TEKNIIKKA JA LIIKENNE

Auto- ja kuljetustekniikka

Autosähkötekniikka

INSINÖÖRITYÖ

REDUNDANTTISET SÄHKÖJÄRJESTELMÄT

Työn tekijä: Timo Virtanen
Työn ohjaaja: Sami Ruotsalainen
Työn ohjaaja: Hannu Martikainen

Työ hyväksytty: ___. ___. 2009

Sami Ruotsalainen
lehtori

ALKULAUSE

Tämä insinöörityö tehtiin Patria Land & Armament Oy:n vetroniikkaosastolle. Insinöörityö oli osa syksylle 2008 sijoittunutta Redundanttisuus-tuotekehityshanketta.
Haluan kiittää kaikkia Redundanttisuus-työryhmän jäseniä. Erityiskiitoksen ansaitsee tuotekehityspäällikkö Hannu Martikainen työn ohjauksesta ja hyvien neuvojen jakamisesta työn edetessä. Kiitän myös Sami Ruotsalaista insinöörityön valvomisesta.

Hämeenlinnassa 5.5.2009

Timo Virtanen

TIIVISTELMÄ

Työn tekijä: Timo Virtanen

Työn nimi: Redundanttiset sähköjärjestelmät

Päivämäärä: 5.5.2009 **Sivumäärä:** 37 s. + 3 liitettä

Koulutusohjelma: Auto- ja kuljetustekniikka

Suuntautumisvaihtoehto: Autosähkötekniikka

Työn ohjaaja: lehtori Sami Ruotsalainen

Työn ohjaaja: tuotekehityspäällikkö Hannu Martikainen

Tämän insinöörityön tarkoituksena on tutkia redundanttisten järjestelmien käyttöä ajoneuvoteollisuuden tuotteissa. Työ tehtiin Patria Land & Armament Oy:lle.

Elektronisten laitteiden lisääntyminen ajoneuvoteollisuudessa on tuonut mukanaan uusia mahdollisuuksia sekä uudenkaltaisia uhkia. Elektronisten laitteiden riskiherkkyys ei ole huomattavasti suurempi verrattuna mekaanisiin ratkaisuihin, mutta riskien vähentäminen on haasteellisempaa. Redundanttinen järjestelmä on järjestelmä, jossa rinnakkaisia yksiköitä on enemmän kuin halutun toiminnon suorittaminen edellyttää, jolloin yhden yksikön vioittuminen tai huolto ei vaaranna järjestelmän toimintaa. Järjestelmä sisältää esimerkiksi n +1 yksikköä, joista n yksikköä riittää suorittamaan halutun toiminnon.

Ajoneuvoissa on perustoimintaan liittyviä ratkaisuja, jotka on perinteisesti toteutettu mekaanisesti, kuten ohjaus sekä jarrut. Vasta näinä päivinä mekaanisten toteutusten rinnalle on haettu sähköisiä ratkaisuja. Sähköisten jarrujen sekä ohjauksen edut ovat kiistattomat: komponenttien sijoittelu on vapaampaa, tarkkuus kasvaa, huoltoa kaipaavat komponentit havaitaan aiemmin ja niin edelleen. Toisaalta luotettavuuden takia redundanttisuus on välttämätöntä, ja toimilaitteita varmistettaessa myös kustannukset nousevat. Vikaherkkyyden lisäksi myös lainsäädäntö estää täysin sähköisen ratkaisun. Ajoneuvoissa on alettu käyttää ilmailuteollisuudesta tuttuja ratkaisuja niissä kohteissa, joissa se on lainsäädännöllisesti ollut mahdollista.

Avainsanat: Redundanttisuus, elektroninen luotettavuus, MTBF

Metropolia

ABSTRACT

Name: Timo Virtanen

Title: Redundant Electrical Systems

Date: 5 May 2009 **Number of pages:** 37 pages + 3 appendices

Department: Automotive & Transport

Study Programme: Automotive Electronics

Instructor: Sami Ruotsalainen, Lecturer

Instructor: Hannu Martikainen, R&D Director

The objective of this graduate study is to research redundant systems in automotive products. Study was assigned by Patria Land & Armament Oy.

The increasing number of electrical equipment in automotive industry has brought new kind of opportunities, but threats as well. Risk rate of electrical devices is not noticeably bigger compared to mechanical solutions, but risk reduction is more challenging. A redundant system is a system, where number of parallel units is bigger than the number units needed for operating the function in question, in other words one unit failure or service does not endanger functionality of the system. The system includes for example n + 1 units and the system can be operated with n unit.

Basic solutions that traditionally operate mechanically, such as steering and brakes, can be found in vehicles. More and more mechanical solutions are nowadays replaced by electrical designs. The benefits of electrical steering and braking systems are undeniable. There are more options to mount the components, handling is more accurately, components needing service can be found earlier and so on. There are also disadvantages. Redundancy is necessary for reliability, thus weight and costs are increasing as well. It appears that development has taken the vehicles closer and closer to aeronautical systems.

Keywords: Redundancy, electronics reliability, MTBF

SISÄLLYS

LYHENTEIDEN SELITYKSET

ABS	Antilock brake system
AMOS	Advanced Mortar System
AMV	Armoured Modular Vehicle
CAN	Controller Area Network
MTBF	Mean time between failure
NBC	Nuclear, Biological, Chemical
PLC	Power Line Communication
SSWG	System safety workgroup
VVKA	Vika-, vaikutus- ja kriittisyysanalyysi

1 JOHDANTO

Tämä insinöörityö tehtiin Patria Land & Armament Oy:n vetroniikka-osastolle. Patria on kansainvälisesti toimiva puolustus- ja ilmailuteollisuuskonserni, joka toimittaa omaan erityisosaamiseensa ja kumppanuuksiin perustuvia ratkaisuja asiakkailleen. Land & Armament -liiketoimintayksikkö kehittää ja valmistaa panssariajoneuvoja ja kranaatinheitinjärjestelmiä. Liiketoimintayksikön päätuotteet ovat AMV-panssariajoneuvo ja AMOS-kranaatinheitinjärjestelmä.

Redundanttinen järjestelmä on järjestelmä, jossa rinnakkaisia yksiköitä on enemmän kuin halutun toiminnon suorittaminen edellyttää, eli yhden yksikön vioittuminen tai huolto ei vaaranna järjestelmän toimintaa. Järjestelmä sisältää esimerkiksi n +1 yksikköä, joista n yksikköä riittää suorittamaan halutun toiminnon. [1, s. 91.]

Tämän dokumentin tarkoituksena on esitellä ajoneuvoteollisuudessa käytettyjä redundantteja ratkaisuja. Esitetty materiaali toimii tukevana materiaalina suunnittelijalle syventämällä redundanttiuden käsitettä. Näin redundantit vaatimukset tunnistetaan jo tuotteiden suunnitteluvaiheen alussa ja ne osataan ottaa entistä paremmin huomioon. Dokumentti alkaa katsauksella vikaantuvista kohteista, joihin varmennus olisi kohdistettava. Tämän jälkeen vertaillaan yleisimpiä käytössä olevia varmennusratkaisuja ja siirrytään edelleen vikaantuvien kohteiden analysointimenetelmiin. Varmentamisella pyritään riskin, epäedullisen tapahtuman minimoimiseen. Siitä syystä riskien analysointiin on esitelty ajoneuvoteollisuudessa käytettäviä riskianalyyseja. Jälkimmäisessä vaiheessa painoarvo siirtyy ajoneuvokäytössä oleviin redundanttisiin ratkaisuihin.

1.1 Vikaantuvat kohteet

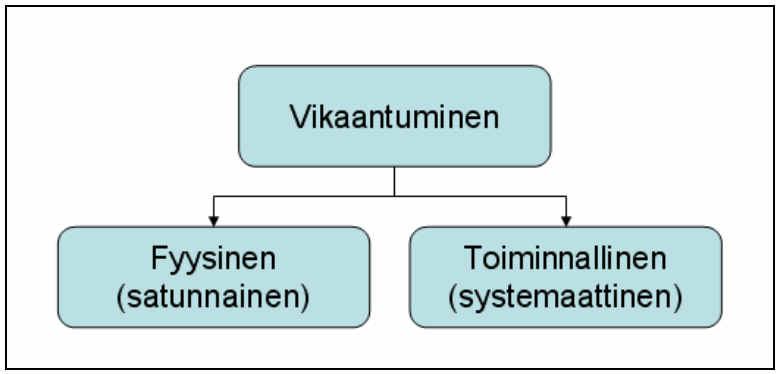
Vikaantuminen tapahtuu silloin, kun laite (järjestelmä, yksikkö, moduuli tai komponentti) ei kykene suorittamaan sille tarkoitettua toimintoa. Järjestelmien vikaantumisen estämiseksi on syytä perehtyä vian aiheuttaviin syihin. Kun vikaantumisen syy selviää, on järjestelmien rakenteita mahdollista parantaa.

Jotta järjestelmä voidaan ymmärtää riittävän syvästi, on tarkasteltava sen kaikki tasot. Turvallisuus- ja luotettavuusnäkökulmia analysoidessa voidaan määritellä neljä eri tasoa. Järjestelmä koostuu yksiköistä. Mikäli järjestelmä on redundanttinen, käytetään useampia yksiköitä. Yksiköt koostuvat moduuleista ja moduulit puolestaan koostuvat komponenteista.

Monet ohjausjärjestelmät rakentuvat edellä mainittujen tasojen perusteella. Siitä huolimatta, että rakenne välttämättä seuraa orjallisesti taso-ajattelua, käytetään sitä turvallisuuden ja luotettavuuden analysoinnissa. [2, s. 31.]

1.1.1 Vikaantumisen tyypit

Vikaantumiset voidaan jakaa lähteidensä perusteella kahteen eri kategoriaan. Kategoriat ovat fyysiset sekä toiminnalliset viat. Vikojen jakoa kahteen tukee myös vikojen esiintymisväli. Fyysiset viat esiintyvät satunnaisesti ja toiminnalliset systemaattisesti, aina samalla tavalla. Kategoriat ovat esitetty kuvassa 1.



Kuva 1. Vikaantumisen tyypit [lähdettä 2 mukaillen]

Fyysinen vikaantuminen

Fyysistä vikaantumista kutsutaan nimellä satunnainen vikaantuminen. Monessa tapauksessa ainoastaan fyysinen vikaantuminen mielletään oikeaksi viaksi. Vikaantuminen tapahtuu silloin kun komponentti tai moduulin sisäinen komponentti vikaantuu. Vika on useimmiten pysyvä. Se voidaan estää tai ainakin riskiä voidaan vähentää testaamalla komponenttia riittävästi ennen sen käyttöönottoa tai valitsemalla etukäteen riittävän suuren luotettavuustason omaavia komponentteja. Tyypillinen esimerkki fyysisestä vikaantumisesta on löysän liitoksen aiheuttama kontaktin häviäminen. Toinen, yleinen vikatilanne on tehonsyötön halvaantuminen, syöttömoduulin ulostulosta ei tule jännitettä. Tehonsyötön tarkastelu osoittaa, että kondensaattorin varauk-

senottokyky on heikennyt huomattavasti. Varauksenottokyvyn huonontuminen johtaa lopulta tilanteeseen, jossa kondensaattorit eivät pysty ylläpitämään latausta ja niistä tulee avoimia piirejä. Varauskyvyn huonontuminen tapahtuu pitkän aikavälin kuluessa, joten syiden analysointi on haasteellista. Kuitenkin syihin päästään käsiksi luomalla jokaisesta vikaantumistapahtumasta kuvaustaulukko (taulukko 1). [2, s. 34-35.]

Taulukko 1. Esimerkki vian kuvaustaulukosta [lähdettä 2 mukaillen]

Otsikko	Tehonsyötön halvaantuminen
Vikaantumisen päällimmäinen syy	Kondensaattorin varauskyvyn heikentyminen
Vikaantumisen tyyppi	Fyysinen
Ensisijainen aiheuttaja	Jännite, virta
Toissijainen aiheuttaja	Lämpötila, heikko kotelointi

Toiminnallinen vikaantuminen

Toiminnallinen vikaantuminen tarkoittaa tilannetta, missä järjestelmä kykenee toimimaan, muttei suorita haluttua funktiota. Tyypillinen esimerkki tilanteesta on ohjelmiston kaatuminen. Ohjainyksikkö ei kykene suorittamaan haluttua toimintoa, mutta mikään komponenteista ei ole vikaantunut, fyysistä vikaa ei ilmennyt. Toiminnallisen vian ohittaminen on mahdollista järjestelmän resetoinnin avulla, toisin kuin fyysisen vian. Vikaantuminen on usein seuraus suunnitteluvirheestä. Toiminnallisia vikaantumisia on vaikeata analysoida, mutta mahdollisuuksia on olemassa. Yksi tapa havainnointiin on automaattisien lokien avulla, niihin voidaan tallentaa vian ilmetessä vallinneet olosuhteet, kuten suoritettu komento ja antureiden sen hetkiset arvot. [2, s. 35–36.]

Kumpikin vikaantumistyyppi sisältää attribuutteja, jotka ovat tärkeitä system safety- sekä luotettavuusanalyyseihin. Attribuuttien sisältämää tietoa tarvitaan määritellessä miten tulevaisuudessa vastaavat vikaantumiset voidaan välttää.

1.1.2 Vikaantumisen aiheuttajat

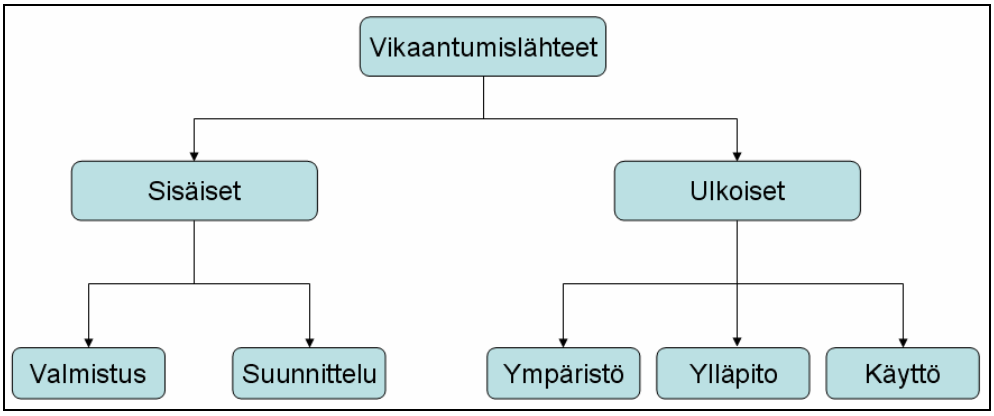
Taulukossa 2 on esitelty häiriötilanteita, joita esiintyy sähköisissä laitteissa. Häiriötilanteen tyypin lisäksi taulukossa on oma sarakkeensa häiriön luokalle. Kohta häiriönlähde edellä mainitussa sarakkeessa tarkoittaa sitä, että kyseinen ilmiö voi aiheuttaa joko toiminnallisen tai fyysisen häiriön.

Taulukko 2. Sähkölaitteiden tyypillisiä häiriötilanteita [lähdettä 2 mukaillen.]

Tyyppi	**Luokka**
Kosteus	Häiriön lähde
Ohjelmointivirheet	Toiminnallinen häiriö
Lämpötila	Häiriön lähde
Häiriöjännitepiikki	Häiriön lähde
Järjestelmän suunnitteluvirhe	Toiminnallinen häiriö
Elektrostaattinen piikki, ESD	Häiriön lähde
Akun loppuun kuluminen	Fyysinen häiriö
Rikkoutuneet johtimet	Fyysinen häiriö
Korroosion aiheuttamat katkokset	Fyysinen häiriö
Satunnaisen komponentin hajoaminen	Fyysinen häiriö
Korjaajan tekemä virhe	Häiriön lähde
Radiotaajuinen kohina, RFI	Häiriön lähde
Väärän kytkimen ohjaus	Toiminnallinen häiriö
Värinä	Häiriön lähde
Puutteellinen maadoitus	Häiriön lähde
Väärä ladattu konfiguraatio	Toiminnallinen häiriö
Väärä korvaaja	Toiminnallinen häiriö
Komponentti valmistettu virheellisesti	Häiriön lähde
Väärä ohjelmistoversio asennettu	Toiminnallinen häiriö

Monet tekijät voivat aiheuttaa vikaantumisen, yksinään tai yhdistettynä johonkin toiseen. Esimerkiksi kosteus ei yksinään aiheuta vikaantumista. Laitteiden luvataan toimivan, mikäli kosteusprosentti on 10:n ja 90:n välisellä alueella. Kuitenkin kosteus kiihdyttää korroosion etenemistä, ja pahoin korroosiosta kärsivä kontakti tulee lopulta pettämään. Korroosio on siis syy vikaantumiseen, mutta kosteus on kiihdyttänyt sen etenemistä. Kosteus olisi syynä, mikäli asetettu korkeusprosentti ylittyisi ja liitinpintaan kondensoituisi vettä aiheuttaen fyysisen vikaantumisen. Vikaantumista aiheuttavat kuvan 2 mukaisesti sekä sisäiset että ulkoiset tekijät. Sisäiset tekijät ovat tulosta ma-

teriaali-, valmistus- sekä suunnitteluvirheistä. Virhe voi ilmetä mille tahansa tasoille, komponenteille, moduuleille, yksiköille tai järjestelmille. [2, s. 37-38.]



Kuva 2. Vikaantumislähteet [lähdettä 2 mukaillen]

Sisäinen - Suunnittelu

Suunnitteluvirheet ovat suurin syy toiminnalliselle vikaantumiselle. Joissain tapauksissa on mahdollista, että suunnittelija ei tunne koko järjestelmää, koska hän työskentelee pienemmän osa-alueen kanssa. On myös mahdollista, että laitetta käytetään ympäristössä, jossa suunnittelija ei ole sitä ajatellun käytettävän. [2, s. 38.]

Sisäinen - Valmistus

Valmistusvirhe ilmenee silloin, kun jokin komponentin, moduulin, yksikön tai järjestelmän valmistusvaihe on tehty virheellisesti. Monessa tapauksessa valmistusvirhe laskee komponentin kestävyyttä ja siten vähentää sen käyttöikää. [2, s. 39–40.]

Ulkoinen - Ylläpito

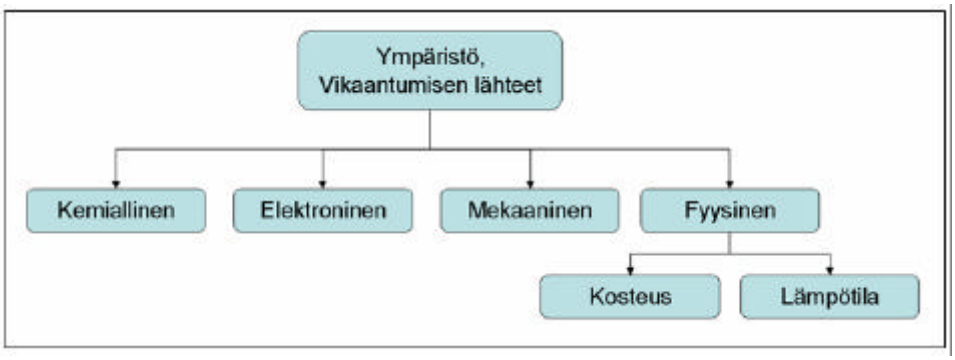
Ylläpidosta aiheutuvat vikaantumislähteet liittyvät suoraan ylläpidon laiminlyöntiin. Tällöin laitteita ei ole huollettu säännöllisesti tai huoltoa ei ole suoritettu ohjeiden mukaistesti. Tilanne johtaa laitteen vikaantumiseen sen elinkaaren keskivaiheilla ja siten vähentää laitteen suunniteltua elinikää. [2, s. 43.]

Ulkoinen - Käyttö

Laitteen käyttäminen ohjeiden vastaisesti johtaa samaan tilanteeseen kuin ylläpidon laiminlyöntikin ja laitteen elinikä lyhenee huomattavasti. [2, s. 43.]

Ulkoinen - Ympäristö

Ympäristön aiheuttamilla vikaantumisilla tarkoitetaan vikoja, jotka ilmenevät toimintaympäristön erityispiirteiden takia. Edelleen ympäristön vikaantumiset voidaan jakaa alempiin tekijöihin (kuva 3). [2, s. 40.]

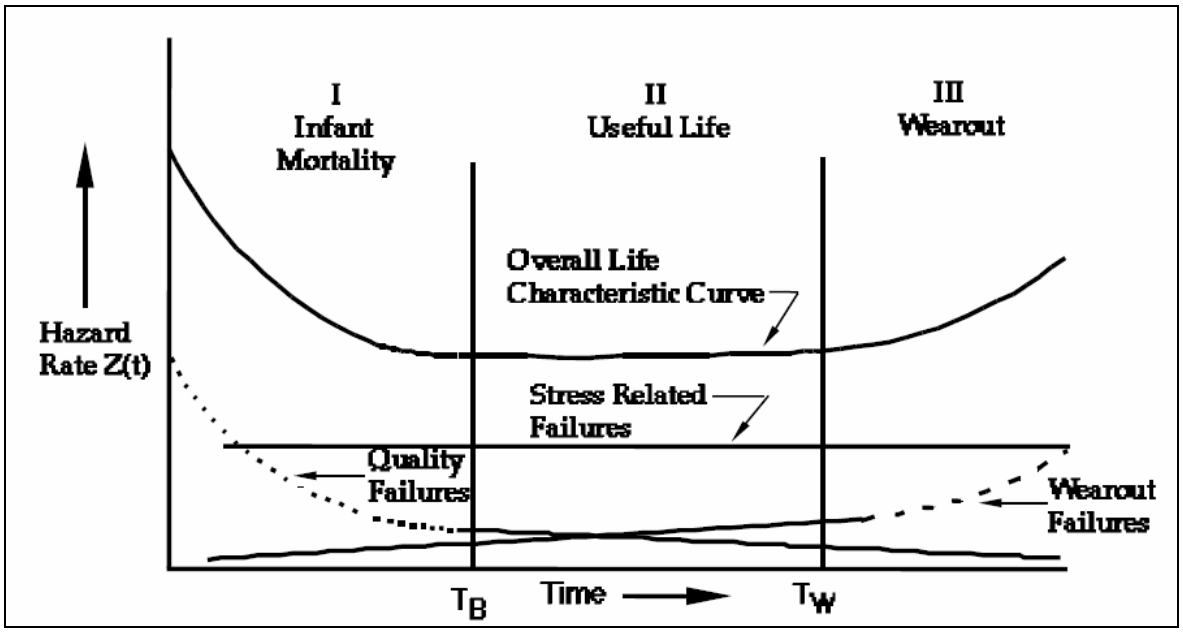


Kuva 3. Ympäristön vikaantumislähteet [lähdettä 2 mukaillen]

Kemiallisia vikaantumislähteitä voivat olla syövyttävät kemikaalit. Elektronisella vikaantumisella tarkoitetaan vikaa, joka syntyy toisen samassa piirissä olevan laitteen vikaantumisen takia. Elektronista vikaantumista voidaan estää komponenttien valinnalla. Valitsemalla toimintavarmempia komponentteja alkuperäiseen kokoonpanoon ja suojaamalla ne huolellisesti, saadaan tämän vikatyypin ongelmia vähennettyä huomattavasti. Mekaanisia vikaantumislähteitä esiintyy aina ajoneuvojen yhteydessä. Ajoneuvon liikkuessa syntyy harmonisia sekä epäsäännöllisiä värähtelyitä, joita pyritään ehkäisemään mekaanisten ratkaisujen avulla. Värähtelyjen estäminen täysin on mahdotonta, mutta niiden määrää voidaan vähentää suunnittelun avulla. Sähkölaitteille kriittisimpiä vikaantumissyitä ovat fyysiset olosuhteet. Kosteus sekä rajut lämpötilamuutokset ovat ongelmallisia, mutta niiden vaikutusta voidaan suunnittelun avulla ehkäistä. Muun muassa liittimien valinta sekä laitteiden huolellinen kotelointi ovat tehokkaita keinoja. [2, s. 40–43.]

1.1.3 Vikaantumiskuvaaja

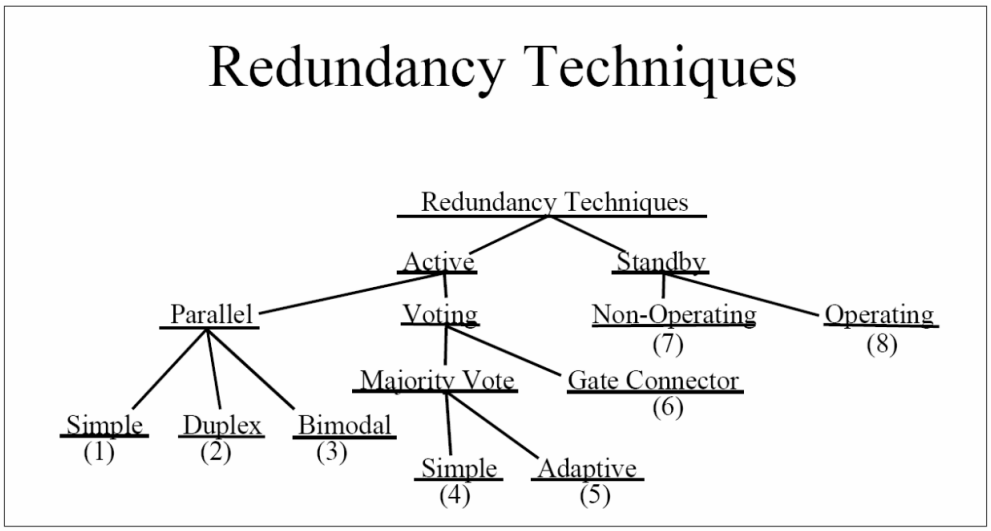
Vikaantumiskuvaaja (failure rate curve) esittää tyypillisen laitteen vikaantumiskäyttäytymisen eri ajanjaksoilla (kuva 4). Kuvaajan mukaisesti laitteen vikaantumisriski Z on suurimmillaan laitteen heti käyttöönoton jälkeen (alue I, Infant Mortality). Infant Mortalitylla tarkoitetaan uuden laitteen haavoittuvuutta. Alueella I oleva kuvaaja muodostuu kahden eri virhetyypin muodostamana, lineaarisesti käyttäytyvän kuormituksen aiheuttama vikaantumisen (stress related failures) sekä laatuvikojen aiheuttaman vikaantumisen (quality failures), joka ilmenee laskeva toisen asteen kuvaajana. Laitteessa on laatutekijöihin liittyvät virheet ilmenevät siis alueen I aikana. Niiden ilmeneminen on todennäköisintä heti laitteen käynnistyksen jälkeen. Kokonaiskäytettävyyden kuvaaja (Overall Life Characteristic Curve) muovautuu kahden edellä mainitun kuvaajan summasta. Alue loppuu ajanhetkeen T_B, jonka jälkeen laitteelle ei enää ilmene laatuun liittyviä vikoja. Mikäli laitteella on riittävä laatutaso, saavuttaa se alueen II (Useful life). Alueella II laitteen toiminta on lineaarista, sillä sen toimintaan liittyy ainoastaan lineaarisesti käyttäytyvä kuormituksen aiheuttama vikaantuminen. Aluetta III kutsutaan nimellä loppuun kuluminen (Wearout). Loppuunkuluminen alkaa ajankohdasta T_W, jonka jälkeen kuormituksen aiheuttamaan vikaantumiseen lisätään loppuun kulumisen aiheuttamat vikaantumiset (Wearout failures). Tämä kuvaaja on laatuvikojen aiheuttamia vikaantumisia esittävät kuvaajan kaltainen, mutta vastakkaisen suuntainen, kuvaaja nousee toisen asteen kulmakertoimella ajansuhteen funktiona. Aluetta II on syytä tavoitella jo suunnitteluvaiheessa. Komponenttien laadulla saadaan vaihetta yksi ajallisesti lyhennettyä. Laadun parannuttua siirtyy kokonaiskäytettävyyden kuvaajan alkupiste alemmaksi, ja siten kuvaajan laskeutuminen alueen II tasolle tapahtuu nopeammin. Laadun parantaminen pidentää myös aluetta II ajallisesti, alueen III saavuttamista ei voida millään ratkaisulla estää, mutta se voidaan siirtää ajallisesti mahdollisimman pitkälle. [3, s. 5-28–5-29.]



Kuva 4. Vikaantumiskuvaaja. [3, s. 5-29.]

2 REDUNDANTTIUS

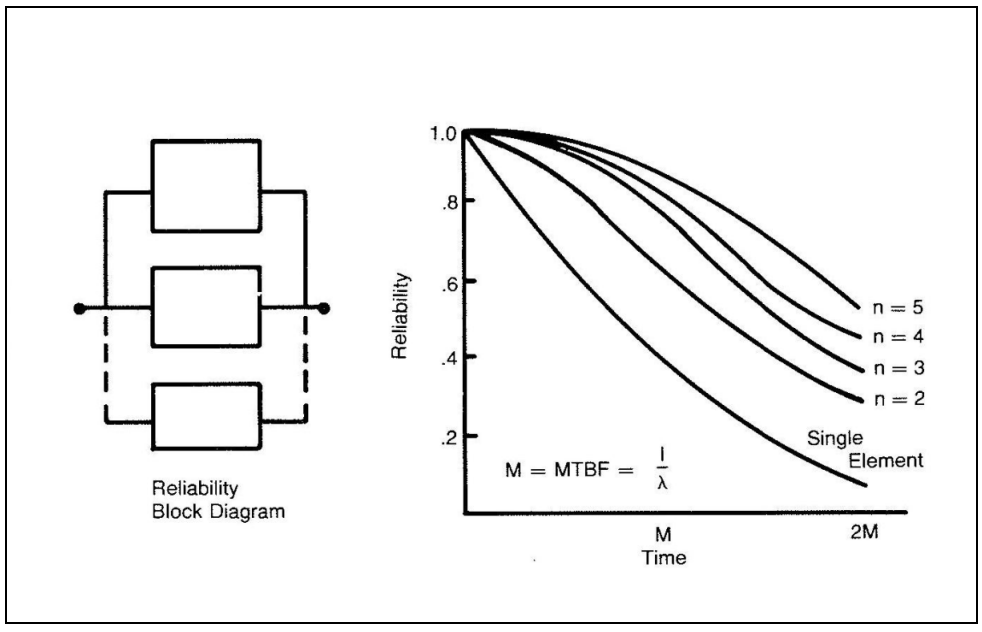
Redundanttisilla järjestelmillä tavoitellaan toimintavarmuuden maksimointia. Mitä kriittisempi laite on, sitä toimintavarmempi sen on oltava. Ajoneuvoissa yleisesti käytettyjä redundansseja ovat vikaherkkien sähköisten ja hydraulisten toimintojen korvaaminen mekaanisilla ratkaisuilla. Kuitenkin tässä insinöörityössä keskitytään elektroniikan redundanssien suunnitteluun sekä analysointiin. Redundanssit voidaan jakaa toiminnallisuutensa perusteella kahteen pääryhmään, aktiiviseen (active redundancy) sekä valmiudessa olevaan (stand by). Aktiivisessa ratkaisussa erinäistä, vian tunnistavaa ja viallisen laitteen poissulkevaa yksikköä ei tarvita. Rinnakkaiset laitteet ovat siis jatkuvasti toiminnassa. Valmiudessa olevassa ratkaisussa korvaava laite nimensä mukaisesti aktivoidaan vain tarvittaessa, joten edellä mainittuja toimintoja suorittava, erillinen yksikkö on välttämätön. Kumpikin pääryhmä jakaantuu useampaan alaryhmään (kuva 5). [4, s. 319.]



Kuva 5. Redundantit järjestelmät. [4, s. 319]

2.1 Simple paraller

Simple paraller on redundanssiratkaisuista yksinkertaisin. Nimensä mukaisesti ratkaisussa on rinnakkain (paraller) useita yksiköitä. Yksikköjen määrä määrittää suoraan varmuustason. Seuraavana on esiteltynä lohkokaavio sekä luotettavuuden tasosta kertova kuvaaja (kuva 6). [4, s. 320.]



Kuva 6. Simple paraller -järjestelmä ja sen luotettavuuskuvaaja [4, s. 320]

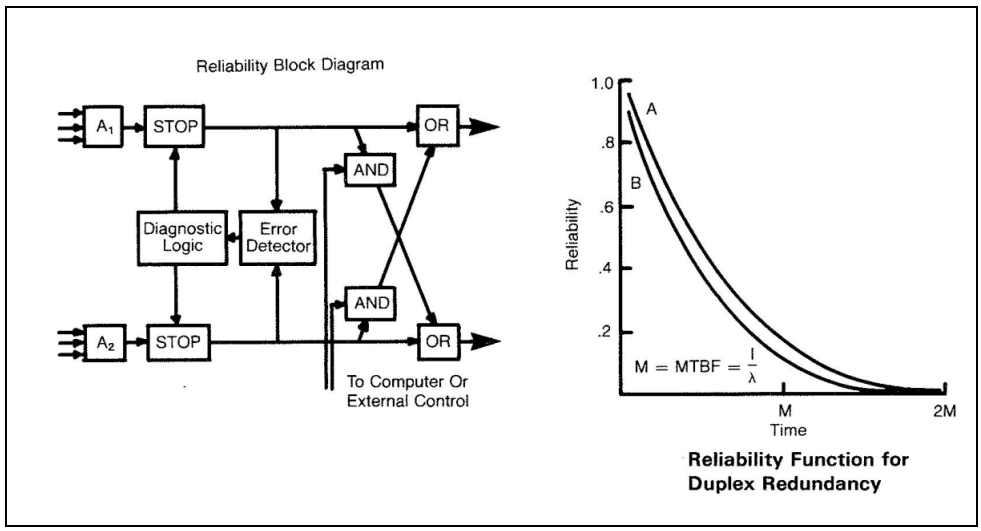
Kuvaajissa Y-akseli kertoo varmuustason (Reliability). 1,0 taso vastaa 100 prosentin varmuustasoa. X-akseli ilmaisee toimintakelpoisuusajan, jonka yksikkö on yhtämittaisesti aktiivisena. Kuvaajassa esiintyvä määritelmä MTBF on lyhenne sanoista mean time between failures. MTBF siis tarkoittaa keskimääräistä aikaa sen edellistä käyttökuntoon saattamisen ja uudelleen vikaantumisen välillä. Koska redundanttisissa järjestelmissä on enemmän kuin yksi laite, on koko järjestelmän toimintakelpoisuusaika enemmän kuin MTBF. Tällöin on järkevää käyttää ajanjaksoja aina 2M:ään asti (M = MTBF). Kirjain n ilmaisee käytettävien yksiköiden määrän. [5.]

Kuvaajaa tulkitessa voidaan huomata, kuinka laitteen toimintavarmuus laskee sen mukaisesti, kuinka kauan laitetta pidetään aktiivisena. Samalla havaitaan, että varmuus ajan funktiona kasvaa sen mukaisesti, kuinka monta yksikköä rinnakkain on asennettuna. Yksinään toimiva yksikkö saavuttaa ajassa 2M noin 10 prosentin varmuustason, kun taas viittä yksikköä käyttämällä saavutetaan 60 prosentin taso. Ratkaisun etuna on yksinkertaisuus, sen käyttöönotto vaatii pieniä muutoksia ja siten sitä voidaan pitää kustannustehokkaana. Sitä voidaan käyttää sekä analogi- että digitaalipiirien yhteydessä. Huonoina puolina voidaan pitää virtakuormien jakamista yksiköiden kesken, samasta syystä ratkaisu voi aiheuttaa suunnitteluvaikeuksia. Lisäksi vikaantumisen etenemisen estäminen eli vikaantuneen laitteen eristäminen on vaikeaa. [4, s. 323.]

2.2 Duplex

Duplex-tekniikka logiikkapiireille tarkoitettu ratkaisu. Ratkaisu vaatii kaksi signaalin sisääntuloa, tulot A1 sekö A2. Signaalit ovat keskenään identtisiä, ja niitä seurataan Error Detection -toimilaitteen avulla. Mikäli Error Detection havaitsee signaalin poikkeavan normaalista, logiikkapiireillä käytettävästi 0 tai 5,0 Voltin jännitteestä, kytkee se Stop-estotoiminnon Diagnostic Logic-laitteen välityksellä. And-logiikkapiiri yhdistettynä Or-logiikkapiiriin saadaan sama signaali kummastakin ulostulosta samansuuruisina ulos. And kopioi suoraan rinnakkaisen signaalin, ja Or havaitsee, ettei sisääntulosta tule signaalia Stop-toimilaitteen sen estettyä, ja valitsee Andin läpi tulleen signaalin. And-toimilaitteita voidaan lisäksi valvoa ulkoisella tietokoneella erillisellä ohjainlaitteella. Tekniikan tarkoituksena on ainoastaan estää virheellisen ohja-

uslogiikan aiheuttaman häiriön siirtymisen muihin logiikkapiireihin. Toiminta sekä luotettavuuskuvaaja selviää kuvasta 7. [4, s. 325.]



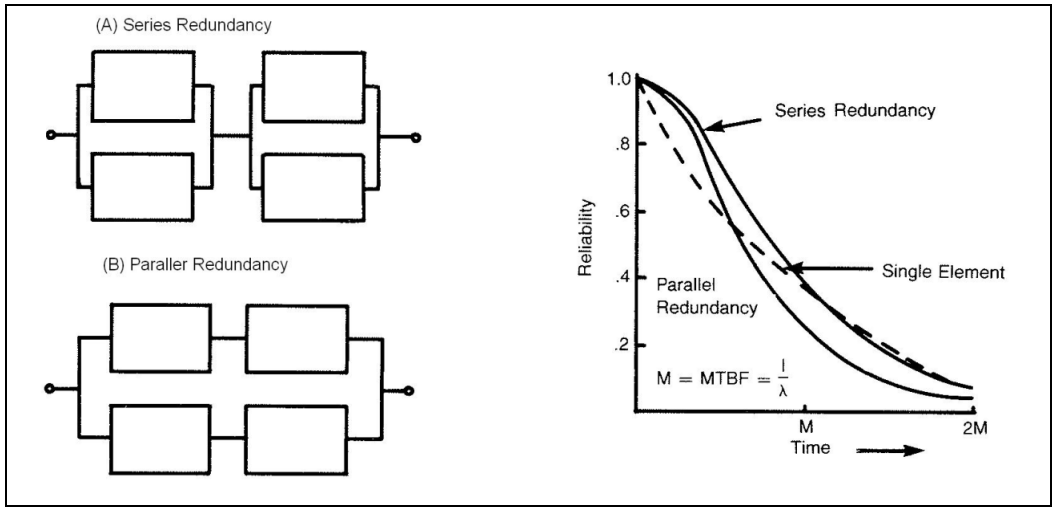
Kuva 7. Duplex -järjestelmä ja sen luotettavuuskuvaaja [4, s. 320]

Kuvaajassa esitetyt käyrät esittävät toimilaitteiden yhdistelmien luotettavuustasoja. Käyrään A on sisällytetty Error detector tai Diagnostics -toimilaitteen luotettavuustaso. Käyrä B huomioi näiden laitteiden yhdistelmän. Kuten kuvaajasta voidaan havaita, laitteiden yhdistelmä ei kykene samaan varmuustasoon kuin yksittäinen toimilaite. Useamman toimilaitteen yhdistelmä lisää riskin suuruutta, sillä kummankin laitteen oma vikaantumisriski kertaantuu yhdistelmään. Järjestelyn etuna on suojautumismahdollisuus katkoksia sekä lyhytaikaisia virhetiloja vastaan. Haittapuolina voi olla diagnoosiohjelmiston tarve sekä anturoinnin monimutkaisempi rakenne. [4, s. 325.]

2.3 Bimodal

Bimodal on Simple Parallerin kaltainen järjestely, jossa yksiköt ovat rinnakkaisuuden lisäksi asennettuna peräkkäin kuvan 8 mukaisesti. Peräkkäisten yksikköjen avulla saadaan varmistettua piirin toiminta siinä tapauksessa, että jokin yksiköistä vikaantuu. Näin vikaantuminen ei pääse etenemään piirissä pidemmälle, koska toinen saman ryhmän laitteista jatkaa toimintaa normaalisti. Bimodal voidaan toteuttaa kahdella tavalla riippuen siitä, minkälaisiin vikoihin piirissä halutaan varautua. Kytkentä A on järkevä silloin, kun halutaan varautua vikaan, jossa yksikkö muuttuu avoimeksi piiriksi. Tällöin signaali kulkee kytkennän keskellä olevan solmupisteen kautta, eikä vaikuta järjes-

telmän toimivuuteen. Kytkentä B:tä käytetään yksiköiden yhteydessä, joilla on taipumus oikosulkea itsensä vikaantuessa. Tällöin laite muuttuu suoraksi kytkennäksi, mutta järjestelmä kykenee jatkamaan toimintaa sarjaan kytketyn redundanssin avulla. [4, s. 324.]



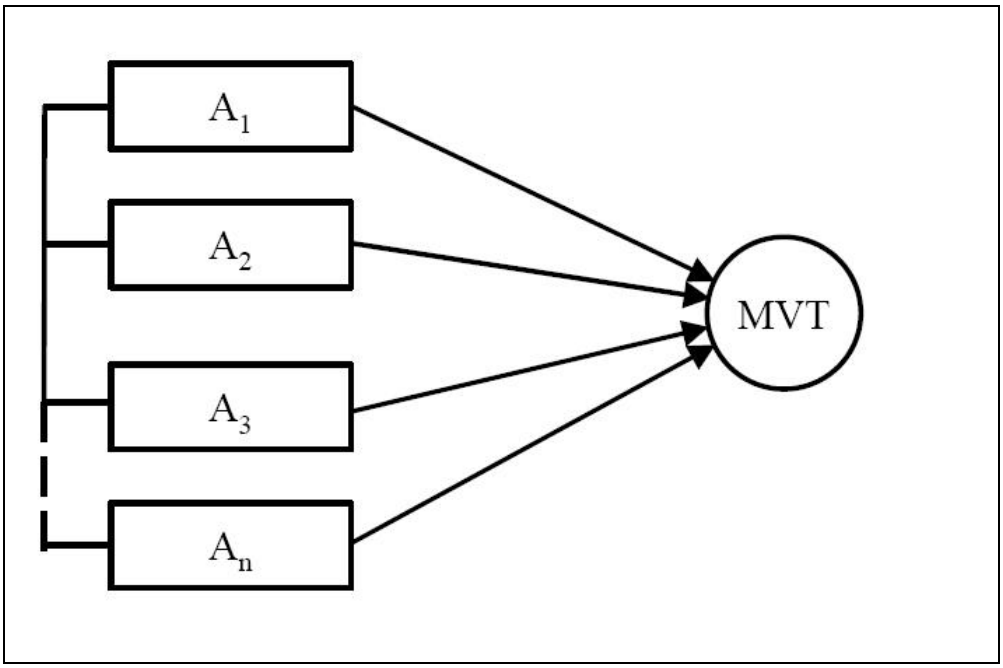
Kuva 8. Bimodal -järjestelmä ja sen luotettavuuskuvaaja [4, s. 320]

Luotettavuuskuvaajasta huomaamme, että Bimodal-kytkennän edut tulevat lyhyellä aikavälillä esiin, mikäli vertaamme sitä katkoviivalla merkityn yksittäisen yksikön (Single Element) luotettavuuteen. Kuitenkin pidemmällä aikavälillä kytkennän rajoitteet tulevat vastaan, ajan funktiona kytkennän luotettavuus laskee samassa suhteessa verraten yksittäiseen komponenttiin. Tämä johtuu siitä, että kytkemällä yksiköitä peräkkäin, kertaa kytkentä kunkin yksikön vikaherkkyyden. Tällöin vikaherkkyydestä voi muodostua suurempi kuin yksittäisen yksikön. Kytkennässä B luotettavuus on jopa alhaisempi, ajanhetkellä M sen luotettavuus on vain 20 prosenttia, kun yksittäisen yksikön arvo samalla ajanhetkellä on noin 35 prosenttia. Bimodal-kytkentöjen luotettavuus on lyhyemmällä aikajaksolla parempi kuin yksittäisen yksikön. Esimerkiksi ajanhetkellä 0,5 M sekä A- että B-tyyppisen ratkaisun luotettavuus on noin 80 prosenttia verrattuna yksittäisen yksikön vastaavan ajanhetken 65 prosenttiin. Tämän ajanhetken jälkeen kummankin Bimodal-kytkennän luotettavuus laskee huomattavasti suuremmalla kulmakertoimella, ja ajankohdan M kohdalla A-kytkennän luotettavuus on samaa tasoa yksit-

täisen yksikön kanssa, mutta B-kytkentä häviää huomattavasti, kuten aiemmin mainittiin. Bimodal onkin siis toimiva ratkaisu piirien kohdalla, joiden toimintakelpoisuusaika (uptime) on lyhytkestoinen ja sillä voidaan estää suuren vikaantumisriskin omaavia laitteita lamauttamasta koko järjestelmää. Toisaalta ratkaisun suunnittelu voi muodostua haasteelliseksi eikä sitä voi soveltaa yksikkötasoa suurempiin kokonaisuuksiin. [4, s. 324.]

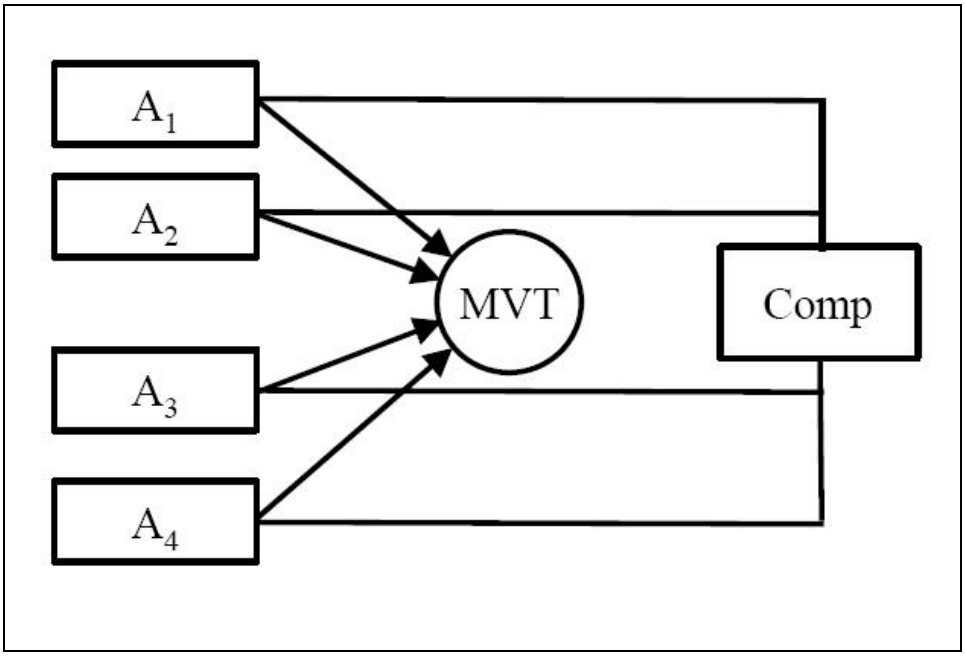
2.4 Majority Voting

Majority voting -järjestelmän perustana on yksiköiden luokittelu niin sanotun äänestyksen (voting) perusteella. Yksiköt ovat keskenään identtisiä, ja niiden antamaa signaalia verrataan jatkuvasti keskenään MVT:n (Majority Voting Transuder) toimesta. Yksiköiden lukumäärä on rajoitettu siten, ettei niiden määrä saa olla kahdella jaollinen. Tällöin yksiköiden vähimmäismäärä on kolme. MVT vertaa signaaleja keskenään ja äänestää niiden perusteella eroavan signaalin pois. Seuraavassa kuvassa (kuva 9) on esitelty yksikertaisin Majority Votingin toteutus, Simple Majority Voting. Simple Majority Voting on yksinkertaisin äänestystä käyttävä toteutus. Tässä ratkaisussa on monistettujen yksiköiden lisäksi yksi toimilaite, MVT. Huomattavaa on, että MVT tekee oikean ratkaisun vain siinä tapauksessa, että oikeaa arvoa lähettävien yksiköiden määrä on suurempi kuin vikaantuneiden. [4, s. 326.]



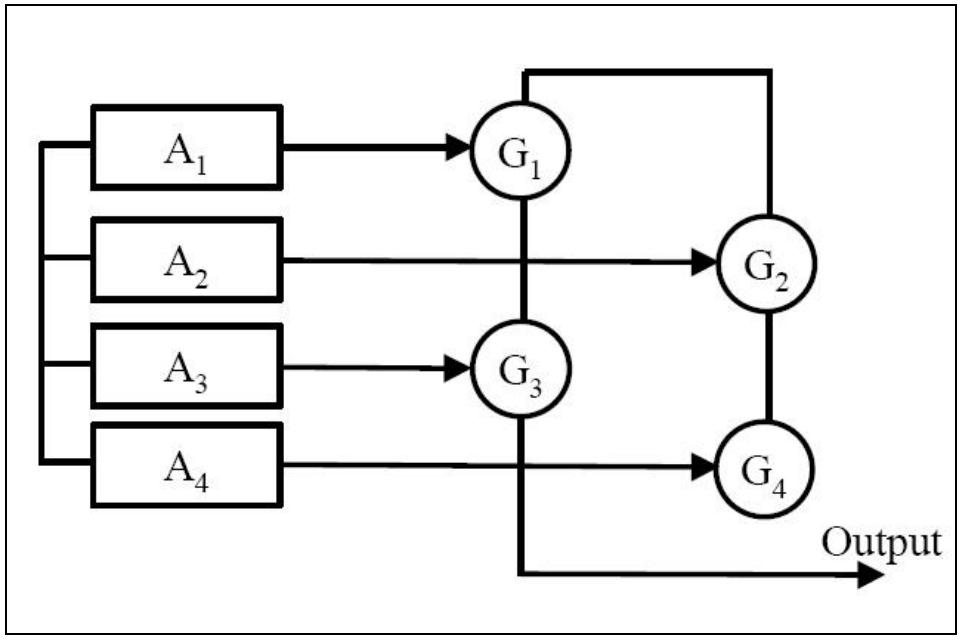
Kuva 9. Simple majority voting [4, s. 321]

Edellisen version ongelmana on tosiseikka, että mikäli useampi laite lähettää väärän signaalin, voi MVT äänestää oikeellisen signaalin pois ja käyttää virheellistä. Äänestystä voidaankin kehittää siten, että virheellinen laite eliminoidaan jo ennen, kuin se lähettää signaalin eteenpäin. Ratkaisua kutsutaan nimellä Adaptive Majority Voting (kuva 10). Tässä ratkaisussa on edellisten komponenttien lisäksi Comparator eli vertaaja. Vertaajan tehtävänä on eristää vikaantuneet laitteet äänestysjonosta. Vertaaja havaitsee ensimmäisen virheellisen signaalin, ja tässä vaiheessa eristää laitteen äänestyksestä. Näin on mahdollista välttää tilanne, jossa vikaantuneita laitteita on yhtä paljon kuin toimivia. [4, s. 326.]



Kuva 10. Adaptive majority voting -järjestelmä [4, s. 321]

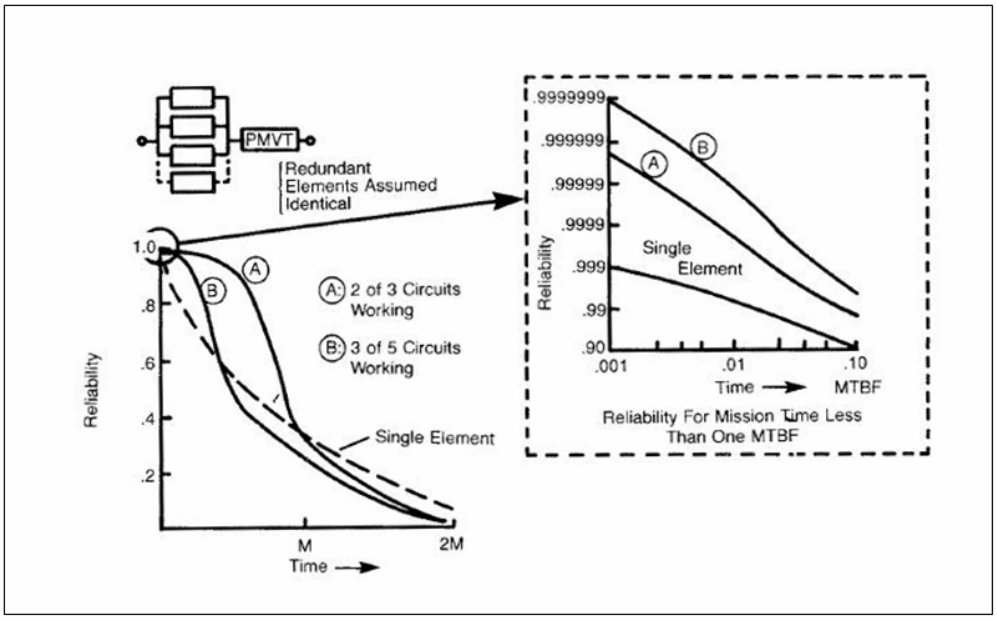
Kolmas periaatetta hyödyntävä ratkaisu, Gate Connector Voting, on toiminnaltaan samankaltainen kuin Simple Majority Voting, mutta sitä käytetään logiikkapiirien yhteydessä (kuva 11). Logiikkapiireillä ulostulona voi olla joko TRUE tai FALSE. Binääristen ulostulojen (A1 … A4) signaalit syötetään porteille (G1 … G4) jotka suorittavat äänestyksen. Portit eivät sisällä sellaista osia, jotka voisivat aiheuttaa redundanttisen piirin vikaantumisen. Vikaantumisen yhteydessä portit käsittelevät logiikkapiirien tietosisältöä kuten FALSE-signaalia. [4, s. 321.]



Kuva 11. Gate connector voting -järjestelmä [4, s. 321]

Kaikkiin edellisiin äänestysratkaisuihin koskee sama luotettavuuskuvaaja (kuva 12). Kuvaajassa on esitettynä kolme käyrää, A esittää luotettavuustasoa kun kaksi yksikköä kolmesta on toimintakelpoisia, B:n tapauksessa toiminnassa on kolme yksikköä viidestä. Kuvaajaa tulkitessa on huomattava, että yksiköiden on oltava keskenään identtisiä. Katkoviivalla merkitty esittää yksittäisen yksikön (Single element) varmuustasoa. Kuvaajaa leimaa samantapaisen käytös kun muissakin redundanttisista ratkaisuissa, luotettavuus laskee rajusti ajanjakson ollessa pidempi. Kuvaajan suurennoksesta näemme, missä tilanteessa äänestys kasvattaa luotettavuuden määrää. Lyhyemmillä ajanjaksoilla äänestyksen luotettavuustasot ovat huomattavasti paremmat kuin yksittäisen elementin, mutta ajanhetkellä M yksittäinen yksikkö omaa jo paremman luotettavuustason. Se, onko viiden vai kolmen yksikön tekniikka parempi, riippuu käytettävän järjestelmän käynnissäoloajasta. Erittäin lyhyillä käynnissäoloajoilla viiden yksikön ratkaisu on hyvin lähellä 100 prosentin varmuustasoa. mutta pidemmillä toiminta-ajoilla alkaa viiden yksikön (käyrä B) varmuus laskemaan rajusti, ½ M:n kohdalla lähes pystysuorasti. Kolmen yksikön kohdalla (Käyrä A) varmuustason romahdus tapahtuu ¼ aikayksikköä myöhemmin. Voting-järjestelmien eduiksi voidaan lisäksi laskea mahdollisuus vikaantuneiden yksiköiden nopeaan havaitsemi-

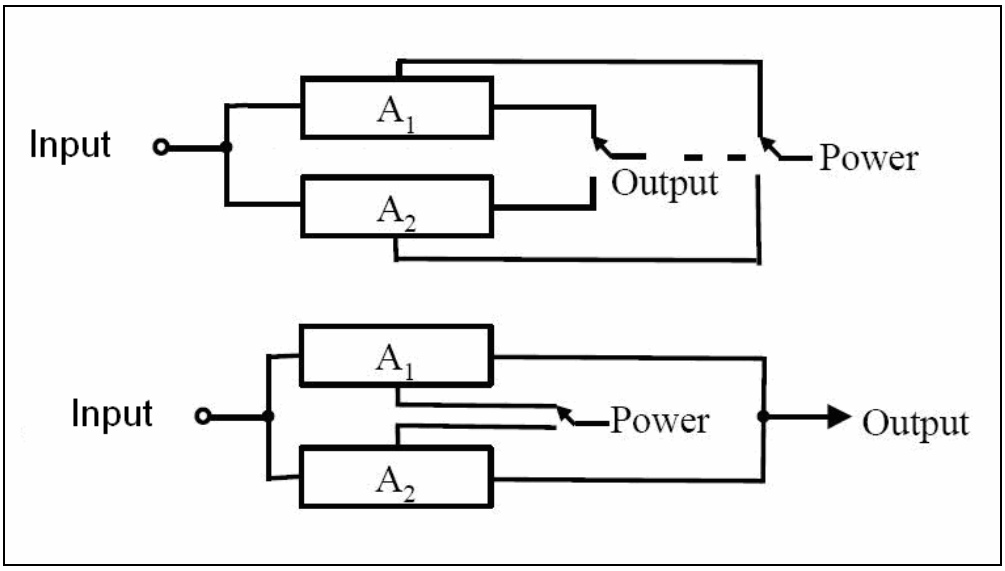
seen. Huonona puolena on varmuustason nopea laskeminen pidemmillä ajanjaksoilla sekä MVT:n tarve omata suurempi varmuus kuin muilla komponenteilla. [4, s. 326.]



Kuva 12. Majority Voting-järjestelmän luotettavuuskuvaaja [4, s. 321]

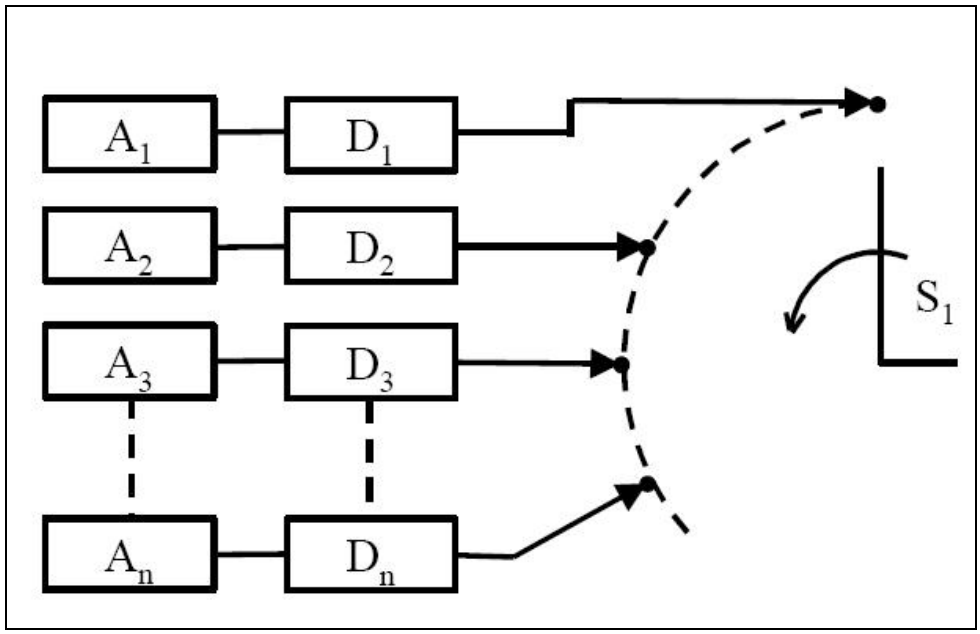
2.5 Stand-by

Stand-by-redundansseilla tarkoitetaan järjestelyä, jossa kahdennetut järjestelmät ovat lepotilassa. Ne herätetään siinä vaiheessa, kun ensisijainen järjestelmä vikaantuu. Stand-by-järjestelmät voidaan edelleen jakaa kahteen osaan, Non-Operating- ja Operating-tyyppisiin. Non-operating tarkoittaa järjestelyä, jossa redundanssina olevat yksiköt ovat normaalin laitteen toimiessa irrallisena piiristä. Seuraavassa kuvassa (kuva 13) on esitelty kaksi yleisintä tapaa kytkeä vaihtoehtoinen toimilaite käytettäväksi. [4, s. 327.]



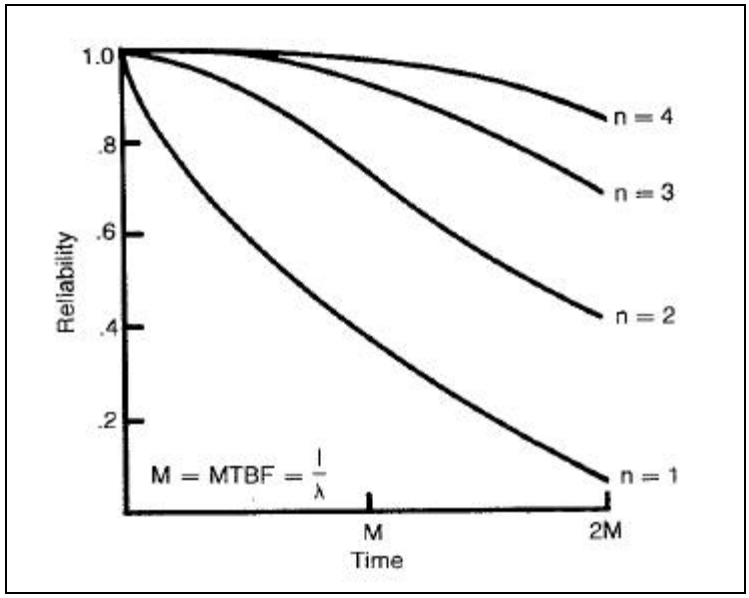
Kuva 13. Non-operating -järjestelmä [4, s. 321]

Ylemmässä ratkaisussa kytketään irrallisena olevalle laitteelle sekä jännitteensyöttö että signaalin ulostulo erikseen. Mikäli halutaan käyttää yksinkertaisempaa ratkaisua ja mikäli järjestelmän rakenne sen mahdollistaa, voidaan laite ottaa käyttöön ainoastaan kytkemällä siihen jännitteensyöttö alemman rakenteen mukaisesti. Operating-tyyppinen järjestely eroaa edellä esitetystä ratkaisusta siten, että useampi yksikkö on samanaikaisesti liitettynä samaan kytkentään, rinnakkain. Yksiköiden lisäksi ratkaisu vaatii laitteen S_1, jonka tehtävänä on yksiköiden hallinta. Kaikki yksiköt lähettävät jatkuvasti signaalia, riippumatta siitä hyödynnetäänkö sitä vai ei. S_1:n tehtävänä on vaihtaa signaalilähdettä, mikäli signaali ei sovi etukäteen annettuihin ohjearvoihin. Näin S_1 vaihtaa seuraavaan yksikköön, ja hyödyntää sen lähettämää signaalia. Vaihto tehdään vain yksikön vikaantuessa, muuten samaa laitetta käytetään niin kauan, kunnes se vikaantuu (kuva 14). [4, s. 327.]



Kuva 14. Operating-järjestelmä [4, s. 321]

Alla olevassa kuvaajassa on esitettynä Stand-by-tekniikan luotettavuustasot yhdestä neljään yksikköön (kuva 15). Kumpikin, sekä Non-Operating- että Operating-järjestelmät seuraavat samoja tasoja. Aiempien luotettavuuskuvaajiin verrattaessa Stand-by-tekniikan edut tulevat esiin pidemmillä ajanjaksoilla. Ylitettäessä ajanhetki M, pystyy neljällä yksiköllä toteutettu ratkaisu lähes luotettavuustasoon 1,0. Kolmella yksiköllä saavutetaan samalla toimintakelpoisuusajalla 90 prosentin varmuustasoon. [4, s. 327.]



Kuva 15. Stand-by-järjestelmän luotettavuuskuvaaja [4, s. 327]

Stand-by-järjestelmän eduiksi voidaan lukea soveltamismahdollisuus sekä analogisiin että digitaalisiin piireihin. Lisäksi järjestelmä on immuuni hetkellisille häiriöille. Huonoina puolina on virheen havaitsemisen ja kytkemisen välinen viive sekä rakenteen monimutkaistuminen. [4, s. 327.]

2.6 Yhteenveto

Redundanssitekniikan valinta heijastaa suoraan vaadittavaan varmuustasoon. Lyhyemmillä toiminta-ajoilla redundansseista ei saada maksimaalista hyötyä, ne voivat tietyllä aika-alueella laskea koko järjestelmän luotettavuutta. Syynä tähän on seikka, että rinnakkaisten laitteiden vikaantumisriski kertaantuu, tämä ilmiö näkyy selvästi Bimodal-tekniikan luotettavuuskuvaajaa verrattaessa yksittäiseen laitteeseen. Siksi redundanssien hyödyntämistä on syytä välttää niin kauan, kuin sama luotettavuustaso saavutetaan muilla ratkaisuilla, esimerkiksi komponenttien laadun parantamisella. Lisäksi redundanttisuus lisää ratkaisun hintaa, monimutkaistaa sitä sekä kasvattaa painoa. Ajoneuvon suunnittelun yksi tavoite on hyötykuorman maksimoiminen, siitä syystä viimeinen seikka on olennainen syy redundanttisuuden välttämiseksi.

Mikäli järjestelmä ei toiminnan kannalta ole kriittinen, ei sen varmistamiseen kannata uhrata resursseja. Esimerkiksi panssariajoneuvojen kohdalta tällainen järjestelmä on siviililainsäädännön edellyttämä ulkovalaistus. Ulkovalaistus ei ole olennainen käyttöympäristössä missä ajoneuvo on suunniteltu toimimaan, siksi sen varmistaminen ei ole nähty tarpeelliseksi. Siviiliajoneuvoissa ajovalojen ja niiden vaihtoehtoisien valaisimien suunnitteluun on kiinnitetty huomiota, koska valoja tarvitaan niiden käyttöympäristössä jatkuvasti.

Override

Redundanssin tunnusmerkit täyttyvät myös järjestelyllä, jossa tietyn laitteen käyttöympäristön rajoitteita jätetään huomioitta. Militaariajoneuvoilla tilanteet voivat muuttua nopeasti mutta laitteiden käytettävyys on oltava katkotonta, vaikka rajoitteet eivät täyttyisikään. Rajoitteita ohittavaa toimintoa kutsutaan nimeltä override.

3 ANALYSOINTIMENETELMIÄ

Riskienhallinnaksi (risk management) kutsutaan väljästi ilmaistuna kaikkia niitä toimenpiteitä, joilla riskejä pyritään pitämään hyväksyttävällä tasolla. Tietoisesta riskien hallinnasta on hyötyä aina, kun on olemassa epäedullisten tapahtumien mahdollisuus — eli likimain kaikessa ihmisen toiminnassa. Mitä merkittävämmät riskit ovat, sitä tärkeämpää on, että järjestelmällinen riskienhallinta on mukana toiminnassa alusta loppuun saakka. Riskienhallintaa ja sen mukana riskianalyysiä on syytä kuitenkin pitää osana kaikkien järjestelmien suunnittelua ja käytön aikaista muutoksenhallintaa. Riskienhallinnan ensimmäinen vaihe on riskianalyysi. Riskianalyysin tehtävä on tunnistaa riskit ja tuottaa tietoja niiden suuruuksista riskien merkityksen arviointia varten. Luotettavuuden ja turvallisuuden analysointia helpottamaan on kehitetty useita apuvälineitä. Tässä insinöörityössä analyysien soveltaminen suurempiin järjestelmiin ei ole järkevää työn laajuuden takia. Siitä syystä niiden käyttö esitellään yksinkertaisien esimerkkien avulla. [6, s. 1.]

3.1 Kriittiset järjestelmät

Kriittisillä järjestelmillä tarkoitetaan toimintoja, joiden toimivuus on oltava katkotonta kaikissa olosuhteissa. Mikäli jokin kriittisistä järjestelmistä vikaantuu, voi seurauksena olla hengenvaarallinen tilanne miehistölle tai edellytys operatiiviseen toimintaan on uhattuna. AMV:n kriittiset järjestelmät ovat seuraavat (taulukko 3). Huomattavaa on, että vaikka pääjärjestelmä ei olisikaan kriittinen, on mahdollista että jokin sen alijärjestelmä luetaan kriittiseksi. Tällaisia ovat esimerkiksi takaoven käytön esto uintimoodin yhteydessä.

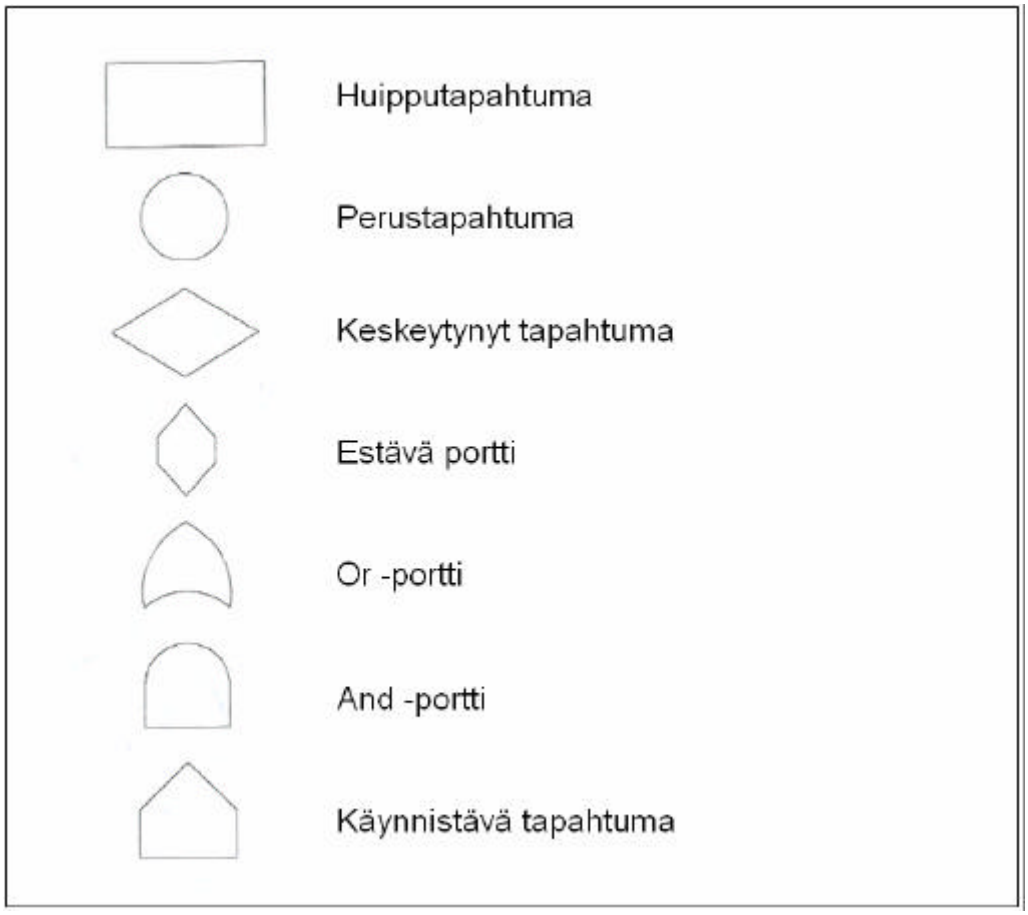
Taulukko 3: AMV:n kriittiset järjestelmät

Järjestelmän nimi	**Järjestelmän tyyppi**
Etenemiskyky (voimansiirto, ohjaus)	Pääjärjestelmä
Asejärjestelmä	Pääjärjestelmä
Luukkujen ja ovien turvapiiri	Alijärjestelmä (asejärj.)
Jarrujärjestelmä	Pääjärjestelmä
Omasuojajärjestelmä	Pääjärjestelmä
NBC-laite	Alijärjestelmä (omasuoja-järj.)
Takaoven estotoiminto uidessa	Alijärjestelmä (uintijärj.)

3.2 Vikapuuanalyysi

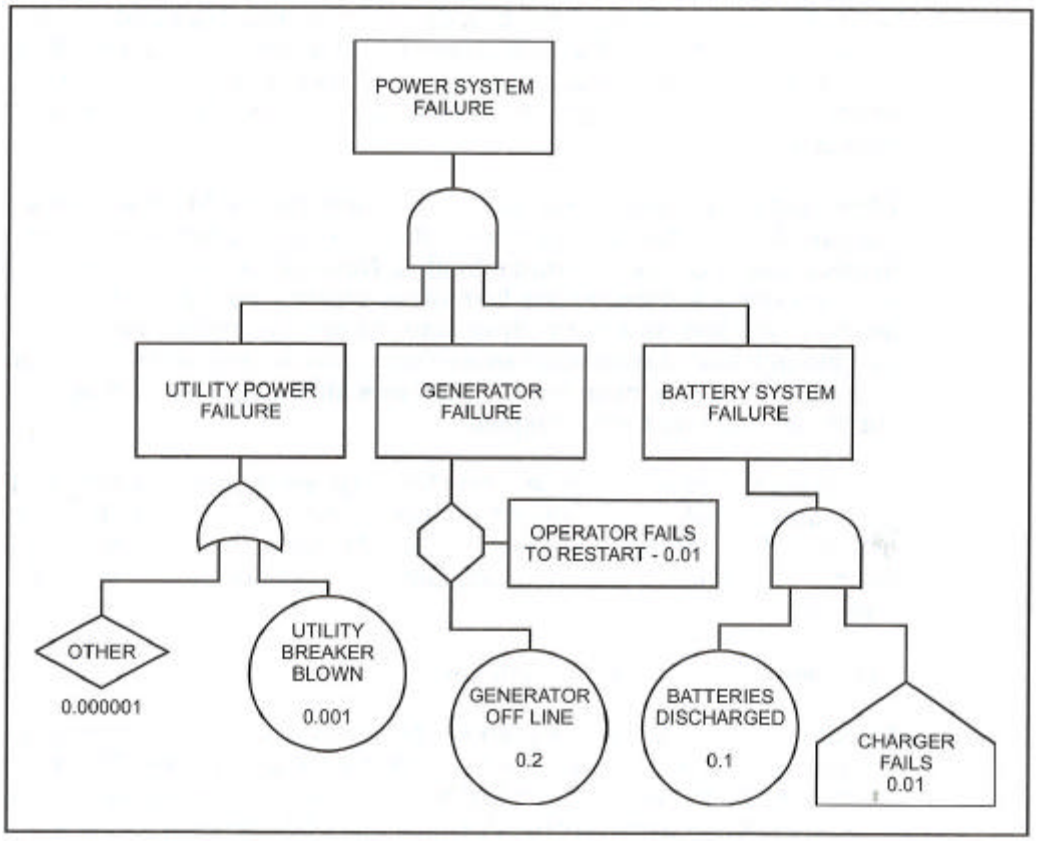
Vikapuuanalyysi (Fault tree analysis) on ylhäältä alas -tyyppinen menetelmä. Tässä menetelmässä pohdinta alkaa lopputuloksista, vioista joita järjestelmän toiminnassa voi esiintyä. Näistä edetään syy-seuraus-ketjussa taaksepäin kohti vian mahdollisesti aiheuttaneista syitä. Lähestymistavan perusteella vikapuut soveltuvat tapauksiin, joissa järjestelmän vikatoimintojen joukko on tunnettu paremmin kuin sen osien vikaantumistavat. Sitä voidaan hyödyntää myös tapauksessa, missä halutaan nimenomaan analysoida tiettyjä järjestelmän osuuksia koko järjestelmän sijasta. Analyysi siis voidaan ulottaa haluttuun syvyyteen saakka työmäärän rajaamiseksi. Analyysi aloitetaan listaamalla järjestelmän viat eli huipputapahtumat (top event). Kukin huipputapahtuma on seuraavassa vaiheessa oman puunsa juurisolmuna. Kussakin puussa eritellään aluksi, minkä ehtojen voimassa ollessa kyseinen vika voi esiintyä. Ehdot muodostavat puun seuraavan tason ja niitä yhdistää yleensä And- tai Or-operaattori. Nämä ehdot puolestaan muodostavat puun seuraavan tason ja niin edelleen. Puuta jatketaan, kunnes lehtitason solmuina on sellaisia syitä, joiden todennäköisyys on helppo määrittää. Näitä kutsutaan perustapahtumiksi (basic event). Joidenkin haarojen kasvattaminen voidaan jättää kesken, mikäli niiden vaikutus nähdään mitättömäksi tai ketjua ei yksinkertaisesti osata jatkaa pidemmälle. [6, s. 6-7.]

Vikapuiden yhteydessä hyödynnetään amerikkalaisia logiikkaporttien symboleja. Symbolit ovat esitelty kuvassa 16. Symbolit voidaan jakaa kahteen osaan, tapahtumiin sekä portteihin. Tapahtumaa voidaan pitää jonkin prosessin tuloksena, kun taas portteja käytetään useamman tapahtuman liittämiseksi toisiinsa. Huipputapahtuma (top event) on puuanalyysin lopputulos, se mihin tilaan järjestelmä siirtyy, kun jokin alemmista tapahtumista toteutuu. Huipputapahtuman alapuolella sijaitsevia tapahtumia kutsutaan nimellä välitapahtuma. Perustapahtuma (basic event) on virhetila, mikä syntyy käynnistävän tapahtuman (trigger event) johdosta. Perusvirhe voi kuitenkin ilmetä ilman käynnistävää tapahtumaa. Keskeytynyt tapahtuma (incomplete event) on nimensä mukaisesti prosessi, joka keskeytyessään aiheuttaa vikatilanteen. Estävä portti (inhibit gate) estää vikaantumisen etenemisen vikapuussa, mikäli toinen porttiin tulevista ehdoista ei täyty. Näiden lisäksi käytetään logiikkapiireissä hyödynnettäviä And- ja Or-portteja. [6, s. 6–7.]



Kuva 16. Vikapuuanalyysissä käytettävät piirrosmerkit [lähdettä 2 mukaillen]

Siinä vaiheessa, kun puurakenne on saatu valmiiksi, lisätään siihen perus-, käynnistävän sekä keskeytyneen tapahtuman todennäköisyydet. Todennäköisyydet esitetään kuvassa murtoluvun muodossa matemaattisen käsittelyn mahdollistamiseksi. Seuraavassa kuvassa on esitelty ajoneuvon sähköjärjestelmän vikapuuanalyysi (kuva 17). Sähköjärjestelmän vikapuu toimii symboleiden käytön kohdalla hyvänä esimerkkinä, sillä siinä esiintyy kaikki esitellyt symbolit. [2, s. 104.]



Kuva 17. Ajoneuvon sähköjärjestelmän vikapuuanalyysi [2, s. 111]

Ylinnä kuvassa on esitetty sähköjärjestelmän vikaantuminen (power system failure) eli huipputapahtuma. Ylhäältä alas edetessä havaitsemme, että vikaantuminen koostuu kolmesta syystä, akkujärjestelmän vikaantumisesta (battery system failure), latauslaitteen vikaantumisesta (generator failure) tai sähköverkon vikaantumisesta (utility power failure). Nämä kolme ovat puun välitapahtumia ja ne yhdistyvät huipputapahtumaan And-portin välityksellä. And-portti esiintyy puussa siitä syystä, että vasta kun kaikki kolme välitapahtumaa ovat voimassa, on koko sähköjärjestelmä vikatilassa. Akkujärjestelmän vikaantuminen koostuu perustapahtumasta akut purkautuneet (batteries discharged) ja käynnistävästä tapahtumasta latauslaite vikaantuu (charger fails). And-portti näiden yläpuolella kertoo, että käynnistävä tapahtuma esiintyy yhdessä perustapahtuman kanssa, latauslaitteen hajotessa myös akut alkavat purkautumaan. Latauslaitteen vikaantumisen alla esiintyy estävä portti sekä kaksi ehtoa, latauslaite ei käynnissä (generator off line) ja operaattori ei kykene uudelleen käynnistämään (operator fails to restart). Estävä portti vaatii, että kumpikin ehdoista täyttyy, ennen kuin ylempi välitapahtuma latauslaite vikaantunut on voimassa. Sähköverkon vikaantuminen koostuu Or-portista, jonka alla on ylivirtasuoja on lauennut (utility breaker blown) ja

muu (other). Or-portti tarkoittaa puolestaan sitä, että välitapahtuma on voimassa mikäli toinen ehdoista täyttyy. Keskeytynyt tapahtuma muu pitää sisällään kaikki muut tapahtumat, mitkä voivat esiintyä sähköverkossa ja aiheuttaa sen vikaantumisen. [2, s. 106–112.]

Todennäköisyydet kertomalla keskenään saamme selville koko järjestelmän vikaantumistaajuuden ?. Todennäköisyys, että useampi tapahtuma, esimerkiksi akkujärjestelmän ja latausjärjestelmän vikaantuminen samanaikaisesti, saadaan kertomalla näiden alaiset perus- sekä käynnistävät tapahtumat keskenään. Redundanttisten järjestelmien luotettavuuskuvaajissa esiintynyt MTBF on vikaantumistaajuuden vastaluku.

Esimerkin tapauksessa koko järjestelmän vikaantumistaajuus ? on seuraavan kaavan mukainen (1). Sulkuja käytetään eri välitapahtumien erottamiseksi toisistaan. Jälkimmäinen kaava (2) selittää puolestaan vikaantumisriskin R sekä ajan välisen yhteyden. [7, s. 55.]

$$l = 1/MTBF$$
$$l = (0{,}1 * 0{,}01) * (0{,}2 * 0{,}01) * (0{,}001) = 0{,}000000002 \quad (1)$$

$$R = e^{-lT} \quad (2)$$

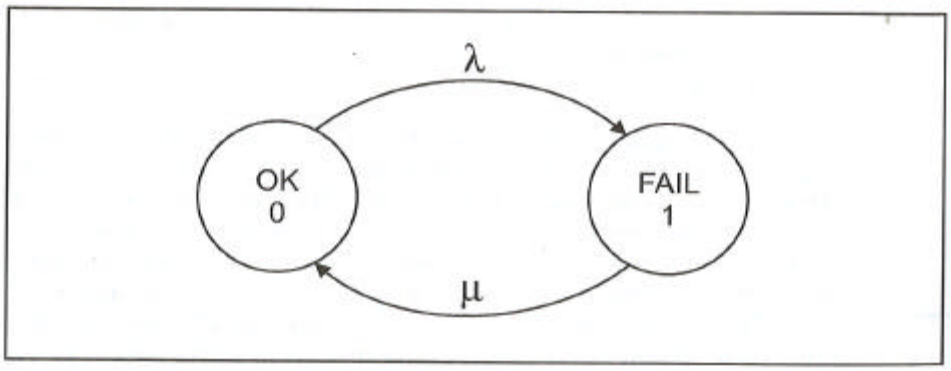
Kahden kaavan perusteella havaitsemme, että latausjärjestelmän vikaantumistaajuutta ei voida hyödyntää ilman että otamme toiminta-ajan huomioon. Ajanhetken T:n lisääntyessä vikaantumisriski R kasvaa eksponentiaalisesti. Siitä syystä riski vikaantumiseen kasvaa ajanhetken edetessä, ja pitkillä toiminta-ajoilla riski muodostuu huomattavaksi. Riskiä voidaan siis vähentää lyhentämällä järjestelmän toiminta-aikaa. Toinen riskiä vähentävä tekijä on vikaantumistaajuuden ?, eli komponenttien luotettavuustason kasvattaminen.

3.3 Markovin malli

Markovin malli on tilapohjainen analysointimenetelmä, jota voidaan käyttää sekä yksittäisten että koko järjestelmän luotettavuuden laskemiseen. Käyttäytyminen kuvataan komponenttien tilojen tai järjestelmän komponenttien todennäköisyyksinä siirtyä tilasta tai komponentista toiseen. Tilaa esittävää

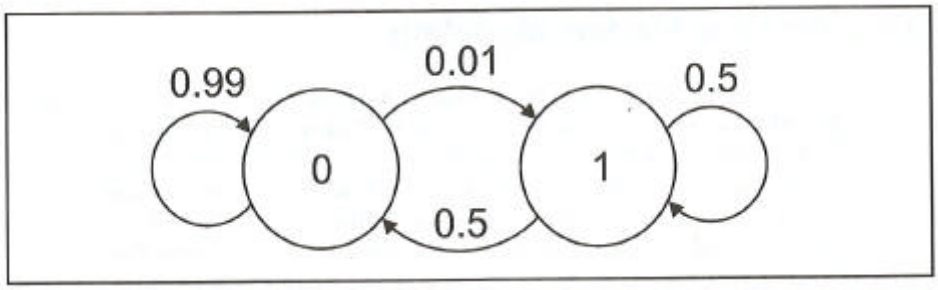
piirrosta kutsutaan nimellä Markovin ketju. Mallintamisessa hyödynnetään vain kahta piirrosmerkkiä, tilasta kertovaa ympyrää sekä nuolta, mikä osoittaa tilan vaihtumisen toiseen (kuva 18). Tiloista 0 kertoo laitteen olevan normaalisti toiminnassa (ok), 1 puolestaan sen siirtymisestä vikatilaan (fail). Tilojen nuolten yhteyteen merkitään siirtymän todennäköisyys. [8, s. 27.]

Todennäköisyydet jaetaan kahteen osaan, tilasta 0 tilaan 1 siirtyvää nuolta merkitään lambdalla (?), ja vastakkaiseen suuntaan siirtyvää puolestaan myylla (μ). Samasta tilasta eli ympyrästä voi lähteä useampia nuolia. Kaikkien tiloista lähtevien nuolien todennäköisyydet yhteen laskemalla saadaan luku 1. Malli voi esittää niin ei korjattavissa, osittain korjattavaa tai täysin korjattavaa järjestelmää. Useita virheitä voidaan mallintaa käyttämällä niin monta virhetilaa kuin on tarpeellista. [2, s. 152.]



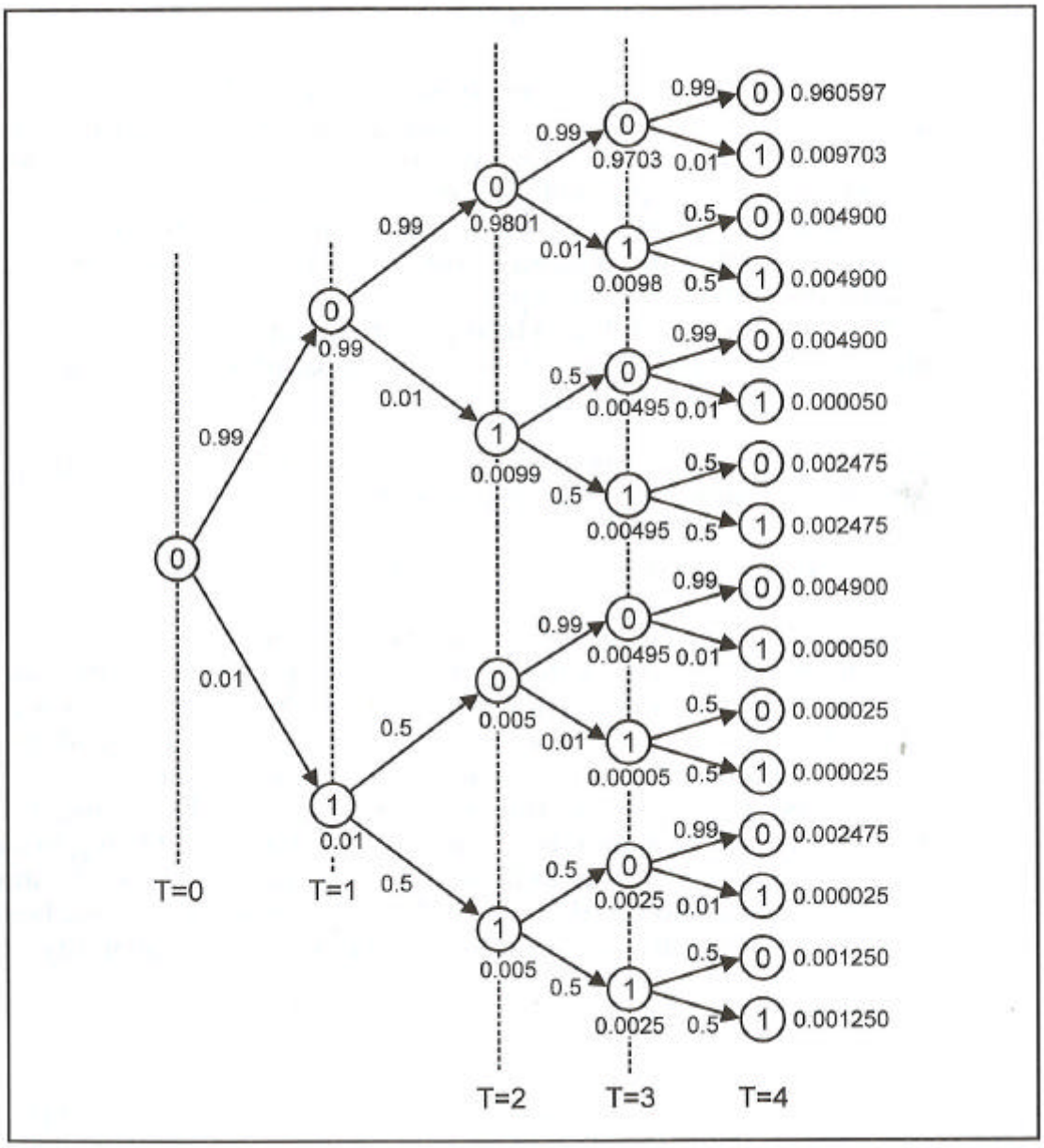
Kuva 18. Tilaesityksessä käytettävät piirrosmerkit [2, s. 150]

Seuraavassa on esitetty yksinkertainen järjestelmä, jossa esiintyy kaksi tilaa, 0 ja 1 (kuva 19). Tila 0 muuttuu 0,01 todennäköisyydellä tilaksi 1 (fail), joten se pysyy samassa tilassa todennäköisyydellä 0,99. Mikäli siirrytään tilaan 1, se korjaantuu 0,5 todennäköisyydellä 0:ksi (ok), ja pysyy samalla todennäköisyydellä samassa tilassa. [2, s. 152.]



Kuva 19. Yksinkertainen tilaesitys [2, s. 152]

Edellistä esitystä voidaan tulkita edelleen jakamalla se aika-tasoihin (kuva 20). Ajanhetki esitetään kuvassa vaaka-akselina, analyysin alussa ajanhetkenä T = 0. Siirryttäessä ajanhetkeen T = 1, voidaan edetä edellisen esityksen mukaisesti kahta reittiä, pysyä tilassa 0 tai vaihtamalla tilaa 1:ksi. Nuolien yhteyteen on merkitty sama todennäköisyys, mikä esiintyy aiemmin esityksen (kuva 19) yhteydessä. Ajanhetkellä T = 2 reitti jakaantuu jälleen kahdeksi ja niin edelleen. Kun polku on käyty ajanhetkeen T = 4 asti, voidaan laskea eri polkujen todennäköisyydet. Kuvaa tulkitessamme huomaamme, että todennäköisin kulkureitti on laitteen pysyminen 0 -tilassa, todennäköisyydellä ~0,96. Muut todennäköisyydet ovat huomattavasti pienempiä, joten laitteen luotettavuustaso on erittäin hyvä. Suurempia järjestelmiä analysoitaessa aika-tasokuvaajaa ei ole mahdollista tehdä, jolloin analyysi suoritetaan matriisilaskennan avulla. [2, s. 153–154.]



Kuva 20. Tilamuutokset aikatasossa kuvattuna [2, s. 153]

4 AJONEUVOTEOLLISUUDEN RATKAISUT

Ajoneuvoteollisuuden lisääntynyt elektroniikan määrä on mahdollistanut myös redundanttien ratkaisujen hyödyntämisen entistä laajemmin. Erityisesti turvallisuuteen liittyvät ratkaisut ovat kriittisyytensä vuoksi varmennettuja. Tällaisia ovat esimerkiksi jarrut, ajonvakautusjärjestelmät, passiiviset turvalaitteet jne. Usein redundanttiutta ei kyseisellä nimellä myydä loppuasiakkaalle, mutta varmentaminen liitetään suoraan auton turvallisuuteen, jota puolestaan pidetään suurena kilpailutekijänä. Ajoneuvoissa on perustoimintaan liittyviä ratkaisuja, jotka on aina toteutettu mekaanisesti, kuten ohjaus sekä jarrut. Vasta näinä päivinä mekaanisten toteutusten rinnalle on haettu sähköisiä ratkaisuja. Sähköisten jarrujen sekä ohjauksen edut ovat kiistattomat, komponenttien sijoittelu on vapaampaa, tarkkuus kasvaa, huoltoa kaipaavat komponentit havaitaan aiemmin ja niin edelleen. Mutta haittapuoliakin löytyy: luotettavuuden takia redundanttius on välttämätöntä, ja toimilaitteita varmistettaessa myös kustannukset nousevat. Vikaherkkyyden lisäksi myös lainsäädäntö estää täysin sähköisen ratkaisun.

Toisaalta ajoneuvoissa on alettu käyttää ilmailuteollisuudesta tuttuja ratkaisuja niissä kohteissa, joissa se on lainsäädännöllisesti ollut mahdollista. Tästä hyvänä esimerkkinä toimii kaasupohjin. Kuljettaja painaa poljinta ja siten tekee pyyntöjä vääntömomentin määrästä, ja ohjainyksikkö päättää mitä parametreja säätämällä pyyntö toteutetaan. Mahdollisuuksia ovat esimerkiksi ilmamassa tai sytytyksen ajoitus. Kuljettaja ei siis tiedä, miten moottorinohjaus pyynnön toteuttaa. Tilanne on verrattavissa lentokoneissa ohjainsauvan kääntämiseen. Lentäjä vain esittää toiveen koneen kallistumisesta ja ohjainyksikkö toimilaitteineen suorittaa laskennan ja lentoradan korjauksen parhaalla näkemällään tavalla. Virheherkkyyden takia myös redundanttisuus on tuotu lentoteollisuudesta ajoneuvopuolelle.

4.1 Moottorinohjaus

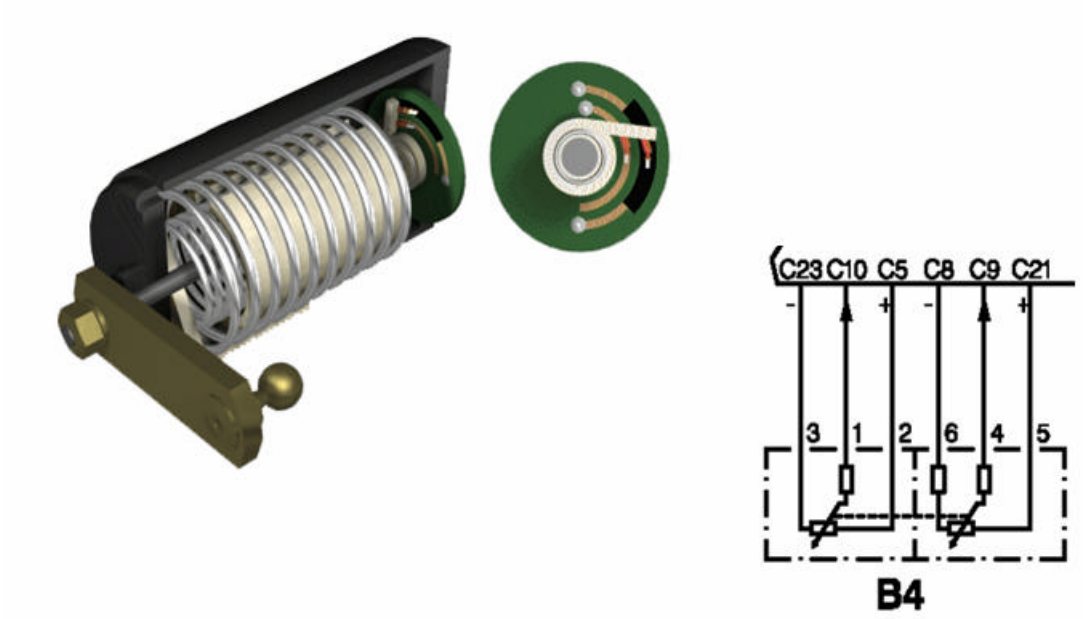
Termillä moottorinohjaus tarkoitetaan ohjainyksikköä, johon on koottu aiemmin erillään olleet kaksi toimintoa, sytytyksen ja ruiskutuksen ohjaus. Aiemmin sytytyksen ohjaus on tapahtunut mekaanisesti, jolloin säätömahdollisuudet ovat olleet rajalliset. Kiinnostus esimerkiksi sytytyksen ajoituksen

säätämiseen selittyy vääntömomentin sopeuttamisella, ajoitus kun on yksi momenttia säätävistä parametreista. Tarve yhteiselle moottorinohjaukselle on siten kiistaton.

Uusissa järjestelmissä myös redundanttius on viety aiempaa pidemmälle. Mikäli vanhemmissa järjestelmissä jokin anturitieto puuttui, ei kyseinen moottorinohjaus kyennyt toimimaan. Uusiin järjestelmiin on integroitu useita toimintoja, jotka palvelevat redundanttisia tarpeita. Yksi olennaisimmista toiminnoista on korvausarvot. Mikäli jokin anturitieto häviää esimerkiksi johdinkatkoksen takia, tunnistaa moottorinohjaus sen välittömästi ja siirtyy korvausarvoja käyttävään tilaan. Tällöin moottori laskee muista muuttujista ja aiemmin olleista olosuhdetietoista anturille arvon, ja korvaa puuttuvan sillä. Tyypillisiä korvattavia arvoja ovat lämpötila- ja painearvot. Paine ja lämpötila ovat myös toisistaan suoraan riippuvaisia, joten toisen tietämällä pystyy toisen laskemaan riittävällä tarkkuudella. Toisien antureiden kohdalla edellisen kaltaista suoraa riippuvuutta toiseen muuttujaan ei löydy, jolloin käytetään hyväksi jotakin perusarvoa. Arvo voidaan laskea monella tavalla; yksi runsaasti käytetty arvo on vaihtelualueen keskiarvo.

Optimaalinen tilanne olisi se, että moottori toimii kuten aiemmin. Kuitenkin anturi voi olla siinä määrin merkittävä, että kuljettaja huomaa muutoksen moottorin käytöksessä.

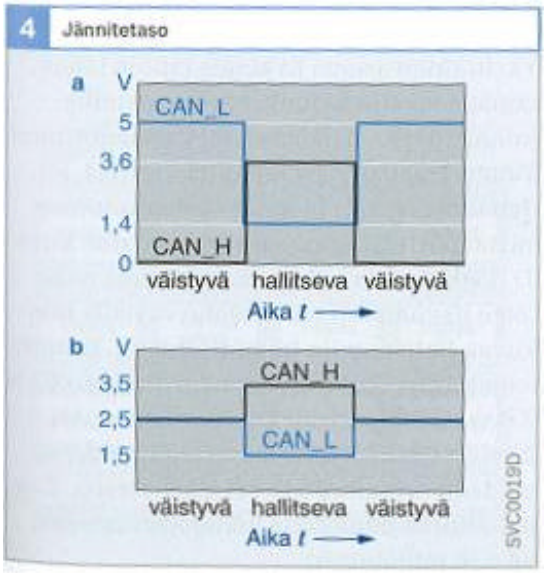
Toinen tyypillinen redundanssin tunnuspiirteet täyttävä toiminto on kahdennetut anturiarvot. Esimerkiksi kaasupolkimen muututtua sähköiseksi, on entinen, mekaaninen kaasuläppä muuttunut toimilaitteeksi, jossa sähkömoottoria ohjataan kaasupolkimen toivomuksien mukaisesti. Laitteen kriittisyyden takia anturointiin on kiinnitetty huomiota, kaasuläpän ei saa vikaannuttuaan jäädä auki ja lisäksi tarkka asento on jatkuvasti oltava moottorinohjauksen tiedossa. Tästä syystä läpän asentoa mittaa kaksi potentiometriä, jotka mittaavat vastakkaisia muuttujia, toinen mittaa läpän aukioloa ja toinen puolestaan kiinnioloa. Redundanssina toimii kahdennettu anturiarvo, toisen arvon puuttuessa toisen avulla laitetta voidaan käyttää ja sen asento tunnetaan. Molempien antureiden puuttuessa askelmoottorin ohjaus lopetetaan. Tällöin läpän sulkeutumisen hoitaa jousi, jota vastaan sähkömoottori normaalisti tekee työtä. Tyypillistä kahdennettua arvoa antavaa potentiometria esittää kuva 21.



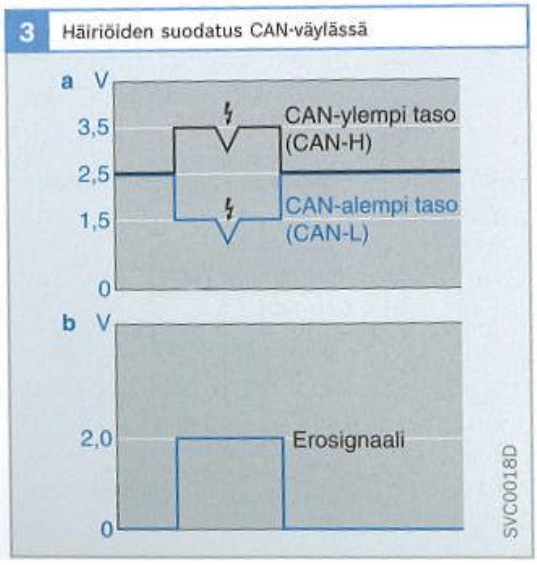
Kuva 21. Tyypillinen kaksoispotentiometrin rakenne.

4.2 Väyläliikenne

Controller Area Network, myöh. CAN on 1980-luvulla Bosch Gmbh:n kehittämä väyläratkaisu ajoneuvojen tiedonsiirron tarpeisiin. Väylä toimii hajautettuna järjestelmänä. Kaikki laitteet ovat kytketty saman väylän varteen samanarvoisina. Näin vältetään keskitetyn ohjainyksikön tarve ja laitteiden lisääminen väylälle on saatu vaivattomaksi. Redundanttisuus on ollut ratkaisun yksi perusajatuksista. Fyysisenä rakenteena väylä koostuu kahdesta johtimesta, CAN-H:sta ja CAN-L:sta (kuva 22). Väylillä kulkee sama viestisisältö, mutta toistensa peilikuvina. Tällä on saavutettu kaksi etua, ensinnä häiriöiden suodatus. Fyysisesti kaapelina käytetään kierrettyä paria. Koska pari on tiiviisti kierrettyä, johtuvat ympärillä olevat häiriöt samanmuotoisina molempiin linjoihin. Signaalit ovat toistensa peilikuvia, vähentämällä jännitetasot keskenään saadaan erotukseksi nolla. Kun molempaan väylään johtuu häiriöitä, erotuksena ei olekaan nolla, vaan häiriön suuruus, jolloin kyseinen jännitekomponentti voidaan helposti suodattaa pois (kuva 23). Kaksijohdinjärjestelmä toimii myös redundanssina, sillä CAN-laitteet voivat kommunikoida keskenään myös ainoastaan yhden johtimen avulla. Vastaanottavat laitteet käyttävät omia kanaviaan, ja molemmille on omat signaalinkäsittelyyksikkönsä. Toisen johtimen vikaannuttua toinen jatkaa toimintaansa normaalisti, ja laite pystyy edelleen toimimaan. Tällöin on kuitenkin mahdollista, että häiriöt siirtyvät signaalien mukana ja häiritsevät väyläliikennettä.



Kuva 22. CAN-H- ja CAN-L-signaalitasot [10]



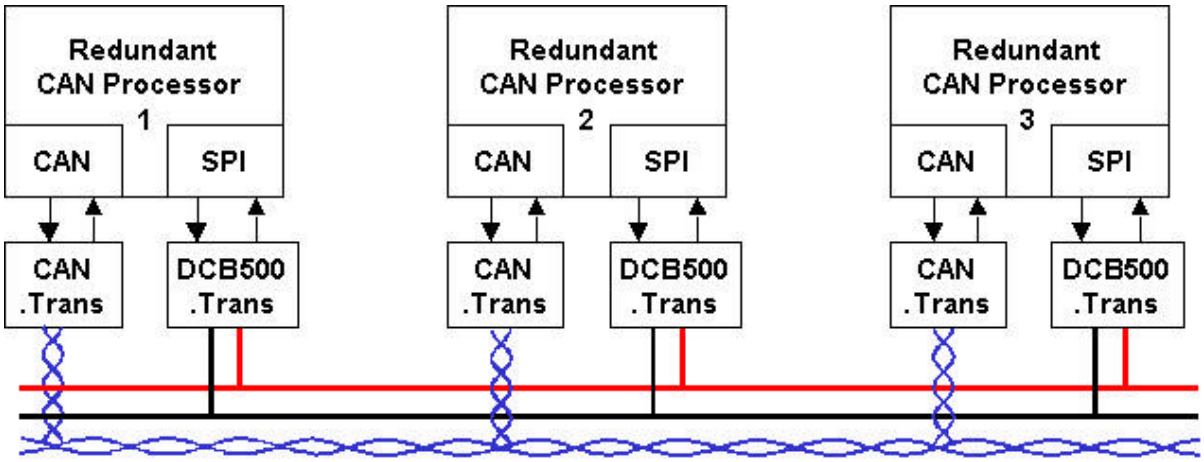
Kuva 23. CAN-tiedonsiirron häiriösuodatus [10]

Edellisen lisäksi mahdollista käyttää jännitteensyöttöä tiedon siirtämiseksi (kuva 24). Jännitteensyöttö on usein toteutettu huomattavasti vankemmin, joten sen vikaantuminen on huomattavasti harvinaisempaa. Onkin siis järkevää hyödyntää ”kantaverkkoa” myös tiedonsiirron tarpeisiin. Syöttöverkon käyttäminen myös helpottaa asennusta sekä laskee järjestelmän painoa yksinkertaistamalla johdotuksen rakennetta. Tiedonsiirtoa syöttöverkon kautta kutsutaan nimelle Power Line Communication, myöh. PLC. Perinteisen CAN-verkko ei voi taata luotettavaa tiedonsiirtoa vakavammissa häiriötilanteissa, kuten noodien yhteyskatkoissa, lähetys- tai vastaanottotilan aktiiviseksi jäämisessä tai molempien väyläkaapeleiden yhtäaikaisessa katkeamisessa. Todellisen redundanttisen tiedonsiirron luomiseksi tiedon on siirryttävä fyysisesti eri reittiä määränpäähänsä. PLC:n käyttö vaatii kuitenkin erityispiirteidensä huomioonottamista.

Perinteinen CAN perustuu siihen, että kaikki laitteet olevat samalla väylällä, ja ne kuulevat kaiken viestiliikenteen. Laitteet osaavat vastaanottaa viestejä viestikehyksen laitetunnuksen mukaan. Väylällä ei voi kulkea kuin yksi viesti kerrallaan, joten niiden priorisointi on välttämätöntä. Priorisointi on toteutettu arbitraation avulla. Arbitraatiossa laitteet ovat asetettu prioriteettinsä mukaan järjestykseen siten, että kaikista tärkeimmällä laitteella on binäärimuotoisesti pienin järjestysluku. Nolla (0) on dominantti ja ykkönen (1) puolestaan recessiivinen eli väistyvä. Tällöin nolla dominoi aina ykköstä, ja lopulta pienimmän järjestysluvun omaava laite on tärkein, esim. 0001 on tärkeämpi

kuin 0010. Järjestysluvut lähetetään aina viestikehysten alussa, ja muiden laitteiden vastaanotettua viestin ne siirtyvät kuuntelemaan.

PLC:n haasteena onkin se, että eri laitteet voivat voittaa arbitraation eri tiedonsiirtoverkoissa. Tällöin verkoille vaaditaan valvoja joka tarpeen mukaan suorittaa PLC:n herättämisen ja ohjaa liikenteen perinteisen CAN:n rajapinnasta PLC:n puolelle.



Kuva 24. Kahdennettu väyläratkaisu jännitteensyöttöä hyödyntäen [11, s. 2]

Väylien avulla myös toimilaitteiden vaihtaminen vikaantuneesta toimintakuntoiseen on mahdollista. Tätä toimintoa hyödynnetään muun muassa ajoneuvojen valaisimissa. Kesken ajotilanteen hajonnut polttimo on mahdollista nykyisillä väylärakenteilla korvata toisella. Valaistusta ohjaava yksikkö havaitsee palaneen polttimon mittaamalla sen virrankulutusta. Esimerkiksi ajovalopolttimon vikaannuttua voidaan jarruvalopolttimoa syöttää matalammalla jännitteellä ajovalon kirkkauden aikaansaamiseksi, tai jopa ajovaloumpio on mahdollista vaihtaa toiseen. Takasumuvalo on harvaan käytössä oikeassa tarkoituksessaan, joten useat autovalmistajat ovat ottaneet sen hyötykäyttöön normaalin ajovalon vikaannuttua. Redundansseja käytetään myös etuvaloissa. Ajovalopolttimon palaessa voidaan sytyttää saman puolen etusumuvalo ja käyttää sitä normaalia matalammalla jännitteellä.

Väyläliikenteen varmentamisessa pätevät myös alussa esitellyt sähköverkkojen ratkaisut, myös väylälaitteita voidaan kahdentaa. Eri redundanssitasoja väyläliikenteen järjestämiseen on siis useita. Kaikkea väyläliikennettä ei ole kustannussyistä järkevää kahdentaa varmimman mukaan. Siksi onkin järkevää jakaa väylät useampaan prioriteettitasoon, ja sovittaa jokaiselle

omat varmistustasonsa. Voimansiirron, jarrujen ja turvalaitteiden varmennus on järkevää suunnitella varmaksi kustannuksista huolimatta, informaatiojärjestelmille riittää kevyempi ja halvempi toteutus.

5 RISKIANALYYSIN TEKEMINEN

Tässä luvussa otetaan kantaa siihen, miten redundanttiset ratkaisut olisivat järkevää ottaa huomioon jo suunnitteluvaiheessa. Syy, miksi redundanttisuutta hyödynnetään on luotettavuustason kasvattaminen. Kuitenkin ennen kuin voidaan edetä suunnitteluun asti, on tunnistettava vikaantuvat järjestelmät tai toiminnot. Paras työkalu tähän on riskianalyysin tekeminen. Riskianalyysin tekemiseen voidaan käyttää jotain edellä mainituista analysointimenetelmistä, mikäli riskit eivät ole edeltä ennustettavissa. Havaittujen riskien kirjaamiseen ja edelleen käsittelyyn on luotu valmiita pohjia. Seuraavassa käytetty pohja on ruotsalaisen System säkerhet -käsikirjan vastaavan suomennettu versio. Saman pohjan käyttäminen mahdollistaa sen, että kumpikin malli seuraa MIL-STD-882C -standardia. Suomeksi analyysi on nimetty VVKA, joka koostuu sanoista vika-, vaikutus- ja kriittisyysanalyysi. Analyysin tehtävänä on selvittää riskin kriittisyyden lisäksi sen esiintymisen todennäköisyyteen sekä siihen, millä tavalla riskin tasoa saadaan laskettua.

Ensimmäinen sivu toimii analyysin teossa ohjeistuksena (liite 1). Sivulle on koottu kaikki tarvittava tieto analyysin tekoon, joten pohja on määritelty erittäin helpoksi käyttää.

5.1 Kansilehti

Yleisyys

Riskin yleisyys on jaettu aakkosten ensimmäisen kuuden merkin mukaisesti siten, että a on yleisin riskin toistumisväli; Yleinen, toistuva, tiheä ja f edustaa harvinta toistumisväliä; Ei juurikaan mahdollista.

Seuraus

Ymmärrettävästi seuraus, jonka riski aiheuttaa, koskettaa sekä ajoneuvon miehistöä että itse ajoneuvoa sekä sen alijärjestelmiä. Tässä analyysipohjan mallissa seuraukset ovat jaettu kahteen pääryhmään, vaikutukseen miehistöön ja vaikutukseen ajoneuvoon ja sen järjestelmiin. Seuraus on jaettu puo-

lestaan numeraalein tasoihin yhdestä neljään siten, että taso 1 tarkoittaa katastrofi-tasoista seurausta ja taso vähäisen mahdollisuuden tasoa.

Riskien sulkeminen

Riskin sulkeminen voi tarkoittaa joko riskin hyväksymistä sen alhaisen todennäköisyyden takia tai riskiä vähentävän ratkaisun esittämisellä ja hyväksymisellä. Sulkeminen vaatii katselmointia, johon on osallistuttava järjestelmäturvallisuudesta vastaava, suunnittelun edustaja ja tuotteesta riippuen myös asiakas. Viimeinen osallistuu riskin sulkemiseen muun muassa silloin, kun riski on asiakkaan havaitsema. Suuremmissa organisaatioissa voi olla tarvetta myös erillisen turvallisuustyöryhmän ja jopa tämän alaisen projektiryhmän perustamiseen. Näin saadaan useamman alan asiantuntijoita mukaan päätöksentekoon.

Riskien luokitus

Riskien luokituksella tarkoitetaan matriisia, joka yhdistää kolme edellistä tekijää, yleisyyden, seurauksen ja riskien sulkemisen. Matriisia tarkastellessa huomataan, että puolustusväliteollisuudessa standardit vaativat asiakkaan hyväksynnän jo kolmannen tason riskeille, mikäli näiden toistumisväli saavuttaa yleisen tason. Esimerkiksi siviiliajoneuvoteollisuudessa tällainen toimintamalli ei olisi mahdollista.

5.2 Analyysin tekeminen

Analyysin tekoa varten liitteenä on esitetty esimerkki yhdestä tapauksesta (liite 1). Tässä esimerkissä analysoidaan ajoneuvoissa käytettävien jarrujärjestelmien toimintaa. Lukkiutumattomien jarrujen yhteydessä lainsäädäntö sanelee, että ensisijaisten ABS-jarrujen vikaantuessa on jarrutusenergia pystyttävä tuottamaan muulla tavoin. Ajoneuvoissa käytetään korvaavana järjestelmänä perinteistä, hydraulista tai pneumaattista jarrujärjestelmää.

Nro

Ensimmäinen sarake toimii laskurina, sen arvo kasvaa sitä mukaa kuin uusia riskitapauksia lisätään. Laskurin hyöty tulee esille silloin, kun riskitapauksia on kirjattu useampia. Tällöin se helpottaa tiedon hakemista.

Riski nro

Jokaisella riskitapauksella on oltava oma riskinumeronsa. Tässä vaiheessa voidaan myös nimetä tapaukset joko riskin suuruuden mukaisesti, esimerkiksi kriittisin tapaus on Axxx ja vähemmän kriittinen Bxxx ja niin edelleen. Toinen tapa lajitella on nimetä tapaukset alijärjestelmän mukaan, mikäli analyysi koskee kokonaista ajoneuvoa tai suurempaa järjestelmää.

Riskin kuvaus

Riskin kuvaus esittää vikatilanteesta lyhyen kuvauksen. Kuvauksen on oltava kuitenkin niin eksakti, että analyysin lukija ymmärtää mistä riskistä on kyse.

Onnettomuus

Onnettomuus-sarakkeeseen on syytä lisätä kuvaus, mikäli riski on aiheuttanut onnettomuuden tai useampia.

Riskin vaikutus

Seuraava sarake kertoo, mihin riski vaikuttaa. Panssariajoneuvojen tapauksessa tunnistettiin neljä vaikutusaluetta: henkilö, järjestelmä, ympäristö ja operatiivinen toiminta. Järjestelmä sisältää tässä tapauksessa ajoneuvon minkä tahansa alijärjestelmän tai koko ajoneuvon kuten lukkiutumattoman jarrujärjestelmän tapauksessa. Jarrujen rikkoutuminen vaikuttaa ajoneuvon lisäksi henkilöön sekä operatiiviseen toimintaan. Jarrujen rikkoutuminen kesken operatiivisen toiminnan voi johtaa operaation vaarantumisen lisäksi henkilövahinkoihin.

Tilanne

Tilanne-sarake kertoo, missä tilanteessa riski ilmenee. Jarrujärjestelmän riski ilmenee ymmärrettävästi jarrutettaessa.

Alkuluokitus

Tässä vaiheessa riskille luodaan luokitus käyttäen apuna ensimmäisen sivun ohjeistusta. Luokitus kootaan kolmesta tekijästä: yleisyydestä, seurauksesta ja riskin sulkemisluokka. Viimeinen nähdään suoraan ensimmäisen sivun matriisin avulla, yleisyysrivin ja seuraussarakkeen leikkauspisteessä. Esi-

merkin kohdalla alkuluokitukseksi d1B. Yleisyys vähäinen mahdollisuus (d) selittyy jarrujen jatkuvalla käytöllä. Seuraus on luokiteltu suurimpaan mahdolliseen kategoriaan 1, sillä jarrujen katoaminen on erittäin kriittistä.

Päivämäärä

Päivämääräksi kirjataan kaikki riskiin liittyvät päivämäärät, kuten riskin havaitseminen, katselmointipäivät, toteutuspäivämäärä ja niin edelleen.

Kuvaus riskin alentamisesta

Riskin alentumiskuvaukseen pätee samat kriteerit kuin riskin kuvaukseen. Haasteena voi olla ratkaisun aukikirjoittaminen siten, että kuvaus aukeaa analyysin lukijalle.

Tila

Tilaan kirjataan vaiheet, miten riskin ratkaiseminen on työryhmältä edennyt. Tiloina voidaan käyttää ratkaisun edistymistä prototyypin esittelystä tuotteeksi. Tilojen avuksi on otettu samankaltaisia yleistiloista kertovia kirjaimia kuin vaikutuksia määrittävässä kohdassa. Tiloja voi valita tarvittava määrän. Tässä analyysipohjassa valittiin tilat vaatii edelleensuunnittelua, redundanttisuusratkaisu olemassa sekä koulutus. Koulutus päätyi analyysiin siitä syystä, että vaikkei riski vähenisikään, voidaan koulutuksella minimoida riskin aiheuttamat vahingot vikaantumisen tapahtuessa.

Jälkiluokitus

Viimeinen sarake kertoo riskin luokituksen tehtyjen toimenpiteiden jälkeen. Esimerkissämme ABS-jarrujen rinnalla olevat perinteiset jarrut laskivat luokitukseksi f1D. Molempien jarrujärjestelmien vikaantuminen samaan aikaan on luokiteltu ei juurikaan mahdolliseksi (f). Seuraus-luokitukseen ratkaisu ei vaikuta, sillä jarrujen vikaantuminen on edelleenkin katastrofaalinen. Riski on kuitenkin laskenut siinä määrin, että sen hyväksymiskynnys on helpompi ylittää.

6 YHTEENVETO

Tämän insinöörityön tarkoituksena oli tarkastella ajoneuvoteollisuudessa käytettäviä redundantteja ratkaisuja. Pääpaino on elektronisten redundanssien esittelyssä, sillä niiden määrä tulee lisääntymään ajoneuvoissa räjähdysmäisesti. Koska aihe liittyy läheisesti luotettavuuden kasvattamiseen sekä riskien tunnistamiseen, otti työ esille myös toimintatapoja näitä koskien.

Työtä on tarkoitus hyödyntää Patria Land & Armament Oy:n vehicle electronics -ryhmän toimesta. Työssä esiteltyjä tekniikoita käyttää moni komponenttitoimittaja, mutta niiden hyödyntäminen Patrian omassa suunnittelussa on kohtuullisen vähäistä. Silti vaatimukset panssariajoneuvoja kohtaan koventuvat jatkuvasti. Vaatimuksiin vastaaminen vaatii entistä enemmän suunnittelua ja siten myös uudenlaisia työkaluja. Insinöörityön kolme kantavaa teemaa: redundanttisuus, luotettavuus sekä riskianalyysi tulevat esille juuri tällöin.

Ennen työn aloitusta asetettiin sen tavoitteeksi toimia sähkösuunnittelijoiden apuna redundanttisuuteen liittyvissä seikoissa niin sanottuna kuvausdokumenttina. Työ oli osa syksylle 2008 sijoittunutta Redundanttisuus-tuotekehityshanketta. Hankkeen tavoitteena oli kuvausdokumentin lisäksi analysoida AMV-ajoneuvon tämänhetkiset redundanttiset ratkaisut sekä tehdä vetroniikan järjestelmistä kriittisyysanalyysi. Olemassa olevien ratkaisujen selvittäminen mahdollisti sen, että työtä pystyttiin hyödyntämään markkinoinnin materiaalin tuotannossa. Kriittisyysanalyysi tehtiin ennen kaikkea suunnitteluosaston tarpeisiin. Työlle asetetut tavoitteet saavutettiin halutussa laajuudessa.

VIITELUETTELO

[1] *Varmennetut sähkönjakelujärjestelmät.* Helsinki: Sähkötieto Oy. 2005.

[2] Goble, William M., *Control Systems Safety Evaluation & Reliability, 2nd edition*. Yhdysvallat: ISA - The instrumentation, Systems, and Automation Society. 1998.

[3] *Military Handook. Electronic Reliability Design Handbook.* Yhdysvallat: MIL-HDBK-338B. 1998.

[4] Society of Automotive engineers, *Automotive electronics reliability handbook.* Yhdysvallat: SAE Inc. 1987.

[5] Scott Speaks Reliability and MTBF Overview [verkkodokumentti]. Saatavissa: http://www.vicorpower.com/documents/quality/Rel_MTBF.pdf.

[6] Meriläinen, Jouni. *Riskianalyysimenetelmät*. [verkkodokumentti]. Saatavissa: http://www.cs.helsinki.fi/group/turvasem/papers/merilainen.pdf.

[7] Clifton A. Ericson II. *Fault tree analysis* [verkkodokumentti]. Saatavissa: http://www.fault-tree.net/papers/ericson-fta-tutorial.pdf.

[8] Niskanen, Antti. Työkalu *luotettavuuden mallipohjaiseen analysointiin.* Espoo: VTT:n sähköiset julkaisut. 2006. Saatavissa: http://www.vtt.fi/inf/pdf/tiedotteet/2006/T2331.pdf.

[9] Seppälä Juha, Diagno Finland Oy. Luentomateriaali. 2009.

[10] *Ajoneuvojen verkottuminen.* Helsinki: Autoalan koulutuskeskus Oy. 2008.

[11] Maryanka, Yair. *The vehicle power line as a Redundant channel for CAN Communication.* 2005. Saatavissa: http://www.yamar.com/The-Vehicle-Power-Line-as-a-Redundant-Channel-for-CAN-Communication.pdf

Patria Land & Armament Oy
Timo A Virtanen

Turvallisuusanalyysi, kansilehti

AMV 8x8

Tämä turvallisuusanalyysi perustuu Ruotsin Puolustusvoimien "System Safety Manual":n (H systSäk 1996, M7740-784861) sekä MIL-STD-882 C System Safety standardiin

Yleisyys	Taso
Yleinen, toistuva, tiheä	a
Todennäköinen	b
Satunnainen, ajoittainen	c
Vähäinen mahdollisuus	d
Epätodennäköinen	e
Ei juurikaan mahdollista	f

Seuraus	Taso	Vaikutus miehistöön	Vaikutus ajoneuvoon ja sen järjestelmiin
Katastrofi	1	Hengenlähtö, pysyvä työkyvyn menetys jne.	Ajoneuvo uusittava perusteellisesti
Erittäin vaarallinen	2	Silmävamma, pitkäaikaista sairaalahoitoa vaativa jne.	Vaatii pitempiaikaista huol-toa
Marginaalinen	3	Sairaalahoitoa vaativa toimenpide jne.	Vaatii ajoneuvon toimittamista korjaamolle
Vähäinen mahdollisuus	4	Vähäinen vamma, mustelma jne.	Ei häiritse ajoneuvon toiminnallisuutta

Riskien sulkeminen	Luokka	
Luokka	A	Asiakas ja projektipäällikkö yhdessä voi hyväksyä ja sulkea riskin
Luokka	B	Turvallisuustyöryhmä (SSWG) voi hyväksyä sulkea riskin
Luokka	C	Projektiryhmä ja tuoteturvallisuusinsinööri voi yhdessä hyväksyä ja sulkea riskin
Luokka	D	Pve:n Tuoteturvallisuusinsinööri (SS manager) voi sulkea ja hyväksyä riskin

Riskien luokitus					
		Seuraus			
		1	2	3	4
Yleisyys	a	A	A	A	B
	b	A	A	B	C
	c	A	B	C	C
	d	B	C	C	D
	e	C	C	D	D
	f	C	D	D	D

Riskimatriisi, luokitukset A … D yleisyys- ja seuraustasojen mukaisesti

Patria Land & Armament Oy

Timo A Virtanen
AMV 8x8

Vika-, vaikutus- ja kriittisyysanalyysi

8.12.2008

Vetroniikan järjestelmät

H = Henkilö
J = Järjestelmä
Y = ympäristö
O = Operatiivinen toiminta

S = Vaatii edelleen suunnittelua
R = Redundanttisuusratkaisu olemassa
K = Koulutus

Nro	Riski	Riskin kuvaus	Onnettomuus	H	Tilanne	Alku luokitus			Pvm	Kuvaus riskin alentamisesta	Tila	S		Jälki luokitus		
	Nro			J								R				
				Y								K				
				O												
1	H001	Jarrujen katoaminen, lukkiutumattoman jarrujärjestelmän vikatilanne: - Väyläliikenne katkeaa - Ohjelmisto vikaantuu - Toimilaite vikaantuu - Anturointi vikaantuu		H J O	Jarrutettaessa	d	1	B		Jarrujen ohjaus siirtyy tilaan, missä ohjataan suoraan hydrauliikan välityksellä, kovat jarrut. Riskin todennäköisyys d -> f ratkaisun avulla		R		f	1	C