

Tallinna Tehnikaülikool
Elektroonikainstituut

**"Missioonikriitilise kaugseiresüsteemi serverkomponendi
kõrgkäideldavuse tagamine riistvaraliste vahenditega"**

**"Hardware Means for Provision of High Availability Operation of
a Server Component in a Mission Critical Remote Monitoring
System"**

Magistritöö

Autor: Erkki Moorits
Juhendaja: Aivar Usk

Hoiatus: Käesolevas bakalaureusetöös kirjeldatud tehnilised lahendused on Cybernetica AS intellektuaalne omand, mille kasutamine mistahes eesmärgil kas osaliselt või täielikult on lubatud ainult Cybernetica AS poolt kirjalikult antud loal.

Tallinn 2008

Autorideklaratsioon

Deklareerin, et käesolev magistritöö on minu iseseisva töö tulemus ning töö tervikuna ega selle osad ei ole kopeeritud teiste autorite tööd ilma sellekohaste viitamisteta.

Autor: Erkki Moorits

6. veebruar 2008

Resüme

Käesolevas magistritöös kirjeldatakse autori osalusel projekteeritud, toodetud, katsetatud ja käivitatud mitmekomponendilise hajusa kaugseiresüsteemi serverkomponendi kõrgkäideldavuse tagamiseks välja töötatud riistvaralist olekukontrollilahendust ("watchdog" ehk valvekoer), mis põhineb autori poolt loodud originaalsel skeemilahendusel. Töö sissejuhatavas osas antakse ülevaade elektronsüsteemide käideldavuse ja töökindluse määramise põhimõtetest ning valdkonna standardite nõuetest.

Abstract

This thesis paper presents an original hardware solution developed by the author - a "watchdog" - for provision of high availability operation of a server component in a mission critical distributed remote monitoring system. The monitoring system itself was developed, manufactured, tested and deployed with participation of the author. Introductory part of the paper provides an overview of the principles of availability and reliability in electronic systems, and of the requirements of relevant standards.

Sisukord

<u>1. Sissejuhatus</u>	lk. 7
<u>2. Töö eesmärk</u>	lk. 9
<u>3. Kasutatavad lühendid ja mõisted</u>	lk. 10
<u>4. Reaalse töökindla süsteem näide</u>	lk. 13
<u>5. Arvutisüsteemi töökindlus</u>	lk. 14
<u>5.1. Serverkomponendi operatsioonisüsteemi töökindlus</u>	lk. 15
<u>5.2. Serverkomponendi rakendustarkvara töökindlus</u>	lk. 16
<u>5.3. Riistvara vead</u>	lk. 16
<u>5.4. Tarkvara vead</u>	lk. 17
<u>5.5. Võimalikud variandid töö käigus tekkinud vea kõrvaldamiseks</u>	lk. 19
<u>5.6. Käideldavus reserveerimata ja reserveeritud süsteemidele</u>	lk. 20
<u>5.6.1. Reserveerimata süsteemi käideldavus</u>	lk. 20
<u>5.6.2. Reserveeritud süsteemi käideldavus</u>	lk. 21
<u>5.7. Funktsionaalne ohutus</u>	lk. 23
<u>5.7.1. Reserveerimata süsteemi tõrketõenäosus</u>	lk. 24
<u>5.7.2. Reserveeritud süsteemi tõrketõenäosus</u>	lk. 27
<u>5.8. Valvekoeraga ja valvekoerata süsteemide võrdlus</u>	lk. 28
<u>6. Nõuded riistvaralisele valvekoerale</u>	lk. 31
<u>6.1. Nõuded valvekoerale</u>	lk. 31
<u>6.2. Ülevaade riulitoodetest valvekoertest</u>	lk. 32
<u>7. Valvekoera realisatsioon</u>	lk. 33
<u>7.1. Lahenduse valik</u>	lk. 33
<u>7.2. Sisendaste</u>	lk. 35
<u>7.3. Väljundaste</u>	lk. 37
<u>7.4. Viite seadistamine</u>	lk. 37
<u>7.5. Töökindlus</u>	lk. 39
<u>7.6. Lahenduse põhiahela katsetused prototüübi abil</u>	lk. 42
<u>7.7. Lõpliku valvekoera põhimõtteline lahendus</u>	lk. 43
<u>8. Kokkuvõte</u>	lk. 45
<u>9. Kasutatud kirjandus ja Interneti lingid</u>	lk. 46
<u>10. Lisa</u>	lk. 48

<u>10.1. Tõrkemäära tabel</u>	lk. 48
<u>10.2. Tõrketõsiduse tabel 1</u>	lk. 48
<u>10.3. Tõrketõsiduse tabel 2</u>	lk. 48
<u>10.4. Avastamismäära tabel</u>	lk. 49
<u>10.5. Valvekoera FMECA tabel</u>	lk. 50

Jooniste loetelu

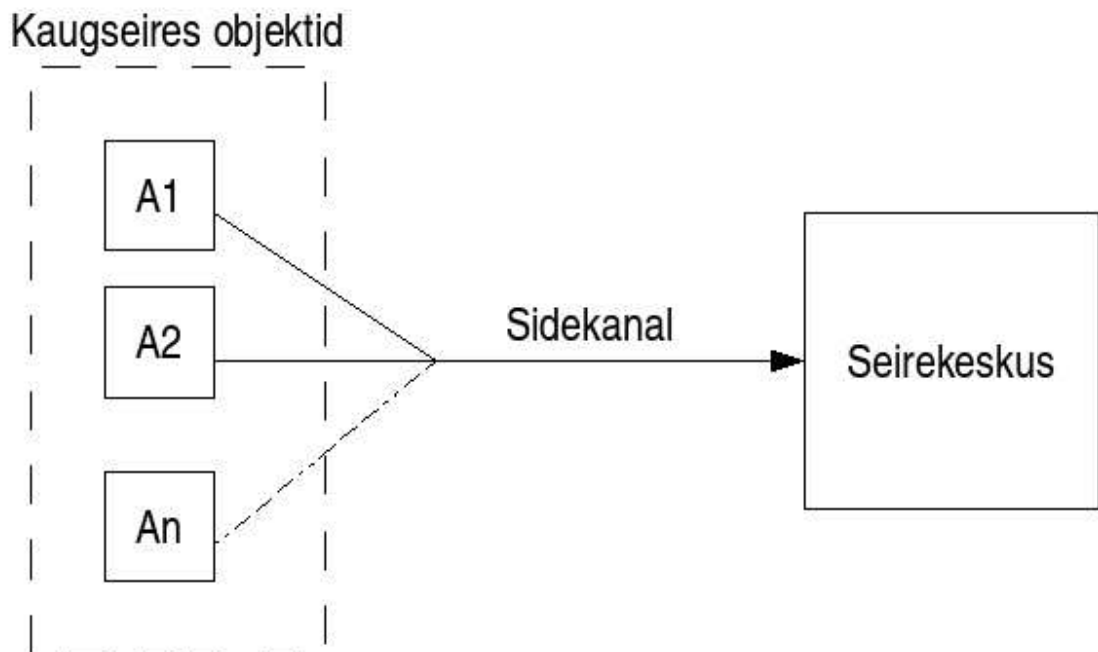
Joonis 1: Hajutatud kaugseiresüsteemi tüüpiline arhitektuur.....	7
Joonis 2: Reaalne GSM/GPRS kaugseire süsteem.....	13
Joonis 3: Reserveerimata süsteem.....	20
Joonis 4: Reserveeritud süsteem.....	21
Joonis 5: Reserveerimata süsteem.....	24
Joonis 6: Reserveeritud süsteem.....	27
Joonis 7: Valvekoerata süsteemi käideldavus.....	28
Joonis 8: Valvekoeraga süsteemi käideldavus.....	29
Joonis 9: Süsteemi tõrketõenäosus.....	29
Joonis 10: 4536 põhimõtteskeem.....	34
Joonis 11: Optron sisendaste.....	35
Joonis 12: 4536 mikroskeemi RC generaatori väline osa.....	37
Joonis 13: Sageduse vea ja temperatuuri sõltuvus.....	38
Joonis 14: Valvekoera prototüüp.....	42
Joonis 15: Valvekoera lõplik põhimõtteskeem.....	44

Tabelite loetelu

Tabel 1: Tõrkesagedused kõrge nõudlusega süsteemi jaoks.....	23
Tabel 2: Tõrkesagedused madala nõudlusega süsteemi jaoks.....	24
Tabel 3: Valvekoera perioodi (2N) ja temperatuuri sõltuvus.....	39
Tabel 4: Valvekoera kõikide komponentide FIT tabel.....	40
Tabel 5: Valvekoera pooljuhtkomponentide FIT tabel.....	41

1. Sissejuhatus

Kaasajal kasutatakse mitmesuguste hajutatud süsteemide tehnilisest olekust ülevaate saamiseks selliste objektide kaugseiret, mille korral mitmetel seireobjektidel paiknevad sideseadmed edastavad objektile paiknevatelt anduritelt lähtuvat oleku- ja olekumuutusinformatsiooni seirekeskusele (Joonis 1).



Joonis 1: Hajutatud kaugseiresüsteemi tüüpiline arhitektuur

Sageli on sedasorti süsteemides liikuv informatsioon ajakriitilise iseloomuga ning tihti võivad lisanduda sellistele süsteemidele ka standardis IEC-61508-1[1] sätestatud ohutusalsed nõuded. On ilmne, et suurimad riskid seda sorti süsteemides on seotud seirekeskuses kasutatava süsteemikomponendiga, millele enamasti esitatakse ka kõrgendatud käideldavusnõudeid.

Tööks ohuskriitilistes rakendustes kasutatakse spetsiifiliselt selleks otstarbeks loodud arvutustehnilisi tooteid, mis on kitsa turu ja pikaajaliste testimis- ja sertifitseerimisprotseduuride tõttu kallid ning sageli mõnevõrra aegunud. Seetõttu eksisteerib ahvatlus kasutada võimaluse korral standardseid arvutikomponente, mille eelisteks on parem

jõudlus, lihtsam asendatavus, varuosade saadavus ja hind, mõningaseks puuduseks aga sageli raskesti määratav töökindlus ja tõrgete esinemise tõenäosus.

Turu surve elektroonikatoodele paneb nii tarkvara kui ka riistvara arendajad raskesse olukorda, kus tuleb minimaalse ajaga valmis saada töötav toode ja seda konkurentidest odavamalt. Selline olukord teeb küllaltki keerukaks süsteemi projekteerimise ja testimise. Oma osa annab siia juurde ka see, et osades sardsüsteemides on programmid on kasvanud küllaltki suureks, kusjuures ei ole eriti haruldane see kui programmi suurus on mõnikümmend megabaiti. Lisaks programmi vigadele võib esineda ka väliste elektromagnetväljade poolt põhjustatud tõrkeid.

Enamusel juhtudel väljendub viga süsteemi “kokkujooksmisena”, mis ei riku küll riistvara, kuid seiskab seireotstarbelise tarkvara töö ning katkestab süsteemi töö (missiooni). Juhul, kui kokkujooksnud süsteem asub näiteks kodus ja ei põhjusta midagi muud peale ebameeldivuste, siis pole eriti hullu. Samas, kui kokkujooksnud süsteem asub kaugemal, kus on talle raske juurde pääseda, on probleem tõsisem; kui aga sellest kokkujooksnud süsteemist sõltub kellegi vara puutumatus või tervis ja elu, on olukord kriitiline. Muidugi võib esineda ka selliseid olukordi, kus viga on olnud niivõrd tugev, et pärast süsteemi taaskäivitamist ei ole võimalik seadet tööle saada; selliste vigade puhul aitab ainult süsteemi remont või väljavahetamine.

2. Töö eesmärk

Töö eesmärgiks on uurida arvutisüsteemi töökindlusega ning sellest tuleneva tarkvararakenduse käideldavusega seotud tegureid ning leida sobiv lahendus kaugseiresüsteemi serverkomponendi kõrgendatud töökindluse või käideldavuse tagamiseks riistvaraliste meetoditega, riistvaralise valvekoera (watchdog timer) mõju süsteemile töökindlusele ja teha kindlaks, millisest hetkest on mõttekas kasutada valvekoera. Lisaks valvekoera mõju uurimisele süsteemile tuleb leida sobiv robustne ja universaalne riistvaraline lahendus, mis oleks tunduvalt töökindlam kui arvuti, millega ta ühendatakse. Vajadus eraldiseisva valvekoera järgi on tingitud sellest, et olemasolevad integreeritud ja lisakaartidena saadaval olevad valvekoerad on programmiselt keerulise juurdepääsuga ja tihtipeale ei ole nendega võimalik jälgida konkreetselt kasutaja missiooni tagava tarkvararakenduse (programmi) tööd.

3. Kasutatavad lühendid ja mõisted

DC	<i>Diagnostic Coverage</i> , testide poolt avastatud tõrgete suhe teoreetiliselt kõikidest võimalikest avastavatest tõrgetest, näidatakse üldiselt protsentides [2].
EMC	<i>Electromagnetic compatibility</i> , elektromagnetiline ühilduvus.
ESD	<i>Electrostatic discharge</i> , on kiire staatilise elektri potentsiaalide ühtsustamine kahe üksteisele lähedal asuva laetud keha vahel. Piisavalt suure pinge korral on elektroonikaseadmete kahjustamine võimalik.
FIT	<i>Failures In Time</i> , statistiline eeldatav tõrgete määr miljardi 10^9 töötunni kohta. Peamiselt on kasutatavad FIT väärtusi pooljuhtkomponentide tootjad [3].
FMECA	<i>Failure Mode, Effects, and Criticality Analysis</i> , analüüsi protseduur millega determineeritakse süsteemi kõik võimalikud tõrke režiimid ja klassifitseeritakse kõik potentsiaalsed tõrkerežiimid vastavalt nende tõsidusele [4]. FMECA analüüs tõstab oma tulemustega esile suurema tõenäosusetega ja tõsisemate tagajärgedega tõrkeid [5][6].
ISA	<i>Industry Standard Architecture</i> , IBM PC-ga ühilduvate arvutite siin, ISA siini lauseks on 8 või 16 bitti, praeguseks vananenud ja tootmisest kõrvaldatud [7].
Käideldavus (availability)	Käideldavus on toote suutlikkus olla sellises seisundis, mis võimaldab täita vajalikku funktsiooni vastavalt etteantud tingimustele suvalisel ajahetkel või intervalli järel, eeldusel et vajalikud välisressursid on olemas [8][4].
Mission	Mission on eesmärk mis on antud kindlatele inimestele, inimgruppidele, organisatsioonidele või seadmetele [9].
Mission-critical (missioonikriitiline)	Termin missioonikriitiline viitab faktorile (varustus, protsess, protseduur, tarkvara, jne), millest sõltub edukas ülesande või projekti täitmine. Lisaks võib see termin viidata ka projektile mille täitmine on organsatsioonile eluliselt tähtis [10].

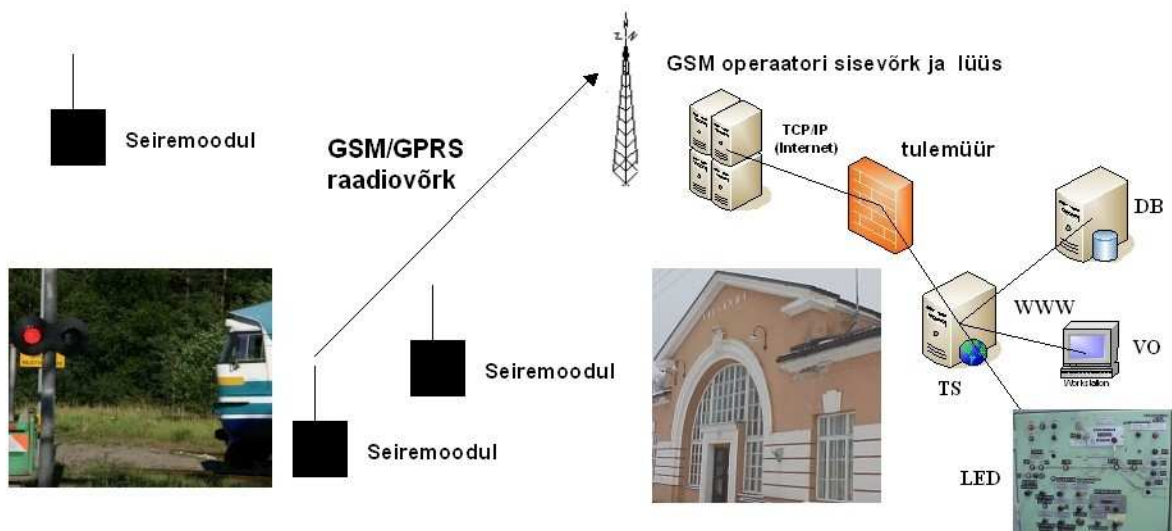
MTBF	<i>Mean Time Between Failures</i> , keskmine tõrgetevaheline aeg, kehtib süsteemi kohta mida on võimalik parandada [4]. Arvutustes eeldatakse et peale igat tõrget parandatakse süsteem aja MTTR jooksul ja seatakse tööle peale vea parandamist. Üldiselt kehtib riistvara kohta, kuid saab ka kasutada tarkvara puhul, selleks korrutatakse defektide esinemissagedus KLOC (<i>Kilo Line Of Code</i>) väärtusega mis täidetakse sekundi jooksul.
MTTR	<i>Mean Time To Recovery</i> , või <i>Mean Time To Repair</i> , keskmine taastumis aeg, aeg mille jooksul seade taastub veast, tarkvara puhul loetakse taastumiseajaks aega mille jooksul tarkvara seab ennast peale veadetektimist uuesti töökorda. Juhul kui on tegemist vea parandamisega või hooldamisega, siis on see peamine võrdlusparameeter seadmete hooldatavusel [4].
PCI	<i>Peripheral Component Interconnect</i> , Inteli poolt väljatöötatud 32 või 64 biti laiune arvuti siin, üheksakümnendate lõpus tõrjus turult välja aeglasema ISA siini [11].
PDF	<i>Probability of Failure on Demand</i> , tõrke tõenäosus seadme või mõne selle funktsiooni kasutamise vajadusel. Kehtib madala nõudlusega süsteemidele [1].
PFH	<i>Probability of Failure on Hour</i> , tõrke tõenäosus tunnis. Kehtib kõrge nõudlusega süsteemidele [1].
RoHS	<i>Restriction of Hazardous Substances</i> , 1 juulil 2006 Euroopa liidus kehtima hakanud ohtlike ainete piiramise direktiiv. Elektroonikatööstusel oli kõige suuremaks muutuseks plii kadumine jootmisprotsessist [12].
SIL	<i>Safety Integrity Level</i> , tõenäosuse tase et ohutuskriitiline süsteem ei täida talle ettenähtud funktsioone eelnevalt määratletud parameetrite ja perioodi jooksul [2].
SMD	<i>Surface-Mount Device</i> , pindmontaaži komponent.
USB	<i>Universal Serial Bus</i> , universaalne seriaal liides arvutiga väliste seadmete ühendamiseks, võimalikud kiirused on 1,5 Mbit/s, 12 Mbit/s ja 480 Mbit/s[13].

Valvekoer

Watchdog Timer (WDT), süsteemi komponendi “tervist” jälgiv ning oodatud lähtestamissignaali puudumisel etteantud ajalise intervalli möödumisel komponendi taaskäivitust teostav riistvaraline elektroonikasõlm. Käesolevas töös vaadeldakse kõige lihtsamat versiooni valvekoerast mis ei jälgi otseselt protsessori tööd [14].

4. Reaalse töökindla süsteem näide

Järgnevalt on toodud reaalne näide raudteeülesõidukoha fooriautomaatika kaugseiresüsteemist kus kasutatakse lihtsal Töökindlal Serveril (TS) põhinevat lahendust, mis töötab küll madala intensiivsusega või mõõdukate sisend- ja väljundinfovoogude ja koormusega, kuid peab omama kõrgendatud käideldavust. Võrguoperaator (VO) töötab kaitstud kohtvõrgus, kasutades serverikomponendiga suhtlemiseks standardseid WWW tehnoloogiaid (veebibrauser ja HTML leheküljed). Operaatori kiireks informeerimiseks kaugobjekti oleku kriitilistest muudatustest kasutatakse serverikomponendi poolt juhitavaid, otse raudteejaama infopaneelis paiknevaid valgusdiodindikaatorid (LED). Missioonikriitiliseks komponendiks on selles süsteemis serverarvuti koos seirerakendusega (TS).



Joonis 2: Reaalne GSM/GPRS kaugseire süsteem

Joonisel 2 toodud reaalne kaugseiresüsteem kasutab nii GSM/GPRS kui ka vahepealset üldkasutatavat andmeside võrku. Ülesõidukoha informatsiooni peale operaatori näevad ainult selleks volitatud isikud. Seda tüüpi süsteemil ei ole küll suuri edastatavaid andmehulkasid ja ei ole ka väga kriitiline talletada pikalt olekuinformatsiooni, kuid kindlasti ei tohi olla süsteemi töös tõrkeid, käideldavus peab olema vägagi kõrge ning ülesõidu olekud peavad operaatorini jõudma võimalikult lühikese ajaga.

5. Arvutisüsteemi töökindlus

Arvutisüsteemi töökindluse määravad peamiselt kaks faktorit – riistvara töökindlus ja tarkvara (programmide) töökindlus. Lisaks on võimalik mõlemat faktorit mõjutada väliselt. Näiteks, kui arvutisüsteem on suurte elektromagnet häiretega keskkonnas siis võivad välised häired arvuti tööandmeid rikkuda ja sellega põhjustada arvuti töös vigu, mis võivad olla isegi katastroofilised. Eelpool mainitule lisandub potentsiaalse vea allikana ka veel inimfaktor ja võimalik, et isegi veel suuremal määral kui seda on muud põhjused.

Tüüpilise süsteemikomponendina kasutatava x86 arhitektuuriga emaplaadi tootja poolt antud tõrketa tööaeg (MTBF) on 30 000 kuni 50 000 tundi. Kõvaketastel on tavaliselt tõrketa tööaeg 100 000 kuni 250 000 tundi.

Eeldades, et süsteemis kasutatava tarkvara korral on rakendatud kõiki võimalikke kõrget töökindlust tagavaid meetmeid, on kõrgendatud käideldavusnõuete saavutamiseks võimalikud järgmised riistvaralised meetodid:

- Kaitse elektrilise ülekoormuse ja teiste väliste mõjude eest
- Pöörlevate osadeta komponentide kasutamine
- Katkematu toiteallika kasutamine
- Valvekoera kasutamine
- Reserveerimine
- Paralleelarhitektuuri kasutamine

Nagu eelnevalt mainitud, võib arvutisüsteemis tekkinud vigu jaotada kaheks – tarkvara vead ja riistvara vead. Järgnevalt vaatleme mõlemat tüüpi vigasid lähemalt, võimalusi nende vähendamiseks, käideldavust ja tõrketõenäosust. Käideldavuse ja tõrketõenäosuse juures vaadeldakse ka reserveeritud ja reserveerimata süsteeme eraldi.

5.1. Serverkomponendi operatsioonisüsteemi töökindlus

Serverkomponendi missiooni tagamisel süsteemis on võtmeküsimuseks serverkomponendis kasutatava operatsioonisüsteemi töökindlus. Tänapäeval kasutatakse operatsioonisüsteemi Linux paljudes rakendustes serverina, seda isegi väga töökindlates süsteemides, samas on Linux'it vägagi hea kasutada ka stabiilse kliendi operatsioonisüsteemina.

Linuxi põhiliseks eeliseks on esmapilgul hind. Kuigi on olnud palju juttu, et puudub süsteemi tootjatugi, ei ole tuge ka nii väga palju vaja, enamusesjuhtudel on vaja lihtsalt algselt süsteem korrektselt tööle saada, mille järel praktiliselt puudub vajadus teda pidevalt hooldada. Kusjuures pikk tööaeg ongi Linuxi juures vägagi ahvatlev omadus. Lisaks pikale tööajale on viimase kümne aasta jooksul on väga palju tegeldud vabavara levitamise ja arendamisega, seega on Linuxil praktiliselt olemas ka kõik vajaminevad programmid ja teegid. Linuxi kasuks räägib ka veel see, et isegi suured riistvaratootjad nagu IBM, Dell ja HP on viimasel viiel aastal hakanud Linuxile suuremat tähelepanu pöörama ja isegi võtnud ametlikult Linuxi kasutusele mõningatesse oma toodetesse. Peale riistvaratootjate on ka tarkvara tootjad sama teed läinud, väga paljudel Windowsi programmidel on Linuxi all ka töötav alternatiiv olemas. Lisaks suhteliselt laiale programmide valikule toetab Linuxi tuum (kernel) ka väga paljusid erinevaid arvutiarhitektuure, esindatud on isegi suhteliselt väikese jõudlusega ARM mikrokontrollerid. Samas Linuxi puuduseks võib lugeda selle, et standardse kerneliga Linux ei vasta kindlasti reaallaja nõuetele, mis seab Linuxi kasutamisele mõningad piirid, kuid on olemas ka spetsiaalseid kerneli laiendusi, mis võimaldavad Linuxit kasutada ka reaalaega nõudvates lahendustes.

Olukord, kus Linux ei ole praktiliselt mitte ühegi suurfirma ei oma, tekitab keeruka probleemi sertifitseerimise ja töökindluse tõestamise juures. Üheks võimaluseks on see, et mõni valitsuse poolt rahastatud organisatsioon teeb sertifitseerimise ära, kuid siamaani pole seda teadaolevalt tehtud. Samas on tehtud küll uuringuid [15], mis näitavad, et on võimalik kasutada Linuxit ohutuskriitilistes rakendustes ning SIL tasemed 1 ja 2 pole üldiselt probleem, 3 on natukene keerukam kuid mitte ületamatult, aga SIL tase 4 ei ole ühe Linux-põhise süsteemiga reaalne. Kõik uuringud on tehtud reserveerimata süsteemiga, juhul kui on tegemist reserveeritud süsteemiga, siis ei tohiks ka SIL tase 4 probleem olla.

5.2. Serverkomponendi rakendustarkvara töökindlus

Rakendustarkvara töökindlus sõltub peamiselt programmeerija töö kvaliteedist, seda just eriti väikeste projektide puhul, kus on küllaltki väike arendusmeeskond. Peamiseks teguriks töökindluse juures on testijate hulk ja kasutatavad testmeetodid ning just väikestel arendusmeeskondadel võib mõnikord tulla puudu testimise osast. Samas teine tegur töökindlusele on programmeerimisvahendid ja arvutis asuvad nende tööteegid. On võimalik selline olukord, et rakendusprogramm on tehtud korralikult ja testmasinas töötab, aga objektile ei pruugi ta enam töötada kuna teises masinas võivad teised teegid olla. Seega tuleb kindlasti teekide erinevust testiarvutis ja objektile vältida. Lisaks teekide võimalikule erinevusele võib töökindlus sõltuda otseselt arvuti riistvarast, näiteks paljusid kompilaatoreid ja teekide pole hetkel saadud mitme protsessoriga arvutil korralikult tööle.

Ohutuskriitilistele süsteemide töö tagamiseks on esitatud palju nõudeid, mida tuleb täita tarkvara arendusprotsessis. Põhilisteks nõueteks ohutuskriitilise süsteemi tarkvara tegemisel on vägagi detailne dokumentatsioon mis hõlmab nii projekti juhtimist, programmeerimist, kui ka testimist. Projektijuhtimisel peaks lähtuma V tüüpi lähenemisest [8], mis koosneb „ülalt–alla“ ja „alt–üles“ etappidest ning mis hõlmab kogu ohutuse elutsükli. Lisaks korrektsele projektijuhtimisele ja dokumentatsioonile on mõnel juhul vaja ka välise organisatsiooni poolt tehtud tarkvara kontrolli (valideerimist ja verifitseerimist). Üldiselt peaks programmeerija kasutama mõnda keelt, mis ei võimalda eriti vigu teha ja kindlasti peab olema korrektne programmi kirjutamise stiil ning ei tohi mitte mingil juhul kasutada mittemingisuguseid programmeerimiskeele dokumenteerimata lisasid.

5.3. Riistvara vead

Riistvara vead jagunevad kaheks – mööduvad vead ja püsivad vead. Mõlemat tüüpi vigade põhjustajaks saavad olla kas tootmispraak, vananemine või välismõju. Toomispraaki ja vananemise vastu on kasutajal suhteliselt vähe teha, ainukene variant on valida kindel tootja ja toote oletatava eluaja lõpul vahetada toode välja. Kuid on võimalus et tootja on teinud praakpartii, siis lõpetavad reeglina kõik ühes partiis tehtud seadmed enamvähem samal ajal töö, selletõttu tuleks vältida täpselt samast partiid kõikide seadmete juures. Samas välismõju

poolt annab kasutajal küllaltki palju ära teha, näiteks süsteemile sundjahutuse panemine, õhuniiskuse kontroll ja väliste tugevate elektromagnet väljade eest kaitsmine.

Arvuti riistvara töökindluse puhul mängib olulist rolli temperatuur, mida kõrgem temperatuur seda väiksem töökindlus. Töökindluse sõltuvus temperatuurist on tingitud sellest, et kõrgematel temperatuuridel toimub mikroskeemides elektrit juhtivate radade materjali liikumine (*electromigration*) [16][17]. See efekt sõltub temperatuurist ja mikroskeemi tehnoloogiast, mida väiksemate mõõtmetega tehnoloogija seda suurem on materjali liikumise oht. Materjali liikumiset tingitud vead ei ole mööduvad vead.

Mõlemat tüüpi vead avalduvad ühtemoodi, kas täieliku või osalise seadme töövõime kaotuisena. Kuid vea kõrvaldamise meetodid on mõlemat tüüpi vigadel erinevad – püsiva vea puhul peab rikkis seadme välja vahetama, aga mööduva vea puhul piisab tihti ainult taaskäivitusest (resetist) või siis toitelülitamisest.

5.4. Tarkvara vead

Enamusjaolt on tarkvara vead põhjustatud programmeerija vigadest, muidugi väiksemal määral võivad olla vigade põhjustajaks ka kompilaatorid või translaatorid ning operatsioonisüsteem ise. Järgnevalt vaatlen võimalikke vea põhjuseid ja meetodeid, mille kasutamine võimaldaks vigu ära hoida.

Kuna suurem osa tarkvara vigu teeb programmeerija ise, siis tuleks piirata tal selliseid vea tekitamise võimalusi. Üheks võimaluseks, millega saab vähendada programmeerija poolt tekitatud vigu, on kasutada programmeerimiskeeli, mis on mõeldud missioonikriitilistele süsteemidele, nagu on näiteks Ada. Samas ei ole standardis IEC-61508-3 [18] täpselt välja toodud ühtegi spetsiifilist keelt, mis oleks mõeldud missioonikriitilisele süsteemile, on ainult toodud soovituslik nimekiri. Lisaks sellele on ära märgitud, et on võimalik kasutada suvalist programmeerimiskeelt, ainukeseks kitsenduseks suvalise keele kasutamise puhul on pärastine programmi koodi automaatne kontroll selleks tehtud spetsiaalse programmi poolt, näiteks Splint [19] C keele puhul. Kuid ikkagi ei ole võimalik viia eelkirjeldatud meetmetega programmeerija poolt tehtud vigade arvu nulli; kõige paremaks näiteks selle juures võib tuua

Ariane 5 lennu 501 õnnetuse [20], mis ei olnud ainult programmeerija viga, kuid programmeerija oleks saanud seda ära hoida. Ariane 5 lend 501 oli täielik läbikukkumine – raketi juhtarvuti keeras umbes 35 sekundit pärast starti düüsid sellisesse asendisse, mis tekitas raketi keres väga suuri mehaanilisi pingeid, mille tulemusena oleks rakett lihtsalt mitmeks osaks purunenud; et raketi purunemist mitmeks osaks vältida, anti maapealt enesehävituskäsk. Muidugi täielikult ei saa tarkvara vigade põhjustamises ka programmeerijat süüdistada; statistika näitab, et umbes 50% tarkvara vigadest on tulnud vigasest tarkvara projekti juhtimisest ning vigast juhtimist on väga raske elimineerida. Lisaks sõltub tarkvara vigade arv programmi suurusest, näiteks tarkvara MTBF väärtuse arvutamisel võetakse seda isegi arvesse, seega on võimalik, et viletsamal riistvaral võib lihtsam tarkvara tunduvalt paremaid tulemusi anda kui töökindlal riistvaral keerukas kuid vigane tarkvara.

Lisaks programmeerija poolt ja projektijuhtimisel tehtud vigadele ning programmi pikkusest tingitud vigadele võib tarkvara vigu põhjustada ka operatsioonisüsteem ise. Hetkel on praktiliselt võimatu leida tarkvara süsteemi mis oleks ainult ühe protsessiga, erandiks on ainult lennukite Fly-By-Wire [21] süsteemid, millest mõningad on täiesti lineaarsete programmidega. Operatsioonisüsteemi viga seisneb selles, et suurematel ja keerukamatel protsessoritel on võimalik jaotada protsesside mäluosasid nii, et üks protsess ei muudaks teise mäluosa, seevastu väiksematel protsessoritel ei ole see võimalik. Siit tekibki väiksematel protsessoritel probleem – suhteliselt keerukas on ette ennustada protsesside olekut ja mäluhõivet ning seega on võimalik olukord, kus üks protsess kirjutab teise protsessi mäluosa üle ja põhjustab sellega kogu süsteemi kokkujooksmise. Kuigi suuremates protsessorites on mälu eelnevalt ära jaotatud, siis selline olukord on suuremalt jaolt välistatud, kuid on võimalik, et kuskil tekib mäluleke ja selle tulemusena võib osa süsteemist või kogu süsteem ikkagi kokku joosta.

Kolmandaks veapõhjuseks on kompilaatori või translaatori viga. Kuigi IEC-61508-3 [18] standardis on märgitud, et tuleb kasutada sertifitseeritud kompilaatoreid või translaatoreid ei ole jälle mitte ühtegi spetsiaalselt välja toodud. Kuid standardis on jäetud võimalus, et võib kasutada muid kompilaatoreid ja translaatoreid; ainukeseks piiranguks on nende korrektsuse tõestamine, mida võib tõestada eelnevate toodete ajaloo baasil.

Tarkvaralise vea puhul käitub süsteem samamoodi nagu mööduva riistvaralise vea puhulgi – süsteem võib osaliselt või täielikult oma funktsionaalsuse kaotada. Järgnevalt on eeldatud, et kõik tarkvaralised vead on taastuvad, ehk kompilaator on teinud programmi, mis ei jookse kokku samas kohas, ning programm–mälus olev programm ei ole mingi põhjusel kannatada saanud.

5.5. Võimalikud variandid töö käigus tekkinud vea kõrvaldamiseks

Nii riistvara kui ka tarkvara vea kõrvaldamine käib sarnaselt, millest esimene ja eelistatum võimalus on töö käigus vea kõrvaldamine ja teine võimalus on mõningase töökatkestusega vea kõrvaldamine. Juhul, kui riistvara on tehtud reserveerimisega, siis tihtipeale on võimalik mõlemat tüüpi viga elimineerida selliselt, et see ei mõjuta kogu süsteemi tööd. Juhul, kui ei ole reserveerimist tehtud, siis on ikkagi võimalik et saab viga kõrvaldada, ilma et see mõjutaks kogu arvutisüsteemi tööd; selleks on vaja, et vea kõrvaldamine käiks kiiremini kui süsteemi nõutav reageerimisaeg.

Riistvaralise reserveerimisega tehtud arvutisüsteemil, millel on vähemalt kolm paralleelset arvutusosa ja väljundväärtus leitakse enamushääletusega, on võimalik, et igal arvutusosal on oma vahikoer, mis kontrollib selle arvutusosa tööd. Selline lahendus on võimeline taastama süsteemiosa funktsionaalsust, ilma et kogu süsteem kaotaks oma funktsionaalsust. See kehtib täielikult mööduva tarkvaralise ja riistvaralise vea puhul. Püsiva tarkvaralise ja riistvaralise vea korral on vajalik teenindava personali sekkumine.

Ilma riistvaralise reserveerimiseta jääb üle ainult eelpool mainitud vea kiire elimineerimine või siis mingi märgatava viitega elimineerimine. Ja nagu ka reserveeritud süsteemi püsiva vea puhul on siin võimalik, et vigade kõrvaldamiseks läheb vaja teenindava personali sekkumist, seda kindlasti suurema tõenäosusega kui reserveeritud arvutisüsteemil puhul.

5.6. Käideldavus reserveerimata ja reserveeritud süsteemidele

Käideldavus on serverikomponendi jaoks üks tähtsamaid näitajaid (missiooni parameetreid). Käideldavusi analüüsid on võimalik võrrelda erinevaid arvutisüsteeme kui ka leida võimalikke kitsaskohti süsteemides, näiteks kui andmeedastus käib erinevaid kanaleid pidi ning need kanalid on erineva stabiilsusega.

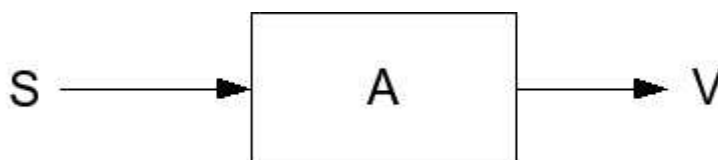
Käideldavus on leitav järgnevalt:

$$A = \frac{\text{TotalTime} - \text{DownTime}}{\text{TotalTime}} = \frac{\text{MTBF}}{\text{MTBF} + \text{MTTR}}$$

Eelnev käideldavuse valem kehtib eksploatatsioonilise käideldavuse kohta, edaspidi on kõikide käideldavuste all mõeldud eksploatatsioonilist käideldavust.

5.6.1. Reserveerimata süsteemi käideldavus

Vaatleme järgnevat ühest lülist koosnevat süsteemi, kus S on sisend, V väljund ja A arvutisüsteem.



Joonis 3: Reserveerimata süsteem

Näiteks võib võtta reaalse reserveerimata süsteemi mis asub teenindavast personalist kaugel ja on valvekoerata. Süsteemi tööperioodiks on näites 5040 tundi, mille jooksul on olnud kolm viga millest keskmiselt iga vea kestvus oli 48 tundi.

$$A = \frac{\text{TotalTime} - \text{DownTime}}{\text{TotalTime}} = \frac{5040 - 144,0}{5040} = 0,9714$$

See vastab umbes 250 tunnile või 10,4 päeva aastas.

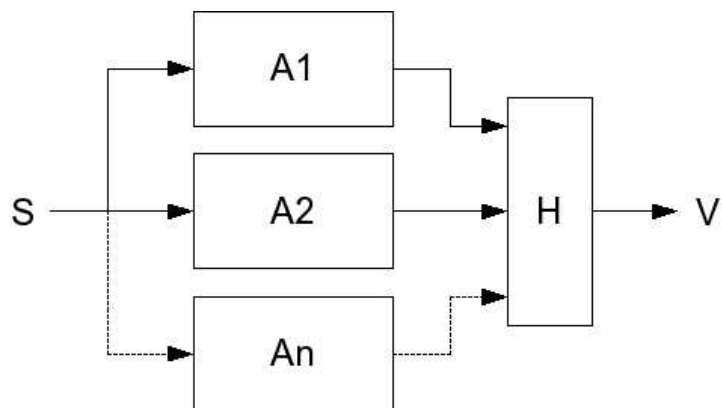
Juhul kui sellele süsteemile paigaldada valvekoer, millega on saavutatud 5040 vaatluse tunni jooksul kõigest 30 minutit seisakuaega (0,5 tundi), siis on käideldavus järgmine:

$$A = \frac{TotalTime - DownTime}{TotalTime} = \frac{5040 - 0,5000}{5040} = 0,9999$$

See vastab 52 minutile aastas ja annab valvekoerata süsteemiga võrreldes 288 korda suurema käideldavuse.

5.6.2. Reserveeritud süsteemi käideldavus

Vaatleme järgnevat paralleelsüsteemi, kus $A_1 \dots A_n$ on arvutisüsteemid, H on enamushääletussüsteem, S sisend, V väljund.



Joonis 4: Reserveeritud süsteem

Järgnevates arvutustes on eeldatud, et enamushääletuse osa käideldavus on tunduvalt suurem kui süsteemi ülejäänud osadel, seega ei võeta enamushääletusosa vaatluse alla. Kuna eelnevalt oli leitud käideldavus ühele süsteemile, siis ei hakka me siin uuesti ühe osa käideldavust leidma.

Käideldavus n paralleelsest alamosast koosnevale süsteemile on järgnev:

$$A_p = 1 - [(1 - A_1)(1 - A_2) \dots (1 - A_n)]$$

Juhul, kui kõik alamsüsteemide käideldavused on võrdsed, kehtib seos:

$$A_p = 1 - (1 - A)^n$$

Näitena võib võtta reaalse kolmest paralleelsest arvutusüsteemist koosneva süsteemi, mis asub teenindavast personalist kaugel ja on valvekoerata. Süsteemi tööperioodiks on 5040 tundi, mille jooksul on olnud kolm viga, millest keskmiselt iga vea kestvus oli 48 tundi, kokku 144 tundi; võrdsete kestvustega vead on kõige halvem juhul mis saab olla. Kuna eelnevalt oli ühe osa käideldavus leitud, siis leiame paralleelse käideldavuse.

$$A_p = 1 - (1 - A)^3 = 0,99998$$

See vastab 12,25 minutile aastas.

Juhul, kui igal osal on oma valvekoer, siis on mõttekas leida arv, mis näitab, kui palju üheksaid on pärast koma, et iseloomustada süsteemi "üheksate arvuga":

$$A_{pN} = -\log_{10}(1 - (1 - (1 - A)^n)) = -\log_{10}((1 - A)^n)$$

Kolme paralleelse arvutussüsteemiga seadmel, mille igal alamsüsteemil on valvekoer, on järgmine käideldavus:

$$A_{pN} = -\log_{10}((1 - A)^3) = 12$$

Arvutuslikult on sellise süsteemi tööseisakute aeg aastas 32 mikrosekundit.

5.7. Funktsionaalne ohutus

Funktsionaalne ohutus on üheks näidikuks turva- või missioonikriitilisel süsteemil. Väga laialt on levinud rahvusvaheline standard IEC-61508 koos oma alamosadega, mis määratleb funktsionaalne ohutuse elektrilisele, elektroonilisele või programmeeritavale (E/E/PES) ohutuskriitilisele süsteemile. See standard on aluseks paljudele teistele standarditele ning kehtiv peaaegu kõikides tööstusharudes, siia alla kuuluvad: raudtee, mõningane maapealne lennunduse juhtimine, tuumatööstus jne.

IEC-61508 ja tema seitse alamosa hõlmavad täielikult ohutuskriitilise süsteemi kõiki kuuteteist elutsüklit, mis jagunevad kolme faasi: faasid 1–5 analüüsi faas, faasid 6–13 realiseerimise faas, faasid 14–16 töö faas. Standard ise koosneb seitsmest osast, osad 1–3 on standardi nõuded (normatiivid), osad 4–7 informatiivsed näited. Standardi IEC-61508 eesmärgiks on viia ohutuskriitilise süsteemi risk võimalikult vastuvõetava tasemeni, rakendades selleks vastavaid ohutuse tagamise nõudeid. Samas, kui teiste tehnoloogiate abil saab suurendada süsteemi turvalisust, siis selle standardi järgi pole neid lisameetmeid kasutada keelatud.

Standard IEC-61508-1[1] määratleb selle, missuguse ohutustasemega seadet võib kasutada mingil objektil ja seob ohutustaseme tunnis esinevate ohtlike tõrgete arvuga. Järgnevalt on ära toodud kaks tabelit tõrkesagedustega ja nendele vastavate ohutustasemetega, millest esimene on kõrge nõudlusega süsteemile (*high demand*) [1][2] ja teine madala nõudlusega (*low demand*) [1][2].

SIL	Ohtlike tõrget esinemissagedus tunnis (PFH)	Keskmiselt üks tõrge t töötunni kohta (MTBF)
4	$10^{-9} \leq x < 10^{-8}$	$10^8 \leq t < 10^9$
3	$10^{-8} \leq x < 10^{-7}$	$10^7 \leq t < 10^8$
2	$10^{-7} \leq x < 10^{-6}$	$10^6 \leq t < 10^7$
1	$10^{-6} \leq x < 10^{-5}$	$10^5 \leq t < 10^6$

Tabel 1: Tõrkesagedused kõrge nõudlusega süsteemi jaoks

SIL	Ohtlike tõrgete esinemissagedus aastas (PFD)	Keskmiselt üks tõrge t tööaasta kohta (MTBF)
4	$10^{-5} \leq x < 10^{-4}$	$10^4 \leq t < 10^5$
3	$10^{-4} \leq x < 10^{-3}$	$10^3 \leq t < 10^4$
2	$10^{-3} \leq x < 10^{-2}$	$10^2 \leq t < 10^3$
1	$10^{-2} \leq x < 10^{-1}$	$10^1 \leq t < 10^2$

Tabel 2: Tõrkesagedused madala nõudlusega süsteemi jaoks

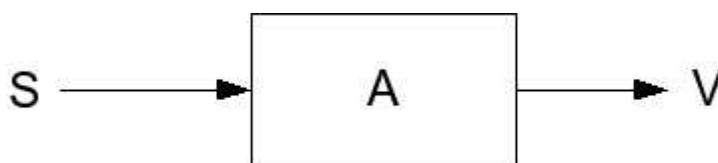
Kõrge nõudlusega süsteemid on süsteemid mida kasutatakse rohkem kui üks kord aastas, näiteks liikluse juhtimine. Seevastu madala nõudlusega süsteemid on süsteemid, mida kasutatakse kuni üks kord aastas, näiteks avarii stopp nupp tööpingil.

Kuna enamust arvutisüsteeme kasutatakse rohkem kui kord aastas, siis edaspidi vaadeldakse ainult kõrge nõudlusega süsteeme.

Järgnevad arvutused on tehtud IEC-61508-6 [22] soovitude järgi.

5.7.1. Reserveerimata süsteemi tõrketõenäosus

Vaatleme järgnevat ühest lülist koosnevat süsteemi, kus S on sisend, V väljund ja A arvutisüsteem.



Joonis 5: Reserveerimata süsteem

Näitena võib võtta reaalse reserveerimata arvutisüsteemi mis asub teenindavast personalist kaugel ja on valvekoerata. Näidissüsteemi tööperioodiks 8760 tundi ehk 365 päeva, mille jooksul on olnud neli viga millest keskmiselt iga vea kestvus oli 48 tundi. Eeldame et see süsteem on kõrge nõudlusega süsteem. Eelneval joonisel oleva süsteemi tõrkeks piisab ainult sellest et arvutuseade oleks töökorrast väljas, ehk tegemist on süsteemiga 1oo1 – 1 out of 1.

Sellise süsteemi poolt demonstreeritud MTBF on järgmine:

$$MTBF = \frac{T}{n} = 2190 \text{ h}$$

Veasagedus on seega:

$$\lambda = \frac{1}{MTBF} = 4,57 \cdot 10^{-4} \text{ h}^{-1}$$

Eeldame, et pooled vigadest on ohtlikud:

$$\lambda_d = \frac{\lambda}{2} = 2,28 \cdot 10^{-4} \text{ h}^{-1}$$

Järgnevalt on vaja leida avastamata ja avastatud vigade tõenäosus, kuna enamalt jaolt on arvutivedad lihtsalt avastatavad, siis võtame DC 99%.

Ohtlikke avastamata vigu on seega:

$$\lambda_{du} = \frac{\lambda}{2} (1 - DC) = 2,28 \cdot 10^{-6} \text{ h}^{-1}$$

Ja ohtlikke avastatud vigu:

$$\lambda_{du} = \frac{\lambda}{2} DC = 2,24 \cdot 10^{-4} \text{ h}^{-1}$$

Kombineeritud töökatkestuste aeg kogu süsteemi komponentidele:

$$t_{ce} = \frac{\lambda_{du}}{\lambda_d} \left(\frac{T}{2} + MTTR \right) + \frac{\lambda_{dd}}{\lambda_d} MTTR = 91,8 \text{ h}$$

Seega saab tuletada järgneva tõrke tõenäosuse:

$$PFH = (\lambda_{du} + \lambda_{dd}) t_{ce} = 2,10 \cdot 10^{-2}$$

Kui samal süsteemil oleks valvekoer, mis viib vea kestvuse (tööseisaku aja) alla maksimaalselt 15 minuti peale, saaksime järgnevad tulemused:

$$t_{ce} = \frac{\lambda_{du}}{\lambda_d} \left(\frac{T}{2} + MTTR \right) + \frac{\lambda_{dd}}{\lambda_d} MTTR = 44,05 \text{ h}$$

$$PFH = (\lambda_{du} + \lambda_{dd}) t_{ce} = 1,00 \cdot 10^{-2}$$

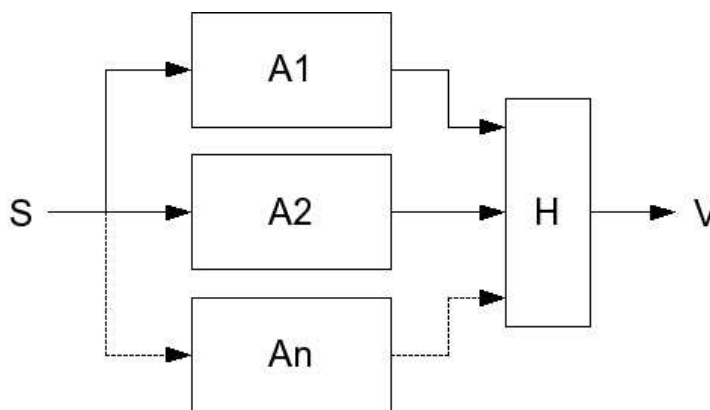
Nagu näha, väheneb valvekoera lisamisega tõrketõenäosus ainult natuke üle kahe korra, kuigi samas on süsteemi käideldavus tõuseb tunduvalt.

Juhul, kui süsteem lülitub vea ilmnedes ennast ümber ohutule režiimile, siis on tõrketõenäosus võrdne ohtliku avastamata vea tõenäosusega.

$$PFH = \lambda_{du} = 2,28 \cdot 10^{-6}$$

5.7.2. Reserveeritud süsteemi tõrketõenäosus

Vaatleme järgnevat paralleelsüsteemi, kus $A_1 \dots A_n$ on arvutisüsteemid, H on enamushääletussüsteem, S sisend, V väljund.



Joonis 6: Reserveeritud süsteem

Järgnevat arvutustes on eeldatud et enamushääletuse osa töökindlus on tunduvalt suurem kui ülejäänud osadel, seega ei võeta enamushääletusosa vaatluse alla. Kuna eelnevalt on leitud, $MTBF$, λ , λ_d , λ_{du} ja t_{ce} , siis neid ei ole enam mõtet uuesti arvutada. Võtame süsteemiks 2oo3 (2 out of 3) mille tõrge tekib siis kui kaks osa kolmest ei tööta.

Valvekoerata süsteemi tõrketõenäosus:

$$PFH = 6((1 - \beta_d)\lambda_d + (1 - \beta)\lambda_{du})^2 t_{ce} + \beta_d \lambda_{dd} + \beta \lambda_{du} = 3,04 \cdot 10^{-5}$$

Kus $\beta = 2\%$ ja $\beta_d = \frac{\beta}{2}$. β – mitme sündmuse kokkusattumisel tekkinud avastamatu põhjusega vea osa, β_d – mitme sündmuse kokkusattumisel tekkinud avastatud põhjusega vea osa.

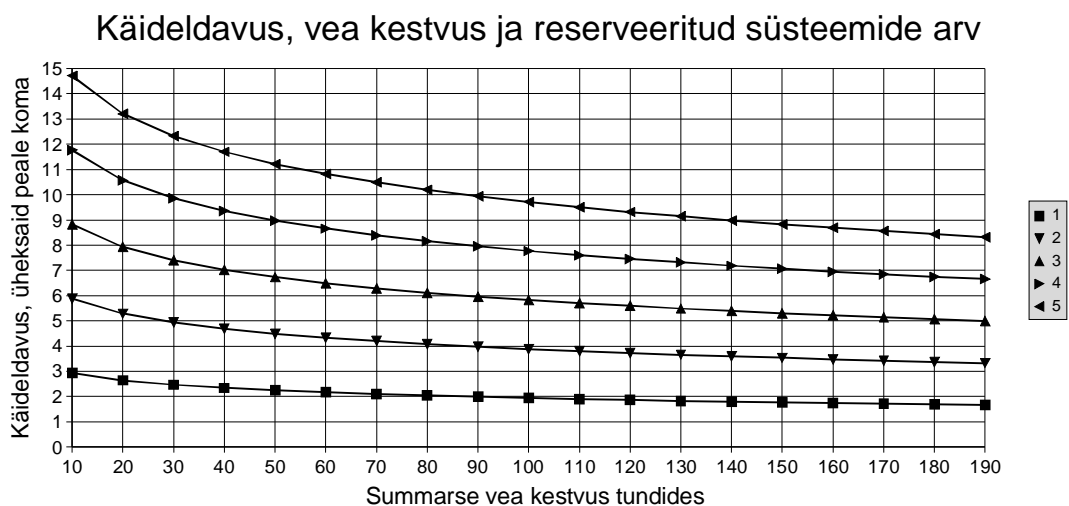
Siis valvekoeraga süsteemi tõrketõenäosus:

$$PFH = 1,58 \cdot 10^{-5}$$

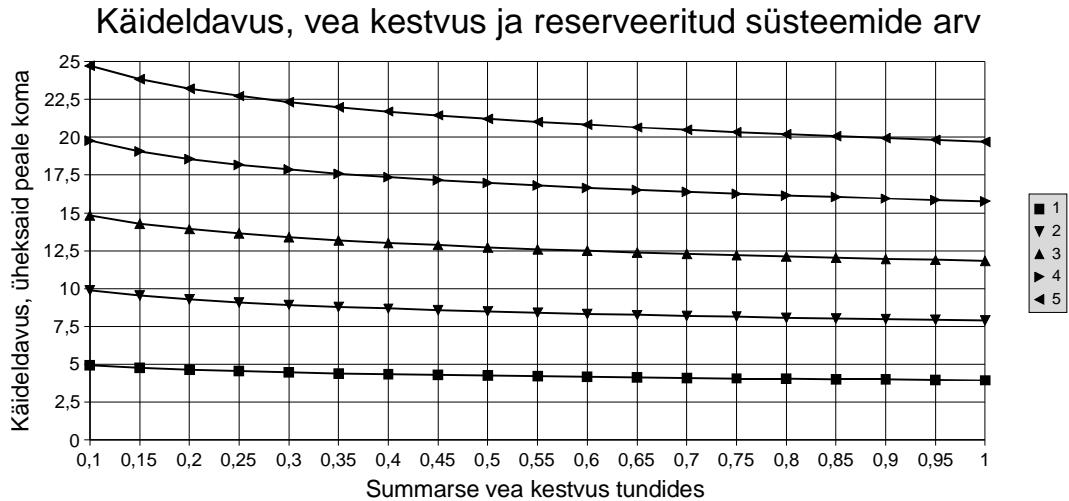
Nagu jälle näha, vähendab valvekoer süsteemi tõrketõenäosust ainult kaks korda ja samas on käideldavus valvekoeraga süsteemil tunduvalt parem kui ilma valvekoerata süsteemil.

5.8. Valvekoeraga ja valvekoerata süsteemide võrdlus

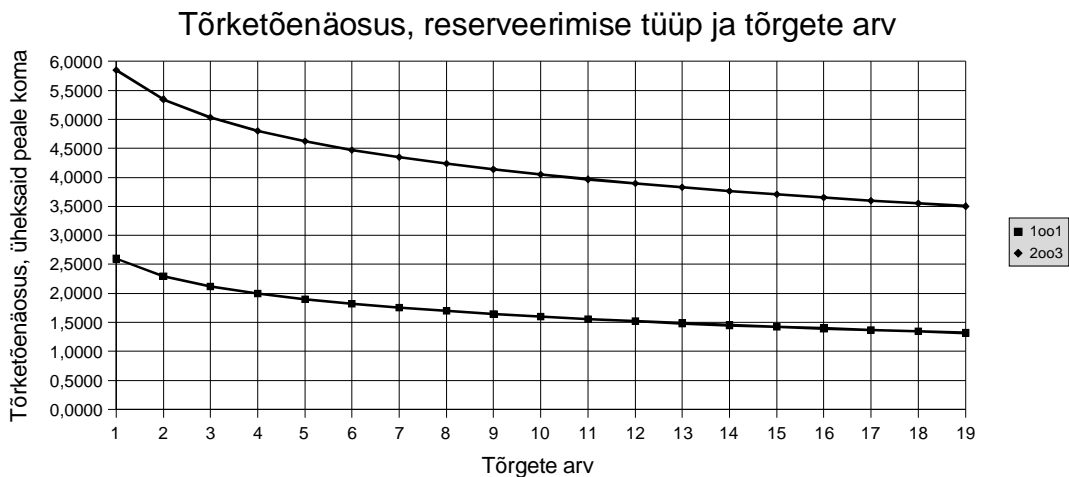
Järgnevalt on ära toodud kolm graafikut, kus esimesel on ühest kuni viie arvutusosani koosnevad süsteemid ilma valvekoerata, teisel on valvekoeraga ja kolmandal on reserveeritud ja reserveerimata süsteemi tõrketõenäosus. Kahel esimesel graafikul on X teljel summaarne vigade kestvus ja Y teljel vigade arv tunnis, kolmandal graafikul on X teljel tõrgeta arv aastas ja Y teljel tõrketõenäosus. Vaadeldavaks perioodiks on võetud 8760 tundi, ehk 365 päeva (1 aasta).



Joonis 7: Valvekoerata süsteemi käideldavus



Joonis 8: Valvekoeraga süsteemi käideldavus



Joonis 9: Süsteemi tõrketõenäosus

Nagu joonistel 7 ja 8 on näha, suurendab valvekoer käideldavust vähemalt ühe suurusjärgu võrra, seda tingimusel, et valvekoera asemel oleks muidu teenindav personal, kes ei pruugi kohe viga tähele panna (hooldusmeeskonna reaktsiooniaeg võib olla märkimisväärne). Kuna tõrketõenäosused ja käideldavus on väga nõrgalt seotud, siis ei ole eriti suurt vahet, kas valvekoer on kasutuses või mitte. Kuid tõrketõenäosust vähendab tunduvalt paralleelne süsteem ja väike tõrgete arv. Seega – kui on nõutav kõrge SIL tase, on kõige lihtsam kasutada paralleelsüsteeme, aga kui on nõutav süsteemi kõrge käideldavus, peab olema garanteeritud kiire vea avastamine ja selle kõrvaldamine. Eelnevate jooniste järgi saaks konstrueerida paberil näitesüsteemi, mis vastab SIL4 tasemele, millel on valvekoer mis kõrvaldab tõrked kahe minuti jooksul alates tekkimisest, kogu tõrgete arv aastas võib olla

ainult kolm katkestust, mis oleksid kokku kuus minutit. Kuid samas, SIL4 tasemele süsteem ilma valvekoerata, võib teha aastas isegi 200 tunnise kogupikkusega tõrke kuid ikkagi jääb SIL4 tasemele, ainult käideldavus on sellisel juhul tunduvalt väiksem.

Lisaks käideldavuse suurendamisele vähendab valvekoer ka tööjõukulusid. Näiteks kui teenindav personal peab tulema iga süsteemi tõrke järel süsteemi uuesti käivitama, tähendab see aastas 2...48 töötundi pikkust spetsialisti hõivamist. Suure tõenäosusega on umbes kaheksa töötundi pikkune spetsialisti hõivamine sama kallis kui seda on valvekoer ise. Seega võib järeldada, et valvekoera ei ole vaja sellises süsteemis, kus ei ole nõutud väga kõrget käideldavust, süsteem on võimeline alati peale taaskäivitamist kiiresti ilma vigadeta taastuma ja on samas piisavalt töökindel et on aastas ainult mõni üksik kokkujooksmine.

6. Nõuded riistvaralisele valvekoerale

Valvekoera ülesandeks on arvutirakenduse kõrgendatud töökindluse tagamine arvutile taaskäivituse tegemise teel arvuti reset-kontaktide lühiajalise kokkuühendamise meetodit kasutades olukorras, kus arvutirakendus on lõpetanud valvekoera kontrollintervalli lähtestamise USB-pordi või optiliselt eraldatud loogikasisendi abil. Kontrollintervalli lähtestamiseks saadab arvutirakendus läbi USB valvekoerale süstemaatilisel ebaolulise sisuga baite.

6.1. Nõuded valvekoerale

1. Toide:

1.1. USB liidesest või väline 5...12VDC, < 75mA

2. Sisendliidesed:

2.1. USB liidesega arvutisisesse ühenduse tegemiseks ette nähtud nelja kontaktiga pin header või USB B liides arvuti tagapaneelis

2.2. Võimalusel optroniga loogikasisend; 2 kontaktiga pin header

3. Väljundliidesed:

3.1. Kaks ümberlülitatavat potentsiaalivaba kontaktipaari, pingetaluvusega vähemalt 50V ja voolutaluvusega vähemalt 1 A.

4. Ajalised parameetrid:

4.1. Kontrollintervalli pikkuse seadistamine vahemikus 2s kuni 1024s (2^{10}).

5. Muud nõuded

5.1. Robustsus, kõrge töökindlus ja pikk eluiga ka kõrgendatud töötemperatuuridel arvutikorpuses (-25...+70°C, MTBF > 20a).

5.2. Vastavus kehtivatele RoHS ja EMC nõuetele, eriti immuunsuse osas.

6.2. Ülevaade riulitoodetest valvekoertest

Internetiotsingu abil õnnestus leida ainult kaks tootjat, kes toodavad tõsiseltvõetavaid valvekoeri personaalarvutitele.

Esimeseks oli Saksa firma QUANCOM Informationssysteme GmbH [23], kellel on küllaltki lai valik erinevaid valvekoeri. Lisaks pakutakse kaasa peale driverite nende lähtekoodi ja täielikku manuaali. Kuid kahjuks on kõik selle firma valvekoerad kas ISA või PCI kaartidena. Seega võib selle firma tooted kõrvale jätta.

Teine tootja on USA firma Berkshire Products Inc. [24], kes pakub peale ISA ja PCI valvekoera kaartidele ka USB valvekoera. Berkshire USB valvekoer on täiesti sobivate arvutiühendustega, on olemas kaks releed, mis mõlemad on piisava voolu ja pingetaluvusega, ainukeseks riistvaraliseks puuduseks on sellel valvekoeral optronisendi puudumine. Lisaks on Berkshire valvekoeral ka küllaltki hea MTBF mis on 59 aastat, ehk 500 000 tundi, samas töötemperatuuri vahemik on $-20^{\circ}C \dots +65^{\circ}C$, mis võiks muidugi kümne kraadi võrra kõrgem olla. Nagu selgub selle valvekoera käsiraamatust, on Berkshire toode sisemise kontrolleri, mis põhimõtteliselt ei sobi missioonikriitilisse süsteemi kontrollisüsteemiks [25]. Veel selgub käsiraamatust, juhul kui on vaja valvekoer panna kasutaja programme jälgima, siis peab veel paigaldama spetsiaalse driveri Windowsile, või siis Linuxile kompileerima uue tuuma (kerneli), millel on selle seadme toetus sees. Kusjuures praktiliselt on võimatu Berkshire valvekoera panna ilma spetsiaalsete driveriteta jälgima kasutaja programmide tegevust, on ainult võimalik panna operatsioonisüsteemi jälgima.

Seega tuleb välja, et hetkel pole turul usaldusväärset tootjat, kellel oleks parasjagu vajaminevat valvekoer riulist võtta. Seetõttu jääb ainukeseks variandiks valmistada ise valvekoer, mis vastaks täielikult kõigile etteantud nõuetele.

7. Valvekoera realisatsioon

7.1. Lahenduse valik

Lähtuvalt valvekoerale esitatud nõuetest - seade peaks olema töökindel ja robustne - on arendusülesanne mõningal määral komplitseeritud.

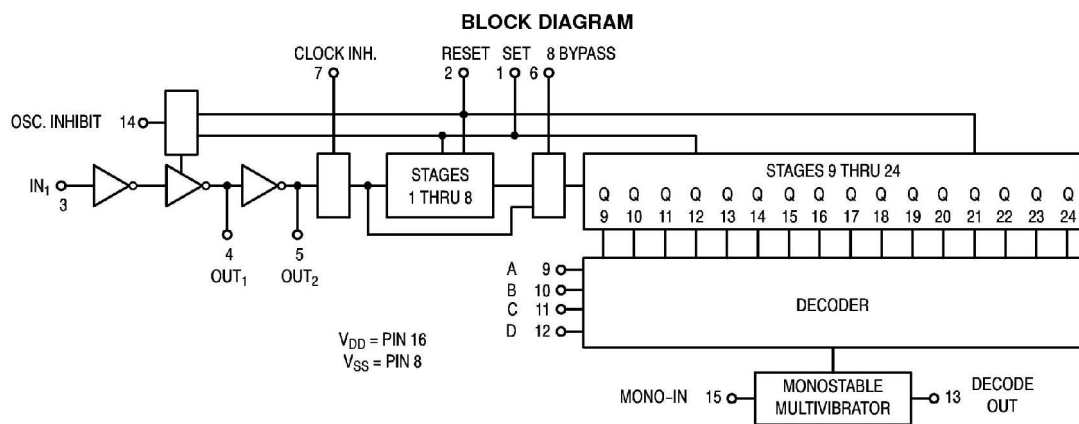
Et saada võimalikult kõrge töökindlusega süsteemi, peab selles süsteemis olema võimalikult vähe komponente; samas peavad kõik komponendid olema võimalikult lihtsad. Selline lähenemine välistab muidugi omakorda mikrokontrollerite kasutamise valvekoerana, lisaks on enamustel mikrokontrolleritel flash programm-mälu, mille MTBF ei pruugi olla kõrgetel temperatuuridel väga suur. Ainukeseks probleemiks töökindlusele on nõuetejärgne USB liides; hetkel on küll saada spetsiaalseid USB konvertereid ühtse mikroskeemina, kuid nad kõik on vägagi keeruka ehitusega ja seega võivad just need kontrollerid saada süsteemi nõrgimaks kohaks.

Nagu eelpool mainitud peab valvekoer olema võimalikult väheste komponentidega teostatav, lisaks on veel nõuetes kirjas, et peab olema võimalik seada 1024 sekundi pikkust kontrollintervalli, seega praktiliselt on välistatud NE555 baasil tehtavad valvekoerad. NE555 töötab komparaatorite baasil ja vajab nii pika perioodi saamiseks väga suure mahtuvusega kondensaatorit ja selle kondensaatori laadimiseks väga suure takistusega takistit. Lisaks suurele kondensaatorile ja takistile oleks küllaltki keerukas seadistada perioodi. Samad põhjused välistavad ka kõik muud ühe taimer baasil tehtud lahendused.

Kuna eelnevalt on välistatud ühe taimer baasil tehtud lahendus, siis üheks võimaluseks lisada taimerile loendur. Loendureid mis on võimelised vähemalt 1024 sekundilist väärtust lugema on olemas päris palju erinevaid ja on olemas ka selliseid loendureid millel on sisemine generaator, mida on võimalik otse loenduriga ühendada. Lihtsamatest loogikaperekondadest on selliseid taimer-loendureid nii 74 kui ka 4000 seeria loogikas, kuid nagu oli nõuetes mainitud on vajalik seadme töövõime pingetel vahemikus 5–12V, siis on mõttekas isegi võtta 4000 seeria loogika, kuna see töötab reeglina vahemikus 3–15V. 74

seeria loogika puhul peaks lisama veel ühe lisakomponendi – stabilisaatori – et oleks võimalik töötada kõrgematel toitepingetel kui 5V. 4000 seeria taimer–loenduritest on ainult kaks mikroskeemi mis võiksid sobida – esimene on 4526 ja teine 4536. Võimalustelt on nad mõlemad peaaegu samad, välja arvatud see, et 4536 mikroskeemil on väljundosas võimalik kasutada monovibraatorit, muidu on mõlemad mikroskeemid samade omadustega. Seega ongi ainukene taimer valik 4536, kuna monovibraator võimaldab lülitada väljundi mõneks ajaks sisse, millega saab formeerida piisava reseti impulsi pikkuse.

Järgneval joonisel on äratoodud 4536 mikroskeemi põhimõtteskeem:

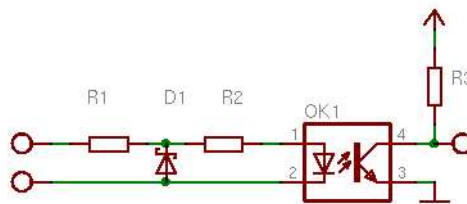


Joonis 10: 4536 põhimõtteskeem

Nagu skeemilt näha on saab seada sisenditega A, B, C, D dekodeeri jagamis väärtust, tänu millele on võimalik näiteks lihtsa pöördlülitiga seada valvekoera perioodi. Vajaliku perioodi nullimist saab teha läbi reset–sisendi, reseti aktiveerimiseks on vaja maksimaalselt mõne millisekundi pikkust impulssi reset–sisendil. Et ei peaks kasutama väga suurte väärtustega kondensaatoreid ja takisteid, vajaliku ajabaasi saamiseks tuleb kindlasti ka sisse lülitada esimesed kaheksa jagaja järku, selleks tuleb 8 BYPASS ühendada loogilise nulliga.

7.2. Sisendaste

Välise madalpinge impulsside jaoks mõeldud optronsisend on valvekoera üks kõige kriitilisemaid kohti, kuna on võimalik, et just see sisend ühendatakse mingisuguse väga suure pingega lülituse külge või on suured häired sellel sisendil. Kuid enamuses jaolt peaks rahuldama järgnev sisendaste:



Joonis 11: Optron sisendaste

Kui võtta R_1 ja R_2 väärtusteks $150\ \Omega$ ja supressori D_1 stabiliseerimispingeks $U_{br} = 7,5V$, supressor on SMB korpuses ja takistid on 1206 suurused ning võimsusega $0,25W$, siis saame järgnevad pingetaluvused.

Maksimaalne pidev päripinge sisendis:

$$U_{sis} = \sqrt{P R_1} + U_{br} = \sqrt{0,250 \cdot 150} + 7,50 = 13,6V$$

Maksimaalne pidev vastupinge sisendis:

$$U_{sis_{vastu}} = \sqrt{P R_1} + U_{supr_f} = \sqrt{0,250 \cdot 150} + 1,50 = 7,62V$$

Kus: U_{supr_f} - Supressori päripinge, $1,5V$

Maksimaalne päripinge sisendis, lähtudes takistite võimsusest ja katseimpulsi kestusest:

$$U_{sis_p} = \sqrt{\frac{P R_1}{T_{puls}}} + U_{br} = \sqrt{\frac{0,250 \cdot 150}{49,4 \cdot 10^{-6}}} + 7,50 = 879V$$

Kus: T_{puls} – katse impulsi pikkus, $49,4 \mu S$

Hetkel on enamustel 1206 mõõdus olevatel SMD takistitel maksimaalseks pingetaluvuseks näidatud 400V ja maksimaalsekt tööpingeks 200V [26]. On võimalik kasutada ka kõrgema pinget taluvusega takisteid, kuid neid on raskem kätte saada ja nad on kallimad. Seega ei garanteeritud et optronsisend kannataks üle 400V pinget.

Valvekoera välise nullimise sisendil on elektromagnetilise ühilduvuse tagamiseks vajalik, et kõik komponendid asuksid piisavalt kaugel teistest komponentidest, mis ei kannata suuri pingeid. Sisendi rajad on kõige lähemal üksteisele kas supressori juures, või siis optroni sisendil, mõlemal juhul on radade vahed vähemalt 2 millimeetrit, mis lubab sisendisse anda vähemalt 1500V lühiajalise pingehüppe [27]. Lisaks tuleb sisendkomponendid paigutada ülejäänud komponentidest võimalikult kaugemale, arvestades sellega et optronsisendit ei ole eriti võimalik paigutada korpusest eriti kaugemale, maksimaalne kaugus sisendi ja korpuse vahel on umbes 5 millimeetrit. Seega on vaja, et optroni sisendpoole komponendid oleksid ülejäänud komponentidest ka vähemalt 5 millimeetri kaugusel.

USB jaoks sisendi tegemine on seevastu tunduvalt lihtsam – võime lähtuda sellest, et valvekoer asub arvuti sees ja kaablid on lühikesed, alla ühe meetri. Väikest ESD lisakaitset annab ka USB kontrolleri sisene kaitse, näiteks FT232BM USB kontrollerial on sisene 3000V ESD taluvus [28]. Selliste eelduste puhul pole praktiliselt vaja erilisi kaitsmeid sisenditele, kuid sisendis võiks olla mõningane häirefilter mis koosneks ühest RC lülist.

Kuna valvekoera taimer-loenduri nullimiseks on vaja ainult impulssi, siis saab ühendada sisendid läbi kondensaatori mikroskeemi resetiga, mis välistab võimaluse, et nullimise impulsside lõppemine ja signaali konstandina paigale jäämine ei põhjusta valvekoera pidevat resetis olekut. Lisaks võimaldab selline ühendusviis ühendada küllaltki palju erinevaid nullimiseks mõeldud välisliideseid taimer-loenduriga.

7.3. Väljundaste

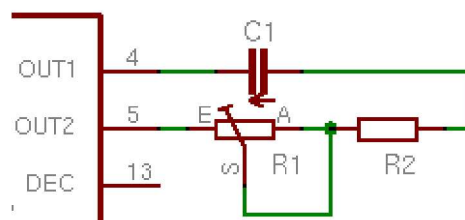
Nõuete järgi peab väljundis olema kaks ümberlülitatavat kontakti. Ümberlülitatava kontaktide jaoks kõige lihtsam lahendus on tavaline kontakt rele. Viimasel ajal on müügile tulnud küll igasuguseid pooljuht–releesid, aga neid ei ole mõtet kasutada selles süsteemis, kuna rele ümberlülitamine toimub eelduste kohaselt ülimalt harva, siis ei ole pooljuht releel küll mingi olulist eelist.

Kuna releele esitatavad nõuded ei ole eriti kõrged, siis võib kasutada praktiliselt igasugust standardse DIL korpuse jalasammuga releed. Eriti hästi sobivad oma väikeste mõõtmetega Omroni G5V ja G6H seeria releed.

7.4. Viite seadistamine

Tänu mikroskeemis 4536 sissehitatud generaatorile on vaja ainult ühte või kahte takistit ja ühte kondensaatorit, et saada mikroskeemi taimeri osa tööle. Kui panna mikroskeemi sisemise generaatori sageduseks 128 Hz ja lülitada kaheksaga jagamise lüli vahele, siis on vastavalt seadistuse viikude ühendamisele võimalik väljundisse saada impulsi, mille periood on kahe astme kordne. Väljundperioodi kordajad saavad olla kahe astmed kuni astmeni 16, mis võimaldab valida väljundimpulsi pikkust vahemikus 2 sekundit kuni 18,2 tundi.

Mikroskeemi 4536 sisemise generaatori kasutamiseks on vaja ühendada generaatori viikudele järgnev väline RC lüli:



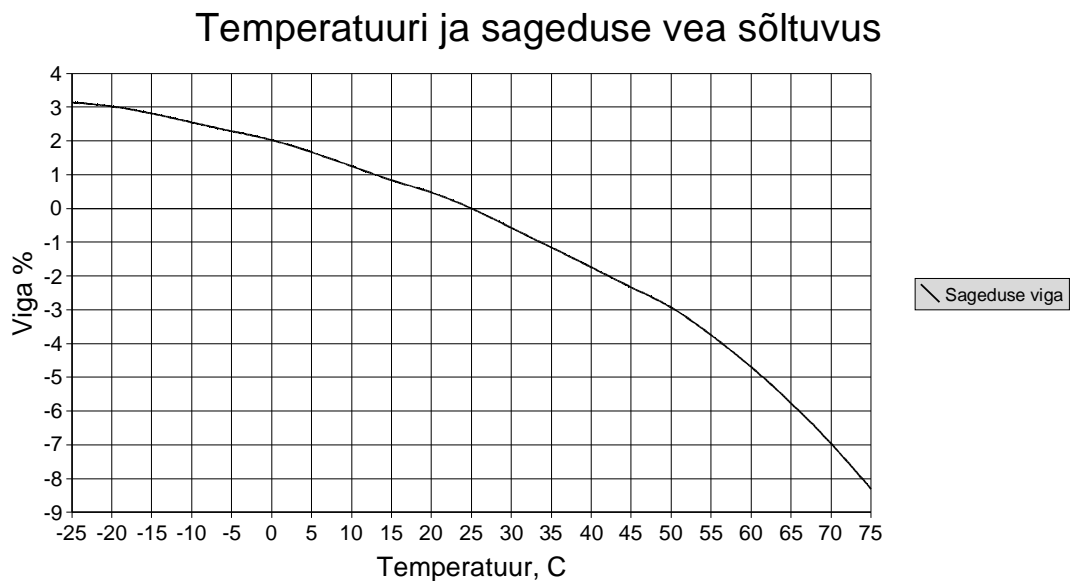
Joonis 12: 4536 mikroskeemi RC generaatori väline osa

Kus häälestamiseks tootmisel on takisti R_1 .

Sellise RC generaatoriga skeemi ajaline stabiilsus sõltub peamiselt takistite ja kondensaatori temperatuuri triivist. Tüüpilise trimmer takisti takistus muutub vahemikus $-25^{\circ}C \dots +70^{\circ}C$ $300 \text{ ppm}/^{\circ}C$, tavalise SMD takisti takistus $100 \text{ ppm}/^{\circ}C$ ja X7R dielektrikuga kondensaatori mahtuvuse muutus on $+3\% \dots -7\%$, sealjuures kondensaatori mahtuvuse muutus ei ole lineaarne. Et saada 128 Hz sagedust peab valima kondensaatori C_1 suuruseks 220 nF , takisti R_1 suuruseks $12 \text{ k}\Omega$ ja takisti R_2 suuruseks $4,7 \text{ k}\Omega$. RC generaatori sageduse leidmiseks on tootja andnud 4536 spetsifikatsioonis [29] järgneva valemi:

$$f \approx \frac{1}{2,3 \cdot R \cdot C}$$

Mille järgi tuleb sageduse veaks üle kogu temperatuuri $+3,14\% \dots -8,31\%$. Järgneval joonisel on äratoodud sageduse vea sõltuvus temperatuurist:



Joonis 13: Sageduse vea ja temperatuuri sõltuvus

Tabelis 3 on erinevate valvekoera perioodide pikkuste sõltuvused temperatuurist.

	-20	-10	0	10	20	30	40	50	60	70
2	2,062	2,052	2,052	2,041	2,025	2,009	1,966	1,943	1,910	1,870
4	4,125	4,105	4,105	4,083	4,051	4,019	3,932	3,886	3,821	3,740
8	8,249	8,209	8,209	8,166	8,102	8,038	7,863	7,772	7,641	7,479
16	16,50	16,42	16,42	16,33	16,20	16,08	15,73	15,54	15,28	14,96
32	33,00	32,84	32,84	32,66	32,41	32,15	31,45	31,09	30,57	29,92
64	66,00	65,68	65,68	65,32	64,81	64,30	62,90	62,18	61,13	59,83
128	132,0	131,4	130,6	129,6	128,6	127,3	125,8	124,4	122,3	119,7
256	264,0	262,7	261,3	259,3	257,2	254,5	251,6	248,7	244,5	239,3
512	528,0	525,4	522,6	518,5	514,4	509,1	503,2	497,4	489,0	478,7
1024	1056	1051	1045	1037	1029	1018	1007	994,8	978,1	957,3

Tabel 3: Valvekoera perioodi (2^N) ja temperatuuri sõltuvus

7.5. Töökindlus

Kuna hetkel pole tehtud EMC ja EMI mõõtmisi valvekoeraga, siis hetkel saab ainult ennustada EMI ja EMC tulemusi. Praeguse komponentide baasi puhul ei ole ette näha eriti suurt elektromagnet häirete kiirgust valvekoerast. Skeemis on kaks võimalikku pidevalt kiirgavat komponenti. Millest esimene, taimer–loendur käib 128 Hz sagedusega ja kõik välised generaatori komponendid on küllaltki ligidal mikroskeemile, seetõttu ei tohiks taimer–loendur eriti palju häireid kiirata. Teine potentsiaalselt kiirgav komponent on USB kontrolleri sees on 48 MHz sagedusega PLL, kuid kõik kõrge sagedusega sõlmed asuvad selle kontrolleri sees, lisaks on olnud kõik USB kontrolleriid ka SMD komponendid, millel ei ole pikki kiirgavaid väljaviike. Seega ei tohiks olla eriti suurt välist kiirgust USB kontrolleriist. Ka immuunsusega ei ole ennustatavaid probleeme ette näha, sest enamuse takisteid on valitud küllaltki madala takistusega ja üldiselt on skeemis olevad voolud piisavalt suured, mis peaks küllaltki palju immuunsust juurde andma. Lisaks suhteliselt väikestele takistustele ei ole skeemis väga kiirelt toimivaid lülisid. Võttes arvesse kõiki neid eeldusi, ei tohiks sellel valvekoeral olla probleeme töötamiseks arvuti lisakomponendina.

MTBF väärtuse leidmiseks on kõige lihtsam kasutada komponentide statistilisi FIT väärtusi (tõrkeid/ajavahemikus, antud miljardi tunni kohta). Kuna kõikidele komponentidele tootjad FIT väärtust ei avalda, siis on järgnevas tabelis üks FIT väärtus vabalt valitud ja hõlmab kõiki ülejäänud komponente. Arvutustest on välja jäätud relee FIT väärtus; kuna relee puhul sõltub tema eluiga lülituste arvust, pingest ja voolust, siis normaalolukordades ei saavutata kunagi nii suuri väärtusi, mis oleksid piiride lähedal. Näitena võib tuua relee G5A [30] ja G6H [31] lülituste arvu, mis on 10^8 lülitust. Tabelis olevad väärtused kehtivad juhul kui seadet kasutatakse $25^{\circ}C$ juures ja ei ületata lubatud pingeid.

<i>Komponent</i>	<i>Kogus</i>	<i>FIT</i>
Mikroskeem 4536	1	3,75
USB kontrollier	1	224,3
Bipolaar transistor	4	4,1
SMD takisti	25	6,39
SMD kondensaator, X7R dielektrikuga	12	2,135
Ülejäänud komponendid	1	50

Tabel 4: Valvekoera kõikide komponentide FIT tabel

Eelneva tabeli järgi saab leida valvekoera MTBF väärtuse tundides:

$$MTBF = \frac{10^9}{\sum FIT} = \frac{10^9}{479,82} = 2,08 \cdot 10^6$$

Saadud MTBF väärtus on aastates on 237,9 aastat, mis on tunduvalt rohkem kui ülesandes oli nõutud.

Arvestades asjaolu, et nii kondensaatoritel kuid ka takistitel sõltub enamusjaolt MTBF nendele rakendatud pingetest ja vooludest, siis juhul, kui valida kõik komponendid selliselt, et nende maksimumväärtusteks märgitud pingetest jääksid reaalselt rakendatavatest pingetest ja voolud vähemalt kümme korda madalamaks, siis võib neid komponente mitte arvestada. Järgnev tabel ongi tehtud eeldusel, et kõikidele takistitele ja kondensaatoritele rakendatakse tunduvalt madalamaid väärtusi kui on nende maksimaalsed väärtused.

<i>Komponent</i>	<i>Kogus</i>	<i>FIT</i>
Mikroskeem 4536	1	3,75
USB kontrolleri	1	224,3
Bipolaar transistor	4	4,1

Tabel 5: Valvekoera pooljuhtkomponentide FIT tabel

Tabeli 5 MTBF väärtuseks on $4,09 \cdot 10^6$ tundi, ehk 467,0 aastat.

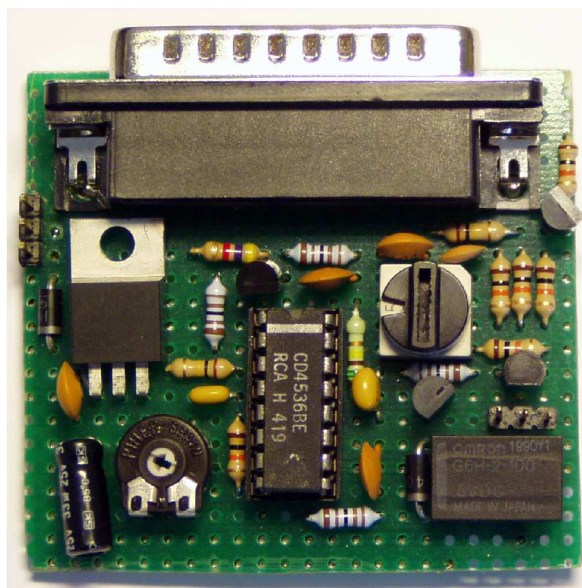
Eelnevates tabelites toodud FIT väärtused kehtivad ainult siis kui tegemist on väga korraliku montaažiga, ehk komponendid pole montaaži käigus saanud staatilist elektrit. Väikeste partiide puhul, mille tootmine toimub täielikult käsitsi on staatilise elektri tõenäosus suhteliselt suur, seda isegi küllaltki heades tingimustes. Seega võib realselt olla MTBF näitaja tunduvalt madalam, võibolla isegi üks suurusjärk.

Eeldatav eluiga valvekoeral jääb tõenäoliselt vahemikku 7 kuni 15 aastat. Kuna realselt pole veel ühtegi sellist valvekoera toodetud, siis puuduvad statistilised andmed ning eluiga saab ainult ennustada. Eluea puhul mängib suurt rolli viimastel aastatel juurutatud RoHS nõue, kuna väikeste koguste puhul, kui komponendid joodetakse käsitsi peale on käsitsi jootmine RoHS nõude järgi küllaltki täpsust ja hoolt nõudev – ilma pliita tina ei voola nii hästi kui tina mis sisaldab pliid. Peale RoHS nõude määrab eluea ka kogu jootmise protsessi pikkus, enamusel komponentidel on kõige suurem eluea lühendaja just jootmine. Kui eeldada, et jootmine on tehtud piisavalt kvaliteetselt, siis tuginedes eelnevale kogemusele 4000 mikroskeemide puhul, USB kontrolleri, transistorite, kondensaatorite ja takistite puhul võib eeldatavaks elueaks pakkuda kuni 7 – 15 aastat. Eluea arvestuse puhul ei ole mõtet arvestada relee elueaga, kuna kõik relee testid on tehtud lülitamistega, aga kui relee lülitamisi on aastas mõned üksikud, siis on sellise relee eluiga väga pikk. Tuginedes eeldatavale elueale võib selle toote garantiiajaks pakkuda 3 kuni 5 aastat.

Võimalike tõrgete analüüsil on kasutatud FMECA meetodeid. FMECA tabel on ära toodud käesoleva töö lisan.

7.6. Lahenduse põhiahela katsetused prototüübi abil

Esialgselt loodud prototüüp oli ilma USB liideseta, ainukeseks ühendusvõimaluseks oli paralleelpordi ühendus, mis ei oma tulevikus perspektiivi (eeldatavasti kaob arvutitelt). Kuna esimeses versioonis ei olnud USB liidest kust oleks toite saanud, siis tuli toide eraldi võtta arvuti emaplaadilt. Järgneval pildil on prototüüp.



Joonis 14: Valvekoera prototüüp

Prototüübi elektrilised ja mehaanilised parameetrid olid järgnevad:

1. Valvesolekuvool: 5,6 mA
2. Rakendusvool: 22 mA
3. Reseti pulsi kestvus: 380 ms
4. Mehaanilised mõõtmed ; 4,5 mm x 5,5 mm

Prototüübi katsetamiseks oli tehtud tarkvararakendus graafilises programmeerimiskeskkonnas LabVIEW, mis mõõtis kahe lülituse vahelist perioodi täpsust, katse ise kestis 72 tundi. Valvekoera perioodiks oli pandud 64 sekundit, realselt koos reset-impulsiga oli perioodi keskmine pikkus 64,2050 s, minimaalne perioodi pikkus oli 63,8816 s, maksimaalne pikkus 65,2638. Protsentuaalselt oli minimaalne viga -0,5059% ja maksimaalne viga 1,622%. Realselt võib olla maksimaalne vea protsent umbes kaks korda

väiksem, kuna andmete salvestamine toimus läbi Windows PC arvuti, kus vahepeal kindlasti käisid mõningad perioodilised toimingud.

Järgneval katseperioodil testsüsteemis, mis kestis kaks kuud, ei tulnud ette ühtegi valvekoera prototüübi tõrget. Perioodi jooksul tekitati seitse katsearvuti kokkujooksmist, mille puhul valvekoer tegi arvutile iga kord edukalt taaskäivituse. Kuna enamus kokkujooksmisi (viis kokkujooksmist) toimusid õhtuti pärast tööpäeva lõppu, ka reedel, siis võib tõdeda, et valvekoerast oli küllaltki palju abi.

Arvutuslikult võinud esineda vähemalt 70 tundi katkestust arvuti töös, seega käideldavus oleks ilma valvekoerata olnud järgmine:

$$A = \frac{1370,0}{1440,0} = 0,95139$$

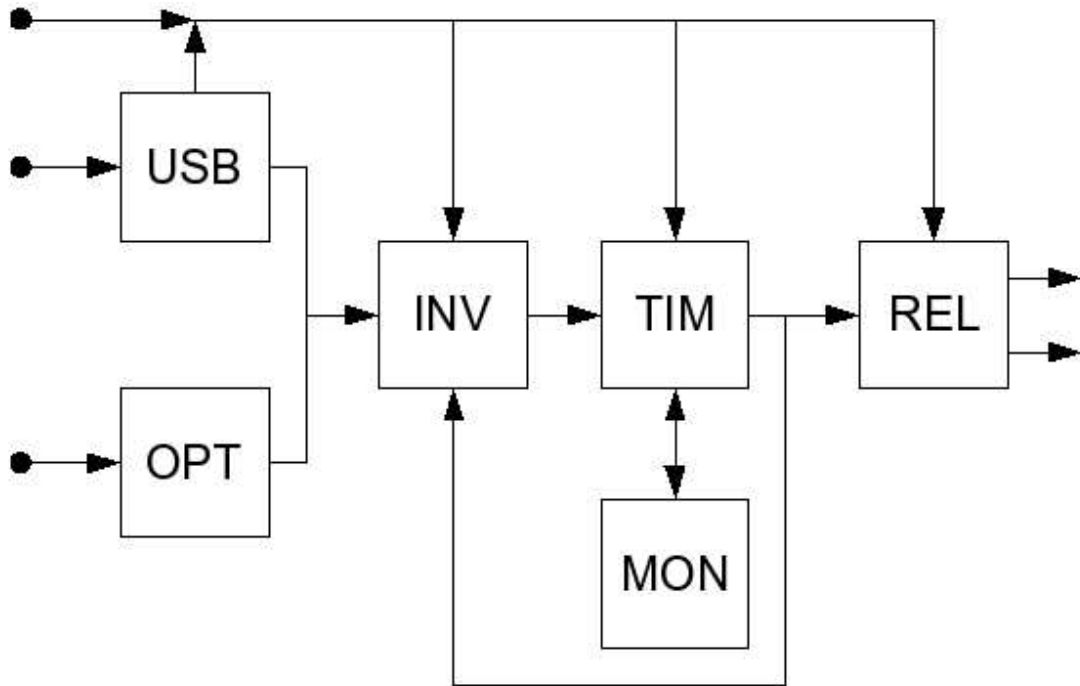
Kuid arvestades, et valvekoera veatuvastamise aeg on 64 sekundit ja arvuti taaskäivitamise aeg on umbes 55 sekundit, mis seitsme korra kohta kokku teeb umbes 14 minutit, siis on käideldavus vaadeldud perioodi jooksul järgmine:

$$A = \frac{1439,8}{1440,0} = 0,99984$$

Ilma valvekoerata ja valvekoeraga süsteemide käideldavuste erinevus on seega 300 korda.

7.7. Lõpliku valvekoera põhimõtteline lahendus

Lõplikus valvekoera lahenduses puudub võimalus valvekoera arvutiga paralleelpordi kaudu ühendamiseks, selle asemel on ette nähtud valvekoera ühendamine arvutiga USB järjestikliidese kaudu, lisaks on jäetud võimalus ka välise madalpingesignaaliga valvekoera nullida. Järgneval joonisel on toodud valvekoera plokk-skeem.



Joonis 15: Valvekoera lõplik põhimõtteskeem

Plokkide tähistuste tähendused: USB – USB liidese kontrolleri, OPT – optrosisend, INV – sisendimpulsi inverter ja ajalise pikkuse formeeriija, TIM – taimer–loendur, MON – taimeri monovibraatori impulsi pikendaja, REL – väljundrelee.

Valvekoera lõplikus ehk tootmis versioonis on kogu valvekoera trükiplaat ja montaaž tehtud nii et oleks seadet võimalik paigutada arvuti korpusesse olevasse vabasse lisakaardi pesse, ning on välja toodud välise madalpinge signaali sisend. Lisaks on veel lõplikus versioonis võimalik kasutada Berkshire poolt toodetud valvekoera Linuxi kerneli moodulit ja võimalik, et ka Windowsi drivereid.

8. Kokkuvõte

Käesoleva töö eesmärgiks oli uurida arvutisüsteemi töökindlusega seotud tegureid ja leida sobiv lahendus kaugseiresüsteemi serverkomponendi kõrgendatud töökindluse tagamiseks. Töö kajastab ainult ühte konkreetset osa autori poolt Cybernetica AS töökindla kaugseiresüsteemi arendusmeeskonna koosseisus aastatel 2007 ja 2008 tehtud töödest – originaalse riistvaralise valvekoeramooduli arendust vastavuses nõuetega töökindlatele elektronsüsteemidele.

Töö tulemusena tuvastati, et kõige paremaid tulemusi serverkomponendi töökindluse tõstmiseks annab valvekoera kasutamine, kuid valvekoer ise peab olema töökindlam kui seda on jälgitav süsteem. Valvekoeraga süsteemi võrdlusest valvekoerata süsteemiga tuleb välja, et valvekoer võib suurendada süsteemi käideldavust mitu suurusjärku, kusjuures lisaks käideldavuse suurendamisele vähendab valvekoera kasutamine ka tööjõu kulusid süsteemi teenindava hoolduspersonalilt. Valvekoera kasutamisega ei ole siiski võimalik vähendada süsteemi tõrketõenäosust.

Kaubanduslike riulitoodetena olevad valvekoerad on kõik kas sobimatu liidesega või liiga keeruka ühendusviisiga ja madala töökindlusega, sobiliku valvekoera saamiseks on ainukeseks võimaluseks valmistada valvekoer. Kõige töökindlam variant valvekoera valmistamiseks on kasutada võimalikult palju riistvaralisi lahendusi ja hoiduda programmeeritavate süsteemide kasutamisest. Etteantud nõuete järgi sai valmistatud töötav prototüüp, mis oma kahekuise katseperioodi jooksul toimis täielikult veavabalt, suurendades tunduvalt süsteemi käideldavust. Tehtud töökindlusarvutuste järgi on omavalmistatud valvekoer neli kuni kaheksa korda töökindlam kui seda on teiste tootjate riulitooted.

Töös kirjeldatud originaalse valvekoera arendus on praktiliselt lõpetatud, ees seisavad juba käivitatud tootepartii katsetused.

9. Kasutatud kirjandus ja Interneti lingid

- [1]: IEC, IEC 61508, Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 1: General requirements, 2003
- [2]: IEC, IEC 61508, Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 4: Definitions and abbreviations, 2007
- [3]: Wikipedia, Failure rate, URL:http://en.wikipedia.org/wiki/Failure_rate, 2008
- [4]: Department Of Defense, Washington, DC 20301, MIL-STD-721C: Definitions Of Terms For Reliability And Maintainability, 1981
- [5]: Wikipedia, Failure Mode, Effects, and Criticality Analysis, URL:http://en.wikipedia.org/wiki/Failure_Mode,_Effects,_and_Criticality_Analysis, 2008
- [6]: Marvin Rausand, System Analysis: Failure Modes, Effects, and Criticality Analysis, URL:<http://www.fmeainfocentre.com/presentations/fmeca.pdf>, 2005
- [7]: Wikipedia, Industry Standard Architecture, URL:http://en.wikipedia.org/wiki/Industry_Standard_Architecture, 2008
- [8]: EVS, EVS-EN 50129:2005, Raudteealased rakendused. Side-, signalisatsioon- ja andmetöötlussüsteemid. Ohutust tagavad elektroonikasüsteemid signalisatsiooniks, 2005
- [9]: Wikipedia, Mission, URL:<http://en.wikipedia.org/wiki/Mission>, 2008
- [10]: Wikipedia, Mission critical, URL:http://en.wikipedia.org/wiki/Mission_critical, 2008
- [11]: Wikipedia, Peripheral Component Interconnect, URL:http://en.wikipedia.org/wiki/Peripheral_Component_Interconnect, 2008
- [12]: National Weights & Measure Laboratory (NWML) , RoHS, URL:<http://www.rohs.gov.uk/>, 2007
- [13]: Wikipedia, Universal Serial Bus, URL:<http://en.wikipedia.org/wiki/USB>, 2008
- [14]: IEC, IEC 61508, Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 2: Requirements for E/E/PE safety-related systems, 2003
- [15]: CSE International Limited, Preliminary assessment of Linux for safety related systems, 2002
- [16]: Wikipedia, Electromigration, URL:<http://en.wikipedia.org/wiki/Electromigration>, 2008
- [17]: Dr. Danny Rittman, Nanometer Reliability, 2005
- [18]: IEC, IEC 61508, Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 3: Software requirements, 2003
- [19]: Splint, Splint - Secure Programming Lint, URL:<http://www.splint.org/>, 2008

- [20]: Prof. J. L. Lions, ARIANE 5 Flight 501 Failure,
URL:<http://sunnyday.mit.edu/accidents/Ariane5accidentreport.html>, 1996
- [21]: Wikipedia, Aircraft flight control systems,
URL:http://en.wikipedia.org/wiki/Aircraft_flight_control_systems, 2008
- [22]: IEC, IEC 61508, Functional safety of E/E/PE safety-related systems –Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3, 2003
- [23]: QUANCOM Informationssysteme GmbH, PC Watchdog, URL:http://www.pc-watchdog.de/quancom/html.nsf/pages/pc_watchdog.html, 2007
- [24]: Berkshire Products, Inc., USB PC Watchdog,
URL:http://www.berkprod.com/usb_pc_watchdog.htm, 2007
- [25]: Ian Sommerville, The Ariane 5 Launcher Failure, URL:<http://www.cs.st-andrews.ac.uk/~ifs/Resources/CaseStudies/Ariane5/Ariane5failure.pdf>, 2004
- [26]: Panasonic, Datasheet: Thick Film Chip Resistors, 2007
- [27]: Homi Ahmadi, Calculating Creepage and Clearance Early Avoids Design Problems Later, URL:<http://www.ce-mag.com/ce-mag.com/archive/01/03/ProductSafety.html>, 2003
- [28]: Future Technology Devices Intl. Ltd, FT232BM USB UART (USB - Serial) I.C. , 2005
- [29]: Motorola, MC14536B datasheet, 1995
- [30]: Omron, G5V-1 PCB Relay,
URL:http://www.omron.com/ecb/products/pry/111/g5v_1.html, 2008
- [31]: Omron, G6H PCB Relay, URL:<http://www.omron.com/ecb/products/pry/111/g6h.html>, 2008

10. Lisa

10.1. Tõrkemäära tabel

Tõrkemäär	Kirjeldus	
1-2	Väga ebatõenäoline (very unlikely)	Ükskord 1000 aasta jooksul.
3-4	Kauge (remote)	Ükskord 100 aasta jooksul.
5-6	Juhuslik (ocasional)	Ükskord 10 aasta jooksul.
7-8	Tuntav (probable)	Ükskord aasta jooksul.
9-10	Tihe (Frequent)	Ükskord kuus või tihedamini.

10.2. Tõrketõsiduse tabel 1

Tõrketõsidus	Tõrke tõsiduse klass	Kirjeldus
10	Katastroofiline (Catastrophic)	Tõrke põhjustab personaalile tõsiseid vigastusi või surma.
7-9	Kriitiline (Critical)	Tõrge põhjustab personalile väiksemaid vigastusi või personali kokkupuutumist ohtlike kemikaalide või radioaktiivsete ainetega või põhjustab tulekahju või laseb ohtlikud keemilised ühendid keskkonda.
4-6	Oluline (Major)	Tõrge põhjustab personalile väiksema kokkupuute ohtlike ainetega või aktiveerib asutuse alarmsüsteemi.
1-3	Väike (Minor)	Tõrge põhjustab väiksema süsteemi kahjustuse, aga ei põhjusta personalile vigastusi, ei põhjusta kokkupuudet ohtlike ainetega, ei võimalda kemikaalidel keskkonda sattumist.

10.3. Tõrketõsiduse tabel 2

Tõrke tõsidus	Kirjeldus
10	Tõrge põhjustab kliendil suuremat sorti rahulolematuse ning põhjustab süsteemi toimise mittevastavalt ettenähtule või mittevastavalt valitsuse regulatsioonidega määratule.
8-9	Tõrge põhjustab kliendil suurema rahulolematuse ja põhjustab süsteemi mittetoimise.
6-7	Tõrge põhjustab kliendil väiksema rahulolematuse ja pahameele ning põhjustab süsteemi töökindluse vähenemist.
3-5	Tõrge põhjustab kliendil väiksemat pahameelt ja/või süsteemi töökindluse vähenemist.
1-2	Tõrge on piisavalt väike, tõenäoliselt jääb kliendil märkamata.

10.4. Avastamismäära tabel

Avastamise määr	Kirjeldus
10	Väga väikene vea avastamis tõenäosus. Verifitseerimine või kontroll ei suuda leida seda viga.
8-9	Väikene tõenäosus, et viga leitakse. Verifitseerimine või kontroll tõenäoliselt ei leia seda viga.
5-7	Keskmine tõenäosus, et viga leitakse. Verifitseerimine või kontroll tõenäoliselt leiab vea.
3-4	Kõrge tõenäosus, et viga leitakse. Verifitseerimine või kontroll suure tõenäosusega leiab vea.
1-2	Väga kõrge tõenäosus, et viga leitakse. Verifitseerimine või kontroll peaaegu alati leiab vea.

10.5. Valvekoera FMECA tabel

Süsteemiosa kirjeldus			Tõrke kirjeldus			Tõrke mõjud		Tõrke- määr (O)	Tõrke tõsidus (S)	Avas- tamise määr (D)	RPN (OxSxD)
Nimi või number	Funktsioon	Töörežiim	Tõrke olemus	Tõrge	Tõrke avastamise meetod	Alam- süsteemile	Kogu süsteemile				
Valvekoer	Relee kontaktide ühendamine alglähestamise impulsi puudumisel	Rakendunud	Pidevalt rakendunud, olenemata impulsside olemasolust	Taimer-loenduri väljund pidevalt aktiivne	Arvuti ei käivitu	-	Kogu süsteem ei tööta	2	10	1	20
				Relee juht transistor lühises							
Relee kontaktid kokku jäänud											
Valvekoer	Relee kontaktide ühendamine alglähestamise impulsi puudumisel	Rakendunud	Rakendub iseenesest kui impulsid on sisendis	Arvuti ei saada määratud perioodi sees nullimis signaali	Arvuti taaskäivitub iseenesest	-	Süsteemi käideldavus on langenud ja tõrketõenäsus tõusnud	7	7	8	392
				Optronsisend on vigane							
				Optronsisendi puhul võib sisend impulss olla liiga lühiajaline							
				Võimalikud elektromagnet häired lähedalasuvatest seadmetest							

Süsteemiosa kirjeldus			Tõrke kirjeldus			Tõrke mõjud		Tõrke- määr (O)	Tõrke tõsidus (S)	Avas- tamise määr (D)	RPN (OxSxD)
Nimi või number	Funktsioon	Töörežiim	Tõrke olemus	Tõrge	Tõrke avastamise meetod	Alam- süsteemile	Kogu süsteemile				
		Mitterakendunud	Ei rakendu kui impulsid puuduvad	Valvekoera sisend USB kontroller vigane Taimer-loenduri väljund pidevalt mitteaktiivne Monovibraatori abilüli ei tühjenda kondensaatorit Relee juht transistor ei toimi Relee ei ühenda kontakte	Arvuti on vea tõttu kooku jooksnud, aga ei käivitu	-	Kogu süsteem tõenäoliselt ei tööta	3	10	1	30
			Ei rakendu iga kord	Monovibraatori abilüli ei tühjenda kondensaatorit	Arvuti on vea tõttu hangunud, kuid mõningase ajajooksul käivitub		Süsteemi töös pikem katkestus	5	5	9	225