

Uuden ja vanhan asetinlaitteen yhteensovittaminen, testaus ja käyttöönotto

Mipro Oy toimittaa uudet elektroniset asetinlaitteet Niiralan, Kotkan Kotolahti-Mussalon sekä Vainikkalan ratapihoille Rautateiden turvalaitejärjestelmien uusiminen osahankinta 1 -hankkeessa (jatkossa korjausvelkahanke). Toimitukseen sisältyy rajapinnat usean toimittajan eri aikakausina rakentamiin asetinlaitteisiin:

- Niiralassa rajapinta rakennetaan Venäjälle puolautomaattiseen suojustukseen sekä Mipron omaan vanhemman sukupolven elektroniseen asetinlaitteen suojustukseen.
- Kotolahti-Mussalossa asetinlaiterajapinta rakennetaan VR76-releasetinlaitteeseen sekä kulku- että vaihtokulkuteille.
- Vainikkalassa tehdään rajapinta Venäjälle puolautomaattiseen suojustukseen sekä suojustusliityntä Siemensin elektroniseen SIMIS-C-asetinlaitteeseen.

Junaliikenteen kannalta rajapinnoissa on aina oleellista, että rajapinta toimii saumattomasti ja luotettavasti sekä käytettävyyden että turvallisuuden näkökulmasta. Rajapinta ei saa aiheuttaa turhaa häiriötä junaliikenteelle. Toisaalta liikenteenohjauksen näkökulmasta rajapinnan tulisi olla automaattinen eli esimerkiksi ylimääräisiä komentoja ei tulisi joutua antamaan ja kauko-ohjausjärjestelmän junanumeroautomaatiikan tulee pystyä toimimaan. Turvallisuus ei saa missään tilanteessa heikentyä rajapinnassa: juna ei voi esimerkiksi kadota, opastin ei voi näyttää väärää opastetta, suojustuksen pitää pystyä turvaamaan junan kulku. Kun kyseessä on eri aikakausien järjestelmien yhdistäminen toisiinsa, haastetta kaikkien edellä mainittujen osa-alueiden täyttämisessä on paljon. Erityisesti turvallisuuden osalta yhtään kompromissia ei saa hyväksyä.

Vaatimukset rajapinnoille

Asetinlaitevaatimuksina käytetään Liikenneviraston Suomen asetinlaitevaatimuksia (FIR) ja RATO6:ta. Näistä FIRin ulkolaitevaatimuksista löytyy FIR-QR516-REQ..FIR-QR519-REQ vaatimukset, joissa esitetään vaatimukset uudelle asetinlaitteelle ja sen mahdollisuudelle tarjota rajapinta erityyppisiin asetinlaitteisiin: keskinäisten riippuvuuksien huomioiminen, ohjaukset, luvanpyynnöt, luanannot ja vaatimukset. Vaatimuksissa ei juurikaan oteta kantaa, miten rajapinta suunnitellaan ja mitä asioita tulisi huomioida. Liikenneviraston julkaisu ”Suojustusrajapinnat – sovellusohje” antaa konkreettisia suunnitteluperusteita ja työkaluja rajapintojen suunnitteluun. Myös Mipron korjausvelkahankkeessa ratapihoille sovellusohjetta on sovellettu mahdollisimman paljon.

Liikenneviraston ohjeiden lisäksi suunnittelua ohjaavat Cenelec-standardit 50126 (yleiset RAMS-vaatimukset) ja 50128 (turvakriittisten ohjelmistojen toteutus). Näiden standardien mukaan suunnittelun, toteutuksen ja todentamisen tulee seurata tarkoin määritettyjä työkaluja, menetelmiä ja prosessia.



Suvi Hyyryläinen
Mipro Oy

Standardien mukaisesti vaatimukset tulee arvioida riittäviksi ja yksiselitteisiksi sekä jakaa eri osajärjestelmille. Jotta vaatimukset voidaan jakaa, tulee tuntea hyvin myös osajärjestelmien rajoitteet, joita kutsutaan turvallisuuteen liittyviksi rajoitteiksi (safety related application conditions, SRAC) sekä osajärjestelmän toiminnallisuus rajapinnassa. Tämä on haastavaa erityisesti vanhempien aikakausien asetinlaitteiden osalta, joista ei ole kattavia toiminnallisia kuvauksia ja kytkentäkuvatkin voivat olla päivittymättömiä. Korjausvelkahankkeen osan rajapintojen osalta asiantuntijoita on enää muutamia ja kuvauksia on vähän. Liikenneviraston erinomaisella tuella kaikki mahdolliset lähtötiedot on kuitenkin saatu kerättyä.

Turvallisuuden todentaminen

Asetinlaitteiden tärkein ominaisuus on turvata junan turvallinen liike, minkä tulee olla tärkein suunnittelukriteeri rajapintojen suunnittelussa. Turvallisuus varmistetaan turvallisten menetelmien lisäksi suunnittelun, toteutuksen ja testauksen eri vaiheissa verifiointi- ja validointimenetelmillä. Menetelmiä ovat mm. erilaiset katselmoinnit, tarkastukset ja testaukset. Turvallisuuden todentamisen todiste on safety case. Koska vanhoista järjestelmistä on vähän tietoa, on vaikeaa todentaa dokumentein, miten muun muassa vanha järjestelmä toimii, mitkä ovat järjestelmien rajoitteet, miten siihen voidaan liittyä. Periaatteessa Cenelec-standardien mukaisesti jo käytössä olevistakin järjestelmistä tulisi tehdä toiminnallinen kuvaus, mutta käytännössä mikäli kuvausta ei ole, se kuvataan rajapintojen suunnitteluvaiheessa osaksi rajapinnan kuvausta. Koska hyviä ja kattavia kuvauksia ei ole, tulee riskien tunnistamiseen panostaa.

Riskianalyysit ovat iso osa turvallisuuden varmistamista. Turvallisuus tulee taattua sitä paremmin mitä laajempi ja asiantuntevampi tiimi suunnittelee ja todentaa turvallisuutta.

Suunnittelu ja toteutus

Korjausvelkahankkeen rajapintojen suunnittelua ohjasi Liikenneviraston tahtotila siitä, että olemassa oleviin järjestelmiin tehdään mahdollisimman vähän muutoksia. Tätä tavoitetta noudattaen ja olemassa olevien järjestelmien dokumenttien (mm. käyttöohjeiden) sekä erityisesti asiantuntijoiden avustuksella Mipro on toteuttanut rajapintojen suunnitelmat siten, että mahdollisimman paljon nykyvaatimuksista voidaan täyttää. Kaikkia vaatimuksia ei ole pystytty toteuttamaan, sillä vanhoissa liitettävissä järjestelmissä ei ole kyseisiä ominaisuuksia olemassa. Suunnitelmia tukevat myös aiemmista hankkeista hyviksi todetut riskianalyysit (hazop-analyysit), jotta myös mahdolliset riskit rajapinnoista on tiedossa. Tämän hetkisen tiedon mukaan käytettyä ei ole voitu saada parhaalle mahdolliselle tasolle.

Kuten vaatimuksetkin myös suunnittelu on tarkastettava. Mipron suunnittelun tarkastaa kokenut suunnittelija ja koska korjausvelkahankkeessa päädyttiin siihen, että vanhoja järjestelmiä ei juurikaan muuteta, tarkastuksen tuleekin keskittyä Mipron suunnitteluun. Hankkeissa, joissa vanhoja asetinlaitteita muutetaan paljon, olisi syytä tarkastukseen nimittää suunnittelija, joka arvioi rajapinnan toimivuuden kokonaisuutena.

Suunnittelun onnistuminen vaikuttaa toteutuksen onnistumiseen. Mitä paremmin suunnittelu on onnistunut, sitä paremmin rajapintojen muutokset eri osapuolten tekeminä kohtaavat. Koska rajapintoja toteuttavat eri toimittajat, jotka myös testaavat ja todentavat omat osuutensa suunnittelua vasten, nähdään kokonaisuuden toimiminen vasta integrointitestauksessa.

Integrointitestaus

Integrointitestauksella tarkoitetaan järjestelmän testaamista kokonaisuutena, jotta varmistutaan, että eri osat ja eri osapuolten toteuttamat järjestelmät toimivat yhdessä täydellisenä kokonaisuutena. Aiemmissa hankkeissa testaus on tehty vasta juuri ennen järjestelmien käyttöönottoa tai käyttöönoton yhteydessä. Tässä on suuret riskit, että joko rajapintoja muutetaan käyttöönoton aikana, jolloin vikojen todennäköisyys kasvaa, tai rajapintaan jää puutteita tai rajapintaa ei voida ottaa käyttöön ollenkaan. Kuten aina testeissä, on haastavaa arvioida, mikä on riittävä testaus, mitä kaikkea tulee testata, jotta voidaan olla varmoja, että rajapinta toimii odotetusti kaikissa tilanteissa.

Korjausvelkahankkeessa Niiralan ja Vainikkalan osalta Venäjän suunnan rajapintaa on testattu ja testataan jo paljon ennen käyttöönottoa vanhan järjestelmän rinnalle rakennetun rajapinnan avulla. Tämä lisää varmuutta rajapinnan toimivuudesta ja toisaalta auttaa myös suunnittelemaan rajapinnan käyttöönotossa tehtävät toimet paremmin. Lisäksi yllätykset vähenevät. Myös muut rajapinnat pyritään testaamaan hyvissä ajoin ennen käyttöönottoa siten, että uusi järjestelmä kytketään vanhaan



Vuosikymmeniä sitten rakennetun ja nykyvaatimukset täyttävän asetinlaitteen yhdistäminen sisältää haasteita. Niiralan ratapihalla Mipro rakentaa rajapinnat Venäjälle puolautomaattiseen suojustukseen sekä Mipron omaan vanhemman sukupolven elektroniseen asetinlaitteen suojustukseen.

ja palautetaan testien jälkeen testejä edeltävään tilanteeseen. Hyvissä ajoin ja rauhassa tehty testaus lisää sen todennäköisyyttä, että testit ovat riittävät ja rajapinnan toimivuus erilaisissa tilanteissa on varmistettu.

Käyttöönotto

Usein rajapinnat ovat olleet suurimpia riskejä käyttöönotossa viimehetkeen, juuri ennen käyttöönottoa tai käyttöönottoon jääneen testauksen vuoksi. Tähän tilanteeseen on johtanut se, että jo käytössä oleviin järjestelmiin on jouduttu tekemään paljon muutoksia ja toisaalta samanlaista ajatusta uuden rajapinnan rakentamisesta rinnalle kuten Niiralassa ja Vainikkalassa ei ole käytetty.

Korjausvelkahankkeen huolellinen suunnittelu, selkeät linjat Liikenneviraston tahtotilasta ja vaatimuksista sekä hyvin tehdyt testaukset, vähentävät riskiä paljon ja tulevat käyttöönotot on voitu suunnitella hyvin ja rajapintojen toimivuus on varmistettu jo hyvissä ajoin etukäteen.

Kohti parempia rajapintoja

Jo käytössä olevan järjestelmän ja erityisesti vuosikymmeniä sitten rakennetun asetinlaitteen ja nykyvaatimukset täyttävän asetinlaitteen yhdistäminen ei ole koskaan helppoa. Hyvällä suunnittelulla, erityisesti vanhojen järjestelmien asiantuntemuksella ja selkeillä vaatimuksilla, pystytään toteuttamaan toimivia ja erityisesti turvallisia rajapintoja. Suunnittelu on kehittynyt hankehankeelta ja uusia käytäntöjä ja työkaluja on otettu käyttöön. Suojustusrajapintojen sovellusohje on hyvä alku ja sitä on käytetty rajallisesti, muun muassa riskianalyysia ja rajapintasignaalien suunnittelua on pyritty soveltamaan ohjeen mukaisesti erityisesti uusien asetinlaitteiden osalta. Erityisen tärkeää on testauksen mahdollistaminen ennen käyttöönottoa ja sitä kautta myös käyttöönoton parempi suunnittelu.