Teollisuusautomaation standardit
Osio 8

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

matti.sundquist@sundcon.fi

Turvaväylät ja niiden valinta: tekninen raportti IEC TR 62513

Matti Sundquist
Sundcon Oy

Kenttäväylät

- Digitaalisten tietoliikennejärjestelmien, joita nimitetään kenttäväyliksi, tarkoituksena on sarjamuotoisen digitaalisen tiedon siirtäminen laitteiden ja järjestelmien välillä.
- Kenttäväyläprotokollia on standardoitu toistakymmentä kappaletta.

Kenttäväylien käytön etuja

- Selkeämpi rakenne:
  - vähennetään ja yksinkertaistetaan kaapelointia
  - nopeutetaan laiteasennuksia ja vähennetään kaapelointivirheitä
  - helpotetaan automaatiojärjestelmän hallintaa ja muunneltavuutta.
- Kehittyneempää tiedonsiirtoa on:
  - parempi vikadiagnostiikka
  - parempi yhteensopivuus
  - langaton tiedonsiirto mahdollinen.

Tekninen raportti IEC/TR 62513

- Tekninen raportti IEC/TR 62513 ”*Koneturvallisuus – suuntaviivat tietoliikennejärjestelmien käyttämiseen turvallisuuteen liittyvissä sovelluksissa*” käsittelee kenttäväylien soveltamista turvallisuuteen liittyvien tietojen siirtoon koneiden turvatoimintojen toteutuksessa eli turvallisuuteen liittyviä tietoliikennejärjestelmiä eli turvaväyliä.

Kenttäväylät vs. turvaväylät #1

- Jos koneen ohjausjärjestelmän on tarkoitus pienentää riskiä turvallisuuteen liittyvien ohjaustoimintojen (turvatoimintojen) avulla, tavalliset kenttäväylät eivät ole riittäviä vaan on käytettävä turvaväylää.
- Kenttäväylistä modifioiduilla turvaväylillä saadaan aikaan turvallisuuteen liittyvien signaalien luotettava siirto eri laitteiden välillä.

Kenttäväylät vs. turvaväylät #2

- Turvaväylät ovat joko kokonaan erillisiä väyläratkaisuja tai useimmiten tavallisiin kenttäväyliin lisättyjä turvallisuuteen liittyvään tiedonsiirtoon tarkoitettuja ”turvaprotokollakerroksia”.

Turvaväylien toimintaperiaatteet

- Turvaväylän turvaprotokolla tuottaa kattavaa diagnostiikkaa, jolla
  - valvotaan yhteyksiä ja
  - varmistetaan signaalin eheys.
- Suurimman viiveen ylittäminen tai turvasignaalin virhe johtavat automaattisesti kohteen turvalliseen tilaan.
- Ohjattavalla kohteella on oltava määritettävissä turvallinen tila, johon se voidaan ohjata vikaan reagoivalla toiminnolla kun vikaantuminen havaitaan.

Tekninen raportti IEC/TR 62513

- Raportissa oletetaan, että standardissa IEC 62061 määritetty toiminnallisten turvallisuusvaatimusten hallinta on toteutettu (ks. osio 4) ja raportissa kiinnitetään huomiota lähinnä niihin seikkoihin, jotka koskevat erityisesti turvallisuuteen liittyviä tietoliikennejärjestelmiä.

Tekninen raportti IEC/TR 62513

- Raportissa annetaan ohjeita hallittavista asioista, jotka on otettava huomioon turvaväyläsovellusten määrityksissä, muun muassa
  - valintojen hallinta
  - konfiguroinnin ja parametroinnin hallinta (valmisteilla)
  - asennuksen hallinta
  - kelpuutuksen hallinta
  - käytön, ylläpidon ja määräaikaistarkastusten hallinta
  - muutosten hallinta.

Turvallisuuteen liittyvän tietoliikennejärjestelmän suunnittelu

- Raportissa oletetaan, että turvatoiminnot suunnitellaan ja toteutetaan standardin IEC 62061 mukaisesti:
  - turvatoimintojen vaatimukset määritetään ja dokumentoidaan (Safety Requirements Specification, SRS)
  - turvatoiminnot suunnitellaan ja toteutetaan siten, että em. turvatoimintojen vaatimukset täytetään
  - järjestelmän kelpoistuksessa tarkistetaan, onko kaikki turvallisuusvaatimukset (SRS) täytetty.

Vikatarkastelu

- Turvallisuuteen liittyvä tietoliikennejärjestelmä tulisi valita ja yhdistää turvallisuuteen liittyvään sähköiseen ohjausjärjestelmään ottaen huomioon seuraavat kohdat:
  - tarkoitettu käyttö mukaan lukien ennakoitavissa oleva väärinkäyttö,
  - toimintahäiriöt (vikaantumiset) ja
  - ennakoitavissa olevat inhimilliset virheet käytettäessä laitetta sen käyttötarkoituksen mukaisesti.

Turvallisuuden eheyden tasot

- Esimerkkejä toimintahäiriöistä (vikaantumisista):
  - tietojen syötön virheet johtuen erilaisista kytkimistä ja havaintolaitteista
  - tietojen prosessoinnin virheet johtuen solmun toimintahäiriöstä
  - toimilaitteen toiminta tietoverkosta tulevan virheellisen lähdön tapauksessa
  - solmun tulot ja lähdöt tietoverkon vikatapauksessa
  - tulot ja lähdöt ohjaavan laitteen vikatapauksessa jne.

Turvallisuuden eheyden tasot

- Turvatoiminnon saavuttama eheyden taso määritetään turvatoiminnon vaarallisten vikaantumisten todennäköisyyden [tuntia kohden] avulla (Probability of dangerous Failure per Hour, PFH), mikä on sama kuin vikataajuus:

  PFH = [1/tunti]
  missä λ_D = vaarallisten vikojen taajuus

Laitteiden turvallisuuden eheys standardin IEC 62061 mukaan

Turvatoimintoa toteuttavan laitteiston vaarallisen satunnaisvian esiintymistaajuus λ_D on kaikkien ohjaustoimintojen toteuttamiseen vaikuttavien sarjamuodossa olevien alajärjestelmien vaarallisten satunnaisvikojen summa, **johon voi kuulua myös digitaalisen tiedonsiirron (TE) vaarallisten vikaantumisten taajuus:**

$$\lambda_D = \lambda_{D1} + \ldots + \lambda_{Dn} + \lambda_{TE}$$

Bittivirheiden todennäköisyys

Bittivirhetodennäköisyys (1/s) erilaisille yhteyksille:

- $>10^{-3}$ radioyhteys
- 10^{-4} suojaamaton datayhteys
- 10^{-5} suojattu parikaapeli
- $10^{-6}...10^{-7}$ ISDN
- 10^{-9} koaksiaalikaapeli
- 10^{-12} valokuitu

Lähde: VTT

Turvaväylän vikataajuus

- Tekninen raportti IEC/TR 62513 (esimerkki): lähtötiedot ei-redundanttiselle arkkitehtuurille:

  m = 32 (yhteyksien lukumäärä)
  u = 100/s (turvallisuuteen liittyvien sanomien taajuus)
  R(p)= 10^{-16} (jäännösvirheen todennäköisyydelle oma laskentakaava)

- Tulokset:

  $\lambda = 1.1 \times 10^{-7} < 10^{-6}$ eli saavutetaan SIL 2.

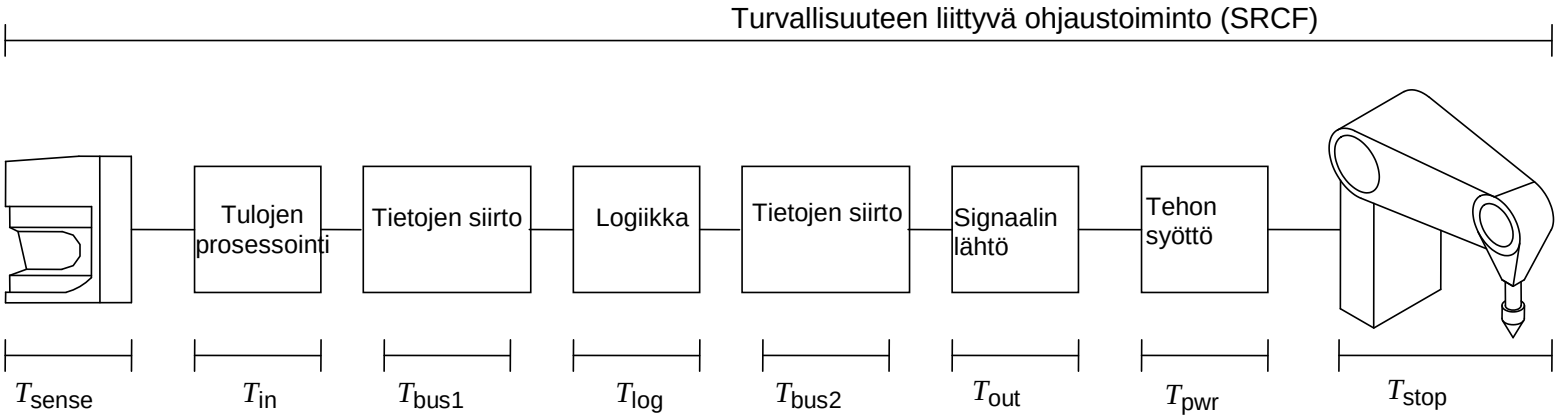
Lähde: ISA

Suurin vasteaika

- Suurimman vasteajan määrittämiseksi signaalin siirron on oltava mahdollisimman deterministinen.
- Turvasignaalin suurimman vasteajan on oltava pienempi kuin mitä tarvitaan ohjattavan kohteen saattamiseen turvalliseen tilaan.
- Turvallinen tila koskee sekä ohjattavaa kohdetta että sitä ohjaavaa automaatiojärjestelmää
  - prosessit: kokonaisvasteaika
  - koneet: kokonaispysähdysaika.

Lähde: ISA

Järjestelmän vasteaikakomponentit



IEC 190/08

Tsense = anturin vasteaika
Tin = tulon vasteaika
Tbus1 = väylän 1 vasteaika
Tlog = logiikan vasteaika
Tbus2 = väylän 2 vasteaika
Tout = lähdön vasteaika
Tpwr = teholähteen vasteaika
Tstop = toimilaiteen pysähtymisaika

On tärkeätä huomata, että *T*bus1 ja *T*bus2 eivät riipu ainoastaan väylän yhden jakson tai yhden viestin vaatimasta ajasta, vaan ne voivat myös sisältää toistoa, virheiden käsittelyä, synkronoinnin aiheuttamia viiveitä jne.

Diagnostiikka

- Diagnostiikalla on tarkoitus tunnistaa virheelliset signaalit eli turvasignaalin eheys.
- Signaalin eheyden varmistamiseksi sitä valvotaan esim. ”ohjelmallisen” redundanssin tai tarkistuspolynomin avulla.
- Aikaisemmin turvallisuuteen liittyvät signaalit erotettiin muista käyttötoimintoihin kuuluvista signaaleista ja kapseloitiin erikseen viestin osaksi, mutta nykyisin ei turvasignaalia enää eroteta muista tiedoista, vaan valvonta koskee koko signaalia.

Vikatarkastelut

Tietoliikenteen vikamahdollisuuksia:

- toisto
- menetys
- lisäys
- väärä järjestys
- virheellinen sanoma
- viive
- väärä osoite.
- tms.

Virheiden korjaus

Havaitsemis- ja suojautumiskeinoja sanomaliikenteen virhemuodoille

	Suojautumiskeino						
Virhe	Järjestys-numero	Aika-leima	Aika-valvonta	Lähettäjän ja vastaanottajan tunniste	Palaute-sanoma (kuittaus)	Tunnistus-menettely	Turva-koodi
Toisto	X	X					
Menetys	X						
Lisäys	X			X [1)]	X [1)]	X [1)]	
Väärä järjestys	X	X					
Virheellinen sanoma							X [1)]
Viive		X	X				
Väärä osoite					X [1)]	X [1)]	
Huom. Näihin kohtiin on standardissa EN 50159-2 lisätty huomautuksia.							

Turvaväylät

Turvaväyliä:

- Profisafe
- AS-i Safety at Work
- SafetyBUS p
- EsaLAN
- CANopen
- Devicenet Safety
- Interbus safety
- SafeEthernet
- TTP/C
- Flextray

Turvaväyläprotokolla sertifioidaan itse väylän mukana.

Tiedonsiirtokyky

- Järjestelmätoimittajan tuki ja sen jatkuvuus on tärkeätä.
- Sovellukseen tulee valita riittävä ja siihen sopiva tiedonsiirtokyky, jonka arvioinnissa otetaan huomioon:
  - siirtonopeus
  - siirtoetäisyys
  - maksimi vasteaika
  - vaadittu solmumäärä, jotta turvallisuuteen liittyvä toiminto voidaan suorittaa
  - vapaat solmut tulevaa käyttöä varten.

Suurin vasteaika #1

- Turvaväylän suurin vasteaika voi vaihdella riippuen sovelluksen ominaisuuksista.
- Turvatoiminto ei saa ylittää missään olosuhteissa ohjattavalle järjestelmälle vaadittua suurinta vasteaikaa.
- Vasteaikaa arvioitaessa otetaan huomioon tiedonsiirron virheet, EMC-vaikutukset, järjestelmän käyttäytyminen vikatilanteessa jne.

Suurin vasteaika #2

- On tärkeätä huomata, että vasteaika ei riipu ainoastaan väylän yhden jakson tai yhden viestin vaatimasta ajasta, vaan ne voivat myös sisältää toistoa, virheiden käsittelyä, synkronoinnin aiheuttamia viiveitä jne.
- Laskettaessa pahimman tapauksen vasteaikaa tulisi ottaa huomioon myös turvatoimintoon liittyvistä synkronoimattomista prosesseista johtuvat viiveet.

Suurin vasteaika #3

- Suurinta vasteaikaa arvioitaessa otetaan huomioon:
  - verkkoon kytkettyjen solmujen lukumäärä
  - logiikan prosessointiaika
  - verkon asetukset, kuten uudelleen yritysten lukumäärä
  - toistimen viive
  - asynkroninen/synkroninen tiedonvälitys
  - laitteiden vasteaika.

Siirtoetäisyys ja siirtonopeus

- Turvaväylän asetukset siirtoetäisyydelle ja siirtonopeudelle on tehtävä toimittajan määrittelemien kaapelityyppien ja pituuden mukaisesti. Suuri tiedonsiirtonopeus vastaa lyhyempää suurinta siirtoetäisyyttä.

Ympäristöolosuhteet

- Turvaväylä tulee valita siten, että valmistajan toimittamia erittelyjä ympäristöolosuhteiden vaatimuksista voidaan ottaa huomioon, esimerkiksi
  - lämpötila
  - tärinä ja mekaaniset iskut
  - EMC-vaikutukset.

Standardin IEC 60204-1 ”*Koneiden sähkölaitteistot*” vaatimukset on aina otettava huomioon.

Asetus- ja konfigurointityökalut

- Turvaväylän yhteydessä käytettävien asetus- ja konfigurointityökalujen tulisi olla valmistajan suosittelemia.
- Katso myös osio 10.