VTT TIEDOTTEITA – MEDDELANDEN – RESEARCH NOTES 1745

Työkoneiden ja automaation CAN-väyläsovellusten turvallisuus

Marita Hietikko
VTT Valmistustekniikka

Jarmo Alanen
VTT Automaatio

Risto Tiusanen
VTT Valmistustekniikka

VALTION TEKNILLINEN TUTKIMUSKESKUS
ESPOO 1996

ISBN 951-38-4900-7
ISSN 1235-0605

JULKAISIJA – UTGIVARE – PUBLISHER

Valtion teknillinen tutkimuskeskus (VTT), Vuorimiehentie 5, PL 42, 02151 ESPOO
puh. vaihde (90) 4561, telekopio 456 4374, teleksi 125 175 vttin sf

Statens tekniska forskningscentral (VTT), Bergsmansvägen 5, PB 42, 02151 ESBO
tel. växel (90) 4561, telefax 456 4374, telex 125 175 vttin sf

Technical Research Centre of Finland (VTT), Vuorimiehentie 5, P.O.Box 42, FIN–02151 ESPOO, Finland
phone internat. + 358 0 4561, telefax + 358 0 456 4374, telex 125 175 vttin sf

Tekninen toimitus Leena Ukskoski

VTT OFFSETPAINO, ESPOO 1996

Hietikko, Marita, Alanen, Jarmo & Tiusanen, Risto. Työkoneiden ja automaation CAN-väyläsovellusten turvallisuus [The security of CAN bus applications in working machines and automation]. Espoo 1996, Valtion teknillinen tutkimuskeskus, VTT Tiedotteita - Meddelanden - Research Notes 1745. 100 s. + liit. 1 s.

UDK 681.518.5:331.45:681.3

Avainsanat safety, safety engineering, work machines, automation, control systems, controller area network, knowledge based systems, computers, safety factors

TIIVISTELMÄ

Työkoneiden ohjausjärjestelmät ovat nykyään yhä enemmän useista älykkäistä yksiköistä koostuvia reaaliaikaisia hajautettuja järjestelmiä, joiden tiedonsiirtoliikennöinnissä käytetään CAN-väylää. CAN-väylän käyttö on lisääntynyt myös muissa automaation sovelluksissa. Koneiden käyttöturvallisuuden kannalta hajautettu ohjaus toisaalta mahdollistaa koneen toimintojen entistä tehokkaamman diagnosoinnin, mutta on myös uusi ja entistä vaikeammin hallittava riskitekijä. Ilman riittäviä varmistuksia tietokoneohjattu työkone voi vikaantuessaan toimia täysin odottamattomasti, kuten lähteä liikkeelle, kääntyä, käynnistää työlaitteen ohjauksen tai lukita jarrut.

Tutkimuksen tavoitteena oli tuottaa tietoa siitä, miten tunnistetaan ja hallitaan CAN-väyläjärjestelmiin liittyviä turvallisuustekijöitä ja mitä tekniikoita on käytettävissä turvallisuuden varmistamiseksi tai sen lisäämiseksi työkoneiden ja automaation CAN-väyläsovelluksissa. Suomessa jo toteutettuihin CAN-väylällä varustettuihin työkonesovelluksiin on turvallisuusongelmiin kehitetty ratkaisuja lähinnä yleisten koneturvallisuusvaatimusten ja ohjausjärjestelmiä koskevien vaatimusten pohjalta.

CAN-väyläsovellusten turvallisuutta tutkittiin tässä hankkeessa kolmen case-järjestelmän avulla. Näille tehtiin turvallisuusanalyysejä, joiden avulla selvitettiin mahdolliseen ei-toivottuun tapahtumaan johtavat syyt eri case-kohteina käytetyissä CAN-järjestelmissä. Tutkittiin, mitkä näistä syistä kohdistuvat CAN-väylän laitteiston tai ohjelmiston osalle ja miten järjestelmät on varmistettu ei-toivottujen tapahtumien varalta. Analyysien perusteella voitiin tehdä turvallisuuteen liittyviä ehdotuksia CAN-järjestelmien tai niiden suunnittelukäytännön kehittämiseksi.

Hankkeen tuloksena saatiin tietoa niistä turvallisuustekniikoista, menetelmistä ja toimenpiteistä, joita hajautettujen CAN-väyläjärjestelmien laitteisto- ja ohjelmistosuunnittelussa voidaan käyttää turvallisuuden parantamiseksi ja joita ei mainita nykyisessä turvallisuuteen liittyviä järjestelmiä koskevassa IEC 1508 -standardiluonnoksessa. Tässä julkaisussa kerrotaan tämän tiedon ja case-kohteiden lisäksi CAN-väyläjärjestelmien suunnitteluun liittyvistä turvallisuusvaatimuksista, CAN-järjestelmän vikamuodoista ja siitä, miten diagnostiikasta saadaan apua turvallisuuteen.

Hietikko, Marita, Alanen, Jarmo & Tiusanen, Risto. Työkoneiden ja automaation CAN-väyläsovellusten turvallisuus [The security of CAN bus applications in working machines and automation]. Espoo 1996, Technical Research Centre of Finland, VTT Tiedotteita - Meddelanden - Research Notes 1745. 100 p. + app. 1 p.

UDK 681.518.5:331.45:681.3

Avainsanat safety, safety engineering, work machines, automation, control systems, controller area network, knowledge based systems, computers, safety factors

ABSTRACT

Control systems of working machines are today more and more often real-time distributed systems consisting of several intelligent units. These systems use Controller Area Network (CAN) for communication, and the use of CAN has also increased in other automation applications. When thinking of the user safety of machines, the distributed control makes it possible to diagnose the functions of a machine more effectively, but, however, on the other hand the distributed control is a new and serious risk factor. A computer controlled working machine can, without sufficient checking, work unexpectedly. It may for example start moving, turn to a wrong direction, trigger the control of a device, or lock brakes.

The aim of the study was to produce information on methods for identifying and mastering the safety factors associated with CAN systems and on techniques that are available for ensuring or increasing the safety in working machines and other CAN applications in automation area. For those working machine applications with CAN system that are already implemented in Finland the safety problems have been solved from the basis of general machine safety and control system requirements.

In this project the safety of CAN applications were studied with the aid of three systems as examples. The safety analyses were carried out for these CAN applications, the purpose of which was to clear up the causes of undesirable events. It was studied, which of these causes are directed to hardware or software of a CAN system and how these systems are ensured against undesirable events. From the basis of the analyses that were carried out, suggestions for developing CAN systems or their design practice could be done.

As a result of this study a knowledge of those safety techniques and measures which can be applied in the design of CAN system hardware or software for improving safety was obtained. These techniques and measures are not mentioned in the existing IEC 1508 standard draft concerning safety related systems. In addition to this information and studies with example systems, safety requirements related to the design of CAN systems, failure modes of CAN systems and CAN diagnostics as an aid for safety are described in this report.

ALKUSANAT

Tämä raportti on syntynyt Työsuojelurahaston ja yritysten rahoittaman hankkeen ”Työkoneiden ja automaation CAN-väyläsovellusten turvallisuus” tuloksena. Hankkeeseen ovat osallistuneet Marita Hietikko, Risto Tiusanen ja Risto Kuivanen VTT Valmistustekniikan tutkimusyksiköstä, Jarmo Alanen VTT Automaation tutkimusyksiköstä, Ari Tuunanen ja Jarmo Mäkelä asiantuntijaryhmineen Tamrock Oy:stä, Mauno Ruuska asiantuntijaryhmineen Vammas Oy:stä, Jorma ja Veijo Kiiski Pirkan Elektroniikka Oy:stä sekä Urpo Hirvikoski UH-Tekniikka Oy:stä. Kiitämme kaikkia hankkeeseen osallistuneita henkilöitä yhteistyöstä.

Luvussa 4 esiteltävä diagnostiikka-arkkitehtuuri on suunniteltu TEKESin ja VTT:n LOKKI-hankkeessa (liikkuvien työkoneiden ohjausohjelmistojen komponentointi ja kokoaminen) vuosina 1992 - 1993.

Tämä raportti julkaistaan Työsuojelurahaston avustuksella.

Tampereella 26.7.96

Tekijät

SISÄLLYSLUETTELO

1 JOHDANTO

Elektroniikka- ja digitaalilaitteiden sekä älykkäiden antureiden ja toimilaitteiden määrä on kasvanut niin työkoneissa kuin yleensä koneautomaatiossakin. Useista älykkäistä yksiköistä muodostuu *hajautettu ohjausjärjestelmä*, jossa eri yksiköiden välinen tiedonsiirtoväylä muodostaa tärkeän osan koko järjestelmää. CAN-väylä on yksi reaaliaikaisen ja hajautetun järjestelmän tiedonsiirtojärjestelmistä. Fyysisesti CAN-väylä on parikaapelilinja, jonka kautta tieto siirtyy järjestelmässä yksiköstä toiseen. Koneiden käyttöturvallisuuden kannalta hajautettu ohjaus toisaalta mahdollistaa koneen toimintojen entistä tehokkaamman diagnosoinnin, mutta se on myös *uusi ja entistä vaikeammin hallittava riskitekijä*. Ilman riittäviä varmistuksia tietokoneohjattu työkone voi vikaantuessaan toimia täysin odottamattomasti, kuten lähteä liikkeelle, kääntyä, käynnistää laitteen ohjauksen tai lukita jarrut.

CAN (Controller Area Network) on alun perin ajoneuvokäyttöön kehitetty sarjaväyläjärjestelmä. Suomessa CAN-väyläratkaisuja on sovellettu mm. kallionporauslaitteiden ja metsäkoneiden ohjauksiin. Väylä yhdistää esimerkiksi moottorin, voimansiirron, jarrujen, työlaitteen ja käyttöliittymän ohjausyksiköt. Automaation sovelluksissa CAN-väylää käytetään nykyään mm. hisseissä sekä rakennusten lämpö- ja ilmastointijärjestelmissä.

Työkoneympäristö asettaa väylälle kovia vaatimuksia. Näitä ovat mm. hyvä sähkömagneettisten ja muiden häiriöiden sietoisuus ja havaitseminen, laaja lämpötila-alue, helppokäyttöisyys sekä alhaiset komponenttikustannukset.

Hajautetuille tietokoneohjauksille ei ole olemassa vielä erityisiä turvallisuusvaatimuksia. Myöskään tietoliikenteeseen tai väyläarkkitehtuuriin liittyen ei ole olemassa yleisesti hyväksyttyjä vaatimuksia siitä, mitä varmistustoimenpiteitä tarvitaan sovellusten ja ohjaustoimintojen eri riskitasoilla. Sarjaväylien turvallisuusvaatimuksista (toiminnallisista tai laadullisista) ei ole vielä saatettu voimaan standardia. Ohjausjärjestelmän eri toiminnoilta *vaadittava turvallisuustaso* selviää koko konejärjestelmälle tehtävän *vaara- ja riskianalyysin perusteella.* Vaara-analyysissä määritelty turvallisuustaso vaikuttaa CAN-kommunikointijärjestelmän toteutukseen. On mahdollista, että vaara-analyysin perusteella asetetut turvallisuusvaatimukset sulkevat pois CAN-väylän käytön turvallisuuden kannalta kaikkein kriittisimmistä ohjauksista.

Hätäpysäytyksen perusvaatimus on se, että pysäytyksen tulee toimia ehdottoman luotettavasti kaikissa käyttötilanteissa. Ei ole itsestään selvää, voiko väylällä kulkea hätä- ja turvapysäytyssanomia. Ongelmia ovat myös, miten konejärjestelmän siirtyminen turvalliseen tilaan varmistetaan, jos väyläyhteys katkeaa, ja miten turvallinen toiminta varmistetaan, jos kriittisiä sanomia väylällä hukataan eikä ole tietoa siitä, mitä sanomia hävisi. Muita toteutuksen turvallisuuteen liittyviä kysymyksiä ovat mm:

- Mikä on maksimi väyläkuormitus?
- Onko CAN-protokollan päälle rakennettava lisää protokollaa?
- Mikä on väylällä lähetettävän tiedon merkitys käyttöturvallisuudelle?

- Miten tunnisteita on käytettävä eli miten sanomat priorisoidaan?

Nämä ongelmat liittyvät lähinnä ohjelmistoteknisiin ratkaisuihin. Laitteiston osalta ratkaistavia kysymyksiä ovat mm. väylän kahdennus, galvaanisen erotuksen käyttö, sähkömagneettisen yhteensopivuuden (EMC) varmistaminen jne. CAN-väylä voidaan periaatteessa rakentaa yhden vian sietäväksi, mutta jos sen täytyy sietää kahta yhtäaikaista vikaa, täytyy kahdentaa väylä tai käyttää erillistä varmistusta.

VTT:n koneautomaation tutkimusalueella on tutkittu CAN-väylän käyttöönottoon liittyviä teknologisia ongelmia ja niiden ratkaisutapoja yhteistyössä yritysten kanssa, mm. Tampereen paikallisen teknologiahankkeen (TAMTEK) yhteydessä. Hankkeen yhteydessä ei käsitelty tarkemmin turvallisuuteen liittyviä näkökohtia. Projektissa rakennettiin mm. demojärjestelmä, jossa oli neljä solmuasemaa. Järjestelmän suorituskykyä arvioitiin CAN-järjestelmien kehitystä tukevilla työkaluilla, kuten analysaattorilla ja simulaattorilla. Hankkeessa kartoitettiin myös muita CAN-järjestelmien kehitystä tukevia työkaluja (Alanen 1992).

Myös CAN-väyläjärjestelmän ylemmän kerroksen kommunikointiarkkitehtuureja on tutkittu VTT:n koneautomaation tutkimusalueella (Alanen & Virtanen 1994). Ohjelmoitavien elektronisten järjestelmien turvallisuuden arviointia ja sen menetelmäkehitystä on puolestaan tehty VTT:n turvallisuustekniikan tutkimusalueella (Tiusanen et al. 1994). Tutkimuskohteena ei kuitenkaan ole ollut hajautettuja järjestelmiä.

Tämän tutkimuksen tavoitteena oli tuottaa tietoa siitä, miten tunnistetaan ja hallitaan CAN-väyläjärjestelmiin liittyviä turvallisuustekijöitä ja mitä tekniikoita on käytettävissä turvallisuuden varmistamiseksi tai sen lisäämiseksi työkoneiden ja automaation CAN-väyläsovelluksissa. Suomessa jo toteutettuihin työkonesovelluksiin, joissa on CAN-väyläjärjestelmä, on turvallisuusongelmiin kehitetty ratkaisuja lähinnä yleisten koneturvallisuusvaatimusten ja ohjausjärjestelmiä koskevien vaatimusten pohjalta.

CAN-väyläjärjestelmien turvallisuuteen ja käyttövarmuuteen liittyviä tekijöitä tunnistettiin ja arvioitiin kolmen ohjausjärjestelmän avulla. Ohjattavat järjestelmät olivat Tamrock Oy:n tuotantoporauslaite, Vammas Oy:n lentokenttien lumenraivauskone sekä Pirkan Elektroniikka Oy:n ja UH-tekniikka Oy:n varavoimalakäyttö.

2 HAJAUTETTUJEN JÄRJESTELMIEN SUUNNITTELUUN LIITTYVIÄ TURVALLISUUSVAATIMUKSIA

2.1 KONEDIREKTIIVIN JA STANDARDIEN VAATIMUKSET

Valtioneuvoston päätös koneiden turvallisuudesta (Vnp 1314 1994) esittää koneiden suunnittelua ja rakennetta koskevat olennaiset terveys- ja turvallisuusvaatimukset. Päätöstä sovelletaan kaikkiin koneisiin ohjausjärjestelmän rakenteesta riippumatta. Koneiden hallintajärjestelmiä koskevia vaatimuksia on eritelty hallintalaitteille, käynnistämiselle, pysäytyslaitteille, toimintatavan valinnalle, energiansyötön häiriöille, ohjauspiirin häiriöille ja ohjelmistolle.

Vnp 1314:ssä sanotaan mm., että koneen hallintajärjestelmä on suunniteltava ja rakennettava siten, että se kestää tavanomaisen käytön ja ulkoisten tekijöiden vaikutukset ja että logiikkavirheet eivät johda vaaratilanteisiin. Hallintalaitteiden on oltava selvästi nähtävissä ja tunnistettavissa, tarkoituksenmukaisesti merkityt sekä siten sijoitetut, että niitä voidaan käyttää turvallisesti, nopeasti ja yksikäsitteisesti. Jos hallintalaiteen on tarkoitus suorittaa useita eri toimintoja, suoritettavan toiminnon on oltava selvästi ilmaistu ja tarvittaessa varmistettu. Tällaisia hallintalaitteita ovat esim. näppäimistöt, joilta puuttuu hallintatoiminnon ja sen vaikutuksen yksiselitteinen vastaavuus.

Koneen näyttölaitteista Vnp 1314:ssä sanotaan mm., että käyttäjän ja koneen hallintajärjestelmän välisen vuorovaikutteisen ohjelmiston on oltava käyttäjäystävällinen. Koneen hallitsemiseksi tarvittavan tiedon on oltava yksikäsitteistä ja käyttäjän on voitava helposti ymmärtää sitä. Hallintaan tarvittava tieto ei saa olla niin liiallista että käyttäjä ylikuormittuu.

SFS-EN 292-standardin tarkoituksena on antaa suunnittelijoille ja valmistajille yleiset ohjeet, jotta he voisivat tuottaa koneita, jotka ovat turvallisia koneiden tarkoitetussa käytössä. Standardin mukaan ohjausjärjestelmät on suunniteltava siten, että käyttäjän on mahdollista vaikuttaa turvallisesti ja helposti koneen toimintaan (SFS-EN 292-2 1992). Standardi antaa yleisperiaatteet ohjausjärjestelmien suunnitteluun turvatoimintojen aikaansaamiseksi ja vaarallisen toiminnan estämiseksi.

Ohjelmoitaville ohjausjärjestelmille on valmisteilla useita standardeja sekä IEC:n että CEN/CENELECin työryhmissä. IEC 1508 -standardiluonnoksessa esitetään niitä piirteitä, joita turvatoimintoja suorittavan ohjelmoitavan elektronisen järjestelmän tulee sisältää. Kohdassa 2.2 kerrotaan tämän standardiluonnoksen turvallisuuden elinkaarimallista.

Standardiluonnoksessa prEN 954-1 (1994) kerrotaan *ohjausjärjestelmien turvallisuuteen liittyvien osien* turvallisuusvaatimuksista ja annetaan ohjeita niiden suunnitteluperiaatteista. Ohjausjärjestelmien turvallisuuteen liittyville osille määritellään kategoriat ja eri kategorioihin kuuluvien turvatoimintojen piirteitä kuvataan. Kategoriat esitetään taulukkomuodossa liitteessä 1. Standardi kattaa myös kaikenlaisten koneistojen ohjelmoitavat järjestelmät ja niihin liittyvät suojalaitteet, ja

siten standardi koskee myös CAN-järjestelmiä. Standardia sovelletaan kaikkiin ohjausjärjestelmien turvallisuuteen liittyviin osiin käytetystä energiatyypistä (esim. elektroninen, hydraulinen, pneumaattinen, mekaaninen) riippumatta. Standardi ei kuitenkaan määrittele, mitä turvatoimintoja ja mitä kategorioita tietyssä tapauksessa tulee käyttää.

Standardi SFS-EN 60204-1[1] (1993) käsittelee koneiden sähkölaitteiden yleisiä vaatimuksia. Standardissa koneen *pysäytystoiminnot* jaetaan kolmeen luokkaan. Pysäytysluokassa 0 koneen toimilaitteilta kytketään välittömästi tehot pois. Pysäytysluokassa 1 pysäytys tapahtuu hallitusti, ja vasta pysähtymisen jälkeen toimilaitteilta kytketään tehot pois. Pysäytysluokassa 2 pysäytys tapahtuu myös hallitusti, mutta toimilaitteilta ei kytketä tehoja pois, vaikka liike pysähtyy. Luokissa 0 ja 1 pysäytysten on oltava aina mahdollisia riippumatta koneen toimintamoodista. Pysäytysluokka 0 on aina etusijalla. Pysäytystoiminnot poistavat energian koneen pääpiireiltä ja estävät koneen toimintojen aloitukset. Tarvittaessa on käytettävä suojalaitteita ja lukituksia. Pysäytystoiminnoista ja pysäytystiloista tulisi mennä viesti ohjausjärjestelmän logiikalle. Pysäytystoiminnon resetointi ei saa käynnistää vaaratilannetta.

Hätäpysäytykseltä vaaditaan em. pysäytystoiminnoille asetettujen vaatimusten lisäksi, että se ohittaa kaikki muut koneen ohjaustoiminnot kaikissa toimintamoodeissa ja kytkee tehot pois mahdollisimman nopeasti koneen toimilaitteista, jotka voivat aiheuttaa vaaratilanteen, aiheuttamatta muita vaaroja. Lisäksi vaaditaan, että hätäpysäyttimen resetointi ei saa käynnistää konetta. Tarvittaessa on käytettävä useaa hätäpysäytintä. Hätäpysäytys tapahtuu pysäytysluokan 0 tai 1 mukaisesti. Hätäpysäytyksen luokan valinta on tehtävä koneen riskin arvioinnin perusteella.

SFS-EN 60204-1 -standardissa sanotaan, että ohjelmoitavia elektroniikkalaitteita ei saa käyttää luokan 0 *hätäpysäytystoiminnoissa*, vaan ainoastaan kiinteästi johdotetut sähkömekaaniset komponentit ovat sallittuja. Toiminta ei saa riippua elektroniikan logiikasta (laitteistosta tai ohjelmistosta) eikä ohjauskäskyjen siirtämisestä tiedonsiirtoverkon tai -yhteyden kautta. Luokan 1 hätäpysäytystoiminnossa lopullinen tehon poistaminen koneen toimilaitteilta on myös varmistettava ja toteutettava sähkömekaanisilla komponenteilla. Standardin määräykset eivät kuitenkaan estä CAN-väylän kautta tapahtuvaa hätäpysäytystä luokan 1 hätäpysäytystoimintoa käytettäessä.

Hätäpysäytykselle tämä standardi, kuten myös hätäpysäytystä koskeva standardi SFS-EN 418, mainitsee monia muitakin vaatimuksia. Tässä käsitellään vain nimenomaan ohjelmoitavia järjestelmiä, joihin CAN-väyläjärjestelmät kuuluvat, koskevia vaatimuksia.

---

[1] Standardin esikuvana on standardi IEC 204-1:1992, johon on tekeillä muutoksia. Tässä esitetään nykyisin voimassa olevia vaatimuksia.

Turvallisuuteen liittyvissä pysäytystoiminnoissa standardi SFS-EN 60204-1 suosittelee käytettäväksi kiinteästi johdotettuja sähkömekaanisia komponentteja. Toiminnot eivät saisi riippua ohjelmoitavista elektroniikkalaitteista. Mikäli ohjelmoitavia elektroniikkalaitteita käytetään tällaisiin toimintoihin, on käytettävä sopivia toimenpiteitä, joita ovat

- koneen suojalaitteet (esim. toimintaan lukitut suojukset, lähestymispysäyttimet),
- sähköisten piirien lukitukset turvatoimintaan,
- hyväksi koettujen piiritekniikoiden ja komponenttien käyttö,
- toimenpiteet osittaisen tai täydellisen varmennuksen tai erilaisuuden käyttämiseen ja
- toimenpiteet toiminnallisia testejä varten.

Nämä vaatimukset eivät saa estää ohjelmoitavan elektroniikkalaitteen käyttöä turvallisuuteen liittyvien pysäytystoimintojen valvonnassa, testauksessa tai varmistamisessa, mutta elektroniikkalaite ei saa estää näiden toimintojen oikeaa suorittamista. On vaikeaa luotettavasti todeta, että yksikanavaisen ohjelmoitavan elektroniikkalaitteen oikeaan toimimiseen voitaisiin luottaa, jos ohjausjärjestelmän virhetoiminnoista voi aiheutua merkittävää vaaraa (SFS-EN 60204-1 1993).

Muisteja käytettäessä on varmistettava koneen oikea toiminta jännitehäiriötilanteissa esim. käyttämällä pyyhkiytymätöntä muistia, mikäli muistin häviäminen voi aiheuttaa vaarallisen tilan. Sopivin toimenpitein on myös estettävä asiattomien henkilöiden suorittama muistin muuttaminen.

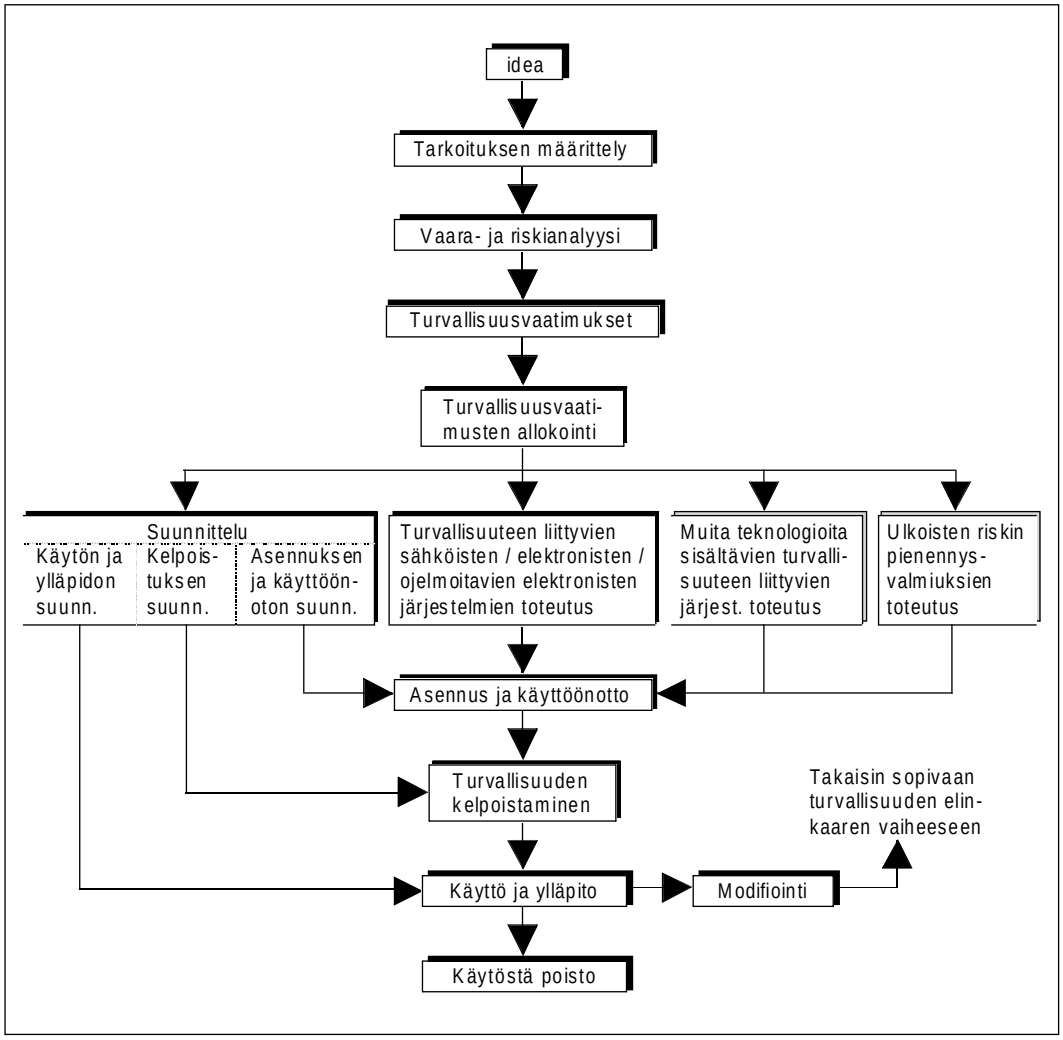
SFS-EN 60204-1-standardissa sanotaan vielä, että ohjelmoitavien ohjauslaitteiden on oltava asiaankuuluvien IEC-standardien mukaiset. Tässä kohdassa viitataan standardiin IEC 1131, joka käsittelee ohjelmoitavia ohjauslaitteita.

Varsinaisista CAN-standardeista ei tässä raportissa kerrota, ellei kyse ole turvallisuuteen liittyvistä ominaisuuksista. CAN-standardeista on kerrottu tarkemmin mm. julkaisussa ”Ylemmän kerroksen kommunikointiarkkitehtuurit” (Alanen et al. 1994).

2.2 TURVALLISUUDEN ELINKAARIMALLI

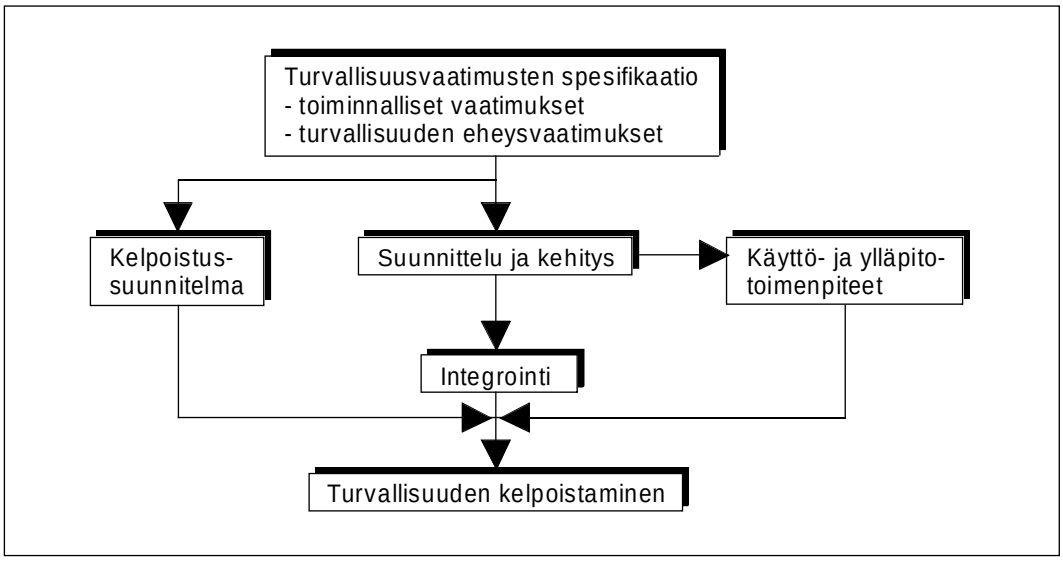
IEC 1508 -standardiluonnoksessa käsitellään turvallisuuteen liittyvien sähköisten, elektronisten tai ohjelmoitavien elektronisten järjestelmien koko elinkaaren aikana huomioon otettavia näkökohtia. Kuvassa 1 on tämän standardiluonnoksen pohjalta piirretty turvallisuuden elinkaarimalli, joka koskee koko ohjattavaa järjestelmää. Standardiluonnos on sovellettavissa mm. prosessiteollisuuden, valmistavan teollisuuden, liikenteen ja lääketieteen alueen turvallisuuteen liittyviin sähköisiin, elektronisiin ja ohjelmoitaviin elektronisiin järjestelmiin, rajoittumatta kuitenkaan pelkästään näihin sovellusalueisiin. Standardin päätarkoitus on auttaa sovelluskohtaisten standardien kehitystyössä, mutta standardia voidaan soveltaa turvallisuuteen liittyvän järjestelmän kehitystyössä silloin, kun sovelluskohtaista standardia ei

ole käytettävissä. Standardiluonnoksessa ei puhuta hajautettujen järjestelmien väyläliikenteeseen liittyvistä asioista.



Kuva 1. Ohjattavan järjestelmän turvallisuuden elinkaari.

Ohjelmoitavan elektronisen järjestelmän laitteisto- ja ohjelmistototeutukselle voidaan esittää kuvan 2 mukainen turvallisuuden elinkaarimalli. Näitä laitteiston ja ohjelmiston turvallisuussuunnittelun toteutusvaiheita varten standardiluonnos esittelee joukon tekniikoita, menetelmiä ja toimenpiteitä, joiden käytölle on annettu erilaisia suosituksia turvallisuuden eri eheystasoille.



Kuva 2. Laitteiston ja ohjelmiston turvallisuuden elinkaari.

Standardiluonnoksessa esitetyt suositukset eri tekniikoiden, menetelmien ja toimenpiteiden käytöstä auttavat ohjausjärjestelmän suunnittelijaa päättämään mm., millainen hänen ohjausjärjestelmänsä tulisi olla rakenteeltaan ja ohjelmiston ominaisuuksiltaan ja mitä menetelmiä ja tekniikoita hänen tulisi käyttää laitteiston ja ohjelmiston suunnittelussa määrätyn turvallisuuden eheystason sovelluksessa, jotta turvallisuus toteutuisi koko laitteiston ja ohjelmiston elinkaaren aikana.

Seuraavassa on selitetty kuvan 1 kaavio kohta kohdalta.

Ideavaiheessa luodaan käsitys ohjattavasta laitteesta ja sen ympäristöstä. Näin ollen tässä vaiheessa perehdytään perinpohjaisesti laitteeseen ja sen ohjausjärjestelmään sekä fyysiseen ympäristöön. Ideavaiheessa tunnistetaan myös todennäköisten vaarojen lähteet ja hankitaan tietoja niistä. Tietoja hankitaan myös nykyisistä kansallisista ja kansainvälisistä turvallisuusmääräyksistä. Myös vuorovaikutuksesta toisten laitteiden kanssa aiheutuvat vaarat tulee ottaa huomioon.

Tarkoituksen määrittelyvaiheessa määritetään laitteen rajat sekä vaara- ja riskianalyysin ulottuvuus. Tässä identifioidaan vaara- ja riskianalyysiin sisällytettävä fyysinen laitteisto (laite + ohjausjärjestelmä) sekä tunnistetaan analyysissä huomioon otettavat ulkoiset tapahtumat. Lisäksi tunnistetaan vaaroihin liittyvät osajärjestelmät ja onnettomuuksia aloittavat tapahtumat.

Vaara- ja riskianalyysin tavoitteena on laitteen ja sen ohjausjärjestelmän vaarojen tunnistaminen kaikissa toimintatiloissa ja odotettavissa olevissa olosuhteissa vikatilanteet, väärinkäyttö ja inhimilliset tekijät mukaan lukien. Tunnistetaan myös vaaroihin liittyvät tapahtumaketjut ja määritetään vaaroihin liittyvä riski. Vaarojen eliminointiin tulee kiinnittää huomiota. Arvioidaan vaaratapahtumiin liittyvät potentiaaliset seuraukset ja vaaratapahtuman esiintymistaajuus tai todennäköisyys.

Yleiset **turvallisuusvaatimukset** spesifioidaan kaikille turvallisuuteen liittyville järjestelmille (SRS) ja muille riskin pienennysvalmiuksille toiminnallisen turvallisuuden saavuttamiseksi. Spesifikaatio koostuu toiminnallisista vaatimuksista ja

turvallisuuden eheysvaatimuksista. Edellisessä spesifioidaan turvatoiminnot, joilla varmistetaan turvallinen toiminta kunkin tunnistetun vaaran yhteydessä, ja turvallisuustaso jokaista tunnistettua vaaraa kohden. Spesifioidaan myös tarpeellinen riskin vähentäminen em. turvallisuustason saavuttamiseksi. Jälkimmäisessä spesifioidaan turvallisuuden eheysvaatimukset kutakin turvatoimintoa kohden turvallisuuden eheystasoina (safety integrity levels).

Turvallisuusvaatimukset allokoidaan määrätyille SRS:ille ja muille riskin pienennysvalmiuksille. Tavoitteena on myös turvallisuuden eheystason allokointi kullekin turvallisuusvaatimusten spesifikaatioon sisältyvälle turvatoiminnolle. Määrätyt toiminnallisen turvallisuuden saavuttamiseksi käytettävät SRS:t spesifioidaan.

Käyttö- ja ylläpitosuunnitelma kehitetään sen varmistamiseksi, että SRS:ien toiminnallinen turvallisuus ylläpidetään toiminnan ja huollon aikana. Tämä suunnitelma spesifioi mm. toiminnallisen turvallisuuden ylläpitämiseksi suoritettavat rutiinitoiminnat, toiminnat ja tarpeelliset pakkokeinot vaarallisen tilan ehkäisemiseksi (esim. käynnistyksen aikana) ja vaaratapahtuman esiintyessä, tiedot ylläpidettävistä tallenteista (esim. vaaratapahtumat), ylläpitoaktiviteettien soveltamisalueen ja käyttö- ja ylläpitopäiväkirjan sisällön.

Koko SRS-kombinaation ja muiden riskin pienennysvalmiuksien kelpoistamista varten tehdään **kelpoistussuunnitelma**. Kelpoistussuunnitelma sisältää mm. sellaisia tietoja kuin kelpoistuksen menettelytavan, ympäristön (esim. testien kohdalla kalibroidut työkalut ja varusteet), ajankohdan, ketkä tekevät, ennen laitteen käyttöönottoa kelpoistettavat SRS:t ja muut riskin pienennysvalmiudet, tarvittavat toimenpiteet, joilla varmistetaan kunkin turvatoiminnon yhdenmukaisuus turvatoimintojen vaatimusmäärittelyn ja turvallisuuden eheysvaatimuksen kanssa, sekä kelpoistuksen arviointimenettelyt. Kelpoistuksessa otetaan huomioon laitteen kaikki toimintavaiheet.

Kelpoistussuunnitelmassa on tunnistettava kaikki vaatimukset kelpoistamisprosessin kaikkien vaiheiden toteuttamiseksi. Suunnitelma olisi kehitettävä samanaikaisesti ohjausjärjestelmän turvallisuuteen liittyvien osien suunnittelun kanssa, mutta se voidaan esittää asiaankuuluvassa C-tyypin standardissa (prEN 954-1 1994).

SRS:ien ja muiden riskin pienennysvalmiuksien **asennus ja käyttöönotto suunnitellaan** siten, että toiminnallinen turvallisuus saavutetaan. Asennussuunnitelmassa esitetään mm. asennusajankohta, menettelytapa, ketkä henkilöt tekevät minkäkin osan asennuksesta jne. Käyttöönottosuunnitelmassa esitetään käyttöönoton ajankohta, menettelytapa, ketkä henkilöt suorittavat käyttöönoton ja yhteys kelpoistukseen.

Tavoitteena on, että **turvallisuuteen liittyvät elektroniset, sähköiset ja ohjelmoitavat elektroniset järjestelmät toteutetaan** turvallisuusvaatimusspesifikaation mukaisiksi. Sekä laitteistolle että ohjelmistolle laaditaan aluksi turvallisuusvaatimusten spesifikaatiot, jotka koostuvat turvatoimintojen vaatimusten spesifikaati-

osta ja turvallisuuden eheysvaatimusten spesifikaatiosta. Tämän jälkeen laitteiston ja ohjelmiston kehitys etenee kuvan 2 mukaisesti.

SRS-kombinaatio ja ulkoiset riskin pienennysvalmiudet **asennetaan ja otetaan käyttöön** suunnitelmien mukaisesti. Asennusraportti sisältää tiedot asennusprosessista ja siihen kirjataan myös tiedot mahdollisista vioista ja yhteensopimatto

Kelpoistusprosessi tapahtuu kelpoistussuunnitelman mukaisesti. Tavoitteena on muuksista. kelpoistaa se, että koko SRS-kombinaatio ja muut riskin pienennysvalmiudet noudattavat joka suhteessa yleistä turvallisuuden kelpoistusspesifikaatiota. Kelpoistusaktiviteetit ja niiden tulokset sekä työkalut ja varusteet kalibrointitietoineen kirjataan kelpoistamisraporttiin.

Laitetta ja sen ohjausjärjestelmää sekä koko SRS-kombinaatiota muine riskin pienennysvalmiuksineen **käytetään ja ylläpidetään** suunnitelman mukaisesti siten, että toiminnallinen turvallisuus säilyy. Tässä vaiheessa pidetään lokikirjaa, johon tallennetaan tiedot mm. tehdyistä modifikaatioista, testeistä, sattuneista vikaantumisista sekä turvatoimintojen käynnistymisien syistä ja ajankohdista.

Lopuksi varmistetaan, että toiminnallinen turvallisuus SRS:n ja muiden riskin pienennysvalmiuksien osalta on tarkoituksenmukainen **modifioinnin** aikana ja sen jälkeen sekä **käytöstä poiston** aikana ja sen jälkeen. Modifioinnin seuraus SRS:ien toiminnalliseen turvallisuuteen tai muihin riskin pienennysvalmiuksiin tulee analysoida ja dokumentoida. Myös käytöstä poistoon liittyvät toimenpiteet dokumentoidaan.

2.3 MUIDEN SARJAMUOTOISTEN VÄYLIEN TURVALLISUUSTEKNIIKOITA

Sarjamuotoisia väyliä ja kenttäväyliä koskeva standardisointityö on varsin keskeneräistä. Tässä esitetään poimintoja standardiluonnoksesta IEC 1491 vuodelta 1995 ja standardista IEC 870-5-1 vuodelta 1990. IEC 1491 -standardiluonnoksessa kerrotaan sarjamuotoisesta tietoyhteydestä reaaliaikaiseen ohjausyksiköiden ja käyttöjen väliseen viestintään. IEC 870-5-1 käsittelee kauko-ohjattujen laitteiden ja järjestelmien siirtoprotokollia, erityisesti kehysmuotoja.

2.3.1 IEC 1491 -standardiluonnos

IEC 1491 -standardiluonnoksen luvussa 10 puhutaan virheenkäsittelystä. Luku on jaettu seuraaviin otsikoihin: käyttölaitteen turvatoiminnot, sanomien vikaantuminen, kommunikointivaiheiden vaihtaminen (nousevat ja laskevat kommunikointivaiheet), valvonta isännässä (Master) ja orjassa (Slave), reaktio kättelyaikavalvontaan (handshake-timeout), vastaus virheilmoituksiin käyttökanavalla ja virhelaskurit isännässä ja orjassa. Virheenkäsittely perustuu periaatteeseen, jonka mukaan käyttölaitteet varustetaan valvovilla toiminnoilla, jotka takaavat alasajon tilanteissa, joissa oikea vastaus ohjausyksiköltä tuleviin käskyihin on estynyt. Seuraavassa kuvataan IEC 1491 -standardiluonnoksen luvussa 10 esitettyjä periaatteita.

Standardiluonnoksen IEC 1491 luvussa 10 sanotaan sanomien vikaantumisesta siten, että sanoma on hyväksyttävä, jos CRC-tarkistus ei löydä virhettä, sanoma saapuu määritellyissä aikatoleranssirajoissa ja sanoman pituus on oikea. Lisäksi MST (Master Sync Telegram) on hyväksyttävä ainoastaan, jos INFO-tavu ilmaisee oikean kommunikointivaiheen.

Jos vika ilmenee MST:ssä, MDT:ssä (Master Data Telegram) tai AT:ssä (Drive Amplifier Telegram), isännän tai orjan tulee vastata seuraavasti:

- Viimeisten oikeiden käskyarvojen perusteella käyttölaite voi laskea sisäiset käskyarvot korvaamaan puuttuvan sanoman.
- Käyttöliittymän synkronointi tulee ylläpitää.
- Sisäinen laskuri tulee inkrementoida puuttuvien sanomien vuoksi.
- AT lähetetään vain, jos MST on vastaanotettu.

Sanomien vikaantumiseen liittyen standardiluonnoksessa esitetään seuraavat virhemallit kaikille tiedonsiirtovaiheille: MST:n häviäminen tai vikaantuminen, MDT-sanomien vikaantuminen ja AT-sanomien vikaantuminen. Kunkin tiedonsiirtovaiheen kohdalla esitetään reaktiot isännässä ja orjassa.

2.3.2 IEC 870-5-1 -standardi

IEC 870 -standardisarjaa sovelletaan kauko-ohjauslaitteisiin ja järjestelmiin, joissa käytetään koodattua sarjamuotoista datan siirtoa erilaisten prosessien valvontaan ja ohjaukseen. Standardisarjan osa 5 määrittelee normit tietyn datan eheyden vaatimukset täyttävälle, muuttuvan ja kiinteän pituiselle datakehyksen koodaukselle, muodolle ja synkronoinnille.

Kauko-ohjauksessa datan siirtoon liittyy kolme datan eheyttä (data integrity) kuvaavaa luokkaa: I1, I2 ja I3 (taulukko 1). Sovelluksessa tarvittavan datan luonne määrää vaadittavan luokan. Korkeat datan eheyden vaatimukset saavutetaan pienentyneen informaation nopeuden kustannuksella, joten näiden kahden vaatimuksen välillä on tehtävä kompromissi, jotta järjestelmälle asetetut vaatimukset täyttyvät. Siirtolinjan kuntoa valvotaan jatkuvasti.

Eheysluokka riippuu käytetyn koodausmenetelmän Hamming distance d:stä. Hamming distance on binäärilukujen erilaisuuden määrää kuvaava yksikkö. Se on lukuarvo, joka kertoo, kuinka monta eri bittiä binääriluvuissa on. Lukua käytetään digitaalisessa tietoliikenteessä kuvaamaan viestien häiriösietoa (Malm et al. 1995). Keskimääräisen bittivirheiden (d kpl kääntynyttä bittiä) todennäköisyyden on oltava pienempi kuin 10^{-4}, jotta saavutetaan vaadittu datan eheysluokka ja informaation siirtoaika. Minimi Hamming distance 2 vaaditaan alimmassa eheysluokassa I1. Luokissa I2 ja I3 vaaditaan koodi, jossa minimi Hamming distance on 4. Lisäksi vaaditaan, että luokassa I3 virhe ei ylitä arvoa $R= 10^{-12}$.

Taulukko A. Datan eheysluokat (IEC 870-5-1 1990).

Eheysnumerot sanomapituudelle n = 100 bittikehystä, kun v = 1200 bittiä/s ja p = 10^{-4} .			
Datan eheysluokka	Jäännösvirhe-määrä R	Keskim. aika T havaitsemattomien virheiden välillä	Tyypillinen sovellus
I1	10^{-6}	1 päivä	Jaksottaiset päivitysjärjestelmät; kaukomittaus
I2	10^{-10}	26 vuotta	Tapahtumasta alulle pantava lähetys; kaukoilmaisu; kaukolukeminen
I3	10^{-14}	260 000 vuotta	Kriittisen tiedon lähettäminen; kaukokomennot

Kauko-ohjausjärjestelmän toiminnot on jaettu erillisiin kerroksiin ISOn OSI (Open System Interconnection) -mallin mukaisesti. Tämä standardin osa määrittelee fyysisen kerroksen kauko-ohjausvaatimukset ja linkkikerroksen normaalilähetyksen kehysmuodot.

Fyysinen kerros eristää ohjauspaikan galvaanisesti siirtolinjasta, siirtää signaalin linkkikerroksesta siirtolinjaan, huolehtii bittien synkronoinnista, lisää ja poistaa kehyksen synkronoinnin sekä valvoo signaalin laatua ja siirtolinjaa. Fyysisestä kerroksesta johtuvia datan eheyteen ja siirron tehokkuuteen vaikuttavia tekijöitä ovat signaalinopeus, signaali-kohinasuhde ja bittivirheet.

Linkkikerros hyväksyy, suorittaa ja valvoo siirtoon liittyviä palveluja, joita korkeammat kerrokset pyytävät. Se ilmoittaa siirron onnistumisesta ja virheistä korkeammille kerroksille sekä myös havainnoista siirtolinjojen ja ohjausasemien toimintatiloista. Linkkikerros vastaa siitä, että informaatio säilyttää määritetyn datan eheysluokan ilmaisemalla havaitut virheet, generoimalla ja valvomalla virheitä havaitsevia koodeja ja ohjaamalla virheitä korjaavia menetelmiä. Se sarjoittaa ja purkaa kehyksen, lisää ja poistaa kehyksen rajoittimet, havaitsee kehyksen synkronointivirheet ja pituusvirheet, tunnistaa tietylle asemalle osoitetut kehykset ja valvoo signaalin laatua, ellei fyysinen kerros sitä tee. Standardi määrittelee kolme palveluluokkaa taulukon 2 mukaisesti.

Taulukko B. Linkkikerroksen palveluluokat (IEC 870-5-1 1990).

Palveluluokka	Funktio	Selitys
S1	LÄHETTÄÄ / EI VASTAUSTA	Lähettää sanoman; linkkikerroksen sisällä ei pyydetä saanti-ilmoitusta eikä vastausta
S2	LÄHETTÄÄ / VAHVISTAA	Lähettää sanoman; linkkikerroksen sisällä pyydetään saanti-ilmoitus
S3	PYYNTÖ / VASTATA	Lähettää pyynnön; vastaus pyydetään linkkikerroksen sisällä; vastaus saattaa sisältää dataa tai negatiivisen saanti-ilmoituksen

Palveluluokkaa S1 (SEND/NO REPLY) käytetään jaksoittaisia ja toistuvia tehtäviä suorittavissa järjestelmissä tai yksisuuntaisissa järjestelmissä, joissa ei ole käy-

tettävissä vastauskanavaa. Vastaanottimessa havaitut kehysvirheet aiheuttavat häviöitä vastaanotetussa informaatiossa.

Palveluluokkaa S2 (SEND/CONFIRM) käytetään esim. lähetettäessä satunnaisesti informaatiota. Vastaanottimen linkkikerros tarkistaa vastaanotetun sanoman; jos virheitä ei havaita, se lähettää takaisin lähettimelle positiivisen ACK-ilmoituksen (acknowledgement) vahvistaen sanoman oikean vastaanoton. Jos vastaanottimen puskuri ei ole vapaa, lähetetään negatiivinen NACK-ilmoitus (negative acknowledgement). Jos sanoman kehyksessä havaitaan virhe, ei vastausta lähetetä ja sanoma hylätään.

Lähetysaseman linkkikerros on valmis vastaanottamaan uuden tehtävän saatuaan positiivisen ilmoituksen. Se raportoi ilmoituksen vastaanotosta korkeammille kerroksille. Jos ilmoitusta ei havaita, sanoman lähetys toistetaan. Sanoma toistetaan useita kertoja (ennalta sovittu määrä), ja jos vastausta ei edelleenkään kuulu, linkkikerros raportoi ”lähetysvirhe”-ilmoituksen korkeammille tasoille ja sanoma hylätään. Häiriöiden aiheuttamat virheelliset ilmoitukset voidaan estää esimerkiksi käyttämällä juoksevaa kehysnumerointia tai siten, että vastaanottimen puskuri vastaanottaa sanoman oikein ennen kuin se vastaanottaa kehyksen, jolloin lähetysasema ei toista edellistä kehystä.

Palveluluokka S3 (REQUEST/RESPOND) toteuttaa ”LUE”-käskyjä. Vastaanottoaseman linkkikerros lähettää pyydetyn datan, jos se on saatavissa. Muuten se vastaa negatiivisella ilmoituksella. Vastausta ei lähetetä, jos sanomassa havaitaan kehysvirhe. Jos vastausta ei havaita tai vastauksessa on häiriöitä, lähetysaseman linkkikerros toistaa kehyksen lähetyksen. Jos vastausta ei kuulu toistoista huolimatta (tietty määrä toistoja), ilmoitetaan ”lähetysvirhe” korkeammille kerroksille, muussa tapauksessa vastaanotettu vastaus toimitetaan eteenpäin.

Kaikki kolme palveluluokkaa soveltuvat informaation lähettämiseen yhden lähetysaseman ja yhden pääteaseman (single address), pääteasemaryhmän (group address) tai pääteaseman tyyppisten muiden asemien välillä (global address). Palveluluokat tukevat kolmea lähetyksen aloitusmuotoa taulukon 3 mukaisesti.

Taulukko C. Lähetyksen aloitusmuodot (IEC 870-5-1 1990).

Lähetyksen aloitusmuoto	Palveluluokka
Jaksoittainen lähetys	Luokka S1 - LÄHETTÄÄ / EI VASTAUSTA
Tapahtumasta alulle pantava lähetys (spontaaninen lähetys)	Luokka S2 - LÄHETTÄÄ / VAHVISTAA
Lähetys pyydettäessä	Luokka S3 - PYYNTÖ / VASTATA

Määrätyt vaatimukset täyttävä kehys muodostetaan tietyllä tavalla formaattiluokista. **Formaattiluokka FT1.1** määrittelee koodin, jossa Hamming distance on 2. Tämä muodostetaan lisäämällä aloitusbitti, pariteettibitti ja lopetusbitti kahdeksan bitin muodostamaan informaatio-osaan. Lisäämällä formaattiluokan FT1.1 koodiin tarkistussummamerkki saadaan FT1.2-koodi, jonka Hamming distance on 4.

Formaattiluokassa FT1.2 vastaanotin tarkistaa aloitusbitin, lopetusbitin ja parillisen pariteettibitin sekä kehyksen aloitusmerkin, tarkistussumman ja loppumerkin. Kehysten välillä on tietyn pituinen tauko. Kehys hylätään, jos jokin tarkistuksista epäonnistuu; muuten se on käyttäjän käytettävissä. Kehys voi olla pituudeltaan myös muuttuva.

Formaattiluokka FT2 määritellään koodilla, jonka Hamming distance on 4 ja joka sisältää maksimissaan 15 dataoktettia (8 bittinen) ja yhden tarkistusoktetin. Kehys alkaa oktetin suuruisella aloitusmerkillä. Tietyllä polynomilla ja parillisella pariteettibitillä generoidaan tarkistuskoodi. Kaikki 8 tarkistusbittiä on käännetty. Vastaanotin tarkistaa signaalin laadun, aloitusmerkin, tarkistuskoodin ja kehyksen pituuden. Myös tässä on kehysten välissä tietyn pituinen tauko. Kehys hylätään, jos jokin tarkistuksista epäonnistuu; muuten se on käyttäjän käytettävissä. Kehys voi olla myös muuttuva pituudeltaan.

Molemmat kehysformaatit, FT1.2 ja FT2, täyttävät datan eheysluokan I2 vaatimukset. Formaattiluokassa FT1.2 saavutetaan pienempi virhe, erityisesti silloin, kun bittivirheiden todennäköisyys on suuri. Formaattiluokassa FT2 kehyksen siirto on nopeampaa.

Vaativin **formaattiluokka FT3** määritellään koodilla, jonka Hamming distance on 6 ja joka sisältää maksimissaan 16 dataoktettia ja kaksi tarkistusoktettia.

Informaatiokentän pituus vaihtelee oktetin suuruisina moninkertoina. Formaattiluokkien FT2 ja FT3 lyhennetetyt versiot, joissa informaatiokenttää (k) on supistettu oktetin suuruisin askelin minimisuuruuteen (k=8 bittiä) asti, ovat sallittuja.

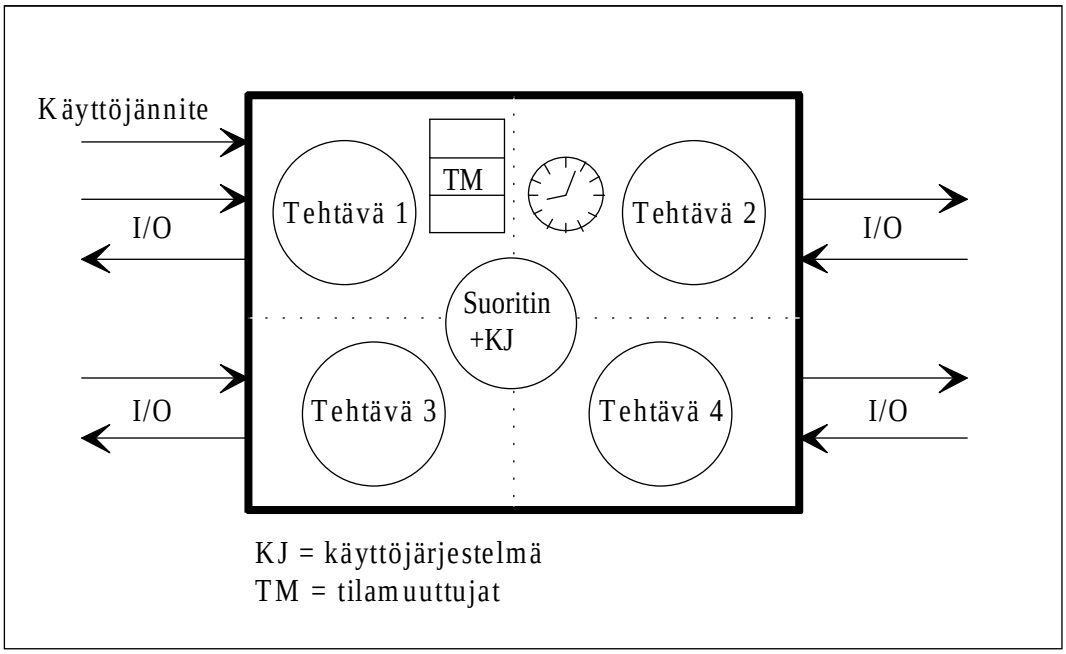
Formaattiluokka FT1.1, jonka Hamming distance on 2, soveltuu käytettäväksi järjestelmissä, joissa vaaditaan alhaista datan eheysluokkaa, ts. järjestelmän toiminnot ovat yksinkertaisia ja toistuvia. Formaattiluokkia FT1.2 ja FT2, joissa Hamming distance on 4, käytetään ohjausjärjestelmissä, joissa datan eheysvaatimukset ovat korkeat ja järjestelmän suorittamat toiminnot vaativia. Formaattiluokkaa FT3, jonka Hamming distance on 6, on sovellettava, kun datan eheydelle asetetaan erityisen korkeat vaatimukset.

3 CAN-JÄRJESTELMÄN VIKAMUODOT

3.1 HAJAUTETUN JA KESKITETYN JÄRJESTELMÄN EROT

Tässä luvussa tarkastellaan, mitä uusia vikamuotoja hajautetussa järjestelmässä - erityisesti CAN-väylää käyttävässä järjestelmässä - on keskitettyyn järjestelmään verrattuna. Suojautumiskeinoja vikamuotoja vastaan esitetään edempänä.

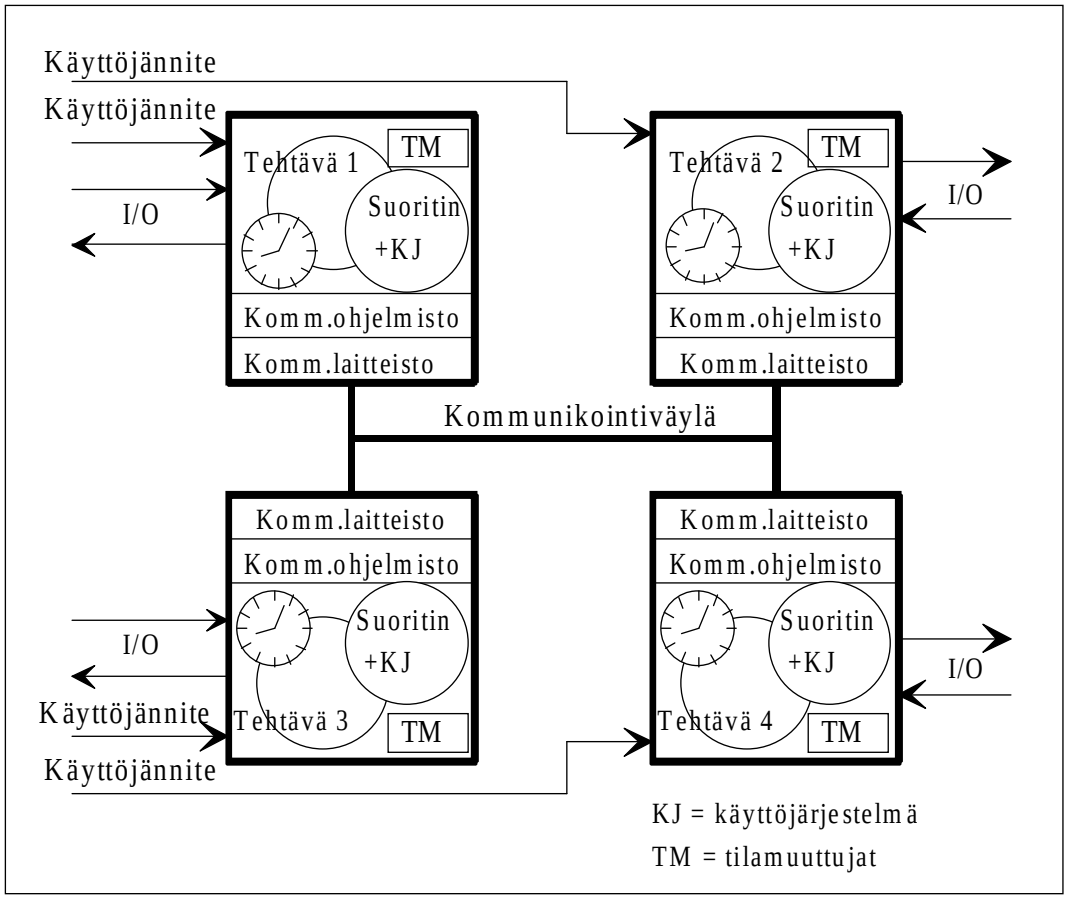
Perinteisessä keskitetyssä järjestelmässä (kuva 3) on yksi suoritin, joka suorittaa kaikki järjestelmään liittyvät tehtävät, kuten anturien lukemisen, ohjausalgoritmin suorituksen ja toimilaitteiden ohjauksen.



Kuva 3. Keskitetty järjestelmä.

Hajautetussa järjestelmässä on useita suorittimia, jotka suorittavat rinnakkaisesti järjestelmän osatehtäviä (kuva 4). Hajautuksesta aiheutuvia uusia vikatilanteita ovat

- vika kommunikointijärjestelmässä (kaapelissa, liittimissä, lähetin-vastaanottimessa, protokollapiirissä tai kommunikointiohjelmistossa)
- liian pitkät kommunikointiviiveet
- eri solmuilla olevat tehtävät eivät ole keskenään oikeassa tahdissa, koska
  - solmut ovat eri tilassa (esim. yhden solmun yllättävän uudelleenkäynnistyksen takia)
  - solmuilla on eri käsitys ajasta
  - solmuilla on ristiriitainen käsitys yhteisten tilamuuttujien arvoista.



Kuva 4. Hajautettu järjestelmä.

Edellä mainittujen vikatilanteiden lisäksi voidaan kuvitella tilanne, jossa yksi tai osa solmuista pimenee täysin, esimerkiksi käyttöjännitteiden häviämisen takia (regulaattori rikkoutuu). Tämä vikamuoto ei poikkea keskitetyn järjestelmän vastaavasta vikamuodosta muuten kuin siten, että järjestelmä ei tällaisesta vikatilanteesta halvaannu kokonaan vaan voi mahdollisesti vielä “nilkuttaa kotiin”.

3.2 KOMMUNIKOINTIJÄRJESTELMÄN VIKAMUODOT

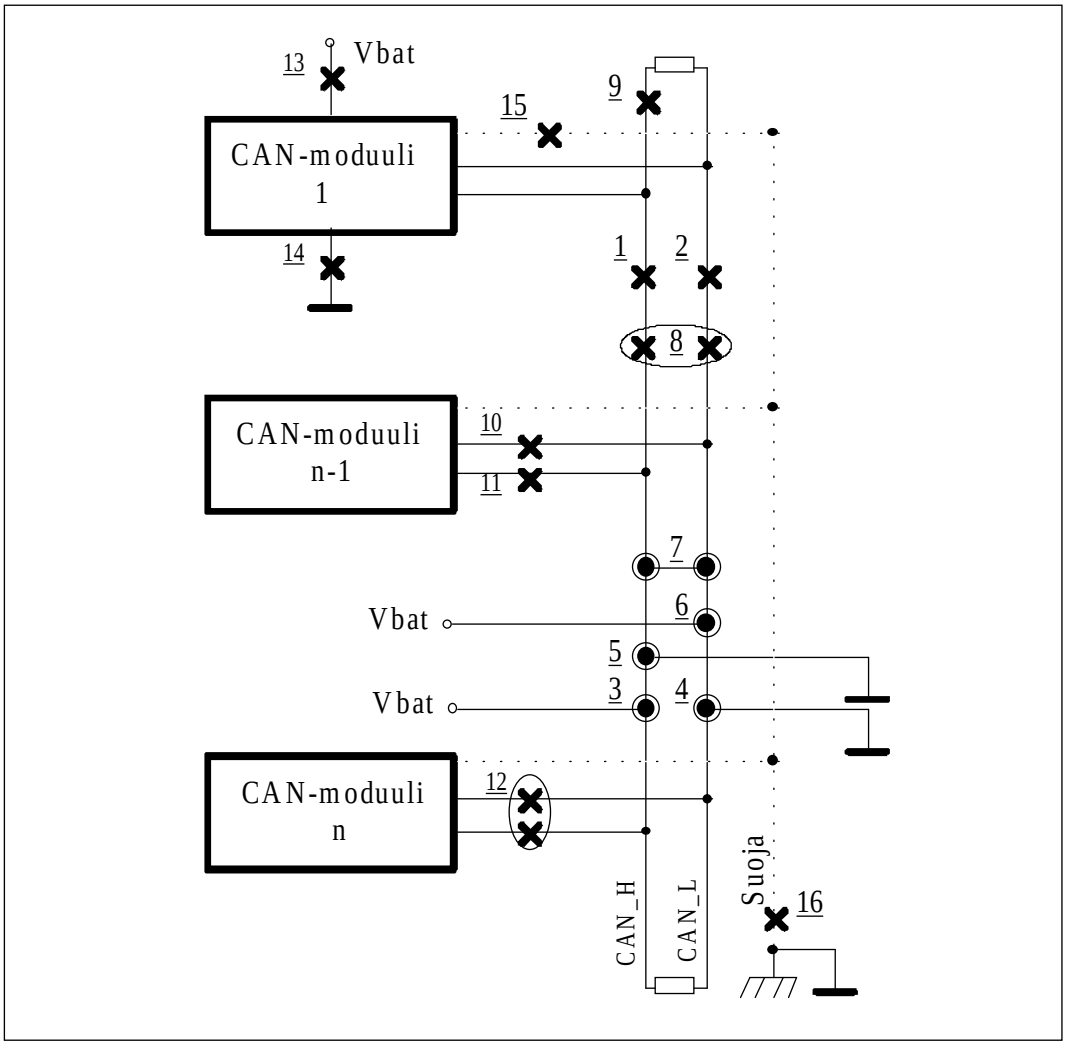
3.2.1 Fyysinen kerros

Kommunikointijärjestelmän vioista tyypillisimpiä ovat **kaapeli- ja liitinviat**. Väyläkaapelissa kulkee CAN-väylän tapauksessa vähintään kaksi johdinta, jotka ovat suurilla siirtonopeuksilla (> 125 kbit/s) kierrettynä parina, mutta joita voidaan matalilla siirtonopeuksilla käyttää myös rinnakkain kulkevina johtimina. Jos halutaan suojautua erityisen hyvin sähkömagneettisia häiriöitä vastaan, kierretty pari voidaan suojata suojavaipalla. Joskus väyläkaapelissa halutaan välittää myös käyttöjännitteet CAN-moduuleille. Pitkillä etäisyyksillä (esimerkiksi >200 m) CAN-väylä kannattaa erottaa galvaanisesti muusta järjestelmästä. Tällöin väylä-

kaapelissa kulkee edellä mainittujen johtimien lisäksi CAN-väylän käyttöjännitteet.

Kuvassa 5 on esitetty ISOn CAN-standardin (ISO 11898) esittämät väylän fyysiset vikatilanteet tapauksessa, jossa väyläkaapelissa on ainoastaan CAN-signaalijohtimet ja suojavaippa. Vikojen selitykset ovat taulukossa 4. Vikaa numero 16 ei varsinaisesti ole ISOn standardissa, mutta kyseinen vikatilanne poikkeaa viasta 15, jos suojavaippa on maadoitettu yhdestä pisteestä.

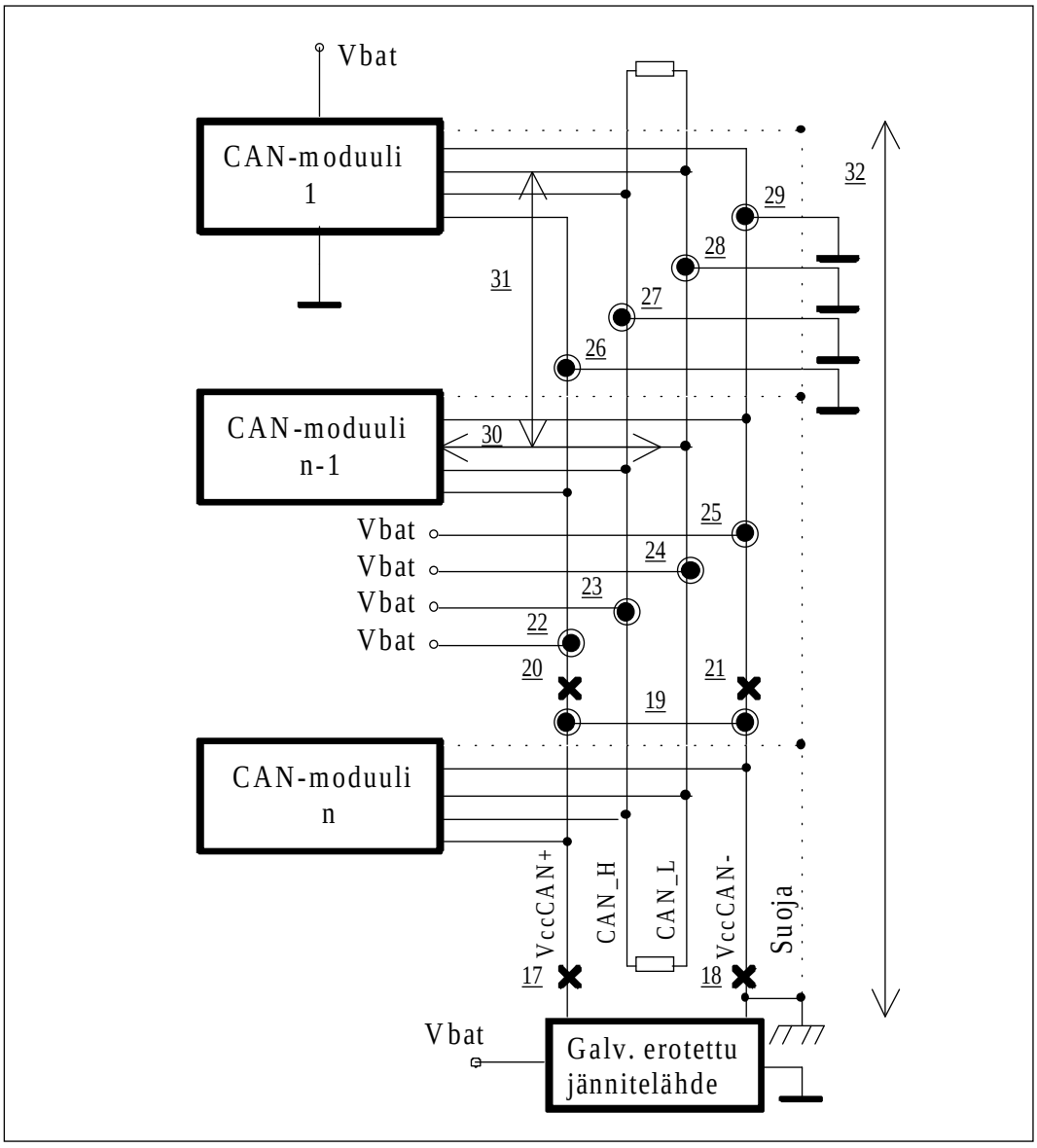
Kuvassa 6 ovat vastaavasti ne uudet vikatilanteet, jotka aiheutuvat käytettäessä optoerotettua CAN-väylää. Mukana ovat myös topologiavirheet. Vikojen selitykset ovat taulukossa 5. Näitä vikatilanteita ei ole ISOn standardissa. Siksi taulukossa ei ole suosituksia, miten vikatilanteissa pitäisi toimia.



Kuva 5. ISO-standardin (ISO 11898) mukaiset CAN-väyläkaapelin vikatilanteet.

Taulukko D. ISO 11898 -standardin vikamuodot fyysiselle CAN-väylälle.

VIKATYYPPI	SUOSITELTU TOIMINTA VIKA-TILANTEESSA	VAATIMUSTASO
Yksi solmu irtoaa väylältä. (10, 11, 12)	Jäljelle jääneet solmut jatkavat kommunikointia.	Suositellaan.
Yhden solmun käyttöjännite katkeaa. (13)	Jäljelle jääneet solmut jatkavat kommunikointia huonontuneella signaali-kohinasuhteella.	Suositellaan.
Yhden solmun maadoitus häviää. (14)	Jäljelle jääneet solmut jatkavat kommunikointia huonontuneella signaali-kohinasuhteella.	Suositellaan.
Yhteys suojavaippaan katkeaa millä tahansa solmulla. (15)	Kaikki solmut jatkavat kommunikointia.	Suositellaan.
Katkokset ja oikosulut		
1 CAN_H-johdin poikki.		
2 CAN_L-johdin poikki.		
3 CAN_H oikosulussa käyttöjännitteeseen.	Kaikki solmut jatkavat kommunikointia huonontuneella signaali-kohinasuhteella.	Suositellaan.
4 CAN_L oikosulussa maahan.		
5 CAN_H oikosulussa maahan.		
6 CAN_L oikosulussa käyttöjännitteeseen.		
7 CAN_H ja CAN_L-johtimet oikosulussa keskenään.	Kaikki solmut jatkavat kommunikointia huonontuneella signaali-kohinasuhteella.	Optio.
8 CAN_H ja CAN_L molemmat poikki samasta kohdasta.	Järjestelmä ei toimi kokonaisuudessaan. Syntyneistä kahdesta osajärjestelmästä se, jonka puolella on päätevastuskytkentä, jatkaa kommunikointia.	Suositellaan.
9 Päätevastuskytkennän toinen pää irti.	Kaikki solmut jatkavat kommunikointia huonontuneella signaali-kohinasuhteella.	Suositellaan.

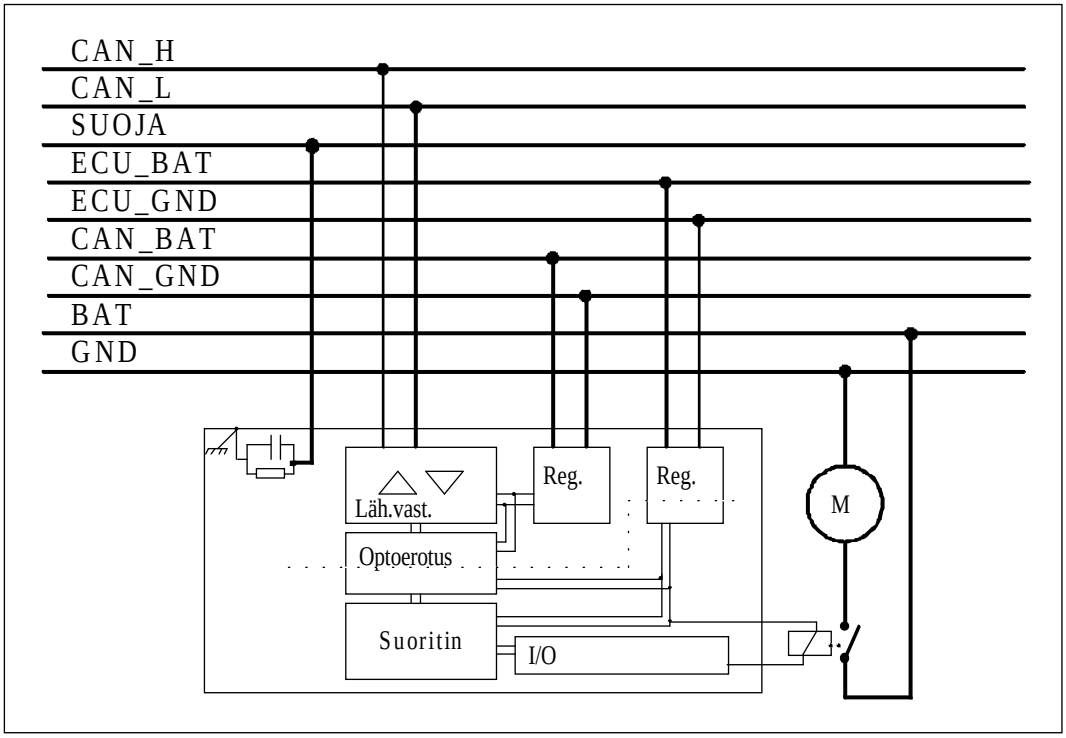


Kuva 6. Optoerotetusta CAN-väylästä aiheutuvat uudet vikatilanteet.

Taulukko E. Topologiavirheet ja optoerotuksesta aiheutuvat uudet vikatilanteet.

VIKA	KUVAUS	HUOM.!
17	CAN-jännitteiden plus-johdin katkeaa	
18	CAN-jännitteiden miinus-johdin katkeaa	
19	CAN-jännitteiden plus- ja miinus-johtimet oikosulussa keskenään	
20	CAN-jännitteiden plus-johdin katkeaa siten, että vain osa solmuista jää ilman CAN-jännitteitä	
21	CAN-jännitteiden miinus-johdin katkeaa siten, että vain osa solmuista jää ilman CAN-jännitteitä	
22	CAN-jännitteiden plus-johdin oikosulussa käyttöjännitteeseen	
23	CAN_H oikosulussa käyttöjännitteeseen	Tämä on eri tilanne kuin ISO 11898 -taulukon vastaava vikatilanne (3), koska CAN_H ja Vbat ovat tässä galvaanisesti erotettuja
24	CAN_L oikosulussa käyttöjännitteeseen	Tämä on eri tilanne kuin ISO 11898 -taulukon vastaava vikatilanne (6), koska CAN_L ja Vbat ovat tässä galvaanisesti erotettuja
25	CAN-jännitteiden miinus-johdin oikosulussa käyttöjännitteeseen	
26	CAN-jännitteiden plus-johdin oikosulussa maahan	
27	CAN_H oikosulussa maahan	Tämä on eri tilanne kuin ISO 11898 -taulukon vastaava vikatilanne (5), koska CAN_H ja Vbat ovat tässä galvaanisesti erotettuja
28	CAN_L oikosulussa maahan	Tämä on eri tilanne kuin ISO 11898 -taulukon vastaava vikatilanne (4), koska CAN_L ja Vbat ovat tässä galvaanisesti erotettuja
29	CAN-jännitteiden miinus-johdin oikosulussa maahan	
30	Haaran pituus liian suuri	Maks. 30 cm, kun siirtonopeus on 1 Mbit/s (ISO 11898)
31	Solmujen välinen etäisyys liian pieni	Min. 10 cm (ISO 11898)
32	Väylän kokonaispituus liian suuri	Maks. 40 m, kun siirtonopeus on 1 Mbit/s (ISO 11898)

Edellä todettiin, että väyläkaapeli voi sisältää myös käyttöjännitejohtimet CAN-moduulien tehonsyöttöä varten. Lisäksi voidaan varata toinen käyttöjännitejohdinpari erikseen laitteille, jotka eivät vaadi häiriötöntä sähköä tai jotka itse aiheuttavat häiriöitä, kuten moottorit (kuva 7). Kuvan 7 mukaista kaapelia ei tosin käytetä usein, mutta esimerkiksi maa- ja metsätalouskoneitten standardissa (ISO/CD 11783-2) tällaista kaapelia käytetään traktorin ja sen perään liitettävän työkoneen välissä. Tosin kyseisessä standardissa CAN_BAT- ja CAN_GND-johtimilla on eri merkitys kuin kuvassa 7; kyseisessä standardissa CAN_BAT- ja CAN_GND-johtimissa viedään käyttöjännitteet erityiselle päätekytkennälle, joka poikkeaa normaalista päätevastuskytkennästä.



Kuva 7. Eräs esimerkki väyläkaapelissa kulkevista johtimista.

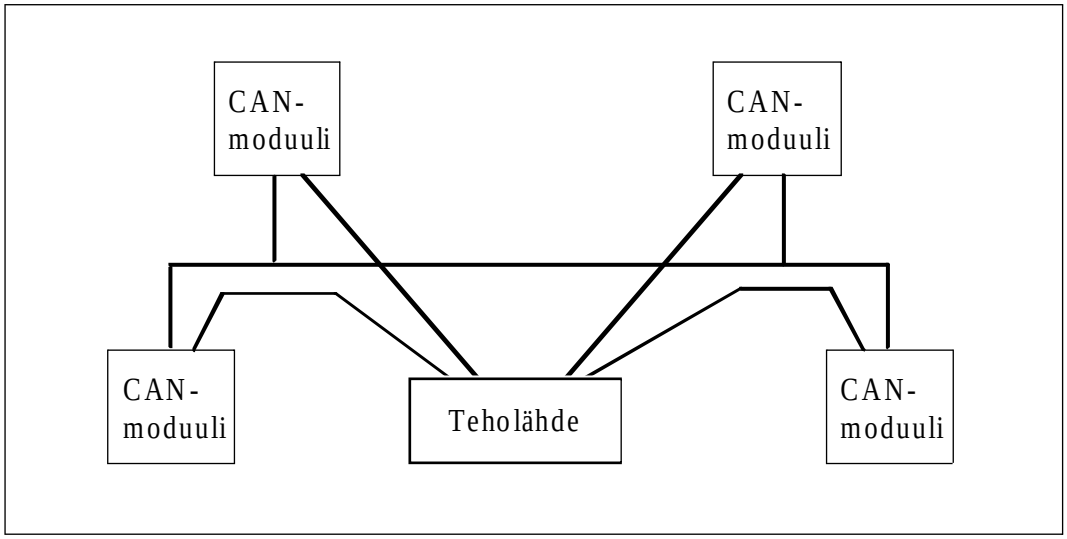
Huomaa, että BAT- ja GND- sekä ECU_BAT- ja EGU_GND-johtimet voivat tulla suoraan samalta jännitelähteeltä, esimerkiksi akulta, mutta koska ne tulevat omina johtiminaan, ECU_BAT/ECU_GND-johdinpari pysyy häiriöttömämpänä.

Tyypillinen konfiguraatio kuitenkin on, että väylällä on viisi johdinta: CAN_H, CAN_L, suoja ja moduulin käyttöjännitteet. Näin on esimerkiksi Allen Bradleyn DeviceNet-väylässä ja Honeywellin SDS-väylässä. DeviceNet-väylässä isoloidut jännitteet generoidaan paikallisesti moduulin sisällä, joten erillisiä johtimia optisesti erotettua CAN-väylää varten ei tarvita. Suojajohdin maadoitetaan yhdestä paikasta, ja jos mahdollista, keskeltä väylää. DeviceNet-spesifikaatiossa suojajohdin kytketään vastuksen ja kondensaattorin kautta moduulin metallikoteloon. Vastuksen arvo on 1 MΩ ja kondensaattorin 0.01 μF. Vastus ja kondensaattori on kytketty rinnan.

Väyläkaapelointiin voidaan lisätä erityinen johdin tai johtimia turvallisuusfunktioita varten. Näin on tehty esimerkiksi vammaisten apuvälineitten, erityisesti pyörätuolien, CAN-standardissa (M3S 1995). Kyseisessä standardissa väylällä kulkevat CAN-johtimien ja käyttöjännitejohtimien lisäksi key line- ja DMS line -johtimet. Key line -johtimen avulla kytketään tai katkaistaan kaikkien solmujen käyttöjännitteet. Sitä voidaan käyttää siten hätä-seis-linjana, koska sen avulla kaikki solmut voidaan sammuttaa varmasti ja yhtäaikaa. DMS line -johdin aktivoidaan, jos käyttäjä aktivoi erityisen kytkimen, jota kutsutaan kuolleenmiehenkytkimeksi. Ajomoottorit toimivat vain, jos DMS line -johdin on aktiivinen.

Kun käyttöjännitejohtimet kulkevat samassa kaapelissa ja samoissa liittimissä CAN-johtimien kanssa, todennäköisyys kuvien 3 ja 4 mukaisiin oikosulkuihin on suurempi tilanteessa, jossa käyttöjännitejohtimet kulkevat eri kaapelissa. Jos voidaan käyttää suojaamatonta parikaapelia, oikosulkujen mahdollisuus maapotentiaaliin vähenee entisestään, jolloin ainoastaan CAN-johtimien tai päätevastuksen katkokset tai CAN-johtimien keskinäiset oikosulut ovat todennäköisiä (vikamuodot 1, 2 ja 7 - 9 taulukossa 4). Toisaalta, jos suojajohdinta ei käytetä, CAN-kaapeloinnin EMC (electromagnetic compatibility) -ominaisuudet huononevat. Joissakin lähteissä, esimerkiksi McLaughlin (1993), todetaan kuitenkin, että pelkällä kierretyllä parikaapelilla ilman suojavaippaa saavutetaan riittävän hyvät EMC ominaisuudet. Tämä vaatii kuitenkin sitä, että pulssin nousuaikaa voidaan pidentää. Joissakin CAN-väylää varten tehdyissä lähetin-vastaanotinpiireissä on tällainen valmius. Yleisenä sääntönä voidaan todeta, että nousuajan kontrollointia kannattaa käyttää hyväksi, jos siirtonopeus sen sallii.

Jos käyttöjännitejohtimien ei tarvitse kulkea samassa kaapelissa CAN-johtimien kanssa, käyttöjännitteet voidaan johdottaa tähtimäisesti, jolloin katkos tai oikosulku yhdessä kohdassa ei lamauta koko järjestelmää (kuva 8).



Kuva 8. Tähtimäinen tehosyöttö.

Jos fyysisen väylän halutaan toimivan myös vikatilanteissa (viat 1 - 9 taulukossa 4), väyläkaapeloinnissa täytyy olla jonkin asteista redundanssia, esimerkiksi **kahdennetut kaapelit, liittimet ja lähetin-vastaanottimet**. Kahdennetusta väylästä

saadaan täysi hyöty vain, jos väylät johdotetaan eri reittiä. Tällöin varmistetaan, ettei pienelle alueelle kohdistunut mekaaninen isku riko molempia väyläkaapeleita yhtä aikaa. Kahdennetun väylän ongelmana ovat suuremmat kustannukset, varsinkin jos kaapelointi liittimineen on muutenkin suuri kustannustekijä. Periaatteessa normaalitapauksessakin, eli pelkässä CAN-parikaapelissa, on redundanssia; jos toinen parikaapelin johtimista katkeaa tai oikosulkeutuu joko käyttöjännitteeseen tai maapotentiaaliin, liikennöintiä voidaan jatkaa ainoastaan yhdellä johtimella. Tämän toteuttamiseksi vaaditaan erityinen lähetin-vastaanotinkytkentä. Tällaisesta lähetin-vastaanotinkytkennästä on esimerkki lähteessä Tanaka et al. (1991). Kytkentä perustuu suojajohtimen käyttöön vertailutasona. Kytkentä on suhteellisen monimutkainen verrattuna yksinkertaisiin lähetin-vastaanotin-piireihin ja päätevastuksenkin paikalla on kytkentä, jossa on neljä transistoria ja seitsemän muuta komponenttia. Ehkä tästä syystä tämäntyyppisiä kytkentöjä ei ole juurikaan käytännössä näkynyt.

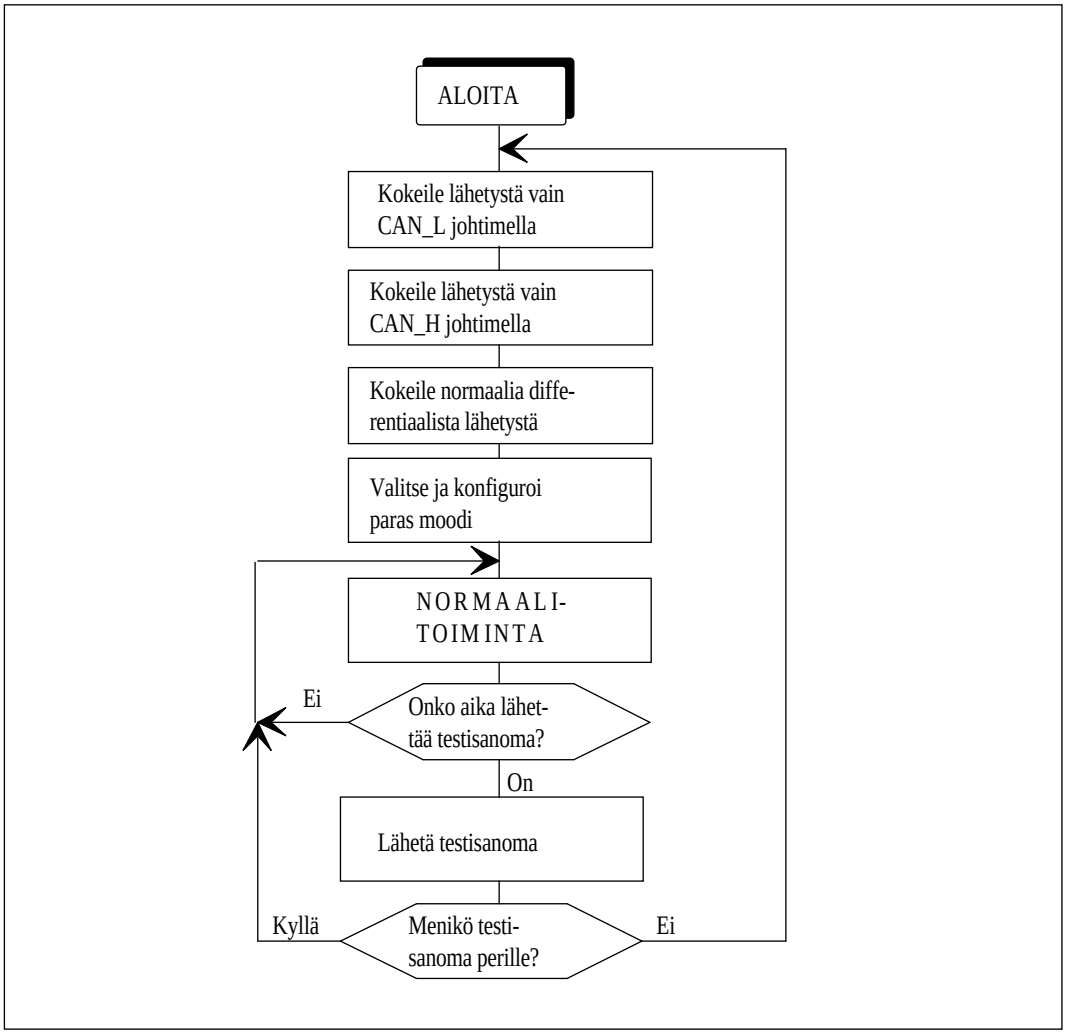
Toinen tapa on käyttää solmun sisäistä referenssijännitettä korvaamaan viallinen väyläjohdin. Suojavaippaa ei siis tarvita. Tällöin vaaditaan, että lähetin-vastaanotinkytkentä kykenee irrottamaan protokollapiirin CAN-johtimen väylältä ja liittämään sen referenssijännitteeseen. Lähteessä Pehrs (1992) on kuvaus tällaisesta menetelmästä (perustuu 8xC592-piirin sisäisen lähetin-vastaanottimen hyväksikäyttöön). Fyysinen kerros voidaan Pehrsin (1992) mukaan suunnitella siten, että se toipuu automaattisesti katkoksista, jolloin ainoastaan oikosulut tarvitsee havaita ohjelmallisesti. Tällöin riittää, että väylällä on vikavalvoja, joka lähettää testisanomia solmuille sopivin välein. Testisanomaa on käytettävä, koska protokollapiiri ei välttämättä anna luotettavaa vikatietoa väyläviasta; esimerkiksi jos väylä on juuttunut dominanttiin tilaan ja on siinä tilassa, kun solmut käynnistetään, jokainen solmu luulee, että väylä on varattu. Ne eivät tällöin yritä lähettää väylälle mitään eivätkä siten generoi virhetietoa. Testisanoma sisältää tiedon, milloin seuraava testisanoma on tulossa. Jos testisanoma ei mene perille, kaikki solmut käynnistävät väylätestin, jossa kokeillaan kaikki kolme väylän konfiguraatiomahdollisuutta (kuva 9). Koska tässä menetelmässä käytetään paikallisia referenssijännitteitä vioittuneen johtimen korvaamiseen, solmujen maapotentiaalien välillä ei saa olla suuria eroja. Tällaisen menetelmän ongelma on pitkä vasteaika vian esiintymisestä sen havaitsemiseen.

CAN-väylään on saatavissa Temic-yhtiöltä lähetin-vastaanotinpiiri (B10011S), joka kykenee kommunikointiin yhdellä johtimella, mutta signaalitasot eivät ole ISO 11898 -standardin mukaiset, vaan ne noudattavat ISO/CD 11992-1[2] -standardiluonnosta.

Kahdennetun väylän käyttö on hyvin harvinaista, eikä tämän tutkimuksen yhteydessä löydetty yhtään kytkentää tai ohjetta, kuinka kahdennettu CAN-väylä pitäisi toteuttaa (paitsi optisena väylänä). Kenttäväylien puolella tilanne on asiantuntijoiden mukaan sama, eli väylää yksistään ei kovin herkästi kahdenneta. Syynä tähän

[2] ISO/CD 11992-1. Electrical connections between commercial vehicles and trailers equipped with 24 V systems. Interchange of digital information. Part 1. Physical layer and data link layer.

on, että itse väylän on todettu olevan niin paljon kenttälaitteita luotettavampi, että kahdennus aloitetaan kenttälaitteista tai koko ohjausjärjestelmä kahdennetaan (esim. voimalaitoksissa). Teollisuusautomaatiossa väyläkaapelointi ei joudu niin kovaan rasitukseen kuin koneautomaation sovelluksissa, kuten metsäkoneissa, kaivoskoneissa ja traktoreissa. Siten tarve väyläkaapelin kahdennukseen on koneautomaatiossa suurempi kuin teollisuusautomaatiossa, mutta toisaalta koneautomaatio on usein kustannuskriittisempää, joten kahdennuksia ei koneautomaatiossakaan herkästi käytetä.



Kuva I. Toipumis-algoritmi tapauksessa, jossa on mahdollista kommunikoida yhdellä väyläjohtimella (Pehrs 1992).

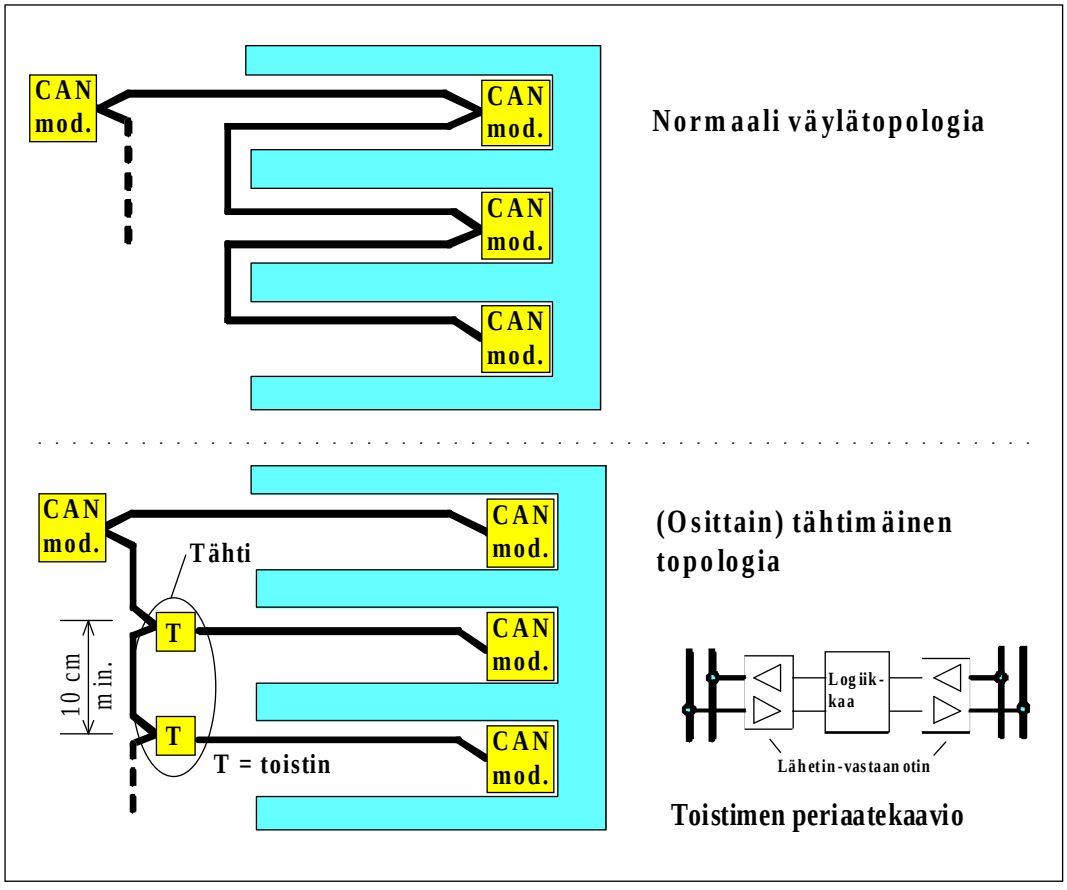
CAN-väylä voidaan toteuttaa myös **optisena väylänä**. Käytännöllisiä vaihtoehtoja ovat tähti- ja rengastopologiat. Tähtitopologiasta on esimerkki lähteessä Meuris et al. (1992) ja rengastopologiasta lähteessä Kuntz et al. (1993). Kuntz et al. esittelee rengastopologian, jossa on kahdennettu rengas. Toinen renkaista kiertää vastakkaiseen suuntaan. Erityisellä lähetin-vastaanotinkytkennällä tällainen väylä toipuu yksittäisestä viasta ja joistakin yhtäaikaisista vioista. Itse optinen väyläsegmentti

on tunteeton sähkömagneettisille häiriöille, mutta lähetin-vastaanotin, jossa sähkö muutetaan valoksi ja päinvastoin, on altis häiriöille tai generoi itse häiriöitä.

Optisilla väylillä vikamuodot ovat:

- lähetin-vastaanotin menee rikki (pysyvästi valo päällä tai pysyvästi pimeä)
- optinen väyläsegmentti vioittuu (esim. katkeaa)
- solmulta katkeavat jännitteet, jolloin solmu ei toista signaalia (rengastopologiassa)
- tähti vioittuu (tähtitopologiassa; erityisesti aktiivinen tähti).

ISO 11898 -standardi vaatii, että **väylätopologian** tulisi vastata mahdollisimman hyvin tilannetta, jossa väylä kiertää jokaisen solmun kautta, eli pitkiä haaroja väylältä solmulle ei heijastusvaikutusten takia sallita. Järjestelmän haavoittuvuuden kannalta tähtitopologia olisi parempi, varsinkin jos tähtipiste osaisi eristää oikosulkeutuneen haaran muusta väylästä. Tyhmempikin tähtipiste takaa sen, että katkos yhdessä haarassa ei estä muiden solmujen välistä liikennettä. Tähtitopologia voidaan toteuttaa toistimilla (kuva 10) tai hyvin mitoitetulla verkolla.



Kuva 10. Normaalin ja tähtimäisen topologian erot.

Vaikka toistin periaatteessa lyhentää väylän enimmäispituutta aiheuttamansa lisäviiveen takia, tietyissä tapauksissa kaapeloinnin enimmäispituus kasvaa. Kuvan 10 esimerkki on juuri tällainen tapaus; katkoviivalla merkitty osuus CAN-kaapeloinnista voi olla pidempi toistimilla varustetussa topologiassa. Toistin on tosin uusi vikaantuva komponentti, joten kokonaisluotettavuuden parantuminen tähtitopologiassa riippuu toistimen vikatiheydestä.

Topologian vaikutusta väyläsignaalin vääristymiseen voidaan kompensoida valitsemalla **sopivat siirtoparametrit** (mm. näytteenottohetki, näytteiden määrä bittiä kohden, synkronointi joko vain toisella tai molemmilla pulssin reunoilla). Siirtoparametrit voidaan asettaa ohjelmallisesti yleisimmillä CAN-protokollapiireillä, mutta esimerkiksi Philipsin 82C150 CAN-SLIO (Serially Linked I/O) -piirillä siirtoparametrit ovat kiinteät; ainoastaan siirtonopeutta voidaan muuttaa. Huolellinen siirtoparametrien viritys on tärkeää, kun halutaan minimoida bittivirheet. Tähän motivoi seuraava CAN-protokollan ominaisuus: **sanoma voi kahdentua ilman, että vastaanottaja sitä huomaa**. Kahdentuminen voi sattua kahdessa eri tapauksessa:

- Kehyksen viimeinen bitti vääristyy (resessiivisestä dominantiksi); tällöin CAN-spesifikaation mukaan vastaanottaja kuitenkin hyväksyy sanoman, kun taas lähettäjä tulkitsee viimeisen bitin vääristymisen viaksi ja lähettää sanoman uudelleen; vastaanottaja saa siten sanoman kahteen kertaan.

- Vastaanottajien lähettämä kuittausbitti viivästyy liiaksi, jolloin lähettäjä luulee, että yksikään solmu ei saanut sanomaa, ja lähettää sen uudelleen; vastaanottajat hyväksyvät molemmat sanomat.

Näistä edellinen on CAN-spesifikaation ominaisuus eikä sitä vastaan ole muita keinoja kuin pyrkiä vähentämään bittivirheiden mahdollisuutta ja suunnitella järjestelmä sellaiseksi, että sanoman kahdentumisesta ei ole haittaa. Jälkimmäinen tilanne johtuu liian pitkistä kaapeleista siirtonopeuteen nähden tai huonosti valituista siirtoparametreista tai optoerottimien aiheuttamasta lisäviiveestä.

Edellä on puhuttu väyläkaapelin vikamuodoista. Seuraavana tulevat **lähetin-vastaanotinelektroniikan viat**. Lähetin-vastaanotin voi vioittua siten, että solmu hiljenee väyläliikenteen kannalta täysin sallien muun liikenteen tai siten että solmu estää kaiken liikenteen väylällä. Jälkimmäinen vikamuoto tarkoittaa CAN-väylän tapauksessa yleensä sitä, että lähetin-vastaanotin on juuttunut dominanttiin tilaan, vaikka se voi periaatteessa juuttua myös resessiiviseen tilaan. Optoerotus on tehtävä siten, että solmu lähettää dominantin bitin silloin, kun optoerottimen sisäinen LED-valo on syttyneenä. Muutoin käy niin, että jos prosessorin puoleiset käyttöjännitteet sammuvat, esimerkiksi regulaattorin rikkoutumisen takia, solmu jää dominanttiin tilaan ja estää siten väyläliikenteen. Lähetin-vastaanottimia saa ISO 11898 -standardin (ISO High Speed) mukaiseen väylään valmiina integroituina piireinä. Ne on yleensä suunniteltu siten, että niiden CAN_L- ja CAN_H-johtimet kestävät oikosulut 12 V:n ajoneuvojärjestelmissä ($\Rightarrow$ maks. Vcc = 16 V). Niistä on tulossa myös versioita, jotka kestävät oikosulut myös 24 V:n järjestelmissä ($\Rightarrow$ maks. Vcc = 32 V). 24 V:n piireillä tosin maksimi siirtonopeus on toistaiseksi

500 kbit/s. Kummassakaan tapauksessa kommunikointi ei ole mahdollista oikosulun sattuessa, mutta piiri ei kuitenkaan oikosulusta rikkoonnu.

3.2.2 Siirtoyhteyskerros

Siirtoyhteyskerrokseen luetaan tässä protokollapiiri ja sitä ohjaava laiteajuri, joka on toteutettu ohjelmistolla. **Protokollapiirin viat** ovat harvinaisia. Protokollapiirin vika tai erityisesti **kommunikointiohjelmiston huono toteutus** voi aiheuttaa sanoman hukkumisen. Vika protokollapiirissä tai kommunikointiohjelmistossa voi myös aiheuttaa virhetilanteen, jossa solmu lähettää villisti jotakin sanomaa väylälle. Tällainen virhetilanne voi johtua myös sovellusohjelman viasta siinä tapauksessa, että kommunikointiohjelmisto hyväksyy kaikki sovellukselta tulevat lähetyspyynnöt ilman rajoituksia eli kommunikointiohjelmisto ei aseta vähimmäisaikavaatimusta saman sanoman perättäisten lähetyspyyntöjen väliajalle.

Varsinainen CAN-protokolla on varsin luotettava. Protokollapiiri tekee automaattisesti seuraavat tarkistukset:

- lähettävän solmun tekemät tarkistukset

  - onko väylällä se bitti, joka sinne on kirjoitettu
  - onko kuittausbitti dominantti

- vastaanottavan solmun tekemät tarkistukset

  - CRC-tarkistus (Cyclic Redundancy Check)
  - stuff-säännön rikkominen, eli ei pitäisi olla enempää kuin 5 samanlaista bittiä peräkkäin

- sekä lähettävät että vastaanottavat solmut tarkistavat

  - ovatko sanomakehykseen kuuluvat kiinteät bitit oikeat.

Nämä tarkistukset takaavat, että

- kaikki globaalit virheet havaitaan
- kaikki paikalliset viat lähettäjissä havaitaan
- satunnaiset bittivirheet sanomassa havaitaan, jos niitä on enintään 5
- peräkkäiset bittivirheet sanomassa havaitaan, jos niitä on enintään 15
- jos bittivirheitten lukumäärä sanomassa on pariton, ne havaitaan.

Jäännösvirhetodennäköisyys on pienempi kuin $p_{error} \times 4{,}7 \times 10^{-11}$ (CAN Specification, version 2.0. 1991), jossa p_{error} on sanoman virhetodennäköisyys. Kenttäväylästandardi IEC 1158-2 vaatii, että tietyissä häiriöolosuhteissa jäännösvirheiden lukumäärä 20 vuodessa on pienempi kuin yksi. Jos p_{error} on 10^{-3}, jäännösvirhetodennäköisyys on pienempi kuin $4{,}7 \times 10^{-14}$. Jotta virheiden lukumäärä

20 vuodessa olisi keskimäärin pienempi kuin yksi, tänä aikana saa tulla $1 / 4{,}7 \times 10^{-14}$ sanomaa, eli $2{,}1 \times 10^{13}$ sanomaa, eli noin 34 000 sanomaa sekunnissa, jos kone käy yötä päivää. Tällaisiin sanomanopeuksiin ei CAN-väylällä ole edes mahdollista päästä, sillä teoreettinen maksimi väyläkuormitukselle on 1 sanoma / 47 μs ≈ 21 000 sanomaa / s. Jos p_{error} olisi 10^{-2} eli 1 %, sanomanopeus voisi olla noin 3 400 / s, mikä on sekin vielä suurehko nopeus, ja kun oletuksena oli, että kone käy yötä päivää 20 vuotta, voidaan johtopäätöksenä todeta, että on (huomattavasti) todennäköisempää, että koneeseen tulee jokin muu vika kuin CAN-sanoman vääristyminen niin, ettei sitä havaita ja korjata. Artikkelissa Unruh et al. (1990) on analysoitu jäännösvirhetodennäköisyyden vaikutusta henkilöautoissa. Laskelmissa on käytetty seuraavia parametriarvoja:

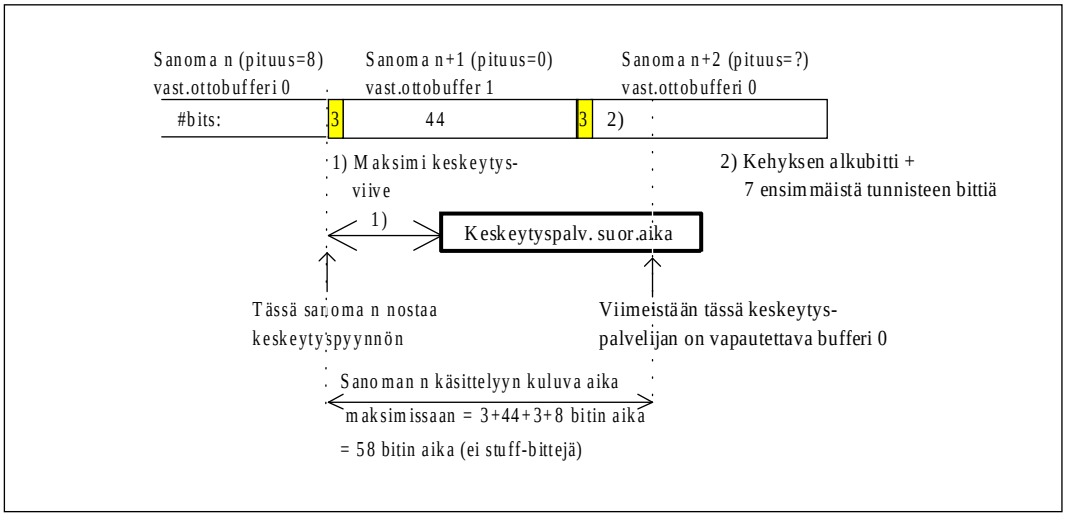
- ajoneuvon elinikä: 4 000 h
- väylän siirtonopeus: 1 Mbit/s
- väyläkuormitus: 30 %
- sanoman pituus keskimäärin: 90 bittiä.

Tällöin havaitsematta jäävien virheiden lukumääräksi auton eliniän aikana on laskettu **$4{,}1 \times 10^{-3}$**, kun p_{error} on arvioitu olevan 10^{-3}. (Tässä jäännösvirhetodennäköisyydelle on käytetty eri approksimaatiota kuin edellä, so. $p_{error} \times 8{,}5 \times 10^{-11}$.)

Solmu on normaalisti ns. aktiivisessa virhetilassa, jolloin se virheen havaittuaan lähettää väylälle kuusi dominoivaa bittiä. Kuusi dominoivaa bittiä rikkoo bit-stuff-säännön. Tällöin kaikki solmut hylkäävät sanoman ja lähettävä solmu lähettää kyseisen sanoman uudelleen. Protokollapiireillä on virhelaskurit sekä lähetysvirheille että vastaanottovirheille. Solmu, jonka lähetysvirheiden lukumäärä saavuttaa arvon 256, poistuu automaattisesti väylältä, jolloin se ei häiritse muuta liikennettä. Sitä ennen se siirtyy ns. passiiviseen virhetilaan, jossa virhekehyksessä ei enää lähetetä dominantteja bittejä vaan ainoastaan resessiivisiä bittejä. Täten passiivisessa virhetilassa oleva solmu ei enää estä muiden solmujen välistä liikennettä, mutta se yrittää silti lähettää ja vastaanottaa sanomia. Passiiviseen virhetilaan siirrytään, jos lähetys- tai vastaanottovirhelaskuri saavuttaa arvon 128. Esimerkiksi protokollapiiri 82C200 antaa varoituksen, jos jompi kumpi virhelaskureista ylittää arvon 96, ja väylältä poistumisilmoituksen (bus off), kun lähetysvirheiden laskuri ylittää arvon 255. Samoin annetaan ilmoitus, jos protokollapiiri menettää sanoman tilanteessa, jossa sen molemmat vastaanottotietovarastot ovat varattuina. Tällaiset vikailmoitukset kannattaa tallentaa vikalokiin. Bus off -vikatilanteesta kannattaa ilmoittaa myös käyttäjälle, että käyttäjä tarkistaisi CAN-kaapeloinnin. Bus off -vikatilanteesta voidaan yrittää toipua myös automaattisesti alustamalla CAN-piiri uudestaan.

Edellä kuvattu tarkistus- ja uudelleenlähetysmenettely takaa sen, että jos lähettäjä saa lähetettyä sanoman, jokin vastaanottavista solmuista on saanut sanoman oikein eikä kukaan ole saanut sitä virheellisenä. Jos jokin vastaanottavista solmuista ei ole saanut sanomaa laisinkaan, esimerkiksi liittimen irtoamisen takia, tällaista virhetilannetta ei CAN-protokolla havaitse. Siksi yleensä käytetään lisänä solmuvalvontaprotokollaa, esimerkiksi siten, että järjestelmässä on yksi isäntä, joka tarkistaa vuorotellen testisanoman avulla, ovatko kaikki solmut vielä väylällä.

Solmu voi hukata sille relevantin sanoman, jos sen CAN-keskeytyspalvelija on liian hidas lukemaan sanomia pois protokollapiirin vastaanottotietovarastosta. Tämä pätee, jos käytetään BasicCAN-protokollapiiriä eli piiriä, jossa ei ole kaksiporttimuistia sanomien tallettamiseen, tai jos käytetään kaksiporttimuistillisen protokollapiirin (FullCAN-piiri) BasicCAN-ominaisuutta. Kriittisin tilanne on, jos solmulle tulee peräkkäin kolme sille relevanttia sanomaa, joista ensimmäisen tietokentän pituus on kahdeksan tavua[3] ja seuraavan nolla tavua. Kolmannen tavumäärällä ei ole merkitystä. Kuvassa 11 on analysoitu tätä tilannetta.



Kuva 11. Vastaanottokeskeytyspalvelijan kannalta kriittisin tilanne.

BasicCAN-tyyppisessä vastaanotossa väylällä oleva sanoma talletetaan vuorotellen vastaanottobufferiin 0 tai 1. Täten kaksi peräkkäistä sanomaa saadaan varmasti talteen, mutta kolmas sanoma tarvitsee jälleen bufferia 0, joten se on vapautettava, ennen kuin kolmannen sanoman tunnistekentän ensimmäinen tavu on valmis talletettavaksi bufferiin 0. Kuvasta 11 nähdään, että aikaa bufferin vapautukseen ensimmäisen sanoman aiheuttamasta keskeytyksestä ko. hetkeen on 58 x bitin pituus. 1 Mbit/s siirto-nopeudella ajaksi tulee 58 µs. Tähän aikaan sisältyy keskeytysviive ja keskeytyspalvelijan ajasta alkuosuus vastaanottobufferin vapauttamiseen saakka. Jos keskeytyspalvelija käsittelee yhden sanoman kerrallaan, keskeytysviiveeseen on laskettava myös keskeytyspalvelijan loppuosuus. Tällöin kokonaisaika on keskeytysvaste[4] + keskeytyspalvelijan suoritusaika. Kokonaisaika saa siis olla korkeintaan 58 x bitin pituus. Keskeytysvaste riippuu olennaisesti muista keskeytyksistä ja niiden priorisoinnista. Vaikka CAN-keskeytykselle annettaisiin korkein prioriteetti, se ei takaa lyhyttä keskeytysvastetta, jos matalamman prioriteetin keskeytys pitää keskeytyksiä kiellettynä, kunnes se saa tehtävän-

[3] Tässä oletetaan, että keskeytyspalvelijalla kuluu eniten aikaa kahdeksan tavun mittaisen sanoman käsittelyyn, koska kopioitavia tavuja on siinä tapauksessa eniten.

[4] Keskeytysvasteella tarkoitetaan tässä sitä vasteaikaa, jolla solmun prosessori reagoi CAN-keskeytykseen normaalitilanteessa, eli kun aikaisemmat CAN-keskeytykset on jo ehditty käsitellä.

sä tehtyä. Siksi on varmistauduttava, että muut keskeytyspalvelijat vapauttavat keskeytyskäsittelyn ajoissa.

Normaalisti keskeytyspalvelija kannattaa tehdä siten, että se käsittelee kaikki keskeytykset, ennen kuin se vapauttaa prosessorin suorittamaan muita tehtäviä. Keskeytyspalvelijan lohkokaavio olisi silloin esimerkiksi kuvan 12 kaltainen.

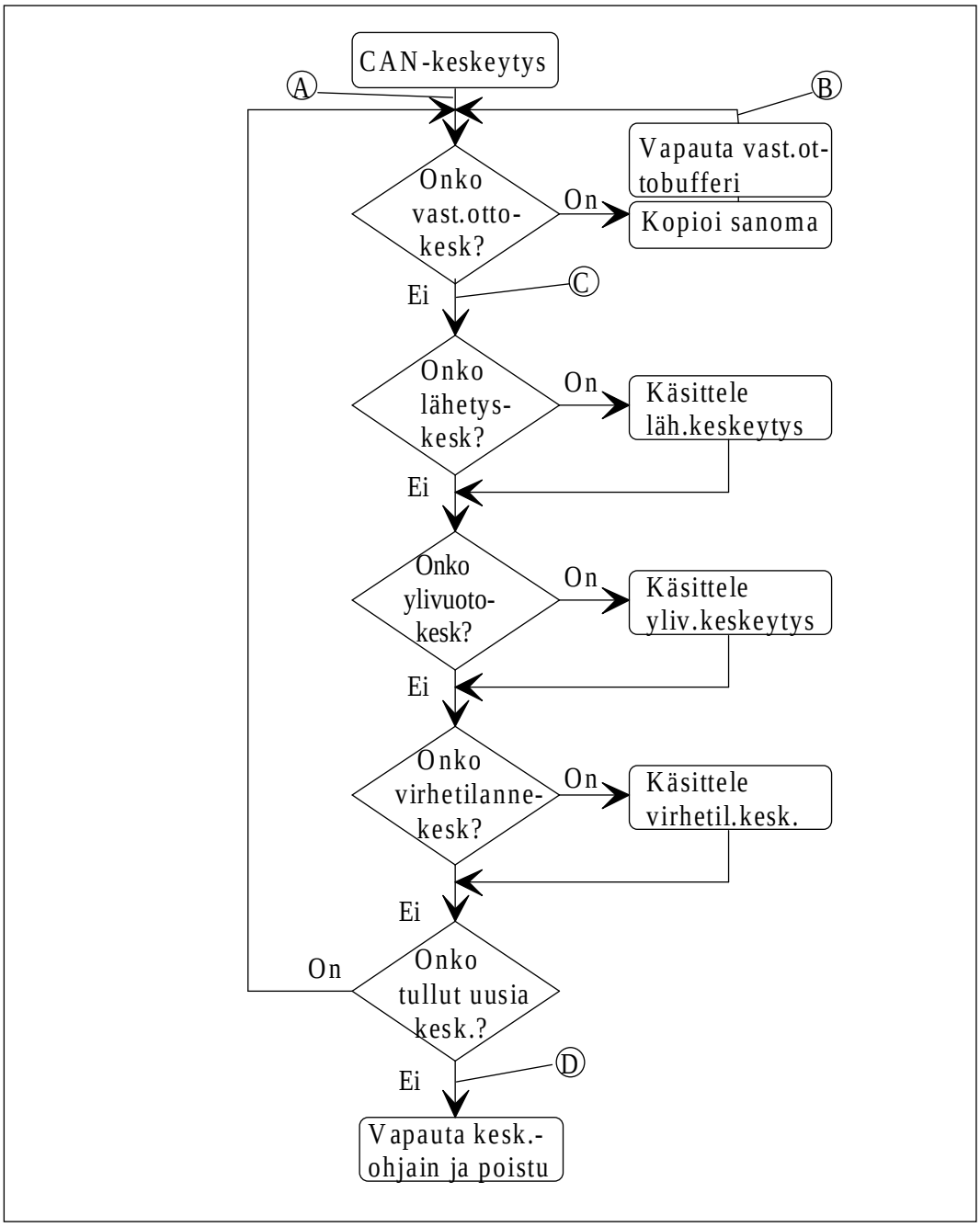
Kuvan 12 keskeytyspalvelijan periaate on, että jos uusi vastaanottokeskeytys ehtii tulla, kun edellistä vielä käsitellään, uusi vastaanottokeskeytys käsitellään heti, kun edellinen on käsitelty. Sen jälkeen tarkistetaan lähetys-, ylivuoto- ja virhetilannekeskeytykset. Kun ne on käsitelty, tarkistetaan jälleen, onko tänä aikana ehtinyt tulla uusia vastaanotto- tai muita keskeytyksiä. Jos on, käsitellään taas kaikki vastaanottokeskeytykset ensin ja sitten muut. Lähetys-, ylivuoto- ja virhetilannekeskeytysten käsittelyiden täytyy olla mahdollisimman lyhyitä, esimerkiksi lähetyskeskeytyspalvelijassa ei tehdä muuta, kuin vapautetaan lähetysrekisterin käytön estävä semafori. Ylivuoto- ja virhetilannekeskeytyspalvelijat voisivat esimerkiksi ainoastaan asettaa vikatilanteesta kertovan lipun tai kasvattaa virhetilannelaskuria. Virhetilannelaskurin arvo talletettaisiin sitten ylempien ohjelmistokerrosten toimesta vikalokiin.

Kuvan 12 mukaisen keskeytyspalvelijan suorituskyky analysoidaan seuraavasti:

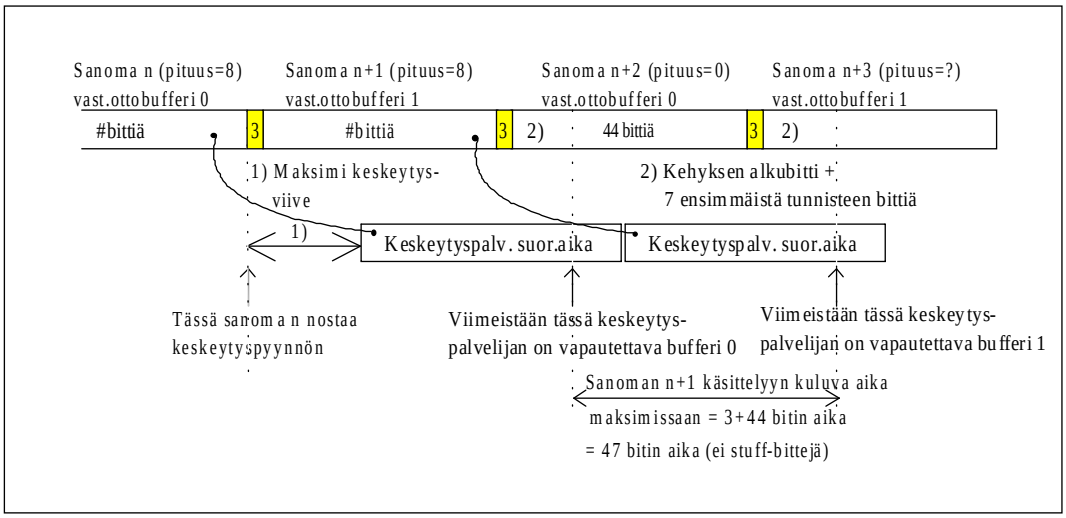
- Mittaa tai määritä keskeytysvaste eli aika keskeytyksen asetushetkestä kohtaan A; merkitään aikaa τ_I:llä.
- Mittaa tai määritä aika, joka kuluu keskeytyspalvelun alusta (kohdasta A) hetkeen, jolloin vastaanottobufferi vapautetaan (kohta B); merkitään aikaa τ_r:llä.
- Mittaa tai määritä ‘häntäaika’ eli aika, joka kuluu hetkestä, jolloin viimeinen keskeytysrekisterin tarkistus on tehty (kohta D), hetkeen, jolloin keskeytysohjain on vapautettu; merkitään aikaa τ_T:llä.
- Laske $\tau_A = \tau_i + \tau_r + \tau_T$.
- Mittaa tai määritä aika, joka kuluu hetkestä, jolloin havaitaan, ettei vastaanottokeskeytyksiä enää ole (kohta C), hetkeen, jolloin vastaanottobufferi vapautetaan (kohta B). Tämä aika vastaa tilannetta, jossa vastaanottokeskeytys tulee sinä aikana, kun muita keskeytyksiä käsitellään; merkitään aikaa τ_B:llä.
- Mittaa tai määritä aika, joka kuluu kahden perättäisen vastaanottobufferin vapautuksen välillä (kohdasta B kohtaan B) silloin, kun pyöritään sisemmässä silmukassa, eli kun uusi vastaanottokeskeytys ehtii tulla, ennen kuin edellinen kahdeksan tavun mittainen sanoma on ehditty käsitellä (tämä aika täytyy olla pienempi kuin 47 x bitin aika, ks. kuva 13); merkitään aikaa τ_C:llä.
- Maksimi siirtonopeus, jossa sanomia ei hukata, on silloin:

  $$b_{max} = \min (58 \times \tau_{bit} / \max (\tau_A, \tau_B), 47 \times \tau_{bit} / \tau_C),$$

  jossa τ_{bit} on yhden bitin aika ja b_{max} on maksimi siirtonopeus.

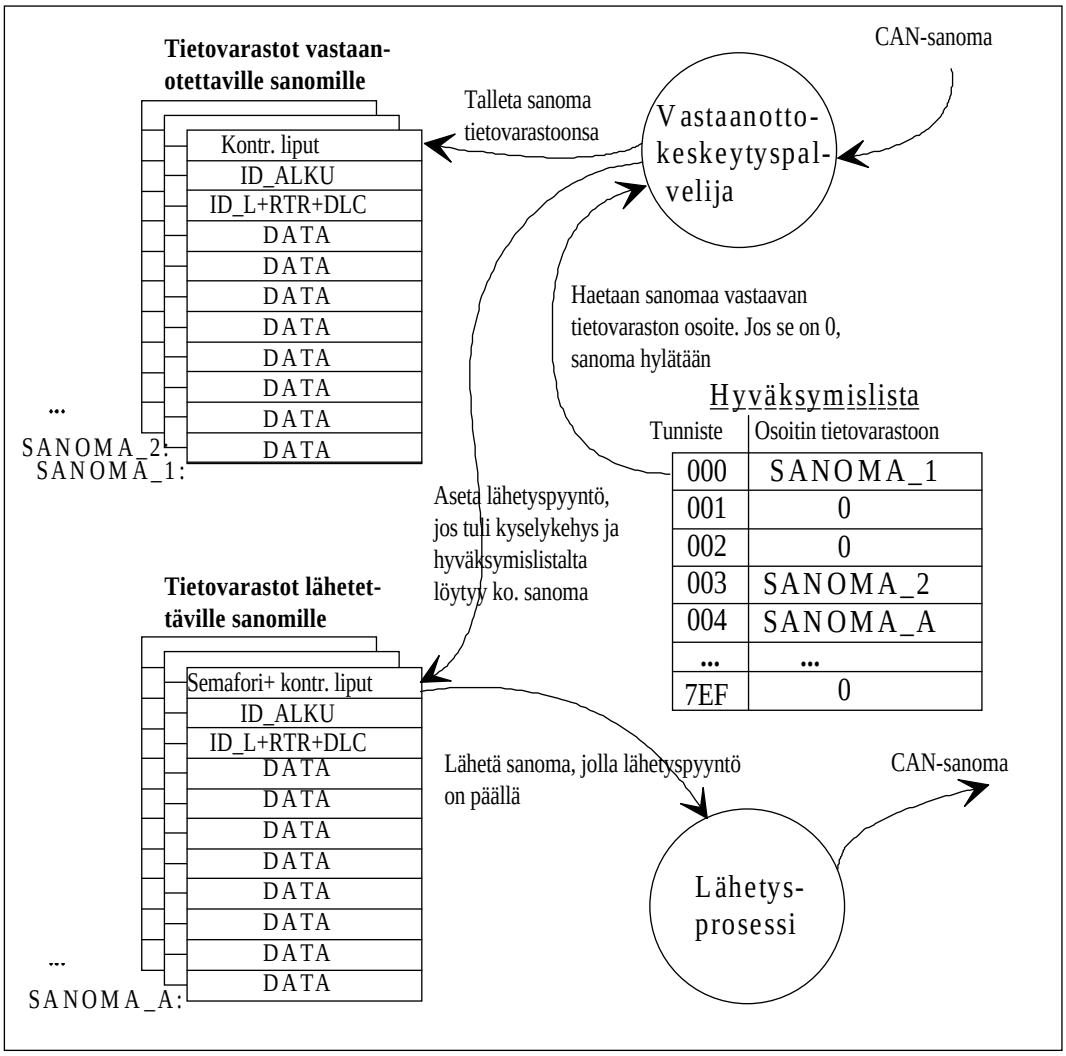


Kuva 12. CAN-keskeytyspalvelijan lohkokaavio.



Kuva 13. Keskeytyspalvelijan vastaanottosilmukan kierrosajan analyysi.

Keskeytyspalvelija siis tallettaa vastaanotetut sanomat muistiin. Talletus voi tapahtua jonoon tai sanomalle varattuun tietovarastoon (bufferiin). **Ennen talletusta kannattaa tarkistaa, että CAN-kehyksen tietokentän pituus -koodi (DLC) on pienempi tai yhtäsuuri kuin kahdeksan**. Jos näin ei tehdä ja DLC-koodia käytetään suoraan esimerkiksi kopiointisilmukan kierroslaskurina, tietovarasto korruptoituu, jos DLC-koodi on jostakin syystä suurempi kuin kahdeksan. Sanomien lähetys voi tapahtua myös jonosta tai sanomalle varatusta bufferista. Jonomaisen lähetyksen ongelma on se, että matalan prioriteetin sanoma estää korkeamman prioriteetin sanomia pääsemästä väyläkilpaan. Kuvassa 14 on esitetty tietovarastoja käyttävän vastaanoton ja lähetyksen periaate. Se vastaa kaksiporttimuistia käyttävien protokollapiirien (FullCAN-tyyppiset piirit) sanomakäsittelyn periaatetta. Vastaanotossa on huomioitava, että sovelluksen on tarkistettava, onko vastaanottokeskeytyspalvelija päivittänyt tietovaraston sisällön kesken lukemisen. Lukeminen on tehtävä tällöin uudestaan. Semaforia ei kannata käyttää, koska tällöin sovellus saattaa estää keskeytyspalvelijaa pääsemästä tietovarastoon epämääräisen pituisen ajan, jolloin aiemmin esitetty analyysi maksimisiirtonopeudelle ei enää päde. Lähetysprosessi lähettää tietovarastosta sanomat, joille on asetettu lähetyspyyntö joko sovelluksen toimesta tai kyselykehyksen vastaanoton yhteydessä. Lähetettävien sanomien tietovarasto on suojattava semaforilla, ettei sovellus pääse päivittämään tietovaraston sisältöä kesken lähetyksen. Lähetysprosessi ei ole CAN-keskeytyspalvelijan sisällä.



Kuva 14. Sanomakohtaisia tietovarastoja käyttävä vastaanotto- ja lähetysperiaate.

Kuvan 14 mukaisessa vastaanotossa tapahtuu ylivuoto, jos tietty sanoma tulee uudestaan, ennen kuin sen edellinen arvo on ehditty lukea. Tästä ei ole haittaa, jos halutaan tieto ainoastaan viimeisimmästä arvosta. Jonomaisessa lähetyksessä tapahtuu ylivuoto, jos lähetysprosessi ei ehdi tai pysty lähettämään sanomia riittävän nopeasti tai jos sanomia vastaanotetaan nopeammin, kuin sovellus ehtii niitä käsittelemään. Tällöin järjestelmä on mitoitettu väärin. Jotta tällaiset tilanteet paljastuisivat tuotekehitysvaiheessa (ja miksei kentälläkin), ylivuototilanteista kannattaa panna tieto vikalokiin.

Eri protokollapiireillä on erilaisia ominaisuuksia tai jopa virheitä, jotka täytyy ottaa huomioon. Esimerkiksi 82527-piirin globaali maskirekisteri, jonka pitäisi suodattaa vain vastaanotettuja sanomia, vaikuttaa myös lähetettäviin sanomiin. Tämä virhe korjattaneen jossakin myöhemmässä piirin versiossa. Kyseisellä piirillä on lisäksi se ominaisuus, että sanomat lähetetään kaksiporttimuistista siinä järjestyksessä, kuin ne on sinne konfiguroitu, eikä prioriteettijärjestyksessä. Ohjelmoijan on siis huolehdittava siitä, että sanomat konfiguroidaan piirille prioriteettijärjestyk-

seen. Käytettäessä BasicCAN-piiriä 82C200 tai FullCAN-piiriä 82526 on huomattava, että samassa verkossa ei voida käyttää RC-oskillaattoreita käyttäviä SLIO-piirejä (Serially Linked I/O), vaan SLIO-piirit on varustettava kideoskillaattoreilla. Tämä johtuu CAN-spesifikaation eri versioista: 82C200 käyttää spesifikaation versiota 1.1, 82526 versiota 1.0 ja SLIO-piirit versiota 2.0 (Anon. 1991). Versiota 1.1 myöhemmissä spesifikaatioissa (1.2 ja 2.0) protokollaa on muutettu siten, että se sallii 1,58 % kellotoleranssin bittien ajoituksessa. Aikaisemmin kellotoleranssi oli 0,5 %. Vanhoja protokollan versioita käyttävät piirit ovat täysin yhteensopivia myöhempien versioiden kanssa, jos kaikki protokollapiirit käyttävät kideoskillaattoria ja käytetään ainoastaan standardimuotoista sanomakehystä (l. tunnistekentän pituus on 11 bittiä).

FullCAN-tyyppisiä piirejä käytettäessä on varmistauduttava myös siitä, että kyselykehysten tietokentän pituus -koodi (DLC) on aina arvoltaan se, mikä FullCAN-piirille on konfiguroitu. Eri FullCAN-piirit saattavat reagoida eri tavalla virhetilanteeseen, jossa jokin solmu kysyy sanomaa eri pituuskoodilla, kuin mitä FullCAN-piiri olettaa sanoman pituudeksi.

BasicCAN-piirin 82C200 ongelma on se, että se ei pysty lähettämään sanomia täysin peräkkäin vaan jättää sen verran väliä, että matalamman prioriteetin sanoma joltakin muulta solmulta pääsee väliin. Täten esimerkiksi myöhemmin esiteltävä vasteaika-analyysi ei päde 82C200-piirille. Myös BasicCAN-piirejä käytettäessä täytyy varmistua siitä, että kaikilla solmuilla on yhtenevä tieto sanomien DLC-koodeista. Se, miten virhetilanteessa toimitaan, on ohjelmoijan itse päätettävissä, koska BasicCAN-piirit eivät itse vastaa kyselykehyksiin.

Piirien 87C592 ja 87CE598 (OTP/EPROM-versiot) DMA (Direct Memory Access) -siirtoa käytettäessä on huomioitava, että DMA:n käynnistyksen jälkeisen käskyn on käytettävä kaksi kellojaksoa, esimerkiksi:

```
        MOV     CANADR, #100xxxxxB  ; DMA:n käynnistys
        SJMP    DMAEND              ; kahden kellojakson käsky
DMAEND: ...
```

Jos DMA:n käynnistyksen jälkeen käytetään yhden kellojakson käskyä (esim. NOP-käskyä), yksittäiset tietotavut saattavat mennä vääriin muistipaikkoihin.

3.2.3 Ylemmät kerrokset

Varsinaisen CAN-protokollan päälle joudutaan usein lisäämään palveluita, joita CAN-spesifikaatiossa itsessään ei ole. Tällaisia palveluita ovat esimerkiksi lohkosiirto, ylemmän kerroksen kuittaukset, verkonhallintapalvelut ja sanomien ajoitus (skedulointi). Tässä yhteydessä myös sanomatunnisteiden jaon ajatellaan kuuluvan ylemmän kerroksen piiriin (tai sovelluksen piirin, jos järjestelmäsuunnittelija jakaa sanomatunnisteet käsin). **Turvallisuuden kannalta perusvaatimus on, että järjestelmässä ei saa olla kahta solmua, jotka lähettävät sanomia samalla sanomatunnisteella** (paitsi jos sanoman tietokentässä ei ole yhtäkään tavua).

Lohkosiirtoa ei tässä yhteydessä käsitellä tarkemmin. Ylemmän kerroksen kuittauksilla tarkoitetaan tässä sitä, että **vastaanotettu sanoma kuitataan toisella sanomalla** joko kommunikointiohjelmiston sisältä, kun sanoma on talletettu, tai sovelluksen toimesta, kun sovellus on lukenut tai käsitellyt sanoman. Kuittaukset lisäävät väyläkuormitusta, joten niitä ei kannata käyttää turhaan, vaan ehkä ainoastaan tilanteissa, joissa 'hätä seis' -tyyppisen (satunnaisen ja harvinaisen) sanoman perillemeno halutaan varmistaa. Periodisia sanomia ei kannata kuitata, koska se lisäisi väyläkuormitusta turhan paljon. Toinen tapa varmistua sanoman perillemenosta on lähettää sama sanoma useamman kerran peräkkäin (esimerkiksi) kolme kertaa). Tällaista tapaa käytetään CAN-standardissa (DIN 9684, Teil 3, 1993)[5], jonka sovellusalueena ovat traktorin perään liitettävät työkoneet. DIN 9684 -standardissa määritellään, että hätä seis -kytkimen painalluksen jälkeen väylälle on lähetettävä hätä seis -sanomaa (system stop) periodisesti 100 ms:n välein. Standardin mukaan jokaisen työkoneen on tällöin mentävä turvalliseen tilaan. Kun hätä seis -kytkin vapautetaan, väylälle lähetetään vapautussanoma viisi kertaa 100 ms:n välein. Standardissa on lisäksi määritelty hätä seis -sanoma yksittäiselle työkoneelle. Standardin luonnoksesta ei käy ilmi, täytyykö hätä seis -kytkin johdottaa vielä erikseen; yleensä näin vaaditaan.

Traktori ja sen perään liitettävä työkone on esimerkki tapauksesta, jossa edeltä päin ei voida tietää, mitä laitteita - ja siten CAN-solmuja - järjestelmässä tulee kulloinkin olemaan. Tällöin riittävän alhaista väyläkuormitusta ei voida etukäteen varmentaa. Tällöin **tarvitaan väyläkuormituksen valvontaa** ja palvelu, jolla solmujen lähetysperiodeihin voidaan vaikuttaa.

Verkonhallintapalveluista tärkeimmät ovat solmujen alustus (= kytkeminen verkkoon sisältäen mm. tunnisteiden jaon), käynnistys, pysäyttäminen, uudelleenkäynnistys (resetointi) sekä solmuvalvonta. Yleensä näitä palveluita varten verkon yksi solmuista määrätään olemaan verkonhallintaisäntä. Se ei siis ole isäntä varsinaisen kommunikoinnin tai sovelluksen kannalta. Ylemmän kerroksen palveluita käsitellään tarkemmin lähteessä Alanen & Virtanen (1994).

Kuten jo aikaisemmin kohdassa 3.2.2 todettiin, CAN-protokolla ei pysty havaitsemaan vikatilannetta, jossa yksi solmuista on kokonaan poistunut väylältä. Tällaiset vikatilanteet havaitaan **solmuvalvonnan** avulla. Väylältä poistumiseen voi olla syynä kaapelikatkos, liittimen irtoaminen, solmun rikkoutuminen (esim. lähetin-vastaanotin rikkoutuu), virtakatkos solmulla tai protokollapiirin kytkeytyminen irti väylältä sisäisen virhelaskurin ylitettyä raja-arvon. Solmuvalvonta voidaan tehdä siten, että jokin solmuista (esim. verkonhallintaisäntä) voidaan määrätä kiertokyselijäksi tai solmut voivat kysellä läsnäoloa solmuilta, jotka ovat niille relevantteja. Solmuvalvontaa ei tarvita, jos solmut lähettävät periodisia sanomia; jos sanomaa ei enää tule, solmun voidaan päätellä poistuneen väylältä. Solmuvalvonnan aikaväli riippuu sovelluksen vaatimasta vasteesta vikatilanteessa. Esimerkiksi CAN Appli-

[5] DIN 9684 -standardisarjaa vastaava ISO-standardisarja on ISO 11783. Se ei ole yhteensopiva DIN-standardisarjan kanssa. ISO-standardisarja on lähempänä amerikkalaista J1939-standardisarjaa.

cation Layer (CAL) -protokollassa (CiA/DS201 ... 1994) voidaan aikavälin lisäksi määrittää elinaika eli se, kuinka monta kertaa solmuvalvontakysely saa epäonnistua, ennen kuin tilanteeseen reagoidaan. Protokollapiirin tyypistä riippuen solmuvalvoja voi saada lisätietoja siitä, mistä sanoman puuttuminen johtui, solmuvalvojan liittimen irtoamisesta, valvottavan solmun viasta tai irtoamisesta vaiko väylän juuttumisesta joko dominanttiin tai resessiiviseen tilaan.

CAN-protokolla ei ole deterministinen, eli kommunikointiviiveitä ei voida tarkasti määrittää, ellei sanomien lähetyksiä synkronoida keskenään ylemmän tason protokollan avulla. Lisäksi uudelleenlähetykset aiheuttavat epämääräisen pituisia kommunikointiviiveitä. **Jos jonkin sanoman liian pitkä kommunikointiviive voisi aiheuttaa turvallisuusongelmia, jollakin tavalla on varmistauduttava siitä, että sanoma pääsee aina ajoissa perille**.

Ajallisuuden varmistamiseksi on ainakin neljä erilaista tapaa. Ensimmäinen tapa perustuu **odotusaikojen käyttöön**, toinen perustuu **sanomaliikenteen laskennalliseen analyysiin (tai simulointiin) ja sanomien järjestelyyn**. Kolmas tapa perustuu **sanomaketjujen käyttöön** ja neljäs tapa **aikajakoiseen kommunikointiin**. Nämä esitellään tarkemmin seuraavassa.

I. Mille tahansa sanomalle voidaan taata tietty maksimi kommunikointiviive, jos yksittäisille kommunikointiobjekteille asetetaan minimi **odotusaika**, joka niiden on odotettava, ennen kuin ne voidaan seuraavan kerran lähettää väylälle. Lähteessä Fredriksson (1995) on esimerkki tällaisesta menettelystä:

- Sanomat jaetaan tunnisteiden perusteilla ryhmiin, esim. tunnisteet 1 - 40 kahdeksaan ryhmään, jolloin jokaisessa ryhmässä on viisi tunnistetta. Ryhmät numeroidaan 1 - 8.

- Kun sanoma, joka kuluu ryhmään N, on lähetetty, sen täytyy odottaa 3 x N ms, ennen kuin se voidaan lähettää uudestaan

- Mikä tahansa muu sanoma voidaan lähettää milloin vain.

Oletetaan, että sanoman lähetykseen kuluu aikaa korkeintaan 200 µs ja solmut noudattavat edellä laadittuja sääntöjä. Oletetaan, että kaikki solmut ryhtyvät lähettämään sanomia niin taajaan kuin edellä mainitut säännöt sallivat. Tällöin sanomat välitetään seuraavan listan mukaisesti (jonossa olevat ovat sulkeissa, ja kun ne pääsevät väylälle, numero on vahvennetulla tekstillä):

ms	Ryhmä	Tunnisteet, jotka pääsevät läpi
0 - 3	123(45678+)	1 - 15
3 - 6	1**45**	1 - 5, 16 - 25
6 - 9	12**6**	1 - 10, 26 - 30
9 - 12	13**7**	1 - 5, 11 - 15, 31 - 35
12 - 15	124	1 - 10, 16 - 20
15 - 18	15**8**	1 - 5, 21 - 30, 36 - 40
18 - 21	123(6)	
21 - 24	1**6**7	
24 - 27	124(8)	
27 - 30	13**8**	
30 - 33	125	
33 - 36	1xx	1 - 5 + kaksi ryhmiin kuulumatonta
36 -39	123(46)	
39 ...	...	...

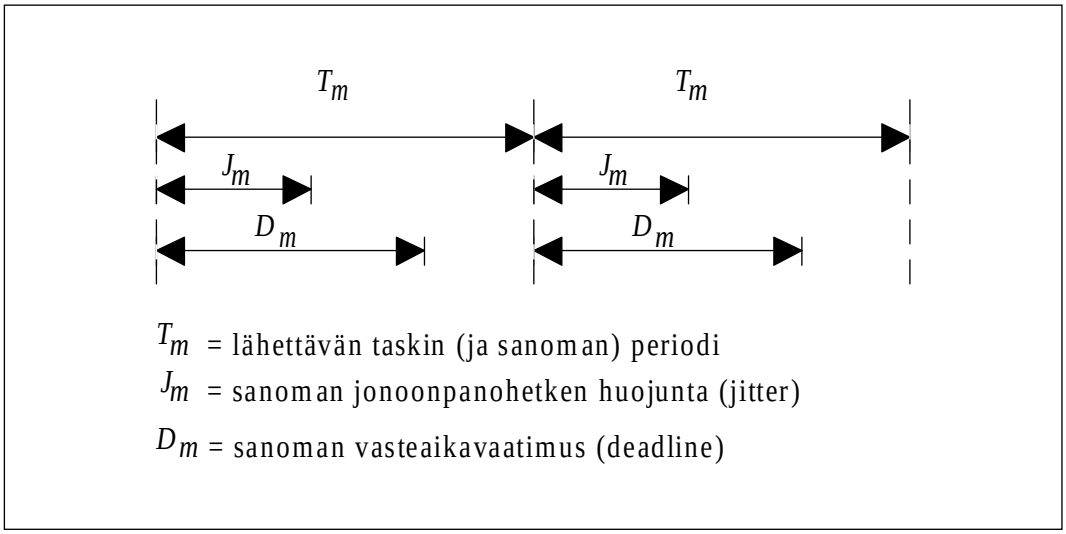
Tuloksena tästä saadaan seuraavat maksimiviiveet (aikaan on lisätty 200 µs, joka kuluu suurin piirtein, jos väylälle on juuri päässyt jokin sanoma, jonka lähetyksen loppumista on odotettava):

Tunniste	Maksimiviive	Odotusaika
1	400 µs	3 ms
5	1,2 ms	3 ms
--	----	----
25	6,2 ms	15 ms
--	----	----
40	18,2 ms	24 ms
41	34,4 ms	0 ms

Ensimmäisestä listasta nähdään, että väyläliikenteeseen järjestyy kaksi aukkoa, joiden aikana voidaan välittää mikä tahansa muu sanoma. Siten sanomatunnisteelle 41 saadaan myös määrättyä maksimiviive (34,4 ms), vaikka sille ei ole määritelty mitään odotusaikaa. Kvaser AB on patentoinut tämän algoritmin (PCT WO 91/10960, 1991).

II. Lähteessä Tindell & Burns (1994) esitellään, miten sanomien **ajallisuus voidaan laskennallisesti suunnitella** etukäteen. Periaate on se, että kun sanomilla on tietty lähetysperiodi (joka periytyy lähettävän taskin periodista), tietty pituus ja

tietty huojunta (jitter), sanomille voidaan laskennallisesti määrittää niiden vasteajat. Näitä verrataan sitten sanomien vasteaikavaatimuksiin. Huojunnalla tarkoitetaan tässä yhteydessä sitä epämääräistä aikaa, mikä kuluu lähettävän taskin käynnistymisestä siihen hetkeen, kun sanoma on valmis lähetettäväksi eli ryhtyy jonottamaan pääsyä väylälle (ks. kuva 15).



Kuva 15. Sanoman periodi, huojunta ja vasteaikavaatimus.

Tindell & Burns (1994) priorisoivat sanomat siten, että ne sanomat, joiden D - J on pienin, saavat suurimman prioriteetin. Käytännössä tämä tarkoittaa sitä, että ne sanomat saavat korkean prioriteetin, joilla on vähiten aikaa jonottaa pääsyä väylälle.

Sanoman vasteajan (R_m) määritellään olevan aika, joka kuluu lähettävän taskin aloitushetkestä siihen, kun sanoma saapuu vastaanottaville solmuille (yhtälöt 1 -5 lähteestä Tindell & Hansson [1995]):

$$R_m = t_m + C_m , \tag{1}$$

jossa t_m on sanoman väyläkilvasta johtuva jonotusaika ja C_m on sanoman maksimipituus sisältäen kaikki CAN-kehyksen bitit ja maksimimäärän ymppäysbittejä (stuff-bits). C_m lasketaan seuraavasta kaavasta

$$C_m = \left(\left\lfloor \frac{29 + 8s_m}{4} \right\rfloor + 47 + 8s_m \right) \tau_{bit,} \tag{2}$$

jossa s_m on sanoman tietokentän pituus tavuissa ja τ_{bit} on yhden bitin pituus. Jonotusaika lasketaan kaavasta

$$t_m = B_m + \sum_{\forall j \in hp(m)} \left\lceil \frac{t_m + J_j + \tau_{bit}}{T_j} \right\rceil C_j \,, \tag{3}$$

jossa *hp(m)* on niiden sanomien joukko, joilla on korkeampi prioriteetti kuin sanomalla *m*. B_m on pisimmän matalamman prioriteetin sanoman pituus eli

$$B_m = \max_{\forall k \in lp(m)} (C_k), \tag{4}$$

jossa *lp(m)* on matalamman prioriteetin sanomien joukko. Jos vasteaika-analyysiin kuulumattomien matalampien prioriteetin sanomien (löysästi reaaliaikaiset sanomat) pituutta ei ole rajoitettu, vaan se voi olla täydet kahdeksan tavua, $B_m = 134\tau_{bit}$.

Koska t_m esiintyy yhtälössä 3 molemmin puolin yhtälöä, t_m on ratkaistava seuraavasta yhtälöstä iteroimalla, kunnes $t_m^{n+1} = t_m^n$:

$$t_m^{n+1} = B_m + \sum_{\forall j \in hp(m)} \left\lceil \frac{t_m^n + J_j + \tau_{bit}}{T_j} \right\rceil C_j \tag{5}$$

Seuraavassa sovelletaan Tindellin ja Burnsin analyysiä lähteessä Tuominen (1995) esitettyyn esimerkkiin, joka liittyy työkoneen hydrostaattiseen tehonsiirtoon. Taulukossa 6 on listattu järjestelmän signaalit ja niiden parametrit. (Taulukossa kirjain S tarkoittaa sporadista eli tapahtumapohjaista sanomaa.)

Taulukko F. Esimerkkijärjestelmän signaalit ja niiden parametrit (Tuominen 1995).

Signaali	Tavuja	Periodi	Vasteaika	Signaalin nro
MOOTTORINOHJAIN				
Moottorin ohjaus	2	10 ms	5 ms	1
Moottorin kierrosnopeus (rpm)	2	10 ms	2 ms	2
Kaasupedaali; sähköinen	2	10 ms	2 ms	3
Paine 1 (p1)	2	10 ms	2 ms	4
Pumpun ohjaus	2	10 ms	5 ms	5
PUOMIN OHJAUS				
Sylinterin 1 ohjaus	6	20 ms	10 ms	6
Sylinterin 2 ohjaus	6	20 ms	10 ms	7
Kääntömoottorin ohjaus	6	20 ms	10 ms	8
Sylinterin 1 asema	2	20 ms	10 ms	9
Sylinterin 2 asema	2	20 ms	10 ms	10
Kääntömoottorin kulma	2	20 ms	10 ms	11
Sylinterin 1 paine (A,B)	4	20 ms	5 ms	12
Sylinterin 2 paine (A,B)	4	20 ms	5 ms	13
Kääntömoottorin paine (A,B)	4	20 ms	5 ms	14
Puomin sauvaohjaus (joystick)	6	20 ms	5 ms	15
OHJAUKSEN JA LUISTON OHJAUS				
Pyörän 1 ohjaus	2	10 ms	5 ms	16
Pyörän 2 ohjaus	2	10 ms	5 ms	17
Pyörän 3 ohjaus	2	10 ms	5 ms	18
Pyörän 4 ohjaus	2	10 ms	5 ms	19
Pyörän 5 ohjaus	2	10 ms	5 ms	20
Pyörän 6 ohjaus	2	10 ms	5 ms	21
Pyörän 1 kierrosnopeus	2	10 ms	5 ms	22
Pyörän 2 kierrosnopeus	2	10 ms	5 ms	23
Pyörän 3 kierrosnopeus	2	10 ms	5 ms	24
Pyörän 4 kierrosnopeus	2	10 ms	5 ms	25
Pyörän 5 kierrosnopeus	2	10 ms	5 ms	26
Pyörän 6 kierrosnopeus	2	10 ms	5 ms	27
Ohjauksen sauvaohjaus (joystick)	6	10 ms	5 ms	28
Hätä-seis	1	S	1 ms	29
Jarrut	1	S	2 ms	30
Valot 1	2	S	100 ms	31

Suoraviivaisin tapa on laittaa kukin signaali omaan CAN-sanomaan. Tässä on huojunta (*J*) asetettu kaikille sanomille nollaksi ja oletettu, että järjestelmässä ei ole muita sanomia kuin taulukossa 6 esitetyt. Lisäksi oletetaan, että käytetään 11-bittistä tunnistetta (standard frame) ja ettei virheellisiä kehyksiä ole. Ympäysbittejä oletetaan olevan maksimimäärä. Tällöin saadaan seuraavanlainen tulos vasteajoille (taulukossa *T* on periodin pituus ja *D* takaraja [deadline]; toteutunut vasteaika on merkitty kirjaimella *R*; ‘x’ tarkoittaa, että vasteaikavaatimukset sanomalle eivät täyty; ‘*‘ tarkoittaa, että sanoma ei ole päässyt väylälle, ennen kuin sen seuraava päivitys olisi jo valmiina lähetettäväksi; satunnaiset sanomat on lihavoitu; sanomat ovat prioriteettijärjestyksessä).

Taulukko G. Vasteaika-analyysi taulukon 6 esimerkkijärjestelmälle.

Signaalin nro	**Koko / tavua**	***T* / µs**	***D* / µs**	***R* / µs 125 kbit/s**	***R* / µs 250 kbit/s**	***R* / µs 500 kbit/s**	***R* / µs 1 Mbit/s**
29	1	50 000	1 000	x 1 424	712	356	178
2	2	10 000	2 000	x 2 016	1 008	504	252
3	2	10 000	2 000	x 2 608	1 304	652	326
4	2	10 000	2 000	x 3 200	1 600	800	400
30	1	50 000	2 000	x 3 712	1 856	928	464
1	2	10 000	5 000	4 304	2 152	1 076	538
5	2	10 000	5 000	4 896	2 448	1 224	612
12	4	20 000	5 000	x 5 648	2 824	1 412	706
13	4	20 000	5 000	x 6 400	3 200	1 600	800
14	4	20 000	5 000	x 7 152	3 576	1 788	894
15	6	20 000	5 000	x 8 064	4 032	2 016	1 008
16	2	10 000	5 000	x 8 656	4 328	2 164	1 082
17	2	10 000	5 000	x 9 248	4 624	2 312	1 156
18	2	10 000	5 000	x 9 840	4 920	2 460	1 230
19	2	10 000	5 000	x 10 432	x 5 216	2 608	1 304
20	2	10 000	5 000	*	x 5 512	2 756	1 378
21	2	10 000	5 000	*	x 5 808	2 904	1 452
22	2	10 000	5 000	*	x 6 104	3 052	1 526
23	2	10 000	5 000	*	x 6 400	3 200	1 600
24	2	10 000	5 000	*	x 6 696	3 348	1 674
25	2	10 000	5 000	*	x 6 992	3 496	1 748
26	2	10 000	5 000	*	x 7 288	3 644	1 822
27	2	10 000	5 000	*	x 7 584	3 792	1 896
28	6	10 000	5 000	*	x 8 040	4 020	2 010
6	6	20 000	10 000	*	8 496	4 248	2 124
7	6	20 000	10 000	*	8 952	4 476	2 238
8	6	20 000	10 000	*	9 248	4 624	2 312
9	2	20 000	10 000	*	9 544	4 772	2 386
10	2	20 000	10 000	*	9 840	4 920	2 460
11	2	20 000	10 000	*	x 10 136	5 068	2 534
31	2	100 000	100 000	*	10 136	5 068	2 534

Taulukon 7 vasteaika-analyysi pätee ainoastaan siinä tapauksessa, että käytössä oleva protokollapiiri ei jätä välejä lähettämiensä sanomien välille, jos ne ovat yhtä aikaa valmiina lähetettäviksi väylälle. Esimerkiksi 82C200-piiri ei täytä tätä ehtoa, mutta 82527-piiri täyttää. Käytettäessä 82527-piiriä on muistettava, että sanomat on pantava kaksiporttimuistiin prioriteettijärjestyksessä, koska ko. piiri ei lähetä sanomia prioriteettijärjestyksessä vaan alkaen kaksiporttimuistin alusta.

Taulukossa on satunnaisille sanomille annettu periodiksi 50 ms tai 100 ms, vaikka sanomat eivät ole periodisia. Nämä arvot ovat arvioita siitä, kuinka nopeasti kyseisiä signaaleja voi maksimissaan tulla peräkkäin. Tindell & Burns (1994) antaa satunnaisille käyttäjän (ihmisen) aiheuttamille sanomille vasteaikavaatimukseksi (deadline) 20 ms[6]. Tällöin käyttäjästä näyttää siltä, että hänen toimenpiteisiinsä reagoidaan välittömästi.

[6] Yleensä 20 - 50 ms on riittävä vasteaikavaatimus tällaisille tapahtumille.

Taulukosta 7 nähdään, että vasteaikavaatimukset toteutuvat 500 kbit/s ja 1 Mbit/s siirtonopeuksilla, mutta ei kahdella alemmalla nopeudella. Seuraavaksi kannattaa ryhtyä niputtamaan signaaleja samoihin CAN-sanomiin. Niputus onnistuu, jos sanomat ovat samoilla solmuilla ja niiden yhteinen pituus ei ylitä kahdeksaa tavua. Uuden sanoman periodi- ja vasteaikavaatimukset valitaan niin, että ne täyttävät kaikkien siihen niputettujen signaalien periodi- ja vasteaikavaatimukset. 82527-piirillä ei ole tilaa kovin monelle lähetettävälle sanomalle (enintään 14 sanomaa), joten niputus auttaa myös tähän ongelmaan. Myös satunnaisia sanomia voidaan niputtaa yhteen periodisten sanomien kanssa (tai niputtaa satunnaisista tapahtumista periodisia sanomia). Tällöin valitaan sellainen periodinen sanoma, jonka periodi ja vasteaikavaatimus summattuna täyttävät satunnaisen sanoman vasteaikavaatimuksen. Taulukossa 8 on esimerkki, miten sanomia tässä tapauksessa voitaisiin niputtaa yhteen.

Taulukko H. Vasteaika-analyysi taulukon 6 järjestelmälle, kun signaaleja on niputettu yhteen sanomaan.

Sign. num.	**Koko / tavua**	***T* / µs**	***D* / µs**	***R* / µs 125 kbit/s**	***R* / µs 250 kbit/s**	***R* / µs 500 kbit/s**	***R* / µs 1 Mbit/s**
29	1	50 000	1 000	x 1 584	792	396	198
2- 4	6	10 000	2 000	x 2 496	1 248	624	312
30	1	50 000	2 000	x 3 008	1 504	752	376
1,5	4	10 000	5 000	3 760	1 880	940	470
12,13	8	20 000	5 000	4 832	2 416	1 208	604
14	4	20 000	5 000	x 5 584	2 792	1 396	698
15	6	20 000	5 000	x 6 496	3 248	1 624	812
16,17,22,23	8	10 000	5 000	x 7 568	3 784	1 892	946
18,19,24,25	8	10 000	5 000	x 8 640	4 320	2 160	1 080
20,21,26,27	8	10 000	5 000	x 9 712	4 856	2 428	1 214
28	6	10 000	5 000	x 10 624	x 5 312	2 656	1 328
6,9	8	20 000	10 000	x 17 488	5 848	2 924	1 462
7,10	8	20 000	10 000	x 18 560	6 384	3 192	1 596
8,11	8	20 000	10 000	x 19 152	6 680	3 340	1 670
31	2	100 000	100 000	19 152	6 680	3 340	1 670

Taulukosta 8 nähdään, että vieläkään ei pystytä toimimaan 250 kbit/s siirtonopeudella, paitsi jos sanoman numero 28 (ohjauksen sauvaohjaus) vasteaikavaatimuksesta voidaan tinkiä. Väyläkuormitukset edellä esitetyissä tapauksissa ovat esitettyinä taulukossa 9.

Taulukko I. Väyläkuormitukset taulukon 7 ja 8 tapauksissa.

Siirtonopeus	**Taulukon 7 sanomajako**	**Taulukon 8 sanomajako**
125 kbit/s	151 %	90 %
250 kbit/s	75 %	45 %
500 kbit/s	38 %	23 %
1 Mbit/s	19 %	11 %

Tämä analyysi ei ota huomioon virhekehyksiä. Tindell & Burns (1994) jatkavat analyysiä ottamalla myös ne huomioon. Virheiden esiintymistiheydestä ja esiinty-

mistavasta tehdään siinä malli, jonka perusteella virheiden vaikutus vasteaikoihin voidaan laskea. Virhetilanteisiin voidaan varautua myös siten, että lisätään analyysivaiheessa järjestelmään kaksi valesanomaa, toinen esimerkiksi kahdeksan tavun mittainen ja toinen nollamittainen. Virhetilanteesta toipumiseen kuluu aikaa 29 x τ_{bit} uudelleenlähetyksen lisäksi, joten yksi valesanoma ei riitä mallintamaan uudelleenlähetyksen vaatimaa lisäaikaa. Periodiksi valitaan pienin järjestelmässä oleva periodi, jolloin jokaista periodia kohti on aukko uudelleenlähetystä varten. Vasteajat tässä tapauksessa ovat taulukon 10 mukaiset.

Taulukko J. Vasteaika-analyysi, kun järjestelmään on lisätty kaksi valesanomaa, jotka tekevät tilaa uudelleenlähetykselle virhetilanteessa.

San. num.	Koko / tavua	*T* / µs	*D* / µs	*R* / µs 125 kbit/s	*R* / µs 250 kbit/s	*R* / µs 500 kbit/s	*R* / µs 1Mbit/s
29	1	50 000	1 000	x 3 088	x 1 544	772	386
2-4	6	10 000	2 000	x 4 000	2 000	1 000	500
30	1	50 000	2 000	x 4 512	x 2 256	1 128	564
1,5	4	10 000	5 000	x 5 264	2 632	1 316	658
12,13	8	20 000	5 000	x 6 336	3 168	1 584	792
14	4	20 000	5 000	x 7 088	3 544	1 772	886
15	6	20 000	5 000	x 8 000	4 000	2 000	1 000
16,17,22,23	8	10 000	5 000	x 9 072	4 536	2 268	1 134
18,19,24,25	8	10 000	5 000	x 10 144	x 5 072	2 536	1 268
20,21,26,27	8	10 000	5 000	*	x 5 608	2 804	1 402
28	6	10 000	5 000	*	x 6 064	3 032	1 516
6,9	8	20 000	10 000	x 20 496	6 600	3 300	1 650
7,10	8	20 000	10 000	*	7 136	3 568	1 784
8,11	8	20 000	10 000	*	7 432	3 716	1 858
31	2	100 000	100 000	*	7 432	3 716	1 858

On huomattava, että taulukon 7, 8 ja 10 analyysit on tehty olettaen, että ymppäysbittejä on täysi määrä. Käytännössä ymppäysbittejä on 99,9 % todennäköisyydellä useita bittejä sanomaa kohti vähemmän, joten sanomille jää jonkin verran varmuusmarginaalia (Rauchaupt 1994[7]).

Uudelleenlähetykset tekevät joka tapauksessa CAN-protokollasta epädeterministisen. Jos löytyy CAN-protokollapiirejä, joissa uudelleenlähetys voidaan estää, vasteajat voidaan ennustaa deterministisesti. Tällöin kommunikoinnin luotettavuus olisi hoidettava jollakin toisella tavalla, esimerkiksi kahdentamalla väylä ja lähettämällä sanoma yhtä aikaa molemmille väylille. Näin tekee esimerkiksi Kopetz (1994) TTP (Time Triggered Protocol) -arkkitehtuurissaan. TTP ei ole kuitenkaan CAN-pohjainen arkkitehtuuri, joten sitä ei esitellä tässä yhteydessä tarkemmin.

III. **Sanomaketjujen käyttö** on verrattavissa valtuudenvälitysprotokollaan. Sanomaketjulla tarkoitetaan sitä, että kun solmu saa tietyn sanoman, se sen seurauk-

[7] Rauchaupt käyttää ymppäysbittien laskemisessa hieman virheellistä kaavaa eli Tindellin & Burnsin (1994) mukaista kaavaa. Korjattu kaava on lähteessä Tindell & Hansson (1995). Ymppäysbittejä on korjatussa kaavassa 1 - 3 kpl enemmän riippuen sanoman pituudesta.

sena lähettää oman sanomansa (tai useita sanomia), joka taas liipaisee seuraavalla solmulla uuden sanoman lähetyksen. Tällainen ketju voi olla suljettu tai avoin. Avoimessa ketjussa alkusolmu lähettää ensimmäisen sanoman oman kellonsa tahdissa tai jonkin tapahtuman seurauksena. Suljetussa ketjussa ketjun viimeinen solmu liipaisee jälleen ketjun ensimmäisen solmun.

IV. **Aikajakoinen kommunikointi** vaatii, että solmuilla on yhtenäinen käsitys ajasta eli solmuilla on paikalliset kellot, joita pidetään ajassa järjestelmän pääkelloon nähden. Tarkkuusvaatimus on sovelluskohtainen. Solmuilla on oikeus lähettää sanomansa sille omistetun aikaviipaleen aikana. Järjestelmässä voi olla myös vapaita aikaviipaleita, joiden aikana voidaan lähettää sanomia, jotka eivät ole aikakriittisiä. Lähteessä Fredriksson (1995) on esimerkki siitä, miten tällainen aikajakoinen protokolla voidaan toteuttaa järjestelmään. Lähteessä Gergeleit & Streich (1994) on esimerkki siitä, miten paikalliset kellot pidetään ajassa pääkelloon nähden. Algoritmi on pääpiirteissään seuraavanlainen: pääkellon omistaja lähettää kellosanoman ja tallentaa muistiin hetken, jolloin sanoman lähetys on päättynyt (jolloin saadaan lähetyskeskeytys protokollapiiriltä); vastaanottaja tallentaa muistiin hetken, jolloin se sai sanoman (jolloin saadaan vastaanottokeskeytys); tämä aika on suurin piirtein sama kuin lähetysaika, ainakin aikaero on vakio; seuraavalla kierroksella lähettäjä lähettää kellosanomassaan edellisen kellosanoman lähetyshetken; vastaanottaja voi nyt korjata oman kellonsa vertaamalla oikeaa lähetysaikaa siihen, minkä se tallensi muistiinsa.

Tiukasti reaaliaikaisissa (hard real-time) järjestelmissä sanoman viivästyminen merkitsee vikaa, joten arvon oikeellisuuden tarkistuksen lisäksi saatetaan tarvita ajallisuuden tarkistusta. CAN-protokolla huolehtii arvon oikeellisuuden tarkastuksesta automaattisesti, mutta ajallisuuden tarkistusta varten ei ole määritelty palvelua. Globaalia aikaa voidaan käyttää sanomien aikaleimaukseen ja siten sanomien ajallisuuden tarkistamiseen. Protokollapiiri saattaa tukea aikaleimausta.

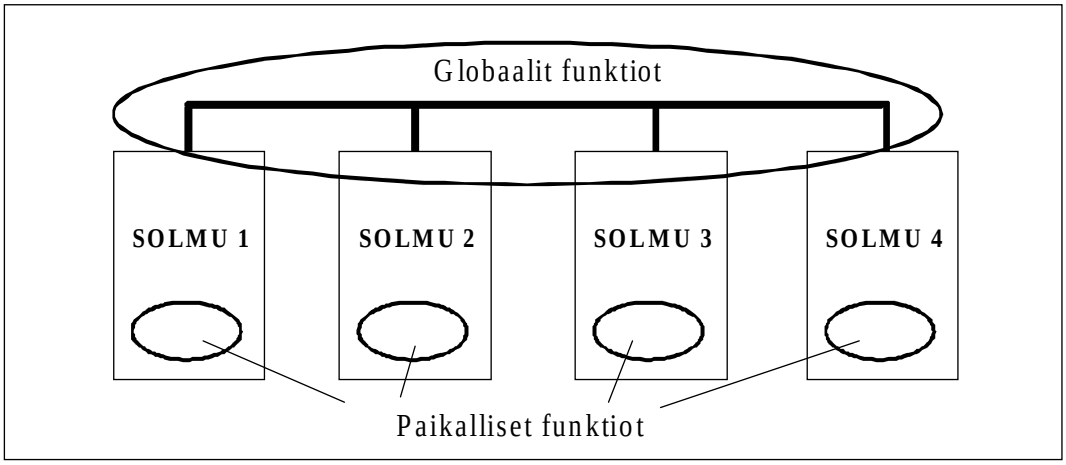
3.3 ESIMERKKEJÄ TURVALLISUUSTEKNIIKOISTA

Tässä kohdasa esitellään turvallisuustekniikoita, joita on käytetty hajautettujen järjestelmien arkkitehtuureissa. Esiteltävät arkkitehtuurit ovat Vehicle Internal Architecture (VIA), Multiple Master Multiple Slave (M3S) ja CANopen.

3.3.1 VIA-arkkitehtuuri

VIA-arkkitehtuuri (Lawson et al. 1992) on suunniteltu Ruotsissa sikäläisen autoteollisuuden tukemana. VIA on siis autojen reaaliaikainen ohjausjärjestelmäarkkitehtuuri. Autojen reaaliaikajärjestelmissä turvallisuuskysymykset korostuvat, joten VIA-arkkitehtuurissa on erityisesti kiinnitetty huomioita arkkitehtuurin turvallisuusominaisuuksiin. Seuraavassa esitellään luettelomaisesti arkkitehtuurin pääpiirteet (nimenomaan arkkitehtuurin vikasietoinen versio, jota on kehitelty Chalmersin teknillisessä korkeakoulussa):

- Paikalliset funktiot (esim. pyörän ohjaus [kuva 16]) ovat yhden vian sietäviä ja toisesta viasta ne menevät turvalliseen tilaan.



Kuva 16. Globaalit ja paikalliset funktiot.

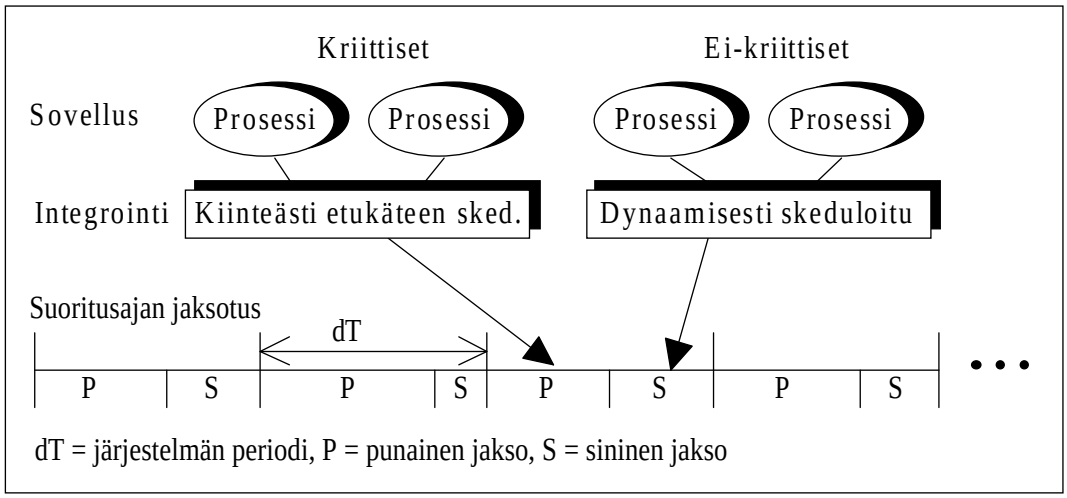
- Globaalit funktiot (esim. jousituksen ohjaus [kuva 16]) ovat kaksi vikaa sietäviä ja kolmannesta ne menevät turvalliseen tilaan.

- Vikasietoisuus saadaan aikaan redundanssilla. Solmu koostuu viidestä osasta, jotka ovat tehon syöttö, prosessoiva elementti, paikallinen I/O, väyläliityntä ja tilamuuttujien muisti. Nämä osat on kahdennettu, eli CAN-väyläkin on kahdennettu. Jotta globaalit funktiot saataisiin kaksi vikaa sietäväksi, niitä vastaavat solmut on kahdennettava tai globaalit funktiot on monistettava usealle solmulle (esim. jousituksen ohjaus voidaan monistaa pyörän ohjaus -solmuille, jolloin erillistä jousituksen ohjaus -solmua ei ole).

- Sovellusta ajetaan aikajakoisesti; periodi on 10 ms, jona aikana luetaan kaikki anturit, tehdään kaikki laskenta, päivitetään lähdöt ja välitetään kaikki globaalit parametrit.

- Jos havaitaan vika, joka esiintyy vain yhden syklin aikana, vika tulkitaan hetkelliseksi eikä siihen reagoida $\Rightarrow$ hetkelliset viat siedetään (sovelluksen täytynee kestää yhden syklin kestävä virhetieto lähdössä).

- Sykli jaetaan punaiseen ja siniseen jaksoon; punainen jakso on kiinteästi ajoitettu (etukäteen ohjelmointivaiheessa) turvallisuuskriittisille funktioille (hard real-time), ja kommunikointi on aikajakoinen ja siten deterministinen; sininen jakso on varattu ei-kriittisille funktioille (soft real-time), ja kommunikointi tapahtuu kilpailemalla jäljelle jääneestä kommunikointiajasta, joten kommunikointi ei ole determinististä (kuva 17).



Kuva 17. Suoritusajan jaksotus kriittisille ja ei-kriittisille toiminnoille.

VIA-arkkitehtuuri ei ota kantaa siihen, mitä kommunikointiprotokollaa käytetään, mutta CAN-protokollaa voidaan käyttää sen yhteydessä. Tosin osa suorittimen resursseista kuluu tällöin CAN-protokollan päälle rakennettavan aikajakoisen protokollan suoritukseen.

3.3.2 M3S-arkkitehtuuri

M3S-arkkitehtuuri on suunniteltu vammaisten apuvälineisiin, etenkin pyörätuoleihin. Yksinkertaisimmassa M3S-sovelluksessa on seuraavat kaksi solmua: sauvaohjain ja moottoreiden ohjain. Näiden lisäksi järjestelmässä voi olla esimerkiksi näyttö, manipulaattorin ohjain, navigaattori ja langaton liityntä ulkomaailmaan. M3S on CAN-pohjainen arkkitehtuuri. Se on kehitetty eurooppalaisissa tutkimushankkeissa, mm. TIDE-hankkeessa[8]. M3S-spesifikaatio tulee olemaan pohjana ISOn työryhmälle ISO/TC-173/SC-1/WG-7[9]. Protokollaa ei esitellä tässä yksityiskohtaisesti, vaan ainoastaan sen turvallisuustekniset ratkaisut, jotka ovat

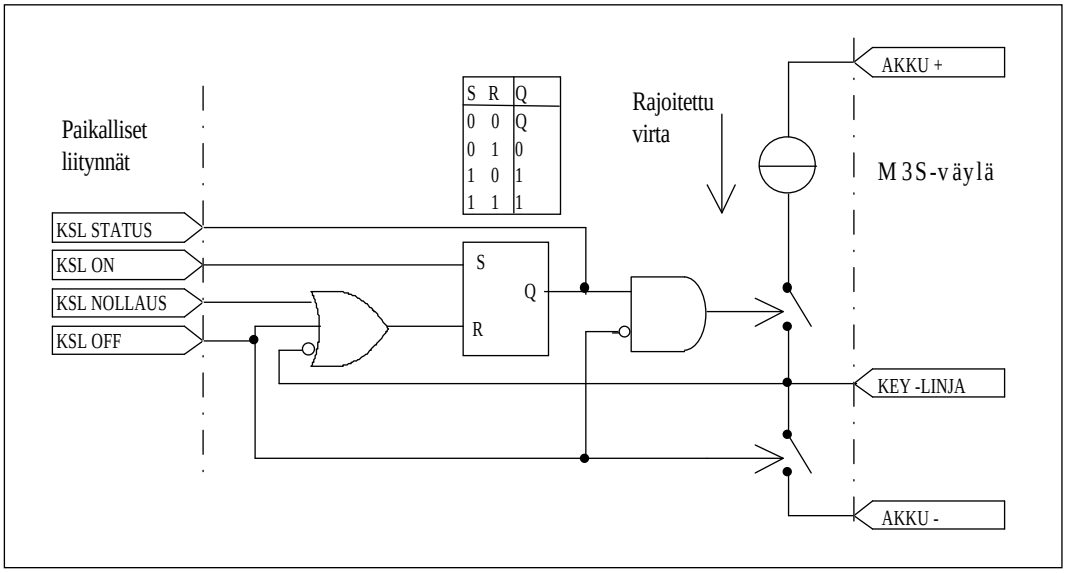
- virtakytkin, jolla voidaan sammuttaa kaikki laitteet yhtä aikaa
- kuolleenmiehenkytkin
- turvallisuusyhtälöt
- turvallisuuden monitorointi paikallisesti ja globaalisti
- poikkeustilannekäsittely.

Fyysisessä M3S-väyläkaapelissa on CAN-signaalijohtimien ja käyttöjännitejohtimien lisäksi kaksi johdinta, joista toinen välittää tiedon **virtakytkimeltä** (key

[8] Technology for the socio-economic Integration of Disabled and Elderly people project #128.

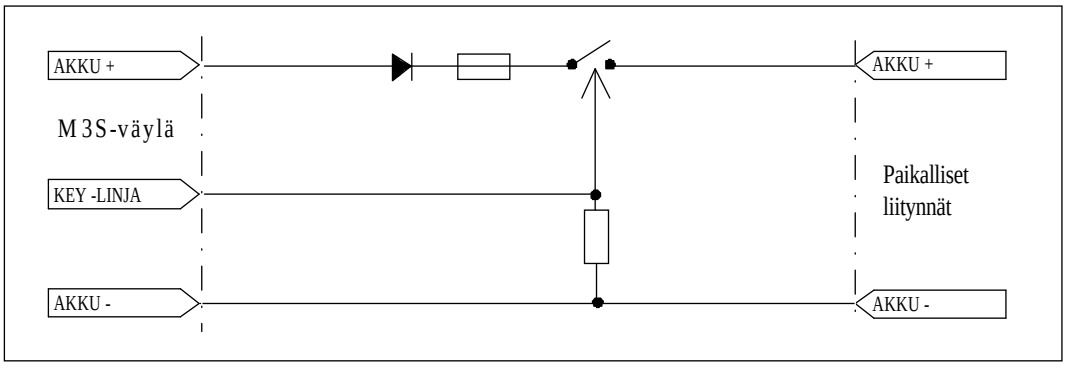
[9] International Organisation for Standardisation, Technical systems and aids for disabled or handicapped people, Sub Committee wheelchairs, Working Group serial interface for electric wheelchair controllers.

switch) ja toinen kuolleenmiehenkytkimeltä (dead man switch). Vähintään yhdellä solmuista tulee olla varsinainen fyysinen virtakytkin, jolla aktivoidaan M3S-väylällä kulkeva key-linja. Kun key-linja on aktivoitu, väylällä olevat solmut kytkevät päälle käyttöjännitteensä. Vastaavasti, kun key-linja passivoidaan, solmut sammuttavat käyttöjännitteensä. Key-linja passivoidaan erillisellä sammutuskytkimellä tai hätätapauksissa turvallisuusmonitorointia tekevän solmun toimesta. Kuvassa 18 on key-toiminnon periaatekytkentä solmulla, jolla on virtakytkin.



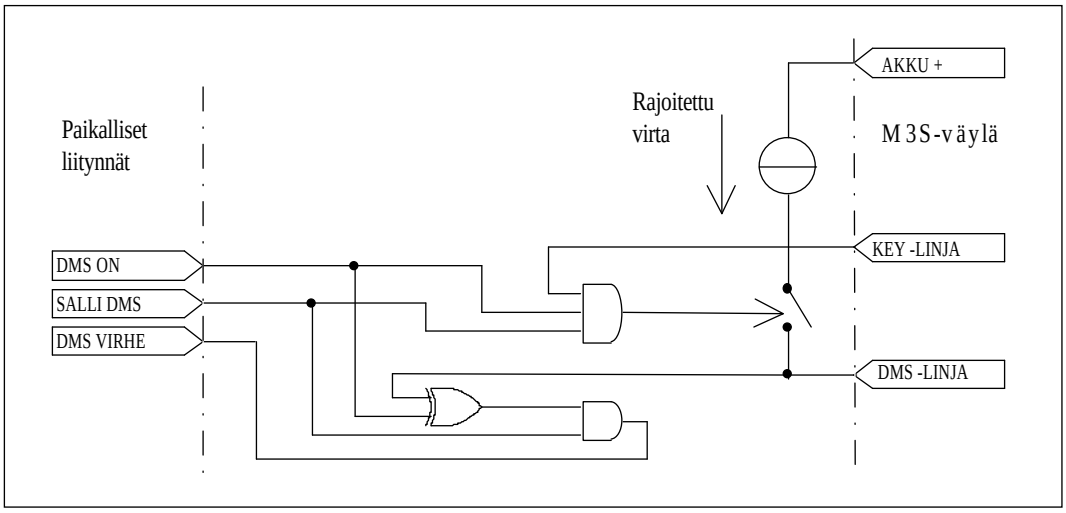
Kuva 18. Key-toiminnon periaatekytkentä solmulla, jolla on virtakytkin (M3S 1995).

Varsinainen virtakytkin kytketään linjaan KSL ON. Virtakytkin ei saa olla mekaanisesti lukkiutuva, vaan lukkiutuminen tehdään lukkopiirillä (RS-latch). Virtojen sammutukseen on oma kytkin, joka kytketään linjaan KSL OFF. Solmun prosessori voi myös sammuttaa virrat linjan KSL NOLLAUS avulla, jos se saa nollauskomennon turvallisuusmonitorointia tekevältä solmulta. Virrat sammuvat vain, jos mikään muu virtakytkimen sisältävä solmu ei pidä key-linjaa aktiivisena. Solmun prosessori voi tarkkailla oman virtakytkimensä tilaa linjasta KSL STATUS. Jokaisella solmulla on kuvan 19 mukainen kytkentä käyttöjännitteiden päällekytkemiseksi.



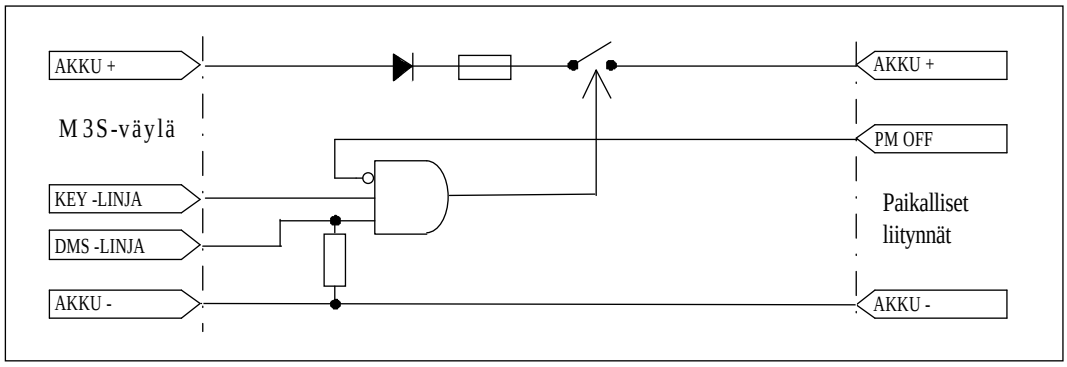
Kuva 19. Solmujen käyttöjännitteiden ohjaus key-linjan avulla (M3S 1995).

Kuolleenmiehenkytkintä (DMS) käytetään normaalisti pyörätuolin ajomoottoreiden aktivoimiseksi. Jos käyttäjä ei pidä kuolleenmiehenkytkintä aktivoituna, pyörätuoli pysähtyy. Kuolleenmiehenkytkimen periaatekytkentä on kuvan 20 mukainen.



Kuva 20. Kuolleenmiehenkytkimen periaatekytkentä (M3S 1995).

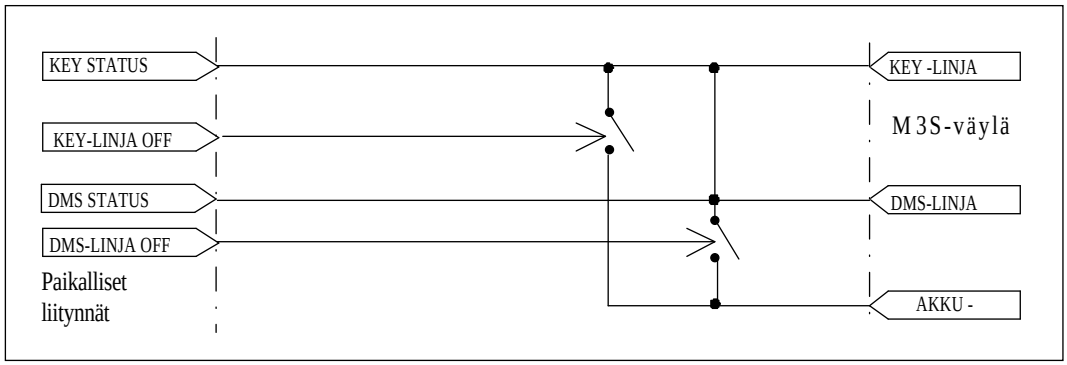
Kuolleenmiehenkytkin kytketään linjaan DMS ON. Kytkin ei saa olla lukkiutuva. DMS-linja aktivoituu, jos key-linja on aktivoitu, kuolleenmiehenkytkin on aktivoitu ja solmun prosessori sallii DMS-linjan aktivoinnin SALLI DMS -linjan välityksellä. Tämän se tekee saatuaan siihen luvan turvallisuusmonitorointia tekevältä solmulta. Jos DMS-linja on eri tilassa kuin fyysinen kuolleenmiehenkytkin, prosessori havaitsee tällaisen virhetilanteen DMS VIRHE -linjasta. Virhetilanteesta lähetetään tieto turvallisuusmonitorointia tekevälle solmulle. Ajomoottoreiden ohjaimella vastaavasti on kuvan 21 mukainen kytkentä.



Kuva 21. Ajomoottoreiden käyttöjännitteiden ohjauskytkentä (M3S 1995).

Ajomoottorit saavat käyttöjännitteet vain kun sekä key-linja että DMS-linja ovat aktiivisia. Ohjaimen prosessori voi myös sammuttaa ajomoottoreiden virran PM OFF -linjan välityksellä.

Turvallisuusmonitorointia tekevä solmu (CCM = Configuration and Control Module) voi passivoida sekä key-linjan että DMS-linjan joko CAN-väylän kautta komentamalla solmua, joka pitää vastaavaa linjaa aktivoituna, tai suoraan oikosulkemalla vastaavan linjan maahan (kuva 22).



Kuva 22. Key-linjan ja DMS-linjan kytkentä turvallisuusmonitorointia tekevällä solmulla (M3S 1995).

CCM-solmulle voidaan konfiguroida joukko **turvallisuusyhtälöitä** (safety equations). Seuraavassa on yksi esimerkki tällaisesta yhtälöstä:

HighSpeed = LowSeat AND NOT ManipulatorFoldedOut

Yhtälön kaikki muuttujat ovat tyyppiä BOOLEAN. Muuttujien *LowSeat* ja *ManipulatorFoldedOut* arvot lähetetään asianomaisilta solmuilta erillisinä tapahtumina silloin, kun niiden arvot muuttuvat. CCM suorittaa tällöin turvallisuusyhtälön ja lähettää solmuille uuden *HighSpeed*-arvon. Asianomaiset solmut saavat täten esimerkin tapauksessa tiedon, voidaanko ajaa suurella nopeudella vai ei. *HighSpeed*-muuttujaa kutsutaan turvallisuusehdoksi (safety restriction) ja *LowSeat*- sekä *ManipulatorFoldedOut*-muuttujia kutsutaan turvallisuustapahtumiksi (safety events).

Turvallisuusmonitorointia tehdään paikallisesti jokaisella solmulla ja globaalisti CCM-solmun toimesta. Jos M3S-järjestelmässä on langattomia linkkejä, myös niiden turvallisuutta monitoroidaan. CCM-solmu tekee seuraavat globaalit turvallisuustarkistukset käyttäen hyväksi solmujen paikallisen turvallisuusmonitoroinnin tuloksia:

- vikavalvonta; viat jaetaan viiteen tasoon: rajoitettu toiminta, ei-vakava vika, vakava vika, vika, joka vaatii käyttöjännitteiden sammutuksen laitteelta ja linkkivika. Rajoitettu toiminta on kyseessä silloin, kun solmu toimii muuten normaalisti, mutta se ei pysty toimimaan jossakin tietyssä moodissa. Ei-vakava vikatilanne on mm. tilanne, jossa ajomoottoreiden ohjain ei ole tietyn ajan sisällä saanut uutta vapausastesanomaa (XY-tietoa). Vakava vika on esim., jos solmu ei ole saanut solmuvalvontakyselyä 100 ms:n aikana tai jos solmun CAN-protokollapiiriltä tulee varoitus (bus off warning) häiriöllisestä CAN-liikenteestä tai jos DMS-linjan tila ei ole oikea. Vikoja, jotka vaativat käyttöjännitteiden sammutuksen, ovat mm. CAN-protokollapiirin poistuminen väylältä (bus-off) ja solmuvalvontakyselyn puuttuminen 200 ms:n ajan, jos kyseessä on turvallisuuskriittinen solmu. Linkkivikoja ovat langattoman liikenteen erityisviat. Solmu ilmoittaa CCM:lle vikatilanteista erityisillä sanomilla (jos CAN-väylä on kunnossa) tai toisaalta CCM voi kysellä solmuilta niiden tilarekistereitten arvot, joista se näkee vikatilanteet. Vikatilanteissa CCM voi komentaa solmua joko alustustilaan tai sammuttamaan käyttöjännitteet (emergency stop). Jos CCM ei voi käyttää CAN-väylää komentojen lähettämiseen, se vetää key-linjan alas.

- solmuvalvonta; CCM valvoo solmuja lähettämällä niille solmuvalvontakyselyn 100 ms:n välein, jos solmu on aktiivinen, ja 1 000 ms:n välein, jos solmu on ei ole aktiivinen.

- akkujen valvonta; CCM kyselee akkuja valvovalta solmulta akkujen tilan 10 000 ms:n välein. Järjestelmässä täytyy olla vähintään yksi solmu, joka valvoo akkuja. CCM lähettää kyselykehyksen, johon akkuja valvova solmu vastaa sanomakehyksellä. Sanomakehyksessä on tieto akkujännitteestä, virrasta, jäljellä olevasta kapasiteetista ja maksimivirrasta.

- virtakytkimen oikosulkuvalvonta; normaalitilanteessa CCM ei pysty havaitsemaan, jos virtakytkin on juuttunut aktiiviseen tilaan, mutta tilanteessa, jossa useat solmut tarjoavat virtakytkinpalvelun ja CCM haluaa vaihtaa palvelun tarjoajan toiseen, CCM havaitsee, että vanha palvelun tarjoaja ei kyennyt nollaamaan virtakytkimen lukituspiiriä. Tällaisessa tilanteessa CCM informoi käyttäjää ja estää turvallisuuskriittiset toiminnot.

- key-linjan oikosulun valvonta; CCM huomaa, jos key-linja on oikosulkeutunut aktiivitilaan, koska se saa tiedon kaikilta virtakytkinpalvelujen toimittajilta niiden lukituspiirien tiloista ja toisaalta CCM pystyy suoraan näkemään key-linjan todellisen tilan. Tällainen oikosulkutilanne on vakava, koska käyttäjä ei pysty sammuttamaan järjestelmää. CCM tarkistaa tämän tilanteen 1 000 ms:n välein. Vikatilanteesta informoidaan käyttäjää ja turvallisuuskriittiset toiminnot estetään.

- DMS-linjan oikosulun valvonta; CCM huomaa tämän samalla tavalla kuin edelläkin. Myös tällainen oikosulkutilanne on vakava, koska pyörätuoli ei pysähdy, vaikka käyttäjä vapauttaa kuolleenmiehenkytkimen. CCM tarkistaa tämän tilanteen 1 000 ms:n välein ja voi pysäyttää järjestelmän key-linjan avulla. Vikatilanteesta informoidaan käyttäjää ja turvallisuuskriittiset toiminnot estetään.

- globaalin tilatiedon lähettäminen solmuille; solmut lähettävät tilatietonsa CCM:lle vastauksena solmuvalvontakyselyyn tai kun tila vaihtuu. CCM muodostaa globaalin tilatiedon tekemällä loogisen TAI-operaation solmujen tilatiedoista. CCM lähettää globaalin tilatiedon solmuille, jos tilatiedoissa tapahtuu muutos. Täten kaikki solmut saavat tiedon, jos esimerkiksi joku solmuista on mennyt tilaan VIKAANTUNUT (FAILED). Tähän tilaan solmu menee, jos se huomaa vakavan vian eikä pysty siitä toipumaan.

- turvallisuusehtojen lähetys; CCM lähettää solmuille turvallisuusehdon päivityksen aina, kun se saa joltakin solmulta turvallisuusehtoon vaikuttavan turvallisuustapahtuman. Turvallisuusehdon CCM laskee turvallisuusyhtälöstä.

M3S-spesifikaatio määrittelee lisäksi **poikkeustilanneinformaation lähetyksen**; solmut voivat lähettää käyttäjälle poikkeustilanneinformaatiota teksti- ja ikonimuodossa. Poikkeustilanteet jaetaan neljään kriittisyystasoon, jotka ovat vika (solmu ei toimi enää), ongelma (toimii, mutta ei kunnolla), varoitus (toimii kohta huonosti) ja informaatio (toimii kunnolla, mutta annetaan lisätietoa). Solmu lähettää poikkeustilanneinformaation näyttöön CCM:n kautta lohkosiirtona. Poikkeustilanneteksti tai ikoni voi olla jo valmiina CCM:n tai näytön muistissa, jolloin solmun ei tarvitse lähettää tekstiä tai ikonia lohkosiirtona, vaan pelkkä poikkeustilanteen numero riittää.

3.3.3 CANopen

CANopen-sovellusprofiilia[10] standardoidaan CAN in Automation (CiA) -ryhmässä. Sen pohjana on CiA-ryhmän CAN Application Layer (CAL) -sovelluskerros. CANopen tarkoitettu automaatiosolun sisäiseen tiedonsiirtoon. CANopen arkkitehtuurissa käytetään erityistä tahdistussanomaa (SYNC message), jonka avulla verkko tahdistetaan ja kommunikoinnista tehdään aikajakoista. Sen lisäksi voidaan käyttää tapahtumapohjaisia sanomia, jotka lähetetään synkronisten sanomien jälkeen. Tämä vastaa siis pääpiirteissään VIA-arkkitehtuurin jakoa punaiseen ja siniseen kommunikointijaksoon (ks. kuva 17). Protokolla on lyhyesti esitettynä seuraavanlainen: järjestelmässä on isäntä, joka lähettää SYNC-sanomaa; orjasolmut ottavat näytteet takaisinkytkentämuuttujista saatuaan SYNC-sanoman ja lähettävät ne väylälle (isännälle); isäntä lähettää orjasolmuille uudet tehtäväkomennot, jotka suoritetaan seuraavan SYNC-sanoman vastaanoton jälkeen.

[10] Tätä kirjoitettaessa CANopen sovellusprofiilista oli ainoastaan luonnos saatavissa.

Tässä yhteydessä CANopen-sovellusprofiilia ei esitellä tämän tarkemmin; ainoastaan turvallisuuteen liittyvät ratkaisut esitetään lyhyesti.

- Järjestelmässä on isäntä, joka on vastuussa järjestelmän virhekäsittelystä. Se suorittaa solmuvalvontaa CAL-spesifikaation mukaisesti. Jos isäntä ei saa vastausta joltakin solmulta tai solmun tila on eri kuin mitä isäntä olettaa, isäntä pysäyttää sovellusohjelmansa, antaa operaattorille virheilmoituksen ja saattaa kaikki järjestelmän solmut turvalliseen tilaan. Yleensä se tapahtuu siten, että isäntä pakottaa kaikki solmut irti väylältä ("disconnected"-tilaan). Tämä onnistuu myöskin siinä tapauksessa, että CAN-väylä ei enää toimi, sillä solmu irrottaa itsensä väylältä, kun se lakkaa saamasta solmuvalvontakyselyjä isännältä. Kun kaikki solmut on irrotettu väylältä, isäntä alustaa verkon uudelleen, jos se on mahdollista.

- Jos isäntä vioittuu ja lakkaa lähettämästä solmuvalvontakyselyjä, orjasolmu menee "disconnected"-tilaan. Sovellusprofiilin luonnoksessa ei sanota, pitääkö orjasolmun mennä tässä yhteydessä turvalliseen tilaan vai ei.

- Solmuvalvontaa ei käytetä solmuille, jotka lähettävät periodisia sanomia SYNC-sanoman tahdittamana. Isäntä havaitsee periodisen sanoman puuttumisesta, että solmulla on vakava vika. Lisäksi periodisessa sanomassa voi olla pari lippua, jotka ilmaisevat, jos solmulla on jokin vakava tai vähemmän vakava vika. Täten isäntä voi reagoida vikaan nopeammin kuin solmuvalvonnan tapauksessa.

- Sisäisissä vikatilanteissa (laiteviat, korkeat lämpötilat jne.) orjasolmut voivat lähettää isännälle hätäsanoman (emergency telegram). Jos isäntä ei reagoi hätäsanomaan tietyn ajan kuluessa, solmu menee itse turvalliseen tilaan. Hätäsanoma koostuu yhdestä neljän tavun mittaisesta CAN-kehyksestä, jossa kaksi tavua on varattu virhekoodille ja kaksi tavua lisäinformaatiolle. Hätäsanoma lähetetään vain kerran yhtä virhetilannetta kohden. Kun virhetilanteesta on toivuttu, lähetetään hätäsanoma virhekoodilla: "ei enää virheitä". Hätäsanomalle annetaan korkein prioriteetti (tunnistenumero 0; SYNC-sanoman tunnistenumero on 1).

3.4 YHTEENVETO

Seuraavassa on listattu tärkeimmät asiat, jotka täytyy ottaa huomioon, kun suunnitellaan luotettavaa CAN-järjestelmää:

- Miten toimitaan ISO 11898 -standardin mukaisissa 9 vikatilanteissa (oikosulut ja katkokset),

  - käytetäänkö yhtä johdinta kommunikointiin (vaatii erityisen lähetin-vastaanotinkytkennän; EMC-ominaisuudet huononevat)
  - käytetäänkö kahdennettua väylää?

- Pitääkö CAN-väylä erottaa galvaanisesti muusta järjestelmästä?

- Voi olla tarpeellista, esimerkiksi jos väylän pituus on suurempi kuin 200 m.

- EMC-ongelmat:

  - Pitääkö käyttää suojattua kaapelia?
  - Pienillä siirtonopeuksilla kannattaa pidentää nousuaikaa, jos lähetin-vastaanottimessa on siihen valmius.

- Topologia:

  - Topologian tulisi olla sellainen, että heijastukset minimoituisivat.
  - Järjestelmäsuunnittelijan on voitava ohjelmoida kaikkien solmujen siirtoparametrit (BTR0- ja BTR1-rekisterit), että näytteenottohetki saataisiin viritettyä järjestelmän käyttämään topologiaan ja väyläpituuteen (ja kellotoleransseihin) nähden.
  - Voitaisiinko käyttää tähtimäistä topologiaa toistimien avulla (tai ilman toistimia, jos haarojen pituudet ovat riittävän pieniä siirtonopeuteen nähden).

- Mitä signaaleja väyläkaapelissa kulkee mukana?

  - Oikosulut käyttöjännitteisiin ja maapotentiaaliin ovat todennäköisempiä, jos käyttöjännitejohtimet kulkevat samassa kaapelissa CAN-johtimien kanssa.
  - Pitäisikö kaapelissa olla myös hätä-linja, jonka avulla kaikki solmut voitaisiin komentaa turvalliseen tilaan (hätä-seis)?
  - Pitäisikö kaapelissa olla kuolleenmiehenkytkin-linja; jos se ei ole aktiivinen, jokin osa järjestelmää ei suostu toimimaan (esimerkiksi ajomoottorit pyörätuolissa)?

- Duplikoitumisongelma; vastaanottaja saa saman sanoman kahteen kertaan, jos

  - kehyksen viimeinen bitti vääristyy (CAN-spesifikaation ominaisuus)
  - kuittausbitti viivästyy (liian pitkä väylä tai muuten liian pitkät viiveet).

- CAN-keskeytyspalvelija ei saa hukata sanomia missään tilanteessa.

  - Kriittisin on tilanne, jossa solmulle tulee peräkkäin kolme sille relevanttia sanomaa, joista ensimmäisen tietokentässä on kahdeksan tavua, toisessa nolla tavua ja kolmannessa mikä tahansa tavumäärä (0 - 8); keskeytyspalvelijan pitää ehtiä käsittelemään tämä tilanne kaikissa tilanteissa, myös silloin, kun jokin muu keskeytyspalvelu on käynnissä tai jokin muu keskeytys haluaisi tulla palvelluksi.

- Miten protokollapiirin laiteajuri on toteutettu?

  - Jonomainen lähetys aiheuttaa sen, että matalan prioriteetin sanoma estää korkeamman prioriteetin sanomaa pääsemästä väyläkilpaan.
  - Jonot voivat vuotaa yli; ainakin tuotekehityksen aikana tiedot näistä virhetilanteista pitäisi tallettaa muistiin (esimerkiksi vikalokiin).

- Jos jokaiselle sanomalle on varattu oma tietovarasto, seuraava sanoma saattaa tulla, ennen kuin vanha on ehditty lukea; usein tästä ei ole haittaa, mutta jos siitä on haittaa, tällainen virhetilanne kannattaa tallettaa vikalokiin ainakin tuotekehityksen aikana.
- Tarkista vastaanotettaessa pituustieto, ettei se ole suurempi kuin 8; muuten muisti saattaa korruptoitua, jos olet varannut kiinteän määrän tavuja muistista sanoman kopiolle olettaen, että sanoman pituus on enintään 8.

- Ota huomioon eri protokollapiirien erityisominaisuudet ja virheet.

  - Esim. 82527-piirin globaali maski vaikuttaa myös sanomien lähetykseen, vaikka sen pitäisi vaikuttaa ainoastaan vastaanottoon.
  - Missä järjestyksessä kaksiporttimuistia käyttävä protokollapiiri (FullCAN-tyyppi) lähettää sanomat väylälle, prioriteettijärjestyksessä vai siinä järjestyksessä, kuin ne ovat kaksiporttimuistissa ⇒ laita sanomat kaksiporttimuistiin prioriteettijärjestyksessä.
  - Tarkista, miten FullCAN-tyyppinen protokollapiiri reagoi tilanteeseen, jossa kyselykehyksen pituuskentän arvo on eri kuin protokollapiirille on ohjelmoitu.
  - Jos väylällä on CAN-spesifikaation versioita 1.0 tai 1.1 noudattavia piirejä (esim. 82C200- ja 82526-piirit), kaikilla solmuilla täytyy olla kideoskillaattorit, joten RC-oskillaattorilla käyviä SLIO (Serially Linked I/O) -piirejä ei voi tällaisessa verkossa käyttää.
  - Piirien 87C592 ja 87CE598 DMA-siirtoa käytettäessä on huomioitava, että DMA:n käynnistyksen jälkeisen käskyn on käytettävä kaksi kellojaksoa.

- Älä käytä samaa sanomatunnistenumeroa usealla solmulla;

  - sallittua, jos tietokentän pituus on nolla; muuten tapahtuu törmäys, jota CAN-protokolla ei hallitse.

- Pitäisikö jotkut (turvallisuuskriittiset) sanomat kuitata tai lähettää useamman kerran peräkkäin?

- Käytä solmuvalvontaa.

  - Jokin solmuista (esim. verkonhallintaisäntä) voidaan määrätä kiertokyselijäksi tai
  - solmut voivat kysellä läsnäoloa toisilta solmuilta.
  - Valvontaa ei tarvita, jos järjestelmässä käytetään periodisia sanomia jokaisella solmulla; jos sanoma lakkaa tulemasta, solmun voidaan päätellä poistuneen väylältä.

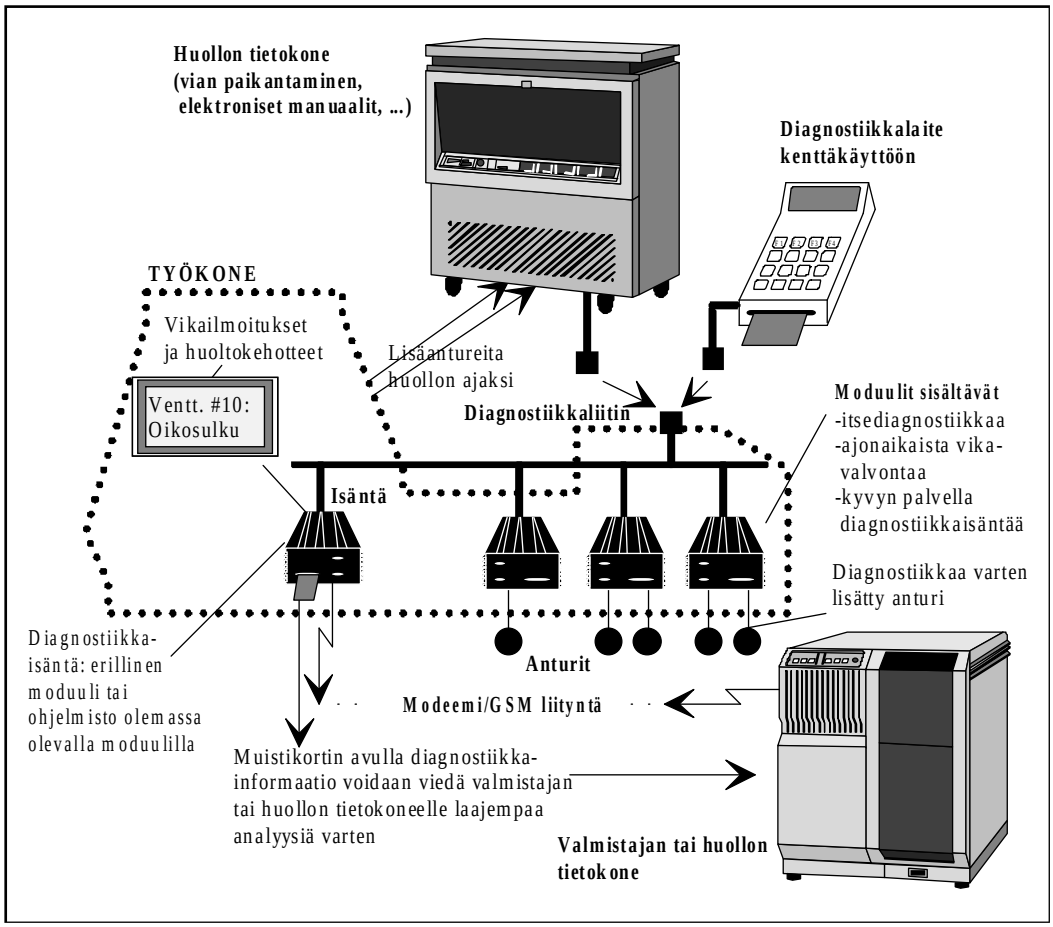
- Miten verkonhallintaisäntä reagoi, jos yksi solmuista uudelleenkäynnistyy yllättäen, tai miten orjasolmut reagoivat, jos verkonhallintaisäntä uudelleenkäynnistyy yllättäen?

- CAN-protokolla ei ole deterministinen.

- Maksimisiirtoviivettä ei voida taata kuin sanomalle, jonka tunnistenumero on nolla; on siis varmistauduttava muulla tavoin, että kaikki sanomat pääsevät väylälle ajoissa; vaihtoehtoja ovat esimerkiksi odotusaikojen käyttö, laskennallinen analyysi, aikajakoinen kommunikointi tai sanomaketjut.
- Uudelleenlähetykset aiheuttavat edeltä arvaamattomia kommunikointiviiveitä, ellei niiden määrää voida lukea protokollapiiriltä tai niitä ei voida kieltää.
- Sanomat voidaan aikaleimata, jos halutaan olla varmoja niiden ajallisuudesta.

4 DIAGNOSTIIKASTA APUA TURVALLISUUTEEN

Varsinkin kenttäväylätekniikassa turvallisuutta haetaan diagnostiikan avulla. Koska kenttälaitteet sisältävät älyä, ne voivat pitää tilastoa käyttötunneista ja käyttökerroista ja täten ilmoittaa operaattorille, jos on aika vaihtaa kyseinen laite tai sen osa. Tällaista ennakoivaa diagnostiikkaa kannattaa käyttää myös koneautomaation järjestelmissä. Käynnistyksen yhteydessä tehty itsediagnostiikka voi paljastaa vikoja, joiden seurauksena konetta ei voi turvallisesti käyttää. Ohjausjärjestelmä voi tällaisessa tapauksessa itse estää koneen käytön. Viat, jotka syntyvät toiminnan aikana, pyritään havaitsemaan jatkuvalla vikavalvonnalla. Vian esiintyessä ohjausjärjestelmä voi asettaa koneen turvalliseen tilaan. Jos jatkuva tila on järjestelmän ainoa turvallinen tila, ainoa tapa taata turvallisuus on lisätä järjestelmään redundanttisuutta, jonka avulla yksittäisen vian yli päästään. Vika voidaan hälyttää ja korjata siten vasta myöhemmin. Pelkällä diagnostiikalla ei siis saavuteta vikasietoisuutta, mutta sillä voidaan ehkäistä vikoja ja mahdollistaa turvallinen toiminta vikatapauksissa. Tässä luvussa esitellään joitakin diagnostiikkaan liittyviä yleisiä näkökohtia. Kuvassa 23 esitellään aluksi diagnostiikkajärjestelmän yleiskuva.



Kuva 23. Diagnostiikkajärjestelmän yleiskuva.

Kuvan 23 koneenohjausjärjestelmä koostuu neljästä CAN-solmusta, joista yksi solmu toimii isäntäsolmuna. Diagnostiikkajärjestelmä koostuu solmujen diagnos-

tiikkaominaisuuksista, diagnostiikkasolmusta (tai jollakin solmulla - esimerkiksi isäntäsolmulla - olevasta diagnostiikkataskista), kentälle mukaan otettavasta huoltolaitteesta, huollon diagnostiikkalaitteesta ja tehtaan tai huollon tietokoneesta. Ohjausjärjestelmä voi tehdä itsediagnostiikkaa joko ajonaikaisesti (on-line) tai kun kone on pysäytetty (off-line). Kattavaa itsediagnostiikkaa varten järjestelmään voidaan joutua lisäämään antureita, joita ei varsinaiseen koneenohjaukseen tarvittaisi. Huoltolaitteella voidaan diagnosoida järjestelmää CAN-solmujen kautta. Tällöin edellytetään, että solmut tarjoavat mittaus-, testaus- tai diagnostiikkapalveluja huoltolaitteelle. Näitä diagnostiikkapalveluja voidaan käyttää myös tehtaan tai huollon tietokoneelta esimerkiksi modeemiyhteyden kautta. Mittaus- ja vikatietoa voidaan välittää myös muistikortin avulla. Huollon diagnostiikkalaite on kentälle vietävää huoltolaitetta monipuolisempi; se voi sisältää kattavat elektroniset huoltokirjat ja vianhakuohjeet (tai automaattisen vianhaun) sekä antureita, joilla koneesta saadaan lisää diagnosointia helpottavaa tietoa.

4.1 MITÄ DIAGNOSOIDAAN, OHJAUSJÄRJESTELMÄÄ VAI KONETTA?

Kun työkonetta tai sen osajärjestelmiä ohjataan ohjausjärjestelmällä, tarvitaan joukko antureita, toimilaitteita, kaapeleita ja elektroniikkakortteja ohjelmistoineen. Tällaisessa ohjausjärjestelmässä esiintyy aina käytön aikana vikoja, joiden havaitsemista, paikantamista ja korjaamista varten järjestelmään lisätään diagnostiikkaominaisuuksia. Kokonaan toinen taso on varsinaisen koneen diagnostiikka, jota voidaan nimittää myös kunnonvalvonnaksi. Esimerkiksi, kun nykyaikaisen auton moottorin suihkutusjärjestelmässä tarvitaan happianturi, sitä lukevalla elektroniikkayksiköllä on diagnostiikkaa happianturia varten. Se ei kuitenkaan lisää auton diagnostiikkaominaisuuksia verrattuna vanhanaikaiseen autoon, jossa happianturia ei tarvita. Sen sijaan, jos kyseiseen autoon lisättäisiin renkaiden ilmanpainetta valvovat elektroniset venttiilinhatut, diagnostiikkaominaisuudet olisivat paremmat kuin vanhemmassa automallissa. Toisin sanoen, jotta nykyaikaisen tietotekniikkaan perustuvan ohjausjärjestelmän käytettävyys olisi yhtä hyvä kuin perinteisen, järjestelmässä täytyy olla diagnostiikkaa.

Varsinaista koneen diagnostiikkaa kutsutaan tässä siis kunnonvalvonnaksi. Kunnonvalvonta edellyttää usein sitä, että järjestelmään kytketään lisäantureita, joita ilmankin järjestelmä voisi toimia. Tämä lisää tietenkin kustannuksia ja voi työkoneiden yhteydessä olla este kunnonvalvonnan toteuttamiselle. Sen sijaan huoltopaikalla tällaista kunnonvalvontaa tai diagnostiikkaa voidaan tehdä. Tällöin huoltolaitteeseen kuuluu antureita, jotka asennetaan koneeseen huollon ajaksi. Seuraavassa esitellään joitakin mahdollisia kunnonvalvonnan kohteita:

-hydraulijärjestelmän paine
-hydrauliöljyn puhtaus
-hydraulipumpun värähtely (laakeriviat)
-hydraulijärjestelmän tukkoisuus
-voiteluöljyn paine, lämpötila ja pinnankorkeus
-jäähdytysveden lämpötila ja pinnankorkeus
-jarrujärjestelmän paine

-pakokaasun lämpötila
-polttoaineen pinnankorkeus ja virtausnopeus
-renkaiden ilmanpaine
-latausjännitteet, akkujen kunto.

Nämä ovat siis yksittäisen toimilaitteen, mekanismin tai järjestelmän osan kunnonvalvontaa. Kunnonvalvonnan yläpuolelle voidaan ajatella vielä yksi taso: prosessinvalvonta. Eli, vaikka kaikki osat olisivat kunnossa, järjestelmä ei välttämättä tuota sitä mitä sen pitäisi. Normaalisti tätä tasoa ei ajatella kuuluvaksi diagnostiikan piiriin. Kohdan 4.4 kuvassa 24 esitellään yksi tapa jakaa mekatroninen järjestelmä osiin tai tasoihin diagnosoinnin kannalta.

4.2 MISSÄ DIAGNOSTIIKKAFUNKTIOT SIJAITSEVAT, KONEESSA VAI ULKOPUOLISESSA DIAGNOSTIIKKALAITTEESSA?

Diagnostiikkaohjelmistot, elektroniset manuaalit, käyttäjäliityntä ja mahdolliset lisäanturit voidaan upottaa ohjausjärjestelmään (on-board-diagnostiikka) tai niitä varten voidaan tehdä erillinen, koneen ulkopuolinen testauslaite (off-board-diagnostiikka). On-board- ja off-board-diagnostiikka eivät ole vaihtoehtoisia toteutustapoja, vaan yleensä molempia joudutaan käyttämään yhdessä. Tärkeä kysymys on se, mihin vedetään raja, eli kuinka paljon diagnostiikkaominaisuuksia upotetaan koneeseen ja mitkä jätetään diagnostiikkalaitteeseen.

Erillinen diagnostiikkalaite voi olla kentälle mukaan otettava mikrotietokone tai huollossa oleva suurempi tietokone. Tällaisen diagnostiikkalaitteen tehtäviä ovat

- virhetietojen kuittaaminen
- talletettujen diagnostiikkatietojen lukeminen vikalokista
- parametritiedon lukeminen esim. antureilta
- arvojen kirjoittaminen esim. D/A-muuntimelle
- muistialueiden lukeminen
- muistialueille kirjoittaminen
- solmujen pysäyttäminen ja uudelleenkäynnistäminen yhdessä ja erikseen
- käskeminen suorittaa tarjolla olevia diagnostiikkaohjelmia
- toimilaitteiden komentaminen haluttuun tilaan
- päätöksenteko vian paikallistamiseksi
- kalibrointi
- toimiminen elektronisena manuaalina

(-uusien ohjelmaversioiden päivittäminen).

Usein käytetään termiä itsediagnostiikka. Itsediagnostiikka on osa on-board-diagnostiikkaa. Kaikki on-board-diagnostiikka ei välttämättä ole itsediagnostiikkaa, vaan osa on-board-diagnostiikasta on sellaista, joka aktivoituu ja voi toimia vasta, kun ulkopuolinen diagnostiikkalaite kytketään järjestelmään. Ehkä itsediagnostiikaksi voidaan määritellä koneen käyttäjästä tai huoltohenkilöstä riippumaton on-board-diagnostiikka.

4.3 MILLOIN DIAGNOSOIDAAN, AJONAIKAISESTI VAI KONEEN SEISOESSA?

Diagnostiikkaa voidaan tehdä ajonaikaisesti (on-line) tai kun kone on pysäytetty (off-line). Ajonaikainen diagnostiikka tai monitorointi paljastaa vikoja, joita ei koneen ollessa pysähdyksissä voida havaita. Ajonaikaista diagnostiikkatietoa voidaan tallettaa yhdessä aika- ja olosuhdetiedon kanssa vikalokiin, josta sitä voidaan myöhemmin tutkia joko käyttäjäliitynnän kautta tai erillisellä diagnostiikkalaitteella. Lokitietoa kannattaa ryhmitellä kriittisyyden mukaan, esimerkiksi seuraavasti:

1. kriittiset (turvallisuuskriittiset) viestit
2. järjestelmä rikkoutuu tai lakia rikotaan
3. järjestelmää ei voi enää käyttää tai se on käynnistettävä uudelleen
4. huoltokehotteet, varoitukset tai heikentynyt toiminta
5. pelkästään informatiiviset viestit.

Virheviestejä kannattaa suodattaa ainakin siten, että vain korkeamman prioriteetin viestit pääsevät kuljettajalle, jos useita virheitä esiintyy yhtä aikaa. Näin voidaan estää vikailmoitusten tulva. Suodatusta voi tehdä myös siten, että virhetilanteet lasketaan vioiksi vasta sitten, kun ne ovat voimassa riittävän pitkän ajan. Vikatietoa kannattaa myös kompressoida jotenkin, ettei yksi ja sama vika täytä koko lokia. Kompressointi voi yksinkertaisimmillaan olla sitä, että yksittäinen vika talletetaan lokiin vain kertaalleen. Tällöin siihen liitetään tieto, milloin ko. vika esiintyi ensimmäisen kerran, milloin viimeksi ja montako kertaa vika on esiintynyt yhteensä.

Lokitietoon voidaan liittää olosuhdetietona lämpötilatietoja, painetietoja, tieto järjestelmän tilasta tai tieto ohjelman kohdasta, missä virhe tapahtui, jne. Vikatietojen lisäksi lokiin voidaan tallettaa myös väärinkäytöstä kertovia viestejä, esimerkiksi tieto ylikierroksista tai ylinopeudesta.

Ajon aikana voidaan monitoroida kuljettajalle esimerkiksi anturitietoja. Monitorointi voi olla jatkuvaa tai vasta vikatilanteessa tapahtuvaa tai jossakin tietyssä järjestelmän tilassa (esim. diagnostiikkatilassa) tapahtuvaa.

On-line-diagnostiikkaa voidaan harrastaa myös siten, että kone on työssä kentällä ja samaan aikaan tehtaalla tai huollossa seurataan modeemin välityksellä lähetettyä diagnostiikkatietoa. Viallisen koneyksilön diagnostiikkaa voidaan tehostaa asentamalla ko. koneeseen lyhyeksi ajaksi diagnostiikkamoduuli, joka kykenee monipuolisempaan ajonaikaiseen diagnostiikkaan kuin vakiovarusteena oleva on-board-diagnostiikka.

Seuraavassa on luettelo joistakin mahdollisista on-line-diagnostiikan kohteista (Tripp & Hubby 1988):

- rekisterien tarkistus; kirjoitetaan tunnettu arvo rekisteriin ja luetaan se

- lisäprosessorin testi; lisäprosessorin annetaan suorittaa tehtävä, jonka tulosta verrataan oikeaan
- PROM-muistin tarkistussumma; PROM-muistin sisältö luetaan RAM-muistiin ja siitä lasketaan tarkistussumma
- paristotesti; paristoja voidaan hetkellisesti kuormittaa ja mitata kuormituksen aikainen jännite
- vahtikoirat; vahtikoira on ajastin, joka täytyy virkistää ohjelmallisesti tietyin väliajoin. Vahtikoira laukeaa, jos ohjelma on juuttunut. Jotkut vahtikoirat reagoivat myös liian taajaan tapahtuvaan virkistykseen, esimerkiksi jos ohjelma on jäänyt silmukkaan, jonka sisällä sattuu olemaan virkistyskomento
- kommunikointivirheet; havaitaan lisäämällä tarkistuskoodeja sanomiin
- semaforien lukkiutumisen testaus; varmistetaan, ettei mikään prosessi ole jättänyt semaforia päälle estäen näin muiden prosessien pääsyn semaforin kontrolloimalle resurssille
- pinojen, jonojen ja tietovarastojen (buffereiden) ylivuotojen ja alivuotojen valvonta
- lämpötilatestit; sopivista paikoista mitatut lämpötilat voivat paljastaa vikatilanteita
- RAM-muistin testaus; RAM-muistiin kirjoitetaan ja sieltä luetaan arvoja
- jännitesyöttöjen testaus; jännitelähteiden ulostuloja monitoroidaan
- arvot luetaan takaisin ennen suoritusta; esimerkiksi D/A-muuntimelle kirjoitettu arvo luetaan takaisin rekisteristä ja muunnos käynnistetään vain, jos arvo on sama kuin sinne kirjoitettu
- analogisten sisääntulojen itsekalibrointi; tunnettu analogia-arvo voidaan lukea säännöllisesti.

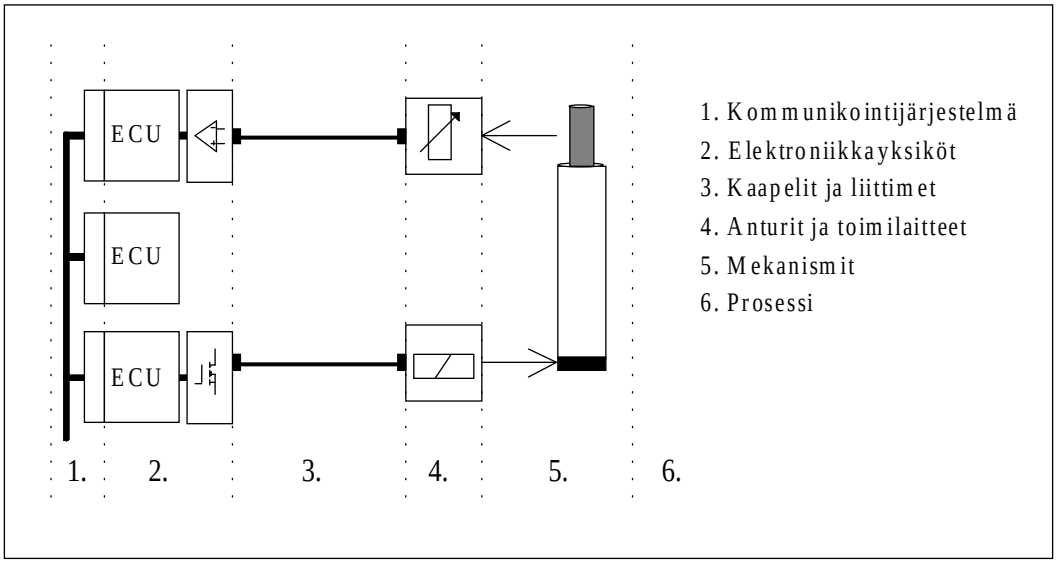
Off-line-diagnostiikkaa voidaan tehdä joko käyttäjäliitynnän avulla tai erillisellä diagnostiikkalaitteella. Käyttäjäliitynnässä olisi hyvä olla tällöin riittävät grafiikkaominaisuudet, että sillä voitaisiin näyttää manuaalisivuja ja kuvia koneenosista (elektroninen manuaali). Minimissään off-line-diagnostiikka voidaan toteuttaa yhdellä LED-lampulla, joka vilkuttaa vikalokiin kertyneet virhekoodit. Off-line-diagnostiikan pääpaino on kuitenkin huollossa, jossa voi olla monipuoliset diagnostiikkalaitteet. Tällaisissa laitteissa voi olla antureita, jotka kytketään koneeseen huollon ajaksi. Kattavat elektroniset manuaalit ja tietokoneavusteinen vian paikantaminen voidaan toteuttaa myös huollossa olevalla diagnostiikkalaitteella, jos sen ytimenä on riittävän suorituskykyinen tietokone.

4.4 DIAGNOSOINNIN KOHTEIDEN VALINTA

Diagnosoitaviksi kohteiksi kannattaa valita turvallisuuskriittiset 2 kohdetyyppiä, usein vikaantuvat kohteet ja kohteet, joiden vikaantuminen aiheuttaa suuria kus-

tannuksia. Jälkimmäisessä tapauksessa tarvitaan ennustavaa diagnostiikkaa. Kuvassa 24 on eräs jaottelu diagnosoinnin kohteista.

Lähteessä Hänninen et al. (1990) on tutkittu eri mekatronisten laitteiden vikaantumistilanteita. Työkoneista mukana olivat metsäkone ja kallionporauskone. Lähteen mukaan yli 70 % metsätyökoneen ja kallionporauskoneen vioista on anturi-, kaapeli- tai liitinvikoja, joten diagnostiikan pääpainon tulisi kohdistua niihin. Metsäkoneen toimilaitteissa oli yllättävän vähän vikoja (0 %); kallionporauskoneessa toimilaitevikoja oli 13 %. Autoelektroniikan puolella viat jakautuvat Zieghanin & Braunmillerin (1990) mukaan seuraavasti: 60 % kontaktit (sis. liittimet, johtimet, tiivisteet ja kotelon), 15 % toimilaitteet, 15 % anturit, 5 % juotokset ja passiiviset komponentit, 5 % aktiiviset osat (esim. mikroprosessori). Prosessori- tai muistipiiriviat näyttävät siis olevan harvinaisia sekä työkoneissa että autoissa. Aikaisemmin esitettyä listaa on-board-diagnostiikan kohteista tulisi siis painottaa enemmän anturi-, toimilaite- ja kaapelivikojen suuntaan.



Kuva 24. Diagnosoinnin kohteet.

Antureiden arvoja voi tarkkailla järkevyystestien avulla. Järkevyystesti voidaan tehdä yhdelle anturille tai useamman anturin kombinaatiolle. Yhden anturin arvon tulee normaalisti olla tietyllä alueella. Tämän alueen ulkopuolella voivat olla alueet alhainen arvo, korkea arvo, hälyttävän alhainen arvo, hälyttävän korkea arvo, alhaalla oleva viallinen arvo (esim. 0 V) ja ylhäällä oleva viallinen arvo (esim. käyttöjännite) (Kurki et al. 1991). Eräs tapa tarkkailla analogisten antureitten toimivuutta on tarkkailla A/D-muuntimelta luetun arvon vähiten merkitsevää bittiä; jos se on jatkuvasti nollatilassa tai ykköstilassa, anturijohdin tai anturi on ilmeisesti juuttunut johonkin kiinteään tilaan.

Toimilaitteiden diagnostiikka vaatii jonkinlaista takaisinkytkentää. Tämä asettaa vaatimuksia elektroniikkakytkennälle, ellei takaisinkytkentää saada järjestelmän antureiden ja rajakytkimien kautta. Nykyisin venttiilejä ohjataan älykkäillä tehopuolijohteilla, joissa on yleensä yksi ulostulo, josta saadaan diagnostiikkatietoa.

Tällaiset tehopuolijohteet paljastavat katkokset, oikosulut, ylijännitteet tai korkeat lämpötilat.

Ohjausjärjestelmässä voi esiintyä ohjelmavirheitä, jotka myös voidaan tallettaa vikalokiin. Ohjelmiston tulee olla tällöin toteutettu siten, että poikkeustilanteista palautetaan virhekoodi, joka sisältää esimerkiksi tiedon, mistä ohjelman moduulista tai muusta kohdasta virhe tuli ja mikä virhe on kyseessä. Virhekoodi voidaan sitten tallettaa vikalokiin yhdessä aika- ja olosuhdetiedon kanssa (esim. järjestelmän tila, taskien tilat). Ohjelmistovirheille kannattaa mahdollisesti järjestää oma loki.

CAN-kommunikointijärjestelmää on myös syytä diagnosoida. Tässäkin on oletettavaa, että suurin osa vioista tulee olemaan kaapeli- ja liitinvikoja. Tärkeimmät diagnosointimenetelmät ovat fyysisen väylän valvonta ja solmuvalvonta. Näitä käsiteltiin aikaisemmin luvussa 3. Myös kommunikointiohjelmisto voi tallettaa vikalokiin vikatietoja esimerkiksi seuraavista tapahtumista:

- protokollapiiri havaitsee paljon vikoja (bus off -warning)
- protokollapiiri on poistunut väylältä (bus off)
- protokollapiiri hukkasi sanoman (overrun)
- lähetys- tai vastaanottojonon tai -tietovaraston ylivuoto
- aikarajojen ylitykset (time out) esim. lohkosiirrossa.

Näistä varsinkin kolme viimeistä on sellaista, joiden esiintyminen johtuu huonosta suunnittelusta, joten tällaisten vikatapahtumien tallettaminen vikalokiin auttaa ohjelmoijia löytämään suunnitteluvirheitä tuotekehitysvaiheessa.

Kommunikointiväylä tukee erityisen hyvin off-board-diagnostiikkaa, koska väylä parantaa järjestelmän sisäistä näkyvyyttä eli väylän kautta voidaan diagnostiikkalaitteen avulla lukea esimerkiksi eri solmujen muistialueita tai A/D-muuntimia tai komentaa ulostuloja, kuten venttiililähtöjä tai D/A-muuntimia. Tämä edellyttää tietenkin, että tällaisia diagnostiikkalaitetta palvelevia funktioita on solmuille toteutettu. Järjestelmän sisäistä näkyvyyttä voidaan parantaa myös sillä, että käytetään hyväksi CAN-protokollan tarjoamaa kyselypalvelua. Tällöin kaikille diagnostiikkaa kiinnostaville sanomille varataan oma tietovarasto, josta diagnostiikkalaite voi noutaa viimeisimmän lähetetyn sanoman CAN-kyselykehyksen avulla. Tapahtumasanomia pyydettäessä täytyy huomata, että muut solmut tulkitsevat vastauksen kyselyyn tavalliseksi tapahtumaksi.

4.5 VIAN PAIKANTAMINEN

Vian paikantaminen on proseduuri, jonka avulla pyritään löytämään varsinainen vian aiheuttaja. Esimerkiksi anturitiedon vääristyminen voi johtua anturin vioittumisesta, liittimen viasta, kaapelin rikkoutumisesta tai elektroniikkaviasta. Vian paikantamiseksi diagnostiikalla täytyy olla tietoa järjestelmästä ja sen käyttäytymisestä normaalitilanteessa ja vikatilanteissa. Lähteessä Kurki et al**.** **(**1991) on esitelty eri menetelmiä vikadiagnostiikkatietämyksen esitystavoista. Tässä ne ainoastaan luetellaan:

- numeeriset menetelmät; järjestelmästä tai sen osasta on numeerinen malli
- tietämystekniset menetelmät:
  - assosiatiivinen; linkittää oireet suoraan vikoihin
  - abduktiivinen; hyödyntää tietämystä viallisesta käyttäytymisestä yhdistettynä vian levittäytymiseen liittyvään tietämykseen
  - case-pohjainen; käyttää tietämystä aikaisemmista tapauksista
  - mallipohjainen; käyttää tietämystä järjestelmän oikeasta käyttäytymisestä
- sumea logiikka
- temporaalilogiikka.

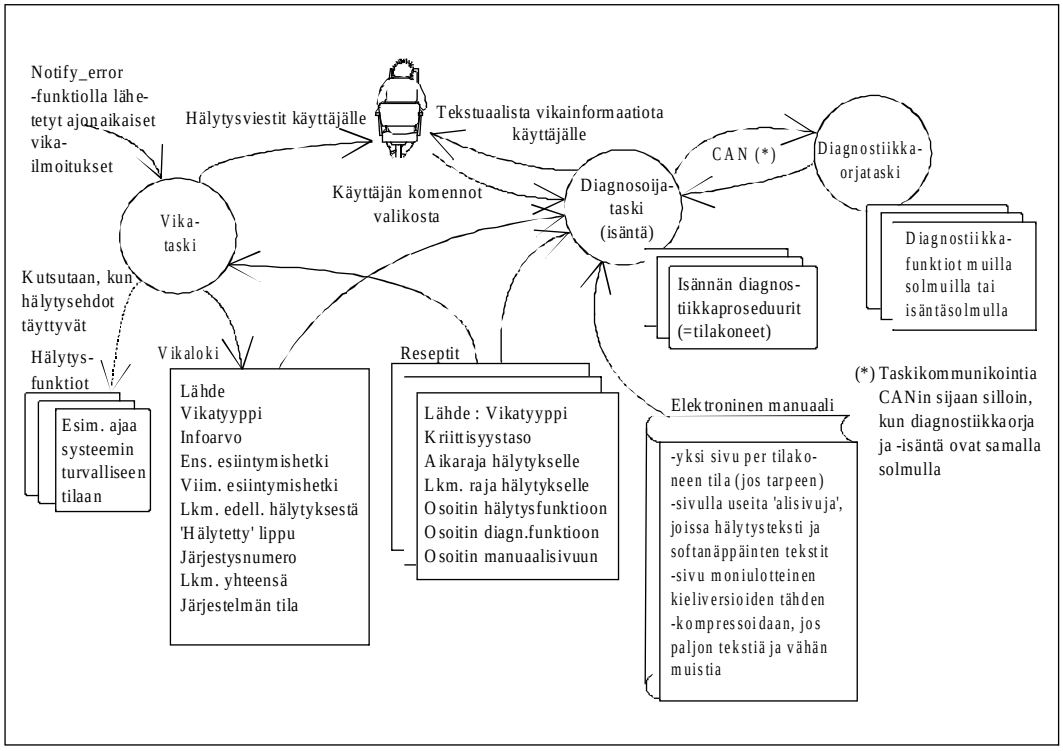
Nämä menetelmät eivät liity pelkästään vian paikantamiseen vaan myös vikojen havaitsemiseen. Näistä menetelmistä yksinkertaisin, vanhanaikaisin ja käytetyin on assosiatiivinen tietämyksen esitystapa, jossa "... ratkaisu kuvataan sääntökantojen, vikapuiden tai vikahakemistojen avulla... Haluttaessa toteuttaa nopeasti pieni järjestelmä, sääntöpohjaiset järjestelmät tarjoavat hyvän tietämyksen esitystavan. Tällöin sovelluksen on oltava kuitenkin sellainen, ettei myöskään ylläpitovaiheessa sääntökannat paisu liian suuriksi" (Kurki et al**.** 1991). Esimerkkejä tällaisesta ovat autojen tai muiden koneiden käyttöohjekirjojen vianhakukaaviot. Käyttöohjekirja voisi olla myös elektronisessa muodossa joko järjestelmän jollakin solmulla tai ulkopuolisessa diagnostiikkalaitteessa. Tällöin vianhakukaaviota edettäisiin syöttämällä ‘KYLLÄ’ tai ‘EI’ diagnostiikkaohjelman esittämiin kysymyksiin. Osan mittauksista ja haarautumisista mittausten perusteella diagnostiikkaohjelma voisi tehdä myös itse.

4.6 ESIMERKKI DIAGNOSTIIKKA-ARKKITEHTUURISTA

Tässä kohdassa esitellään eräs diagnostiikka-arkkitehtuuri, joka sopii CAN-väylää käyttävään koneenohjausjärjestelmään. Kyseinen diagnostiikka-arkkitehtuuri on suunniteltu Teknologian kehittämiskeskuksen (TEKESin) ja VTT:n tutkimushankkeessa *Liikkuvien työkoneiden ohjausohjelmistojen komponentointi ja kokoaminen* (LOKKI).

Peruslähtökohtana on se, että yksi solmu valitaan diagnostiikkaisännäksi[11]. Kuvassa 25 esitellään diagnostiikkaohjelmiston rakenne diagnostiikkaisännällä.

[11] Jos mahdollista, kannattaa valita solmu, jolla on näyttö. Tällöin koneen käyttäjälle voidaan antaa vikailmoituksia ja ohjeita, vaikka kommunikointiyhteys katkeaisi.



Kuva Y. Diagnostiikkaohjelmiston rakenne diagnostiikkaisännällä.

Diagnostiikkaisännän tehtäviä ovat

-vikalokin ylläpito
-hälytysten anto
-diagnostiikkaproseduurien ajo
-elektronisen manuaalin säilytys.

Diagnostiikkaisännällä on seuraavat kaksi taskia (muiden sovellustaskien lisäksi): vikataski ja diagnosoijataski. Vikataski ottaa vastaan järjestelmästä tulevat vikailmoitukset ja tallettaa ne vikalokiin. Vikailmoitukset tulevat CAN-väylän kautta tai diagnostiikkaisännän muilta taskeilta. Diagnosoijataski aktivoituu vasta, kun koneen käyttäjä aloittaa koneen diagnosoinnin käyttäjäliitynnän välityksellä.

Kaikilla orjasolmuilla on diagnostiikkaorjataski, joka ajaa diagnostiikkaisännän tai ulkopuolisen diagnostiikkalaitteen käskemät diagnostiikkafunktiot. Myös diagnostiikkaisännällä on oma diagnostiikkaorjataski, jota diagnosoijataski komentaa taskien välisen kommunikointimekanismien kautta ilman CAN-väylää. Myös ulkopuolinen diagnostiikkalaite voi komentaa diagnostiikkaisännän diagnostiikkaorjataskia.

4.6.1 Vikataski, vikaloki ja reseptit

Järjestelmän lähettämät viat pannaan vikataskin postilaatikkoon, josta vikataski tallettaa niitä vikalokiin. Järjestelmästä tulleessa vikaviestissä on tieto vikalähteestä ja vian tyypistä. Lisäksi vikoihin voi olla liitettynä neljän tavun mittainen informaatioarvo, jonka tulkinta on vikakohtaista; se voi olla esimerkiksi lämpötila-arvo, joka aiheutti ko. hälytyksen. Vikataski liittää näihin tietoihin kellonajan ja kyseisen vian esiintymiskertojen lukumäärän sekä järjestelmän senhetkisen tilan numeron. Vikaan liitetään myös vian järjestysnumero, jota käytetään hyväksi, kun halutaan säilyttää tapahtumajärjestys vikoja tulostettaessa; pelkkä kellonaika ei riitä, koska resoluutio on yksi sekunti ja viat eivät mene vikalokiin peräkkäin, vaan vikalokissa voi olla vapaita paikkoja siellä täällä riippuen siitä, kuinka koneen käyttäjä on niitä kuittaillut. Hälytysehtojen täyttyessä vika leimataan hälytetyksi.

Taulukko K. Vikalokin yhden vikarivin sisältö.

TALLETETTAVA PARAMETRI	TYYPPI	KUVAUS
Solmun numero	Uns Char	Vian lähettäneen solmun numero.
Komponentin numero	Uns Char	Vian aiheuttaneen komponentin numero (voi olla ohjelmistokomponentti tai laitekomponentti).
Vikatyyppi	Uns Int	Numero, joka kertoo vian tyypin, esim. 'oikosulku'.
Info-arvo	Long Int	Vikakohtaista tietoa, esim. lämpötila-arvo, joka aiheutti hälytyksen.
Ensimmäinen esiintymishetki	Long Int	Pvm. ja kellonaika, jolloin vika esiintyi ensimmäisen kerran (sekunneissa).
Viimeisimmän vian esiintymishetki	Long Int	Pvm. ja kellonaika, jolloin vika esiintyi viimeksi (sekunneissa).
Lukumäärä edellisestä hälytyksestä	Uns Int	Ko. vian lukumäärä viimeksi annetun hälytyksen jälkeen.
Hälytysindikaattori	Uns Char	Ilmoittaa, onko ko. vika hälytetty.
Järjestysnumero	Uns Long Int	Ilmoittaa, monesko vika tämä oli kaiken kaikkiaan.
Lukumäärä	Uns Int	Ko. vian esiintymiskertojen lukumäärä.
Järjestelmän tila	Uns Char	Järjestelmän tila (moodi) yhdellä numerolla kuvattuna (esim. 'säätämässä').

Vikaloki on kiinteän mittainen taulukko, joka sijaitsee haihtumattomassa muistissa (tai vaihtoehtoisesti tietokannassa massamuistissa). Jos sama vika[12] tulee useamman kerran, sitä ei talleteta uudelle riville, vaan ainoastaan informaatioarvo, viimeisimmän vian kellonaika, ko. vian esiintymiskertojen lukumäärät, järjestelmän tilan numero ja järjestysnumero päivitetään. Tällä tavalla vikatietoa saadaan kompressoitua, jolloin yksi vika ei pääse täyttämään lokia. Haittapuolena on, että informaatioarvo ja tilatieto sekä järjestysnumero tallettuu vain viimeisen vian osalta. Samoin kellonajoista tallella ovat ainoastaan ko. vian ensimmäinen ja viimeisin esiintymishetki. Vikalokin yhden rivin (tietueen) sisältö on kuvattuna taulukossa 11.

Ohjelmistovirheet ja laiteviat erotellaan toisistaan komponentin numerokoodin perusteella: jos koodin eniten merkitsevä bitti on 0, kyseessä on ohjelmistokomponentti, muutoin laitekomponentti. Ohjelmistovirheet ja laiteviat talletetaan eri lokiin tai samaan lokiin siten, että ohjelmistovirheet käyttävät lokin parilliset rivit ja laiteviat parittomat. Kun ohjelmistovirheet ja laiteviat on eroteltu näin, ohjelmistovirheet eivät pääse viemään tilaa laitevioilta. Ohjelmistovirheitä ei ole tarkoitus näyttää koneen käyttäjälle, vaan ne näytetään ainoastaan huoltohenkilökunnalle salasanan tms. kautta.

Kun vikataski on tallettanut vian lokiin, se etsii vikaa vastaavan reseptin (taulukko 12) reseptitietokannasta ja lähettää koneen käyttäjälle hälytyksen, jos reseptissä sitä vaaditaan. Reseptissä on aikaraja ja lukumääräraja vialle; hälytys annetaan, jos edellisen ja tämän vian väliaika on pienempi kuin aikaraja **JA** ko. vian lukumäärä edellisen hälytyksen jälkeen on suurempi tai yhtä suuri kuin lukumääräraja **TAI** kun vika on turvallisuuskriittinen. Koneen käyttäjälle lähetettävä hälytysteksti haetaan elektronisesta manuaalista. Samalla vikataski käynnistää reseptin määräämän hälytysfunktion. Hälytysfunktio voi esimerkiksi ajaa koneen turvalliseen tilaan ja antaa sopivan äänimerkin. Samanaikaisesti hälytysindikaattorikenttään laitetaan leima: ‘HÄLYTETTY’ sekä nollataan ‘lukumäärä edellisestä hälytyksestä’ -kenttä. Hälytysfunktiolle välitetään ainakin seuraavat parametrit: virheen lähde (solmu ja komponentti), vian tyyppi ja info-arvo.

Jokaista vikaa kohden kirjoitetaan resepti (samasta lähteestä tuleville vikailmoituksille voidaan käyttää myös yhteistä reseptiä). Reseptin kirjoittaa systeemisuunnittelija. Reseptiä käyttää vikataskin lisäksi diagnosoijataski. Se muuntaa vikalokin koodi-informaation tekstuaaliseksi informaatioksi katsomalla reseptistä vikaa vastaavan manuaalisivun osoitteen. Samoin se löytää reseptistä vikaa vastaavan diagnostiikkafunktion osoitteen ja ajaa kyseisen diagnostiikkafunktion, jos käyttäjä niin valitsee.

[12] Vika on sama, jos se tulee samasta solmu- ja komponenttilähteestä ja sen vikatyppi on sama.

Taulukko L. Vikareseptin sisältö.

RESEPTIN PARAMETRI	TYYPPI	KUVAUS
Solmun numero	Uns Char	Nämä kolme ensimmäistä parametria muodostavat yhdessä indeksin eli reseptin numeron, jonka perusteella oikea resepti löydetään. (Virheen tyyppi: FFFFH = yhteinen resepti tästä lähteestä tuleville vioille.)
Komponentin numero	Uns Char	
Virheen tyyppi	Uns Int	
Kriittisyystaso	Uns Char	1. kriittinen, 2. sääntörike, 3. rikkoutuminen, 4. häiriö, 5. varoitus, 6. info.
Aikaraja	Long Int	Jos tämän vian kahden perättäisen esiintymän välinen aika on pienempi tai yhtä suuri kuin 'Aikaraja', viasta lähetetään hälytys, **jos** 'Lukumääräraja' toteutuu (-1 = Ei koskaan, 7FFFFFFFH = Ei aikarajaa).
Lukumääräraja	Uns Int	Jos tämän vian lukumäärä edellisestä hälytyksestä on suurempi tai yhtä suuri kuin tämä parametri kertoo, viasta lähetetään hälytys (0 tai 1 = Ei lukumäärärajaa).
Hälytysfunktion osoite	Pointer	Osoitin hälytysfunktioon, joka pitää suorittaa, kun hälytys tulee (NULL = ei hälytysfunktiota).
Diagnostiikkaproseduurin osoite	Pointer	Osoitin diagnostiikkaproseduuriin, joka käynnistetään koneen käyttäjän toimesta valikon kautta lähdettäessä diagnosoimaan tätä vikaa (NULL = ei diagnostiikkaproseduuria).
Manuaalisivun osoite	Pointer	Osoitin ko. vikaan liittyvään manuaalisivuun (NULL = Ei manuaalisivua).

Vialle voidaan reseptissä määritellä kuusi kriittisyystasoa. Kriittisyystasoarvoa voidaan käyttää kutsuttaessa hälytysfunktiota esimerkiksi antamaan erilaisia äänimerkkejä eritasoisille vioille. Informatiivisten viestien lähetystä voidaan viivästää sopivaan ajanhetkeen, esimerkiksi käynnistyshetkeen. Kriittisyystasot ovat taulukon 13 mukaiset.

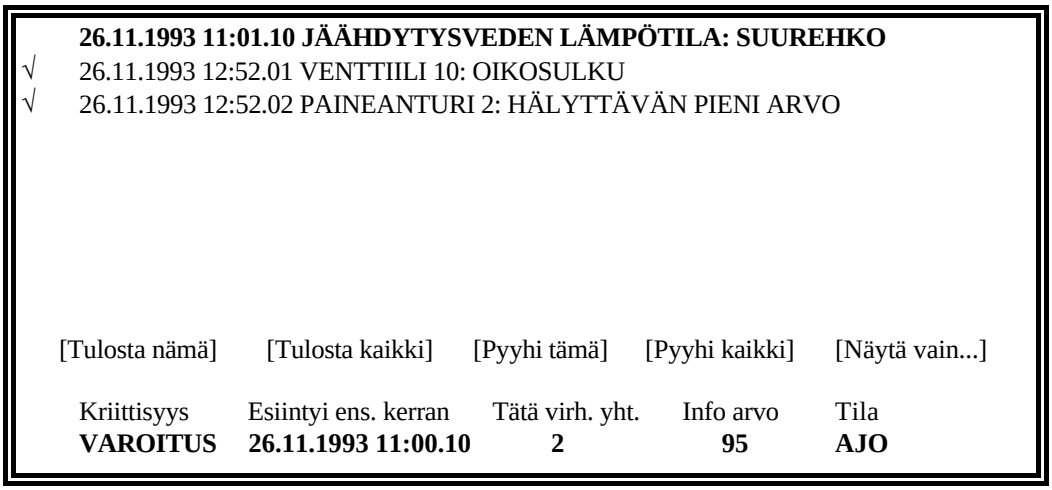
Taulukko M. Vikojen kriittisyystasot.

KRIITTISYYSTASO	KUVAUS
1. Turvallisuuskriittiset	Henkilövahinkoja voi syntyä, jos tätä vikaa ei korjata. Järjestelmän on mentävä turvalliseen tilaan välittömästi.
2. Sääntöjä tai lakia rikotaan	Sääntöjä, lakia tai sopimuksia tai prosessiohjetta rikotaan, esimerkiksi kone tuottaa pahasti vääränlaista tavaraa, jos tätä vikaa ei korjata.
3. Rikkoutuminen	Koneen osa on rikkoutunut tai on rikkoutumassa; vika on korjattava ennen kuin konetta voidaan jälleen käyttää.
4. Häiriö	Koneen käyttöä ei voi nyt jatkaa, mutta pie-nen tarkistuksen ja/tai uudelleenkäynnistyksen jälkeen käyttö voi jatkua.
5. Varoitus	Ominaisuudet ovat huonontuneet tai kalibrointia tarvitaan. Konetta voi vielä käyttää, mutta huoltoa tai kalibrointia suositellaan.
6. Informatiivinen	Pelkästään informatiivista viestiä; ei vikaa järjestelmässä. Esimerkiksi kehotteet määräaikaishuoltoon.

4.6.2 Diagnosoijataskin tehtävät

Diagnosoijataski aktivoituu, kun käyttäjä valitsee päävalikosta diagnostiikkatoiminnon. Sen jälkeen diagnosoijataski on valmiina vastaanottamaan käyttäjältä tulevia diagnostiikkakomentoja, joita kuljettaja valitsee diagnostiikkavalikosta.

Yksi diagnostiikkavalikon ikoneista on VIKALOKI-ikoni, joka käynnistää vikalokin tietojen prosessoimisen tekstuaaliseen muotoon ja lähettää lokirivit tekstinä näyttöön. Lokirivin teksti haetaan elektronisen manuaalin ensimmäiseltä riviltä. Lokinäyttö voi sisältää kuvan 26 mukaisia asioita (√-merkki tarkoittaa, että viasta on lähetetty hälytys):

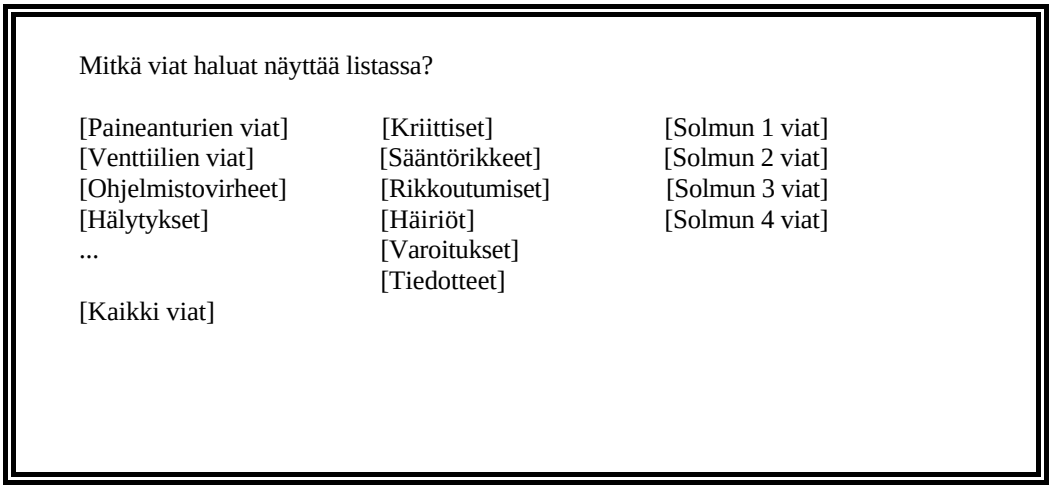


Kuva 26. Lokinäyttö.

Viat on järjestetty esiintymisjärjestykseen viimeisen esiintymiskerran mukaan. Koneen käyttäjä voi liikkua listassa ylös ja alas. Lisätietoa kohdistimen osoittamasta viasta näytetään näytön alaosassa. Jos hän valitsee jonkin vian, diagnosoijataski lähettää kyseiseen vikaan liittyvän manuaalisivun näyttöön. Manuaalisivussa kerrotaan vikaan liittyvää tietoa ja annetaan ohjeita vian korjaamiseksi. Jos vikaa varten on olemassa vianhakuproseduuri, koneen käyttäjä voi käynnistää sen painamalla sopivaa näppäintä tai ikonia. Tällöin diagnosoijataski etsii reseptistä vikaan liittyvän diagnostiikkaproseduurin alkuosoitteen ja lähtee suorittamaan diagnostiikkaproseduuria. Diagnostiikkaproseduurille välitetään vikaan liittyvät parametrit (virheen lähde, tyyppi ja info), jotka luetaan vikalokista. Diagnostiikkaproseduurin aikana diagnostiikkafunktiot voivat lähettää näyttöön uusia manuaalisivuja, joissa voi olla kysymyksiä käyttäjälle, esimerkiksi: 'Mitä koneen lämpömittari näyttää, < 90°C, paina F1; ≥ 90°C, paina F2'. Kysymyksiin vastataan painamalla manuaalisivun kehoittamaa näppäintä. Tämä voidaan toteuttaa esimerkiksi kuudella pehmonäppäimellä, jotka ilmestyvät ruudun alaosaan aina, kun manuaalisivu lähetetään näyttöön. Pehmonäppäimien tekstit voisivat olla esim.: [OK], [PERUUTA], [F1], [F2], [F3], [F4], tai ne voitaisiin lukea kulloiseltakin manuaalisivulta, eli edellä esitetyssä esimerkissä ne olisivat: [<90°C], [≥90°C], [ ], [ ], [ ], [PERUUTA].

Diagnostiikkaproseduurit voidaan toteuttaa esimerkiksi tilakoneena, jonka seuraava tila riippuu diagnostiikkaorjataskin suorittaman diagnostiikkafunktion vasteesta tai käyttäjän vastauksesta. Jokaiseen tilaan liittyy oma manuaalisivu näppäinteksteineen.

Käyttäjä voi myös suodattaa vikalokitulostusta [Näytä vain...] -ikonin alla olevasta valikosta. Valikko voisi sisältää pääpiirteissään kuvassa 27 mainittuja asioita.



Kuva 27. Vikalokitulostuksen suodatusvalikko.

Kun käyttäjä tulee vikalokitulostukseen, mitään suodatuksia ei ole silloin päällä, riippumatta aikaisemmista suodatusasetuksista. Eihän voida olettaa, että käyttäjä muistaa, että suodatuksia on päällä, ja siksi vikaloki voisi näyttää täysin tyhjältä, vaikka siellä olisikin vikoja. Nyt jos käyttäjä menee [Näytä vain...] -valikkoon, siellä on vanhat asetukset tallella, joten jos ne ovat oikein, hänen tarvitsee vain palata takaisin, niin suodatukset menevät päälle. Jos käyttäjä haluaa valita 'kaikki muut paitsi ...' -tyyppisesti, hän voi valita [Kaikki viat] ja sen jälkeen poistaa yksitellen ne, joita hän ei halua näytettävään listaan.

Käyttäjä voi tulostaa kirjoittimelle joko kaikki vikalokin viat ([Tulosta kaikki]) tai ainoastaan näytössä näkyvät viat ([Tulosta näkyvät]). Hän voi pyyhkiä joko koko vikalokin ([Pyyhi kaikki]) tai sen vian, johon kursori osoittaa ([Pyyhi tämä]). Ohjelmistovikoja ei näytetä kuin huoltohenkilökunnalle salasanan kautta.

Edellä on kuvattu, mitä tapahtuu VIKALOKI-ikonin takaa. Diagnostiikkaa täytyy voida tehdä myös silloin, kun vikoja ei ole tullut yhtään. VIKALOKI-ikonin takaa voidaan lähteä diagnosoimaan vain niitä koneen osia, joista on tullut vikailmoitus. Siksi diagnostiikkavalikossa tulee olla muitakin ikoneita, joista voidaan käynnistää sopivien kohteiden diagnosointi. Diagnostiikkaproseduurit ovat pääosin samat kuin VIKALOKI-tapauksessakin, mutta vianhakupuun alkuun päästään nyt suoraan ikonista.

4.6.3 Diagnostiikkaorjataskin tehtävät

Diagnostiikkaorjataski tekee diagnosoijataskin tai ulkopuolisen diagnostiikkalaitteen pyytämät mittaukset tai muut toimenpiteet. Diagnostiikkaorjataski omistaa joukon yleisiä diagnostiikkafunktioita ja joukon sovelluskohtaisia diagnostiikkafunktioita. Tässä määritellään joukko yleisiä diagnostiikka- tai testaus (debuggaus) -funktioita, joista eri solmuille valitaan sopiva osajoukko. Yleiset diagnostiikkafunktiot jaetaan selvyyden vuoksi seitsemään eri ryhmään: **ryhmä 1** solmun hallintaan, **ryhmä 2** muistioperaatiot, **ryhmä 3** I/O-rekisterioperaatiot, **ryhmä 4** ajastinoperaatiot, **ryhmä 5** sarjaliikennetoiminnot, **ryhmä 6** anturi- ja toimilaitetoiminnot ja **ryhmä 7** sovelluskohtaiset ja kehittyneemmät diagnostiikkafunktiot. Ehdotus yleisiksi diagnostiikkafunktioiksi voisi olla seuraavanlainen:

Ryhmä 1

PYSÄYTÄ JA OTA YHTEYS SOLMUUN
PYSÄYTÄ SOLMU
OTA YHTEYS SOLMUUN
KATKAISE YHT. JA KÄYNN. SOLMU
KATKAISE YHTEYS
KÄYNNISTÄ SOLMU
NOLLAA (reset) SOLMU
AJA ITSEDIAGNOSTIIKKA
NÄYTÄ TILA
NÄYTÄ VERSIO

Ryhmä 2

KIRJOITA TAVU
KIRJOITA SANA
ASETA KIRJOITUSOSOITE
KIRJOITA MUISTIIN
LOPETA MUISTIIN KIRJOITUS
NÄYTÄ KIRJOITUSOSOITE
LUE TAVU TAI SANA
ASETA LUKUOSOITE
LUE MUISTISTA
LOPETA MUISTISTA LUKU
NÄYTÄ LUKUOSOITE
KIRJOITA JA LUE MUISTIA (verify)
LASKE MUISTIN TARKISTUSSUMMA
KOPIOI MUISTIA
TÄYTÄ MUISTIA

Ryhmä 3

KIRJOITA I/O-PORTTIIN
LUE I/O-PORTISTA
LUE A/D-KANAVA
TESTAA A/D-KANAVA
KIRJOITA D/A-KANAVAAN

Ryhmä 4

PYSÄYTÄ AJASTIN
NOLLAA AJASTIN
ASETA AJASTIN
KÄYNNISTÄ AJASTIN
LUE AJASTIN
LUE REAALIAIKAKELLON AIKA
ASETA REAALIAIKAKELLON AIKA
LUE TAAJUUS
LÄHETÄ TAAJUUS

Ryhmä 5

LUE SIIRTONOPEUS
ASETA SIIRTONOPEUS
LÄHETÄ MERKKI
LUE MERKKI
LUE CAN-VIRHELASKURIT
NÄYTÄ CAN-LÄH.JONON PITUUS
NÄYTÄ CAN-VAST.OTTOJONON PIT.

Ryhmä 6

KIRJOITA DIGITAALISEEN LÄHTÖÖN
LUE DIGITAALISESTA TULOSTA
LUE ANTURIN ARVO
TESTAA ANTURI
NÄYTÄ VENTTIILIN TILA
AVAA VENTTIILI
SULJE VENTTIILI
TESTAA VENTTIILI
RYHMITÄ VENTTIILEJÄ
ASETA PROPOVENT. PAIKKA (ABS.)
ASETA PROPOVENT. PAIKKA (SUHT.)
ASETA MOOTORIN PAIKKA (ABS.)
ASETA MOOTORIN PAIKKA (SUHT.)
AJA MOOTTORIA n KIERROSTA

Ryhmä 7

AJA DIAGNOSTIIKKAFUNKTIO NRO N

Ryhmän 6 funktiot poikkeavat ryhmän 3 funktioista seuraavasti: esimerkiksi luettaessa anturin arvoa, se voidaan tehdä joko funktiolla LUE A/D-KANAVA tai funktiolla LUE ANTURIN ARVO. Näistä edellinen lukee suoraan A/D-muuntimen raa'an arvon, kun taas jälkimmäinen skaalaa raa'asta arvosta todellisen anturisignaalin arvon. Eli ryhmän 6 funktiot eivät kirjoita suoraan I/O-porttiin tai lähetä suoraan I/O-portista lukemaansa arvoa. Seuraavassa on esimerkki LUE A/D-KANAVA -funktion spesifikaatiosta.

FUNKTIO: **LUE A/D-kanava**

Kuvaus: Lukee sanan A/D-muuntimelta halutulta kanavalta. Jos 'näytteiden määrä' on suurempi kuin 1, otetaan keskiarvo.

KOMENTO:

Tavu 0: Komennon numero = 66
Tavu 1: Kohdeosoite (orjasolmun numero)
Tavu 2: Kanavan numero
Tavu 3: (Varattu)
Tavu 4: Näytteiden määrä; vähiten merkitsevä tavu
Tavu 5: Näytteiden määrä; eniten merkitsevä tavu
Tavu 6: Näytteiden välinen aika; vähiten merkitsevä tavu (10 μs askelein)
Tavu 7: Näytteiden välinen aika; eniten merkitsevä tavu

KUITTAUS:

Tavu 0: Tila: 0 = OK, 1 = komento tuntematon, 11 = kanava tuntematon
Tavu 1: Kohdeosoite (solmun numero; diagnostiikkaisäntä tai diagnostiikkalaite)
Tavu 2: Luetun arvon tai keskiarvon vähiten merkitsevä tavu
Tavu 3: Luetun arvon tai keskiarvon eniten merkitsevä tavu
Tavu 4: Näytteistä pienimmän arvo; vähiten merkitsevä tavu
Tavu 5: Näytteistä pienimmän arvo; eniten merkitsevä tavu
Tavu 6: Näytteistä suurimman arvo; vähiten merkitsevä. tavu
Tavu 7: Näytteistä suurimman arvo; eniten merkitsevä tavu

HUOMIOITA:

1) Palauttaa myös pienimmän ja suurimman arvon.
2) Jos näytteiden määräksi asetetaan 0, luetaan aiemmin talletetut arvot.
3) Jos näytteiden väliseksi ajaksi asetetaan 0, aikaväliin ei tarvitse kiinnittää huomiota, vaan se saa olla, mitä se sattuu olemaan.

4.6.4 Diagnostiikkaisännän ja diagnostiikkaorjataskin välinen protokolla

Jokaisella solmulla ja ulkopuolisella diagnostiikkalaitteella on oma CAN-objekti diagnostiikkaa varten. Diagnostiikkaisäntänä on diagnosoijataski tai ulkopuolinen diagnostiikkalaite. Diagnostiikkaorjana voi olla jokainen solmu, myös se, joka toimii diagnostiikkaisäntänä. Ulkopuolinen diagnostiikkalaite kytketään CAN-väylään.

Diagnostiikkaisäntä lähettää diagnostiikkakomennon CAN-väylälle käyttäen siihen varattua CAN-objektia. Ensimmäinen tietotavu kertoo suoritettavan komennon numeron ja toinen tietotavu kertoo alisolmun numeron, jolle komento lähetetään. Alisolmu vastaa omalla CAN-objektillaan. Ensimmäinen tietotavu kertoo komennon onnistumisesta: '0' tarkoittaa aina, että komennon suoritus on onnistunut, ja '1' tarkoittaa aina, että kyseistä komentoa ei tueta; muut arvot riippuvat suoritettavasta komennosta. Kuittauksen toinen tavu sisältää solmun numeron, jolle kuittaus lähetetään, diagnostiikkalaitteelle vai diagnosoijataskille. Muiden tavujen merkitys sekä komennossa että kuittauksessa riippuu komennosta.

Jos diagnosoijataski lähettää diagnostiikkakomennon sille solmulle, jolla se itse sijaitsee, komento lähetetään diagnostiikkaorjataskin postilaatikkoon samassa muodossa kuin CAN-objektitkin. Kyseinen isäntäsolmu voi käyttää samaa CAN-objektia sekä komentojen lähettämiseen orjasolmuille että kuittausten lähettämiseen ulkopuoliselle diagnostiikkalaitteelle, koska kohdenumero paljastaa, onko kyseessä isäntäsolmun lähettämä komento vai kuittaus. Tällöin diagnostiikkalaitteella täytyy tietenkin olla oma solmunumero.

Seuraavassa esitetään diagnostiikkasanomien (CAN-kehyksen) muoto (numerot suluissa viittaavat CAN-kehyksen tietokentän numeroihin; ID_MASTER_DIAGN ja ID_SLAVE1_DIAGN ovat diagnostiikkaobjekteille valitut CAN-tunnistenumerot):

Komento diagnostiikkaisännältä orjasolmulle →

ID_MASTER_DIAGN	Komento (0)	Kohde (1)	Funktiokohtaiset parametrit (2-7)

← Kuittaus orjasolmulta diagnostiikkaisännälle

ID_SLAVE1_DIAGN	Tila (0)	Kohde (1)	Funktiokohtaiset parametrit (2-7)

4.6.5 Elektronisen manuaalin rakenne

Elektroninen manuaali koostuu sivuista, joilla jokaisella on useita kenttiä. Ensimmäinen kenttä sisältää varsinaisen vikaan liittyvän manuaalitekstin, jonka ensimmäinen rivi kuvaa lyhyesti vian lähteen ja tyypin (esim. 'Paineanturi: hälyttävän pieni arvo'). Tämä rivi tulostetaan katseltaessa vikalokin sisältöä. Toinen kenttä manuaalisivussa sisältää hälytystekstin, joka lähetetään näyttöön hälytyksen sattuessa. Muut kentät ovat näppäintekstejä varten, eli niistä haetaan näppäintekstit diagnosointivaiheessa, kun diagnosoijataski kyselee käyttäjältä jotakin. Manuaali kokonaisuudessaan on moniulotteinen kieliversioiden tähden. Manuaalisivut voidaan tarvittaessa kompressoida.

Kuvassa 28 on esimerkki manuaalisivusta (yksi kieliversio):

POISTOPUTKEN VENTTIILI: OIKOSULKU **Kuvaus**: Poistoputken venttiili näyttää olevan oikosulussa **Mahdollinen syy**: Venttiilin kela on oikosulkeutunut tai venttiiliin menevä kaapeli 100-11 on oikosulussa **Korjaustoimenpiteet**: Tarkista kaapeli 100-11 (ks. ohjekirja) Jos haluat diagnosoida vikaa, paina OK; muussa tapauksessa PERUUTA.					
VIKA POISTOPUTKEN VENTTIILISSÄ: KORJATTAVA HETI					
OK	PERUUTA				

Kuva 28. Esimerkki manuaalisivun rakenteesta.

Esimerkin manuaalisivu on sellainen, joka lähetetään, kun lokinäytöstä on valittu jokin lokirivi. Hälytystekstiä 'VIKA POISTOPUTKEN VENTTIILISSÄ ...' ei tulosteta, vaan se lähetetään ajonäyttöön hälytysehtojen toteutuessa. Manuaalisivuissa, joita vianhakua tekevät tilakoneet käyttävät, ei tarvita hälytystekstiä eikä ensimmäisen rivin tarvitse olla sellainen, että se mahtuisi lokilistan yhdelle riville ajanhetkineen.

4.6.6 Vikailmoitusten lähettäminen

Vikailmoituksia lähetetään ohjausohjelmiston sisältä, käyttöjärjestelmästä ja kommunikointijärjestelmästä eli kaikkialta missä virheentarkistuksia tehdään. Vikailmoitukset lähetetään seuraavalla funktiolla:

FUNKTIO: BYTE Notify_error (BYTE Source, WORD Error_type, LONG Info_value)

Esimerkkikutsu: status = Notify_error (PRESSURE_VALVE, OPEN_LOAD, 0)

Parametrit: *Source*: Kertoo, mikä komponentti on vikailmoituksen lähettäjä. Eniten merkitsevä bitti ilmoittaa, onko kyseessä ohjelmistokomponentti ('0') vai laitekomponentti ('1')
Error_type: Kertoo, minkätyyppinen vika on kyseessä.
Info_value: Vikakohtaista tietoa voi laittaa tähän, esimerkiksi lämpötila-arvon, joka aiheutti hälytyksen. Käytä arvoa 0, jos ei merkitystä.

Palauttaa: *status*: TRUE jos vikailmoitus onnistuttiin välittämään perille (CAN-väylälle), FALSE jos ei onnistuttu.

Kuvaus: Lähettää vikailmoituksen vikataskille CAN-väylän kautta tai solmun sisäisesti, jos vikataski on samalla solmulla.

Huomioita: Tätä funktiota voidaan kutsua myös käyttöjärjestelmän poikkeuskäsittelijässä, jolloin käyttöjärjestelmän virheilmoitukset saadaan myös talteen. Tällöin on huolehdittava siitä, että Source-parametrin ensimmäinen bitti on '0' = ohjelmistokomponentti.

Jokaisella solmulla tulee olla oma CAN-objekti tähän käyttöön, nimeltään esimerkiksi ID_SLAVE1_NTFY_ERR. Turvallisuuskriittisille sanomille voidaan määrätä, että ne on lähetettävä viisi kertaa 100 ms:n välein. Ongelmana tässä on, että orjasolmun ohjelmoijan täytyy tietää, mitkä viat ovat turvallisuuskriittisiä, jotta hän tietäisi lähettää kyseiset viat viisi kertaa. Tämä sotii reseptiajattelua vastaan, jonka mukaan järjestelmäsuunnittelija päättää reseptiä tehdessään, kuinka kriittinen ko. vika on tässä järjestelmässä. Eli sama vika eri järjestelmissä ei ole välttämättä yhtä kriittinen. Toinen mahdollisuus on käyttää kuittauksia kaikilla kriittisyyden tasoilla.

Notify_error-sanoman muoto on seuraavanlainen (numerot suluissa viittaavat CAN-datakentän numeroihin):

Vikailmoitus orjasolmulta diagnostiikkaisännälle →

ID_SLAVE1_NTFY_ERR	**Varattu**	**Source (1)**	**Error_type (2-3)**	**Info_value (4-7)**

Notify_error-vikailmoituksia lähetetään joko joltakin erilliseltä, jatkuvaa vikavalvontaa tekevältä taskilta tai ohjausohjelmiston sisältä, esimerkiksi, jos anturilta luettu arvo ei ole sallittujen arvojen sisällä. Anturin arvoalueet voidaan luokitella esimerkiksi taulukon 14 mukaisella tavalla:

Taulukko N. Esimerkki antureitten arvoalueluokituksesta.

ARVOALUE	KUVAUS
NORMAL	Normaali: jos kaikki on kunnossa, anturin lukeman pitäisi olla tällä alueella.
LOW	Matala: arvo on pienempi kuin normaalisti, mutta ei niin pieni, että kannattaa hälyttää.
HIGH	Korkea: arvo on suurempi kuin normaalisti, mutta ei niin suuri, että kannattaa hälyttää.
ALARM_LOW	Hälyttävän matala: arvo on hälyttävän matala; hälytetään.
ALARM_HIGH	Hälyttävän korkea: arvo on hälyttävän korkea; hälytetään.
SHORT_TO_GND	Oikosulku maahan: arvo on sellainen, joka saadaan silloin, kun anturin aktiivinen johdin on oikosulussa maahan. Voidaan käyttää vain silloin, kun tämä arvoalue jää normaalialueen ulkopuolelle.
SHORT_TO_VCC	Oikosulku käyttöjännitteeseen: arvo on sellainen, joka saadaan silloin kun anturin aktiivinen johdin on oikosulussa käyttöjännitteeseen. Voidaan käyttää vain silloin, kun tämä arvoalue jää normaalialueen ulkopuolelle.
OPEN	Katkos: arvo on sellainen, joka saadaan, kun anturin kaapeli on poikki. Voidaan käyttää vain silloin, kun tämä arvoalue jää normaalialueen ulkopuolelle. Oikosulkuja ja katkoksia ei voi erottaa niiltä osin, kuin niiden arvoalueet menevät päällekkäin.

Tällöin vikailmoitus lähetettäisiin esim. funktiokutsulla:

Notify_error (anturin_numero, ALARM_HIGH, luettu_arvo).

5 CASE-JÄRJESTELMIEN TURVALLISUUDEN ARVIOINTI

5.1 KÄYTETYT TUTKIMUS- JA ANALYYSIMENETELMÄT

CAN-väyläjärjestelmien turvallisuuden arvioinnissa käytettiin tutkimus- ja analyysimenetelminä vika- ja vaikutusanalyysiä (VVA), vikapuuanalyysiä (VPA) sekä ohjelmoitavien elektronisten järjestelmien arviointia varten VTT:n ja yritysten yhteistyönä laadittua tarkistuslistaa, josta kerrotaan tarkemmin lähteessä Tiusanen et al 1994. Lisäksi tutkimuksessa verrattiin CAN-väyläjärjestelmän etuja ja haittoja releohjaukseen verrattuna erilaisten käyttövarmuustekijöiden suhteen.

Vika- ja vaikutusanalyysi on induktiivinen (alhaalta ylöspäin suuntautuva) luotettavuuden analysointimenetelmä, jolla tunnistetaan vikoja ja niiden vaikutuksia tutkittavaan järjestelmään. VVA:ta käytetään pääasiassa kvalitatiivisena analyysimenetelmänä nimenomaan laitteistovikojen tunnistamiseksi. Analyysi yleensä dokumentoidaan käyttäen taulukkoa, josta ilmenee mm. järjestelmän osa, vioittumistapa, mahdollisesti vian syy, vian vaikutus, vian paljastumistapa ja huomautukset tai toimenpiteeet. VVA on hyödyllistä tehdä järjestelmän suunnitteluvaiheessa, jolloin se tukee suunnittelukatselmuksia.

Vikapuuanalyysi on deduktiivinen (ylhäältä alaspäin suuntautuva) luotettavuuden analysointimenetelmä, jolla tunnistetaan ei-toivotun tapahtuman eli huipputapahtuman syitä ja niiden yhdistelmiä. Analyysi on pääasiassa kvalitatiivinen, mutta sitä voidaan käyttää myös kvantitatiivisesti. VPA on itse asiassa graafinen esitys tapahtumista tai tiloista, jotka voivat vaikuttaa huipputapahtuman syntyyn. VPA soveltuu erityisen hyvin monimutkaisten järjestelmien tarkasteluun, ja sitä voidaan käyttää myös ohjelmiston analysointiin. Tällöin analyysillä varmistetaan, ettei ohjelmistosuunnittelun logiikkavirheet aiheuta turvallisuuteen vaikuttavaa vikaa. Laitteistolle ja ohjelmistolle tehdyt vikapuut on mahdollista yhdistää.

Ohjelmoitavien elektronisten järjestelmien tarkistuslistan avulla kerätään tietoa tutkittavasta järjestelmästä ja arvioidaan järjestelmän turvallisuustasoa. Tarkistuslista pohjautuu pääosin IEC 1508 -standardiluonnokseen ja EWICS TC7:n tekemään työhön. Tarkistuslista koostuu järjestelmän laitteiston ja ohjelmiston toteutustekniikoista, menetelmistä, analyyseistä ja muista toimenpiteistä turvallisuuden toteuttamiseksi. Tekniikoille, menetelmille jne. on annettu suosituksia niiden käytöstä eri turvallisuuden eheystasoilla, jotka IEC 1508 -standardiluonnoksessa on luokiteltu 1:stä 4:ään. Tarkistuslista sisältää em. lisäksi tekniikoita ja menetelmiä liittyen mm. laadunvarmistukseen, turvallisuusvaatimuksiin, vikojen paljastumiseen ja hallintaan, kelpoistukseen, asennukseen ja ylläpitoon. Tarkistuslistasta on tehty myös PES CHECK -niminen tietokonesovellus.

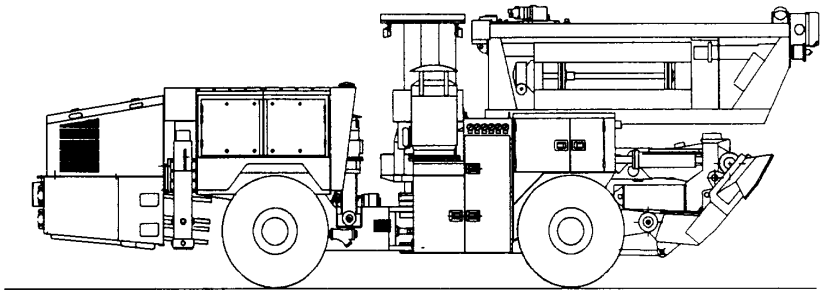
5.2 CASE-KOHTEET

Tutkimuksessa tarkasteltiin kolmen case-kohteen ohjausjärjestelmää. Case-kohteet olivat Tamrock Oy:n SOLO 1000 Sixty -tyyppinen tuotantoporauslaite, Vammas Oy:n PSB 5500 -tyyppinen lentokenttien lumenraivauskone sekä Pirkan Elektroniikka Oy:n ja UH-Tekniikka Oy:n varavoimalakäyttö, jonka ohjausjärjestelmänä on CU 2000 -tyyppinen dieselgeneraattorin ohjaus. Seuraavassa kerrotaan lyhyesti laitteiden ominaisuuksista, järjestelmille tehdyistä analyyseistä ja niillä saaduista tuloksista.

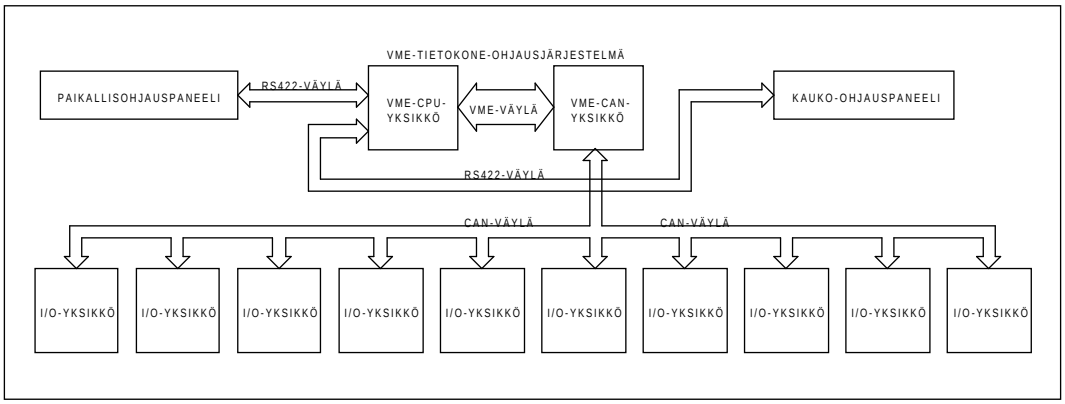
5.2.1 Tuotantoporauslaite

SOLO 1000 Sixty -tuotantoporauslaite on hydraulinen pitkäreikäporauslaite, joka on suunniteltu tuotantolouhintaan yksittäisille pitkille rei'ille sekä ylä- ja alakätisille viuhkoille. Reikäsyvyydet ovat 40 - 60 m ja yleisin reiän halkaisija on 100 mm. Laitetta käytetään maanalaisissa kaivoksissa.

Solo 1000 Sixty -tuotantoporauslaite esitetään kuvassa 29 ja sen ohjausjärjestelmä lohkokaaviona kuvassa 30.



Kuva CC. SOLO 1000 Sixty -tuotantoporauslaite.



Kuva DD. SOLO 1000 Sixtyn ohjausjärjestelmä.

Tavoitteena tämän case-järjestelmän tarkastelussa oli selvittää paitsi turvallisuuteen vaikuttavat vikatilanteet CAN-väylällä ja niiden hallinta myös se, mitä työkaluja on käytettävissä vikojen tunnistamiseksi ja missä laitteen elinkaaren vaiheessa niitä tulisi käyttää.

Solo Sixty -järjestelmän turvallisuustarkastelussa käytetyt menetelmät olivat vikapuuanalyysi sekä ohjausjärjestelmän laitteiston ja ohjelmiston arviointi tarkistuslistan avulla.

SOLO Sixty -porauslaitteen ohjausjärjestelmää arvioitaessa yhdeksi turvallisuuskriittiseksi tekijäksi nähtiin pidon ohjaus putken vaihdossa. Pidon pettäminen voi aiheuttaa vaaran esim. erikoistilanteessa, jossa putkiletkasta menee putki poikki ja käyttäjä on lähellä porauslaitetta, jolloin hän voi saada putkiletkan päähänsä. Pidon ohjaukselle tehtiin vikapuuanalyysi, jonka huipputapahtumaksi määriteltiin ”pito ei purista putken vaihdossa”. Vikapuuanalyysissä etsittiin syitä ja tapahtumapolkuja, jotka voivat johtaa huipputapahtuman syntyyn. Analyysissä käsiteltiin pääasiassa sähköisiä vikoja, ja lähtöoletuksena oli, että käytetään manuaaliohjausta. Tapahtumaketjut piirrettiin vikapuuksi.

Vikapuun laadinnan tarkoituksena oli selvittää sähköisten vikojen osalta, ovatko huipputapahtumaan mahdollisesti johtavat syyt hallinnassa. Näin ollen vikapuun juurella olevat tapahtumat eli huipputapahtuman mahdolliset syyt käsiteltiin siten, että pohdittiin keinoja ja menetelmiä, joiden avulla viat havaitaan, sekä toimenpiteitä, joita tulee tehdä kunkin vikatyypin ilmetessä.

Vikapuuanalyysin perusteella havaittiin, että CAN-väylään liittyvät vikatilanteet ovat valvonnassa ja hallinnassa siten, että niistä tulee virheilmoitus ohjausjärjestelmälle ja vikatilanteissa järjestelmä siirtyy turvalliseen tilaan. Kaapelit ja liittimet olivat analyysin perusteella ja sen jatkotarkastelun kannalta tärkeimmät ja vikaantumiselle altteimmat kohteet.

Vikapuuanalyysi voidaan tehdä turvallisuuteen liittyvien järjestelmien toteutusvaiheessa (ks. kuva 1 luvussa 2), etenkin kelpoistettaessa ohjausjärjestelmän laitteistoa ja ohjelmistoa sekä koko laitteen kelpoistusvaiheessa. Alustava vikapuuanalyysi voidaan tehdä jo turvallisuusvaatimusten allokointivaiheessa.

Solo sixtyn hajautetun ohjausjärjestelmän laitteiston ja ohjelmiston suunnittelu- ja toteutusmenetelmät ja -tekniikat sekä käytetyt analyysimenetelmät käytiin läpi ohjelmoitaville elektronisille järjestelmille laaditun tarkistuslistan mukaisesti. Tarkistuslistan ”läpikävely” tehtiin laitteisto- ja ohjelmistosuunnittelijoiden sekä tutkijoiden välisenä yhteistyönä.

Suunnittelijat pitivät tarkistuslistaa hyvänä muistilistana asioista, jotka turvallisuuden elinkaaren eri vaiheissa tulisi ottaa huomioon. Käytetty tarkistuslistaversio ei kuitenkaan sisältänyt niitä turvallisuuteen ja käyttövarmuuteen liittyviä tekniikoita ja menetelmiä, jotka nimenomaan hajautettujen CAN-väyläsovellusten yhteydessä tulisi arvioida suunnittelun ja toteutuksen eri vaiheissa. Näitä tekniikoita on käsitelty tämän raportin luvuissa 3 ja 4.

5.2.2 Lentokenttien lumenraivauskone

Tutkimuskohteena oli PSB 5500 -tyyppinen lentokenttien lumenraivauskoneena käytettävä, itsekulkeva aura-harja-puhallinkone. Tämän kohteen osalta tutkimuksen tavoitteena oli arvioida ja verrata eri käyttövarmuustekijöitä releohjausjärjestelmän ja mahdollisena toteutusvaihtoehtona olevan CAN-väyläjärjestelmän välillä.

Koneen työlaitteet ovat siis aura, harja ja puhallin. Koneita käytetään siten, että useasta koneesta koostuva airue ajaa lentokentän kiitoradan läpi puhdistaen kertapyyhkäisyllä koko radan. Tämä toimenpide saa kestää n. 2 - 3 min. Koska useita koneita on kentällä yhtä aikaa, kolarit ovat mahdollisia. Aura tai harja voi ottaa väärän työasennon, mistä voi myös aiheutua vahinkoa. Tämäntyyppisiä koneita käytetään alle 500 h vuodessa, ja vuoden aikana niille tehdään yksi perushuolto.

Koneen harjalle ja puhaltimelle on omat käyttömoottorinsa. Näiden työlaitteiden ottotehot ovat n. 120 - 150 kW ja n. 200 kW. Hydraulitoimisesti käytettävää harjaa nostetaan ja lasketaan, joten harjan on oltava tarkasti säädettävissä. Harjassa on säädettävät ja kierrettävät tukipyörät. Harjan kosketuspituus on ihanteellisimmin 5 cm.

Koneessa on hydrauliventtiileille oma keskuksensa. Releistys on pääosin ohjaamossa. Koneessa ei ole sähkökäyttöjä. Koneesta on tehtävissä myös hinattava.

Uudentyyppinen lumenraivauskone on nelivetoinen, kuorma-auton runkoon rakennettava malli, jossa käytetään kuorma-auton ajomoottoria ja jossa hallinta- ja valvontalaitteet sijoitetaan ohjaamoon. Hyväksi havaittu ajomoottoritekniikka rajattiin tutkimuksen ulkopuolelle. Tarkasteluun kuuluivat lumenraivauskoneen työlaitteet ja niiden ohjaus. Tutkimuksessa arvioitiin CAN-väylätekniikan hyötyjä ja haittoja sekä moduulijakoa CAN-väylätekniikkaa sovellettaessa.

Lumenraivauskoneen yhtenä pääasiallisimpana turvallisuusvaatimuksena on, että kone pitää joka tilanteessa olla ajettavissa pois kentältä. Toisena vaatimuksena on, että koneen toiminta ei saa alkaa seota. Esim. aura tai harja saattaa toimintahäiriön seurauksena ottaa väärän työsuunnan. Tekniikan pitäisi tämän vuoksi olla täysin varmaa. Koneelle sattuneita vahinkoja ovat olleet halliin törmäys ja palaminen hydraulivuodon seurauksena (kone on dieselpolttoainekäyttöinen).

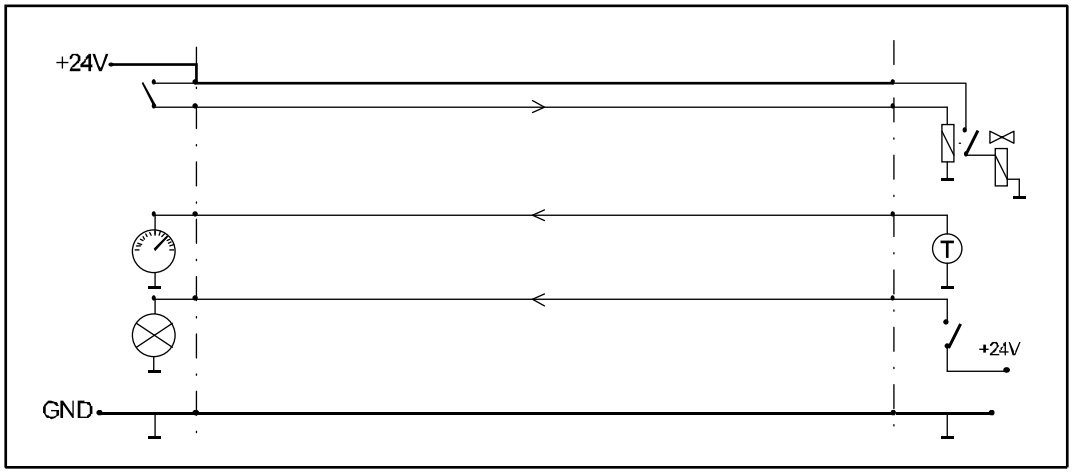
Lumenraivauskoneilta vaaditaan, että ne eivät saa häiritä lentokentän radioliikennettä. Toisaalta radioliikenne ei myöskään saa häiritä lumenraivauskoneen toimintaa.

Muita tekijöitä, joihin ohjaustekniikkaa suunniteltaessa tulisi kiinnittää huomiota, ovat mm.

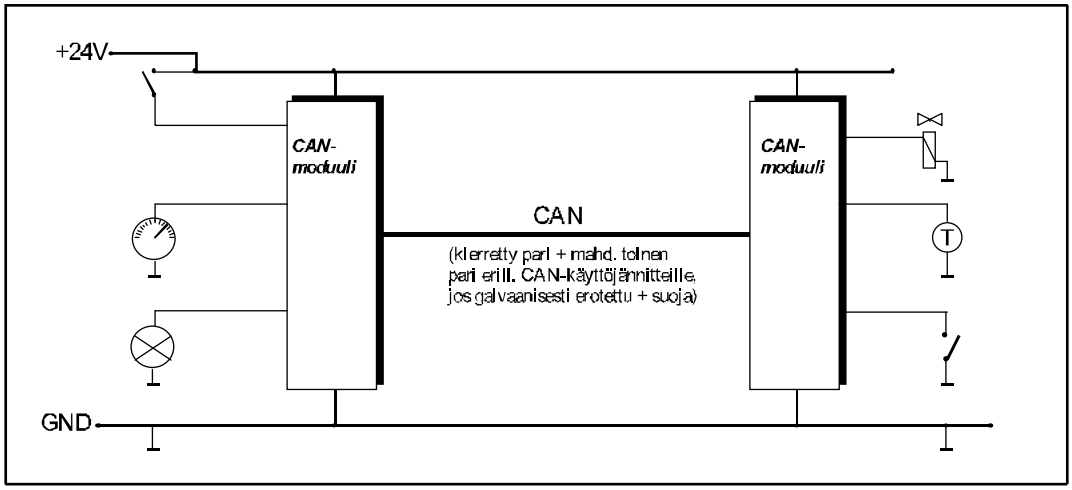
- kriittiset ohjaustoiminnot
- turvatoimintojen luotettavuus (vika turvatoiminnoissa saattaa estää koneen käytön, vaikka kone olisi muuten kunnossa)

- antureiden kunto (anturiviat ovat yleisimpiä vikoja)
- kaapelien ja liittimien määrä ja laatu
- lentokentillä käytettävät jäänsulatuskemikaalit
- muut ympäristötekijät.

Vaihtoehtoja hajautuksen arkkitehtuuriksi on useita. Kuvassa 31 esitetään lähtötilanne, jossa jokainen signaali on johdotettu erikseen. CAN-väylää voidaan käyttää pelkästään multipleksaukseen kuvan 32 periaatteen mukaisesti. Tässä vaihtoehdossa voidaan käyttää nykyisiä painikkeita ja kytkimiä.

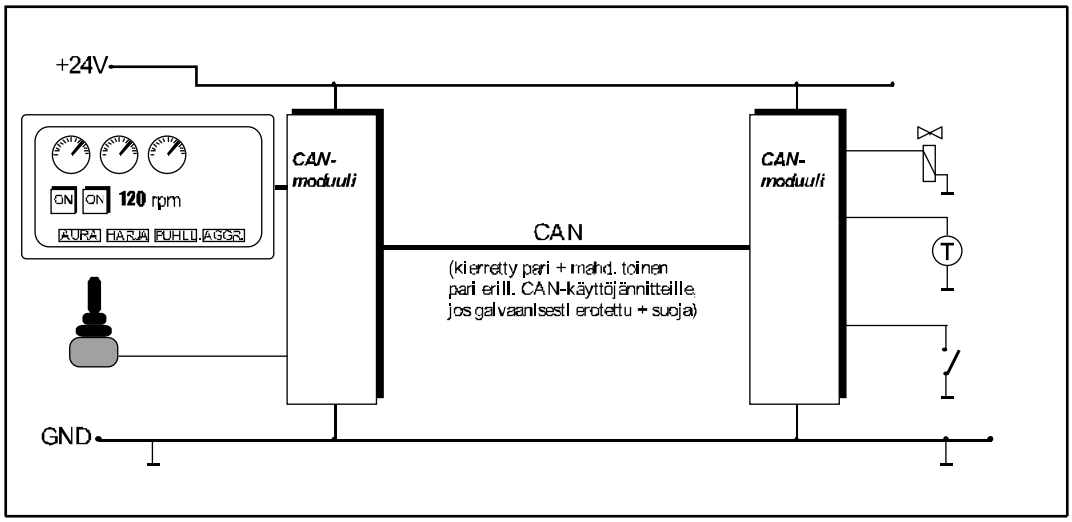


Kuva 31. Lähtötilanne: jokainen signaali johdotettu erikseen.



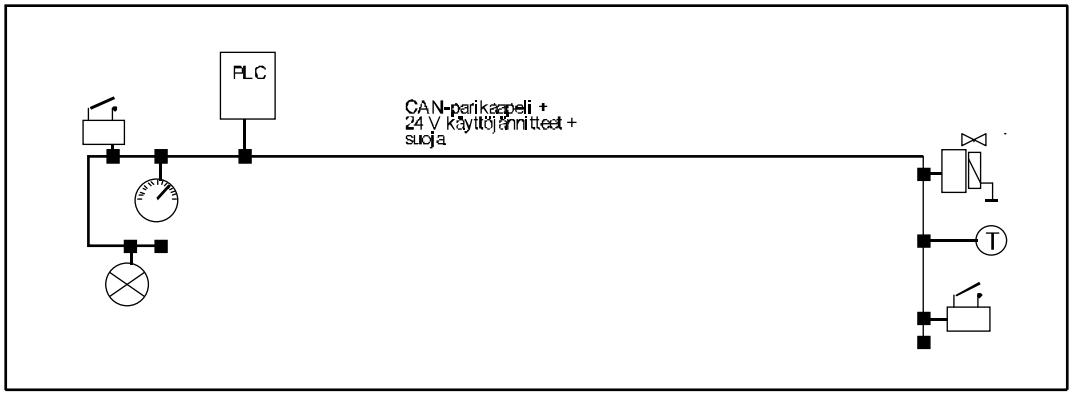
Kuva 32. CAN-väylää käytetty pelkästään multipleksaukseen.

Koneen kuljettajalle näkyvät instrumentit ja ohjauslaitteet voidaan korvata myös graafisella käyttäjäliitynnällä (kuva 33). Mahdolliset näyttövaihtoehdot ovat nestekidenäyttö ja elektroluminenssinäyttö. Nestekidenäytön heikkoutena on se, että näyttö ei yleensä kestä pakkasta. Näytön lämmittäminen on kuitenkin mahdollista konetta käytettäessä. Kun koneita ei käytetä, niitä säilytetään sisätiloissa. Elektroluminenssinäyttö on kalliimpi vaihtoehto kuin nestekidenäyttö.



Kuva 33. Instrumentit ja ohjauslaitteet on korvattu graafisella käyttäjäliitynnällä.

Hajautus voidaan viedä vieläkin pidemmälle siten, että jokainen kytkin tai muu laite liitetään suoraan väylälle (kuva 34). Tällä hetkellä tällainen hajautus ei ole vielä mahdollista, koska kaikkia järjestelmässä tarvittavia laitteita ei ole vielä kaupallisesti saavutettavissa. Honeywellin SDS-järjestelmä ja Allen Bradleyn DeviceNet ovat esimerkkejä tällaisesta hajautusarkkitehtuurista.



Kuva 34. Anturit ja toimilaitteet kytketty suoraan väylälle.

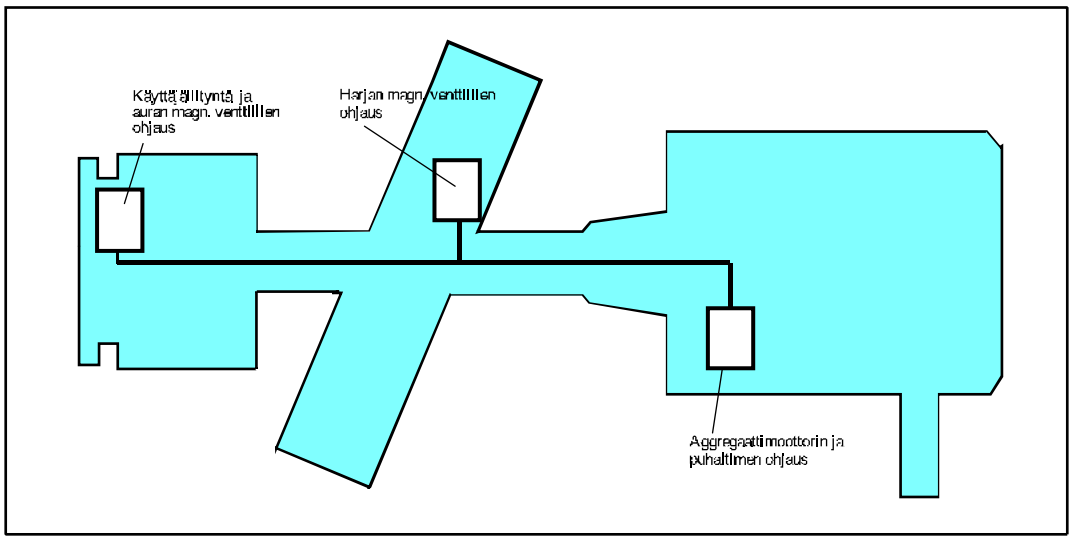
Tutkimuksessa arvioitiin lumenraivauskoneen ohjaustekniikkoihin liittyviä käyttövarmuustekijöitä. CAN-väylätekniikan edut ja haitat releohjaukseen verrattuna näkyvät plussina ja miinuksina taulukossa 15.

Taulukko O. Työkoneen ohjaustekniikkaan liittyvien käyttövarmuustekijöiden arviointi.

Tekijä	**CAN-väylätekniikan edut ja haitat releohjattuun järjestelmään verrattuna**
Sähköasennukset - piirikortit, komponentit - liittimet, kaapelit ja johdotukset	+ huomattavasti yksinkertaisempi kaapelointi, selkeämmät dokumentit + liittimien ja kaapelien määrä putoaa n. 25 %, kokonaispituus lyhenee 25 - 50 %, johtimien määrä putoaa n. 20 %[13]
Tiedonsiirto - nopeus, luotettavuus - oikeellisuuden ja perillemenon tarkistukset - muut varmistukset	+ CAN-tekniikalla voidaan toteuttaa riittävän nopea ja luotettava tiedonsiirto
Komponenttien korvattavuus - elektroniikkakomponentit - sähkömekaaniset komponentit - liittimet, kaapelit, johdotukset	- CAN-moduuli on uusi ja kallis varaosa, joka on kokonaan vaihdettava sen vikaantuessa + releet korvautuvat smart power -puolijohdekytkimillä
Huoltotilanteet - koneen huoltopisteet - huollon helppous	+ huoltokohteet ovat helpommin ymmärrettäviä kaapeloinnin yksinkertaistuessa + järjestelmän 'näkyvyys' paranee huomattavasti väylän ansiosta - uusi tekniikka => kaikkia vikoja ei nähdä yleismittarityyppisillä mittalaitteilla, vaan tarvitaan erityisiä diagnostiikkalaitteita
Käyttöliittymä - ohjaustapa, ergonomia	- jotta graafisesta käyttäjäliitynnästä tulisi ergonomisesti hyvä, suunnitteluun on kiinnitettävä erityistä huomiota
EMC - häiriösietoisuus - häiriöpäästöt	- CAN-moduulit ja kaapelit ovat uusia suojattavia kohteita, mitä perinteisessä tekniikassa ei ole - kokemuksia CAN/EMC-asioista vähän
Käyttö vikaantuneena	- jos esim. CAN-moduulin jänniteregulaattori menee rikki, kaikki siihen liitetyt laitteet menevät toimintakyvyttömiksi
Anturointi	+ pysyy samana, mutta voidaan helpommin lisätä uusia antureita
Hälytykset tai diagnostiikka	+ mahdollista toteuttaa informatiivisemmat hälytykset (esim. ennakoivat hälytykset, kulumisesta informointi, kunnonvalvonta) + magneettiventtiilien keloja ja niille meneviä kaapeleita voidaan valvoa
Ympäristötekijät - kemikaalit - lämpötilarajoitukset, sää - muut ympäristötekijät	- käytettävä pakkaskestävää elektroniikkaa, esim. nestekidenäytön pakkaskestävyyteen kiinnitettävä huomiota - CAN-moduulit suojattava siten, että saavutetaan sama suojaustaso kuin perinteisellä tekniikalla
Ajoneuvon tai työlaitteiden ohjattavuus	+ älykkäämpi ohjaus => koneen työlaitteiden parempi hallittavuus => parempi työjälki myös kokemattomilla kuljettajilla + älykkäämmän ohjauksen ansiosta myös älykkäämmät turvallisuusehdot, ja käyttäjän toiminnoista saadaan yksinkertaisempia => virhetapaukset vähenee
Laajennettavuus - suunnittelu	+ helpommin lisättävissä uusia ominaisuuksia - yksinkertaisenkin osan (esim. lampun) lisääminen vaatii ohjelmointia
Ohjelmisto	- ohjelmisto on uusi vikalähde - uusi komponentti, joka on huollossa pystyttävä päivittämään

[13] Tiedot ovat peräisin lähteestä Furuichi et al. (1992) ja Honeywellin esitteistä.

Tutkimuksessa tehtiin vikapuuanalyysi sekä lumenraivauskoneen releohjausjärjestelmälle että kolme moduulia käsittävälle kuvan 35 CAN-väyläjärjestelmämallille. Vikapuuanalyysin huipputapahtumaksi määriteltiin ”Harja ottaa väärän työasennon”. Vikapuuanalyysissä etsittiin syitä ja tapahtumapolkuja, jotka voivat johtaa huipputapahtuman syntyyn. Tapahtumaketjut piirrettiin vikapuiksi. Vikapuuanalyysissä tarkasteltiin vain yhtä huipputapahtumaa, mutta vian syyt ovat melko samantyyppisiä jonkin muun huipputapahtuman esiintyessä (esim. auran väärä työasento). Vikapuita analysoitaessa ja vertailtaessa havaittiin seuraavassa kuvattuja näkökohtia.



Kuva 35. Kolme CAN-moduulia käsittävä järjestelmä.

Huipputapahtuman syinä voivat olla mekaaniset, hydrauliset tai sähköiset konejärjestelmän viat tai inhimilliset tekijät, tai huipputapahtuman voi aiheuttaa jokin ulkoinen häiriö, kuten jääkimpaleen putoaminen koneen päältä.

Hydrauliikan viat voivat olla venttiilivikoja tai muita hydrauliikan vikoja. Venttiili voi vikaantua mekaanisesti, jumittua tai sen kela voi vikaantua. Muu hydrauliikan vika voi aiheutua esim. epäpuhtaudesta, sylinterin rikkoutumisesta tai letkun katkeamisesta. Hydraulijärjestelmään tullut roska voi aiheuttaa vuodon tai saada aikaan sen, että öljy kulkee huonosti. Tätä ei välttämättä releohjausjärjestelmässä havaita kuin jollakin päättelymenetelmällä. CAN-järjestelmässä mm. kyseinen vikamuoto voidaan havaita helpommin.

Mekaaniset viat voivat olla tukipyörän vikoja tai muita mekaanisia vikoja. Jos tukipyörä ei liiku, se havaitaan painemittarista. CAN-väyläjärjestelmässä voidaan havaita useamman tyyppiset viat kuin releohjausjärjest elmässä.

Mekaanisten ja hydraulisten vikojen syyt ovat melko samantyyppisia sekä releohjausjärjestelmässä että CAN-väyläjärjestelmässä. Sen sijaan ***sähköisten vikojen*** syyt poikkeavat jonkin verran toisistaan. CAN-väyläjärjestelmässä käyttäjän antaman signaalin puuttumisen syynä olisi todennäköisesti näppäin- tai ”joystick”-vika. CAN-järjestelmässä ei myöskään ole nykyisen järjestelmän releitä, vaan nii-

den tilalla on puolijohdekytkimet. Kaapeli- ja liitinv ikoja voi esiintyä sekä nykyisessä järjestelmässä että CAN-väyläjärjestelmässä, mutta jälkimmäisessä kaapelointia on vähemmän. Asennon rajakatkaisijoiden viat voidaan havaita antureiden merkkivaloista, mutta vika ilmenee usein liian myöhään.

Releiden viat on melko hankalasti havaittavissa, mutta niitä vikaantuu harvoin. CAN-väyläjärjestelmässä releiden asemesta käytetään puolijohdekomponentteja, jotka pystyvät tunnistamaan magneettiventtiileiden kelojen oikosulut ja katkokset. Relelogiikan tilalla voitaisiin käyttää ohjelmoitavaa logiikkaa, mutta se vaatisi työläitä muutoksia ohjausjärjestelmään.

Jos CAN-järjestelmän käyttöliittymämoduuli ei anna sanomaa, syinä voivat olla väylävika, piirikortin laitteisto- tai ohjelmistovika, moduuli ei saa sähköä tai moduulille ei tule signaalia kaapeli-, liitin-, näppäin- tai ohjaussauvavian vuoksi. Jos harjamoduuli ei saa sanomaa, syinä voivat olla väylävika, piirikortin laitteisto- tai ohjelmistovika, se että moduuli ei saa sähköä tai väylällä on ohjelmistovian johdosta 100 %:n kuormitus, jolloin signaali ei pääse perille.

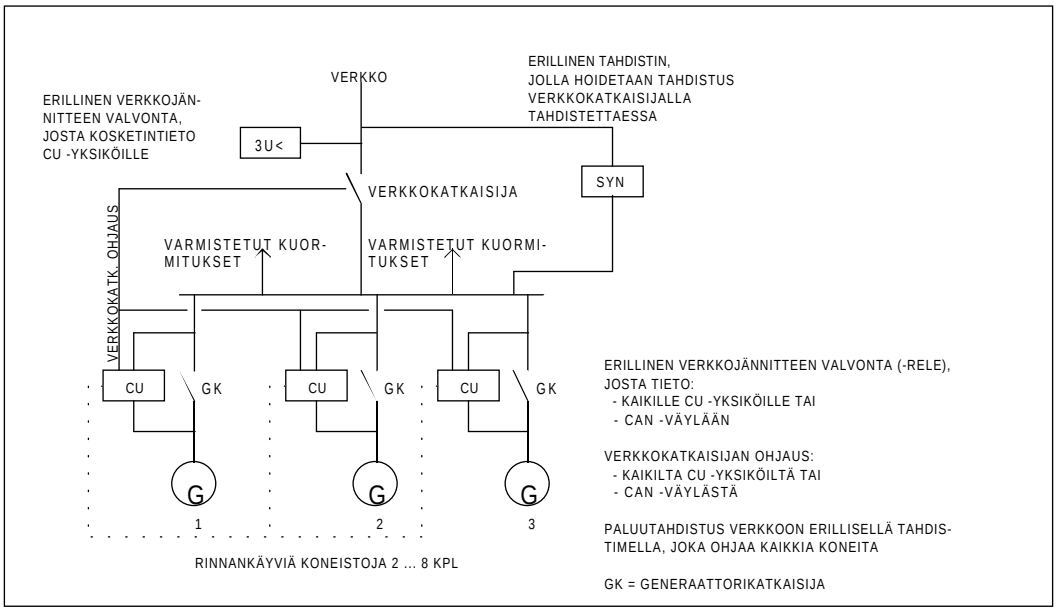
CAN-järjestelmän avulla voidaan vähentää ***inhimillisten tekijöiden*** vaikutusta huipputapahtuman syntyyn, koska käyttäjän toiminnoista voidaan tehdä yksinkertaisempia. Jos esim. vaihto kuljetusasennosta työasentoon voitaisiin tehdä nappia painamalla, sekä inhimillisten tekijöiden vaikutukset että koneen tietyt vikaantumismahdollisuudet vähenisivät.

5.2.3 Varavoimalakäyttö

Varavoimalaitoksia käytetään kohteissa, joissa sähkönsyötön on jatkuttava välittömästi sähkökatkon sattuessa mm. taloudellisten menetysten estämiseksi ja henkilöturvallisuuteen liittyvien toimintojen varmistamiseksi. Tällaisia kohteita ovat esim. sairaalat, puhelinlaitokset, ATK-keskukset ja teollisuuslaitokset.

Varavoimalaitos voidaan toteuttaa myös siten, että useita automaattisia dieselgeneraattoreita käy ja syöttää varmistettuja kuormituksia keskenään rinnan yleisen jakeluverkon häiriötilanteessa. Tällöin tulee huolehtia siitä, että kokonaiskuormitus jakaantuu tasan keskenään rinnan käyvien koneiden kesken (mikäli kaikki koneet ovat samantehoisia) tai koneiden nimellistehojen suhteessa (mikäli kaikki rinnan käyvät koneet eivät ole samantehoisia). Varavoimakoneita voidaan käyttää myös rinnan yleisen sähkönjakeluverkon kanssa tasaamaan yleisestä jakeluverkosta ostetun tehon huippuja (ns. huipunleikkauskäyttö). Varavoimakoneiden koekäyttö tapahtuu toisinaan myös rinnan yleisen jakeluverkon kanssa. Tutkimuskohteena oli CU 2000 -tyyppinen dieselgeneraattorin ohjausjärjestelmä.

Esimerkkinä CAN-väyläjärjestelmästä tarkasteltiin tilannetta, jossa kolme yksikköä on kytkettynä yhteen (kuva 36). Tällaiselle järjestelmälle tehtiin vikapuuanalyysi. Järjestelmälle tehtiin myös vika- ja vaikutusanalyysi (VVA), jossa tarkasteltiin yhden yksikön toimintaa. Varavoimalaitosyksiköitä voidaan kytkeä yhteen CU 2000 -ohjausjärjestelmässä maksimissaan 8 kpl. Tehdyt analyysit toteutettiin osittain tiimityönä ja osittain suunnittelijoiden omana katselmuksena.



Kuva 36. Kolmen varavoimalayksikön kytkentä.

Yhden varavoimalaitosyksikön yhden koneiston teho on yleensä 25 kW - 1 MW. Verkkohäiriötilanteessa kaikki koneet käynnistyvät. Nopeimmin käynnistynyt asettuu isäntäkoneeksi, avaa verkkokatkaisijan ja kytkeytyy syöttämään. Muut koneet on tahdistettava rinnalle. Kun seuraava kone tahdistuu, tulee ilmoitus muille yksiköille. Muut eivät tällöin saa tehdä mitään. On varmistettava, mitkä yksiköt ovat kunnossa ja tahdistusvalmiina. Muiden koneiden kytkeytyminen tapahtuu pienellä viiveellä, kun yksi yksikkö on jo syöttämässä.

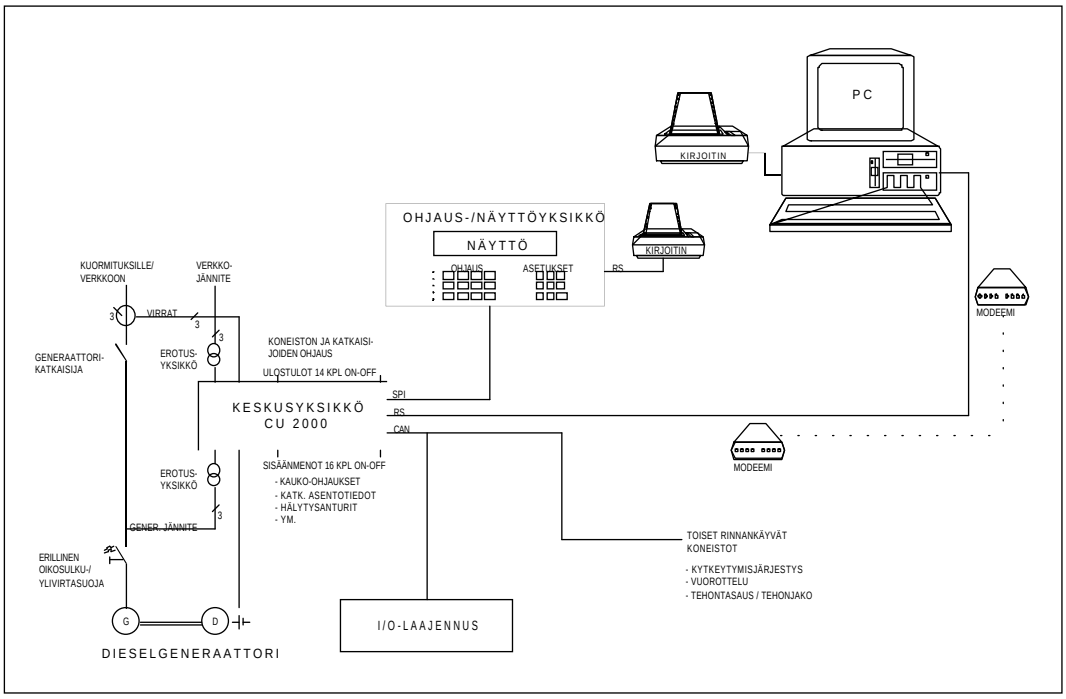
Koneiden keskinäisessä rinnankäytössä koneiden keskinäiset tehot säädetään CU 2000 -järjestelmän ulkopuolisilla tehontasausyksiköillä tai CU 2000 -ohjausjärjestelmien välisenä tehonsäätönä. Jälkimmäisessä tapauksessa CAN-väylällä siirretään koneiden välillä tehontasaustietoja ja -ohjauksia sekä tietoa siitä, montako konetta on kytkeytyneenä. Siten CAN-väylällä on runsaasti liikennettä.

Kun rinnan käyvät koneistot kytketään yleiseen jakeluverkkoon verkkokatkaisijalla, koneistojen tahdistuksesta yleisen jakeluverkon rinnalle huolehtii ulkopuolinen synkronointilaite. Synkronointilaitetta ei järjestelmää tutkittaessa ole otettu huomioon.

Jos koneet kytkeytyvät hallitsemattomasti (epätahdistus), laitevauriot ovat mahdollisia. Laitevauriot ovat mahdollisia myös, jos koneet eivät kytkeydy irti käytön lopussa tai häiriötilanteessa. Myös laaja-alaiset verkkoon suuntautuvat seurannaisvaikutukset ovat mahdollisia.

Pyörimisnopeutta mitataan jatkuvasti. Tehontasaus tapahtuu ulkopuolisella laitteella tai CU 2000:n ohjaamana rinnan käyvien koneiden kesken. Taajuus pidetään vakiona ja tehonjaosta sekä taajuudesta huolehditaan jatkuvasti. Myös tehon suuntaa mitataan. Mikäli tehon suunta vaihtuu kiskosta generaattoriin päin, koneisto on irroitettava, sillä generaattori ei saa alkaa toimia moottorina.

CU 2000 -ohjausjärjestelmä on kuvan 37 mukainen. Näytön ja keskusyksikön välillä on SPI-väylä, ja PC:n ja keskusyksikön välillä RS-väylä (mahdollisesti modeemiyhteys). Rinnan käyvien koneistojen välillä on CAN-väylä.



Kuva 37. CU 2000 -ohjausjärjestelmä.

Varavoimalakäytölle tehtiin vikapuuanalyysi (VPA), jonka avulla selvitettiin ei-toivottuun tapahtumaan eli huipputapahtumaan johtavia syitä. Huipputapahtumaksi määriteltiin ”Laitos ei tuota sähköä”. VPA toteutettiin kuvan 36 mukaiselle järjestelmälle, jossa kolme konetta on kytketty rinnakkain. Näistä yksi toimii isäntäkoneena ja muut orjakoneina.

Syinä huipputapahtuman syntyyn voivat olla konejärjestelmän vika tai inhimillinen tekijä. Jälkimmäinen voi sisältää useita tekijöitä (esim. automaattiasento ei ole päällä), joita analyysissä ei tarkemmin käsitelty. Jos yhdeltä rinnan kytketyltä koneelta ei tule sähköä, muut silti toimivat ja tuottavat sähköä laitokseen. Tehontasauksessa voi tällöin kuitenkin tulla ongelmia, jos koneistot eivät ole samankokoisia. Jotta huipputapahtuma voisi syntyä, on kaikkien kolmen koneiston lakattava syöttämästä.

Huipputapahtuman aiheuttavana konejärjestelmän vikana voi olla esim. se, että katkaisijan ohjaussignaali puuttuu siitä syystä, että kytkentälupa muilta CAN-yksiköiltä puuttuu. Tällaisen vian voi aiheuttaa joko CAN-väylän fyysinen vika tai ohjelmistovika tai sitten jokin vika muissa keskusyksiköissä. Tämän vuoksi CAN-väylän luotettavuuteen on kiinnitettävä huomiota.

Vika- ja vaikutusanalyysi tehtiin CU 2000 -ohjausjärjestelmän keskusyksikölle sekä ohjaus- ja näyttöyksikölle I/O-tasolla. Analyysissä tutkittiin vikojen vaikutusten lisäksi sekä ohjausjärjestelmän että käyttäjän tunnistamat vikojen paljastumistavat.

CU 2000 -ohjausjärjestelmän VVA:n perusteella havaittiin, että suuri osa vikamuodoista on sellaisia, jotka ohjausjärjestelmä pystyy tunnistamaan. Järjestelmässä voi kuitenkin esiintyä myös sellaisia vikamuotoja, joita ***ohjausjärjestelmä ei tunnista.*** Osa tämäntyyppisistä vikamuodoista voi jäädä piileviksi niin, ettei käyttäjäkään niitä heti tunnista. Ne voidaan tunnistaa vain testaamalla toiminta anturilta asti (tällainen vika voi esim. estää häiriöilmoituksen tai häiriöpysäytyksen toiminnan). Jotkut vikamuodot, joita ohjausjärjestelmä ei tunnista, voidaan havaita järjestelmän poikkeuksellisen tai tilanteeseen sopimattoman käyttäytymisen perusteella ja osa voidaan havaita kauko-ohjauksessa.

Muutaman vikamuodon seurauksena kauko-ohjattu käynnistäminen ei ole mahdollista. Nämä vikamuodot voivat jäädä ohjausjärjestelmältä tunnistamatta. Koneiston käyttö voi joidenkin vikamuotojen seurauksena estyä ja jotkut viat voivat aiheuttaa laitevaurioita, mutta nämä vikamuodot yleensä tunnistetaan.

Järjestelmän käyttövarmuutta voidaan parantaa

- tarkistamalla järjestelmän kunto määrävälein (erityisesti piilevien vikamuotojen varalta)

- käyttämällä useita rinnan käyviä koneistoja kohteissa, joissa varavoimalaitosyksikön toimintahäiriö voi aiheuttaa henkilöturvallisuusriskin, jolloin varmistetaan sähkönsyöttö myös yhden varavoimalayksikön vikaantuessa.

CU 2000 -ohjausjärjestelmän laitteisto ja ohjelmisto käytiin läpi VTT Valmistustekniikassa kehitetyn tarkistuslistan mukaisesti. Tarkistuslista pohjautuu IEC 1508 -standardiluonnokseen. Läpikäynti toteutettiin osittain tiimityönä ja osittain suunnittelijoiden omana katselmuksena. Suunnittelijat antoivat kullekin menetelmälle, tekniikalle tai toimenpiteelle arvosanan sen mukaan, miten hyvin he omasta mielestään ovat soveltaneet kutakin tekniikkaa laitteisto- ja ohjelmistosuunnittelussa ja muissa turvallisuuden elinkaaren vaiheissa.

Tämäntyyppiselle järjestelmälle ei ole standardia, joka määrittelisi, mitä tasoa turvallisuuden pitäisi toteuttaa. Järjestelmää analysoitaessa toteutusta verrattiin IEC 1508:n eheystasoon 1, joka vastaa likimain eurooppalaisen standardiluonnoksen 954-1:n kategoriaa 2 (tilanne marraskuussa 1995).

Ohjausjärjestelmän laitteisto, kuten myös ohjelmisto, on eri vaiheissaan toteutettu käyttäen melko kattavasti niitä tekniikoita ja menetelmiä, joita IEC 1508 -standardiluonnos määrittelee erittäin suositeltaviksi. Sekä laitteiston että ohjelmiston osalta löytyi vain pieniä puutteita suosituksiin nähden. (Toisaalta standardikaan ei ole vielä valmis.) Vikojen hallitsemiseksi on käytetty pääsääntöisesti hyväksi havaittuja menetelmiä.

Suunnittelijat ovat dokumenteissaan huomioineet turvallisuuden elinkaaren eri vaiheet ja niihin liittyvät asiat melko kattavasti lähtien käsityksen muodostamisesta ohjattavasta järjestelmästä ja päättyen käytöstä poistoon. Parhaiten tai laadukkaimmin dokumentointi oli toteutettu laitteiston, ohjelmiston ja koko järjestelmän osalta turvallisuusvaatimusten määrittelyvaiheessa. Pääasiallisimmat puutteet

dokumentoinnissa liittyvät vaara- ja riskianalyysiin sekä turvallisuusvaatimusten allokointiin ja toteutukseen, joihin tämä tutkimus tosin toi täydennystä. Järjestelmästä tehtyjä dokumentteja ei tutkimuksen kuluessa VTT:llä tarkasteltu muutamaa kaaviota ja selostusta lukuun ottamatta, vaan dokumenttien laatuun ja laajuuteen liittyvät arviot olivat suunnittelijoiden tekemiä.

6 YHTEENVETO

Tämän julkaisun luvussa 2 tuodaan esiin turvallisuuteen liittyviä elektronisia järjestelmiä koskevia määräyksiä, joita sovelletaan myös hajautettuihin CAN-väyläjärjestelmiin. Standardin SFS-EN 60204-1 mukaan luokan 1 hätäpysäytys voidaan toteuttaa CAN-väylän kautta. Tätä hätäpysäytystä käytettäessä lopullinen tehon poistaminen koneen toimilaitteilta on kuitenkin varmistettava ja toteutettava sähkömekaanisilla komponenteilla.

Hankkeessa tuotettiin tietoa CAN-kommunikointijärjestelmän vikamuodoista, joista tyypillisimpiä ovat kaapeli- ja liitinviat. Luvussa 3 esitetään vikatilanteet tapauksessa, jossa väyläkaapelissa on ainoastaan signaalijohtimet ja suojavaippa. Näihin lisättiin ne uudet vikatilanteet, jotka aiheutuvat käytettäessä optoerotettua CAN-väylää. Mukana ovat myös topologiavirheet.

Kahdennetun väylän käytön turvallisuustekijänä todettiin olevan melko harvinaista. Tutkimuksessa ei löydetty yhtään kytkentää tai ohjetta, miten kahdennettu väylä pitäisi toteuttaa muuna kuin optisena väylänä. Väylän itsessään on todettu olevan väylään liitettäviä laitteita luotettavampi, joten kahdennus yleensä aloitetaan näistä laitteista, mikäli se katsotaan tarpeelliseksi.

Siitä, miten CAN-järjestelmää voidaan diagnosoida ja miten diagnostiikasta saadaan apua turvallisuuteen, kerrotaan luvussa 4. Diagnostiikalla ei saavuteta vikasietoisuutta, mutta sillä voidaan ennaltaehkäistä vikoja ja vikatilanteissa mahdollistaa turvallinen toiminta.

Case-kohteiden tutkimuksessa saatiin vikapuuanalyysien avulla tietoa siitä, mitkä ovat mahdolliseen ei-toivottuun tapahtumaan johtavat syyt kussakin CAN-järjestelmässä, mitkä näistä syistä kohdistuvat CAN-väylän laitteiston tai ohjelmiston osalle ja miten järjestelmät on varmistettu ei-toivottujen tapahtumien varalta. Yhden case-kohteen osalta saatiin vika- ja vaikutusanalyysillä selville paitsi vikojen vaikutukset myös niiden paljastumistavat. PES CHECK -menetelmän avulla kartoitettiin, mitä tekniikoita ja menetelmiä CAN-järjestelmän turvallisuuden varmistamiseksi on käytetty ohjausjärjestelmän määrittely-, suunnittelu-, toteutus- ja testausvaiheissa. Näillä menetelmillä saatiin selville case-järjestelmien nykyinen turvallisuustaso. Analyysien perusteella voitiin tehdä ehdotuksia CAN-järjestelmien kehittämiseksi etenkin turvallisuuteen liittyen.

Tutkimuksessa vertailtiin myös eri käyttövarmuustekijöitä releohjauksen ja CAN-väyläjärjestelmän välillä. Kummallakin ohjausmenetelmällä on sekä etuja että haittoja. CAN-järjestelmää käytettäessä mm. on mahdollista toteuttaa älykkäämmät turvallisuusehdot ja informatiivisemmat hälytykset (esim. ennakoivat hälytykset, kulumisesta informointi, kunnonvalvonta), liittimien ja kaapelien määrä vähenee sekä uusien anturien lisääminen helpottuu. Toisaalta järjestelmä voi vikaantuessaan lamauttaa tietyn osan koko järjestelmästä, esim. CAN-moduulin jänniteregulaattorin rikkoutuminen aiheuttaa kaikkien siihen liitettyjen laitteiden toimintakyvyttömyyden. CAN-moduuli on kokonaan vaihdettava, jos se vikaantuu, mikä on kallista, mutta toisaalta releohjauksen kaapelointiin liittyvästä sähköasennustyöstä syntyy myös kustannuksia.

Julkaisussa luetellaan niitä turvallisuuteen liittyviä tekijöitä, jotka CAN-väyläjärjestelmän suunnittelussa tulee ottaa huomioon. Useimmat niistä tulisi huomioida jo suunnittelun alkuvaiheessa. Raportissa tuodaan esille myös niitä turvallisuustekniikoita, menetelmiä ja toimenpiteitä, joita hajautettujen CAN-järjestelmien laitteisto- ja ohjelmistosuunnittelussa voidaan käyttää turvallisuuden parantamiseksi ja joita ei mainita nykyisessä turvallisuuteen liittyviä järjestelmiä koskevassa IEC 1508 -standardiluonnoksessa.

Yritysten arvion mukaan hankkeen tavoitteet saavutettiin ja tuloksista saatiin konkreettista hyötyä myös niiden suunnittelukäytäntöihin. Mm. turvallisuuteen liittyvää dokumentointia voitiin täydentää ja kehittää. Suurimmat vaikutukset projektista tulevat olemaan tuotteiden seuraavien sukupolvien kehitystyöhön. Tällöin voidaan poistaa puutteita, joita tutkimuksen mukaan tuotteiden tähänastisessa kehitystyössä on tehty tai ei ole osattu riittävästi huomioida.

LÄHDELUETTELO

Alanen, J. 1992. CAN-tiedonsiirtoväylä työkoneissa. Konepajamies nro 6, s. 30 - 32.

Alanen, J. & Virtanen A. 1994. Ylemmän kerroksen CAN-kommunikointiarkkitehtuurit. Espoo: Valtion teknillinen tutkimuskeskus. 61 s. + liitt. 2 s. (VTT Tiedotteita 1561). ISBN 951-38-4495-1

Anon. CAN Specification, version 2.0. 1991. Stuttgart: Robert Bosch GmbH. 68 s.

CiA/DS201 ... CiA/DS205, CiA/DS207. 1994. CAN Application Layer (CAL). Nürnberg: CAN in Automation International Users and Manufacturers Group e.V. 130 s.

DIN 9684 Teil 3. 1993. Landmaschinen und Traktoren - Schnittstellen zur Signalüberteagung - Initialisierung, Identifier (luonnos). Berlin: DIN Deutsches Institut für Normung. 28 s.

Fredriksson, L.-B. 1995. CAN Kingdom. rev. 3.0. Kinnahult: Kvaser AB. 104 s.

Furuichi, K., Ishida, K., Enomoto, K. & Akashi, K. 1992. An Implementation of Class A Multiplex Application. Teoksessa: Multiplex Technology Applications to Vehicle Wire Harnesses. International Congress & Exposition, Detroit, Michigan Febr. 24 - 28, 1992. SAE International. S. 125 - 133.

Gergeleit, M. & Streich, M. 1994. Implementing a distributed high-resolution real-time clock using CAN-bus. Teoksessa: 1. international CAN Conference Proceedings. Erlangen: CAN in Automation e.V. S. 9-2 ... 9-7.

Honeywellin esitteet.

Hänninen, S., Järvenpää, J., Reunanen, M. & Suominen, J. 1990. Mekatronisten komponenttien ja laitteiden vikaantuminen. MET tekninen tiedotus 15/90. Metalliteollisuuden kustannus Oy. 38 s. ISBN 951-817-479-2.

IEC 870-5-1. 1990. Telecontrol equipment and systems. Part 5: Transmission protocols. International Electrotechnical Commission. 79 s.

IEC 1491. 1995. Draft. Electrical equipment of industrial machines - Serial data link for real-time communication between controls and drives. International Electrotechnical Commission. 535 s.

IEC 1508. 1995. Draft - Functional safety: safety related systems. Parts 1-7. International Electrotechnical Commission.

ISO 11898. 1993. Road vehicles - Interchange of difgital information - Controller area network (CAN) for high-speed communication. International Organization for Standardization (ISO). 58 s.

ISO/CD 11783-2. 1994. Tractors, machinery for agriculture and forestry - Serial control and communications network - Part 2: Physical layer. ISO Committee draft (ISO/TC 23/SC19N80). 23 s.

Kopetz, H. 1994. Fault Management in the Time Triggered Protocol (TTP). Warrendale: Society of Automotive Engineers (SAE). 7 s. (SAE artikkeli 940140).

Kuntz, W., Mores, R. & Morse, M.J. 1993. CAN operated on an optical double ring at improved fault-tolerance. European Transactions on Telecommunications and Related Technologies. Vol. 4, nro 4, s. 465 - 470. ISSN 1120-3862.

Kurki, M., Vostrakov, A. & Hirvinen, J. 1991. Tietokoneohjattujen työkoneiden ja -laitteiden turvallisuuden parantaminen diagnosoinnin avulla. VTT Tietokonetekniikan laboratorio, Oulu. 41 s. + liitt. 31 s

Lawson, H.W., Lindgren, M., Strömberg, M., Lundqvist, T., Lundbäck, K.-L., Johansson, L.-Å., Torin, J., Gunningberg, P. & Hansson, H. 1992. Guidelines for Basement: A Real-Time Architecture for Automotive Systems. Göteborg: Mecel, Inc. ja Lidingö: Lawson Publishing and Consulting, Inc. 42 s.

Malm, T., Vanhala, M. & Kivipuro, M. 1995. Nosturin yhdistettyjen ajotoimintojen vaikutus nostotyön turvallisuuteen. Espoo: Valtion teknillinen tutkimuskeskus. 60 s. + liitt. 10 s. (VTT Tiedotteita 1675). ISBN 951-38-4830-2

M3S Specification 2.0. 1995. An intelligent integrated and modular system for the rehabilitation environment. M3S-standardin luonnos 11.07.1995. 191 s. (Saatavilla osoitteesta: *http://www.tno.nl/instit/tpd/m3s/m3s.html*)

McLaughlin, R.T. 1993. The immunity to RF interference of a CAN system. Teoksessa: IEE Colloquium on 'Integrity of Automotive Electronic Systems', London 22 March 1993. London: IEE. S. 4/1 - 8.

Meuris, B., Vandewege, J. & Demeester, P. 1992. Implementation of an optical controller area network (CAN) using plastic optical fibre. Fiber Optics Magazine. Vol. 14, nro 9, s. 22 - 26.

PCT WO 91/10960. 1991. Arrangement for a Distributed Control System. Kent Lennartsson. Julk. 25.07.1991. 38 s. + liitt. 3 s.

Pehrs, J.-U. 1992. CAN bus failure management using the P8xC592 microcontroller. Philips Application Note, Report No: HKI/AN 91 020. Hamburg: Product Concept & Application Laboratory. 16 s.

prEN 954-1. 1994. Final draft. Safety of machinery. Safety related parts of control systems. Part 1: General principles for design. Brussels: European Committee for Standardization (CEN). 36 s.

Rauchaupt, L. 1994. Performance analysis of CAN based systems. Teoksessa: 1. international CAN Conference Proceedings. Erlangen: CAN in Automation e.V. S. 1-12 ... 1-19.

SFS-EN 292-2. 1992. Koneturvallisuus. Perusteet ja yleiset suunnitteluperiaatteet. Osa 2: Tekniset periaatteet ja spesifikaatiot. Helsinki: Suomen Standardisoimisliitto. 73 s.

SFS-EN 60204-1. 1993. Koneturvallisuus - Koneiden sähkölaitteet. Osa 1: Yleiset vaatimukset. Helsinki: Suomen Standardisoimisliitto. 212 s.

Tanaka, M., Hashimoto, K., Himino, Y. & Suzuki, A. 1991. High-reliability physical layer for in.vehicle high-speed local area network. Warrendale: Society of Automotive Engineers (SAE). 9 s. (SAE artikkeli 910464).

Tindell, K. & Burns, A. 1994. Guaranteed Message Latencies for Distributed Safety-Critical Hard Real-Time Control Networks. Technical report YCS229. York: University of York. 17 s. (Lyhennelmä myös artikkelina: Tindell, K. & Burns, A. 1994. Guaranteeing Message Latencies on Control Area Network (CAN). Teoksessa: 1. international CAN Conference Proceedings. Erlangen: CAN in Automation e.V. S. 1-1 ... 1-11.)

Tindell, K. & Hansson, H. 1995. Babbling Idiots, The Dual-Priority Protocol, And Smart CAN Controllers. Teoksessa: 2. International CAN Conference Proceedings 1995. Erlangen: CAN in Automation e.V. (fax +49-9131-601092). S. 7-22 ... 7-28.

Tiusanen, R., Hietikko, M. & Kivipuro, M. 1994. Ohjelmoitavan elektroniikan turvallisuuden arviointi. Espoo: Valtion teknillinen tutkimuskeskus. 44 s. + liitt. 4 s. (VTT Tiedotteita 1596). ISBN 951-38-4711-X

Tripp, R. P. & Hubby, R. N. 1988**.** Increased system reliability through comprehensive self diagnostics. Instrumentation in the Power Industry, Proceedings v 31. St. Petersburg, FL, USA, May 1988. S. 1 - 8. ISSN: 0074-056X.

Tuominen, P. 1995. CAN-pohjaiset reaaliaikajärjestelmät. CAN-seminaari 23.05.1995. Tampere: Tampereen teknillinen korkeakoulu (TTKK/IHA). 31 s.

Unruh, J., Mathony, H.-J. & Kaiser, K.-H. 1990. Error detection analysis of automotive communication protocols. Warrendale: Society of Automotive Engineers (SAE). 10 s. (SAE artikkeli 900699).

Vnp 1314. 1994. Valtioneuvoston päätös koneiden turvallisuudesta. 5 s. + liitt. 32 s.

Zieghan, K.-F. & Braunmiller, U. 1990. Environmental qualification of technical systems components for the vehicle environment. 22nd International Symposioum on Automotive Technology & Automation, Florence, Italy, 14th - 18th May 1990. VOL II, Automotive Automation Limited. S. 1469 - 1486. ISBN 0-947719-36-9.

OHJAUSJÄRJESTELMÄN TURVALLISUUTEEN LIITTYVIEN OSIEN KATEGORIAT

Lähde: prEN 954-1:1994

Kategoria	Yhteenveto vaatimuksista	Järjestelmän käyttäytyminen	Pääperiaate turvallisuuden saavuttamiseksi
B	Koneenohjausjärjestelmien turvallisuuteen liittyvät osat ja/tai niiden suojaavat varusteet sekä komponentit tulee suunnitella, rakentaa, valita, asentaa ja yhdistää asiaan kuuluvien standardien mukaisesti siten, että ne voivat kestää odotettavissa olevaa vaikutusta.	Vian sattuessa turvatoiminto voidaan menettää.	Komponenttien valinta
1	B-kategorian vaatimuksia on sovellettava. Lisäksi tulee käyttää hyviksi koettuja komponentteja ja turvallisuusperiaatteita.	Turvatoiminto luotettavampi kuin kohdassa B.	
2	B-kategorian vaatimuksia ja hyviksi koettuja turvallisuusperiaatteita on sovellettava. Lisäksi koneenohjausjärjestelmän tulee tarkistaa turvatoiminnot sopivin aikavälein. Se, mikä on sopiva, riippuu sovelluksesta ja konetyypistä.	Vian sattuessa tarkistusten välillä turvatoiminto voidaan menettää. Vika havaitaan tarkastustilanteessa.	
3	B-kategorian vaatimuksia ja hyviksi koettuja turvallisuusperiaatteita on sovellettava. Ohjausjärjestelmä tulee suunnitella siten, että - yksittäinen vika ohjauksessa ei johda turvatoimintojen menettämiseen ja - yksittäinen vika havaitaan aina, kun se on mielekkäästi toteuttamiskelpoista	Yksittäisen vian sattuessa turvatoiminto toteutetaan aina. Jotkut viat havaitaan, mutta ei kaikkia. Havaitsemattomien vikojen kertyminen voi johtaa turvatoiminnon menettämiseen.	Rakenne
4	B-kategorian vaatimuksia ja hyviksi koettuja turvallisuusperiaatteita on sovellettava. Ohjausjärjestelmä tulee suunnitella siten, että - yksittäinen vika ohjauksessa ei johda turvatoimintojen menettämiseen ja - yksittäinen vika havaitaan turvatoimintoa seuraavan kerran vaadittaessa tai sitä ennen. Jos tämä ei ole mahdollista, vikojen kertyminen ei saa johtaa turvatoimintojen menettämiseen.	Vikojen sattuessa turvatoiminto toteutetaan aina. Viat havaitaan siinä ajassa, mikä tarvitaan estämään turvatoimintojen menettäminen.	Rakenne