Teollisuusautomaation standardit
Osio 6

Osio 1: SESKOn Komitea SK 65: Teollisuusprosessien ohjaus

Osio 2: Toiminnallinen turvallisuus: periaatteet

Osio 3: Toiminnallinen turvallisuus: standardisarja IEC 61508

Osio 4: Koneiden ohjausjärjestelmät: standardi IEC 62061

Osio 5: Riskin arviointi ja turvallisuuden eheyden tason SIL määrittäminen: standardit IEC 61508-5 ja IEC 62061

Osio 6: Koneiden ohjausjärjestelmien suunnittelutyökalu SISTEMA

Osio 7: Hätäpysäytys: standardit ISO 13850 ja IEC 60947-5-5

Osio 8: Turvaväylät ja niiden valinta: tekninen raportti IEC/TR 62513

Osio 9: Logiikat: standardi IEC 61131-1 ja 61131-3

Osio 10: Turvallisuuteen liittyvän elektroniikan asennus- ja muutostyöt

Koneiden ohjausjärjestelmien suunnittelutyökalu SISTEMA

Matti Sundquist
Sundcon Oy

Standardi EN ISO 13849-1

- Standardi SFS-EN ISO 13849-1 (korvaa standardin SFS-EN 954-1) on tarkoitettu helpottamaan koneiden ohjausjärjestelmien suunnittelua. Standardi kattaa kaikki erilaiset teknologiat.
- Standardi on tarkoitettu koneiden suunnittelijoille, automaation integraattoreille ja muille, jotka ovat mukana turvallisuuteen liittyvän ohjausjärjestelmän suunnittelussa, toteutuksessa ja ylläpidossa.

SISTEMA-ohjelmistotyökalu

- SISTEMA on Saksassa IFA:ssa (Institut für Arbeitsschutz Forschung, ent. BGIA) kehitetty tietokoneavusteinen suunnittelumenetelmä koneiden turvallisuuteen liittyvien ohjausjärjestelmien suunnitteluun.
- SISTEMA kattaa kaikilla eri teknologioilla toteutettavat koneiden ohjausjärjestelmät.
- **SISTEMA perustuu kaikilta osin standardiin SFS-EN ISO 13849-1.**

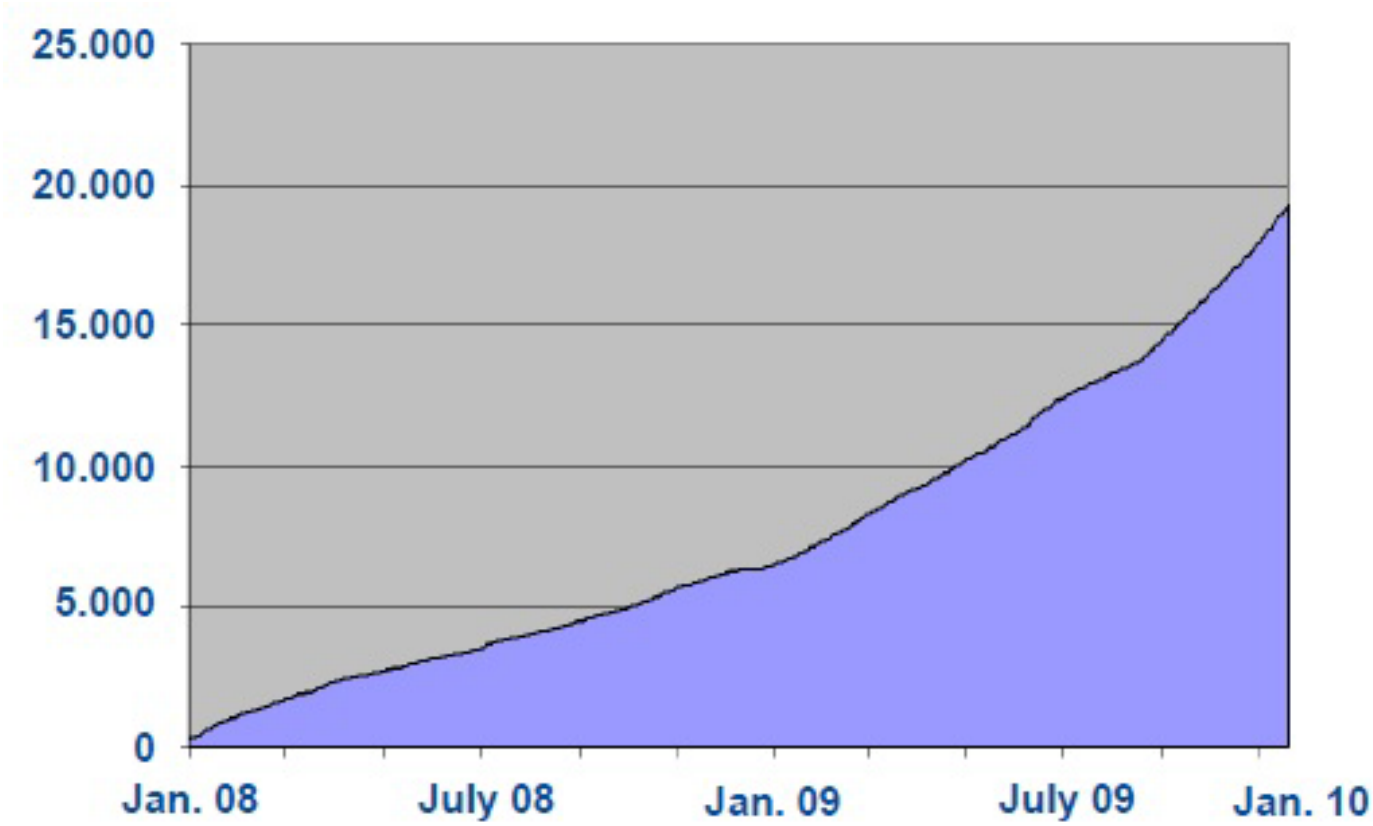
SISTEMAN suomenkielinen versio

- SISTEMA on vapaasti ladattavissa rekisteröitymällä IFA/SISTEMAn verkkosivuilla työkalun käyttäjäksi.
- Sistema on käännetty suomeksi työsuojelurahaston tuella ja kieliversion voi valita ja ladata IFA:n verkkosivulta.

SISTEMA-työkalun käyttö suunnittelussa

- SISTEMA-työkalun käytön edut:
  - voidaan välttää suunnitteluvirheitä, koska suunnittelu tehdään vaihe kerrallaan ja siten voidaan varmistaa vaatimusten täyttyminen
  - yhdenmukaisten käsitteiden käyttö vähentää väärinkäsityksiä ja karkeita virheitä
  - yhdenmukaisten menetelmien käyttö lisää eri ratkaisujen vertailukelpoisuutta
  - työkalun automaattisen laskennan avulla vältetään laskuvirheitä
  - dokumenttien laadinta helpottuu
  - vaatimustenmukaisuuden varmistaminen helpottuu niin asiakkaiden kuin viranomaistenkin suuntaan.

SISTEMA-ohjelmistotyökalun levinneisyys



Lähde: IFA

SISTEMAN toimintaperiaate

- SISTEMAn käyttö alkaa perustamalla projekti, jonka tarkoituksena on varmistaa, että kaikki koneen turvatoiminnot (Safety Function) täyttävät niitä koskevat vaatimukset.
- SISTEMAn avulla suunnitellaan ja tarkistetaan, että turvatoiminnot toteuttavat vaadittavan suoritustason laitteiden satunnaisvikaantumisten osalta.

SISTEMAN toimintaperiaate (jatkuu)

- SISTEMA ohjaa myös ottamaan huomioon systemaattiset vikaantumiset sekä ohjelmistovirheet.
- SISTEMAn päävaiheet perustuvat turvallisuuden elinkaaritarkasteluun.

SISTEMAn päävaiheet

A. Projektin luominen ja turvatoimintojen määritykset.
B. Riskin arviointi ja vaadittavan suoritustason PLr määrittäminen jokaiselle turvatoiminnolle.
C. Turvatoimintoa toteuttavan ohjausjärjestelmän suunnittelu ja toteuttaminen.
D. Saavutetun suoritustason PL vertaaminen vaadittavaan suoritustasoon.

A.1 Projekti

- SISTEMAn käyttö edellyttää, että koneelle on tehty riskin arviointi ja sen tulosten perusteella koneeseen on suunniteltu kaikki tarvittavat turvatoiminnot.
- SISTEMAn ”Projekti” sisältää kaikki koneen ohjausjärjestelmän toteuttamat turvatoiminnot, joiden vaatimukset ja todentaminen käsitellään jokainen erikseen.

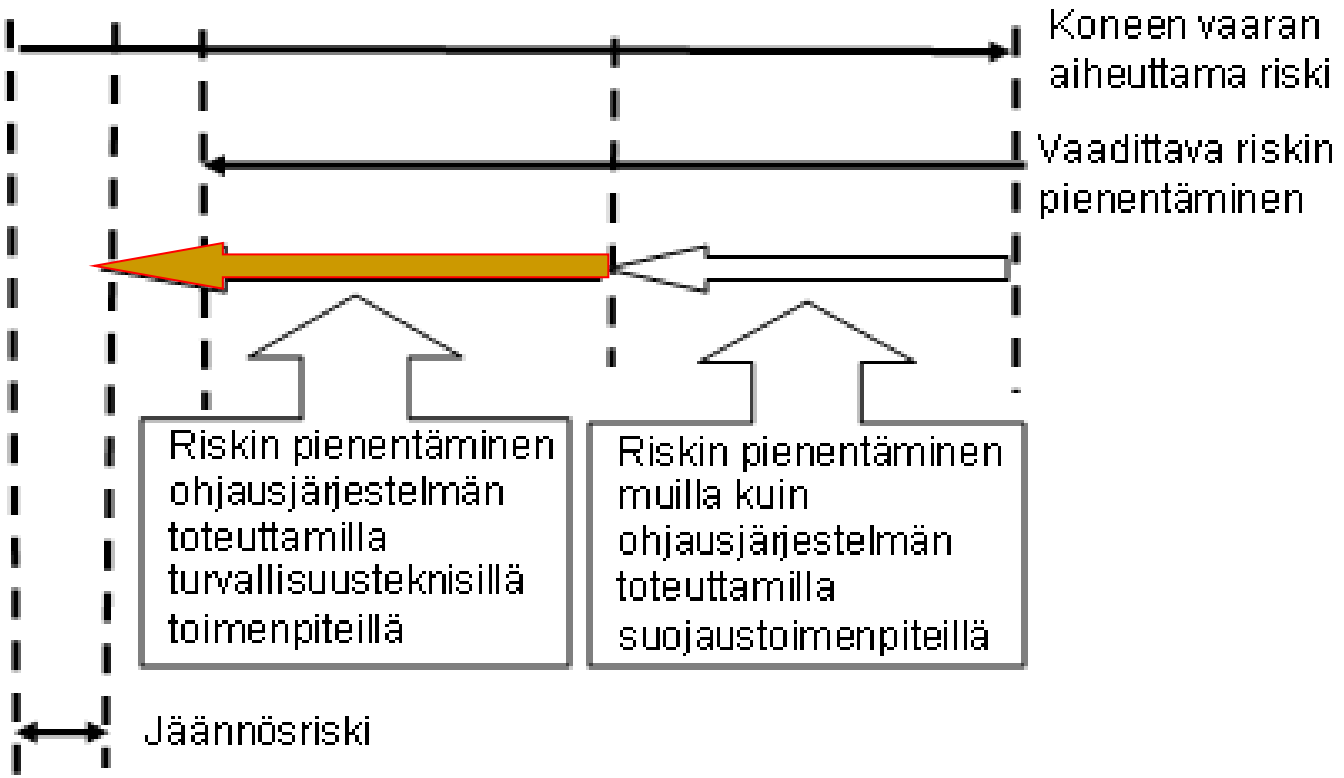
A.2 Turvatoimintojen erittely

- SISTEMA auttaa valitsemaan koneeseen sopivia turvatoimintoja, esim.:
  - suojuksen tai valosähköisen turvalaitteen toimintaankytkentä
  - portin sähköinen lukitus
  - hidastettu liikenopeus
- Turvatoimintojen kuvauksissa on osoitettava:
  - turvatoiminnon oikea toiminta
  - turvatoiminnon suoritustaso.

B.1 Riskin arviointi

- SISTEMAssa käytetään riskigraafia määrittämään jokaiselta turvatoiminnolta vaadittava osuus riskin pienentämisessä (väritetty nuoli seuraavassa kuvassa).
- Riskin arvioinnin tulosten perusteella asetetaan jokaiselle turvatoiminnolle vaadittava suoritustaso PLr (Performance Level/required, em. nuolen pituus on verrannollinen vaatimustasoon PLr).

B.1 Riskin arviointi



Standardi IEC 61508-5 kuva A.1, muunneltuna

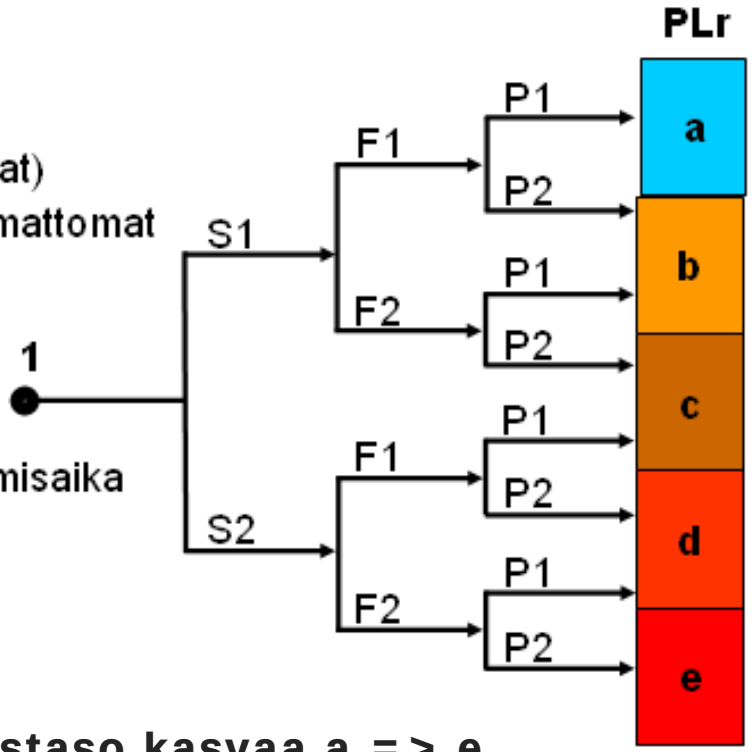
B.2 Riskigraafi

1 Lähtökohta tietyn turvatoiminnon osuudelle riskin pienentämisessä

S Seurausten vakavuus
S1 Pienet vahingot (tavallisesti palautuvat)
S2 Vakavat vahingot (tavalisesti palautumattomat tai kuolema)

F Taajuus ja/tai altistumisaika
F1 Harvoin ja/tai lyhyt altistumisaika
F2 Usein ja/tai jatkuvasti tai pitkä altistumisaika

P Mahdollisuus vaaran välttämiseen
P1 Mahdollista tietyissä olosuhteissa
P2 Tuskin mahdollista



PLr Vaatimustaso kasvaa a => e

Standardi ISO 13849-1 kuva A.1, muunneltuna

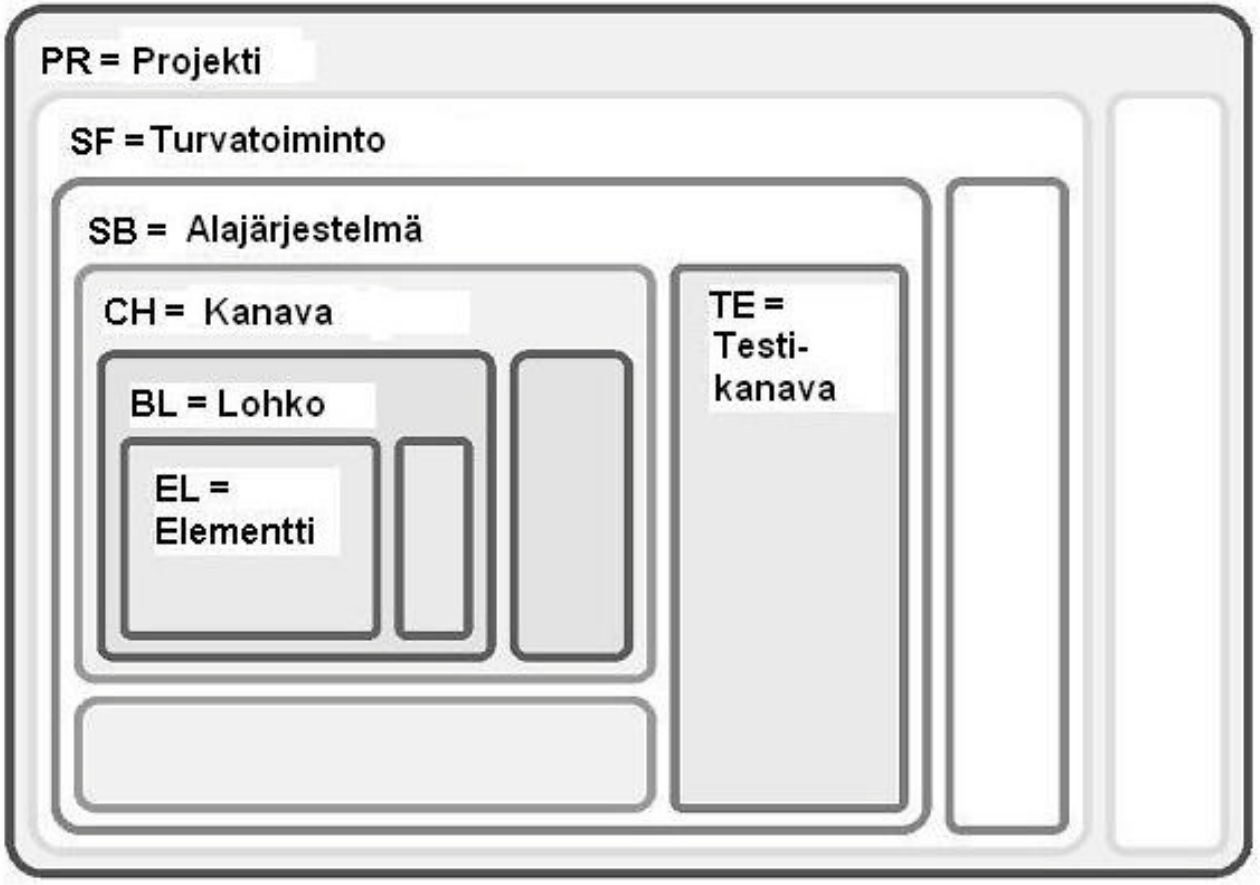
C. SISTEMAn työvaiheet turvatoiminnon suoritustason arvioinnissa

- C.1 Järjestetään turvatoiminnot niitä toteuttavan puurakenteen avulla kuvaamalla
  - turvatoiminto alajärjestelmien avulla
  - alajärjestelmät nimettyjen rakenteiden mukaisten kanavien ja testauskanavien avulla
  - kanavat lohkojen avulla
  - lohkot elementtien avulla.

C.1 SISTEMAN rakenne

- SISTEMAn hierarkkisen puurakenteen tasot:
  - projekti
  - turvatoiminto
  - alajärjestelmä
  - kanava ja testikanava
  - lohko
  - elementti.

C.1 SISTEMAn hierarkia



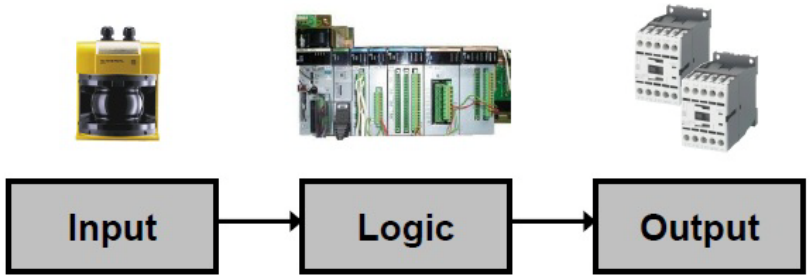
Lähde: IFA

C.1 Alajärjestelmät

- Turvallisuuteen liittyvä ohjausjärjestelmä suunnitellaan siten, että turvatoiminto toteutetaan sarjamuotoon yhdistetyillä alajärjestelmillä (osilla).
- Jokaiselle alajärjestelmälle valitaan jokin nimetyistä rakenteista (Cat. =Luokat: B, 1, 2, 3, 4).

C.1 Alajärjestelmät

- SISTEMA laskee jokaisen alajärjestelmän parametrit alajärjestelmän rakenteen muodostavien kanavien ja testauskanavien sekä siihen kuuluvien lohkojen ja/tai elementtien parametrien avulla.



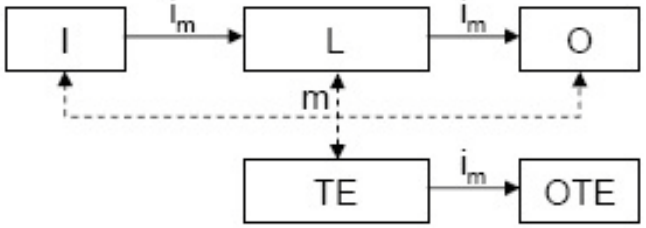
Usein valitaan kolme alajärjestelmää (tulot, logiikka, lähdöt)

Lähde: Siemens

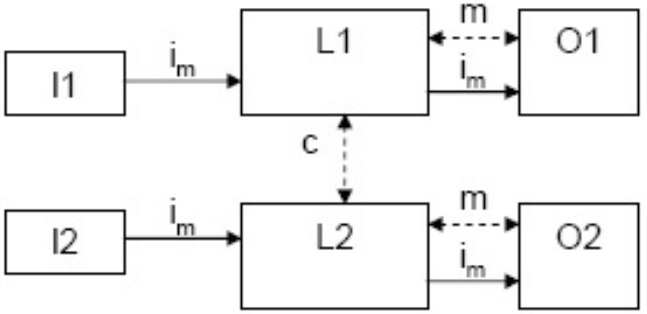
C.2.1 Nimetyt rakenteet, luokat, Cat.

Luokka B ja 1

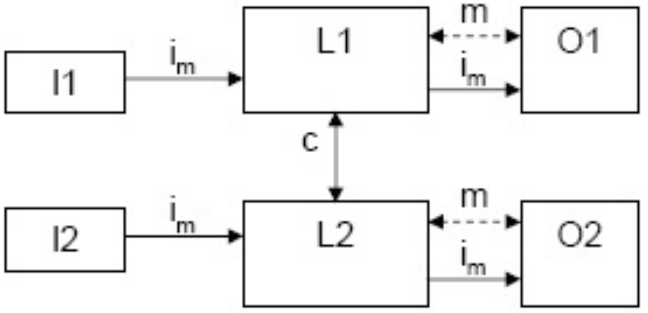
Luokka 2



Luokka 3



Luokka 4

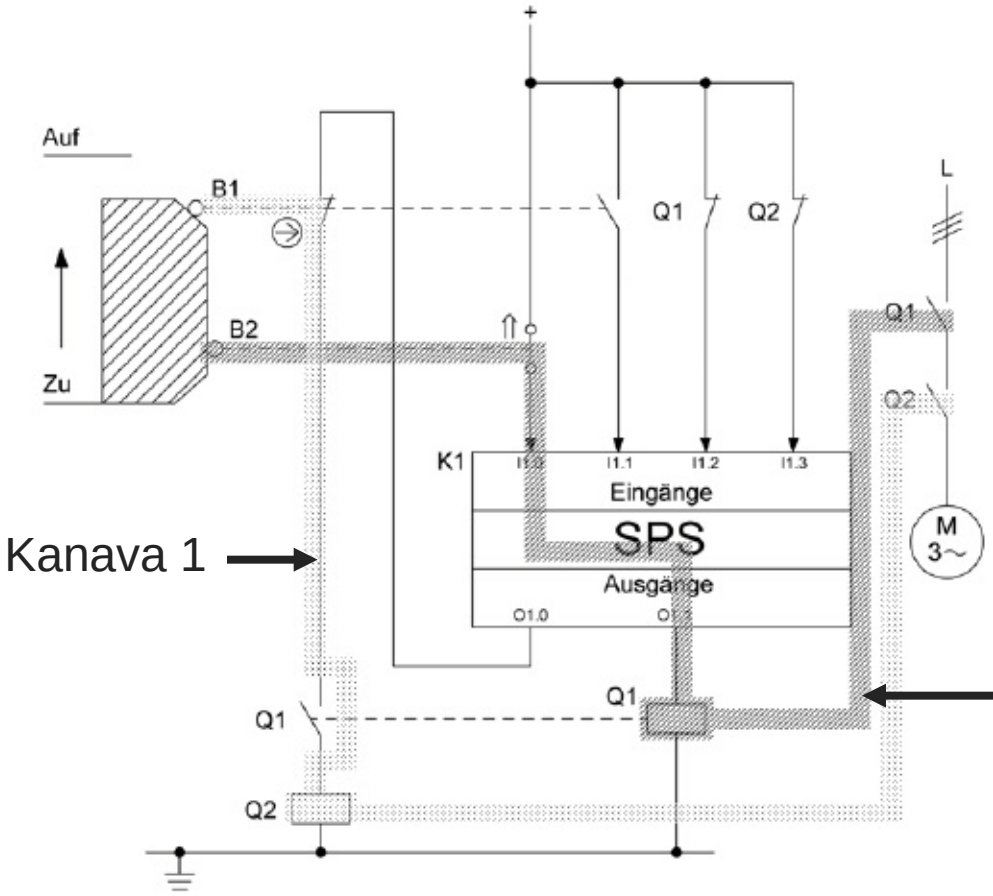


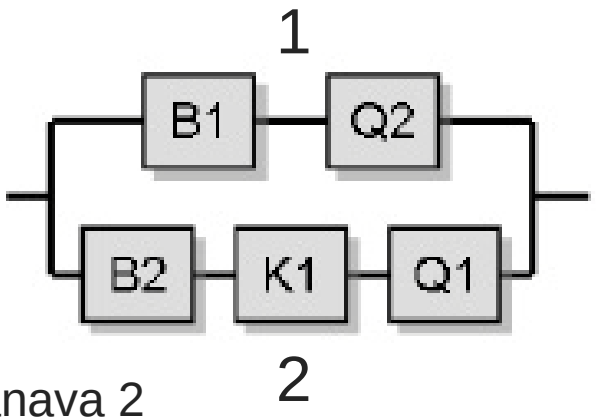
Merkintöjen selitykset

i_m = kytkentävälineet
I = tuloyksikkö (esim. anturi)
L = logiikka
O = lähtöyksikkö (esim. pääkontaktori)
m = valvonta
TE = testauslaitteisto
OTE = testauslaitteiston lähdöt
c = ristiinvalvonta

Standardi 13849-1 kuvat 9...12

C.2.1 Laitekaavio ja turvatoiminnon lohkokaavio





Lähde: IFA

C. SISTEMAn työvaiheet turvatoiminnon suoritustason arvioinnissa

C.2.1 Määritetään elementtien, lohkojen ja/tai kanavien keskimääräiset vaarallisten vikaantumisaikojen MTTFd-arvot

C.2.2 Määritetään elementtien, lohkojen ja/tai kanavien keskimääräiset diagnostiikan kattavuuden DCavg-arvot

C.2.3 Tarkistetaan yhteisvikaantuminen CCF (koskee vain rinnakkaisia kanavia)

C.2.4 Määritetään alajärjestelmien vaarallisen vikaantumisen todennäköisyydet PFH ja DCavg-arvot.

C.2.1
Komponenttien MTTFd-arvojen valinta

Komponenttitietojen ensisijaisuusjärjestys:

1. Käytetään valmistajan antamia tietoja. SISTEMAn kirjastossa on jo kymmenien laitevalmistajien toimittamia komponenttitietoja.
2. Käytetään julkisia tietokantoja, esim. Internetin avulla (standardissa ISO 13849-1 on liitteessä ”Kirjallisuus, Tietokantoja” viittauksia erilaisiin tietokantoihin).
3. Käytetään standardin liitteissä C esitettäviä karkeita likiarvoja.

C.2.1
Kanavien MTTFd-arvojen laskeminen

- Komponenttien MTTFd-arvot saadaan joko
  - syöttämällä tiedossa olevan kanavan MTTFd-arvo suoraan SISTEMAan tai
  - SISTEMA laskee kanavien MTTFd-arvot alemmilla tasoilla olevien lohkojen tai niiden elementtien avulla tai
  - käytetään vikojen poissulkemisen menetelmää, jossa tarkastelun ulkopuolelle suljetaan sellaiset vikaantumiset, joiden osoitetaan olevan niin epätodennäköisiä, että ne eivät vaikuta lopputulokseen.
- SISTEMA yhdistää automaattisesti rinnakkaisten kanavien MTTFd-arvot.

C.2.2 Diagnostiikan kattavuus

- Standardin SFS-ISO 13849-1 liitteessä E annetaan erilaisille diagnostiikkamentelmille suuntaa-antavia arvoja diagnostiikan kattavuudelle ja tämä esitetään myös aputaulukkona SISTEMAssa.
- Kanavien diagnostiikan kattavuudet DC annetaan joko suoraan tai SISTEMA laskee ne joko lohkojen tai lohkojen elementtien diagnostiikan kattavuuksien avulla ja sen jälkeen SISTEMA laskee koko alajärjestelmän diagnostiikan kattavuuden.

C.2.3 Yhteisvikaantumiset CCF

- Standardin SFS-ISO 13849-1 taulukko F.1 osoittaa toimenpiteet yhteisvikoja vastaan.
- Sen mukaan annetaan pisteet jokaiselle käytetylle menetelmälle.
- Tarkistetaan, onko yhteispistemäärä riittävä yhteisvikojen vähimmäisvaatimusten täyttämiseen.

C.2.3 Yhteisvikaantumiset CCF (jatkuu)

Luokissa 2,3 ja 4 yhteisvikojen vähimmäispistemäärä on 65.
Pisteiden maksimiarvo on 100:

Kriteerit	Pisteet
–Erottelu	15 p.
–Diversiteetti	20 p.
–Suunnittelu	15 p.
–Koetellut komponentit	5 p.
–FMEA	5 p.
–Ammattitaito	5 p.
–Ympäristöolosuhteet (EMC)	25 p.
–Muut	10 p.

FMEA = Failure Mode and Effect Analysis, Vika- ja vaikutusanalyysi

Standardi ISO 13849-1 taulukko F.1

SISTEMAn työvaiheet turvatoiminnon suoritustason arvioinnissa

D.1 Määritetään turvatoiminnon saavuttama suoritustaso alajärjestelmien tietojen avulla ja tarkistetaan onko saavutettu suoritustaso PL vähintään vaadittava suoritustaso PLr

D.2 Tarkistetaan systemaattiset vikaantumiset ja virheet.

D.1 Suoritustasovaatimuksen saavuttaminen

- SISTEMA yhdistää automaattisesti alajärjestelmien (osien) saavuttamat suoritustasot ja vertaa koko turvatoiminnon saavuttamaa suoritustasoa PL alussa riskin arvioinnin perusteella asetettuun vaadittavaan suoritustasoon PLr.
- Saavutetun suoritustason PL on oltava yhtä hyvä tai parempi kuin vaadittava suoritustaso PLr. Esimerkiksi PL d ≥ PLr c täyttää vaatimuksen.

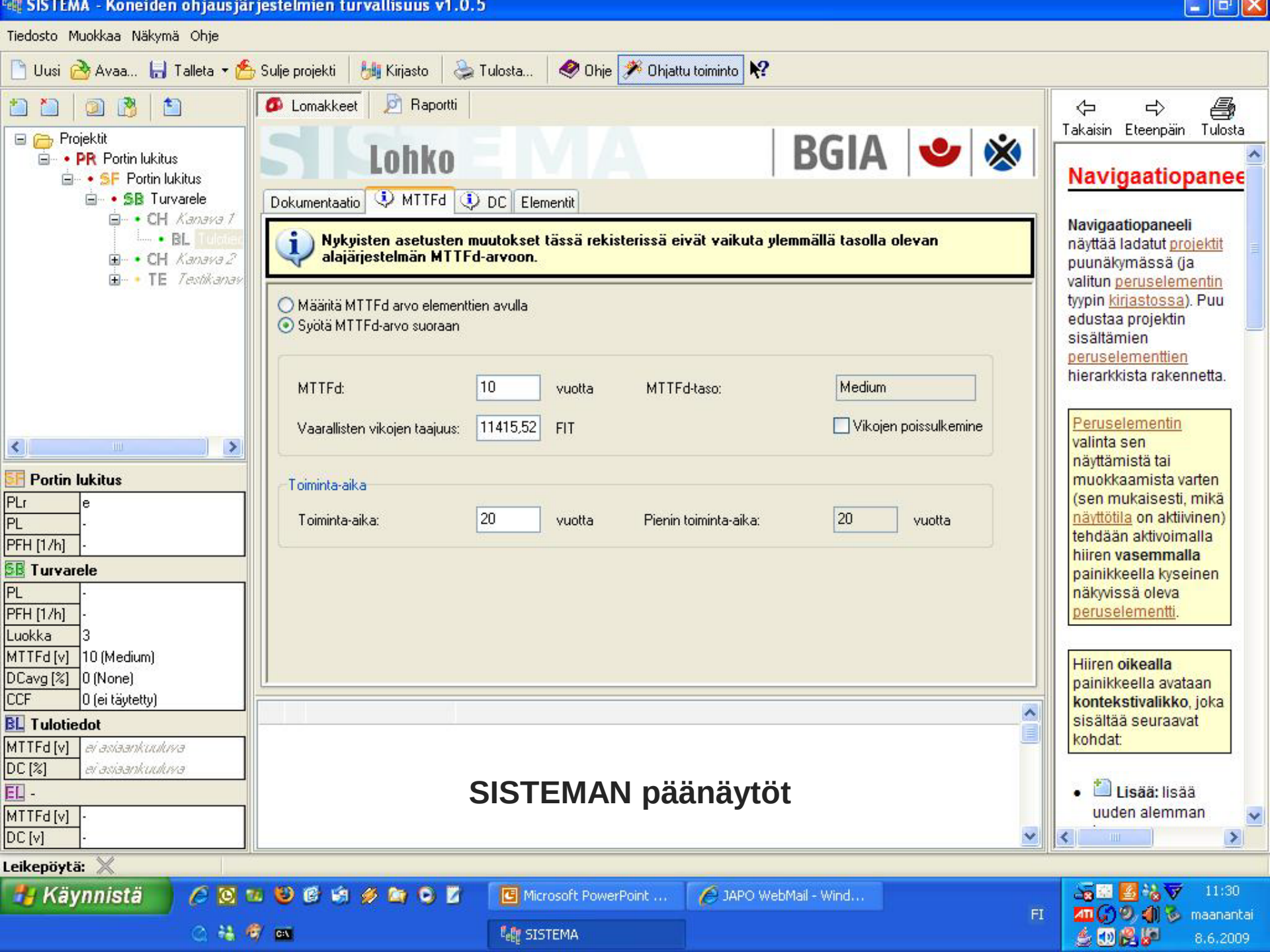
C.3 Alajärjestelmien PFH-arvot eri PL- ja SIL-tasoille

PL	SIL	Turvatoiminnon vaarallisen vikaantumisen todennäköisyys tuntia kohden [1/h]	Turvatoiminnon vaarallisen vikantumisen taajuus λ_d [vuotta]
a	-	$\geq 10^{-5} \ldots < 10^{-4}$	1…10
b	1	$\geq 3 \times 10^{-6} \ldots < 10^{-5}$	10…30
c	1	$\geq 10^{-6} \ldots < 3 \times 10^{-6}$	30…100
d	2	$\geq 10^{-7} \ldots < 10^{-6}$	100…1000
e	3	$\geq 10^{-8} \ldots < 10^{-7}$	1000…10000

Standardi ISO 61508-1 taulukko 3 ja ISO 13849-1 taulukot 2 ja 4 yhdistettynä

D.2
Systemaattiset vikaantumiset ja virheet

- SISTEMA auttaa myös tarkistamaan systemaattiset vikaantumiset tarkistuslistan avulla, mm.:
  - vaatimukset turvatoiminnon käyttäytymiselle järjestelmän ollessa vikaantunut
  - turvallisuuteen liittyvän ohjelmiston vaatimukset
  - suunnitteluvirheiden välttäminen
  - ympäristöolosuhteiden vaatimukset
- Suoritustaso esitetään muodossa: PL x Cat. y, esim: **PL d Cat. 3.**


SISTEMA - Koneiden ohjausjärjestelmien turvallisuus v1.0.5
Tiedosto Muokkaa Näkymä Ohje
Uusi Avaa... Talleta Sulje projekti Kirjasto Tulosta... Ohje Ohjattu toiminto
Projektit
PR Portin lukitus
SF Portin lukitus
SB Turvarele
CH Kanava 1
BL Tulotiet
CH Kanava 2
TE Testikanav
Lomakkeet Raportti
Lohko
BGIA
Dokumentaatio MTTFd DC Elementit
Nykyisten asetusten muutokset tässä rekisterissä eivät vaikuta ylemmällä tasolla olevan alajärjestelmän MTTFd-arvoon.
Määritä MTTFd arvo elementtien avulla
Syötä MTTFd-arvo suoraan
MTTFd: 10 vuotta
MTTFd-taso: Medium
Vaarallisten vikojen taajuus: 11415,52 FIT
Vikojen poissulkemine
Toiminta-aika
Toiminta-aika: 20 vuotta
Pienin toiminta-aika: 20 vuotta
Takaisin Eteenpäin Tulosta
Navigaatiopanee
Navigaatiopaneeli näyttää ladatut projektit puunäkymässä (ja valitun peruselementin tyypin kirjastossa). Puu edustaa projektin sisältämien peruselementtien hierarkkista rakennetta.
Peruselementin valinta sen näyttämistä tai muokkaamista varten (sen mukaisesti, mikä näyttötila on aktiivinen) tehdään aktivoimalla hiiren vasemmalla painikkeella kyseinen näkyvissä oleva peruselementti.
Hiiren oikealla painikkeella avataan kontekstivalikko, joka sisältää seuraavat kohdat:
Lisää: lisää uuden alemman
Portin lukitus
PLr e
PL -
PFH [1/h] -
Turvarele
PL -
PFH [1/h] -
Luokka 3
MTTFd [v] 10 (Medium)
DCavg [%] 0 (None)
CCF 0 (ei täytetty)
Tulotiedot
MTTFd [v] ei asiaankuuluva
DC [%] ei asiaankuuluva
EL -
MTTFd [v] -
DC [v] -
SISTEMAN päänäytöt
Leikepöytä:
Käynnistä
Microsoft PowerPoint ...
JAPO WebMail - Wind...
SISTEMA
FI
11:30
maanantai
8.6.2009

Aineistoja

- SFS:n käsikirjassa 93-6 on koneiden ohjausjärjestelmiä koskevien standardien lisäksi suomenkielinen kuvaus standardin SFS-EN ISO 13849-1 mukaisesta suunnittelumenetelmästä ja ohjeita sen käytöstä.
- IFA on laatinut laajan ohjekirjan, jossa selostetaan luotettavuustekniikan perusteita, kuvataan SISTEMAn toimintaperiaatteet ja annetaan ohjeita ja useita esimerkkejä sen käytöstä. Kirjan voi ladata ilmaiseksi IFA:n verkkosivulta saksan tai englannin kielisenä.