SUOMEN
ATOMITEKNILLINEN
SEURA-

ATOMTEKNISKA
SÄLLSKAPET
I FINLAND r.y.

ATS
YDINTEKNIIKKA

2/93
vol. 22

ATS YDINTEKNIIKKA

2/93, vol. 22

JULKAISIJA Suomen Atomiteknillinen Seura —
Atomtekniska Sällskapet i Finland r.y.

SISÄLTÖ

Kirjapaino Lars Eriksen Oy 1993

DI Antti Piirto on Teollisuuden Voima Oy:n Olkiluodon laitosten käyttötoimiston päällikkö, 938-3815200.

ATS YDINTEKNIIKKA (22) 2/93

Ihminen käytön turvallisuustekijänä

Vuoden 1993 numeroiden teemat ovat:

1/93 Jätteiden käsittely

2/93 Ihminen käytön turvallisuustekijänä

3/93 Varautuminen onnettomuuteen — pelastuspalvelu

4/93 Ekskursio — Keski-Eurooppa

Vuosikerran tilaushinta muilta kuin ATS:n jäseniltä: 200 mk

Ilmoitushinnat: 1/1 sivua 2000 mk
1/2 sivua 1400 mk
1/3 sivua 1000 mk

Toimituksen osoite:
ATS Ydintekniikka
c/o Olli Nevander
IVO International Oy
01019 IVO Rajatorpantie 8
p. 90-508 2613 (suora)
telefax 90-508 3404

ISSN-0356-0473

Antti Piirto, TVO

Ydinvoimalaitos suunnitellaan siten, että käyttötoiminnassa saa tapahtua inhimillisiä virheitä ilman vakavia seurauksia ympäristön turvallisuuden kannalta. Laitoksen monet, toimintaperiaatteeltaan erilaiset suojausjärjestelmät eliminoivat tehokkaasti virheiden vaikutukset. Taloudellisia menetyksiä virheet voivat aiheuttaa mutta turvallisuus on taattu.

Suomen ydinvoimalaitokset on rakennettu 1970-luvulla silloisten tiukkojen suunnitteluperiaatteiden mukaisesti. Turvallisuusajattelussa sittemmin tapahtunut kehitys on huomioitu laitoksiin jälkeenpäin tehdyillä muutoksilla. Tekniikan jatkuva kehitys on johtanut siihen, että teknisten vikojen osuus laitoksen käytön aiheuttamasta kokonaisriskistä on pienentynyt verrattuna inhimillisten virheiden osuuteen.

Tapahtuneet suuronnettomuudet (Tshernobyl, Bhopal, Seveso) osoittavat, että niihin liittyy sekä laitevikoja että inhimillisiä virheitä, joiden vuorovaikutus on usein hyvin monimutkainen. Siksi ydinvoimalaitosten käyttöturvallisuuden parantamistoimissa on tärkeää panostaa inhimillisten virheiden tutkimukseen ja kehittää menetelmiä inhimillisistä virheistä aiheutuvien riskien hallitsemiseksi. Tällöin olisi tarkasteltava inhimillistä toimintaa sekä yksilötasolla eli ydinvoimalaitoksen valvomossa että yleisellä tasolla eli laitoksen käyttöorganisaatiossa.

Ydinvoimalaitosten käyttökertoimet Suomessa ovat olleet varsin hyviä kansainvälisestikin katsoen. Käyttökertoimeen vaikuttaa laitoksen tekniikan ohella käyttöorganisaatio omalla toiminnallaan. Tämän toiminnan laadun mittariksi ei kuitenkaan käyttökerroin ole riittävä. Täytyisi kehittää sellaisia mittausjärjestelmiä, joilla inhimillinen toiminta voidaan paremmin kvantifioida, jotta sen parantaminen mittaustulosten perusteella olisi suunnitelmallisempaa.

Ydinvoimalaitoksen käytössä on tärkeää, että saavutetaan mahdollisimman suuri hyöty ihmisten kyvystä vaikuttaa positiivisesti käyttöturvallisuuteen. Tämä edellyttää henkilöstöltä oikeaa asennetta ja halua kehittää toimintaa jatkuvasti paremmaksi. Erityisen tärkeätä on, että työtä lähinnä olevat ihmiset, työntekijät ja työnjohtajat noudattavat omassa työssään periaatteita, jotka takaavat työn korkean laadun. Omien laitoksien käytöstä saatua kokemuspohjaa tulee pyrkiä laajentamaan tutkimalla muiden laitosten käyttökokemuksia ja ottamalla oppia niistä. Tavoitteena olkoon kaikkien laitoksen käyttöön liittyvien poikkeamien ja häiriöiden poistaminen.

Jukka Laaksonen

TURVALLISUUS TUKEVAMMAKSI KULTTUURIA KEHITTÄMÄLLÄ

Entisessä Neuvostoliitossa tehdyissä Tshernobylin onnettomuuden jälkiselvittelyissä on onnettomuuden perussyyksi tarjottu eri ajankohtina erilaisia asioita. Aluksi syytettiin laitoksen henkilöstöä ja tehtiin luetteloita onnettomuutta edeltäneistä väärinkäytöksistä. Myöhemmin syyttävät sormet ovat kääntyneet vaarallisen reaktorin suunnittelijoiden suuntaan. Samaan aikaan on syytetty niitä, jotka tiesivät reaktoriin liittyneet poikkeukselliset riskit, mutta eivät toimineet korjausten aikaansaamiseksi.

Wienissä syyskuussa 1986 suuren Tshernobyl-kokouksen jälkeen kokoontunut INSAG-asiantuntijaryhmä osui naulan kantaan todetessaan, että onnettomuuden tärkein syy oli puuttuva turvallisuuskulttuuri. Tämä INSAG:n luoma käsite kuvaa yhdellä sanalla sen, mistä kaikki muut onnettomuuteen johtaneet tekijät olivat luonnollista seurausta.

Turvallisuuskulttuurin puute oli niin leimallista Neuvostoliitossa kehitetylle ydintekniikalle, että käsitteen sisältö oli Tshernobyl-onnettomuuden yhteydessä helppo mieltää. INSAG-ryhmän piirissä havaittiin kuitenkin, että turvallisuuskulttuurin tarkempi määrittely tarjoaa missä tahansa maassa tehokkaan keinon turvallisuuteen vaikuttavien toimintojen arviointiin ja järjestelmälliseen kehittämiseen. Turvallisuuskulttuurin perusajatuksia otettiin aluksi mukaan vuonna 1988 julkaistuun IAEA:n raporttiin INSAG-3, Basic Safety Principles for Nuclear Power Plants, ja laaja esitys sen eri puolista koottiin vuonna 1991 julkaistuun IAEA:n raporttiin INSAG-4, Safety Culture.

Suomalaiset ensimmäisiä soveltajia

Suomalaiset olivat mukana INSAG-työssä, ja sen vuoksi turvallisuuskulttuurin perusajatuksia voitiin tuoda tänne samassa tahdissa kuin ne maailmalla kehittyivät. Jo helmikuussa 1991 säädettiin valtioneuvoston päätöksessä ydinvoimalaitosten turvallisuutta koskevista yleisistä määräyksistä seuraavaa:

4§ Turvallisuuskulttuuri

Ydinvoimalaitosta suunniteltaessa, rakennettaessa ja käytettäessä on ylläpidettävä kehittynyttä turvallisuuskulttuuria, joka perustuu asianomaisten organisaatioiden ylimmän johdon turvallisuutta korostavaan asenteeseen ja henkilöstön motivointiin vastuuntuntoiseen työskentelyyn. Tämä edellyttää hyvin järjestettyjä työolosuhteita ja avointa työilmapiiriä sekä valppauden ja aloitteellisuuden edistämistä turvallisuutta vaarantavien tekijöiden havaitsemiseksi ja poistamiseksi.

Vuoden 1991 keväällä alettiin turvallisuuskulttuurin käsitettä tehdä tutuksi suomalaisille ydinenergian käyttäjille. Molemmilla ydinvoimalaitoksilla pidettiin koulutustilaisuudet, joihin osallistui pääosa ao. laitosten insinöörikuntaa ja lisäksi muuta voimayhtiöiden henkilöstöä. Tarkoitus oli tuoda suomalaiseen ydinenergian käyttöön uusia näkemyksiä, joiden pohjalta voitaisiin torjua hyvien käyttökokemusten myötä helposti syntyvää itsetyytyväisyyttä ja osoittaa kehittämiskohteita turvallisuuden varmentamiseksi entistä paremmin. Turvallisuuskulttuuriin keskityttiin lähinnä voimayhtiöiden kannalta, samassa hengessä kuin edellä siteerattu valtioneuvoston päätös.

Valtioneuvoston päätökseen liittyen STUK teki vuonna 1991 kirjallisen arvion kummankin voimayhtiön turvallisuuskulttuurista ja toimitti sen tiedoksi voimayhtiöiden johdolle. Yleisarvio valtioneuvoston päätöksen toteutumista ajatellen oli myönteinen, mutta varaa parantamiseen todettiin olevan monessa asiassa.

Valtiovallan tarjoama kasvualusta välttämätön

Vaikka valtioneuvoston päätös ja sen jälkeen Suomessa tehdyt toimet ovat korostaneet voimayhtiöiden roolia turvallisuuskulttuurin luomisessa, eivät voimayhtiöt voi yksinään saada aikaan haluttuja tuloksia. Kehittynyt turvallisuuskulttuuri edellyttää myös valtiojohdon ja valvontaviranomaisten myötävaikutusta, kuten on konkreettisesti voitu havaita kaikissa Itä-Euroopan maissa. Valtiovallan roolin puntarointi on erityisen tärkeää juuri nyt, kun on pelättävissä, että pitkään jatkunut myönteinen kehitys saattaa yleisen ydinvoimavastaisuuden seurauksena kääntyä vastakkaiseen suuntaan.

Maan ylimmän johdon tehdessä päätöksen ydinenergian käyttöönotosta sen on otettava huomioon, että päätös merkitsee pitkäaikaista sitoutumista tietyistä toimenpiteistä huolehtimiseen. Sitoutuminen ei saa olla riippuvainen poliittisista suhdanteista tai kullakin hetkellä vallitsevasta mielipideilmastosta. Myöhempien poliittisten päättäjien vastuulla on ydinenergia-alan johdonmukainen tasainen kehitys, sillä kehittynyttä turvallisuuskulttuuria ei voida luoda epävarmuuden ilmapiirin vallitessa. Valtiovallan vastuulla ovat mm.

- ydinenergialainsäädännön riittävyys ja ajanmukaisuus,
- kansalaisten valistaminen ydinenergian käyttöön liittyvistä eduista ja riskeistä,
- toimenpiteet, joilla varmistetaan mahdollisten ydinvahinkojen korvaaminen ja ydinenergian käyttäjien toimesta tapahtuva ydinjätteiden turvallinen loppusijoitus sekä
- riittävien resurssien osoittaminen ydintekniikan alan koulutukseen, turvallisuustutkimukseen, turvallisuusvalvontaan ja kansainväliseen yhteistyöhön.

Lainsäädäntö on Suomessa kiistämättä asianmukaisella tasolla. Ydinenergialaissa määritellään selvästi ydinenergian käyttöön osallistuvien organisaatioiden tehtävät, vastuut ja oikeudet. Lainsäädäntö määrittelee myös yksityiskohtaisesti ydinlaitosten luvituskäytännön ja tarjoaa turvallisuutta valvovalle viranomaiselle riittävät toimintaedellytykset, mukaanlukien säännöstön kehittämismahdollisuuden.

Kansalaisten valistamisen yhteiskunnassa vallitsevien aiheettomien pelkojen poistamiseksi pitäisi kuulua valtiovallan yleisiin tehtäviin. Ydinenergia on erityisen vaikea tiedotusasia, koska sen suhteen on liikkeellä paljon huhun tasoista selkeästi virheellistä tietoa. Valtiovallan piirissä ei kuitenkaan tunnuta tiedostetun tähän asiaan liittyvää vastuuta: poliittiset päättäjät eivät ole selkeästi perustelleet päätöksiä, joiden nojalla ydinenergiaa käytetään, eivätkä he ole osoittaneet yleistä ydinenergiavalistusta luotettavaksi koettavan asiantuntijaorganisaation tehtäväksi. Tässä suhteessa meillä olisi paljon opittavaa esimerkiksi Ranskasta.

Ydinvahinkojen korvaamiseen liittyvät vastuukysymykset odottavat edelleen selkeitä valtiovallan kannanottoja. Vaikka nykyiset vastuujärjestelyt ovatkin yleisen eurooppalaisen käytännönmukaiset, on vastuulle asetettu yläraja, joka jättää tilaa aiheelliselle kritiikille.

Ydinjätteiden turvallisen loppusijoituksen suhteen valtiovallan toiminta on ollut tu-

loksekasta. Tarvittavat resurssit kerätään lakisääteisen ydinjäterahaston avulla. Loppusijoituksen turvallisuutta selvitetään laajalla tutkimustoiminnalla. Konkreettiset toimet on jo aloitettu matala- ja keskiaktiivisten jätteiden loppusijoittamiseksi, ja korkea-aktiivisten jätteiden kohdalla on edetty suunnitelmallisesti kohti päätöksiä.

Resursseja ydinenergialle välttämättömän infrastruktuurin kehittämiseen ja ylläpitoon on Suomessa käytetty kohtuullisen paljon. Tulevaisuutta ajatellen ovat kuitenkin koulutus ja tutkimus vaaravyöhykkeessä. Vaarojen torjumiseksi tulee päättäjille viestittää kaikilta tahoilta selkeästi, että supistuksia infrastruktuuriin ei pidä tehdä niin kauan kuin ydinenergiaa maassamme käytetään.

Valvontaviranomaisen asenteet vaikuttavat kehitykseen

Valvontaviranomaisen asenteella ja toimintatavoilla on keskeinen vaikutus kansallisen turvallisuuskulttuurin muotoutumiseen. Valvojan roolissaan viranomaisen pitää luonnollisesti tinkimättä todentaa, että turvallisuuden varmistamiseksi tarpeelliset toimenpiteet tulevat tehdyiksi ja että esiin tulevat ongelmat selvitetään ottamatta ennakoimattomia riskejä. Samalla viranomaisen on kuitenkin asennoiduttava siten, että ydinenergian käyttäjillä on jakamaton vastuu turvallisuudesta. Vastuun kantamiseksi käyttäjille on turvattava mahdollisuus tehdä itsenäisesti teknisiä ratkaisuja ja käytännön toimia koskevat päätöksensä. Viranomaisen toimet eivät saa vähentää käyttäjien motivaatiota ja vastuuntunnetta turvallisuusasioiden hoitamisessa.

Kansallisen turvallisuuskulttuurin edistämiseksi säteilyturvakeskuksessa on korostettu erityisesti:

— johdonmukaisen ja ennustettavan toiminnan tärkeyttä,
— avoimia luottamukseen perustuvia suhteita voimayhtiöihin ja
— ydinturvallisuutta koskevan uusimman tiedon tehokasta välittämistä kaikkien alalla työskentelevien kesken.

Johdonmukainen käyttäytyminen edellyttää, että päätöksenteko pohjautuu vastaavissa asioissa aikaisemmin muodostettuihin kannanottoihin. Kanssakäymisessä voimayhtiöihin tulee noudattaa vakiintuneita muotoja, ja päätökset perusteineen tulee rekisteröidä ja tallentaa, vaikka päätöksiä valmistettaessa pidettäisiin vilkkaastikin epämuodollisia yhteyksiä organisaatioiden välillä. Johdonmukaisuus edellyttää myös sitä, että vaatimukset ja hyväksymiskriteerit ovat voimayhtiön tiedossa jo asioiden suunnitteluvaiheessa. Vaatimustasoa ei pidä muuttaa, ellei siihen ole selvää syytä kuten esimerkiksi uutta tietämystä turvallisuustekijöistä tai valtiovallan taholta asetettuja aiempaa ankarampia turvallisuustavoitteita.

Avoimien suhteiden ja luottamuksen ylläpito edellyttää valvontaviranomaisen puolelta sitä, että viranomaisella on kaikissa asioissa riittävä tekninen tietämys ja että päätökset pystytään perustelemaan erityisesti siinä tapauksessa, että ne eivät vastaa voimayhtiön esitystä. Kiistanalaisissa kysymyksissä viranomaisella pitää olla valmius asian laajempaan käsittelyyn.

Vaatimuksiin liittyviä aikarajoja asetettaessa on varmistuttava niiden realistisuudesta, jotta ei kiireen vuoksi heikennettäisi lopputulosta. Ellei riittävää aikaa voida lisääntyneen (tai aiemmin arvioitua suuremmaksi todetun) riskin vuoksi myöntää, on riski eliminoitava toiminnan keskeyttämisellä.

Voimayhtiön työmoraalin ylläpitämiseksi viranomaisen tulee omalta osaltaan huolehtia siitä, että tarkastustoimintaan ja päätöksentekoon tarvittava henkilöstö on kaikkina aikoina käytettävissä.

Ydinturvallisuutta koskevan tiedon välittämisessä viranomainen on avainasemassa, koska sillä on kiinteät suhteet keskeisiin kotimaisiin ja ulkomaisiin organisaatioihin. Tästä syystä viranomaisella on velvollisuus organisoida mahdollisimman hyvä tiedon kulku kaikkiin suuntiin.

Vaikutukset näkyvät voimayhtiöiden toiminnassa

Turvallisuuskulttuurin ilmentyminen voimayhtiöiden toiminnassa on hyvin monimuotoista, enkä yritäkään käsitellä sitä kattavasti tässä yhteydessä. Sen sijaan tyydyn tuomaan esille muutamia tekijöitä, jotka havaintojeni mukaan ovat edelleen hyvin erilaisella tasolla läntisessä ja itäisessä Euroopassa. Monilla läntisillä laitoksilla mainitut seikat ovat toteutuneet kohtalaisen hyvin, mutta itäisillä laitoksilla tarve muutoksiin on vielä suuri.

Ydinenergiaa käyttävien voimayhtiöiden toiminnassa on välttämätöntä tiedostaa täysi vastuu turvallisuuden ylläpidosta. Korkean turvallisuuskulttuurin vallitessa tämä tietoisuus heijastuu kaikessa päätöksenteossa ja jokaisen yksilön työssä.

Pyrkimys parhaaseen mahdolliseen suoritukseen, sen sijaan että tyydyttäisiin annettujen sääntöjen ja vaatimusten täyttämiseen, on korkeaan turvallisuuskulttuuriin kuuluva itsestään selvyys. Tämä merkitsee käyttäjien itse asettamia kunnianhimoisia tavoitteita ja valmiutta riittäviin investointeihin tavoitteiden saavuttamiseksi. Investointitason pitää olla sitä luokkaa, että laitteiston kunto säilyy uuden veroisena ja että käytön aikana esiin tulleet ongelmat voidaan poistaa parantaen näin koko laitoksen luotettavuutta ja turvallisuutta. Vastaavasti on tarpeen investoida henkilöstön tietotaidon jatkuvaan parantamiseen.

Investointikyky edellyttää tietenkin tervettä ja vahvaa taloudellista pohjaa. Tästä syntyy linkki korkean käyttökertoimen ja korkean turvallisuuskulttuurin välille, vaikka ajatusta eivät kaikki haluakaan hyväksyä. Positiivinen takaisinkytkentä näiden asioiden välillä on kokemusten mukaan kuitenkin ilmeinen, ja se pakottaa myös viranomaisen harkitsemaan, missä vaiheessa voimayhtiön taloutta rasittavat vaatimukset saattavat johtaa turvallisuuden kannalta kielteisiin seuraamuksiin.

Turvallisuusongelmien avoin käsittely ja poistaminen onnistuu ainoastaan ilmapiirissä, jossa yksilöillä ei ole pelkoa tulla rangaistuksi tahattomasta virheestä ja jossa voimayhtiö voi luottaa siihen, ettei viranomaisen taholla synny ylireaktiota raportoidun vian tai yllättäen tiedostetun turvallisuusriskin seurauksena.

Jatkuva haaste voimalaitosten johdolle on miettiä keinoja, jolla kannustetaan henkilöstön aloitteellisuutta ja vastuuntunnetta. Tämä koskee paitsi omia työtehtäviä myös sellaisia asioita, jotka läheisesti sivuavat asianomaisten omaa toimialuetta tai muuten näkyvät päivittäisessä työssä.

Hyödyllinen käytännön työkalu

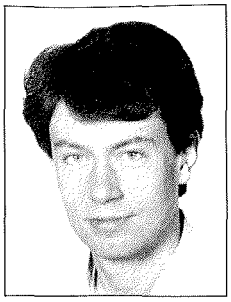
Kansainvälinen Atomienergiajärjestö IAEA on kehittänyt INSAG-raportin pohjalta ohjeiston turvallisuuskulttuurin arviointia varten. Tätä ohjeistoa käsiteltiin kuluvan vuoden huhtikuussa pidetyssä seminaarissa, jonka vetäjinä toimivat IAEA:n edustajat. Osanottajina oli lukuisa joukko suomalaisia voimayhtiöistä, VTT:ltä ja STUK:sta.

Viime aikoina turvallisuuskulttuuriin ja sen osatekijöihin on kiinnitetty yhä lisääntyvää huomiota niin organisaatioiden sisäisissä keskusteluissa kuin myös säteilyturvakeskuksen ja voimayhtiöiden välisessä kanssakäymisessä. Kulttuuritekijät ovat toistuvasti nousseet esille poikkeuksellisten tapahtumien tutkinnassa, ja organisaatioiden johdolle ne ovat osoittaneet, missä vielä voitaisiin pyrkiä suoritustason nostamiseen. Turvallisuuskulttuurin perustuvan ajattelutavan voima onkin juuri siinä, että sen avulla voidaan aina pyrkiä kohti parempaa saavutetusta tasosta riippumatta.

TkL Jukka Laaksonen on Säteilyturvakeskuksen ydinturvallisuusjohtaja, p. 90-7082396.

Pekka Pyy

IHMISEN TOIMINNAN TUTKIMISEN HISTORIA JA NYKYKÄYTÄNNÖT todennäköisyysperustaisen turvallisuus-analyysin kannalta nähtynä



Käytetyt menetelmät eivät aina yksinään selitä saatavien tulosten täydellisyyttä. PSA:n ihmisen toiminnan analyysistä saatava hyöty on loppujen lopuksi suoraan verrannollinen analyysityöhön käytettyyn aikaan ja asiantuntemukseen.

Ihmisen toiminnan luotettavuudelle ja inhimilliselle virheelle on olemassa monia määritelmiä. Saksalainen psykologi Winfried Hacker määrittelee yleisellä tasolla ihmisen toiminnan luotettavaksi, kun toiminta jatkuu laadultaan parhaana mahdollisena ympäristön ja vaatimusten muuttuessa. Ernst Mach puolestaan totesi jo vuosisadan alussa ihmisen toiminnasta suurinpiirtein näin: "onnistuminen ja virhe tulevat samasta lähteestä ja vain ihmisen toiminnnan seurauksien perusteella voidaan erottaa toinen toisesta". Tämä viisaus pätee myös nykyaikana.

INHIMILLINEN VIHRE—HELPPO TEHDÄ, VAIKEA MÄÄRITELLÄ

Luotettavuustekniikassa ihmisen toiminta määritellään oikeaksi tai vääräksi teknisen järjestelmän vasteen kautta. Ihmisen katsotaan tekevän virheen, jos hän ei toteuta tietyn teknisen järjestelmän häiriöttömän toiminnan edellyttämää toimenpidettä annetun onnistumiskriteerin mukaan. Toinen virheen tunnusmerkki on, että ihminen tekee ylimääräisen, haitallisen toimenpiteen.

Todennäköisyysperusteisessa turvallisuusanalyysissä ihmisen toimintaa tarkastellaan nimenomaan tämän luotettavuusteknisen määritelmän pohjalta. Tämä ei kuitenkaan tarkoita sitä, että muiden määritelmien opetuksia ei oteta PSA:ssa huomioon parannustoimenpiteitä suunniteltaessa — päinvastoin.

Jos edellä esitetyt määrittelyt eivät tunnu tarpeeksi kattavilta, jokainen voi yrittää itse määritellä, mitä inhimillinen virhe tarkoittaa. Tähän meillä on myös mahdollisuus, sillä jokainen meistä on tavallaan asiantuntija ihmisen toiminnassa. Ensin tulee kuitenkin pystyä määrittelemään, mitä tarkoittaa oikea ja virheetön toiminta jossain tilanteessa. Koska tehtävä ei ole helppo, kuten Machin edellä lainattu lause kertoo, en aio enää tässä artikkelissa enää käyttää nimitystä inhimillinen virhe. Toinen perustelu kyseisen nimityksen välttämiselle on se negatiivinen sävy, joka väistämättä yhdistetään virheisiin.

Jatkossa käsittelen aihetta PSA:n ihmisen toiminnan luotettavuuden arviointia,

Ihmisen virheet ovat aina olleet osa ihmiskunnan jokapäiväistä elämää. Tässä mielessä aihe ihminen käytön turvallisuustekijänä ei ole mitään uutta. Ihmisen käyttäytyminen on ollut historiassa loputon tutkimuksen aihe ja tulee sitä olemaan myös tulevaisuudessa.

Tämän artikkelin tarkoituksena on tarkastella ihmisen toiminnan tutkimisen historiaa turvallisuusnäkökulmasta. Erityisesti käsitellään todennäköisyysperusteisessa turvallisuustutkimuksessa (PSA) tehtäviä ihmisen toiminnan tarkasteluja. Samalla kuvataan lyhyesti nykyisin käytettäviä menettelyjä ansioineen ja puutteineen.

(HRA = Human Reliability Analysis), puuttumatta ihmisen toiminnan psykologiseen perustaan. HRA:n historian lisäksi esittelen niitä menettelyjä, joiden avulla ihmisen toimintaa tarkastellaan PSA-tutkimuksissa nykypäivänä.

HISTORIA HEIJASTUU NYKYPÄIVÄÄN

Ensimmäisenä järjestelmällisenä menetelmänä ihmisen epätoivottujen toimenpiteiden vähentämiseksi voidaan pitää ammatillista koulutusta ja soveltuvuustestejä. Näistä ammatillisen koulutuksen voidaan katsoa alkaneen 1745 Pennsylvaniassa pidetystä puusepänkurssista, ja nykyaikaisen henkilökunnan soveltuvuustestauksen Galtonin tekemistä aistikokeista 1800-luvun lopulla.

Vasta 1900-luvun alussa ihmisen toimintaa ryhdyttiin tutkimaan tieteellisesti. Tästä ovat esimerkkeinä Gilbrethin tekemä tutkimus turhista työliikkeistä sekä Roethlisbergerin ja Dicksonin tutkimukset valaistuksen määrän vaikutuksesta tehdastuotantoon. Kyseiset tutkimukset olivat suuntautuneita lähinnä käytettävyyden ja työn tehokkuuden parantamiseen.

Asetekniikka edisti tutkimusta

Toisen maailmansodan aikana tehtyjen sotilasteknisten keksintöjen seurauksena syntyi entistä monimutkaisempia ihminen-kone -vuorovaikutuksia. Näin nykyaikaisen ihmisen toiminnan luotettavuuden tutkimuksen voidaan katsoa alkaneen 1940- luvulla. Ensimmäisenä ihmisen virheitä tutkittiin nimenomaan taistelutilanteissa ja sotateollisuudessa, jossa pyrittiin estämään onnettomuuden ohjusten ydinkärkien tuotannossa.

Tutkimuksen siirtäminen siviilielämään ei sujunut nopeasti. Kului noin kymmenen vuotta, ennenkuin teknisten järjestelmien suunnittelussa alettiin järjestelmällisesti ottaa huomioon niitä käyttävä ihminen. Ensimmäinen luotettavuustekninen analyysi, jossa tarkasteltiin myös ihmisen toiminnan vaikutusta, tehtiin 1952 Sandia Laboratories -tutkimuskeskuksessa New Mexicon osavaltiossa Yhdysvalloissa. Tässä analyysissä otettiin huomioon vain ne ihmisen toiminnot, jotka suoraan vaikuttavat laitteiston luotettavuuteen. Jokaisen toiminnon epäonnistumisen todennäköisyyden oletettiin olevan 0,01.

Nykyiset periaatteet 60-luvulta

1960-luvulla ihminen-kone -järjestelmien tutkimus lisääntyi huomattavasti. Esimerkkinä tästä mainittakoon American Institutes for Research -laitoksen tutkimus "An Index of Electronic Equipment Operability", jossa ihmisen toiminta oli jaettu pieniin osatoimintoihin. Niiden todennäköisyysarvot muodostivat AIR Data Store -tietopankin, josta jokaisen ihmisen toiminnon onnistumiselle voitiin laskea todennäköisyys kertomalla alkeistodennäköisyyksiä keskenään. Useat käytössä olevat ihmisen toiminnan onnistumistodennäköisyyden arviointimenetelmät perustuvat tähän ositteluperiaatteeseen.

Samanaikaisesti ihmisen toiminnan onnistumisen todennäköisyyden tutkimuksen myötä kehittyivät myös menetelmät haitallisten toimintojen tai niiden vaikutuksen vähentämiseksi. Koulutuksen ja käyttöohjeiden lisäksi myös työympäristöä alettiin suunnitella vastaamaan paremmin ihmisen toimintaedellytyksiä, ja ensimmäiset ohjeet voimalaitosten valvomoiden suunnittelusta annettiin Yhdysvalloissa vuonna 1960. Kuusikymmentäluvun lopulla — edelleen Yhdysvalloissa - perustettiin lisäksi operaattoreista ja ihmisen toiminnan luotettavuuden asiantuntijoista työryhmä kehittämään ergonomisesti parempia valvomoita.

THERP-menetelmän ensiesittely

Merkittävämpiä tapahtumia ihmisen toiminnan luotettavuuden tutkimuksessa 1960 -luvulla oli kuitenkin Alan D. Swainin THERP-menetelmän esittäminen 1963. Kyseisestä vuodesta lähtien menetelmää on käytetty mallinnettaessa ihmisen toimintaa lukemattomissa turvallisuus- ja käyttövarmuusanalyyseissä ja laskettaessa toiminnan epäonnistumisen todennäköisyyksiä. THERP perustuu alunperin samanlaiselle toiminnan osittelulle kuin AIR- laitoksen menetelmä, mutta siihen on myöhemmin lisätty muun muassa mahdollisuudet käsitellä epäonnistuneiden ihmisen toimintojen korjaamista ja riippuvuuksia eri toimintojen välillä. Sittemmin Swain julkaisi 1983 yhdessä H. Guttmannin kanssa ihmisen toiminnan luotettavuuden arvioinnin raamatun "Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications". Tuskin on olemassa montaa ihmisen toiminnan luotettavuutta käsittelevää julkaisua, jossa ei viitata kyseiseen käsikirjaan.

Ensimmäinen PSA USA:ssa — WASH-1400

Yhdysvalloissa 1970-luvun alussa pyrittiin ensimmäistä kertaa tekemään PSA, jossa otetaan huomioon kaikki mahdolliset onnettomuusketjut seurauksineen. Nuclear Regulatory Commissionin (NRC) vaatimuksesta tehty tutkimus valmistui 1975 nimellä Reactor Safety Study, mutta se tunnetaan paremmin nimellä WASH-1400 tai päävaikuttajansa Norman Rasmussenin mukaan Rasmussenin raportti. Tutkimuksessa käsiteltiin sekä ihmisen toiminnan luotettavuutta että valvomasuunnittelua hyväksikäyttäen etupäässä THERP-menetelmää. Tutkimuksessa esitettiin arvoja valvomossa tehtävien virheiden todennäköisyyksille, mutta samalla todettiin tarvittavan parempia ihmisen toiminnan luotettavuustietoja eri olosuhteille ja tilanteille. Lisäksi huomautettiin ydinvoimalaitosten valvomoiden näyttöjen ja painikkeiden järjestelyjen olevan yleensä erittäin huonoja verrattuna puolustusjärjestelmien vastaaviin kohteisiin.

WASH-1400 -raportin aiheuttaman kohun vuoksi NRC asetti ryhmän arvioimaan tutkimuksen tuloksia. Tämän arvioinnin tulokset tunnetaan Lewisin raporttina, ja siinä todetaan ihmisen olevan tärkeä tekijä useissa WASH-1400 luotettavuusmalleissa. Lewisin raportissa korostetaan järjestelmävikojen todennäköisyyksien riippuvuutta laitoksen henkilökunnan toiminnan epäonnistumisen todennäköisyydestä. Lisäksi Lewisin raportti pitää tärkeänä ihmisen asemaa myös laitevioista aiheutuvia vaaratilanteita estävänä sekä niiden seurauksia lieventävänä tekijänä.

Historiaa myös USA:n ulkopuolella

Tämä historiakatsaus on painottunut toistaiseksi Yhdysvaltoihin, koska PSA ja ihmisen toiminnan luotettavuuden arviointimenettelyt kehitettiin siellä. Erityisesti Three Mile Islandin ydinvoimalaitoksessa 1979 tapahtuneen häiriön seurauksena, jossa henkilökunta tunnisti häiriötilanteen väärin, myös Euroopassa on tehty paljon ihminen-tekniikka -vuorovaikutuksen kehittämiseksi. Tunnetumpia vaikuttajia on ollut englantilainen David Embrey, joka on kehittänyt subjektiivisiin arvioihin perustuvaa SLIM-menettelyä. Electricite de France on käyttänyt paljon simulaattoreita pyrittäessä arvioimaan henkilökunnan toimintaa onnettomuustilanteissa. Tanskalainen Jens Rasmussen ja englantilainen James Reason ovat puolestaan kehittaneet ihmisen toiminnan luokitteluja muita tarkoitusperiä varten, mutta heidän periaatteitaan on käytetty myös PSA- tutkimuksissa. Suomessa tehtyä työtä esitellään muissa tämän lehden artikkeleissa.

Ihmisen toiminta—aina onnettomuuden taustalla

Kehitys on aikaansaanut teollisia prosesseja, jotka normaaliolosuhteissa kohottavat ihmiskunnan elintasoa huomattavasti. Toisaalta niiden häiriöissä ihmisen toiminta yhdistyneinä teknisiin vikoihin ja harvinaislaatuisiin tekijöihin saattaa vaarantaa myös muut kuin laitoksella työskentelevät. Lisäksi voi seurata suuria taloudellisia menetyksiä ja kärsimyksiä.

Tästä meille ovat ikävinä muistoina jo ehkä liiankin usein eri yhteyksissä mainitut Tsernobylin, Bhopalin ja Flixboroughin onnettomuudet. Kaksi viimeksi mainittua ovat prosessiteollisuuden laitoksia, mutta onnettomuuksien syntymiseen vaikuttaneet tekijät ovat yhteistä omaisuutta, joista voidaan oppia. Oppia voidaan myös PSA-tutkimuksista. Niissä on alusta alkaen—ja yhä kasvavassa määrin—kiinnitetty huomiota turvallisuuden kannalta oleellisen ihmisen toiminnan tunnistamiseen, mallintamiseen ja todennäköisyyden arviointiin kaikissa ydinvoimalaitoksen käyttötiloissa latausseisokista tehokäyttöön.

IHMISEN TOIMINNAN TUTKIMUS PSA:SSA

PSA:n ihmisen toiminnan analyysin eli HRA:n tarkoituksena on parantaa riskimalleina käytettävien tapahtuma- ja vikapuumallien kattavuutta siten, että niihin sisällytetään myös ihmisen toiminnan vaikutus. Tätä tarkoitusta varten merkittävät ihmisen toiminot on tunnistettava, niiden vaikutus on mallinnettava ja lopuksi niiden todennäköisyyttä tulee arvioida. PSA:n ihmisen toiminnan analyysin tarkoituksena ei ole syvällinen psykologisten mekanismien käsittely, mutta ihmisen toiminnan perusteiden ymmärtäminen on eduksi myös PSA-työskentelyssä ja parannustoimnepiteiden suunnittelussa.

Luokittelu

Ihmisen toiminnan järkevä luokittelu auttaa tunnistamistyötä merkittävästi. Eräs tapa luokitella toiminnot on tarkastella niiden ajallista sijoittumista riskimallien alkutapahtumaan verrattuna. Usein käy-

→

tetään seuraavaa luokittelua: epäkäytettävyyttä aiheuttavat ihmisen toiminnot, jotka sijoittuvat ajallisesti ennen alkutapahtumaa; alkutapahtuman aiheuttavat ihmisen toiminnot ja alkutapahtuman jälkeiset ydinvoimalaitoksen turvallisuustoimintoihin vaikuttavat ihmisen toiminnot. Alkutapahtumalla tarkoitetaan tällöin poikkeamaa, joka vie laitoksen epäturvalliseen tilaan vaikuttamalla johonkin sen turvallisuustoimintoon.

PSA:n kannalta tärkeät ihmisen toiminnot tunnistetaan yleensä järjestelmien ja alkutapahtumien aiheuttaman laitosvasteen mallintamisen yhteydessä. Tunnistamistyössä käytetään hyväksi turvallisuusjärjestelmien ja niiden apujärjestelmien toimintaan liittyviä käyttö-,huolto-, koestus- ja hätätilanneohjeita. Erityisesti pyritään tunnistamaan jonkin ihmisen toimenpiteen (tai koko ohjeen kohdan) puuttumisen tai väärien toimenpiteiden mahdollisia vaikutuksia prosessiin.

Suorituksen läpikäyminen: tunnistetaan tärkeät toimenpiteet

Turvallisuusjärjestelmien epäkäytettävyyttä aiheuttavia toimenpiteitä voidaan tunnistaa parhaiten tarkastelemalla huoltoja koestusohjeita. On luonnollisesti olemassa myös toimenpiteitä, joiden suorittamista varten ei ole olemassa kirjallista ohjetta. Tällöin tunnistustyö tehdään tarkastelemalla toimenpiteen normaalia suoritustapaa. Kokemuksen mukaan on suositeltavaa täydentää tunnistamistyötä aina käymällä paikan päällä tutustumassa kohteeseen.

Alkutapahtumien aiheuttajina ihmisen toimenpiteet ovat yksi ryhmä muiden alkutapahtuman aiheuttajien joukossa. Näinollen niitä voidaan tunnistaa tarkastelemalla kyseisen alkutapahtuman kaikkia mahdollisia syitä ja käyttämällä lisäksi hyväksi laitoksen ohjeistoa.

Alkutapahtuman jälkeiset toimenpiteet

Alkutapahtuman jälkeen ihmisen toiminta voi edesauttaa laitoksen tilan vakiinnuttamista—mutta myös väärien toimenpiteiden kautta pahentaa tilannetta. PSA:n riskimallien tapahtumaketjuissa esiintyy yleensä toimenpiteitä, jotka ovat luonteeltaan käsin tehtäviä (esimerkiksi jonkin turvallisuusjärjestelmän käsikäynnistys), automaattisesti käynnistyvää turvallisuustoimintoa varmentavia (esimerkiksi käsikäynnistys turvallisuusjärjestelmän automaattisen käynnistyksen epäonnistuttua) tai toimintoja, jotka edellyttävät laitoksen järjestelmien kytkentöjen merkittävää muutosta (esimerkiksi häiriötilanteessa syöttöveden toimittaminen muista kuin turvallisuusjärjestelmistä).

Häiriö- ja hätätilanneohjeita voidaan yleensä aina käyttää häiriöketjujen aikaisten tärkeiden ihmisen toimintojen tunnistamisen ja mallintamisen apuna. Koulutussimulaattori on myös tehokas apuväline eri virhemahdollisuuksien tunnistamisessa. Poikkeuksena tästä säännöstä ovat seisokit, joiden olosuhteita simulaattorin mallit ja hätätilanneohjeet eivät yleensä kata täydellisesti.

SANO SE NUMEROIN

Kun tärkeät ihmisen toiminnot on tunnistettu, toiminnoista ja niihin vaikuttavista tekijöistä laaditaan yleensä HRA:n todennäköisyysarviointia varten malli. Joskus tarvitaan laaja vuorovaikutuksia ja riippuvuuksia kuvaava malli, joskus taas asiantuntijoiden antama subjektiivinen todennäköisyysarvio voi olla riittävä. Omalta laitokselta kerätyt käyttö-, koestus- ja kunnossapitokokemukset ovat kuitenkin ensisijainen tietolähde, jota tulee käyttää myös ihmisen toiminnan onnistumisen todennäköisyyttä määritettäessä. Toisella sijalla soveltuvuudessa on omalta laitossimulaattorilta saatava kokeellinen tieto.

Kun ihmisen toimintojen sisäinen rakenne on mallinnettu HRA:ssa riittävän tarkasti, ja niiden todennäköisyys on määritetty, toiminnot sijoitetaan PSA:n riskimalleihin normaaleina perustapahtumina. Joissain tapauksissa mallinnetaan myös ihmisen toiminnan aiheuttamia riippuvuuksia. HRA ei ole siis mikään itsestarkoitus, vaan sen on kyettävä antamaan arvoja, joiden avulla kyetään arvioimaan ihmisen toimintojen riskivaikutusta yhdessä teknisempien tekijöiden kanssa.

PSF- ja osatoimintomallit

Jos ei käytetä suoraan todennäköisyysarvioina laitokselta kerättyä historiatietoa tai simulaattorikokeiden tuloksia, tietyn ihmisen toiminnon tai toimintokokonaisuuden mallintaminen todennäköisyyden arviointia varten tehdään yleensä: jakamalla ihmisen toiminto osatoimintoihin, tarkastelemalla tärkeimpiä toiminnan onnistumiseen vaikuttavia (niinkutsuttuja PSF-) tekijöitä tai käyttämällä onnistumistodennäköisyyden ja käytettävissä olevan ajan välistä vastaavuutta.

Ihmisen toiminnan jako pienistä osatoiminnoista koostuvaksi loogiseksi malliksi perustuu ajatukseen, että näiden osatoimintojen todennäköisyyden arviointi on helpompaa kuin kokonaisuuden. Tästä loogisesta mallista, joka voi olla esimerkiksi vikapuu tai A. Swainin mallin HRA-puu, lasketaan sitten kokonaistoiminnon onnistumistodennäköisyys. Menettelyn etu on järjestelmällisyys ja yhteensopivuus muun luotettavuusteknillisen käsittelyn kanssa. Menettely pakottaa tutkimaan ihmisen toimintaa yksityiskohtaisesti. Haitta on se, että usein osatoiminnoille ei ole saatavissa niinkään hyviä luotettavuustietoja kuin niiden muodostamalle kokonaisuudelle. Hyvin usein joudutaan käyttämään Swainin käsikirjan yleisiä luotettavuustietoja. Lisäksi menetelmän tuottamissa tuloksissa on esiintynyt kansainvälisissä vertailuissa suuria vaihteluita.

Liian pienien osatoimintojen tarkastelua pyritään välttämään mallintamalla vain tärkeimpien ihmisen toimintaan vaikuttavien tekijöiden vaikutus. Esimerkkeinä näistä PSF-tekijöistä ovat käytettävissä oleva aika, prosessista saatavan vasteen laatu ja tietosisältö, koulutuksen laatu ja määrä sekä käytettävissä olevien toimintaohjeiden laatu. Lyhenne PSF (Performance Shaping Factors) tarkoittaa nimenomaan ihmisen toimintaan vaikuttavia tekijöitä. Menettelyn etu on se, että ihmisen toimintaa ei jaeta liian pieniin palasiin ja että muualta saatuja todennäköisyysestimaatteja voidaan PSF-tekijöiden avulla kalibroida niin, että lopputuloksen voidaan katsoa esittävän oman laitoksen olosuhteita. Haitta on se, että ihmisen eri toiminnoissa PSF-tekijät ovat erilaisia ja tekijöiden väliset riippuvuudet ovat yleensä suuria. Tämä johtuu siitä, että ihmisen toiminta on hyvin paljon edeltävistä tapahtumista ja toimintaympäristöstä riippuvaista.

Kiire vähentää onnistumistodennäköisyyttä

Ihmisen toiminnan onnistumistodennäköisyyden ja toimintaan käytettävissä olevan ajan välillä on todettu olevan selvän vuorovaikutuksen etenkin tilanteissa, joissa aikaa on suhteellisen vähän. Erityisesti valvomovuoron toiminnan onnistumisen vaikeissa häiriötilanteissa on todettu olevan aikariippuvaa. Aika- luotettavuus -vastaavuusmallin voidaan katsoa olevan PSF- mallien erikoistapauksen alkutapahtuman jälkeisessä tilanteessa, jossa häiriön hallintaan käytetävissä oleva aika on selvästi muita tekijöitä merkittävämpi. Mallien etu on yksinkertaisuus ja

-sopivuus simulaattorikokeista saatavan materiaalin kanssa. Suurin haitta on se, että yksinkertaisia aikariippuvuusmalleja käytetään väärin myös sellaisten toimintojen todennäköisyyden arviointiin, joiden tärkein PSF on aivan jokin muu kuin aika.

Swainin käsikirja säilynee alan raamattuna

Mistä sitten löydetään numeroarvoja näihin malleihin, jos niitä ei löydy laitokselta eikä simulaattorilta. Osatoimintoihin jakamiseen perustuvien mallien, joista tunnetuin on Swainin HRA-puu, tärkein luotettavuustietojen lähde on toistaiseksi ollut samaisen Swainin Handbook ja asiantuntijoiden arviot. Jos toiminnot jaetaan hyvin pieniin osatoimintoihin, joihin on mahdotonta kerätä laitoskohtaisia arvoja, Swainin käsikirja säilyttänee asemansa myös tulevaisuudessa.

PSF-mallit edellyttävät myös asiantuntijoiden arvioita, koska yksittäisen PSF-tekijän (esimerkiksi koulutuksen laadun) vaikutusta todennäköisyyteen on hyvin vaikea määrittää kokeellisesti tai laitoskokemuksen perusteella.

Laitossimulaattori ja asiantuntijat apuvälineinä

Aikariippuvuusmallit eivät välttämättä edellytä kumpaakaan edellä mainituista tietolähteistä, jos käytettävissä on laitoksen oma koulutussimulaattori. Muiden laitosten simulaattoreilta saatujen tulosten käyttöä ilman soveltuvuusarviota ei voida suositella. Täten tilanteessa, jossa simulaattoria ei voida käyttää jäävät taas ainoaksi vaihtoehdoksi asiantuntijoiden arviot.

Malleihin voidaan siis yhdistää asiantuntijoiden arvioita joko osittain tai kokonaan. Joskus hyvän, tapauksen syvällisesti tuntevan asiantuntijan arvio on parempi kuin repullinen keinotekoisesti saatuja todennäköisyysestimaatteja, joten asiantuntemusta ei tule ikinä aliarvioida. Asiantuntijoiden arvioita voidaan kerätä joko vertaamalla tapahtumia pareittain, luokittelemalla niitä, järjestemällä ne todennäkösyyden mukaan tai suoran todennäköisyysarvioinnin avulla.

MIHIN ON TULTU

Tänä vuonna tulee kuluneeksi 30 vuotta THERP-menetelmän esittelystä. Kun kysytään, mitä näinä vuosina on tapahtunut voisi ensimmäinen ajatus olla—ei mitään. Swainin menetelmillä on edelleen kiistaton paikka eniten käytettyjen HRA:n todennäköisyyksien arviointimallien joukossa. Paljon enempää tietoa ihmisen toiminnan onnistumisen ja epäonnistumisen synnystä ei ole saatu sitten Machin aikojen. Onnettomuuksia sattuu edelleen ja suuri osa niistä ihmisen toiminnan ansiosta—itse asiassa kaikki, koska kyseisiä teknisiä järjestelmiä ei olisi olemassa ilman ihmistä.

Lohdutonta, vai mitä? Tämä ei kuitenkaan ole koko totuus. THERP menettely on mekanistisuudestaan huolimatta järjestelmällinen ja korostaa ihmisen toiminnan tarkan analyysin tarvetta. Lisäksi keskusteluilmapiiri on muuttumassa. Olen viime vuosien aikana havainnut, että ihmisen toiminnasta ja sen silloin tällöin sattuvasta epäonnistumisesta on alettu keskustella ilmiönä, jossa ei ole mitään peiteltävää. Enää ei myöskään välttämättä viitata vain 'operaattorin virheeseen', vaan tajutaan, että kyseinen tapahtuma voi pitää sisällään laajempia puutteita ihminen-kone -vuorovaikutuksessa. Nämä puutteet voivat olla peräisin esimerkiksi jo laitoksen suunnittelusta, työtehtävien organisoinnista tai henkilösuhteista.

MENNÄKÖ ORAAKELIN LUO

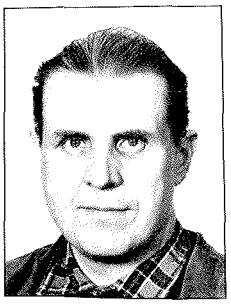
Todennäköisyysarviointi edellyttää tarkkaa tietoa. Yleensä vasta siinä vaiheessa, kun on ryhdyttävä antamaan jollekin ilmiölle numeroarvoja, havaitaan, kuinka vähän siitä itse asiassa tiedetään. Todennäköisyysarvojen löytämiseksi ei ole tavallisesti auttanut muu kuin lähteä penkomaan lisätietoja, mikä ei aina ole ollut helppoa.

Kun Lyydian kuningas Kroisos meni kysymään Delfoin oraakkelilta, kannattaako hänen lähteä taisteluun mahtavaa Persiaa vastaan, oraakkeli vastasi näin: "kun Kroisos ylittää Halys-virran, hän tuhoaa mahtavan valtakunnan". Kuningas päätti siltä seisomalta aloittaa sodan—jonka kuluessa hänen oma rikas valtakuntansa tuhoutui.

Pystyisikö oraakkeli ennustamaan ihmisen toiminnan luotettavuutta ? Ehkä se vastaisi samoin kuin esimerkissä—moniselitteisesti mutta kattavasti. Omasta näkökulmastani katsottuna alan tulevaisuus näyttää sekä hyvältä että huonolta. Hyvältä näyttää sen suhteen, että toivon viime aikoina kehittyneen avoimuuden jatkuvan ja näin lisää tietoa saatavan ihmisen toiminnasta monimutkaisissa teollisuusprosesseissa. Toisaalta tilanne jatkunee huonona, koska toistaiseksi ei ole olemassa keinoja, joilla ihmisen aivotoimintojen mekanismeja pystytään mallintamaan niin, että tuloksena saataisiin todennäköisyyksiä. Aikahan sen sitten näyttää, kuka siihen tulee pystymään, jos vaikka oraakkeli kertoisi...

TkL Pekka Pyy työskentelee VTT:n sähkö- ja automaatiotekniikan laboratoriossa tutkijana, p. 90-4566441

Pentti Haapanen



Uusien laitosten ihmisläheinen valvomoautomaatio

Konventionaalisen voima- ja muun prosessiteollisuuden valvomot ovat viimeisen kymmenen vuoden aikana kokeneet täydellisen muodonmuutoksen. Analogia- ja binääritekniikkaan perustuvista yksittäisinstrumenteista on siirrytty digitaalitekniikkaan ja videovalvomoihin. Korkeiden turvallisuusvaatimusten takia siirtyminen uuteen tekniikkaan on ydinvoimaloissa ollut hitaampaa. Muutos on alkanut prosessin valvontatehtävistä, joissa prosessitietokoneen näytöillä jo on merkittävä asema mm. molemmilla suomalaisilla laitoksilla. Uusilla laitoksilla otetaan käyttöön digitaaliset automaatiojärjestelmät, ja myös operaattorin ohjaustoimenpiteet tullaan suorittamaan automaatiojärjestelmän näyttöjen kautta. Erilaiset tietokonepohjaiset operoinnin tukivälineet tulevat myös edelleen lisääntymään. Tietokone- ja näyttötekniikkojen täysi hyödyntäminen voi pienentää merkittävästi käyttöhenkilökunnan inhimillisten virheiden riskiä.

Laajan ja monimutkaisen ydinvoimalaitosprosessin valvonta ja ohjaus edellyttävät kuhunkin käyttötilanteeseen oleellisesti liittyvän laitoksen tilaa, käyttöehtoja, suunnittelutietoja, ohjeita yms. koskevan tiedon seulomista suuresta tietomäärästä. Digitaalitekniikkaan perustuvassa videovalvomossa tiedon valintaa, strukturointia ja esitystä voidaan huomattavasti tehostaa ja näin avustaa operaattoreita ongelmatilanteiden diagnostisoinnissa sekä ohjaustoimenpiteiden suunnittelussa ja suorittamisessa. Vuoron sisäinen ja vuorojen välinen kommunikointi tehostuu digitaalitekniikkaan siirryttäessä. Edelleen digitaalitekniikka parantaa tiedonsiirtoa laitoksen johdon, kunnossapitohenkilökunnan sekä erilaisten teknisten tukikeskusten ja varaohjauspaikkojen ja valvomon välillä.

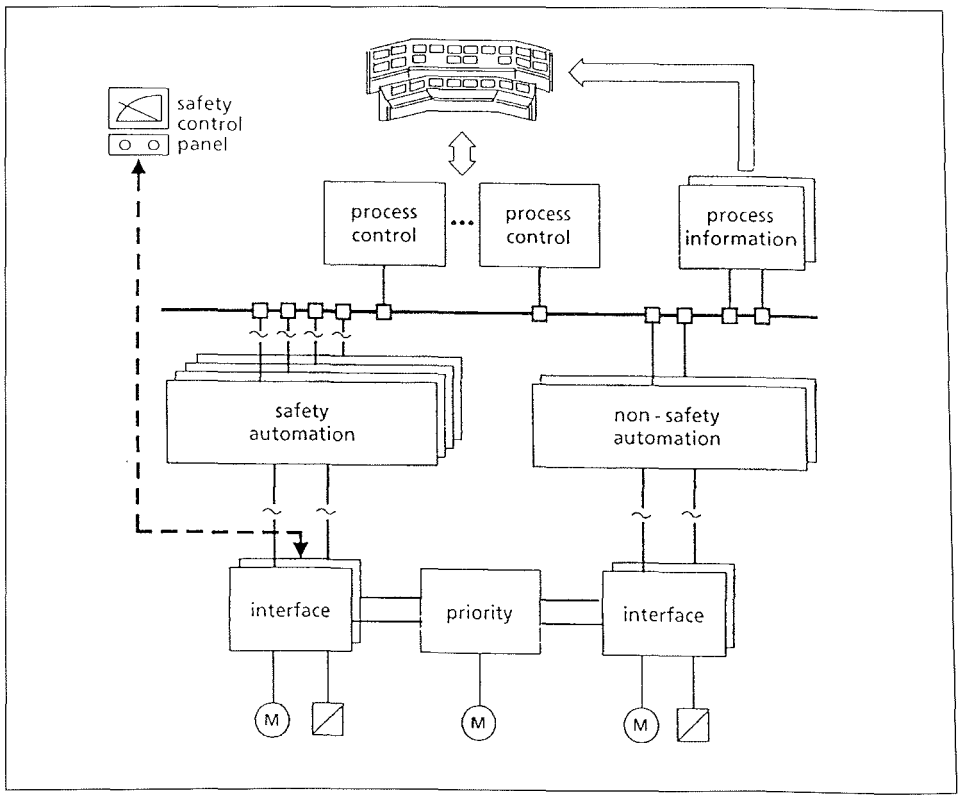
Jokaisella potentiaalisella laitostoimittajalla on hieman toisistaan poikkeavat automaatio- ja valvomokonseptinsa. Seuraavassa ei kuvata minkään yksittäisen toimittajan konsepteja, vaan hahmotellaan niitä yleisiä piirteitä, jotka jossain muodossa sisältyvät eri konsepteihin.

Automaatiokonsepti

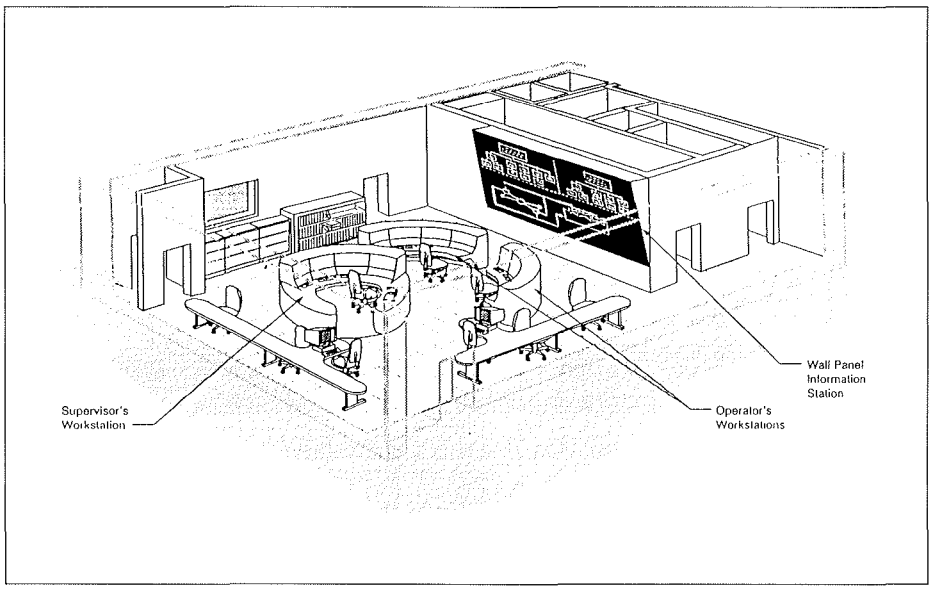
Uuden laitoksen automaatiojärjestelmä muodostuu digitaalitekniikalla toteutetuista käyttö- ja turvallisuusautomaatiojärjestelmistä, jotka turvallisuussyistä on erotettu toisistaan fyysisesti ja toiminnallisesti. Konseptiin kuuluu edelleen erillinen informaatiojärjestelmä ("prosessitietokone"), jonka avulla laitoksen ja automaatiojärjestelmien tilaa koskevaa tietoa voidaan jalostaa ja yhdistää muuhun laitoksen suunnittelua, käyttöä ja ohjeistusta koskevaan tietoon ja esittää se operaattorin kulloistakin työtehtävää parhaiten tukevalla tavalla. Automaatiojärjestelmän suorituskyvyn kasvaessa informaatiojärjestelmän toimintoja tultaneen tulevaisuudessa yhä enemmän siirtämään automaatiojärjestelmän sisälle. Joitakin laitoksen turvallisuuden kannalta keskeisiä valvonta- ja ohjaustoimintoja jouduttaneen lisäksi varmistamaan konventionaalisilla kiinteästi langoitetuilla varajärjestelmillä, joiden avulla keskeisten turvallisuusparametrien tilaa voidaan valvoa ja laitos ajaa valvomosta ja varaohjauspaikalta turvalliseen tilaan.

Valvomon layout

Valvomo koostuu pelkistetyimmillään operaattorien työasemista ja prosessin tilan yleisnäytöstä. Tämän lisäksi valvomossa voi olla erillinen turvallisuusjärjes-

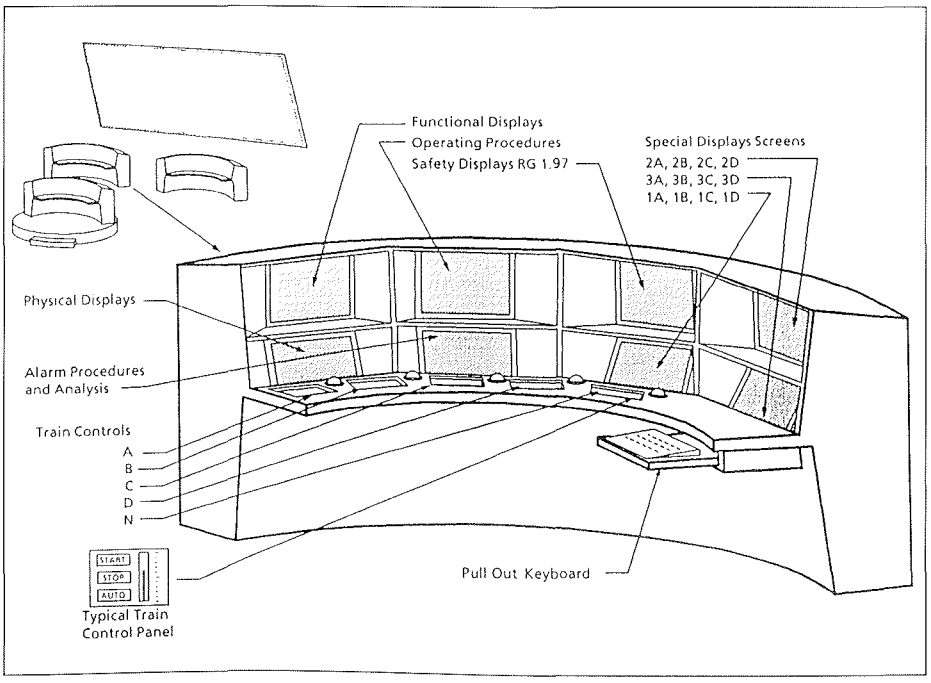


Ydinvoimalaitoksen automaatiojärjestelmän arkkitehtuuri.



Westinghousen AP600-laitoksen valvomon lay-out.

telmän työasema tai paneeli sekä kiinteästi langoitetun varaohjausjärjestelmän paneeli. Operaattorin työasemien määrä vaihtelee eri konsepteissa; tavallinen ratkaisu on omat työasemat kullekin vakiomiehitykseen kuuluvalle operaattorille (esim. 2 kpl) ja vuoropäällikölle. Työasemaan on keskitetty automaatiojärjestelmän näytöt ja ohjaukset sekä informaatiojärjestelmän näytöt. Näytöillä esitetään prosessin tila erilaisten prosessikaavioiden, logiikkakaavioiden ja hälytyslistojen avulla. Informaatiojärjestelmä esittää operaattoreille pitemmälle jalostettua tietoa ja sen avulla toteutetaan erilaisia tukitoimintoja. Sen kautta päästään myös käsiksi laitoksen käyttöhistoriaan ja erilaisiin johdon ja kunnossapidon tietokantoihin ja voidaan saada ennusteita prosessin tilan kehittymisestä.



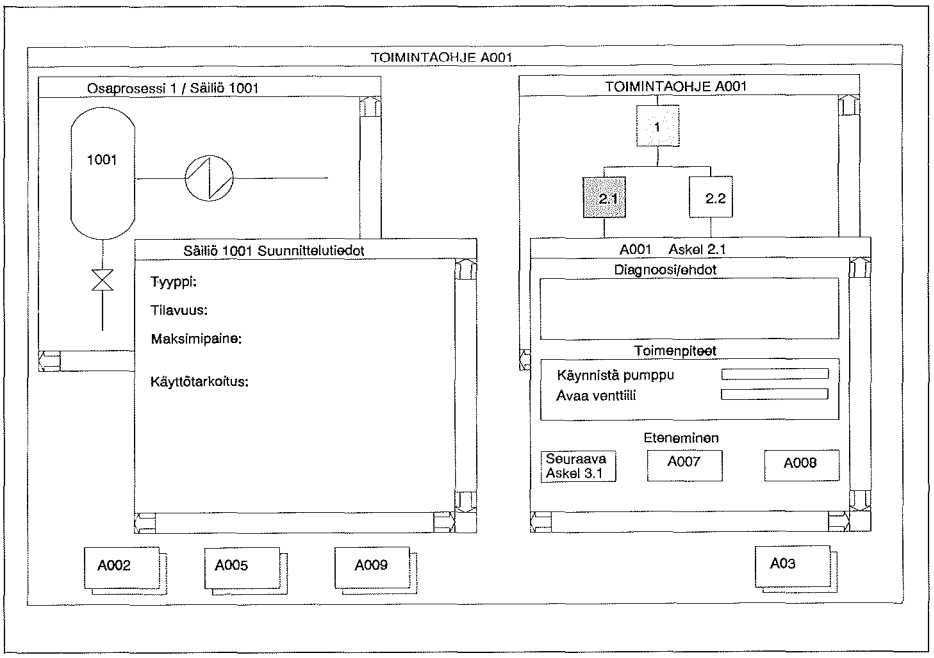
Operaattorin työasema AP600-laitoksen valvomossa.

Operaattorin työaseman näytöiltä voidaan parhaimmillaankin nähdä vain rajoitettu osa prosessin kokonaistilanteesta; tämän vuoksi valvomossa on iso prosessin tilan yleisnäyttö, jolta koko vuoro voi yhdellä silmäyksellä ja yhdessä havaita prosessin kokonaistilanteen. Yleisnäyttö on toistaiseksi tavallisesti toteutettu kiinteällä prosessikaaviolla, lampuilla ja joillakin yksittäisillä tärkeimpien suureiden arvoja näyttävillä indikaattoreilla. Lähitulevaisuudessa suurkuvanäytöillä toteutetut tietokoneohjatut yleisnäytöt kuitenkin tullevat korvaamaan nämä.

Näytöt ja ohjaukset

Katodisädeputki (CRT) on toistaiseksi yleisimmin käytetty näyttötekniikka valvomoissa. Sen hyviä puolia ovat kuvan hyvä kirkkaus ja terävyys, hyvät värit ja korkea luotettavuus. Haittapuolia ovat suuri tilantarve sekä näytön koon kasvaessa jyrkästi nouseva hinta. Muita käytettyjä tekniikkoja ovat mm. plasma- ja nestekidenäytöt. Aivan viime aikoihin asti nämä ovat olleet yksivärisiä ja pienikokoisia, ja esim. nestekidenäytön kirkkaus on vaatimatonta tasoa. Nämä tekniikat kuitenkin kehittyvät nopeasti ja esim. nestekidetekniikkaan perustuvia suurkuvanäyttöjä on tulossa markkinoille. Myös erilaisia videotykkejä on käytetty suurkuvanäyttöjen luomiseen.

Ohjausten suoritus tapahtuu enenevässä määrin suoraan näytöltä. Vaihtoehtoja ovat mm. hiiren tai rullapallon käyttö ohjauskohteen valintaan ja ohjauksen suorittamiseen. Muita vaihtoehtoja ovat mm. kosketusherkät näytöt, joilta ohjaus suoritetaan sormella tai valokynällä.



Ehdotus toimintaohjeen esittämiseksi tukijärjestelmän näytöllä.

Tukijärjestelmät

Tietokonepohjaiset operaattorin tukijärjestelmät ovat saamassa yhtä merkittävämmän roolin ydinvoimalaitoksen turvallisessa ja tehokkaassa käytössä. Ne tukevat laitoksen operointia sekä normaaleissa käyttötilanteissa että häiriö- ja onnettomuustilanteissa. Monia erillisiä tai laitoksen prosessitietokonejärjestelmään integroituja sovelluksia on otettu käyttöön vanhoilla laitoksilla; yhtenä ensimmäisistä olivat NRC:n amerikkalaisilta laitoksilta TMI-onnettomuuden jälkeen vaatimat turvaparametrien näyttöjärjestelmät (SPDS). Uusien laitosten informaatiojärjestelmään integroidut tukijärjestelmät tulevat alusta alkaen olemaan keskeisessä asemassa prosessin valvonnassa. Informaatiojärjestelmän tärkeä ominaisuus on mahdollisuus uusien tukijärjestelmien helppoon toteutukseen järjestelmään sisällytettyjen kehitystyökalujen avulla. Tietämystekniikan, simuloinnin, hyperteksti- ja multimediatekniikkojen yms. soveltaminen avaa uusia tehokkaita tapoja tukijärjestelmien toteutukseen.

UNIPEDE:n ja IAEA:n asiantuntijaryhmät ovat luokitelleet maailmalla kehitteillä tai jo käytössä olevia tukijärjestelmiä:

1. Tehtäväsuuntautuneet näytöt
2. Älykäs hälytysten käsittely
3. Vikojen havaitseminen ja diagnoosi
4. Turvatoimintojen valvonta
5. Tietokoneistettu käyttöohjeiden esitys
6. Suorituskyvyn valvonta
7. Sydämen valvonta
8. Värinän valvonta ja diagnoosi
9. Irtokappaleiden valvonta
10. Materiaalirasitusten valvonta
11. Säteilytilanteen valvonta
12. Ylläpidon tuki

Listan viisi ensimmäistä kohtaa suuntautuvat ensisijaisesti operaattoreille, muut pikemminkin teknisille ja turvallisuusasiantuntijoille ja kunnossapitohenkilökunnalle.

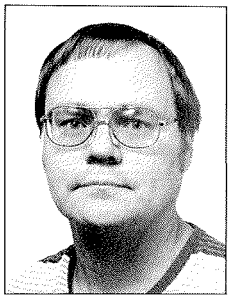
Kelpoistaminen

Digitaalisten automaatiojärjestelmien kelpoistaminen vaatii uusien menetelmien ja käytäntöjen soveltamista johtuen ohjelmoitavan tekniikan luotettavuusarvioiden epävarmuudesta. Ensisijaisesti tämä luonnollisesti koskee laitoksen turvallisuusautomaatiojärjestelmää, mutta myöskin käyttöautomaation ja valvomon toimivuus on varmistettava sitä tarkemmin mitä vähemmän konventionaalisia varajärjestelmiä laitoksella käytetään. Avainasemassa tulevat olemaan sen varmistaminen, että järjestelmän suunnittelussa ja toteutuksessa kauttaaltaan sovelletaan parhaita saatavissa olevia teknisiä ratkaisuja sekä laadunvarmistus- ja projektinhallintamenetelmiä. Viimeisenä lenkkinä varmistusketjussa on riippumattoman tahon suorittama kattava järjestelmän analyysi- ja testaus.

DI Pentti Haapanen on VTT:n Sähkö- ja automaatiotekniikan laboratorion erikoistutkija,
puh. 90-456 6433.

Ari Kautto

VALVOMOAUTOMAATIO INHIMILLISTEN VIRHEIDEN VÄHENTÄJÄNÄ



IVO:ssa on perinteisesti tutkittu voimaprosessin hallintaa häiriötilanteissa. Täysimittakaavaisen Loviisan koulutussimulaattorin valmistuttua (1980) tutkimusta on tehty myös simulaattorilla. Uusia menetelmiä prosessin valvontaan on kehitetty ja otettu käyttöön koskien lähinnä hälytysjärjestelmää. Tällöin ei enää ole tutkittu parannusten vaikutusta inhimillisiin virheisiin, vaan luotetaan myönteiseen vaikutukseen.

Tässä rajoitutaan kuvaamaan valvomoautomaation merkitystä virheiden estämisessä tai niiden havaitsemisessa ja haitallisten seurausten vähentämisessä, erityisesti ydinvoimalaitoksen käytössä vuodesta 1980 alkaen.

Inhimillisten virheiden tutkimusta ja menetelmiä virheiden välttämiseksi prosessin valvonnan alalla on aloitettu jo ennen 1980-lukua pohjoismaisena yhteistyönä, koska vakavien onnettomuuksien mahdollisuus oli jo tiedostettu. Yhteistyö jatkuu edelleen. Päätutkimusalueita vanhimmasta alkaen ovat olleet:

— valvomon suunnittelu
— ihmisen luotettavuus
— onnettomuustilanteen hallinta (informaatiotekninen tuki)
— reaktoriturvallisuus (vakava reaktorionnettomuus)

Harrisburgin, TMI:n onnettomuus tapahtui maaliskuussa 1979, minkä seurauksena maailmalla inhimillisten virheiden tutkimus kasvoi.

Aikakaudesta ennen 1980-lukua todetaan, että prosessiteollisuudessa käytetään perinteisesti komponenttikohtaisia suojauksia, lukituksia, vapautuksia ja kriteeriohjauksia sekä osajärjestelmäkohtaisia ylös- ja alasajoautomatiikkaohjelmia, joilla varmistetaan komponenttien suunniteltu käyttö ja samalla estetään inhimillisiä virheitä, kunhan suunnitteluvaiheessa ei ole sattunut virheitä. Esimerkiksi Loviisan voimalaitos onkin erittäin pitkälle automatisoitu.

Perusperiaatteita

Kantavana periaatteena voidaan pitää, että mitään ei jätetä yksinomaan ulkomuistin varaan. Niinpä prosessitietokoneella tai vastaavalla esitetäänkin mahdollisimman selkeitä virtauskaavionäyttöjä, jotka ovat pääpiirtein mahdollisimman samankaltaisia valvomopaneelimimiikan ja myös prosessi- ja instrumenttipiirustusten kanssa. Kyse on ollut em. esitysten muokkaamisesta selkeään ja yhtenevään esitystapaan.

Tämän lisäksi tarvitaan prosessin valvontaperiaatteita, missä on kyse kiteytetysti sanoen hälytysjärjestelmän toiminnan kehittäminen. Tätä on toki yritetty ja tehtykin tietokoneella jo ennen 1980 lukua. Esitettyjen ideoiden toteutus ja edelleen kehitys on kuitenkin päässyt isommasti vauhtiin 1980 luvulla teknisen välineistön tehostumisen myötä. Kärjistäen voidaankin sanoa, että tärkeintä käyttöhenkilökunnalle on tietää, mitä hälytys merkitsee ja mitä tulee tehdä tilanteen korjaamiseksi. Valvomosuunnittelu onkin eräs IVO International Oy:n automaatioliiketoiminnan vahvoja osaamisaloja.

Prosessin valvontaperiaatteet

Inhimillisiä virheitä tapahtuu myös suunnittelussa. Näiden eliminoimiseksi tai vähentämiseksi täysimittakaavainen koulutussimulaattori on hyvä työväline. Prosessin valvonnan uusien menetelmien kehitys on tehty järjestyksessä: tarvekartoitus, yleinen esisuunnittelu, yksityiskohtainen suunnittelu, asennus simulaattorin prosessitietokoneelle, tekijöiden suorittama esitestaus, validointiajot käyttöhenkilökunnan ja simulaattorikouluttajan kanssa, virheiden korjaus ja tarvittaessa esittely viranomaiselle tai viranomaisen suunnittelemien validointiajojen suoritus. Näiden vaiheiden ohella kehitetty prosessin valvontaperiaate on voitu jo viedä laitoksen prosessitietokoneelle, mutta ilman hälytysmäärittelyä, palautteen saamiseksi todellisesta käyttöympäristöstä. Tyypillisesti on seurattu jokin suunniteltu laitoksen tilamuutos, esimerkiksi alasajo tai ylösajo. Lopuksi ja vihdoinkin suunnitellut hälytykset määritetään hälytyksiksi prosessitietokoneelle.

KRIITTISTEN TURVATOIMINTO-HÄLYTYSTEN TESTAUS

Loviisan koulutussimulaattorilla testattiin vuonna 1982 Combustion Engineering Inc. (CE) kehittämä hälytysjärjestelmä Critical Function Monitoring System (CFMS). Tämä tapahtui yhteistyönä, jossa mukana olivat IVO, CE, Halden Reactor Project (HRP) ja Valtion teknillinen tutkimuskeskus (VTT). CFMS oli joukko algoritmeja, joilla valvottiin prosessin ydinteknillistä turvallisuutta. Hälytyskandidaatit oli koottu yhdelle näyttösivulle. Värinvaihdoksella osoitettiin voimassa oleva hälytys. Turvatoimintohälytyksiä ei siis tarvitse hakea hälytyslistasta, joka isossa häiriötilanteessa on pitkä.

Koe oli varsin mittava. Se sisälsi kaksi simuloitua primääripiirin vuototilannetta, johon oli kytketty vikatilanteita turvajärjestelmiin sekä niihin vaikuttavia vikatilanteita. Kaikki Loviisan käyttövuorot osallistuivat validointiajoihin. Transientteja ajettiin niin, että yhdessä testiajossa vuoro käytti CFMSää ja toisessa ei. Ajoista kerättiin seuraavaa tietoa:

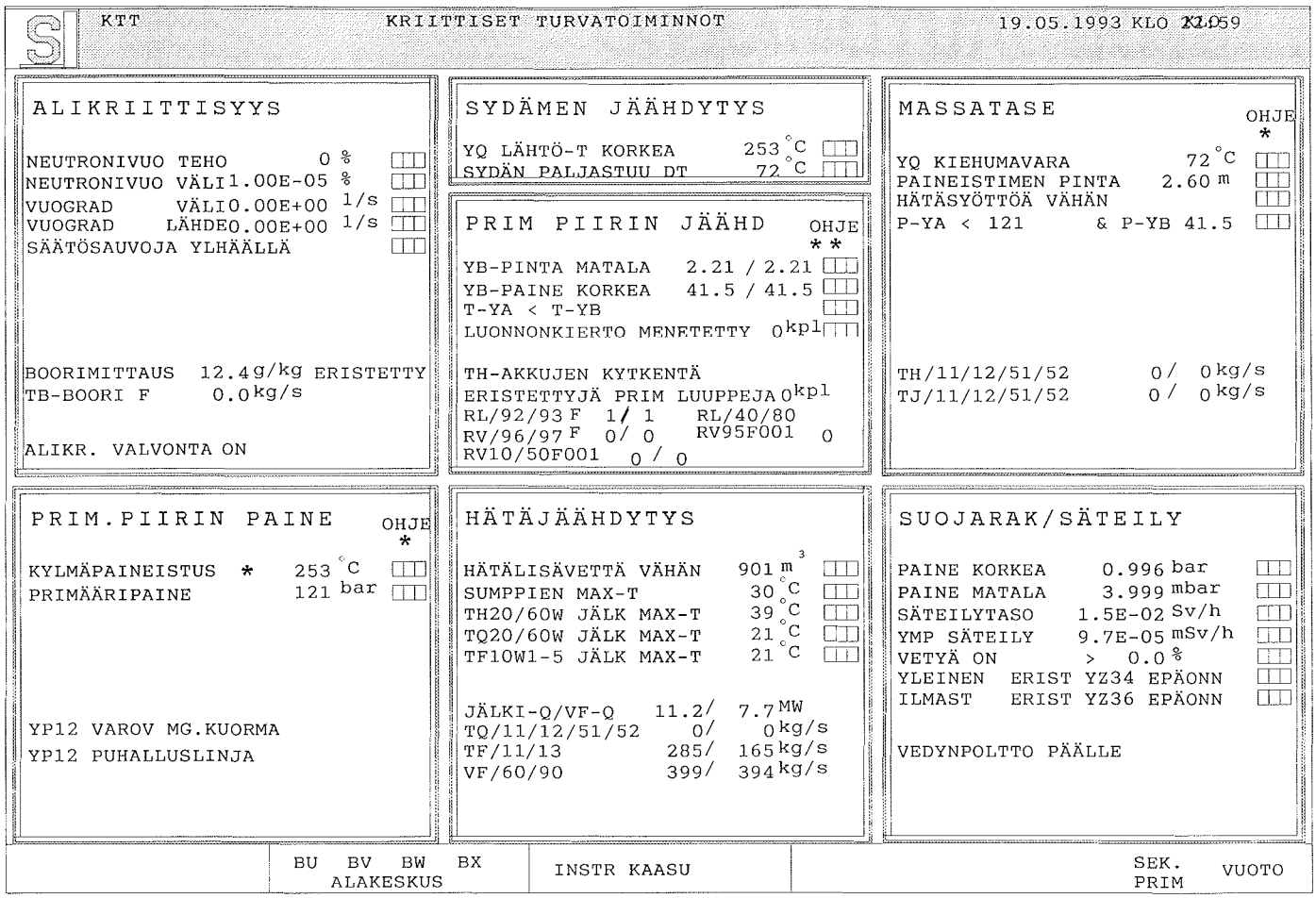
— hälytyslista
— ohjaajien kommunikointi
— videoitiin vuoron toiminta
— ohjaustoimenpiteet
— prosessin päämuuttujien arvot

HRP analysoi tulokset ja tavoitteena oli osoittaa ns. kovalla tilastodatalla, että prosessi hallittiin transienttitilanteessa paremmin käyttämällä CFMSää kuin ilman sitä. Jostakin yksittäisestä ajosta ilmeni, että CFMS:stä oli apua tilanteen vakavuuden havaitsemisvaiheessa, mutta merkittävää tilastollista tukea tavoitteelle ei ilmennyt. Tässä tutkimuksessa ei suoranaisesti tutkittu virheiden tekoa, vaan että oliko CFMS:stä tukea vuorolle.

Validoinnin perusteella ilmeni tarvetta valvoa ja esittää tietokoneella turvajärjestelmien toimintaa. CE kehittikin parannetun konseptin nimeltä Success Path Monitoring System. Se validoitiin Haldenissa v 1987 ja uusi lisäpiirre koettiin hyödylliseksi.

VIRHEIDEN TEOSTA

IVOssa on perinteitä myös Propabilistic Safety Analysis (PSA) menetelmän soveltamisesta. Tässä yhteydessä on tutkittu myös inhimillisen virheen mahdollisia vaikutuksia Loviisan laitoksella ja kokeita



Loviisan kriittisten turvatoimintojen näyttö.

on tehty koulutussimulaattorilla. Vuonna 1985 alkoi inhimillisten virheiden merkityksen tutkimusmenetelmän kehittäminen, jota kesti kaksi vuotta. Simulaattorilla on tutkittu, kuinka kauan kestää joidenkin kriittisten alkutapahtumien tunnistaminen ja tilanteen korjaaminen, kuten epäonnistunut reaktorin pikasulku (säätösauvat jäävät ylös), valtakunnan verkon menetys yhdistettynä puutteelliseen dieselien käynnistymiseen. Tutkimukset ovat ainakin osaksi vaikuttaneet siihen, että valvomoon on lisätty joitakin hälytyksiä. Myös hätätilanneohje epäonnistuneesta reaktorin pikasulusta on kehitetty. Nyt PSA jatkuu laitoksen alkutilan ollessa polttoaineen vaihto ja siinä selvitetään myös inhimillisen virheen osuutta.

Vuonna 1985 tehtiin tutkimus VTT:n Sähkö- ja automaatiotekniikan laboratorion kanssa, millaisia virheitä transienttitilanteen hallinnassa tapahtuu. Samalla testattiin Risn tutkimuslaitoksessa Tanskassa kehitettyä menetelmää simulaattorikoulutuksen yhteydessä suoritettavaa virheiden analysointia varten. Itse menetelmän esitestaukseen oli osallistuttu 80-luvun alussa Pohjoismaisen yhteistyön puitteissa. Virheeksi tulkittiin poikkeama ennalta tehdystä malliajosta, joka tehtiin transientin simuloituja vikatilanteita suunniteltaessa. Poikkeamia toki löytyi, mutta ei sellaisia, joilla olisi ollut merkitystä turvallisuuden kannalta. Virheiden analysoinnin perusteella vaikutti siltä, että häirön monimutkaisuuden kasvaessa joissakin ajoissa tuntui tiedon käytön hyödyntäminen tuottavan vaikeuksia. Tutkimusmenetelmästä havaittiin, että tiedon keruutapa ei tue (optimiajosta) poikkeamien syvällisempää selvittämistä, kun ne liittyvät prosessitiedon hallintaan. Esimerkiksi eräs mahdollisuus on, että on valittu toisenlainen ohjaustapa, joka sinänsä on riittävä, mutta ei niin hyvä kuin optimiajo. Tällöinhän poikkeamia optimiajoon nähden tulee paljon. Tutkimuksella oli myös antia simulaattorikoulutukseen.

Edellisen tutkimusmenetelmän tiedon keruutavan puutteellisuus prosessitiedon ja -tietämyksen käytön syvälliseksi selvittämiseksi antoi aiheen parantaa analyysimenetelmää. Siksi 90-luvun alussa palattiin CFMS-validointiaineistoon ja sitä alettiin tutkia VTT:n sähkö- ja automaatiotekniikan laboratorion kanssa toisesta näkökulmasta. Siinä kehitettiin analyysimenetelmä tarkastella vuoron yhteistyötoimintaa ja nimenomaan tutkittiin häiriön diagnostisointia ja prosessin hallintaa. Tässä perehdyttiin lähtöaineiston puitteissa hyvin tarkasti saatavilla olleen prosessi-informaation käyttöön. Tutkimuksessa keskityttiin ajoihin, joissa ei käytetty CFMS:ää. Tuloksena ilmeni, että joissakin ajoissa tärkeätä prossitietoa käytettiin lähinnä vain operatiivisen toiminnan tukena, jolloin prosessin hallintatapa näytti työläältä. Jos samaa tietoa käytettiin myös toiminnallisessa ja diagnostisessa mielessä, niin prosessitapahtumien kulku luonnollisesti käsitettiin erittäin hyvin. Lisäksi ilmeni, että prosessi voidaan hallita ydinteknillisen turvallisuuden kannalta hyvin, vaikka diagnoosin onnistuminen viivästyisikin. Tällöin prosessin tilan kehittymisen ennakointi on luonnollisesti vaikeampaa ja aiheuttaa lisätyötä verrattuna siihen, että diagnoosi onnistuu jo varhain.

HÄLYTYSJÄRJESTELMÄ

Hälytykset on tyypillisesti suunniteltu valvomaan tehoajoa periaatteella yhdelle suureelle asetetut hälytysrajat. Tästä onkin seurauksena, että alasajossa ja laitoksen päätransienteissa esimerkiksi reaktorin ja/tai turpiinin pikasulussa tulee tilanteeseen nähden paljon virheellisiä ja tarpeettomia hälytyksiä. Tilanteen korjaamiseksi on kehitetty ns. estoehtotoiminto, jolla hälytyksiä tehdään tilanteesta riippuviksi. Esimerkiksi jos virtaukselle on tehty alarajahälytys, niin pienestä virtauksesta on turha hälyttää, mikäli pumppu ei käy. Ehdollistustoiminto oli jo Loviisan vanhassa prosessitietokoneessa. Sen kapasiteettirajoituksen takia tätä ominaisuutta ei täysin päästy hyödyntämään. Nykyisellä prosessitietokoneella mahdollisuudet ovat jo riittävät. Nykyinen prosessitietokone otettiin käyttöön vuosien 1989 ja 1990 vaihteessa.

Koulutussimulaattorilla tehtiin tutkimuksia ja kokeiluja jo 1980 luvun alussa ja estoehtoja asennettiin vanhalle prosessitietokoneelle. Nykyiseen prosessitietokoneeseen estoehtologiikoita on edellisen tutkimuksen tulosten perusteella asennettu lisää ja uusia estoehtologiikoita kehitetään parhaillaan. Lisäksi nykyisessä prosessitietokoneessa on mahdollista tehdä loogisesti koottuja hälytyksiä, jolloin voidaan sanoa, että estoehtologiikka on hälytykseen sisäänrakennettuna.

KRIITTISET TURVATOIMINTO-HÄLYTYKSET LOVIISAAN

Prosessitietokoneen vaihdon yhteydessä aloitettiin kriittisiä turvatoimintoja (KTT) eli lähinnä lämmönsiirtoehtoja valvovien hälytysalgoritmien kehittäminen Loviisaan. Hyvänä pohjana tälle oli aiemmin mainittu CEn konseptin testaus koulutussimulaattorilla.

Turvatoiminnoille määritettiin keskinäinen tärkeysjärjestys ja sisäinen prioriteetti, josta käytetään nimitystä vakavuusaste. Niitä määritettiin kolme hälytystilalle. Lievin vakavuusaste osoittaa ydinteknillisen turvallisuuden kannalta vähäistä poikkeamaa normaalista termohydraulisesta tilasta. Korkein merkitsee sitä, että tilanteen jatkuessa seurauksena on ennemmin tai myöhemmin sydämen jonkinasteinen vaurioituminen. Vakavuusasteet määritettiin, jotta on helpompi hahmottaa prosessin tilan vakavuus ja muutossuunta turvatoiminnoittain. Lisäksi samalla näytöllä esitetään toiminnoittain turvallisuuden kannalta oleellisimpien prosessimuuttujien arvo, sekä toimivatko turvajärjestelmät suunnitellusti mukaanlukien dieselvarmennetut pääkeskukset.

KTT-hälytyksen voimassaolo esitetään myös laitoksen jokaisen näytön vasemmassa yläkulmassa violettina kehikkona laitostunnuksen ympärillä. KTT-näyttö ilmestyy automaattisesti vuoropäällikön kuvaputkelle ensimmäisen KTT-hälytyksen voimaantullessa.

MALLIIN PERUSTUVAA PROSESSIN VALVONTAA

Tekoäly

Vuosina 1987-1988 kehitettiin sekundääripiirin valvontaa; vuotojen tunnistusta, osajärjestelmien kytkentätilan tarkistusta ym. tietämysteknisellä Knowledge Engineering Environment (KEE) järjestelmällä. Siinä käytettiin korrelatiivisia riippuvuussuhteita mm. syöttöveden määrän ja generaattorin tehon välillä, jotta voidaan käyttää liukuvaa hälytysrajaa syöttöveden määrälle. Syöttövesivirtauksen kasvu osoittaa vuotoa, kun turpiinin ohitusvirtaukset on otettu huomioon. Lisäksi käytettiin ehtoja tarkistamaan säilyykö virtaus putkilinjassa. Järjestelmä oli asennettuna koulutussimulaattorille, josta se sai lähtötiedot. Järjestelmää testattiin yhden käyttövuoron ja kouluttajan voimin. Periaatteessa järjestelmä toimi ja tunnistikin tapahtumia oikein, mutta rasitteena oli järjestelmän hitaus, koska siitä ei ollut ajonaikaista versiota. Lähtötietojen päivitysväli oli peräti 40 s. Sääntöjen kehittämisen vaikeudet tulivat myös hyvin esille. Esimerkiksi virtauksen säilymislain käyttö ei välttämättä paikallista ison syöttövesiputken katkeamista, koska äkillisesti kaikki virtausmittaukset voivat näyttää arvoa nolla, tai tarkkaan ottaen jotakin pohjalukemaa. Projektissa tulikin hyvin esille matemaattisfysikaalisten mallien ja muiden laskettujen tunnuslukujen tärkeys häiriön tunnistuksessa.

Prosessihäiriön diagnostiikasta

Haldenissa on testattu Japanissa JAERIssa (Japan Atomic Energy Research Institute) kehitettyä tietämysinsinööripohjaista prosessihäiriöiden diagnostisointijärjestelmää DISKET (DIagnostic System based on Knowledge Engineering Technique). Siinä käytetään tapahtumakohtaista reaalista luotettavuuskerrointa skaalattuna välille -1...1, joista arvo -1 tarkoittaa tapahtumalle vastakkaista havaintoa ja arvo 1 täydellistä tukea tapahtumalle. Muut arvot vastaavat osittaista evidenssiä. Järjestelmä tulostaa ne diagnostiset havainnot, jotka ylittävät asetetun luotettavuuskertoimen arvon. Järjestelmä voi siis ehdottaa eri vaihtoehtoja. Tutkimuksessa ilmeni, että järjestelmästä on hyötyä, jos se on tunnistanut häiriön oikein. Sen sijaan virheellisestä tunnistuksesta voi olla haittaakin.

Häiriön varhainen havaitseminen

Halden Reactor Projektissa on kehitetty vuodesta 1985 Early Fault Detection (EFD) prosessin valvontaan, joka on matemaattisfysikaaliseen mallitukseen perustuva menetelmä. Siinä lasketaan muutamista lähtötiedoista jonkin mitatun suureen arvo, esimerkiksi virtauksen. Laskettua ja mitattua arvoa verrataan toisiinsa ja liian suuresta poikkeamasta hälytetään. Periaatteessa turhia hälytyksiä ei tule. EFD-periaatteeseen voidaan jatkoksi liittää myös tapahtuman ykstyiskohtainen tunnistus.

Kunnonvalvontamielessä EFD-periaatteen mukaan Loviisassa valvotaan korkeapaine-esilämmittimiä ja syöttöveden virtausmittauksia. Loviisassa kerätyn aineiston perusteella myös osoitettiin EFD-menetelmän kelvollisuus käytäntöön.

Primääripiirin vuotodiagnostiikka

Primääripiirin vuodon havaitsemista ja luokitusta päätettiin tukea Loviisan prosessitietokone- järjestelmän laskennan avulla. Tämä tapahtuman diagnostiikka on luonnollinen täydennys KTT:n ohelle. Näkemyksenä on, että oikeita ohjauksia tehdään varmemmin tunnistetussa tilanteessa kuin tunnistamattomassa.

Vuoden 1991 aikana kehitettiin primääripiirin vuodon laskenta. Siinä otetaan huomioon lämpötilan ja paineen vaikutus jäähdytteen tilavuuteen, injektiot ja uloslaskut sekä miten nämä vaikuttavat paineistimen pinnan muutokseen. Lisäksi kehitettiin laskenta, joka pystyy erottamaan vesi- ja höyryvuodon toisistaan. Vuotolaskenta havaitsee hieman yli 3 kg/s vuodon noin minuutin kuluttua tasaisella ajolla ja transienttitilanteessa noin kolmessa minuutissa. Isompi vuoto havaitaan nopeammin.

Hälytykset on koottu vuotodiagnostiikkanäytölle ja toteutettu logiikalla, jotka voidaan kutsua kuvaputkelle. Vuotodiagnostiikkanäytölle on koottu diagnoosin tekoon välttämättä tarvittavat muuttujat. Osa esitetään suoraan ja osa on logiikoissa. Näytöllä esitetään ne tapahtumat, joita varten tunnistuslogiikka on tehty. Värimuutoksella esitetään tietokoneen havaitsema tapahtuma.

Ohjeita prosessitietokoneelle

Tuoreimpana T&K-hankkeena on Loviisan koulutussimulaattorilla selvitetty nykyisen prosessitiekonejärjestelmän soveltuvuutta dynaamista tietoa sisältävän ohjeen esittämiseen. Koulutussimulaattorin prosessitietokoneelle asennettiin hätätilanteen yleisohjeesta kolme toimintoa v. 1992 ja tätä on esitelty vuoroille simulaattorikoulutuksen yhteydessä 1993.

YHTEENVETO

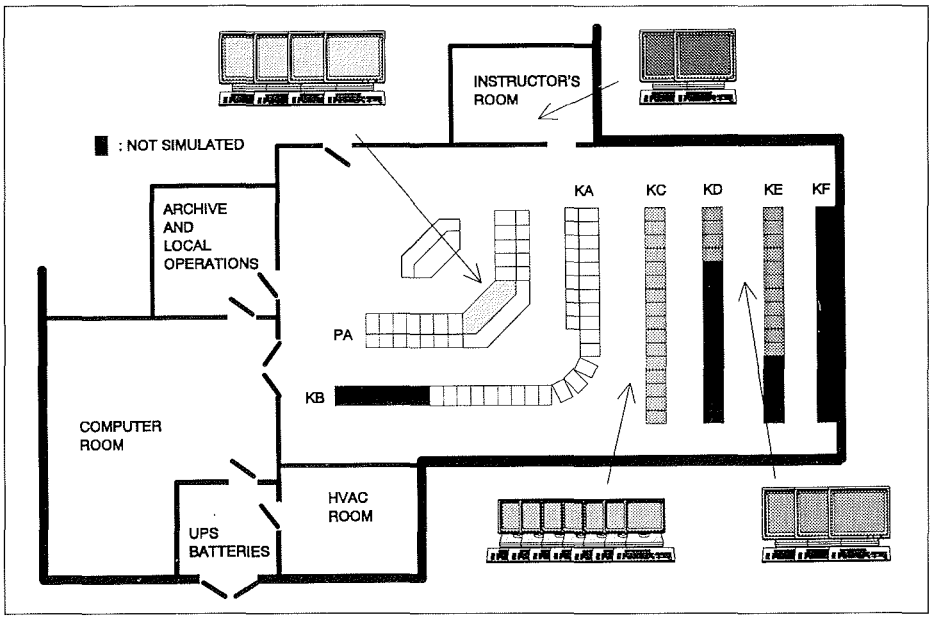
IVO-yhtiöissä on perehdytty voimaprosessin hallinnan vaikeuksiin erityisesti häiriötilanteissa sekä kehitetty entistä parempia prosessinvalvontamenetelmiä. Myös on kiinnitetty huomiota virheiden esiintymiseen ja niiden syihin eri hankkeissa. 1980 luvun alussa Loviisan koulutussimulaattorin valmistuttua työ konkretisoitui edelleen. Sittemmin on kehitetty ja otettu käyttöön uusiakin menetelmiä prosessin valvontaan koskien lähinnä hälytysjärjestelmää. Tällöin ei enää ole toistaiseksi varsinaisesti tutkittu automaation vaikutusta inhimillisiin virheisiin, koska näkemystä on saatu aiemmasta työstä ja lisäksi sellainen tutkimus on varsin työlästä. Vaikuttaa perustellulta luottaa siihen, että parantamalla perusautomaatiota, prosessinvalvontamenetelmiä, käyttöohjeita ja koulutusta sekä virheiden määrä että merkitys tyypillisesti vähenevät. Inhimillinen virhe on kuitenkin sellainen, ettei sitä voi täysin estää.

TkL Ari Kautto työskentelee IVO International Oy:ssä prosessinvalvonnan sovellusasiantuntijana, p. 90-5082501.

Tapio Saarenpää, Kauko Yli-Antola, Eero Patrakka, Markku Malinen

SIMULAATTORIKOULUTUSTA OLKILUODOSSA VUODESTA 1990

Olkiluodon käyttöhenkilökunnan simulaattorikoulutus tapahtui 1980-luvun loppuun saakka Ruotsin ydinvoimayhtiöiden koulutuskeskuksessa Studsvikissa. Vuoden kestäneen soveltuvuustutkimuksen pohjalta TVO päätti vuonna 1987 hankkia oman koulutussimulaattorin Olkiluotoon. Päätös takasi simulaattorin laitosvastaavuuden ja mahdollisti koulutustoiminnan ulkoisen riippumattomuuden.



Simulaattorivalvomon pohjapiirustus

OLKILUODON KOULUTUS-SIMULAATTORI — OLKS

Tapio Saarenpää

Simulaattoriprojekti

Simulaattorin ohjelmiston ja tietokonelaitteiston toimitussopimus allekirjoitettiin yhdysvaltalaisen Singer Link-Miles Simulation Corp:n kanssa. Valvomolaitteet TVO osti ABB Strömberg Oy:ltä Suomesta, ja ne toimitettiin simulaattorivalmistajan tehtaalle Columbiaan, Marylandiin.

Ohjelmisto- ja laitteistopääsopimukset allekirjoitettiin tammikuussa 1988 ja simulaattori asennettiin Olkiluotoon rakennettuun 1330 m²:n koulutuskeskukseen vuodenvaihteessa 1989-90. Toteutunut kokonaistoimitusaika 26 kk on kansainvälisestikin kunnianhimoinen.

TVO:n osuus käsitti suunnittelutietojen keräämisen ja toimittamisen sekä rakennustyöt Olkiluodossa. Tämän lisäksi neljä TVO:n edustajaa oli alusta alkaen työssä toimittajan tehtaalla. Tehdaskokeiden suorittamiseen osallistui lisäksi kaksi kouluttajaa koko ajan ja yhteensä 20 vuoropäällikköä ja reaktori/turpiiniohjaajaa kukin kahden viikon ajan.

Laitteisto

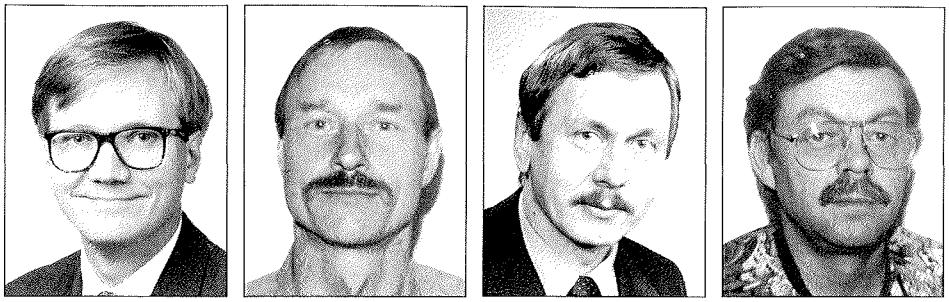
ABB Strömbergin toimitus kattoi kaikki laitteet simulaattorivalvomon primäärisessä ohjausalueessa. Simulaattori sisältää kaikki TVO I/II:ssa ko. pulpeteissa olevat instrumentit täysin identtisinä. Lisäksi kaikki niiden sisältämät signaalit on kytketty I/O-laitteistoon ja ne ovat siten joko malliohjelmien tai kouluttajien ohjattavissa. Simulointilaajuutta kuvaa hyvin se tieto, että laitosvalvomon hälytyksistä on simuloitu 90 %.

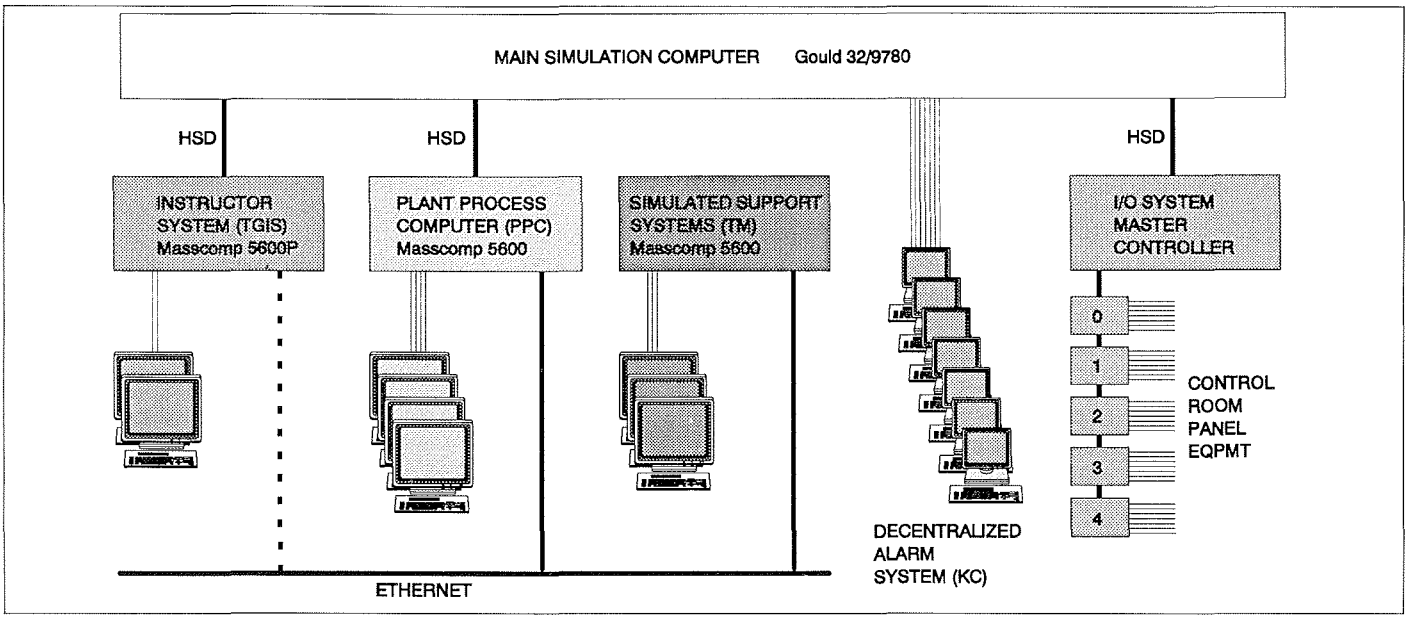
Hälytysjärjestelmän 14 kaappia (KC) on toteutettu toiminnallisesti identtisinä laitosten kanssa, ja kaikki hälytykset on liitetty ohjelmistoon. KC-kaapeissa käyttöliittymä on kuitenkin toteutettu simuloimalla hälytykset kaappien etuseinien hälytysikkunoiden sijasta seitsemällä kuvaputkella.

Valvomon takaosan lämpötilaindikoinnit (KD) ja paperipiirturit (KE) on sekundäärisyytensä vuoksi simuloitu kaappirivien sijaan kolmella 19" korkearesoluutiomonitorilla. Mekaanisia vuotolaskureita sisältävää osaa kaapeista KE samoin kuin laitosvalvomon takaseinän palohälytysjärjestelmän kaappiriviä KF ei ole simuloitu.

Valvomolaitteiden osto	*joulukuu 1987*
Ohjelmisto- ja tietokonesopimukset	*tammikuu 1988*
Laitoksen lähtötietojen toimitus	*toukokuu 1988*
Valvomolaitteet Columbiaan	*elokuu 1988*
Rakennustöiden aloitus	*joulukuu 1988*
Tehdaskokeiden aloitus	*syyskuu 1989*
Koulutuskeskuksen rakennus valmis	*lokakuu 1989*
Pakkaus ja rahtaus Suomeen	*joulukuu 1989*
Lopullinen hyväksyminen	*helmikuu 1990*
Koulutuksen aloitus	*maaliskuu 1990*

OLKS-simulaattorin projektiaikataulun päävaiheita





Tietokonelaitteisto koostuu neljästä yksittäisestä tietokoneesta: (1) pääsimulointitietokone Gould/Encore 32/9780, jossa suoritetaan kaikki reaaliaikamallit, ja kolmesta Masscomp/Concurrent 5600 -koneesta: (2) kouluttajan järjestelmä (TGIS) kahdella työasemalla simulaattorin ohjaukseen, (3) prosessitietokone (PPC) valvomossa ohjaajien käytössä olevien näyttöfunktioiden simulointiin ja (4) tukijärjestelmät (TM) KD- ja KE-kaappien lämpötilavalvonta- ja piirturioimintojen simulointiin.

Ohjelmisto

Ohjelmisto tarjoaa monipuoliset välineet malliohjelmien kehitystyöhön; mm. useat käyttäjät voivat testata malleja taustalla toisistaan ja koulutuksesta riippumatta. Pääkäyttäjällä on käytössään myös tällaisen monen ohjelmoijan järjestelmän edellyttämät versionhallinnan työkalut.

Kaikki laitoksen normaalikäytössä ja häiriötilanteissa tarvittavat komponentit ja järjestelmäosat on simuloitu dynaamisesti. Valtaosa ohjauksista tapahtuu keskusvalvomosta, mutta myös tarvittavat paikalliset ohjaukset on simuloitu.

SIMULAATTORIN KÄYTTÖKOKEMUKSIA

Kauko Yli-Antola

Käytön jakaantuminen eri tarkoituksiin

Simulaattorin kokonaiskäyttöaika jakaantuu koulutuskäytön lisäksi useisiin muihin simulaattoriaikaa vaativiin tarkoituksiin. Nämä voidaan jakaa ohjelmistomuutoksia edellyttäviin havaittujen toimintavirheiden korjauksiin, voimalaitoksella tehtyjen muutosten toteuttamiseen simulaattorilla ja simulaattorin käytön monipuolistamiseen tähtäävään kehitystyöhön. Tämän lisäksi simulaattoriaikaa menee toimintaa varmistavaan ylläpitotyöhön ja näytösajoihin erilaisten vierailujen yhteydessä. Simulaattoria käytetään myös esim. laitoksen ohjeiden verifiointiin ja erilaisiin toimintakoestuksiin.

Simulaattorin kokonaiskäyttöaika oli 1663 tuntia vuonna 1992. Koulutukseen ja sen valmisteluun käytetty simulaattoriaika oli n. 970 h, joten sen suhteellinen osuus kokonaiskäyttöajasta oli n. 60 %. Vuonna 1991 koulutuskäytön suhteellinen osuus oli runsaat 30 %.

Koulutuksen osuuden lähes kaksinkertaistuminen edellisvuodesta johtuu osaksi simulaattorikoulutuksen lisääntymisestä ja osittain siitä, että ohjelmistojen takuukorjaukset valmistuivat vuonna 1991. Käyttövuorojen vuotuinen simulaattorikoulutus lisääntyi 6 päivästä 10 päivään; lisäksi aloitettiin mm. vastaavien johtajien ja laitospäivystäjien simulaattorikoulutus. Koulutuskäytön osuus tulee vuonna 1993 vielä nousemaan johtuen tämän vuoden simulaattoriperuskurssista, joka toistuu 2-3 vuoden välein.

Tähänastiset koulutuskokemukset

Olkiluodon koulutussimulaattorilla saatuja koulutuskokemuksia voidaan verrata niihin kokemuksiin, joita saatiin ennen omaa simulaattoria vuosina 1978—1989. Ruotsissa simulaattorikoulutus järjestettiin KSU:n B1-simulaattorilla, jonka referenssilaitos on Barsebäck 1. Sekä kouluttajat että ohjaajat arvioivat koulutuksen olevan nykyisellä laitosidenttisellä simulaattorilla paljon tehokkaampaa ja mielekkäämpää kuin B1-simulaattorilla. Tärkeimpänä parannuksena pidetään oman simulaattorin laitosidenttisyyttä, mutta merkittäviä ovat myös simulointilaajuuden huomattava lisäys ja simulaattorin hallinnan joustavuus kouluttaja-asemasta B1-simulaattoriin verrattuna.

Ohjaajat ovat olleet tyytyväisiä myöskin mallien realistisuuteen eli siihen, miten hyvin simulaattori eri tilanteissa matkii laitoksen toimintaa. Havaituista toimintavirheistä laaditaan kirjallinen ilmoitus, jonka perusteella malli saatetaan vastaamaan laitoksen toimintaa. Suurin osa havaituista toimintavirheistä on tullut ilmi kouluttajien valmistellessa koulutusajoja.

Simulaattorin käytettävyys on ollut hyvä. Käyttökeskeytyksistä useimmat ovat aiheutuneet 110 kV:n verkon jännitehäiriöistä. Tilanne on tätä nykyä parempi,

kun sähkön syöttö siirrettiin syötön stabiloivan ja varmistavan UPS-laitteiston perään keväällä 1993.

Tulevaisuuden näkymiä

Olkiluodossa on mielestämme moderni ja hyvin koulutuskäyttöön soveltuva simulaattori. Lähiajan suurin haasteemme on pitää simulaattori laitosidenttisenä. TVO:n laitoksilla on suoritettu paljon laitosten käyttövarmuutta ja turvallisuutta parantavia muutoksia, ja näiden muutosten toteuttaminen myös simulaattorissa on välttämätöntä koulutuksen tehokkuuden ylläpitämiseksi. Tällä hetkellä simulaattorilla eniten työtä aiheuttava muutos on prosessitietokoneen käyttöliittymän saattaminen vastaamaan laitoksella toteutettua modernisointia. Uusi järjestelmä käsittää myös SPDS (Safety Parameters Display System)-näytöt. Toinen ajankohtainen suuri laitosmuutos on omakäytön sähkönsyöttöjärjestelmän täydentäminen toisella syöttömuuntajalla.

SIMULAATTORIKOULUTUKSEN PÄÄLINJAT

Eero Patrakka

Koulutuksen kohderyhmät

Kun Olkiluodon koulutussimulaattori otettiin vastaan helmikuussa 1990, oli alusta alkaen selvää, että simulaattorikoulutus ulotetaan jatkossa laajemmalle kohderyhmälle kuin aikaisemmin. Laitospaikalla oleva simulaattori mahdollistaa koulutusohjelmien ja -aikataulujen suunnittelun niin, että erilaisia henkilöstöryhmiä voidaan kutsua lyhyeksikin aikaa joko tutustumaan simulaattorivalvomoon tai saamaan siellä perusteellisempaakin.

Simulaattorikoulutuksen tärkein kohderyhmä on luonnollisesti lisensioitu vuorohenkilöstö: vuoropäälliköt ja ohjaajat. TVO I:ssä ja TVO II:ssa on yhteensä 13 käyttövuoroa, joissa kussakin on vuoropäällikön lisäksi tavallisesti 3 lisensioitua ohjaajaa (reaktoriohjaaja, turpiiniohjaaja ja aluetyönjohtaja). Tähän ryhmään kuuluu kaikkiaan noin 60 henkilöä.

Toinen ryhmä, jolle simulaattorikoulutus on välttämätöntä, kattaa käytön johto- ja tukitehtävissä työskentelevät henkilöt. Näitä ovat esimerkiksi vastuullinen johtaja varamiehineen, käyttöjaosten päälliköt ja päivystäjät.

TIETOJA SIMULAATTORISTA

Laitteisto

Digilink-järjestelmään liitettyjä simuloituja valvomosignaaleja on tyypeittäin seuraavasti:

2200 painonappia
6800 merkkilamppua
600 mittaria
600 analogista prosessiviestiä
1300 digitaalista prosessiviestiä
1500 KC-hälytystä
220 KD-lämpötila-mittausta
230 KE-piirturisignaalia.
Näyttöjen päivitystaajuus 10 Hz

Kunnonvalvonta ja vianpaikallistaminen DORT (Daily Operational Readiness Test) -ohjelma.

Koko tehonkulutus 50 kVA.

Ohjelmisto

Malliohjelmien kokonaislaajuus:
550 000 ohjelmariviä
37 500 Mallimuuttujaa ja vakiota
225 000 Riviä kehitysohjelmistoa

TVO I/II laitosten 200:sta järjestelmästä simuloitu 136

Laitosjärjestelmien dynaamiset mallit: Gouldin Fortran-77

Simulointirajat:

polttoaineen suojakuoren lämpötila 982 °C
reaktoripaine 94,3 bar
suojarakennuksen paine 4,7 bar
lauhdutusaltaan lämpötila 100 °C

Edellä mainitut kohderyhmät saivat simulaattorikoulutusta jo ennen vuotta 1990 KSU:lla Ruotsissa. Uusia kohderyhmiä ovat mm. teknisen valvonnan reaktoriinsinöörit ja kunnossapidon henkilöstö. Koulutustoimisto pyrkii jatkuvasti kehittämään uusia kursseja, jotka kattaisivat muitakin kuin tässä lueteltuja henkilöstöryhmiä.

Simulaattorikurssien toteutus

Lisensioidun vuorohenkilöstön simulaattorikertauskoulutuksen määräksi on nyt vakiintunut 10 päivää vuodessa. Tämä on jaettu siten, että sekä keväällä että syksyllä on 3 päivän pituinen simulaattorijatkokurssi, jonka ohjelma on sama kaikille vuoroille. Lisäksi on vuorokohtaista simulaattoriajoa, jonka ajankohdan ja ohjelman — yhtä päivää lukuunottamatta — vuoro saa itse valita luonnollisesti simulaattorin käytettävyysrajoitusten puitteissa.

Useiden vuosien ajan TVO:ssa on perustettu ns. käytön koulutusryhmä joka toinen vuosi. Tähän on otettu puolisen tusinaa oppilasta joko pelkästään yhtiön sisältä tai myös talon ulkopuolelta. Puolentoista — kahden vuoden kuluessa heistä koulutetaan uusia ohjaajia ja mahdollisesti myös vuoropäälliköitä. Keskeisessä asemassa käytön koulutusryhmän koulutuksessa on simulaattoriperuskurssi, joka viimeisten laajennusten jälkeen kestää 9 viikkoa.

Muille kohderyhmille järjestetyistä simulaattorikursseista ei ole esittää mitään yhtenäistä mallia. Nämä "kurssit" ovat luonteeltaan ja kestoltaan vaihtelevia. ja niiden pituudet vaihtelevat muutamasta tunnista joihinkin päiviin.

Vuorohenkilöstön kertauskoulutus

Simulaattorikurssien ohjelma pyritään laatimaan siten, että se sisältää sekä varsinaisen ajoharjoittelun että luokkahuoneessa tapahtuvan "teoreettisen" osan. Simulaattorikertauskurssin päivittäinen ajoharjoittelu on 4 tuntia. Luokkahuoneessa käydään yhdessä läpi suoritettu harjoittelu ja sen aikana tehdyt havainnot. Teoreettinen osa sisältää myös eräitä TVO:n asiantuntijoiden pitämiä luentoja. Näiden aiheet perustuvat vuorojen 3 vuoden jaksoissa toistuvaan kertauskoulutusohjelmaan.

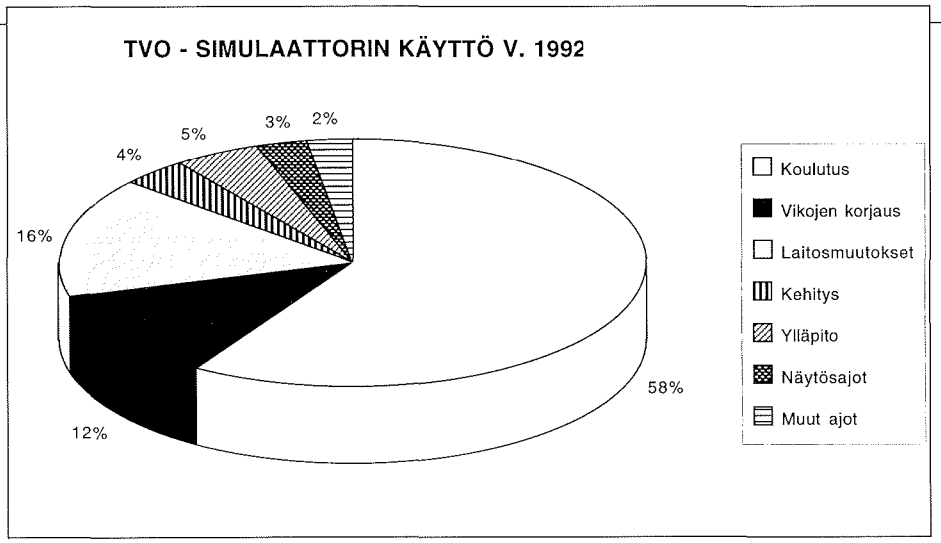
Varsinaisen simulaattoriajoharjoittelun ohjelma riippuu ratkaisevasti siitä, minkä tyyppisestä kurssista puhutaan. Kolmipäiväiseen simulaattorikertauskurssiin kuuluu lähes aina joko ylös- tai alasajo. Kurssiin mahtuu 10-12 häiriötä, jotka pyritään valitsemaan siten, että ne edustavat laitoksen käytössä esiintyviä tyypillisiä tapahtumia tai uusimpia kokemuksia.

Vuoropäälliköiden ja ohjaajien toimintaa erilaisissa häiriö- ja poikkeustilanteissa helpottaa huomattavasti se, että vastaava tai sitä muistuttava tilanne on sattunut simulaattorikoulutuksen aikana. Harjoi-

tellun tilanteen tunnistaminen ja tarvittavien ohjaustoimenpiteiden muistaminen antaa varmuutta työskentelyyn.

Yksinomainen harjoiteltaviin häiriöihin tuijottaminen ei ole hedelmällistä. On harvinaista, että juuri sama häiriö toistuisi uudelleen laitoksen käytössä, jos se on vähänkin erikoisempi tapahtuma. Eräänä simulaattorikoulutuksen päämääränä onkin opettaa ohjaajat toimimaan järkevästi kaikissa eteen tulevissa tilanteissa. Erilaisten häiriöiden harjoittelu auttaa heitä ymmärtämään laitoksen käyttäytymistä entistä paremmin.

On syytä muistaa, että simulaattorikoulutus on kaksisuuntainen prosessi: toisaalta kouluttajat välittävät oppilaille tietoa heidän onnistumisestaan ja toisaalta oppilaat kertovat, millaista harjoittelua he haluavat ja millä tavoin koulutusohjelma ja simulaattori vastaavat heidän toiveitaan.



Kuva esittää simulaattorin käytön jakaantumisen em. tarkoituksiin vuonna 1992, jolloin simulaattorin kokonaiskäyttöaika oli 1663 h. Koulutukseen ja sen valmisteluun käytetyn simulaattoriajon suhteellinen osuus kokonaiskäyttöajasta oli n. 60 %.

Uusia kehityskohteita

Olkiluodon koulutussimulaattori on myös muiden kuin TVO:laisten käytettävissä. Säteilyturvakeskuksen kanssa on sovittu simulaattorikurssin pitämisestä STUK:n tarkastajille kesän 1993 aikana. Lisäksi Olkiluodossa on meneillään VTT:n tutkimus, josta kerrotaan lisää jäljempänä. TVO:n ulkopuolisten organisaatioiden simulaattorikäyttöä rajoittavat luonnollisesti simulaattorin käyttö TVO:n henkilöstön koulutukseen ja TVO:n kouluttajien mahdollisuudet tuottaa palveluja yhtiön ulkopuolelle.

TVO:ssa ei koulutussimulaattoria ole vielä käytetty valmiusharjoitusten yhteydessä. Simulaattorin mukaan ottoa rajoittaa oleellisesti se, että vakavia reaktorionnettomuuksia ei voida simuloida. Toisaalta simulaattori tarjoaa aidon ympäristön valmiustilanteen läpiviennille, jos onnettomuuden aikainen tapahtumaketju lasketaan muilla tavoin valmiiksi. Tulevaisuuden suunnitelmissa on valmiusharjoitusten tekeminen myös simulaattorin avulla. Kehitteillä oleva PC-pohjainen vakavien onnettomuuksien simulointiohjelma auttaa osaltaan tämän pyrkimyksen toteuttamisessa.

Toinen mahdollinen kehityskohde on seisokkiaikaisten tapahtumien sisällyttäminen simulaattorin koulutusohjelmiin. On tiedossa, että eräisiin vuosihuollon aikana suoritettaviin toimenpiteisiin sisältyy riskejä, joihin on varauduttava myös valvomossa.

SIMULAATTORIKOULUTUKSEN ERITYISPIIRTEITÄ

Markku Malinen

Häiriöohjeiden verifiointi

Simulaattorilla on voitu toteuttaa sellaisia häiriötilanteita, joita ei ole koskaan tapahtunut laitoksella ja joiden tapahtumatodennäköisyys on erittäin pieni. Vaikka tällaisia tilanteita varten on laadittu häiriöohjeet, niiden toimivuutta ei ole voitu todentaa laitoksella. Simulaattoriajojen seurauksena on ohjeisiin tehty joitakin korjauksia ja muutoksia.

Simulaattorikoulutuksen yhteydessä on myös herännyt kysymyksiä, millä tavoin jotain järjestelmää pitäisi käyttää tietyssä vikatilanteessa. Nämä kysymykset liittyvät yleensä melko laajoihin apujärjestelmiin, joiden ajotavoissa on eri vaihtoehtoja. Vikatilanteissa toimimista on selvitetty simulaattorilla, ja menettelytapoihin on saatu tarkennuksia.

PSA-analyysit ja hätätilanneohjeet

PSA-analyyseihin sisältyvän inhimillisen tekijän tarkemmaksi selvittämiseksi ja nimen omaan TVO:n ohjaajien suorittamien toimenpiteiden tutkimiseksi ajettiin normaalin simulaattorikoulutuksen yhteydessä kaksi vaikeaa häiriötilannetta, joissa mitattiin ohjaajien suorittamiin ohjaustoimenpiteisiin kuluvaa aikaa. Samalla voitiin testata hätätilanneohjeiden käyttöä ja toimivuutta.

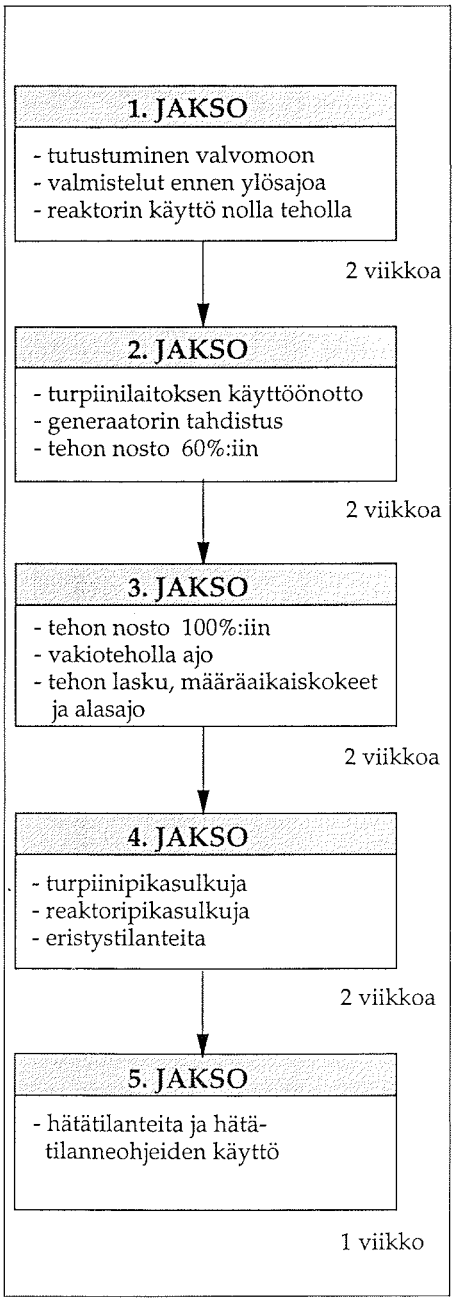
Ensimmäisessä testiajossa menetettiin pääsyöttövesi ja 400 kV:n sähköverkko. Apusyöttövesijärjestelmän automaattinen käynnistys kaikille neljälle osajärjestelmälle oli estetty. Toisessa testiajossa syöttöveden menetyksen lisäksi vikaannutettiin osa lauhdutusaltaaseen puhaltavista venttiileistä auki-asentoon, jolloin reaktorin pinnanlasku on erittäin nopea. Näiden simulointien tuloksena voitiin perustellusti tarkentaa manuaalisten toimenpiteiden onnistumistodennäköisyyden mallinnusta PSA:ssa.

PSA-tulosten hyödyntäminen

Sen lisäksi, että koulutussimulaattoria on käytetty PSA-analyysien tarkentamiseen, on tehty myös päinvastoin eli hyödynnetty PSA-tuloksia simulaattorikoulutuksessa. Palo-PSA:n tuloksista on kerätty tietoja siitä, mitkä laitteet ja sähköjärjestelmien osat menetetään tulipalon sattuessa jossakin huonetilassa. Palotilanne toteutettiin ensin simulaattorilla, minkä jälkeen jokainen käyttövuoro kävi palomiehen johdolla tutustumassa laitoksella siihen tilaan, jossa oli kuviteltu tulipalo.

VTT:n tutkimus

TVO on tilannut Valtion teknillisen tutkimuskeskuksen sähkö- ja automaatiotekniikan laboratoriolta tutkimuksen, jonka nimenä on "Vuoron yhteistoiminta häiriötilanteessa". Tutkimus liittyy VTT:llä suoritettavaan ydinvoimalaitoksen turval-



Simulaattoriperuskurssin ohjelma

lisuuden hallintaa koskevaan SAMA-projektiin ja se kohdistuu valvomovuoron yhteistoiminnan ja kommunikaation kehittämiseen häiriötilanteen hallinnassa. TVO:n kannalta tutkimus palvelee simulaattorikoulutuksen kehittämistä ja edistää sitä kautta ohjaajien ammatillista pätevyyttä.

VTT:n tutkimuksen aikana on tarkoitus kehittää uusi menetelmä vuoron yhteistoiminnan arviointiin osana tavanomaista kouluttajan palautetta. On tarkoitus, että vuorot pystyisivät arvioimaan itse omaa toimintatapaansa. Tutkimuksen erityistavoitteena on selvittää, mitkä tekijät vuoron yhteistoiminnassa parantavat suoriutumista.

Palaute laitokselle

Simulaattorikoulutusta pyritään hyödyntämään myös siten, että kouluttajat antavat palautetta suoraan laitokselle. Kuten aikaisemmin mainittiin, on varsin hyödyllistä testata niin normaaliajon kuin myös häiriöajon käyttöohjeita. Simulaattorikurssin ajo-ohjelmaa laadittaessa samoin kuin simulointimalleja testattaessa joudutaan varsinkin automaattisia toimintoja tutkimaan tarkasti. Tällöin saattaa tulla esille parannusehdotuksia, joista annetaan käyttö- tai turvallisuusorganisaatiolle muutosehdotus. Tämän tyyppisiä muutoksia on laitoksilla suoritettu muutamia.

Paikallisohjauspääte

Normaaliajossa joudutaan ohjaamaan esim. venttiileitä, pumppuja ja katkaisijoita päävalvomon ulkopuolelta. Simulaattorikoulutuksessa tämä on yleensä toteutettu siten, että kouluttajat suorittavat nämä toimenpiteet kouluttaja-aseman päätteeltä. TVO:ssa asia on ratkaistu kuitenkin liittämällä kouluttajajärjestelmään erillinen ns. paikallisohjauspääte, joka on sijoitettu simulaattorivalvomon vieressä olevaan huoneeseen. Koulutettavat suorittavat itse nämä ohjaukset ja joutuvat poistumaan valvomosta kuten laitoksellakin. Tiedossamme ei ole yhtään simulaattoria, jossa paikallisohjaus olisi toteutettu samalla tavoin.

Simulaattori laitospaikalla

Useissa maissa simulaattorikoulutus on keskitetty koulutuskeskuksiin, joissa on useamman laitoksen simulaattorit. Laitospaikalle on näissä tapauksissa ollut tapana hankkia periaatesimulaattori. Esimerkiksi Ruotsissa on tällainen järjestelmä käytössä, ja siellä on käyty vilkasta keskustelua simulaattorin sijoituspaikasta. TVO:ssa ollaan monesta syystä tyytyväisiä siihen, että simulaattori on saatu laitospaikalle.

Simulaattorijatkokurssi 4

	Maanantai	Tiistai	Keskiviikko
7:00	Simulaattori ajo Ryhmä 1	Simulaattori ajo Ryhmä 1	Simulaattori ajo Ryhmä 1
11.00	Ajon läpikäynti	Ajon läpikäynti	Ajon läpikäynti
11:30	Lounas tauko		
12.00	VLJ-varasto	Lauhdejärjestelmä ja 441-pumput	TVO 2:n palo
13.00	TTKE-muutokset	Lauhdejärjestelmä ja 441-pumput	TVO 2:n palo
14.00	Kotimaiset ja ulkomaiset käyttöhäiriöt	Polttoainevuodonseuraukset	Seuranta
15.00	Ruokailu		
15.30	Simulaattori ajo Ryhmä 2	Simulaattori ajo Ryhmä 2	Simulaattori ajo Ryhmä 2
19.30	Ajon läpikäynti	Ajon läpikäynti	Ajon läpikäynti
20.00			

Simulaattorijatkokurssin lukujärjestys

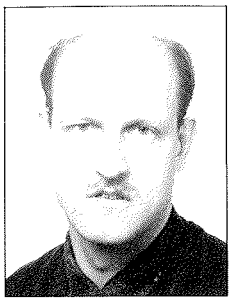
TAPIO SAARENPÄÄ
Teollisuuden Voima Oy
Instrumentointitekniikan toimiston automaatioinsinööri
puh. 938-381 4312

KAUKO YLI-ANTOLA
Teollisuuden Voima Oy
Koulutustoimiston yleiskoulutusjaoksen päällikkö, puh. 938-381 3510

EERO PATRAKKA
Teollisuuden Voima Oy
Koulutustoimiston päällikkö
puh. 938-381 3500 tai 90-6090 6022

MARKKU MALINEN
Teollisuuden Voima Oy
Koulutustoimiston käyttökoulutusjaoksen päällikkö, puh. 938-381 3520

Olli Nevander



PERUSSYYANALYYSI POLKUMENETELMÄLLÄ

Ydinvoimalaitoksen turvallisuutta uhkaavat ilmiöt ja tapahtumat pyritään selvittämään mahdollisimman hyvin etukäteen. Mahdollisia laitteiden aiheuttamia turvallisuusriskejä pienennetään analysoimalla laitoksen käyttäytymistä poikkeustilanteissa ja varautumalla laitteiden toimintahäiriöihin rinnakkaisilla laitteilla. Ihmisten häiriö- ja poikkeuskäytökseen on vaikeampi varautua ennalta.

Yksi osa inhimillisten riskien pienentämistyötä ovat perussyyanalyysimenetelmät. Ne tarjoavat mahdollisuuden parantaa inhimillisiä heikkouksia, organisaatio- ja toimintamalleja sekä ennenkaikkea mahdollistavat maksimaalisen käyttökokemuksien hyväksikäytön. IVO:ssa kehitetyssä menetelmässä on käytetty perussyyanalyysin tehokkaimpia elementtejä: toistuvuutta ja korjaavien toimenpiteiden todentamista.

Voimalaitoksen organisaatio ja toiminnot rakentuvat samoista lähtökohdista tuotettiin generaattoria pyörittävä höyry sitten polttamalla hiiltä, turvetta, kaasua tai öljyä, tai säätelemällä itsestään lämpeneviä uraanitankoja. Voimalaitoksen rakenteiden ja organisaation rakentaminen ja käyttäminen edellyttää aina samankaltaisten "rakennuspalikoitten" käyttöä. Näitä ovat: suunnittelu, valmistus, asennus, käyttö, kunnossapito ja johtaminen.

Maanalaiset rakennuspalikat

Haluttaessa lisätä voimalaitoksen kustannustehokkuutta tai turvallisuutta muidenkin kuin suorien elementtien käyttö on tarpeen. Yleensä vähänkin monimutkaisemman voimalaitoksen kustannuksiltaan tehokas ja turvallinen käyttö edellyttää myös epäsuorien "rakennuspalikoiden" käyttöä. Näistä "rakennuspalikoista " käytetään tässä nimitystä epäsuorat turvallisuuselementit. Osa epäsuorista turvallisuuselementeistä on ydinvoimalaitosten käyttöä säätelevissä laeissa, asetuksissa ja ohjeissa säädetty käytön ehdoiksi.

Tärkeimmät epäsuorat turvallisuuselementit ovat:
onnettomuusanalyysit, laadunvarmistus, todennäköisyyspohjaiset onnettomuusanalyysit (PSA), käyttökokemusten arviointi, perussyyanalyysit ja turvallisuuskulttuuri. Näistä ehkä vähiten tunnettu on tässä esiteltävä perussyyanalyysi.

Juurivauriot esiin perussyyanalyysillä

Perussyyanalyysi on työkalu, jonka avulla pyritään löytämään poikkeuksellisen laitostapahtuman taustana olevat syyt: perussyyt. Perussyy, heikohko käännös englannin termistä "root cause", on määritelmänsä mukaan syy, joka poistamalla tutkittavan tapahtuman kaltaiset tapahtumat vältetään. Perussyyn etsintään liittyy aina myös korjaavien toimenpiteiden etsintä.

Perussyyanalyysi maailmalla

Lähes kaikissa länsimaisissa ydinvoimalaitoksissa käytetään perussyyn selvitykseen jonkinlaista järjestelmällistä ja ennalta ohjeistua selvitystapaa, analyysimenetelmää. Tällaisia ovat mm. IAEA:n käyttämä ASSET-menetelmä, INPO:n laitoksille markkinoima HPES tai ruotsalaisen KSU:n HPES-menetelmän pohjalta kehittämä MTO-menetelmä. Perussyyanalyysimenetelmien esiasteina voi pitää myös IAEA:n ja NEA:n tapahtumaraportointijärjestelmiin kuuluvaa tapahtumien luokittelua ja tapahtuman vakavuusluokitteluun käytettävää INES-asteikkoa seikkaperäisine sovellusohjeineen.

Kaikki varsinaiset perussyyanalyysimenetelmät painottuvat inhimillisten virheiden etsintään ja niiden "pään" sisäisten tai ulkopuolisten syiden arviointiin. Tämä on tietysti luonnollista, koska riittävän kauan haettaessa saadaan ihmisen rakentamassa tekniikassa perussyyksi — ihminen — vajavaisine kykyineen suunnitella, toteuttaa ja ennalta varautua.

Laitosorganisaatio poistaa perussyyn

Kehitetyn menetelmän perussyy on aina korjattavissa. Perussyy ei voi menetelmämäärittelyn mukaan olla laitoksen tai käyttöorganisaation korjaavien toimenpiteiden ulottumattomissa. Tämä tarkoittaa käytännössä laitoksen omien varmennusten ja tarkastusten lisäämistä, jos esim. toimitettu komponentti todetaan vialliseksi. Löydetty perussyy voi tietenkin alunperin sijaita käyttöorganisaation ulkopuolella esim. alkuperäisessä suunnittelussa tai asennuksessa, mutta korjaavat toimenpiteet pitää toteuttaa nykyisen käyttöorganisaation sisällä.

POLKUMENETELMÄN VAIHEET

Vanhojen kaivelu

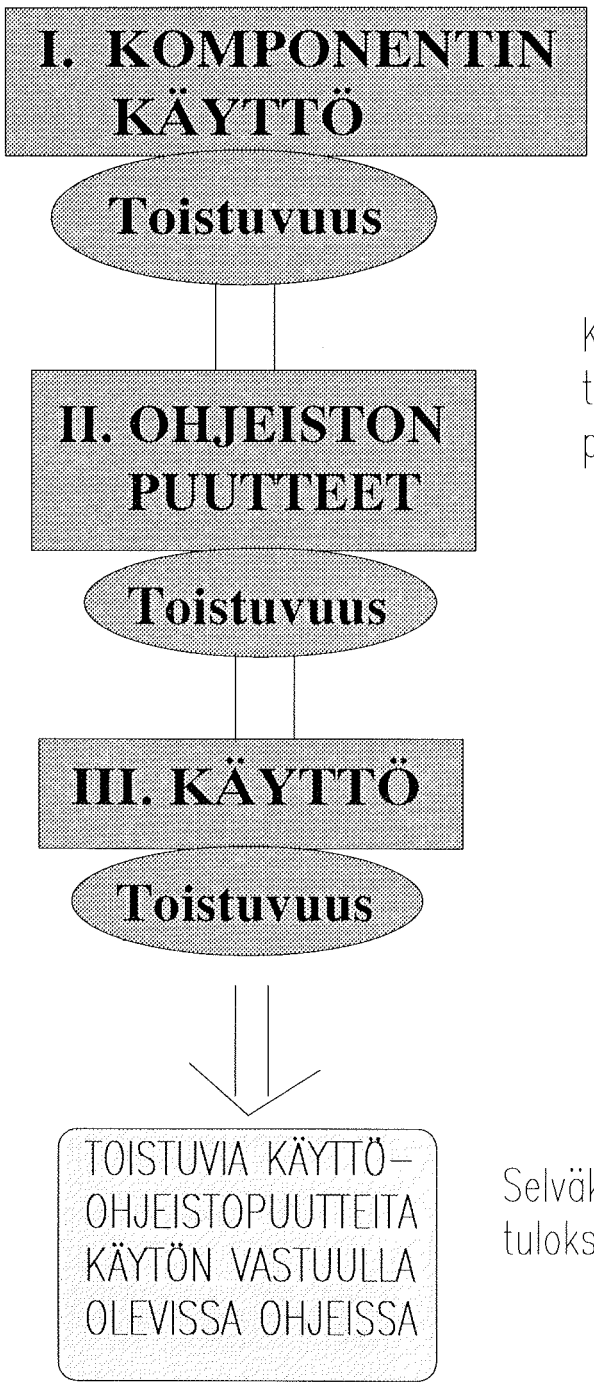
Vastaaviksi määritellyt tapahtumat haetaan käymällä läpi seuraavat tietolähteet: laitoksen kunnossapitohistoria, kansainväliset tapahtumatietopankit sekä tapahtumaselvitykseen kuuluvien haastattelujen kohteiksi valittujen henkilöiden muistikuvat.

Ennen polkukierrosten läpikäymistä arvioidaan dokumenttien keräämisen, vastaavanlaisten tapahtumien muistelemisen ja haastattelujen perusteella mahdolliset syyt, joiden mahdollinen toistuvuus oman tai vastaavien laitosten historiassa haetaan esille. Löydetyt tapahtuman syyt eivät useimmiten ole etsittyjä perussyitä.

Saman syyn löytyminen tapahtumien taustalta johtuu: merkittävästä puutteesta käyttökokemuksista oppimisessa, puutteesta laitoksen alkuperäisessä suunnittelussa tai samasta perussyystä, joka aiheuttaa seurauksia satunnaisesti eri osa-

→

KIERTOPROSESSIN TULOKSENA SAATAVA YHDEN PERUSSYYN POLKU



Kiertoprosessin tuottama kolmiportainen polku

Selväkielinen selitys tuloksesta: perussyy

alueilla. Sama perussyy on esim. vastuusuhteiden epäselvä jako kahden organisaatioryhmän kesken, joka saattaa näkyä ohjeistopuutteina ja työn suoritusvirheinä molempien ryhmien toiminnassa.

Perussyyn etsintä

Varsinainen perussyyn etsintä on prosessi, jossa jokaisen perussyyn kohdalla toistetaan useaan kertaan vaiheet: perussyyehdokkaan arvaaminen, perussyyehdokkaan luokitus ja perussyyehdokkaan toistuvuuden arviointi.

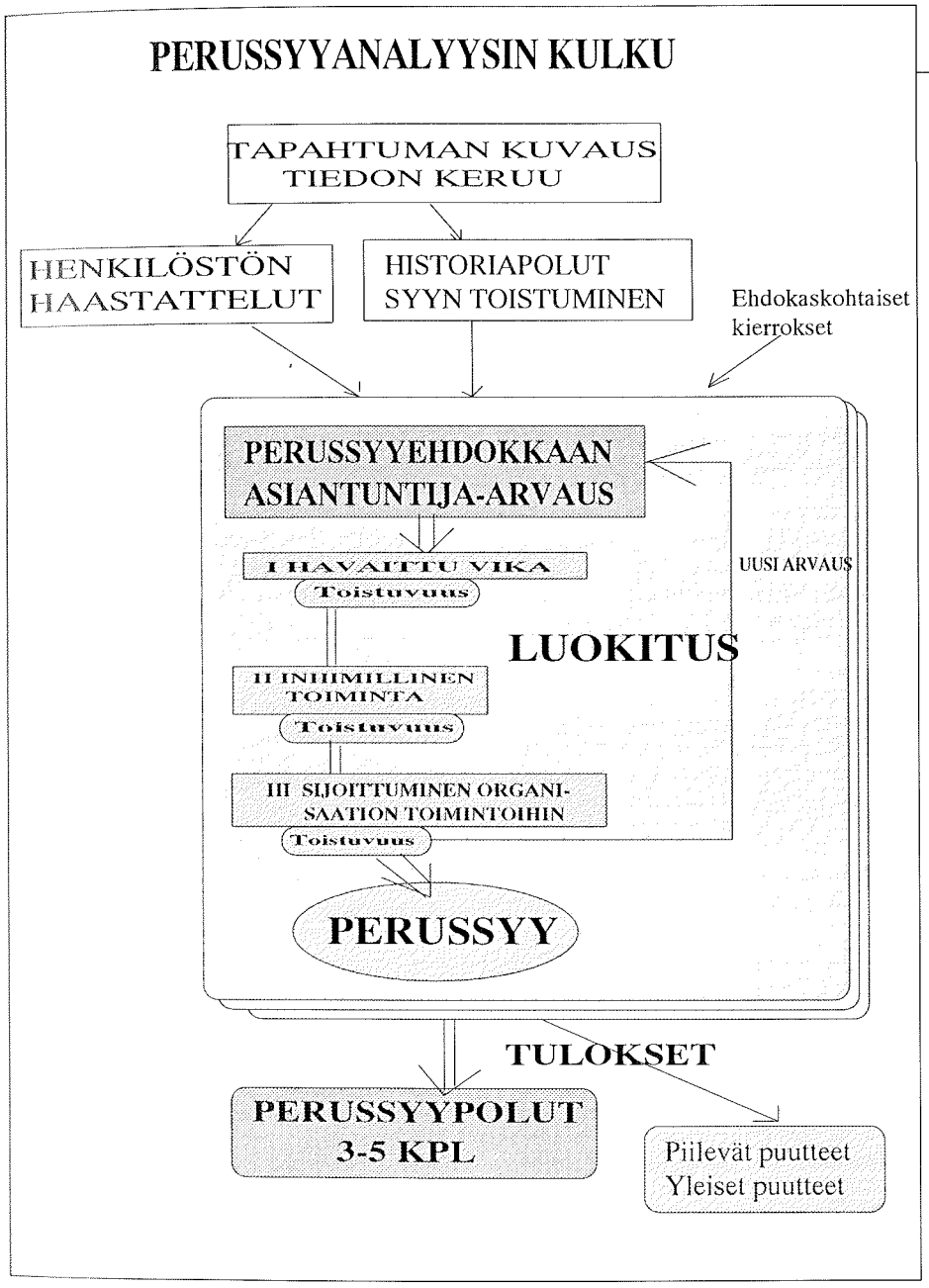
Luokitus

Luokituksessa perussyyehdokkaalle valitaan sopiva kolmeen ryhmään kuuluvista luokista. Nämä ryhmät ovat: havaittu vika, inhimillinen toiminta ja sijoittuminen organisaation toimintoihin.

Luokalla I: "Havaittu vika" pyritään määrittelemään perussyyehdokkaan ajallinen ja toiminnallinen sijainti laitoksen tai laitteen historiassa: luokkia ovat esim. komponentin käyttö, tarkastus, materiaali jne. Luokalla II: "Inhimillinen toiminta" pyritään jakamaan perussyyehdokkaat ihmisen toiminnan mukaan. Luokan II luokkia ovat esim. ohjeiston puutteet, koulutus, pätevyys, jne. Luokalla III: "Sijoittuminen organisaation toimintoihin" pyritään kohdentamaan havaittu puute tiettyyn osaan organisaatiota, johon korjaavat toimenpiteet on helppo kohdistaa. Näitä luokkia ovat esim. kunnossapito, käyttö, suunnittelu jne. Luokittelun tarkoituksena on tehdä työskentely järjestelmälliseksi, pakottaa työryhmään kuuluvat asiantuntijat ajattelemaan muitakin kuin valmiita "latujaan" sekä helpottaa korjaavien toimenpiteiden kohdentamista tiettyyn osaan laitoksen organisaatiota ja toimintoja.

Toistuvuus

Perussyyehdokkaan toistuvuuden arviointi tehdään luokkakohtaisesti ja se tarkoittaa taas vanhojen kaivelua:
käydään läpi vanhat perussyyanalyysit, käyttöhäiriöt ja muistikuvat, jotta saadaan selville löytyykö perussyyn toistuvuutta. Toistuvuus arvioidaan sekä menneisyydessä että tulevaisuudessa: Onko vastaava perussyy aiheuttanut tapahtumia aiemmin? Voiko perussyy aiheuttaa tapahtumia tulevaisuudessa?



Perussyyn toistuvuuden arviointi menneisyydessä todentaa tai korjaa samalla aikaisempien perussyyanalyysien korjaavat toimenpiteet.

LOPPUTULOKSET

Prosessiin siis kuuluvat vaiheet: luova perussyyehdokkaan päätteleminen taphtumakuvauksen perusteella: "asiantuntija-arvaus", saadun perussyyehdokkaan perusteella suoritettava luokitus, perussyy ehdokkaan toistuvuuden luokkakohtainen arviointi, kyllä — ei kysymyksin uuden luokan tai uuden perussyyehdokkaan arvaaminen, uuden ehdokkaan luokitus ja toistuvuuden arviointi.
Perussyyehdokasta kohti muutaman kerran toistetun kiertoprosessin tuloksena on lopulta joukko perussyyehdokkaita ja niitä vastaavat luokitukset ja korjaavat toimenpiteet. Nämä voidaan esittää polkuna: Luokka I—Luokka II—Luokka III -perussyy sanallisesti esitettynä—Korjaavat toimenpiteet.

Ei paperin makua korjauksiin

Polkumenetelmälle on ominaista myös lopppuvaihe, jossa käydään läpi korjaavat toimenpiteet asianosaisten kanssa. Käytännössä tehdään joukko haastatteluja, joissa arvioidaan korjaavien toimenpiteiden tehokkuus tapahtuman toistumista estettäessä. Korjaavien toimenpiteiden käytännön arvioinnilla pyritään välttämään turhat mielekkyydeltään kyseenalaiset korjaavat toimenpiteet, joiden toteutus jää puolittaiseksi.

Perussyyanalyysityöryhmän ehdottamat korjaavat toimenpiteet joutuvat tietenkin kunkin laitoksen päätöksentekijöiden arviointiin mm. kustannusten ja toteutusaikataulujen osalta.

Menetelmän ominaisuudet

Menetelmän antamat perussyyt painottuvat inhimilliseen toimintaan, koulutukseen ja ohjeistoon, kuten kaikille perussyyanalyysimenetelmillä.

Menetelmän käyttö on työryhmätyötä: haastattelujen tekoa, vanhojen dokumenttien kaivelua, tapahtumien vertaamista jne.

Koska tapahtumien, syiden ja perussyiden toistuvuus on menetelmän kulmakivi riippuu menetelmän tehokkuus ja käytön viemä aika aina käyttäjästä.

Käytännön läheisyyttä on pyritty lisäämään edellyttämällä, että menetelmän tuottamat korjaavat toimenpiteet käydään aina läpi yhdessä tapahtumaan osallisten kanssa niiden mielekkyyden arvioimiseksi.

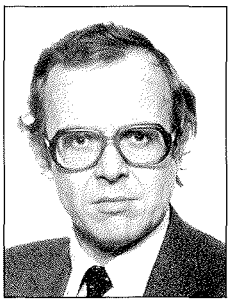
Käytössä Loviisassa ja tulevaisuudessa koko IVO:ssa

Polkumenetelmää on käytetty Loviisassa vuoden 1992 alusta lähtien laitostapahtumien arviointiin. Kaikille tapahtumille, jotka edellyttävät viranomaiselle tehtävää erikoisraporttia on tehty joko täydellinen perussyyanalyysi tai ainakin yksinkertaistettu luokittelu ja polkujen läpikäynti. Tehdyt tapahtuma-analyysit ovat tuottaneet 3-5 perussyytä/analyysi ja vastaavan määrän korjauskohteita laitoksella.

IVO:ssa on tällä hetkellä käynnissä kehityshankkeita, joissa pyritään perussyyanalyysiin liittyvien tapahtumaselvitysmallien käytön laajentamiseen myös konventionaalisille voimalaitoksille.

DI Olli Nevander työskentelee IVO International Oy:ssä turvallisuusinsinöörinä ja on tämän lehden toimitussihteeri, p. 90-5082613.

Björn Wahlström



HUMAN ERRORS AND MISTAKES

Human errors are well known to everybody. They are often considered to carry a blame ie. the person making an error has not given proper attention to his task. Today it is however recognized that human errors have a cause which often is outside the control of the person who made the error. This cause is buried in the design of man-machine interfaces, operational procedures and operator training. With proper system design it is possible to decrease the likelihood of human errors.

An operative explanation of human errors is that they are caused by a resource and demand conflict. This explanation gives a prescription for improving safety. An understanding of difficulties involved in decision making tasks can provide suggestions for additional support systems and therefore a resolution of such conflicts. A systematic search for transients and disturbed situations, which are likely to create abnormal cognitive demands, can thus make it possible to improve the systems.

Studies indicate that 30-70% of all incidents and accidents are either directly or indirectly caused by human errors. The numbers are perhaps revealing more about the depth of the analysis than the actual situation. An analysis of incidents is tracing backwards in the causal chains by asking the question why for observed deviations from accepted norms. In this backtracking procedure there is no formal stopping criterion, because even obvious deficiencies should be further investigated.

SYSTEM ACCIDENTS AND COMPLEXITY

Incidents are often initiated by small operational disturbances which are aggravated by latent failures. A simple transient can thus take a more serious path. Additional stress in responding to unfamiliar signals makes additional errors more likely. If important safety barriers are unfunctional, then even simple transients can take more serious turns. There is usually a relative long latency periods before an incident changes into an accident.

Large accidents (TMI, Bhopal, Chernobyl, Challenger) have shown that many different causes of technical, human and organizational origin are interacting in the sequences of events. Such accidents tend to occur in tightly coupled systems where unexpected interactions between subsystems are brought into the open. Incidents and accidents should be analyzed within a framework of multiple technical, organizational and personnel perspectives. It may even be necessary to expand the analysis beyond the plant and the company operating it, to the regulatory system and the governmental decision-making processes.

Accidents usually reveal deficiencies both in the social and technical control systems. There are often organizational causes for such deficiencies. The errors can again be seen as caused by resource and demand conflicts within the management system. Deficiencies in goal formulation, task definition, feedback of experience, quality assurance and maintaining skills can have a simultaneous influence on safety precautions.

A driving force behind system accidents is a search for improved performance and efficiency. People and organizations are actually performing experiments with the systems to explore borders of a safe operational envelope. An accident can occur when these borders are crossed. Hidden deficiencies are typical for system accidents. Sometimes deficiencies are not even known to pose a safety threat. More often however the hidden deficiencies are not detected due to deficient monitoring procedures. Sometimes the deficiencies are known, but are not corrected, because it is considered unnecessary or too expensive. Most of the problems identified after the TMI accident were actually known beforehand. The Chernobyl accident was a larger surprise, because nobody had seriously considered the possibility that operators might disconnect important safety systems.

System accidents are caused by unexpected interactions between the technical and the social control systems. The complexity of the systems and the interactions implies that the sequences of such events are unpredictable. The unpredictability makes it more likely that the humans in the systems make subtle errors. These errors are interacting in unexpected ways to give a sequence of events containing both deterministic and probabilistic components.

ADAPTING THE SYSTEM TO ITS OPERATOR

The control room has a large influence on how the operators are responding to transients. Investigations of actual control rooms often reveal serious nonconformity even with obvious ergonomic principles. Structuring displays and controls to give the operators an easy access to relevant information is not a straightforward task, but it can be approached by using available guidelines.

Well written and correct procedures are another important part in adapting the system to the operator. Their correctness can be evaluated using simulators and their format can be checked by available guidelines. Relative merits of event and symptom based procedures have been objects for a broad international discussion. The appropriateness of these two approaches depends on to what extent the initiating event can be identified with a large certainty.

Operator support systems can be used to decrease the cognitive load of the operators in disturbed situations. Information should be combined and presented in an easily accessible way. A common requirement in nuclear installations is to have a safety parameter display system (SPDS). The reactor vendors have approached these requirements in different ways. Operator support systems have an additional benefit of forcing a more explicit discussion of operational goals.

Operator support systems can be designed for any task or subtask. Some systems can be aimed on the detection of abnormal conditions and other on the

identification of dangerous situations. Support systems can also be designed for helping the operator in managing the procedures, keeping track of the maintenance status of the plant, managing emergencies, etc.

Control room mock ups and training simulators can also be considered as support systems aimed at giving the operators a possibility to gain familiarity with the plant and certain abnormal situations. Training simulators are used for initial training and a continuous retraining.

It is important to build a good system already from the beginning, because changes are always expensive and difficult make. Operational goals should be set before the system is designed and their realization should be monitored as the design proceeds. There is also a need for an early evaluation of preliminary designs by using mock-ups and simulators.

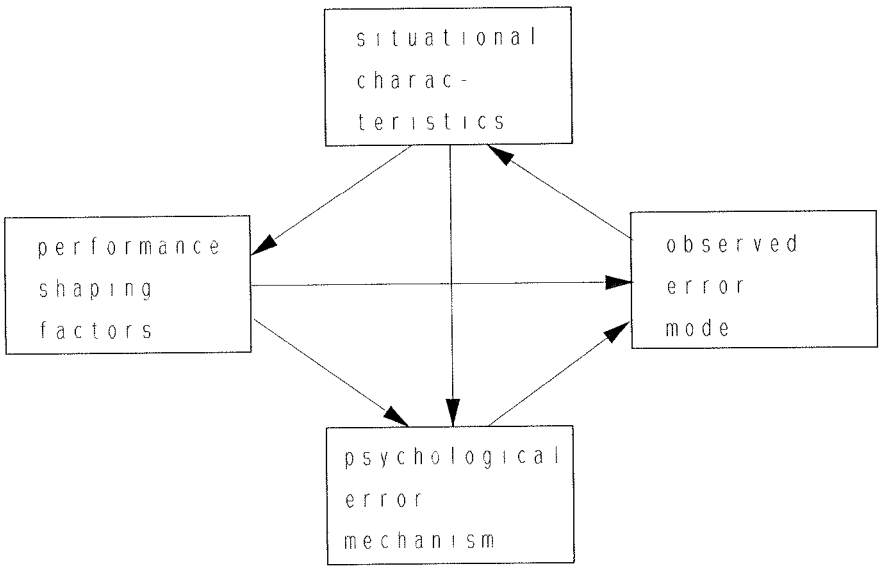


Figure 1. Internations between characteristics of human error.

MODELS OF HUMAN DECISION MAKING

Early attempts to model a human in a control task were initiated in the response to problems with supersonic aircrafts. A simple model of the human controller together with a stability analysis showed that certain aircraft dynamics could make the control unstable.

Other models were developed in response to other needs. The control room situation suggested efforts to be spent on the detection of an abnormality from a large number of meters. Queuing models were developed to mimic the allocation of attention to different tasks in a control room environment.

Among the modelers it soon became evident that these models could not be used for an understanding of human operators in the control room. Jens Rasmussen has in several papers been arguing for using a general structure of models rather than a single model. His notion of skill, rule and knowledge based behavior has been widely adopted.

Another important distinction is a separation between slips and mistakes, where a slip is identified immediately as an error, but a mistake is a true error in the sense that the operator thought the action was correct until a more accurate analysis revealed that it was not. To these categories a category of intentional errors, eg. sabotage and drug misuse, could be added.

A large research effort has been devoted to assessing the influence of human performance in different situations. Situational factors such as man-machine interface, procedures, time and stress are known to shape the performance, but no model has been constructed which is able to give accurate predictions. An additional difficulty is connected to the interactions between situational characteristics, performance shaping factors, psychological error mechanisms and the observed error mode.

In building a model of human decision making a simplified structure can be used. A need for a decision is detected and this is either handled using heuristics in a stimulus response mode or submitted to a conscious consideration. Proposed actions are evaluated using an internal model to give a prediction of outcomes connected to certain actions. This outcome is assessed on a good/bad scale using a value system. Erroneous heuristics, internal models and values are obvious sources of human errors.

Human errors have been modelled in a probabilistic safety analysis (PSA) framework. It is however unpractical to consider all possibilities of human errors. Another difficulty is connected to the need for assigning an error probability to specific actions. Human error probabilities (HEP) are dependent on time, because if no time is available then an error will be certain (HEP0 = 0) and with an infinite time available errors can be avoided (HEP = 1). Attempts have been made to give believable HEP estimates without a real success.

HOW CAN HUMAN ERRORS BE AVOIDED?

The first more systematical assessment of human errors in the nuclear field, was included in the so called WASH-1400 report. This study of the early seventies represented a major step towards the almost routine application of the risk analysis methodology of today. The human errors considered in this study where however relatively simple errors ofomission and commission. The assessment methodology of this study was the so called THERP methodology. It gives a first order approximation, but it is far too simplistic for cognitively demanding situations.

The risk analysis framework provides a systematic methodology for assessing different sequences of events having unwanted consequence. Human errors can be included to interact with the sequences and a total risk estimate can be calculated. The human reliability estimates are unreliable, but the sensitivity of the final →

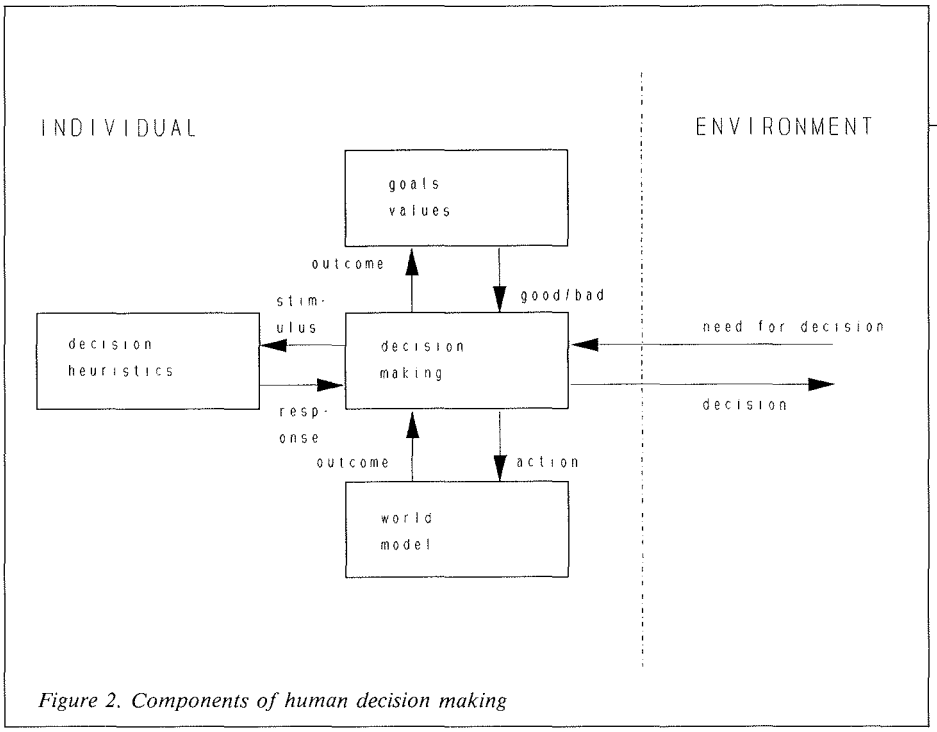


Figure 2. Components of human decision making

result to the assumptions can provide valuable insights. The methodology is very useful for improving the design of new systems.

Is it possible to get errorless performance? The answer is certainly no, because no design can take all contributing factors into account. There are also components of stochasticity in human behavior which make occasional slips possible. It can actually be argued that hidden deficiencies can be detected only through incidents and accidents and we therefore may need the incidents to put headlights on necessary improvements.

A pursuit of a high safety includes a successful management of several conflicting requirements. Safety engineers should be able to dream up credible safety threats, but still be convinced that the installation is completely safe. Automation and operator support systems can improve the safety, but can also impoverishing the skills of the operators. Prethought responses to disturbed conditions are always better than improvisations, but no transient will develop exactly as expected. Good performance can give place for further improvements, but can also throw the organization of guard.

An approach towards safety should always be proactive. This means there should be a continuing effort evaluating also subtle safety threats. The most important prescription for avoiding human errors is to establish an efficient system for the feedback of experience. This system should analyze near misses at own and similar installations. Whenever deficiencies are detected they should be corrected before they have been contributing to something more serious.

The division of tasks between the human operators and the automation system should be clearly defined. Automation is more reliable than humans, but humans can generate sensible responses also in new situations. The operators should be given feedback on their actions. Interlocks should be provided to make it possible to reverse erroneous actions before it is too late. Information should be structured into suitable "chunks". Alarm filtering should be used to avoid information overload during transients. Displays and controls should be structured to present process state and operational goals in an easily comprehendible way. A task analysis should be used to identify excessive demands on the human operator.

The use of training simulators both for initial training and retraining is important. Important transients should be drilled at regular instants, because seldom exercised operations tend to be forgotten. In depth analyses of accident precursors, symptoms and remedial actions should be carried out to give a better understanding of system safety. A participation in research and development projects has the provision of giving the operators a deeper understanding of different contributors to a safe operation.

Safety culture has in the nuclear community been proposed as an approach to foster good operational practices. The concept and some proposed review methods are certainly necessary steps toward an understanding of organizational deficiencies. The question how safety oriented organizations should be managed is however broader. It has even been argued that the organizations actually perform better than what would be expected. One important ability is that organizations are able to handle apparently conflicting objectives.

CONCLUSIONS

The treatment of human errors in the probabilistic safety analysis (PSA) framework has not been completely resolved. The difficulty is connected to the need for giving a numerical estimates for human error probabilities. A high human error probability can introduce expensive investments in automation and redundancy without proper assurance that the fixes are not counterproductive. A resolution of this problem is not only improved models of human behavior, but also a better understanding of the strengths and limitations of the PSA methodology itself.

Existing models of human behavior can be improved in many ways. Predictions for how operators will react in certain situations are needed. Team work is not understood well enough. Maintenance and repair tasks are critical in many ways. Communication between groups of people can sometimes introduce subtle errors and misinterpretations. The influence of organization and management on human errors is not well understood.

In spite of the theoretical difficulties in approaching human errors many good prescriptions are available for decreasing their likelihood. With this fact in mind, it is astonishing that real systems often provide many examples of bad design. This points to a deficiency in present information dissemination and utilization. There seems to be a rather slow and inefficient exchange of experience between different industrial sectors as well as between research and practice.

Björn Wahlström, Technical Research Centre of Finland, VTT/SÄH, P.O.Box 34, SF-02151 Espoo, Finland

Mika Kivimäki, Ph.Lic., Researcher and
Raija Kalimo, Prof., Departmental Director
Institute of Occupational Health, Department of Psychology

ATTITUDES TO RISKS IN NUCLEAR ENERGY PRODUCTION: THE PERSONNEL'S VIEW

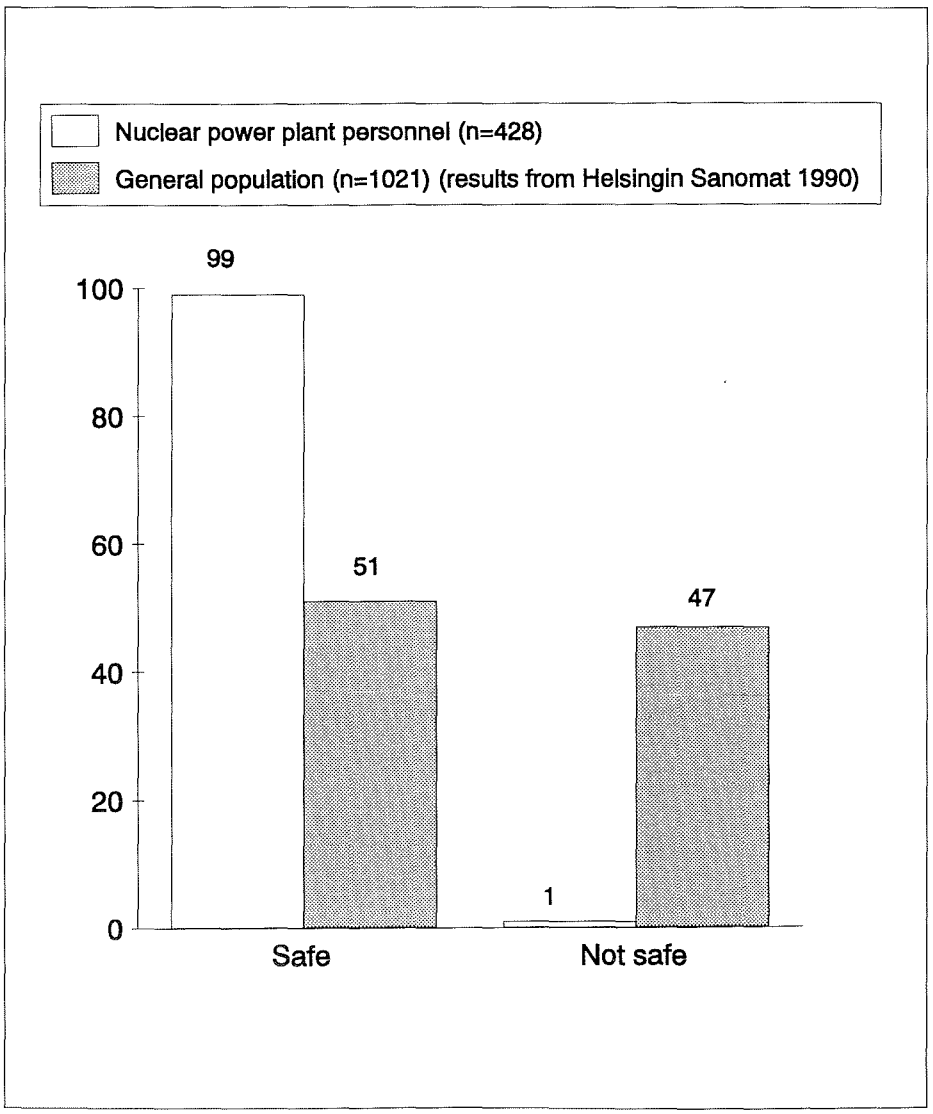
This survey investigated risk perception among nuclear power plant personnel. The study group, 428 employees from a nuclear power plant in Finland, completed a questionnaire which contained the same questions as those in previous surveys on the risk perception of lay persons and industrial workers. The main emphasis of the study was on perceived risk at work and subjective estimations of a serious nuclear accident.

The purpose of the study was to chart the risk-related attitudes that the personnel of a nuclear power plant have, and to study how these attitudes differ from those of other workers in industrial companies and of the general public. The subjects were 428 persons, 80 % of the entire staff of a western-type nuclear power plant in Finland (80 % men and 20 % women; mean age 39.7 years, SD 8.0 years). 32 % of the subjects belonged to managerial staff (including chiefs, supervisors, managers and planners), 27 % were technical employees, 14 % office staff, and 27 % blue-collar workers. The data were collected in the beginning of 1992 by a questionnaire consisting of questions previously used in surveying the attitudes of the general public and of industrial workers (Kalimo et al. 1981, 1989, Elo & Tuominen 1987, Hänninen et al. 1987, Helsingin Sanomat 1990, Kiljunen 1991).

RISKS IN NUCLEAR ENERGY PRODUCTION ARE NOT EXPERIENCED AS A NOTABLE PROBLEM

Ninety-nine per cent of the plant personnel felt that the production of nuclear energy is completely or almost safe. Two per cent of the plant personnel estimated that a serious nuclear power plant accident in the future is quite likely at their own workplace or elsewhere in Finland. There were no significant differences in attitudes between the professional groups or between the persons working in the controlled areas and the others. Compared to a large random sample of the general population in Finland, the plant personnel estimated the safety of the nuclear power plant to be better and an accident in the future as less likely.

Of the nuclear power plant personnel, 68—75 % reported that they were seldom or never at risk of injuring themselves or somebody else at work. 47 % estimated that there was never or seldom any risk of destroying accidentally a valuable machine or work output or of causing great material damage at work. Blue-collar workers ($F = 56.60$, $df = 3$, $p < 0.001$ and the personnel working in the controlled areas ($F = 51{,}99$, $df = 1$, $p < 0.001$ experienced work-related risks more often than did the other professional groups.



Comparison of the results to other industrial employees showed that the overall perceived risks at work of the plant personnel did not exceed the respective risk of the reference groups. The blue-collar workers were the only exception at the plant; they estimated the hazards to be at least as great as the reference groups.

THE PLANT PERSONNEL'S VIEW IS VALUABLE

The estimation of the risks of nuclear energy production was more optimistic among the nuclear power personnel than among the general population. This finding was consistent with the conclusions of the previous American and West-European studies (Lowrance 1976, DuPont 1980, Slovic et al. 1980, Fischhoff & Slovic 1983, Gardner & Gould 1989, McGregor 1991, Sjöberg & Drottz-Sjöberg 1991). The results may indicate, firstly, real differences in the rationally estimated risks, secondly, a self-selection of pro-nuclear energy people to work in the nuclear power plant, and thirdly, some kind of a collective defence and a greater reluctance among the plant personnel to perceive factors which might have a negative effect on the company or on their own well-being.

According to the survey, the overall risk at work perceived by the plant workers did not exceed the risk perceived by a large sample of other industrial workers. As a matter of fact, the nuclear plant personnel, excluding the blue-collar workers, experienced their job-related risks as quite small compared to the reference groups in industry. These findings are new, because before this survey, it was not known to what extent the perceived risks at the nuclear power plants correspond to those of the workers in other fields of industry.

Finally, we note that a better understanding of how the plant personnel perceive risk at work may have important implications for the development of safety in energy production. The plant personnel have an opportunity to observe the potential executive, technical and organizational deficits during the working hours. Rationally and systematically used, this kind of information could be of considerable value in the promotion of safety systems.

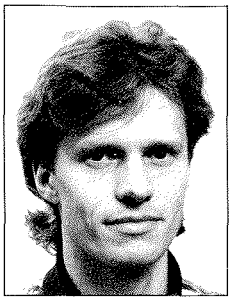
ACKNOWLEDGEMENTS

This study was supported by the Industrial Power Company, Finland.

TABLE 1. Perceived risk at work: Comparison of the study group with previous results on industrial employees (Source: Kivimäki and Kalimo, in press)

	Personnel in the nuclear power plant (n=428)	Employees in industrial companies (n=1344-11142)[a]
Does your work entail a risk of hurting yourself?(%)		
never or seldom	68 (30)[b]	35 - 48
occasionally	24 (50)[b]	30 - 45
often or always	7 (20)[b]	7 - 29
Does your work entail a risk of hurting somebody else?(%)		
never or seldom	75 (54)[b]	79
occasionally	17 (32)[b]	12
often or always	8 (14)[b]	10
Does your work entail a risk of accidentally destroying a valuable machine or work output or of causing considerable material damage?(%)		
never or seldom	47 (32)[b]	24 - 49
occasionally	27 (32)[b]	11 - 53
often or always	25 (37)[b]	21 - 25

[a] results from Kalimo et al. 1981, 1989, Elo & Tuominen 1987, Hänninen et al. 1987
[b] blue-collar workers in parentheses



Ph.Lic. Mika Kivimäki is a Researcher and Prof. Raija Kalimo is the Departmental Director at the Institute of Occupational Health, Department of Psychology, Laajaniityntie 1, SF-01620 Vantaa, Finland, Tel 358-0-47 471, Fax 358-0-890 713.

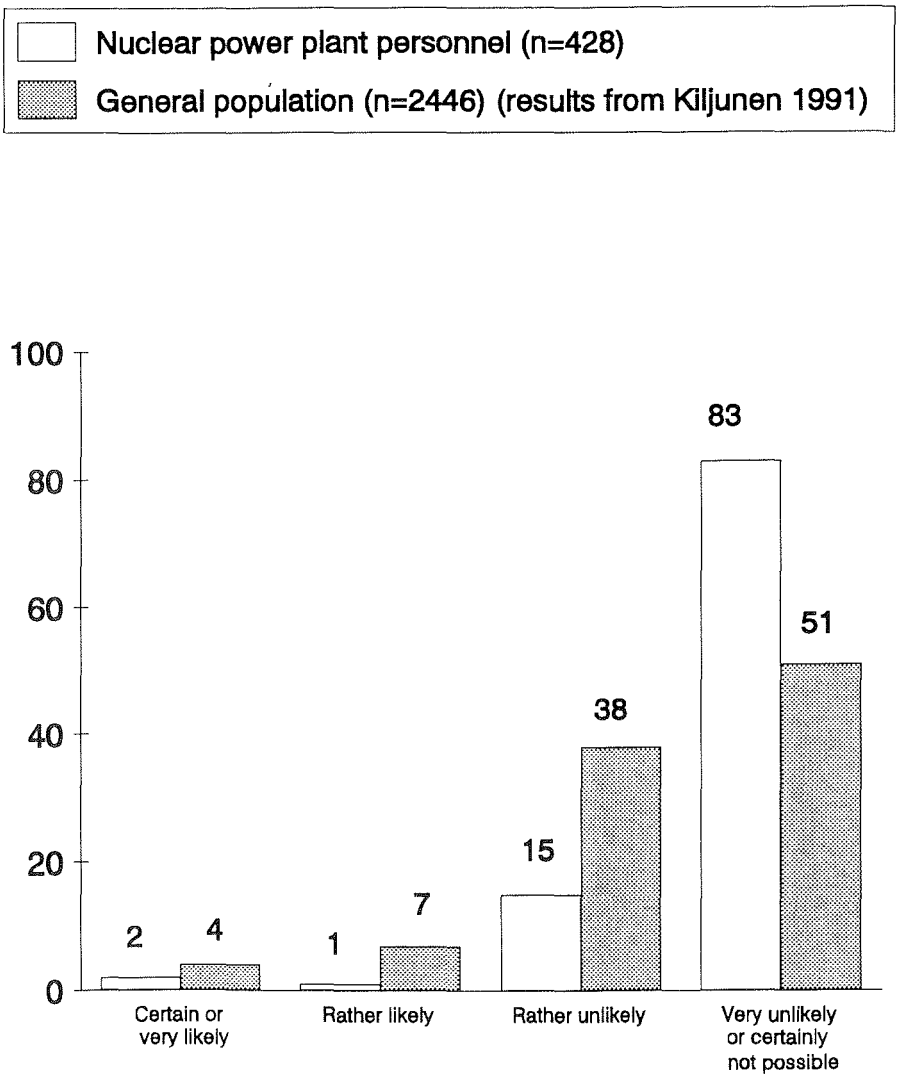


Figure 2. What is the likelihood of a serious nuclear power plant accident in Finland?

REFERENCES

DuPont, R. (1980) Nuclear phobia—phobic thinking about nuclear power. The Media Institute. Washington.

Elo, A.-L., & Tuominen, E. (1987) Stressors in the organization of work, perceived symptoms, and job satisfaction in rubber industry. Työ ja ihminen, 2, 149—162. (In Finnish with English summary).

Fischhoff, B. & Slovic, P. (1983) "The public" vs. "the experts": perceived vs. actual disagreements about risks of nuclear power. In V.T. Covello, W.G. Flamm, J.V. Rodricks & R.G. Tardiff (eds.) The analysis of actual versus perceived risks. Plenum Press. New York.

Gardner, G.T. & Gould, L.C. (1989) Public perceptions of the risks and benefits of technology. Risk Analysis, 9, 225—242.

Helsingin Sanomat (14.12.1990) Perceived safety of nuclear power plants: a survey by Gallup Ltd. Newspaper item, in Finland.

Hänninen, H., Tuominen, E., Rantala, K. & Nyman, K. (1987) Screening of subjective symptoms of early toxic effects. Työ ja ihminen, 3, 201—213. (In Finnish with English summary).

Kalimo, R., Leppänen, A., Seppälä, P., Louhevaara, V. & Koskinen, P. (1981) Work organization, production technology and mental strain: A study in the printing industry. Report of the Institute of Occupational Health, 174. Helsinki. (In Finnish with English summary).

Kalimo, R., Olkkonen, M., Elo, O., Harkki, K., Ruohio, V. & Tuukkanen, A. (1989) Man in progressing production. Final report. The Institute of Occupational Health. Helsinki. (In Finnish).

Kiljunen, P. (1991) Attitudes on energy in 1990: a follow-up study on the public attitudes of the Finnish population toward the energy policy. Tampere University Press. Tampere. (In Finnish).

Kivimäki, M. & Kalimo, R. Risk perception among nuclear power plant personnel: a survey. Risk Analysis (in press).

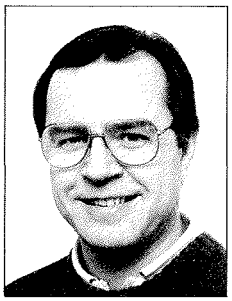
Lowrance, W. (1976) Of acceptable risk: Science and the determination of safety. Kaufman. Los Altos.

McGregor, D. (1991) Worry over technological activities and life concerns. Risk Analysis, 11, 315-324.

Sjöberg, L. & Drottz-Sjöberg, B.-M. (1991) Knowledge and risk perception among nuclear power plant employees. Risk Analysis, 11, 607—618.

Slovic, P., Fischhoff, B. & Lichtenstein, S. (1980) Facts and fears: understanding perceived risk. In R. Schwing & W. Albers,Jr (eds.) Societal risk assessment: how safe is safe enough? Plenum: New York.

Pekka Lehtinen, STUK



Lyhyesti maailmalta

Armenian parlamentti on päättänyt luopua kansanäänestyksestä Armenian ydinvoimalaitoksen maanjäristysuhan vuoksi 1989 pysäytettyjen kahden VVER 440 MW yksikön uudelleen käynnistämisestä. Parlamentti on vakuuttunut ydinvoiman tarpeellisuudesta maan energiatuotannossa. Laitos tuottaisi 25 % Armenian sähköstä. Käynnistämiseen kuluu parisen vuotta.

Nucleonics Week 25.3.1993

Intian haave kahdesta velkarahoitteisesta VVER 1000-yksiköstä näyttää haihtuvan toimittajan rahoitusvaikeuksiin. Aiesopimus tehtiin entisen Neuvostoliiton aikana. Nyt Venäjä ja Intia pitävät hanketta edelleen hengissä, mutta rahoitus riittäisi enää yhteen 500 MW yksikköön. Intia ilmoittaa tulevansa toimeen ilman venäläistä asiantuntija-apua ja on mahdollista, että maa tekee itse korvaavat kaksi pienlaitosta.

Nucleonics Week 15.4.1993

Iso Britannian Sellafieldin käytetyn ydinpolttoaineen jälleenkäsittelylaitoksella sattui helmikuussa työtapaturma, missä radiografiatarkastaja viilsi kyynärpäänsä plutoniumpitoista alfa-aktiivista nestettä sisältävään lasiastiaan. Haavasta puhdistettiin 1 500 Bq alfa-aktiivisuutta, mutta aktiivisten aineiden joutumista verenkiertoonkin pidetään mahdollisena. Asiasta saadaan varmuus biologisten näytteiden analysointien jälkeen kuukausien kuluttua. Tapahtuman vakavuusluokka on 1.

IAEA INES 22.4.1993

Israelin tarkoin vartioidussa Dimonan ydintutkimuskeskuksessa etelä-Israelissa varastoitavaa korkea-aktiivista ydinjätettä saatetaan käyttää fissiilin materiaalin tuotantoon. Jäte sisältää rikastettua uraania ja on peräisin Dimonan ja Nahal Soreqin tutkimusreaktoreista. Käyttökelvoton jätemateriaali loppusijoitetaan alueelle. Dimonan kaupungin asukkaat eivät ole olleet tietoisia toiminnasta ja nyt kaupungin pormestari on vaatinut asiata selvitystä.

Nucleonics Week 4.3.1993

Japanin ensimmäisen täyskokoisen jälleenkäsittelylaitoksen rakentaminen on alkanut. Rokkashomuraan rakennettava laitos on maan kaikkien aikojen mittavin ydinlaitosprojekti. Laitokseen kuuluu 20 rakennusta 3,8 neliökilometrin alueella ja se valmistuu vuonna 2000. Laitos maksaa noin 1000 miljardia jeniä eli 49 miljardia markkaa. Laitoksessa poistetaan käytetystä ydinpolttoaineesta jäämäuraania ja syntynyt plutonium. Aineet voidaan käyttää uuden polttoaineen valmistukseen. Laitos vähentää Japanin tarvetta kuljettaa käytettyä polttoainetta Ranskaan ja Iso-Britanniaan jälleenkäsiteltäväksi.

NucNet 28.4.1993

Liettua Ingalinan ydinvoimalaitoksen jätteenkäsittelyä parannetaan ruotsalaisin voimin (SKB). Ruotsalaiset ovat auttaneet ydinjätehuolto-ohjelman tekemisessä: Käytetyn polttoaineen välivaraston hankinnasta päätetään kevään kuluessa ja kapselointi- sekä loppusijoituslaitosten suunnittelu tullaan käynnistämään lähiaikoina. Keski- ja vähäaktiivisen jätteen loppusijoituslaitoksen suunnittelu aloitetaan. Ruotsin ydin- ja säteilyturvaviranomaiset (SKI ja SSI) valvovat Ruotsin valtion rahoitusta em. parannuksiin ja suunnitteluun.

NucNet 16.4.1993

Ranska on parantanut maailmanennätystään ydinsähkön osuudessa sähköntuotannosta. Uusi ennätys on 78 % ja saavutettiin helmikuun tuotannossa.

NucNet 22.3.1993

Ranskan Superphenix hyötöreaktori muutetaan ironisesti plutoniumin tuottajasta sen kuluttajaksi. Laitos on seissyt korjauksissa yli vuoden ja uuden käyttötavan uskotaan mahdollistavan käynnistysluvan. Laitosta halutaan käyttää myös pitkäikäisen aktinidijätteen hävittämiseen. Ranskan ydinvoimalaitoksissa muodostuu vuodessa seitsemän tonnia plutoniumia, mistä Superphenixin plutoniumpolttoaineessa voitaisiin teoriassa käyttää 0,6 tonnia vuodessa. Hyötö ei ole vielä kannattavaa koska uraanintuotannossa on ylikapasiteettia ja uraanipolttoaineen hinta on edullinen.

Nuclear Engineering International March 1993

Ranskan 57. ydinvoimalaitosyksikkö on valmistunut. Se saavutti kriittisyyden toukokuussa ja kytkettänee valtakunnanverkkoon kesäkuun lopussa 1993. Kyseessä on Goldfech 2 PWR 1 300 MW-yksikkö, joka on viimeinen ranskalaisten 1 300 MW standardiyksiköiden 20 kappaleen valmistussarjasta. Goldfech 2 on sarjan lippulaiva, joka on varustettu mm. onnettomuuden vaikutusten pienentämiseen tarkoitetuilla järjestelmillä kuten suojarakennuksen suodatetulla ulospuhalluksella. Seuraavat ydinvoimalaitosyksiköt tulevat olemaan 1 450 MW kokoluokkaa. Ensimmäisenä valmistuu Chooz-B1-yksikkö vuonna 1995.

Nucleonics week 27.5.1993

Ruotsin Oskarshamn 1 BWR 442 MWe Asea-Atom-yksiköllä on reaktorisra lähtevissä putkissa havaittu läpivuotavia säröjä. Säröt sijaitsevat jälkilämmönpoistojärjestelmän ruostumattomien SIS 2333-25 putkien putkikäyrissä, jotka sijaitsevat ennen eristysventtiileitä. Kyseisiä kohtia ei ole ennen tarkastettu johtuen korkeasta säteilytasosta reaktorin vieressä. Putkiston tarkastusohjelmaa tullaan muuttamaan. Tapauksen vakavuusluokka on 1.

IAEA ERF 17.3.1993

Ruotsin Oskarshamn 1 BWR yksiköllä on löydetty lisää säröjä reaktoriveden puhdistusjärjestelmän putkistossa. Putkien vaihtojen arvellaan kestävän nelisen kuukautta. Säröjen arvellaan aiheutuneen reaktoriveden korkeasta sulfiittipitoisuudesta johtuen ioninvaihtohartsivuodoista ja kylmämuokattujen putkikäyrien huonosta jännityskorroosiokestävyydestä em. olosuhteissa. Oskarshamn 2 yksikön vesikemia on parempi sulfiittiongelman puuttuessa. Barsebäckin ydinvoimalaitosyksikköjen vastaavat putkistot aiotaan myös tarkastaa.

Nucleonics Week 4.4.1993

Ruotsin Ringhalsin neliyksikköisen ydinvoimalaitoksen menoja aiotaan supistaa 10 prosentilla. Laitoksen henkilöstöä (1 200) ei vähennetä, vaikka 50 työntekijän irtisanomisesta on puhuttu. Laitospäällikkö Håkan Johanssonin mukaan henkilöstö on jakautunut epätasaisesti eri tehtäväalueille ja on mahdollista, että ryhdytään tehtäväkierrätykseen. Kustannusleikkauksen suuruus on 100 miljoonaa kruunua ja se on helpoimmin saavutettavissa kunnossapidon leikkauksella muulta kuin turvallisuussektorilta.

Nucleonics week 27.5.1993

Ruotsissa syytetään säteilyannosmittarien hälytysääntä Oskarshamn 1 BWR-yksikön putkiston säröjen piilossapysymisestä. Reaktoriveden puhdistusjärjestelmän putkista löydettiin maaliskuussa 1993 läpimeneviä halkeamia. Halkeamat sijaitsivat reaktoripaineastian lähellä. Särötarkastajien dosimetrien hälytysraja oli asetettu alemmaksi kuin paikan säteilytaso, jolloin kova jatkuva hälytysääni oli aiheuttanut hutilointia tarkastuksissa ja säröt olivat päässeet kasvamaan vaarallisiksi. Ruotsin ydinturvaviranomainen Statens Kärnkraftsinspektion (SKI) vaatii nyt voimayhtiöltä selvitystä tarkastajien työskentelyolosuhteiden parantamisesta.

Nucleonics week 20.5.1993

Ukrainan Tshernobylin ydinonnettomuudessa seitsemän vuotta sitten eniten säteilyä saaneiden henkilöiden joukossa ei ole todettu leukemiaa poikkeavia määriä. Onnettomuuden seurausvaikutuksia tutkivat lääkärit ilmoittavat ryhmän sairastavan sensijaan muita sairauksia. Leukemian aikaisen esiintymisen katsotaan indikoivan muiden syöpäsairauksien myöhempää ilmenemistä.

Nucleonics Week 22.4.1993

Ukraina valitsee kesäkuussa jatkoon 3—6 tarjoajaa Tshernobylin onnettomuusyksikön uuden sarkofagin tekijäehdokkaista. Tarjouksia tuli noin 400. Nykyinen sargofagi tehtiin kiireessä onnettomuuden jälkeen vuonna 1986. Rakenteessa on huono horisontaalinen tuenta, jolloin mahdollinen maanjäristys voi luhistaa sen. Sisällä oleva alati kasvava radioaktiivinen pölymäärä pöllähtää tällöin ulos ja päästöt voivat pahimmillaan ylittää jopa varsinaiset onnettomuuspäästöt. Sarkofagin hinnaksi arvioidaan jopa 1,5 miljardia markkaa ja sen rakentaminen voi kestää viisikin vuotta. Sarkofagi on noin 75 m korkea ja 250—300 m leveä ja pitkä. Perustukset kaivetaan 40 m syvyyteen ja reaktorin alle tehdään uusi betonilaatta.

Nucleonics Week 29.4.1993

Ukrainan Zaprozhe 5 VVER 1000 yksikön turbiinirakennuksessa 21.5. sattuneesta tulipalosta on saatu yksityiskohtaista tietoa. Yksi työntekijä sai surmansa vetyvuotopalossa ja toinen vakavia palovammoja. Generaattorin vetyjäähdytysjärjestelmän pääputkistosta oli sulkuventtiilillä eristetty sivulinja, jota kaksi asentajaa oli irroittamassa sulkuventtiilin laippaliitoksesta. Epähuomiossa he avasivatkin väärän puolen laippaliitoksen, jolloin vetyä purkautui huonetilaan ja seurauksena oli vetyräjähdys ja tulipalo. Teollisuuspalo sammutettiin nopeasti.

NucNet 26.5.1993

Unkarin Paksin ydinvoimalaitoksen onnettomuusriski on suuruudeltaan yksi sydämensulamisonnettomuus 10 000 vuodessa, ilmenee juuri valmistuneesta turvallisuusarviosta. Arviossa todetaan, että paineellinen lämpöshokki ei ole ongelma Paksin reaktoripaineastioiden ehjänäpysymiselle kuten on asian laita ensimmäisen polven VVER 440-reaktoreissa. VVER-reaktorien hyvänä puolena on suuri vesimäärä primääripiirissä, mikä mahdollistaa tehokkaat onnettomuudenhallintatoimenpiteet. Loviisan VVER-yksiköt ja Paksin yksiköt mainitaan usein esimerkkeinä hyvästä VVER-käytöstä.

Nucleonics week 20.5.1993

USA:ssa ryhdytään tehostetusti tutkimaan toimivien ydinvoimalaitosten kaapelien vanhenemista, jotta niiden onnettomuusolosuhdekestävyyttä ei menetettäisi huomaamatta. USA:n ydinturvaviranomainen Nuclear Regulatory Commission (NRC) kartoittaa teknisiä menetelmiä toimivien ydinvoimalaitosten kaapelien kunnon aika-ajoin tapahtuvaksi mittaamiseksi. Eräs menetelmä olisi venytyskestävyyden mittaus. Kartoituksen jälkeen voimayhtiöt velvoitettanee kaapelien entistä tarkempaan kunnonvalvontaan.

Nucleonics Week 13.5.1993

USA:n ydinturvaviranomainen Nuclear Regulatory Commission (NRC) on määrännyt maan kiehutusvesireaktorien (BWR) pinnankorkeusmittaukset parannettaviksi seuraavissa kylmäseisokeissa. Nykyiset pintamittaukset voivat antaa väärää tietoa veden pinnasta reaktorin paineen laskiessa nopeasti esimerkiksi putkikatkostilanteessa (onnettomuustilanteessa). Ongelma johtuu mittausputkistoon kertyneistä lauhtumattomista kaasuista. Uraanipolttoaine voi pahimmassa tapauksessa kuumentua suojakuoren vaurioitumislämpötilaan (1 100 C) vain 16 minuutissa, kun lisäveden tarvetta ei huomata.

Nucleonics week 3.6.1993

Venäjän Kuolan ydinvoimalaitoksen jätteenkäsittelyä parannetaan saksalaisin voimin (NUKEM). Radioaktiivisen jätteen polttolaitos varustetaan poistokaasujen puhdistusjärjestelmällä ja nestemäisille jätteille rakennetaan uusi käsittelyjärjestelmä. Lisäksi käytetyn polttoaineen mittauksiin toimitetaan uudet laitteet.

NucNet 16.4.1993

Venäjän sotilaallisessa Tomsk-7 jälleenkäsittelylaitoksessa Siperiassa tapahtui 6.4.1993 kemiallinen räjähdys uraaniplutoniumliuossäiliössä aiheuttaen rakennuksen ja sen vierusten voimakkaan kontaminoitumisen. Säteilytaso nousi rakennuksessa kymmenien millisievertien suuruiseksi ja laitosalueella kymmenien, satojen mikrosievertien suuruiseksi. Rakennuksia ympäröivää aluetta kontaminoitui merkittävästi useita satoja neliömetrejä. Räjähdystä seurasi tulipalo, joka sammutettiin tunnissa. Tapahtuma ei aiheuttanut välittömiä henkilövahinkoja. Laitoksen lähikaupunki sijaitsee vaikutusalueen ulkopuolella. Tapahtuman alustava vakavuusluokka on kolme.

NucNet 7.4.1993

Venäjän ydinvoimalaitosten turvaparannusten suunnitteluun on päätetty ohjata Euroopan jälleenrakentamis- ja kehityspankin varoja seuraavasti: Ruotsin valtion voimayhtiö Vattenfall etsii RBMK-laitosten turvallisuusparannuksiin tarvittavia laitteita. Ranskan ydinturvaviranomainen Institut de Protection et de Surete Nucleaire selvittää kansallisen onnettomuusvalmiuskeskuksen tekemistä ja VVER-yksikköjen turvaparannusten suunnittelijasta päätetään alkukesällä. Suunnittelupakettiin käytetään 85 000 ECUa.

Nucleonics Week 22.4.1993

Venäjällä on otettu käyttöön ensimmäinen uusi ydinvoimalaitosyksikkö kolmeen vuoteen. Balakovo 4 VVER 1000-yksikkö on kytketty valtakunnan sähköverkkoon ja nostetaan täyteeen tehoon toukokuun alussa.

NucNet 29.4.1993

Ins. Pekka Lehtinen on Säteilyturvakeskuksen ydinturvallisuusosaston tarkastaja, puh. 90-70821.

English abstracts

Editorial

Antti Piirto (page 1)

The basic design of the nuclear power plants allows human errors in connection with operational activities without sevene consequences as regards the environmental safety. Many diverse protection systems limit or eliminate effects of human errors. Economical losses are always possible, of course, but the safety of the environment is secured.

The accidents in Chernobyl, Bhopal and Seveso prove correct the assumption that equipment failures and human errors combined together can cause an accident when the connection of the failures and errors is complex in nature. Therefore when improving the operational safety of nuclear power plants it is of vital importance to do research work on the area of human errors and to develop methods to control risks caused by human errors both in the individual and organizational level.

More safety by improving the safety culture

Jukka Laaksonen (page 2)

In its meeting in 1986, after Chernobyl accident, the INSAG group concluded, that the most important reason for the accident was the lack of safety culture. Later the group realized that safety culture, if it is defined well enough, can be used as a powerful tool to assess and develop practises affecting safety in any country. A comprehensive view on the various aspects of safety culture was presented in the INSAG-4 report published in 1991. Finland was among the first nations include the concept of safety culture in its regulations. this article describes the roles of government and the regulatory body in creating a national safety culture. How safetry culture is seen in the operation of a nuclear power plant is also discussed.

THE RESEARCH HISTORY OF THE HUMAN BEHAVIOUR FROM THE PROBABILISTIC SAFETY ANALYSIS VIEWPOINT

Pekka Pyy (page 4)

The so called human errors have always been apart of the everyday life of the mankind. In that sense, the discussion on man as a contributor to the operational safety of nuclear power plants is nothing new. It is interesting to remark, that there do not exist widely accepted definitions of the human error nor the human reliability. Some of them are discussed at the beginning of this article.

The second Chapter discusses the past and today of the research of man as a contributor to safety. Similarly, the development of Human Reliability Analysis (HRA) is described.

The article, then, discusses the methods used in the contemporary HRA. The division between the identification of important human activities and their probability estimation is made. Especially, the pros and cons of the approaches and data sources used in the HRA are reviewed on a coarse level. At the end, a view on the use of expert judgment is given.

The human behaviour has been an endless topic of research in the history—and will be it in future as well. In the conclusion of the article an opinion is given on the development during the past 30 years. Then, a rapid view on the possible future of the area is given.

User oriented control room automation of the new plants

Pentti Haapanen (page 8)

The control rooms of conventional power plants and other process industries have totally changed during the past ten years. Single analog and binary instruments have been replaced by digital systems and displays. Due to the high safety requirements the nuclear industry has been slow to follow this development. The changeover has started from the process monitoring, where the process computer displays already have a significant role eg. in both Finnish plants. In the new plants also the automation systems will be digital and the operator controls will be done through their displays. At the same time new computerized operator support systems will be taken in use. Full utilization of the potentials of the computer and display technologies can significantly reduce the risk of human errors of the operating staff.

The using of the control room automation against human errors

Ari Kautto (page 11)

The control room automation has developed very strongly during the 80's in IVO. The former work expanded strongly with the building of the full scope training simulator to the Loviisa plant. The important milestones has been, for excample the testing of the Critical Function Monitoring System, a concept developed by Combustion Eng. Inc., in Loviisa training simulator 1982, the replacing of the process and simulator computers in Loviisa 1989, and 1990 and the presenting the use of of the computer based procedures in training of operators 1993.

With developing of automation and procedures it is possibly to minimize the propability of human error. Howewer, it is not possible totally eliminate the risks caused by human errors.

Root cause analysis methodology for IVO—Path-system

O Nevander (page 19)

Since the first criticality of a nuclear power plant the major goals in the work of the operating personnel are produce the electricity, and also improve the safety and the reliability of the plant. Two separate goals, safety and operability, are so near, that in most cases it is possible to use same tools to develope them.

If we look the safety of a nuclear plant as a process which is going on, we could handle the normal management, maintenance and operation as direct elements for improving the safety of a NPP. Usually, these three elements seem to be the most important safety improving elements in a NPP. The effectiveness of these direct tools depends strongly on the safety culture in the NPP. With a weak safety culture the direct tools are competent only for the performance problems. To keep the performance and safety of NPP at high level and if possibly to improve them, it is necessary to add some special elements to the process. In specially in fully organized old plant, for example in Loviisa, these special, indirect elements, are the most important tools to expand the safety.

Root cause analysis is a tool, which is used to find the real, usually hidden reasons for an incident, the hidden reasons behind the cause are root causes. The root cause is a cause, which should been eliminated to avoid all incidents similar as the one been analysed. One important part of analysing root causes is the verification of corrective measures.

The IVO-group has developed a system for analysing the root causes of the incidents in the plant. The methodology, so called Path-system, is developed in 1991 and should also come in use for the incidents in the non-nuclear power plants owned IVO group.

The most important features of the Path-system are the recurrency of the cause and the root cause. Usually the weakest point of the root cause analysis is the identification the similarities between two incidents. A plant could have numerous incidents with the same cause, but if they don't have similar consequences, the corrective actions are always unique and therefore almost useless. The emphasising of the recurrency is specially usefull for old plants which have been operated without root cause analysis many years.

Human errors and mistakes

Björn Wahlström (page 22)

Human errors have a major contribution to the risks for industrial accidents. Accidents have provided important lesson making it possible to build safer systems. In avoiding human errors it is necessary to adapt the systems to their operators. The complexity of modern industrial systems is however increasing the danger of system accidents. Models of the human operator have been proposed, but the models are not able to give accurate predictions of human performance.

Human errors can never be eliminated, but their frequency can be decreased by systematic efforts. The paper gives a brief summary of research in human error and it concludes with suggestions for further work.

ATTITUDES TO RISKS IN NUCLEAR ENERGY PRODUCTION: THE PERSONNEL'S VIEW

Mika Kivimäki and Raija Kalimo (page 25)

This survey investigated risk perception among nuclear power plant personnel. The study group, 428 employees from a nuclear power plant in Finland, completed a questionnaire which contained the same questions as those in previous surveys on the risk perception of lay persons and industrial workers. Risks at work work were not seen as a sizable problem by nuclear power plant personnel. The study group estimated the safety of nuclear power plants better and the possibility of a serious nuclear accident as more unlikely than the general public. Compared to the employees in other industrial companies, the overall perceived risks at work among plant personnel did not exceed the respective perceptions of the reference groups.