei ole mahdollista asettaa, tulee hälytykset ja lokitukset järjestää muulla tavalla, jotta poikkeamat normaalista toiminnasta voidaan havaita.

Vaatus 10: IR (Incident Response)-prosessi. Poikkeamanhallintaprosessi tulee olla olemassa ja kuvattuna sekä se tulee olla osapuolen johdon hyväksymä. Sitä-Tätä tulee pitää ajan tasalla järjestelmien muuttuessa ja kokemuksen tai hyvien käytänteiden mukaisesti. Poikkeamiin mahdollisesti liittyviä asiakkuuksia tulee aina informoida kriittisistä tai vakavista poikkeamista. Sama velvoite toimii myös toiseen suuntaan (NIS2-lain soveltamana).

32.1.2

Fyysinen turvallisuus

Tämä alaluku käsittelee fyysiseen turvallisuuteen liittyviä vaatimuksia ohjaus- ja kaupankäyntijärjestelmille sekä yksittäisille reservikohteille. Reservikohteet, joiden keko tuotekohtainen hyväksytty reservikapasiteetti on alle 10 MW, ovat tämän luvun vaatimusten ulkopuolella. Näiden kohteiden osalta luvussa esitetyt vaatimukset ovat kuitenkin suosituksia. Sama rajausta sekä suositus koskee myös keskitettyjä ohjaus- ja kaupankäyntijärjestelmiä.

Pienemmissä kohteissa voidaan käyttää valmiita kokonaisratkaisuja, jotka sisältävät hälytykset, kameravalvonnan ja etäyhteyden valvomon. Tällaiset ratkaisut voivat täyttää vaatimukset matalan riskin kohteissa. Korkean riskin tai laajojen kiinteistöjen osalta suositellaan aina erillistä vartiointisopimusta ja suunnitelman laatimista yhteistyössä turvallisuussuunnittelijan kanssa laadukkaan lopputuloksen varmistamiseksi.

Jos tässä alaluvussa esitetyjä vaatimuksia ei pystytä toteuttamaan suojattavaan kohteeseen tarkoituksenmukaisesti, voi toimija voi perustellusta ja painavasta

syystä hakea Fingridiltä hyväksyntää poikkeavalle ratkaisulle. Poikkeus on perusteltava riskienhallinnan näkökulmasta ja dokumentoitava. Esimerkkinä tällaisesta tilanteesta on rakenteellisen murtosuojauksen toteutus suojeltujen rakennusten yhteydessä.

Mikäli kohde sijaitsee teollisuusalueella tai siihen rinnastettavassa ympäristössä, alueen olemassa olevia ulkokehän hallintaan ja aluevalvontaan tarkoitettuja ratkaisuja (esim. aitaus, kulunvalvonta, kameravalvonta) voidaan hyödyntää osana **reservikohteen** suojausta. Nämä ratkaisut voivat olla alueen haltijan tai muun toimijan hallinnoimia. Kehäsuojauksen suunnittelussa voidaan huomioida luonnolliset esteet, kuten vesialueet tai kallioleikkaukset, mikäli voidaan perustellusti todeta, että erillinen aitaus ei ole tarpeen. **Reservik**kohteen kuori-, tila- ja kohdesuojaukseen liittyvät vaatimukset on toteutettava täysimääräisesti.

Vaatus 1: Rakenteellinen murtosuojaus. Kohteen murtosuojauksen tulee olla vähintään Finanssialan turvallisuusohjeiden rakenteellisen murtosuojauksen ohje II vastaavalla tasolla.

~~Kohteissa tulee noudattaa Finanssialan turvallisuusohjeiden mukaisia rakenteellisen murtosuojauksen ohjeita II tai III. Tason valinta tehdään kohteen tärkeyden ja riskin mukaan. Kriittisimmissä kohteissa suositellaan käytettäväksi ohjetta III. Vähemmän kriittisissä kohteissa voidaan käyttää ohjetta II.~~

Vaatus 2: Murtohälytysjärjestelmä. Kohteisiin on asennettava murtohälytysjärjestelmä, joka täyttää seuraavat vaatimukset:

- Järjestelmän tulee valvoa kriittisten tilojen ja ulkovaipan ovia. Oviin tulee asentaa avaamisen ja auki jäämisen tunnistavat ilmaisimet.
- Hälytysjärjestelmän on oltava liitetty 24/7 toiminnassa olevaan turvavalvomoon. Hälytyksistä on lähdettävä viiveetön ilmoitus turvavalvomoon, jossa tapahtuu reagointi erikseen sovitun hälytysohjeen mukaisesti.
- ~~Turvav~~Valvomolla tarkoitetaan ~~-toimintayksikköä, jossa murtohälytysjärjestelmän antamia hälytyksiä valvotaan jatkuvasti ja hälytyksiin reagoidaan ennalta määritellyn hälytysmenettelyn mukaisesti.~~
- Vartiointiyrityksen kanssa on sovittava ja dokumentoitava tarkasti toimenpiteet, jotka toteutetaan mahdollisen murtautumisen jälkeen. Järjestelmien toiminta tulee testata uudelleen, ja suojattava kohde on tarkastettava asiantuntijan toimesta mahdollisten sabotaasien tai suojattavaan kohteeseen liitettyjen ulkopuolisten laitteiden varalta.

Vaatus 3: Ikkunasuojaus. Maatasolla sijaitsevat ikkunalliset tilat on varustettava tunkeutumisen havaitsemiseen tarkoitetuilla ilmaisimilla, jotka havaitsevat ikkunoiden kautta tapahtuvat tunkeutumisyritykset ja vahingonteot. Ilmaisimien on oltava kytketty murtohälytysjärjestelmään. Maanpinnan tasolla (1. kerros) olevat ikkunalliset tilat on varustettava lasirikkoilmaisimilla. Lasirikkoilmaisimien tulee olla kytketty murtohälytysjärjestelmään.

Vaatus 4: Kameravalvonta. Kohteissa tulee olla toimiva kameravalvontajärjestelmä. Järjestelmän vähimmäisvaatimukset:

- Sisäänkäynneillä ja sisätiloissa, joissa tapahtuu henkilö- tai tavaraliikennettä, tulee olla kameravalvonta.
- Tallenteet tulee säilyttää vähintään 30 vuorokauden ajan.
- Järjestelmästä tulee olla reaaliaikainen etäyhteys **turvavalvomoon**.

Vaatus 5: Järjestelmien toimivuuden varmistaminen. Murtohälytys- ja kameravalvontajärjestelmien toiminta on tarkastettava säännöllisesti:

- Vähintään kerran vuodessa tulee suorittaa järjestelmien kokonaisvaltainen testaus, mukaan lukien ilmaisimet, yhteydet ja hälytysten välittyminen.
- Vikatilanteet ja puutteet on korjattava välittömästi.

3.2 Häiriöiden ilmaisu ja reagoitokyky niihin

Vaatus 1: Yhteysskatkosta lähtee tieto kohteen ylläpidolle/operaattorille ja siihen reagoidaan.

Vaatus 2: Monitoroinnin piirissä vähintään seuraavat osa-alueet:

- Reserviresurssien tila ja reservisäädön toteutus
- Yhteydet ohjasjärjestelmän sekä reservikohteen ja mittalaitteiden välillä
- Tietoturvaan ja fyysiseen turvallisuuteen liittyvät hälytykset ja reagoinnit hälytysten ja lokien kriittisyyden mukaisesti.

Vaatus 3: Kuvaus reagoinnista mahdollisiin poikkeamiin sekä niihin liittyvät vaste- ja korjausajat. Kuvauksessa tulee huomioida, että vikatapahtumia voi olla useita: yhteysskatko, sähkökatko, laite jumiintuu tai rikkoutuu kokonaan tms.

Vaatus 4: Vaste- ja korjausajan tulee olla kohtuullinen verrattuna poikkeaman aiheuttamaan haittaan.

Vaatus 5: Kuvaus vikasietoisuuden testaamisesta. Testaaminen on kuvattu prosesseihin ja tapahtuu säännöllisin väliajoin, esim. vuosikellon mukaisesti tai päivitysten yhteydessä.

4 Reservitoimittajan ja reservikohteen järjestelmien vaatimukset

Tässä luvussa esitetyt ~~käyttövarmuusvaatimukset toimitusvarmuusvaatimukset~~ liittyvät ~~keskitettyjen- järjestelmäkuvauksen laajuuteen, itse~~ ohjaus- tai kaupankäyntijärjestelmien ~~ominaisuuksiinään~~ sekä toimintaan poikkeamissa. ~~Alaluvut 3.1 ja 3.2 on rakennettu niin että ne ovat järjestykseltään sekä sisällöltään yhtenevät FCR ja FFR reservien hakemuslomakkeiden kanssa~~ ~~Alaluvut 3.1 ja 3.2 on rakennettu niin että ne ovat järjestykseltään sekä sisällöltään yhtenevät eri reservien hakemuslomakkeiden kanssa.~~

~~43.1~~ Keskitetyn ohjausjärjestelmän vaatimukset

Tässä luvussa käsitellään keskitettyihin ohjausjärjestelmiin liittyviä tarkentavia ~~käyttövarmuusvaatimuksia toimitusvarmuusvaatimuksia~~. Keskitetty ohjausjärjestelmä välittää tehokomentoja sen piirissä oleville reservikohteille. Nämä tehokomennot lasketaan ohjausjärjestelmässä sen kauppatietojen, taajuusmittauksen (FFR ja FCR) sekä aktivointisignaalien (aFRR ja mFRR) perusteella.

~~43.1.1~~ Järjestelmän arkkitehtuurin kuvaus ylätasolla

Vaatus 1: Kuvauksesta tulee käydä ilmi järjestelmän merkittävät komponentit sekä tietovirrat niiden väleillä.

Vaatus 2: Kuvauksesta tulee käydä ilmi eri järjestelmän osien sijoittelu (oma palvelin, AWS, Azure tms.)

Vaatus 3: Kuvauksesta tulee käydä ilmi rajapinnat keskitettyyn ohjausjärjestämään sekä niiden käyttäjät ja etäyhteydet (esim. operaattori, asiakas jne.)

Vaatus 4: Viiveeseen vaikuttavat tekijät taajuusmittauksen ja kohteen aktivoinnin välillä tulee olla nähtävissä kuvauksesta selkeästi.

~~43.1.2~~ Ohjausjärjestelmän redundanssi:

Vaatus 1: ~~÷ T~~ Taajuusmittareita vaaditaan vähintään 3 saman hinta-alueen sisällä ~~(FFR ja FCR reservit), mikäli ohjausjärjestelmän alle kuuluvien reservikohteiden yhteenlaskettu tuotekohtainen hyväksytty reservikapasiteetti on yli 10 MW. Vaatus koskee järjestelmiä, joilla ylläpidetään FCR tai FFR reserviä.~~

- Lisäksi taajuusmittareiden tulee olla maantieteellisesti hajautettuja (riippumattomia yhdestä sähköteknisestä viasta ~~pl. suurhäiriö~~).
- Jos mittarin ja ohjausjärjestelmän välinen yhteys on toteutettu langattomasti, tulee yhteyden olla kahdennettu. Yhteyden kahdentaminen voidaan toteuttaa käyttämällä useampaa teleoperaattoria per mittari tai jakamalla mittarit useamman teleoperaattorin verkkoihin.

- Mikäli taajuusmittaus hankitaan palveluntarjoajalta, tulee palveluntarjoajan täyttää sama vaatimus, jos sen taajuusmittausta käyttävien toimijoiden yhteenlaskettu hyväksytty tuotekohtainen reservikapasiteetti on yli 10 MW.

~~Suositus 1: Reservikohteen ja säätöjärjestelmän välinen yhteys on kahdennettu.~~

○

Vaatusmus 2: Mikäli tiedonvälitys tapahtuu ~~3G/~~4G/5G-verkkojen avulla, tulee toimijan käyttää operaattoreilta saatavaa erillistä APN yhteyttä, joka erottaa yhteydet julkisesta internetistä ja luo toimijalle oman mobiiliyhteyden, joka on turvallisempi kuin julkiset internet-yhteydet. Toinen vaihtoehto APN:lle on erillinen tietoturvalaite, joka tekee NAT:n (Network Address Translation) ja johon saapuvat yhteydet ovat IP-rajattuja, jotka sallivat vain toiminnan kannalta välttämättömät yhteydet. Nämä tulee ottaa käyttöön aina kun se on teknisesti mahdollista toteuttaa.

~~rajattu IP-rajoituksella, eikä laite ole alttiina internetiin muuta kuin tiukalla IP-rajauksella.~~

Edellä mainittujen vaatimusten lisäksi suosituksena on kahdentaa reservikohteen ja ohjausjärjestelmän välinen yhteys.

43.1.3

Segmentointi:

Vaatusmus 1: Taajuusmittauksen tulee ohjata vain samalla hinta-alueella sijaitsevia kohteita.

Vaatusmus 2: Erillinen keskitetty ohjausjärjestelmä per hinta-alue.

43.1.4

Ohjausjärjestelmän IT-tuki

Vaatusmus 1: IT-tuki saatavilla, kun ylläpidetään reserviä.

Vaatusmus 2: Osapuolen johdon hyväksymä Hallintamallin kuvaus sekä varautumis- ja toipumissuunnitelma on oltava olemassa kriittisille ja tärkeille palveluille. Lisäksi myös niille palveluille, joista ne ovat suoraan riippuvaisia toiminnan kannalta, mikäli ne eivät jo ole kriittiseksi tai tärkeiksi luokiteltuja.

43.2

Keskitetyn kaupankäyntijärjestelmän vaatimukset (FCR ja FFR-reservit):

Tässä luvussa käsitellään keskitettyihin kaupankäyntijärjestelmiin liittyviä tarkentavia toimituskäyttö varmuusvaatimuksia. Keskitetty kaupankäyntijärjestelmä välittää kauppätietoja sen piirissä oleville reservikohteille ennen käyttöhetkeä. Järjestelmä ei välitä tehokomentoja, vaan kauppojen mukainen aktivoitava teho lasketaan paikallisesti reservikohteiden taajuusmittauksen sekä järjestelmän välittämien kauppätietojen perusteella.

43.2.1 Tiedot lähetetään hyvissä ajoin ennen reservin ylläpidon toimitushetkeä. Vaihtoehtoisesti tai niiden saapuminen voidaan — varmentaa operaattorin toimesta kohteen valvomosta.

Vaatus 1: Tiedot lähetetään viimeistään 3 tuntia ennen toimitushetkeä. Suosituksena on lähettää kauppätiedot koko seuraavan vuorokauden ajaksi kerralla.

Vaatus 2: Vaihtoehtoisesti kauppätiedot voidaan lähettää myöhemmin, mikäli niiden saapuminen varmistetaan manuaalisesti kohteen valvomosta.

Mikäli toimija ei kykene täyttämään vaatimusta 1 tai 2, voi se hakea hyväksyntää poikkeavalle ratkaisulle Fingridiltä. Esimerkiksi vaatimus 2 voidaan katsoa täytetyksi seuraavalla ratkaisulla: Reservikohde lähettää kuittauksen kapasiteetin hyväksymisestä kohteen valvomoon. Kuittausviestin puuttuminen tai sen välittämä tieto vastaanottamisen epäonnistumisesta aiheuttaa hälytyksen valvomossa ja siihen reagoidaan.

43.2.2 Kaupankäyntijärjestelmän IT-tuki

Vaatus 1: IT-tuki saatavilla, kun ylläpidetään reserviä.

Vaatus 2: Osapuolen johdon hyväksymä hallintamallin kuvaus sekä varautumis- ja toipumissuunnitelma on oltava olemassa kriittisille ja tärkeille palveluille. Lisäksi myös niille palveluille, joista ne ovat suoraan riippuvaisia toiminnan kannalta, mikäli ne eivät jo ole kriittiseksi tai tärkeiksi luokiteltuja. Hallintamallin kuvaus sekä varautumis- ja toipumissuunnitelma.

43.2.3 Kauppajärjestelmän piirissä olevien reservikohteiden toiminta yhteyskatkoksen aikana

Vaatus 1: Reservikohteen toiminnalle yhteyskatkoksen aikana on 2 vaihtoehtoista tapaa, jotka ovat suositusjärjestyksessä:

1. Kohde jatkaa jo saadulla kauppadataalla esim. vuorokauden loppuun ja muuttaa tämän jälkeen ylläpidetyn reservin määrän 0 MW:iin.

2. Kohde jatkaa yhteyskatkon hetkellä kauppätiedolla, kunnes toisin ohjataan.

Mikäli toimija ei kykene toteuttamaan kumpaakaan annetuista vaihtoehtoista, voi se hakea Fingridiltä hyväksyntää poikkeavalle ratkaisulle. Toteutuksessa tulee myös huomioida järjestelmätekniisten vaatimusten mahdolliset tarkentavat linjaukset toiminnasta tietoliikennekatkosten aikana.

