Fingrid Oyj

Reservien toimitusvarmuusvaatimukset

30.9.2026

1 Johdanto

Tämän dokumentin tarkoituksena on määritellä reservien ylläpitoon liittyvät toimitusvarmuusvaatimukset. Dokumentti käsittelee mm. tietoturvaan, toimintojen kahdentamiseen sekä poikkeamienhallintaan liittyviä vaatimuksia. Yleiset tekniset vaatimukset ja tarvittavat säätökokeet on määritelty seuraavissa dokumenteissa:

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

Dokumentit ovat saatavilla Fingridin internetsivuilla, ks. liitteet reservituotekohtaisilla 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 reservitoimittajan omaan käyttöön, ellei niitä vaadita erikseen osana reservikohteen hakemuslomaketta. Fingrid voi kuitenkin sopia toimijan kanssa erillisen auditoinnin suorittamisesta, mikäli katsoo sen tarpeellisiksi. 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.

1.1 Lyhenteet ja määritelmät

Määritelmiä:

Keskitetty ohjausjärjestelmä: Järjestelmä välittää tehokomentoja sen piirissä oleville reservikohteille.

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, muuttumaan reservikohteen tilaa ja aloittamaan tarvittaessa vianselvityksen.

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

Reserviresurssi: Yksittäinen säätökykyinen resurssi. Esimerkiksi voimalaitos, kulutuskohde tai energiavarasto.

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

IT-tuki: IT-tuella tarkoitetaan tahoa, jolla on tarvittava 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 internetsivuilta aiheesta ”monivaiheinen tunnistautuminen”.

Kovennus: Laitteen tai tietojärjestelmän kovennuksella tarkoitetaan toimenpiteitä sen hyökkäyspinta-alan minimointiin. Näitä ovat tyypillisesti käyttämättömien palveluiden ja tunnusten poistaminen käytöstä, turvallisuuteen liittyvien oletusasetusten muuttaminen tiukemmiksi, korjauspäivitysten säännöllinen asennus sekä erilaiset valmistajan suositukset ja ohjeet.

1.2 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 Yleiset toimitusvarmuusvaatimukset

Tässä luvussa esitetyt 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 reservitoimittajalla on voimassa olevia sitovia tarjouksia.

Yleisvaatimus 3: Yksittäisen vian takana oleva ylläpidetty reservi (ml. kapasiteetti- ja energiamarkkinat) saa olla enintään:

- 50 MW FFR reserviä
- +/-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 reserviä ja Olkiluoto 3 järjestelmäsuojan kapasiteettia.
  - Yhteensä +/-200 MW FCR-N, FCR-D, FFR, aFRR, mFRR reserviä ja Olkiluoto 3 järjestelmäsuojan kapasiteettia.

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

- Esimerkkejä yksittäisistä vioista ovat: sähkötekninen vika, tietojärjestelmän vikaantuminen, laiterikko tai tietoliikennekatkos.
- Reservitoimittaja on vastuussa palveluntarjoajan vikasietoisuudesta.
- Redundanssin ei tule perustua yksinomaan toimintojen kahdentamiseen saman laitteiston sisällä.
- Kahdennuksen riittävyys varmistetaan käymällä toteutus erikseen läpi Fingridin kanssa ja hyväksyttämällä se Fingridillä.

Ohjeita kahdennusvaatimuksen tulkintaan:

- mFRR tapauksessa kahdentamisvaatimus katsotaan täyttyneeksi välillä Fingrid - Reservitoimittaja, mikäli Fingrid pystyy aktivoimaan säätötarjouksia puhelinsoitolla reservitoimittajan valvomoon. Puhelinsoitto katsotaan myös riittäväksi kahdennustoimeksi välillä Reservitoimittajan valvomo - Reservikohde, mikäli aktivoinnit tapahtuvat normaalisti toista väylää käyttäen.
- Sähköteknisten komponenttien (muuntajat, mittarit, virtatiet tms.) kahdennus arvioidaan reservikohteelta verkkoluvallisen verkon liittymispisteeseen asti.
- Toimijan omaa liittymisjohtoa verkkoluvalliseen verkkoon ei tarvitse kahdentaa aFRR ja mFRR reservien tapauksessa, mutta FFR ja FCR reservien tapauksessa kahdennus vaaditaan.

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.

2.1 Fyysinen- ja kyberturvallisuus

2.1.1 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: Käytänteet ja maantieteellinen sijainti. Fyysisen- sekä kyberturvallisuuden tulee olla alan hyvien käytänteiden mukaisella tasolla, kuten noudattaa direktiivin NIS2, CRA tai standardin ISO27001 käytänteitä ja yleistä tietosuoja-asetusta (GDPR). Esimerkkejä alan hyvistä käytänteistä on mm. henkilöstön kouluttaminen, jatkuva toiminnan kehittäminen, turvallisuuden vastuuttaminen, kokonaisvaltainen riskienhallinta sekä **käytettyjen toimintamallien hyväksyttäminen yhtiön johdolla**. ISO27001 standardi auttaa merkittävästi erilaisten säädösten vaatimuksenmukaisuuden täyttämisessä, vaikkei sen virallinen sertifiointi ole pakollinen vaatimus toimittajien suuntaan. Lisäksi sääntelyn lisääntyessä ja mahdollisesti toimittajan palveluiden laajentuessa, he saattavat täyttää tulevaisuudessa NIS2:n tai CRA:n kriteerit, vaikka eivät niitä vielä täyttäisikään. Kaupankäynti- ja ohjausjärjestelmien tietojärjestelmien tulee sijaita maantieteellisesti Euroopan unionin sisämarkkina-alueella.

Vaatimus 2: Vahva tunnistus. Kaikkien käyttäjien 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 rajauksia on otettu huomioon. Esimerkki kompensoivasta ratkaisuista: liikenne ei kulje internetissä, vaan siitä täysin erillisessä liittymässä sekä käyttäjäryhmät ovat rajattu ylläpito- ja käyttäjäryhmiin käyttäen RBAC:ia (Role Based Access Control), missä käyttäjäryhmillä on ainoastaan lukuoikeudet tai tarkoituksenmukaisesti rajatut muutosoikeudet.

Vaatimus 3: Lokitus ja seuranta. 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 mitäkin toimenpiteitä tehty tai mitkä tiedot ovat vaarantuneet. Lokeja tulee säilyttää vähintään 6kk. Lokeja tulee seurata 24/7/365 kriittisistä ja oleellisista palveluista sekä niihin tulee reagoida niiden kriittisyyden mukaisesti.

Vaatimus 4: Käyttöoikeudet. Käyttöoikeudet rajataan henkilöiden työtehtävien mukaan ja niiden tarpeellisuutta seurataan säännöllisesti. Näin muodostuneilla rooleilla tulee olla elinkaari, jolla on selkeä alku 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 päättymään ennalta. Emergency-tunnusta 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 tunnukset, jossa ei tarvitse olla vahvaa tunnistautumista. Tämän tunnuksen salasana tulee olla salasanasäilössä ja varmuuskopion piirissä tai kassakaapissa. Muita yhteiskäyttötunnuksia ei tule sallia, ilman osapuolen johdon hyväksyntää.

Vaatimus 5: Etäkäyttö ja hallintayhteydet. Etäkäytön mahdollisuus rajataan niihin toimintoihin, joissa se on toiminnan kannalta välttämätöntä, sekä pakotetaan vahva tunnistautuminen (MFA). Hallintayhteys ei lähtökohtaisesti tule olla internetiin avoinna. Jos hallintayhteys on pakko avata internetiin, tulee se IP-rajauksella rajata vain toiminnan kannalta tarvittaviin IP-osoitteisiin ja IP-rajaus 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, turvalliseksi todetut sovellukset sekä ajan tasalla pysyvä päätelaitesuojausohjelmisto ja jatkuvasti päivittyvät komponentit ja käyttöjärjestelmä sekä lokien keräys ja seuranta.

Vaatimus 6: Päivittäminen ja koventaminen. 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 (SBOM, Software Bill of Materials), jotta tiedetään minkä tuotteen ja mitä versioita tulee erityisesti seurata ja päivittää. Hyvä ”seurantavahti” on mm. Traficomin haavoittuvuustiedotteet. Huom. Internetistä erillään olevat laitteet tai hyvin IP-rajauksella suojatut laitteet auttavat merkittävästi estämään kriittisten haavoittuvuuksien hyödyntämisen. Laitteiden konfiguraatiot tulee koventaa laitevalmistajien ohjeiden mukaan ja pitää ne ajan tasalla.

Vaatimus 7: Salaus. Kaikkien API- tai hallintayhteyksien itse järjestelmän ja sen ulkopuolisen kohteiden välillä tulee käyttää joko TLS v1.2 tai TLS v1.3 -protokollaa sekä AES256 tai sitä vahvempaa AES-salausta. Symmetrisessä salauksessa tulee käyttää sekä avainten vaihtoon että IKE-viestien suojaamiseen SHA2:een pohjautuvaa algoritmia sekä SA-elinajat ja uudelleenneuvottelut tulee olla: IKE-SA: < 24 h ja IPsec-SA: < 4 h. Salausavaimen (pre-shared key) tulee olla yli 15 merkkiä koostuen täysin satunnaisista- ja erikoismerkeistä (koskee tyypillisesti VPN-yhteyksiä). Sertifikaatteja käytettäessä tulee heikot salausalgoritmit (cipher suites) karsia kokonaan pois käytöstä ja ohjeena tähän voi käyttää Traficomin suosituksia turvallisille salausalgoritmeille. Mikäli em. salausvaatimukset ovat liian raskaita laitteelle, tulee valita erillinen laite tekemään salausta (VPN-laite) tai käyttää laitteen turvallisinta mahdollista salausalgoritmia tai vaihtaa laite kokonaan uudempaan, joka kykenee parempaan salaukseen. 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. Toimijan tulee huomioida PQC (Post-Quantum Cryptography)-siirtymän tuomat uudet

algoritmit sekä olla hyväksytty suunnitelma niiden käyttöönottamiseksi. Traficomin www-sivuilta löytyy ohje kvanttiturvallisiin salausmenetelmiin.

Vaatimus 8: Internet-yhteydet. Ohjattavista – tai muista kriittisitä laitteista – ei tule olla oletuksena suoria yhteyksiä internetiin. Ainoastaan erikseen määritellyt, 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 päivityssivustoja ja muita toiminnan kannalta välttämättömiä yhteyksiä ja protokollia. Tällä pyritään estämään laitteen luvattomat yhteydet haitallisiin kohteisiin.

Vaatimus 9: Päätelaitesuojaus. Hallinta- ja etäyhteyksissä sekä hyppykoneissa tulee olla ajantasainen tietototurvan päätelaitesuojaus, joka lokittaa ja hälyttää poikkeamista kaikkina vuorokaudenaikoina. Näitä hälytyksiä tulee seurata ja niihin 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.

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

2.1.2 Fyysinen turvallisuus

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

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

Jos tässä alaluvussa esitettyjä vaatimuksia ei pystytä toteuttamaan suojattavaan kohteeseen tarkoituksenmukaisesti, toimija voi perustellusta ja painavasta syystä hakea Fingridiltä hyväksyntää poikkeavalle ratkaisulle. Poikkeus on perusteltava riskienhallinnan näkökulmasta ja dokumentoitava.

Mikäli kohde sijaitsee teollisuusalueella tai siihen rinnastettavassa ympäristössä, alueen olemassa olevia ulkokehän hallintaan ja aluevalvontaan tarkoitettuja ratkaisuja (esim. aitaus, kulunvalvonta, kameravalvonta) voidaan hyödyntää osana kohteen 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. Kohteen kuori-, tila- ja kohdesuojaukseen liittyvät vaatimukset on toteutettava täysimääräisesti.

Vaatimus 1: Murtohälytysjärjestelmä. Kohteisiin on asennettava murtohälytys-järjestelmä, 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.
- Turvavalvomolla 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.

Vaatimus 2: Ikkunasuojaus. Maatasolla sijaitsevat ikkunalliset tilat on varustettava tunkeutumisen havaitsemiseen tarkoitetuilla ilmaisimilla, jotka havaitsevat ikkunoiden kautta tapahtuvat tunkeutumisyritykset ja vahingonteot. Ilmaisimien on oltava kytketty murtohälytysjärjestelmään.

Vaatimus 3: Kameravalvonta. Kohteissa tulee olla toimiva kameravalvontajärjestelmä. Järjestelmän vähimmäisvaatimukset:

- Kaikilla sisäänkäynneillä tulee olla kameravalvonta.
- Tallenteet tulee säilyttää vähintään 30 vuorokauden ajan.
- Järjestelmästä tulee olla reaaliaikainen etäyhteys valvomoon.

Vaatimus 4: 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.

Edellä mainittujen vaatimusten lisäksi suosituksena on toteuttaa kohteen murtosuojaus Finanssialan rakenteellisten murtosuojausohjeiden II tai III mukaisesti.

2.2 Häiriöiden ilmaisu ja reagointikyky niihin

Vaatimus 1: Yhteyskatkoksesta lähtee tieto kohteen ylläpidolle/operaattorille ja siihen reagoidaan.

Vaatimus 2: Monitoroinnin piirissä vähintään seuraavat osa-alueet:

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

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

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

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

3 Reservitoimittajan ja reservikohteen järjestelmien vaatimukset

Tässä luvussa esitetyt toimitusvarmuusvaatimukset liittyvät keskitettyjen ohjaus- tai kaupankäyntijärjestelmien ominaisuuksiin sekä toimintaan poikkeamissa.

3.1 Keskitetyn ohjausjärjestelmän vaatimukset

Tässä luvussa käsitellään keskitettyihin ohjausjärjestelmiin liittyviä tarkentavia 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.

3.1.1 Järjestelmän arkkitehtuurin kuvaus ylätasolla

Vaatimus 1: Kuvauksesta tulee käydä ilmi järjestelmän merkittävät komponentit sekä tietovirrat niiden välillä.

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

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

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

3.1.2 Ohjausjärjestelmän redundanssi:

Vaatimus 1: Taajuusmittareita vaaditaan vähintään 3 saman hinta-alueen sisällä, mikäli ohjausjärjestelmän alle kuuluvien reservikohteiden yhteenlaskettu tuotekohtainen hyväksytty reservikapasiteetti on yli 10 MW. Vaatimus koskee järjestelmiä, joilla ylläpidetään FCR tai FFR reserviä.

- Lisäksi taajuusmittareiden tulee olla maantieteellisesti hajautettuja (riippumattomia yhdestä sähköteknisestä viasta):
- Jos mittarin ja ohjasjärjestelmän 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.

Vaatimus 2: Mikäli tiedonvälitys tapahtuu matkapuhelinverkkojen datayhteyksien, kuten 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.

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

3.1.3 Segmentointi:

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

Vaatimus 2: Erillinen keskitetty ohjausjärjestelmä per hinta-alue.

3.1.4 Ohjausjärjestelmän IT-tuki

Vaatimus 1: IT-tuki tulee olla saatavilla, kun reservitoimittajalla on voimassa olevia sitovia tarjouksia.

Vaatimus 2: Osapuolen johdon hyväksymä hallintamallin kuvaus sekä varautumis- ja toipumissuunnitelma on oltava olemassa kriittisille ja tärkeille palveluille.

3.2 Keskitetyn kaupankäyntijärjestelmän vaatimukset (FCR ja FFR-reservit):

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

3.2.1 Kauppatietojen lähettäminen reservikohteelle

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

Vaatimus 2: Vaihtoehtoisesti kauppatiedot 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.

3.2.2 Kaupankäyntijärjestelmän IT-tuki

Vaatimus 1: IT-tuki tulee olla saatavilla, kun reservitoimittajalla on voimassa olevia sitovia tarjouksia.

Vaatimus 2: Osapuolen johdon hyväksymä hallintamallin kuvaus sekä varautumis- ja toipumissuunnitelma on oltava olemassa kriittisille ja tärkeille palveluille.

3.2.3 Kauppajärjestelmän piirissä olevien reservikohteiden toiminta yhteyskatkoksen aikana

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

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

2. Kohde jatkaa yhteyskatkon hetkisellä kauppatiedolla, kunnes toisin ohjataan.

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