Suomen Soodakattilayhdistys ry

AUTOMAATIOTYÖRYHMÄN KOKOUS III/2001

AIKA	4.9.2001 klo 10:00-15:00
PAIKKA	Messukeskus, Helsinki

LÄSNÄ

Jami Maijanen	UPM-Kymmene Oyj, Kaukas
Raimo Koskinen	Sunila Oy,
Terho Tahvanainen	Honeywell Measurex Oy, Varkaus
Ari Setälä	Metso Automation Oy, Tampere
Pekka Jussila	Jaakko Pöyry Oy, Vantaa
Juha Suikki	Stora Enso Oyj, Imatra
Timo Pärssinen	Kvaerner Pulping Oy, Tampere
Heikki Lappainen	Andritz-Ahlstrom Oy, Varkaus
Tapio Väänänen	Inspecta Oy, Turku
Sebastian Kankkonen	Jaakko Pöyry Oy, Vantaa

LIITTEET

I Soodakattilan turvalukituksiin liittyvä automaatio
II Smart Sensors in Safety Critical Applications

JAKELU (24)
(12) Hallitus
(9) Automaatiotyöryhmä
(3) Arkisto EPT/MTL/SEK

1 POISSAOLOILMOITUKSET

Kauko Ylioinas ilmoitti, ettei voi osallistua kokoukseen.

2 SOODAKATTILAN TURVA-AUTOMAATIOSUOSITUS

Mauri Heikkinen (Jaakko Pöyry) esitteli soodakattilan turvalukituksiin liittyvää automaatiota (liite I).

ATR kommentoi seuraavia asioita

- TLJ-mittauksia tulee halutessa voida käyttää.
- Data tulee viedä muuntumattomana TLJ:ään.
- Liitynnät muihin järjestelmiin joko TLJ:n väylällä tai erillisellä lähtökortilla
- TLJ-yksikkö tulisi olla erillinen tai erillisessä räkissä.
- Kaksikanavaisuus tulisi tehdä selväksi
- Testattavuus tärkeää, käytettävyys sorttaus
- TLJ-hälytyksiä ei ”maskata”

Avoimia asioita: Painonapit, ovat pikatyhjennysventtiilit sähkötoimisia vaiko pneumaattisia

Tapio Väänänen pyytää Janne Kolehmaiselta (Oilon) aineistoa.

ATR kommentoi työtä 18.9. mennessä, seuraava versio julkaistaan 21.9.

Projektikokous pidetään 26.9. Pöyryllä kello 10.00.

Mauri Heikkinen mainitsi vertailun vuoksi paperin “Smart Sensors in Safety Critical Applications” joka on liitteessä II.

3 KOKOUKSEN II/2001 MUISTIO

Edellinen muistio hyväksyttiin muutoksitta.

4 TIEDOTUSASIAT

Soodakattilapäivä pidetään 11.10.2001 Hotelli Haagassa Helsingissä.

5 SOODAKATTILAN SAVUKAASUJEN PÄÄSTÖMITTAUKSET

Petri Intken insinöörityö on valmis loppukommentteja varten. Työn saanti on ollut hankalaa sillä Intke on astunut Suomen Armeijan palvelukseen. Työ lienee valmis syyskuun loppuun mennessä.

6 LIUOTTAJAN PINNAN TIHEYDEN MITTAUS

Pekka Jussila on tehnyt kyselypohjan liuotussäiliön mittausten kartoittamiseksi, Juha Suikki on täyttänyt lomakkeen Kaukopään osalta.

Kysely jaetaan yhdyshenkilöille, jotka jakavat sen edelleen oikeille henkilöille. Saatetekstinä on:

> *Ongelmia liottajan pinnan ja tiheyden mittaamisessa esiintyy jokaisella tehtaalla. Tämän kyselyn avulla pyritään löytämään hyvä tapa, jota yhdistyksen jäsentehtaat voisivat hyödyntää.*

Vastauksia pyritään saamaan lokakuun loppuun mennessä.

7 MUUT ASIAT

Edellisen pöytäkirjan kohdassa 7 esiintyviä asioita, joita pitäisi kartoittaa ja selvittää:

- Liuottajaan liittyvät säädöt ja sen yhteydet kattilan säätöön.
- Uusimmat mittausmenetelmät soodakattilan päästöjen analysointiin
- Ylös- ja alasajot. Tukeeko nykyiset automaatiojärjestelmät hallittua ajoa?
- Lieriön pinnasäädön kehittäminen
- Ylemmän tason nuohouslogiikat
- Lipeäkierron analysaattorit
- Tulipesän paineen mittaus
- Soodakattilan perusmittaukset ja niiden toteutus. ”Parhaiden menetelmien” selvitys

8 SEURAAVA KOKOUS

Seuraava TLJ-projektikokous pidetään torstaina 25.9.2001 Jaakko Pöyryllä. Varsinainen työryhmäkokous pidetään 11.12.2001 UPM_Kymmenen Kaukaan tehtaalla.

Vakuudeksi

Sebastian Kankkonen

LIITE I

SOODAKATTILAN TURVALUKITUKSET

SOODAKATTILAN TURVALUKITUKSIIN LIITTYVÄ AUTOMAATIO

1 YLEISTÄ

Soodakattilalle ei tarvitse rakentaa täysin erillistä TLJ:ää, joka koostuisi omista kenttälaitteista ja logiikkaosasta vaan kenttälaitteina voidaan käyttää normaaliin prosessinohjaukseen käytettäviä laitteita. Tämä kuitenkin sillä varauksella, että mittalaitteiden, ohjauskytkimien, rajakytkimien ym. lähteiden signaalitieto tuodaan ensin TLJ:n logiikkaan, josta signaalia voidaan hyödyntää edelleen prosessiohjaukseen.

Samoin voidaan lähteä siitä, että erillisiä venttiileitä ei asenneta varta vasten TLJ:n ohjauksia varten, vaan tarvittavat sulku-/aukaisutoiminnot toteutetaan prosessiohjausventtiileitä käyttäen.

Soodakattilaprojekteissa on TLJ:n toteutus tehty eheystasoon 2 hyväksytyllä logiikkaosalla ja kahdennetuilla (osittain myös 2/3:sta) mittausvalinnoilla, joka rajoittaa eheystason kenttälaitteidenkin osalta TET 2:een. Tärkeää olisi päättää periaatetasolla, lähdetäänkö suorittamaan täysimittainen vaara- ja riskianalyysi ja määritettäisiin tätä kautta mahdollinen eheystaso, vai tyydytäänkö toteutettuihin ratkaisuihin ja pidetään toteutuksessa TET 2.

2 LOGIIKKAOSA

TLJ:n logiikkaosa tulee olla erillinen logiikka, joka on yhteydessä prosessiohjausjärjestelmään esim. väyläliitännöin. Erillinen logiikka tarkoittaa esim. HIMA:n, Siemensin tai Honeywellin FCS logiikoita, jotka on hyväksytty Suomessa kuin Euroopassa eheystasoon TET 3.

Vaikka esim. edellämainitut logiikat ovat yksi kanavaisena hyväksytty TET 3, tulee soodakattilan yhteydessä logiikkaosa rakentaa kaksi kanavaisena kattilan käytettävyyden takia. Laukaisu kriteerinä voi olla logiikanosalta 2/2, jolloin toisen kanavan kortteja voi vaihtaa ja myös tarvittavia ohjelmaversioita voi päivittää käytön aikana kanava kohtaisesti.

TLJ:ään liittyvien piirien mittaukset johdotetaan logiikkaosaan, jossa turvallisuuteen liittyvä valvontaohjelmisto saa muista järjestelmistä riippumatta primäärimittaustiedon. Logiikkaosasta mittaustieto viedään prosessiohjausjärjestelmään indikointia, raportointia säätöä ym. tarvetta varten joko suoraan väylää pitkin tai erottimia käyttäen langoittamalla.

Turvallisuuteen liittyvien säätöpiirien liittäminen TLJ:ään toteutetaan erillisellä ohjauksella turvalogiikasta, jolla säätöelin (venttiili, pelti, invertteri jne.) saadaan me-

nemään turvalliseen tilaan ns ”kovallapuolella” ohjausjärjestelmän ohjauksesta riippumatta. Säädöt ja säädönohjaussignaalit toteutetaan prosessiohjausjärjestelmässä.

MCC:n liittyvien moottoriventtiileiden ja moottoreiden ohjaus turvalliseen tilaan toteutetaan apureleiden avulla, joita turvalogiikka ohjaa.

2.1 Logiikkaosan suunnittelu (hardware)

Logiikka asennetaan laitetilassa omaan ns. TLJ kaappiin, jonka alaosaan voidaan kentältä tulevat ja lähtevät kaapelit ja käytettävät erottimet tarvittaessa sijoittaa tai kaapin viereen sijoitettavaan ristikytkentä kehikkoon.

Redunttanttiset lähdesignaalit tulee sijoittaa eri korteille siten, että käytettävyyden aste saadaan mahdollisimman korkealle (esim. 2/3:sta valintaperiaatteella olevat mittaukset).

TLJ:ään liittyvät kenttälaitemittaukset ja ohjaukset tulee toteuttaa kiinteää kaapelointia käyttäen. Analogiasignaaleissa käytetään suojattuja kaapeleita. Kenttäväyläratkaisuista ei ole vielä niin paljoa käyttökokemuksia, joskin hyväksyntöjä turvapiireihin varsinkin binääripuolella löytyykin, että niitä voitaisiin käyttää TLJ:ssä mittaus- tai ohjaustiedonsiirtoon muuten kuin ehkä eri TLJ:ien välillä.

TLJ:n liittyviin kaappeihin, kehikoihin, kortteihin ja kanaviin erillinen punainen merkintä osoittamaan, että laitteet kuuluvat turvallisuuteen liittyviin piireihin.

Jännitesyöttö logiikkaosalle tulee järjestää häiriösuojamuuntajalla varustetusta jännitelähteestä. Tämän lisäksi logiikkaosalle (sitä kautta kenttälaitteille) tulee järjestää varasyöttö varsinaisen jännitesyötön katkojen ja häiriöiden varalle. Varasyötön tulee kytkeytyä automaattisesti pääsyötön katkettua. Varasyöttö tulee järjestää UPS-laitteistolla tai tasavirta-akustolla. Varasyötön tulee pystyä syöttämään järjestelmää vähintään 30 min. Sekä pääsyötön että varasyötön kunnonvalvonnasta tulee olla hälytys käyttäjälle.

2.2 Logiikkaosan suunnittelu (software)

TLJ-piirien toiminnoista tulee tehdä omat TLJ-kaaviot (logiikkakaaviot), joista näkyy koko piiri yhdellä dokumentilla lähteestä kohteeseen (laukaisurajat, toiminta, I/O:t, liitynnät muualle).

Kaksi kanavaisena rakennetun logiikkaosien tuloksia verrataan keskenään ja poikkeavuuksista tehdään hälytys.

Käyttöliityntään tulee TLJ:stä tehdä omat näytöt, joista selviää mittaustietojen, binääristen tilatietojen ja ohjausten lisäksi myös mittalaitteiden tila sekä päätetilavalvonta ohjattavista kohteista.

TLJ:lle tulee olla omat hälytyssivut, joissa on TLJ toimintojen lisäksi tulee myös informoida kenttälaitteiden anturi- ja signaaliviat. TLJ:n laukaisuista tulee olla aikaleimalla varustettu ilmoitus- tai hälytysteksti, jonka perusteella laukaisusyy voidaan selvittää. Samoin hälytyksiin kuuluu redundanttisten mittausviestien poikkeamavalvonta.

TLJ:n ohjelmat tulee olla salasanalla suojattuja siten, että pääsy ulkopuolisilta muuttamaan ohjelmia on estetty.

3 KENTTÄLAITTEET

Mittalaitteina tulee käyttää analogisia 2-johdin ja mahdollisimman korkean itsediaknostiikan omaavia lähettimiä. Normaaleita HART-lähettimiä (Rosemount, E+H, Foxboro jne.) käytettäessä tulee mittaukset toteuttaa 2/3:sta vertailevalla periaatteella käytettävyyden saamiseksi korkeammaksi. Ns. älykkäitä turvalähettimiä käytettäessä (paras ratkaisu lähitulevaisuudessa), korkeampaan eheystasoon ja käytettävyyteen päästään kahdella lähettimellä 1/2 periaatteella. Turvalähettimistä on saatavilla kaksi eri signaalia, mittaussignaali ja diagnostiikkasignaali. Diagnostiikkasignaali kertoo lähettimen kunnontilasta ja laitosta ei tarvitse välttämättä ohjata turvalliseen tilaan yhden lähettimen vikaantumisesta vaan vastuu siirretään yksin toiselle lähettimelle ja hälytetään vikatilanteesta käyttäjää.

Kaikki soodakattilan TLJ:n liittyvät paine- ja pintamittaukset toteutetaan paine- ja paine-erolähettimillä. Lähettimiä valittaessa tulee vaatia lähettimille hyväksyntä turvallisuuteen liittyviin mittauksiin. Lähettimet tulee olla ohjelmoinnin estoilla sekä tarkastetuilla laitteilla kalibroituja. Redundanttiset mittaukset tulee olla kalibroitu samalle alueelle.

Turvallisuuteen liittyvissä piireissä mittaussignaaleja ei kompensoida vaan laukaisusignaaleina käytetään raakasignaalia. Tämä siitä syystä, että kompensoinnit lisäävät ensinnäkin TLJ:n piirejä, toiseksi laskentakaavat monimutkistavat kokonaisuuden suorapiirteisyyttä ja kolmanneksi kompensointien merkitys mittauksissa ei ole tavattoman suuri.

Pikapysäytys-, pikatyhjennys- ja hätä-seis-painonapit tulee olla tyypiltään sienipainikkeita, väriltään punaisia, kaksilla kärjillä varustettuja (kanavakohtainen) ja painettaessa pohjaan lukkiintuvia.

Rajakytkimet tulee olla normaalisti kiinni tyyppiä 2-johtimisia (induktiivinen) tai mekaanisia kullatuin koskettimin.

Paloventtiileinä ja pikasulkuventtiileinä (kaasu, öljy, hajukaasu) sulkukäytössä käytetään pneumaattisia jousisulkee toimilaitteita ja tuuletusventtiileinä jousiavaa toimilaitteita. Turvatilaan ohjaaminen toteutetaan magneettiventtiilillä, joka asenne-

taan toimilaitteen yhteyteen siten, että jännitteettömänä magneettiventtiili päästää paineen pois toimilaitteesta ja jousi pakottaa venttiilin turvalliseen tilaan.

Lipeän syöttöventtiileinä käytetään säätöventtiileitä, joissa jousisulkee toiminta toimilaitteen yhteyteen asennetulla magneeettiventtiilillä. Voitaisiinko hoitaa erillisellä syöttölinjassa olevalla on/off –venttiilillä?. Tulisiko olla myös paluulinjassa sulkuventtiili?.

TLJ:ään liittyvät magneettiventtiilit tulee olla ilman käsiohjausmahdollisuutta.

Syöttövesiventtiilit, päähöyryventtiilit, ulospuhallusventtiilit, starttiventtiilit, ruiskuventtiilit, pikatyhjennysventtiilit, lieriön vajennusventtiilit ja jakokammion vajennusventtiilit tulee olla sähkökäytöllä varustettuja ja varavoimalla varmennettuja. Vai tarviiko?.

Pumppujen ja puhaltimien pyörintätiedot otetaan moottoreiden käyntitiedoista sulkeutuvilla koskettimilla moottorikeskuksesta kahdella kosketin tiedolla kanavakohtaisesti. Pyörintävahdit??

4 KENTTÄSUUNNITTELU

TLJ:ään liittyvät kenttälaitteet, prosessiyhteet ja kaapelointi tulee merkitä muusta kenttälaitteistosta eriävällä punaisella merkkauksella.

Sekä juuriventtiilit että asennusventtiilit tulee järjestää lukitusmahdollisuudella ulkopuolisten estämiseksi muuttaa venttiileiden asentoa. Mittalähettimien mittausyhteisiin joko erillinen tai em. venttiileiden yhteyteen tulee järjestää pumppausyhde käyttöönotto- ja määraaikaistestauksia varten.

Kenttäkoteloissa, joihin TL-piirejä johdotetaan, tulee olla oma liitinrima (esim 24 liitintä), jotka johdotetaan omalla runkokaapelilla ristikytkentään TLJ:lle varattuun kenttään.

5 SOODAKATTILAN TURVALUKITUKSET

5.1 Pikapysäytys

5.1.1 Lähde

Pysäytyspainike valvomossa

5.1.2 Kohteet

- Ääni- ja valohälytykset (aktivoituu)

- Kattilasuoja (aktivoituu)
  -lipeän syöttöventtiilit (sulkeutuu)
  -apupolttoaineiden polttoluvat (poistuu)

- Turpiinin suojaus (aktivoituu)

- Apupolttoainelinjojen sulkuventtiilit (kaasu, öljy, metanoli, hajukaasut)
  -sulkuventtiilit (sulkeutuu)
  -tuuletusventtiilit (avautuu)

- Käynnistys-, kuorma-, hajukaasupolttimet (sammuu)

- Primääri- ja hajukaasupuhallin (pysähtyy)

- Lipeäpumput (pysähtyy)
  -jos lipeän syöttöventtiilit ei kaikki kiinni (30s)

- Nuohousohjelma pysähtyy ???

- Nuohoushöyryn venttiili sulkeutuu ???

- Sähkösuotimet pysähtyy ???

5.1.3 Toteutus

Pikapysäytys painike avautuvilla koskettimilla (kahdet koskettimet)

A. Apupolttolinjojen sulku- ja tuuletusventtiilien, poltin kohtaisten venttiilien, polttimien toimilaitteiden sekä sytyttimien ohjausjännitteet syötetään poltinohjauskaapista kahden (kanava kohtaisen) kontaktorin kautta, joilla ko. laitteet saadaan yksiselitteisesti kaikki jännitteettömäksi ja siten turvalliseen tilaan.

B. Apupolttolinjojen sulku- ja tuuletusventtiilit, poltin kohtaiset venttiilit, polttimien toimilaitteet sekä sytyttimet ohjataan suoraan turvalogiikan korteilta omilla lähdöillä.

Muiden kohtien ohjautuminen turvalliseen tilaan toteutetaan erillisten releiden avulla, joita ohjataan turvalogiikalla.

5.2 Pikatyhjennys

5.2.1 Lähde

Tyhjennyspainike valvomossa

5.2.2 Kohteet

Kun määrättyaika (3min) pysäytyksestä kulunut

- Pikatyhjennysventtiilit (avautuu)

- Syöttövesipumput (pysähtyy)

- Päähöyryventtiilit (sulkeutuu)

- Starttiventtiilit (sulkeutuu)
- Ruiskutusventtiilit (sulkeutuu)
- Jatkuva ulospuhallus (sulkeutuu)
- Syöttövesiventtiilit (sulkeutuu)
- Lieriön vajennus (sulkeutuu)
- Pääjakokammion tyhjennysventtiilit (sulkeutuu)

5.2.3 Toteutus

Pikatyhjennyspainike sulkeutuvilla koskettimilla

Turvalogiikka ohjaa erillisiä sulkeutuvia releitä, joiden kautta venttiilit pakko-ohjataan turvalliseen tilaan. Turvaohjauksen yhteydessä lämpöreleet ohitetaan. Normaali ohjaukset ohjausjärjestelmässä ja MCC:ssä.

5.3 Kattilasuoja

5.3.1 Lähteet

- Pikapysäytyspainike valvomossa
- Savukaasutie kiinni (yksi tie auki)
  -tulokanavanpelti pois aukirajalta
  -puhallin ei käy
  -lähtökanavanpelti pois aukirajalta
- Instrumentti-ilman paine alle alarajan
  -2/3-valinnalla
- Kattilan paine yli ylärajan
  -2/3-valinnalla
- Lieriönpinta yli ylärajan (märkäkeittosuoja)
  -2/3-valinnalla
- Lieriönpinta alle alarajan (kuivakeittosuoja)
  -2/3-valinnalla
- Primääri-ilman virtaus alle alarajan (summa)
- Kokonaisilman virtaus alle alarajan (summa)
- O2-% liian matala ????

- Kattila ei tuuletettu ????

- Liikaa sytytyskertoja ????

5.3.2 Kohteet

- Lipeän syöttöventtiilit (sulkeutuu)

- Apupolttoaineiden polttoluvat (poistuu)

5.3.3 Toteutus

Laukaisuehdot (2/3-valinnat, ilmavirtauslaskennat, savutie auki logiikka) toteutetaan turvalogiikassa.

Lipeän syöttöventtiilit on varustettu jousisulkee toimilaitteella ja magneettiventtiilillä, joka jännitteettömänä päästää paineen purkautumaan toimilaitteesta ja jousi sulkee venttiilin. Magneettiventtiilin ohjaus turvalogiikasta.

5.4 Apupolttoaineiden hätä-seis –painikkeet

5.4.1 Lähteet

- Hätä-seis –painike valvomossa

- Hätä-seis –painikkeita kentällä kulkuteiden varsilla
  -Poltin tasoilla, molemmilla puolin kattilaa
  -Sulakourutasolla
  -Katolla tukipolttimilla

- Hätä-seis –painikkeet poltinohjauskoteloissa
  -tulisiko vaikuttaa vain ko. polttimeen ???

5.4.2 Kohteet

- Apupolttoainelinjojen sulkuventtiilit (kaasu, öljy, metanoli, hajukaasut)
  -sulkuventtiilit (sulkeutuu)
  -tuuletusventtiilit (avautuu)

- Käynnistys-, kuorma-ja hajukaasupolttimet (sammuu)

5.4.3 Toteutus

Kuten pikapysäytys.

6 TESTAUKSET

TLJ:n testauksiin kuuluu tehdastestaus (FAT) ja käyttöönottotestaus (SAT) ja muusta normaaliohjausjärjestelmästä poiketen käytön aikaisia määräaikaistestauksia järjestelmän eri osien hyväksynnöistä riippuen aina määrävälein. Normaali testausväli on 24kk. On järjestelmiä, joita testataan 18kk välein ja jopa 4v on käytössä.

Kaikissa edellä mainituissa testauksissa on tärkeää, että testauksista tehdään testaussuunnitelma, tehdään testausohje, pidetään pöytäkirjaa ja testauksista tehdään testausraportti, jonka alle kirjoittavat kaikki osallistujat.

Testauksiin tulee tehdä suunnitelma, jossa esitetään testausorganisaatio, vaatimusmäärittelyt, koestuksen edellytykset, dokumentointi, koestusvälineet, koestuksen suoritus, virheiden korjaaminen, tarkastuksen hyväksyntä ja koestusraportti.

Testauksista tulee tehdä tarkka koestusohje, jossa esitetään kunkin testausvaiheen valmistelevat toimenpiteet, ohjeet lähteiden simuloinneille, ohjeet mahdollisille kanavien väliaisille kytkennöille ja kunkin testausvaiheen lukitukset (kohteet).

Koestuspöytäkirja tulee olla valmisteltu etukäteen mukaillen testausohjetta siten, että ohjeen mukaan toteutetut toimenpiteet ja tapahtuvat lukitukset voidaan todeta tapahtuvaksi OK-merkillä ja vältytään kirjoitustoiminnalta ja testaus etenee nopeaan.

Testausraportti tehdään testauksen lopuksi, jossa todetaan testauskohde, päivämäärä, osallistujat ja maininta testauksen hyväksymisestä ja kaikkien osanottajien allekirjoitukset. Liitteeksi raporttiin liitetään yhteenveto testauksesta, jossa kirjataan testausjärjestelyt, testauksen suoritus ja kaikki mitä testauksessa huomioitiin (puutteet toiminnoissa, virheet testausohjeissa, muutoksia mitä tehtiin jne.) ja testauksessa ollut tokumentointi.

Tehdastestauksessa (FAT) pääpaino on ohjelmatestauksessa. Kenttälaitteita voidaan simuloida erilaisilla keinoilla esim. johdottamalla lähteet ja kohteet kytkin- ja valotauluihin nopeuttamaan testauksen kulkua. Tärkeää on , että kaikki lähteet ja lähteiden eri yhdistelmät (2/3:sta mittausvalinnat) tulee käytyä läpi ja että laskennalliset laukaisurajojen mA-arvot tulee tarkasti käytyä läpi.

Kokonaisuuden käyttöönottotestauksessa (SAT) ja määräaikaistestauksissa kenttälaitteiden lähdesignaalit tulee simuloida mahdollisimman todellisina. Paine- ja paine-erosignaalit pumppaamalla, lämpötilasignaalit lämmittämällä, painonapit ja rajakytkimet todellisilla laitteilla, käyntitiedot todellisista tiedoista (turvakytkimet pois päältä). Kohteet todetaan kentällä myös todellisina, venttiilit kentällä todellisista liikkeistä, moottoreiden pysähtyminen kontaktoreista, releiden liikkeet jne.

Testauksissa on huomioitava, että käytettävistä simulaattoreista on olemassa voimassa olevat tarkastuspöytäkirjat,

Kunkin testausvaiheen testaukset jakaantuvat kahteen vaiheeseen, turvalogiikantestaukset ja kenttäpiirien testaukset.

6.1 Turvalogiikan testaukset

Kunkin testauksen valmistelevissä vaiheissa tulee huomioida, että varmistutaan siitä, että turvakohteen meneminen turvalliseen tilaan johtuu nimnomaan turvalukituksen toimimisesta eikä esim. normaalista prosessilukituksesta. Tämä varmistetaan siten, että poistetaan väliaikaisesti prosessiohjausjärjestelmässä olevat lukitukset.

Kaksi kanavaisessa TLJ:ssä tulee myös huomioida, että testaukset voidaan suorittaa kanavakohtaisesti. Molempien kanavien tulee yksistään pystyä suorittamaan tarvittavat turvaohjaukset täydellisinä.

Turvalogiikan vikatestauksissa tulee huomioida korttien irrottamiset, erilaisten väylien irrottamiset, jännitesyöttöjen katkaisut.

6.2 Kenttäpiirien testaukset

Kenttätestaukset yksittäisen mittalähettimen kohdalla tulee ottaa huomioon normaalin turvarajan testauksen lisäksi myös signaalivika ja lähetinvikatestaukset. Riippuen siitä, miten signaalivika ja lähetinvika lähettimissä on järjestetty, tulee turvalogiikan toiminta rakentaa niin, että viat havaitaan ja turvatoiminta toteutuu.

2/3:sta valintaisissa mittauksissa testaukset tulee järjestää siten, että mittauksia käsitellään pareittaen ja tarkastetaan yksittäiset hälytykset ja pareittain tulevat laukaisut.

Kattilasuojan testauksissa lähdetään aina siitä, että kattilasuoja on simuloitu kuntoon ja testattavilla signaaleilla pareittain joko mA-simulaattoreilla tai kentällä pumppaamalla (käyttöönotto- ja määräaikaistestit) todetaan turvarajan ylityksestä kattilasuojan laukeaminen.

7 DOKUMENTOINTI

Dokumentointi tulee tehdä sellaiseksi, että asiat löytyy yksistä kansista. Sisällysluettelo voisi olla esim. tällainen:

- Kuvaukset
- Logiikkakaaviot
- Näyttökuvat
- Ohjelmakaaviot
- Piiri- ja johdotuskaaviot
- I/O-kortti- ja kaappikuvat
- Testausohjeet ja pöytäkirjat

LIITE II

SMART SENSORS IN SAFETY CRITICAL APPLICATIONS

1 SMART SENSORS IN SAFETY CRITICAL APPLICATIONS

1.1 William M.Goble, Director, Critical Systems

Moore Process Automation Solutions
Spring House, PA, USA

1.2 Jon Keswick, Critical Systems Product Manager

Moore Process Automation Solutions
Copse Road, Lufton, Yeovil, UK
BA22 8RN

1.2.1 Abstract

End users in the process industry are spending vast amounts of time and money designing safety related systems which meet performance criteria set out in soon to be published international standards. To meet both safety and operational criteria, sensor architectures must be considered very carefully. Conventional analogue transmitters can be employed in many different ways, but what are the options, and which is the most economical configuration? This paper seeks to answer these questions by explaining the options and looking at some exciting new research and development in the area of smart safety transmitters.

1.2.2 Introduction

Minimising risk to personnel and the environment is a key goal of any modern industrial process. Not only is it humane to protect one's fellow human-beings, but it becomes extremely worthwhile economically in the long run also. Achieving the dual goals of both an efficient and safe process control system has been the longstanding dilemma of system designers since day one.

At the Texaco refinery in Milford Haven, UK on 24th July 1994, an accident occurred which was the result of a number of mishaps that could have been avoided. Although not directly responsible for the eventual explosion, one of the contributing factors were poorly maintained instruments which gave false readings to the control and shutdown systems. In a report by the UK Health & Safety Executive (HSE) [1] this was considered to have 'contributed significantly to the causes of the incident'. Most of the faults were already present in the system prior to the explosion and could have been avoided by more effective maintenance regimes in the plant. However, there were also faults present that could not have been diagnosed without an engineering investigation. This suggests that a measure of diagnostic intelligence could have contributed to there being a better likelihood of some of the critical loops being diagnosed and fixed earlier. Had the critical loops themselves been identified at the design stage then there would have been a significant reduction in risk.

1.2.3 Design Standards for Programmable Systems in Safety Applications

Minimising risk by employing programmable electronics is fast becoming the de-facto process industry method. Reliance upon discrete systems such as relay based logic has given way to the far more flexible domain of specialist programmable logic controllers. So much so that it is now the subject of a soon to be published draft international standard called IEC61508 [2]. As it will be a 'Basic Safety Publication' there are likely to be further standards that will cross-reference IEC61508 and relate to specific industry areas. This will include IEC61511 as specific to the process industry.

Older national standards such as the German DINVDE0801 were more prescriptive in nature. The new standards are performance based and take a lifecycle approach in order to address both random and systematic types of failure. Systematic failures are generally introduced into the system by poor specification, design or procedures of some sort, a fine example of which is the Milford Haven refinery accident. So called 'random' failures occur when components fail to carry out their intended design function either through poor quality production, or due to some stress condition exceeding the associated 'strength' of the component [3]. The scope of IEC61508 includes not simply hardware, but also embedded and user application software. Software cannot fail randomly, but has systematic errors built into it by humans. These human factors also have an influence upon the overall design, operation and maintenance of the system, and one soon sees the importance of the lifecycle approach to safety that the IEC61508 standard advocates.

The other major area of cross-industry safety terminology that the standard dictates are target failure measures. These target figures are known as Safety Integrity Levels (SIL) and appear in the normative part 1 of IEC61508. For the process industry, generally only the 'low demand mode' of operation column will be relevant, as this is the nature of most applications i.e. emergency shutdown systems. Figure 1 shows the main column, PFDavg (average probability of failure to perform its design function on demand) and its reciprocal RRF - Risk Reduction Factor (not shown in the standard but referred to elsewhere in this paper).

Safety Integrity Level	Average Probability of Failure on Demand (PFDavg)	Risk Reduction Factor (RRF)
4	< 0.0001	> 10,000
3	0.001 - 0.0001	1,000 - 10,000
2	0.01 - 0.001	100 - 1,000
1	0.1 - 0.01	10 - 100

Figure 1. Safety Integrity Levels

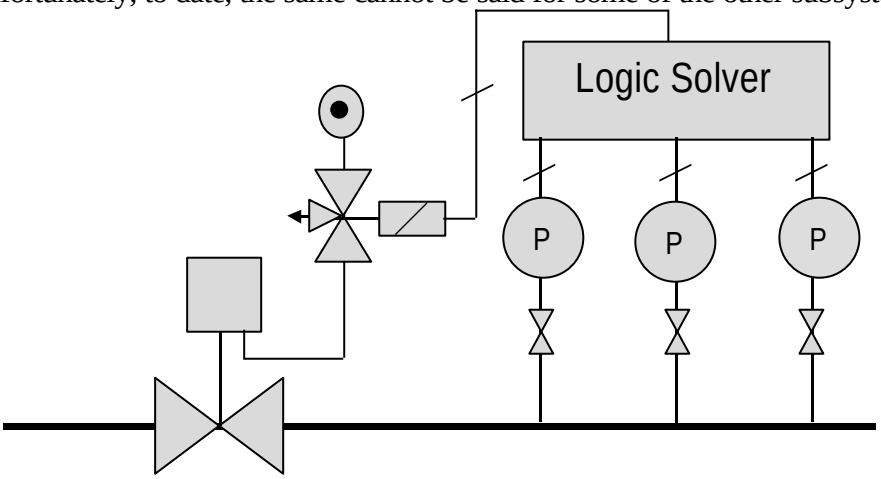
As the name implies, PFDavg is an average target figure for the safety integrity requirements of the various subsystems within the entire safety related system. As a target, most (if not all) systems in the process industry will fall into the SIL1 to SIL3 categories. This paper will now focus on some of the hardware elements necessary to achieve safety integrity within the overall system design.

1.2.4 Safety System Hardware

To make comparisons of achievable SIL's it is important to divide the system into subsystems. The logic solver (PLC) is only one of the subsystems in the critical loop. As can be seen by the illustration in figure 2, just as critical to the Safety Instrumented System (SIS) design are the sensors and actuators that are employed in the loop. From a hardware point of view it is very important to select the correct level of integrity of each subsystem that is involved in carrying out the safety function. Whilst the focus of this paper is on the subject of sensors, it is important to have an overview of the two other main subsystems within a critical loop.

1.3 The Logic Solver

In order for the end user to place complete trust in the logic solver 'black box', some vendors have gone to the great pains of providing fail-safe circuitry, high levels of diagnostics and fault tolerance in their PLC designs. The result is that almost complete faith can be placed in the integrity of Safety PLC's designed specifically with both safety and availability in mind. General PLC's do not have these special attributes and should never be considered for safety applications. Obviously, even a Safety PLC can be misapplied and poorly configured, so further developments in managing software safely are now being developed by some vendors. Modern dual Safety PLC's can now achieve PFD's at the safer end of the SIL3 target, and some are even pushing into the SIL4 boundary.
Unfortunately, to date, the same cannot be said for some of the other subsystems within the critical loop.



1.3.1.1.1.1

1.3.1.1.1.2

1.3.1.1.1.3 Figure 2. A typical pressure protection loop

1.4

1.5

1.6

1.7 Actuators

The actuator is an essential part of the chain that drives a valve to the closed position when required. Shut-off valves for high integrity applications such as pressure protection feature designs that ensure certain, fast closure of the valve and assure a tight seal. However, it is not uncommon for the shut-off valve itself to be regarded as the weakest link in the chain. Due to their mechanical nature, the only way in which to 'diagnose' that a valve has failed is to actually exercise it. As this requires a shutdown to carry out effectively, and process shutdowns cost time and significant amounts of money, it is actually quite rare for a shutdown valve to be fully exercised in this way. However, some manufacturers are providing solutions for partial stroking of the valve which effectively mean that the testing can be carried out on line without the need for traditional solutions such as bypass valves. Most of the solutions currently available are based upon mechanical interlocks, but certain vendors are looking at designing 'intelligent' valve positioners.

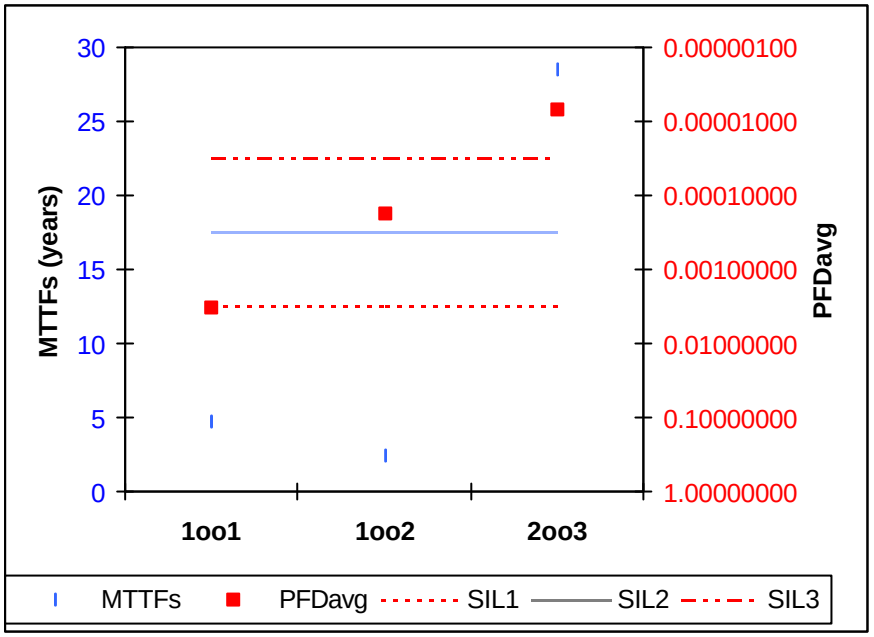
1.8 Sensors

Sensors can be broadly split into two categories, namely discrete and analogue. More and more system designers are turning to analogue sensors for safety applications, the inherent ability to diagnose failure being the primary reason. It is relatively easy to detect a failure in an analogue sensor by noting changes in its normally dynamic signal. It is virtually impossible to detect some failures in a discrete switch that may remain static for months or even years. In a discrete switch there is no functional difference between successful operation and "fail-danger," in both cases the switch appears closed (energised).

In addition to better diagnostics, other advantages of analogue sensors include multiple trip points per sensor and the ability to obtain calculated results. Most sensors are not inherently fail-safe and so they can have a significant effect upon the safety integrity of the SIS. Sensor redundancy is therefore the method used generally in the process industry to enable signals coming from the same process measurement to be compared and voted upon before a shutdown is initiated.

1.8.1 Quantifying Sensor Configurations

The reference to design standards at the start of this document gave certain target failure measures against which systems *and* subsystems can be judged. Sensor failures must be considered just like logic solver subsystems. When considering failures, they must be categorised firstly according to *how often* they fail (typically represented by a Mean Time To Failure or MTTF figure) and *how* they fail (i.e. safely or dangerously). This has already been the subject of some significant new research [4], the results of which show an amazing similarity between logic solver architectures and redundant sensor arrangements.



1.8.1.1 Figure 3. Comparison of Sensor Redundancy Options

For example, a conventional pressure transmitter has data as follows:

MTTF = 40 years

% Safe failures = 35% (Estimated)

For an average repair time of 8 hours, a periodic inspection interval of one year (8760 hours) and average time to restart after a shutdown of 24 hours, the PFDavg and MTTFs (Mean Time To Fail safe) are as appears in Figure 3.

The results provide the following conclusions for sensors :

1. A typical conventional 1oo1 sensor can just achieve the required SIL1 allocation but has a spurious trip rate of around once every 5 years.
2. Using the same sensors in a 1oo2 voted configuration achieves SIL2 comfortably but has the added problem of actually doubling the trip rate.
3. To actually achieve SIL2 or better, and at the same time achieve suitable availability, involves using at least three conventional sensors with 2oo3 comparison voting. Without the comparison, the figures look much worse.

2 SMART TRANSMITTERS

Smart transmitters have great potential in safety-related applications[5]. These include additional diagnostic capability, internal compensation for higher accuracy, remote engineering range change, and digital communications that may be used to provide secondary variables.

However, the current problem with employing “smart” transmitters in safety related applications is not dissimilar to the issues originally encountered with PLC’s. The need to provide a guaranteed fail-safe mechanism is paramount. Likewise, it is of great importance to be able to diagnose a very high percentage of dangerous internal failures in the microprocessor based logic.
As with conventional PLC’s in the 1980’s, conventional transmitters were not designed with safety foremost in the mind. The PLC had to go through a sea change in design in order to have the assurance that is now commonplace with modern safety PLC’s. In exactly the same way, the conventional transmitter is going through re-design in order to be re-born as the safety transmitter.

3 SAFETY TRANSMITTERS

The draft IEC61508 standard now includes tables which separate out completely predictable hardware from hardware with unpredictable failure modes. Microprocessors are, by their nature, complex and unpredictable. To achieve high PFD’s using transmitters that employ microprocessors means being able to justify the diagnostic coverage and fail-safe nature of the transmitter. Just like PLC hardware, this can only be done using Failure Modes, Effects and Diagnostic Analysis (FMEDA).

In order for the diagnostics to provide significant benefit, the failures must be annunciated. A “safety transmitter” must be able to signal to the safety PLC to indicate a detected failure. It is not possible to achieve this with any integrity by using the HART signal. However, using the 4 – 20 mA standard it is possible. Fortunately, a standard exists that already defines analogue current ranges that indicate diagnostic failure in a transmitter. These values of analogue current can be used within a safety PLC to define the appropriate safety action when transmitter failure occurs.

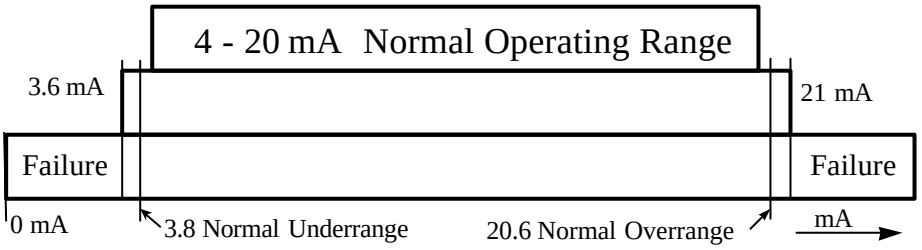


Figure 4. Transmitter Signal Level

Figure 4 shows the current ranges of “NAMUR Empfehlung” NE-43. When an analogue transmitter is sending a signal in the 4 - 20 milliamp range, that is considered normal. Analogue currents beyond 4 - 20 in the 3.8 - 20.5 range account for normal underrange and overrange. An analogue current in the range of 3.6 - 3.8 milliamps or 20.5 - 21 milliamps indicates as failure detected within the smart transmitter. A current range of 0 - 3.6 milliamps probably indicates an open circuit in the field wiring, and a current range of over 21 milliamps probably indicates short circuit in the field wiring. The use of this scale allows a smart transmitter to indicate when and how it has failed.

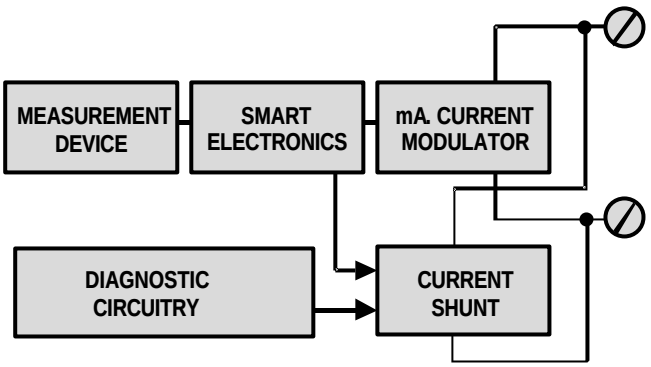
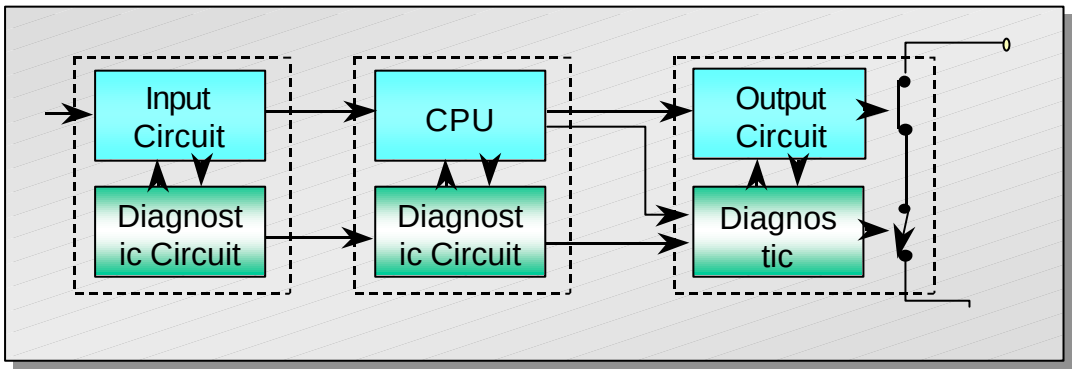


Figure 5. Safety Transmitter

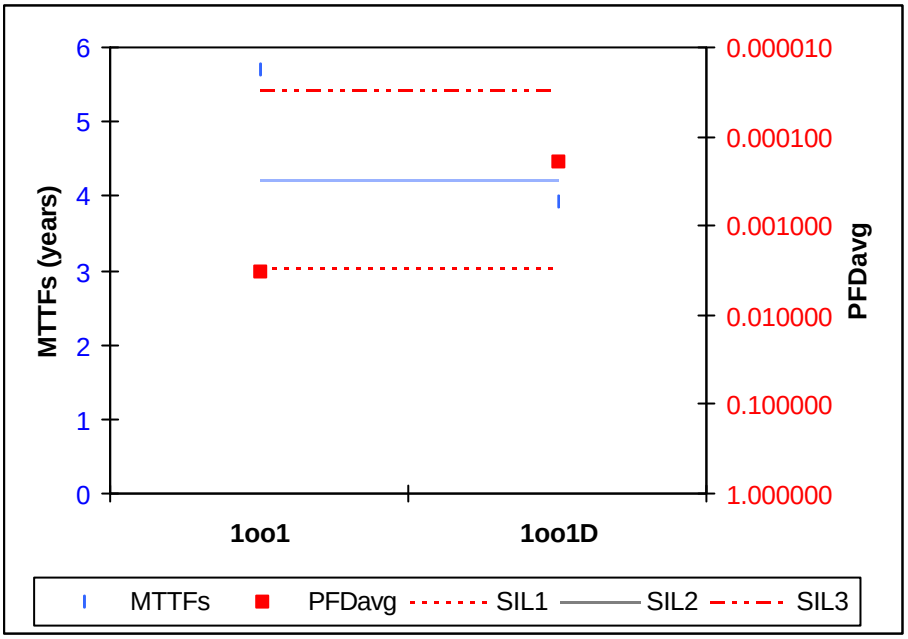
A safety transmitter must provide completely independent circuitry to force the output current to one of the predefined failure ranges (Current shunt on Figure 5). A transmitter with this capability may be connected to a safety PLC and the system could be programmed to respond appropriately to transmitter failure. The ability to discriminate between probable field wiring faults and transmitter failures is also an advantage in reducing downtime. This architecture is equivalent to the safety PLC 1oo1D architecture (Figure 6).



3.1.1.1.1

3.1.1.1.2 Figure 6. Safety PLC 1oo1D

This architecture can also be analysed for PFDavg and MTTFs. If it is assumed that the system will not automatically shut down when a dangerous detected failure occurs (which we assumed), then the PFDavg and PFS equations are the same as the 1oo1. The comparison of 1oo1 and 1oo1D results appears in figure 7.



3.1.1.1.2.1 Figure 7. 1oo1 versus 1oo1D

A single safety transmitter has met the PFDavg budget comfortably, providing performance equivalent to two conventional transmitters (Figure 8).

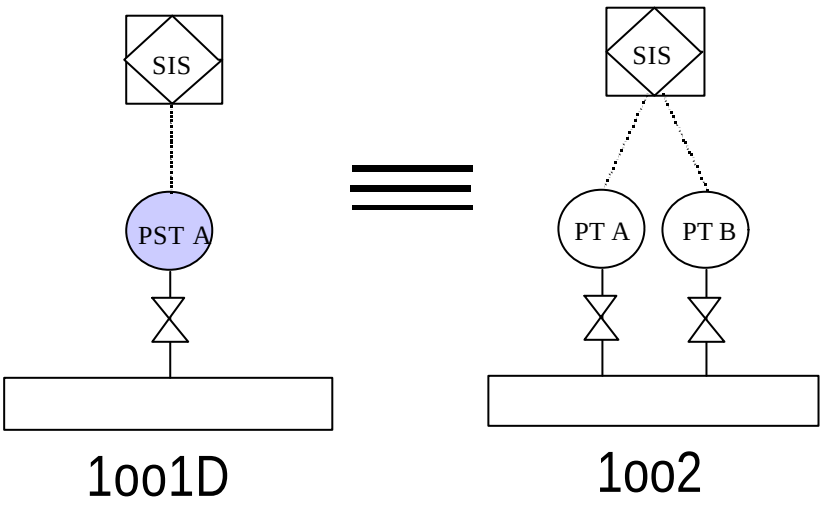


Figure 8. Equivalent safety performance

Another configuration is possible using safety transmitters. Two can be used on the same process measurement in a configuration similar to the 1oo2D (Figure 9). If the safety PLC recognises the NE-43 standard then two signals are available for each transmitter, the process measurement and a diagnostic signal. When both diagnostics signals indicate correct operation, a comparison is done on the analog signals to provide an

extra layer of safety diagnostics. When one diagnostic signal indicates failure in one transmitter, the system continues operation on the other transmitter.
If both diagnostic signals indicate failure or comparison indicates deviation beyond the safety accuracy, the sensor subsystem has failed dangerously.

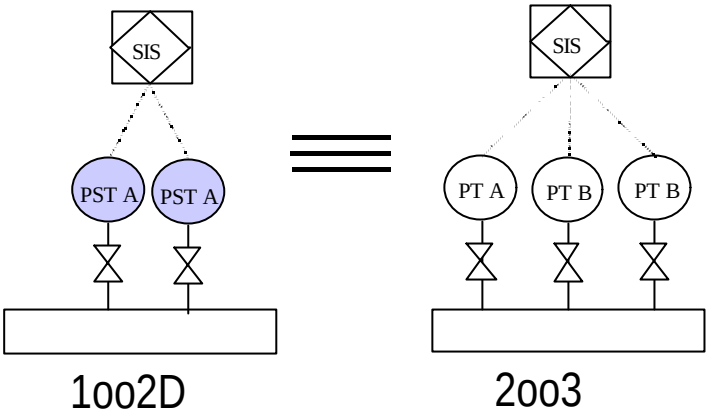


Figure 9. Equivalent safety and availability performance

This configuration provides safety performance superior to the 1oo2 with a superior MTTFs as well. Two safety transmitters provide performance better than three conventional transmitters (Figure 10).

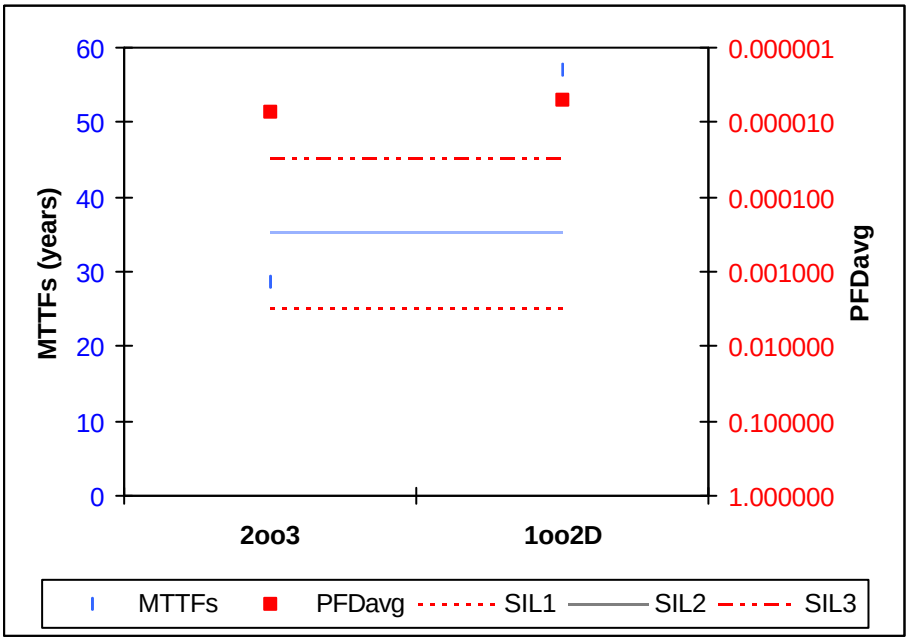


Figure 10. 2oo3 versus 1oo2D

Conclusions

Sensor subsystems must be designed to meet safety performance criteria as required by the target SIL. Given a maximum PFDavg budget, four configurations met the design goal. These included the 1oo2, 2oo3, 1oo1D and 1oo2D. Of these, the 1oo2D had the lowest MTTFs (Fewer false trips). The design rules used to create safety PLCs can be used to build a safety transmitter that can be used in 1oo1D or 1oo2D configurations. These configurations can provide better safety, lower false trip rates and lower system costs.

References

1. HSE Books – The explosion and fires at the Texaco Refinery, Milford Haven, 24 July 994 – ISBN0-7176-1413-1.
2. Draft IEC61508 – Functional Safety of Electrical/Electronic/Programmable Electronic Systems.
3. Goble, W.M. – "*Building Reliable Control Systems*" – INTECH November 1994.
4. Goble, W.M. – "*Using Smart Transmitters in Safety Protection Applications*" – ISA EXPO-98, Houston, Texas.
5. Moore, J. O., *Smart Pressure Sensors for Industrial Applications*, SENSORS Magazine, June 1995, Peterborough, NH