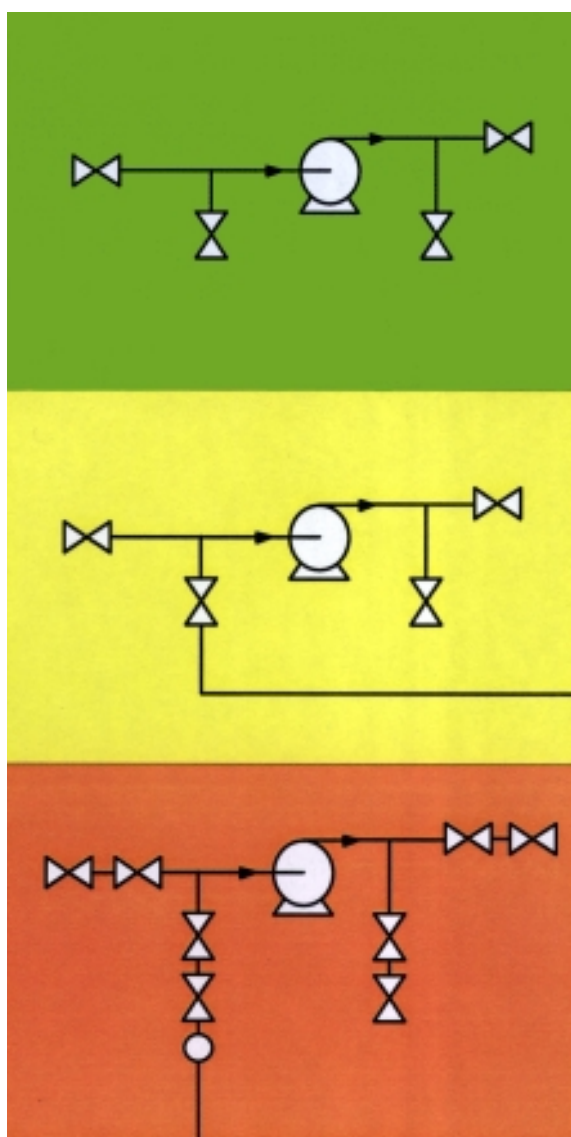


Erkki Kotikunnas & Perttu Heino

Turvallisen prosessilaitoksen suunnittelu

STOPHAZ-projektissa syntyneet työkalut



Turvallisen prosessilaitoksen suunnittelu STOPHAZ-projektissa syntyneet työkalut

Erkki Kotikunnas & Perttu Heino

VTT Automaatio



ISBN 951-38-5697-6 (nid.)

ISSN 1235-0605 (nid.)

ISBN 951-38-5698-4 (URL: <http://www.inf.vtt.fi/pdf/>)

ISSN 1455-0865 (URL: <http://www.inf.vtt.fi/pdf/>)

Copyright © Valtion teknillinen tutkimuskeskus (VTT) 2000

JULKAISIJA – UTGIVARE – PUBLISHER

Valtion teknillinen tutkimuskeskus (VTT), Vuorimiehentie 5, PL 2000, 02044 VTT
puh. vaihde (09) 4561, faksi (09) 456 4374

Statens tekniska forskningscentral (VTT), Bergsmansvägen 5, PB 2000, 02044 VTT
tel. växel (09) 4561, fax (09) 456 4374

Technical Research Centre of Finland (VTT), Vuorimiehentie 5, P.O.Box 2000, FIN-02044 VTT, Finland
phone internat. + 358 9 4561, fax + 358 9 456 4374

VTT Automaatio, Riskienhallinta, Tekniikankatu 1, PL 1306, 33101 TAMPERE
puh. vaihde (03) 316 3111, faksi (03) 316 3282

VTT Automation, Riskhantering, Tekniikankatu 1, PL 1306, 33101 TAMMERFORS
tel. växel (03) 316 3111, fax (03) 316 3282

VTT Automation, Risk Management, Tekniikankatu 1, P.O.Box 1306, FIN-33101 TAMPERE, Finland
phone internat. + 358 3 316 3111, fax + 358 3 316 3282

Toimitus Kerttu Tirronen

Otamedia Oy, Espoo 2000

Kotikunnas, Erkki & Heino, Perttu. Turvallisen prosessilaitoksen suunnittelu. STOPHAZ-projektissa syntyneet työkalut [Designing a safe process plant. Tools created during STOPHAZ-project]. Espoo 2000. Valtion teknillinen tutkimuskeskus, VTT Tiedotteita – Meddelanden – Research Notes 2050. 44 s.

Avainsanat plant design, quality assurance tools, hazard and operability studies, safety analysis, intelligent safe design kyberbook

Tiivistelmä

EU:n ESPRIT-ohjelman tuella toteutetun STOPHAZ-projektin tavoitteena oli edistää turvallisten ja ympäristölle vaarattomien prosessilaitosten suunnittelua. Tietokoneavusteisia menetelmiä kehittämällä parannettiin prosessisuunnittelijan mahdollisuuksia tarkastella turvallisuus- ja ympäristönäkökohtia suunnittelun aikana. Tässä raportissa kerrotaan ELDER- ja HAZID-työkaluista, jotka muodostavat STOPHAZ-projektin keskeisimmät tulokset.

ELDER on hyperkirja, joka sisältää neuvoja lähinnä turvallisuus-, terveys- ja ympäristönäkökohdista. Hyperkirja sisältää tavallisen kirjan sisällysluettelon kaltaisen navigointi-ikkunan, jossa eri prosessiyksiköistä kertovat neuvot on järjestetty ennalta määriteltujen vakio-otsikoiden alle.

Neuvot voivat sisältää tekstiä, laskentalomakkeita, kuvia ja linkkejä toisiin neuvoihin. Neuvoihin liittyy määrittämiä siitä, millaisille laitetyppeille ne ovat päteviä, sekä määrittämiä, jotka kuvaavat neuvon sisältöä. Neuvoihin liitettyjä määrittämiä käyttävien hakutoimintojen avulla käyttäjä pystyy poimimaan neuvokannasta käsillä olevan ongelman ratkaisemista helpottavat neuvot. Laiteympäristön, prosessiaineiden tms. vuoksi tilanteeseen sopimattomat neuvot karsiutuvat tällöin pois hakutuloksista.

HAZID on työkalu vaarojen tunnistamiseksi automaattisesti poikkeamatarkastelua (HAZOP) käyttäen. Lähtökohdiana on tieto prosessin laitteista ja kemikaaleista sekä prosessiolosuhteista, tyypillisesti esitettynä PI-kaaviomuodossa. Tulokseksi saadaan luettelo syy-seurausketjuista, jotka saattavat johtaa vaaratilanteisiin. Tavoitteena on lopputulos, joka vastaa perinteisen ryhmätyönä laaditun poikkeamatarkastelun tulosta sekä laadultaan että kattavuudeltaan.

Syy-seurausketjujen tunnistaminen perustuu yleiskäyttöisiin malleihin, jotka kuvaavat erityyppisten laitteiden vikaantumista ja käyttäytymistä häiriötilanteessa. HAZID yhdistelee näitä malleja annettuun laitoskuvaukseen nojautuen siten, että laitevikojen ja muiden häiriöiden vaikutukset kohdelaitoksen eri osien toimintaan tunnistetaan. Koska analyysi on laitoskuvauksen antamisen jälkeen täysin automaattinen, se on helppo toistaa suunnittelun edetessä tai prosessimuutoksia suunniteltaessa ja siten arvioida muutosten vaikutuksia kohdelaitoksen turvallisuuteen.

Kotikunnas, Erkki & Heino, Perttu. Turvallisen prosessilaitoksen suunnittelu. STOPHAZ-projektissa syntyneet työkalut [Designing a safe process plant. Tools created during STOPHAZ-project]. Espoo 2000. Technical Research Centre of Finland, VTT Tiedotteita – Meddelanden – Research Notes 2050. 44 p.

Keywords plant design, quality assurance tools, hazard and operability studies, safety analysis, intelligent safe design kyberbook

Abstract

The objective of the STOPHAZ project was to promote the safer and more efficient design of process plants through the use of a new generation of quality assurance tools. These tools include an intelligent safe design hyperbook ELDER (Engineering Line Diagram helpER) and HAZID (HAZard IDentification tool).

ELDER is a hyperbook, which contains advice on SHE considerations and related issues. The advice in each chapter is organised under predefined standard headings. These headings (Control and Instrumentation, Operational Considerations, Legislation etc.) aim to guarantee that the advice covers all the considerations that are necessary for safer and more efficient design.

Each piece of advice on a specific topic is called an advice note. These advice notes contain text, diagrams, simple calculation tools, and links to other advice notes. In order to make the system context sensitive, invisible definitions are associated with each advice note. These invisible definitions include query keywords, and the validity range of the advice in terms of topics and equipment subtypes.

HAZID is an automated Hazard and Operability Study (HAZOP) tool based on a signed directed graph (SDG) representation of process equipment faults and their propagation. It accepts the description of the process as input and generates a HAZOP study report as output. This report contains the cause-consequence-chains associated with the identified hazards.

A typical user of the tool is a design engineer who wishes to evaluate the plant design before commencing with a HAZOP study. Alternatively, it could be used at earlier stages of the design process, before detailed process and instrumentation diagrams (P&ID) are available, to screen for possible problems when the cost of design changes is not too high.

HAZID uses process-independent unit models to create a model of fault propagation based on the given process-specific plant description. This SDG model is then examined by applying the HAZOP algorithm. Information on process conditions and the properties of the processed fluids is used for improving the performance of the knowledge-based hazard identification.

Alkusanat

Tässä julkaisussa kerrotaan EU:n tuella toteutetun "Support Tool for Hazard and Operability Studies (STOPHAZ)" -hankkeen tuloksista. STOPHAZ-hanke toteutettiin osana EU:n ESPRIT-tutkimusohjelmaa. Hankkeen koordinaattorina toimi ICI Engineering Technology Englannista.

TEKES ja VTT toimivat hankkeen Suomen osuuden rahoittajina. Hankkeen toteutusta Suomessa ohjasi johtoryhmä, johon kuuluivat Jaakko Pöyry Oy, Neste Oy, Kemira Oy, Outokumpu Oy ja TEKES.

Tekijät haluavat esittää lämpimät kiitoksensa johtoryhmän jäsenille heiltä saamastaan ohjauksesta ja mukana olleiden yritysten osallistumisesta STOPHAZ-ohjelmiston prototyypin kokeiluun. Haluamme myös kiittää työtovereitamme VTT:ssa Tampereella sekä ulkomaisia yhteistyökumppaneitamme heidän panoksestaan ja tuestaan hankkeen onnistuneen toteutuksen takaamiseksi.

Tekijät

Sisällysluettelo

Tiivistelmä	3
Abstract	4
Alkusanat	5
1. Johdanto	8
2. STOPHAZ-projekti	10
3. ELDER	12
3.1 ELDER-hyperkirjaohjelmiston osat	12
3.2 Neuvot	13
3.3 Neuvojen katselu	14
3.4 Navigointijärjestelmä	15
3.5 Asiayhteystietojen asettaminen	18
3.5.1 Käytettävä laitetyyppi	18
3.5.2 Asiasanat	19
3.6 Avainsanahaku	20
3.7 Loki ja muistiinpanot	23
3.7.1 Muistiinpanot	24
3.7.2 Loki	24
3.8 Neuvokirjan luontityökalut	25
4. HAZID	26
4.1 Tietokoneavusteinen poikkeamatarkastelu	26
4.2 HAZID-ohjelmiston rakenne ja toiminta	30
4.2.1 Ohjelmiston perusrakenne	30
4.2.2 Laitemallikirjasto	32
4.2.3 HAZOP-algoritmi	32
4.2.4 Tulosten karsinta	34
5. Käyttökokeilut	35
5.1 ELDER	35
5.1.1 Arvioinnin toteutus	35
5.1.2 Arvioinnin tulokset	35
5.1.3 Johtopäätökset	36
5.2 HAZID	38
5.2.1 Arvioinnin toteutus	38
5.2.2 Arviointimenetelmä	39

5.2.3 Arvioinnin tulokset	40
6. YHTEENVETO	42
Lähdeluettelo.....	44

1. Johdanto

STOPHAZ (Support Tool for Hazard and Operability Studies) -projektin valmistelu käynnistyi englantilaisen kemian alan suuryrityksen ICI:n aloitteesta. Lähtökohtana oli ICI:n tarve tehostaa turvallisuusanalyysien, erityisesti poikkeamatarkastelujen (HAZOP) laadintaa. Maailmanlaajuisesti suuren suosion saavuttanut HAZOP-menetelmä kehitettiin 1970-luvulla ICI:ssa [Knowlton 1992].

ICI:n tarve tehostaa HAZOP-analyysien laadintaa on seurausta turvallisuusanalyysien käytön laajentumisesta kiinteäksi osaksi uusien prosessien suunnittelua. Projektien tiukka aikataulu ja analyysien vaatima suurehko työmäärä koetaan ongelmaksi. Turvallisuusanalyyseissä tarvittavaa työmäärää pyritäänkin pienentämään kehittämällä turvallisuusnäkökohtien tarkastelun tietokoneavusteisuutta.

Lainsäädäntö Euroopassa ja yhä enemmän myös sen ulkopuolella edellyttää nykyään, että turvallisuusnäkökohdat otetaan riittävässä laajuudessa huomioon laitosten suunnittelussa. EY-maat hyväksyivät vuonna 1982 ns. Seveso-direktiivin, joka suosittaa jäsenmaita kehittämään kansallista lainsäädäntöään niin, että turvallisuusselvitysten laadinta on osa uuden laitoksen toimiluvan myöntämistä. Suomessa kemikaalilakia sekä siihen liittyvää kemikaaliasetusta ja eräitä muita asetuksia on viime vuosina täydennetty siten, että ne velvoittavat vaarallisia kemikaaleja käsittelevät laitokset tekemään ns. vaaran arvioinnin ja tietyillä ehdoilla myös ns. turvallisuusselvityksen. Turvallisuusanalyysimenetelmät ovat keskeinen ko. selvitysten laadintaa tukeva työkalu.

Useimmat nykyisin käytössä olevat turvallisuusanalyysin tietokoneohjelmistot keskittyvät lähinnä analyysitulosten kirjaamisen helpottamiseen tekstinkäsittely- ja taulukkolaskentaohjelmistojen tapaan. Näin voidaan säästää aikaa analyysitulosten kirjaus- ja muokkausvaiheissa. HAZOP-analyyseissä kuluu kuitenkin valtaosa resursseista siihen, että asiantuntijat käyvät HAZOP-ryhmän kokouksissa yksityiskohtaisesti läpi tarkasteltavan prosessin toimintaa ja potentiaalisia vaaroja [AIChE 1992]. Tämän vaiheen tehostaminen vaatii työkaluja, jotka kykenevät automatisoimaan osan HAZOP-ryhmän tehtävistä.

Nykyisin prosessisuunnittelun turvallisuustarkastelut, esimerkiksi HAZOP-analyysit, painottuvat suunnittelun loppupuolelle. Tällöin turvallisuuden parantamiseen käytettävissä olevien toimien valikoima on suppeampi kuin suunnittelun aikaisemmissa vaiheissa, ja kustannukset muodostuvat helposti merkittävästi suuremmiksi, koska suunnittelun loppuvaiheessa tehtävät muutokset vaativat myös uudelleensuunnittelua muissa laitoksen osissa. Turvallisuusanalyyseihin ja niistä aiheutuviin muutostoiimiin kuluu aikaa ja resursseja voidaan säästää, jos saadaan parannettua laitossuunnittelun laatua niin, että suunnittelun loppuvaiheen turvallisuusanalyysin kohteena olevassa suunnitelmassa ei enää

ole suuria turvallisuuden liittyviä epäkohtia tai puutteita. Tähän pyrittäessä on tärkeää varmistaa, että suunnittelijan ulottuvilla on aina asianmukaisia ohjeita ja tarkistuslistoja.

STOPHAZ-projektissa valittiin tutkimuksen kohteeksi kolme osa-aluetta:

1. Älykkäiden, erityisesti turvallisuusnäkökohtiin liittyvien neuvojen antaminen suunnittelijalle hänen spesifioidessaan prosessin komponentteja ja oheisjärjestelmiä.
2. Vaarallisten tapahtumaketjujen automaattinen tunnistaminen perustuen etukäteen annettuun prosessikuvaukseen ja tietämyskantoihin koottuun prosessilaitteiden ja prosessiaineiden turvallisuutta kuvaavaan tietämykseen. Automaattisesti generoitujen tulosten tulee olla riittävän korkealaatuisia, jotta aikaa ei hukkaantuisi niiden tarkistamiseen.
3. Prosessin käyttöohjeiden laadinnan tehostaminen ja liittäminen kiinteäksi osaksi suunnittelua.

Osa-alueet valittiin projektin ensimmäisenä vaiheena toteutetun selvityksen perusteella. Selvityksessä haastateltiin yli sataa prosessien suunnittelun ammattilaista tarkoituksena tunnistaa ongelmakohtia, joihin STOPHAZ-projekti voisi pureutua.

Selvityksessä paljastui, että prosessisuunnittelun alkuvaiheessa ei otettu riittävästi huomioon turvallisuus-, terveys- ja ympäristönäkökohtia (SHE considerations). Lisäksi yleiseksi ongelmaksi koettiin hyvien suunnittelukäytäntöjen siirto aloitteleville suunnittelijoille.

STOPHAZ-moduulien ensimmäisten prototyyppien valmistuttua tehtiin joukko käyttökokeiluja. Kokeilujen palaute analysoitiin yksityiskohtaisesti, ja projektin loppuosan tehtävät priorisoitiin palautteen pohjalta.

Palautteen perusteella projektin resurssit jaettiin uudelleen siten, että 60 % resursseista käytettiin älykkään neuvohyperkirjan ohjelmiston (ELDER) ja hyperkirjan sisällön kehittämiseen. Noin 30 % resursseista käytettiin automaattisen poikkeamatarkastelun suorittavan ohjelmiston (HAZID) kehittämiseen ja loput 10 % resursseista käytettiin prosessin käyttöohjeiden laatimisessa käytettävän tukityökalun kehittämiseen.

2. STOPHAZ-projekti

VTT osallistui EU:n ESPRIT-tutkimusohjelman osana toteutettuun kolmivuotiseen STOPHAZ-projektiin, jossa kehitettiin menetelmiä ja työkaluja suunnittelun kuluessa tehtäviä turvallisuustarkasteluja varten. Näiden menetelmien ja työkalujen pohjalta on mahdollista kehittää prosessisuunnittelua tekevän yrityksen suunnittelukäytäntöjä siten, että suunnittelun edetessä turvallisuusnäkökohdat ovat koko ajan mukana tarkasteluissa.

STOPHAZ-projektin tavoitteena oli tarjota käyttöön integroitu joukko ohjelmistotyökaluja, joiden avulla edistetään turvallisten ja ympäristölle vaarattomien prosessilaitosten suunnittelua. Ohjelmistot toteutettiin englanninkielisinä.

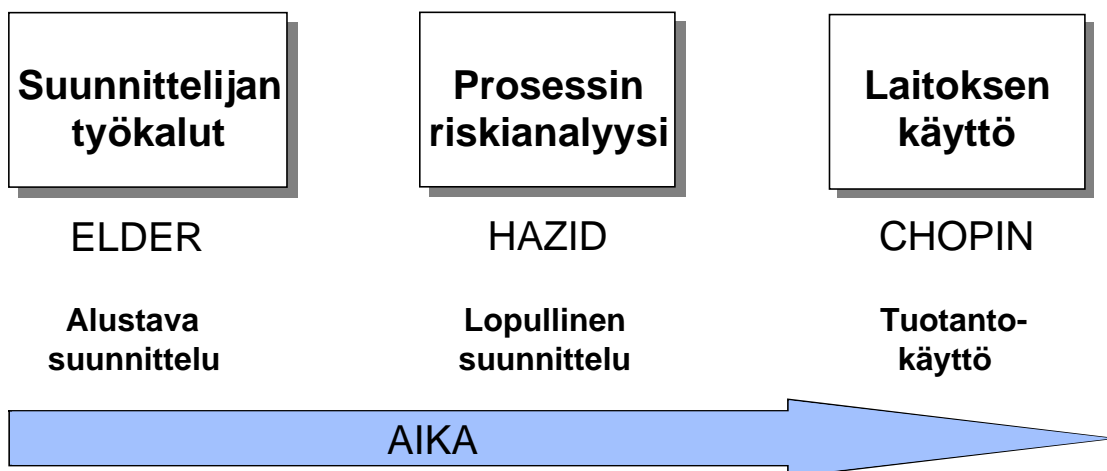
STOPHAZ-projektissa kehitettiin ohjelmisto, joka koostuu kolmesta prosessisuunnittelua tukevasta työkalusta:

ELDER: Prosessisuunnittelua tukeva neuvohyperkirja

CHOPIN: Käyttöohjeiden laadinnan tuki

HAZID: Automaattinen poikkeamatarkastelu.

Kuvassa 1 esitetään STOPHAZ-työkalujen käyttö prosessilaitoksen suunnittelun eri vaiheissa.



Kuva 1. STOPHAZ-työkalujen käyttö laitoksen elinkaaren eri vaiheissa.

Suunnittelun neuvohyperkirjaa (ELDER, Engineering Line Diagram helpER) käytetään täydentämään jo olemassa olevia suunnittelumenetelmiä. Sen avulla saadaan suunnitte-

lussa tarvittavia neuvoja turvallisuusnäkökohdista ja pystytään kirjoittamaan työmuistioita prosessikaavion kehityksen aikana.

ELDER tuo turvallisuuteen liittyvää tietoa suunnittelijan ulottuville tarpeen mukaan ja ohjaa häntä tämän tiedon systemaattisessa läpikäynnissä. Nämä neuvot on koottu ELDERin omaan neuvotietokantaan ja niihin on liitetty hakuoperaatioita tukevia määräytyksiä. Neuvotietokantaan on tallennettu laaja yleiskäyttöinen perusaineisto, mutta kunkin käyttäjäorganisaation on tarpeen täydentää tätä aineistoa omilla yrityskohtaisilla ohjeistoillaan.

Tavoitteena on neuvoja käyttämällä välttää jo suunnittelun alkuvaiheesta lähtien sellaisia ratkaisuja, joihin liittyy tunnettuja turvallisuusongelmia. Käyttämällä tarjolla olevia hakumenetelmiä suunnittelija pystyy nopeasti löytämään neuvoista asianmukaista tietoa prosessilaitteista.

CHOPIN auttaa suunnittelijaa dokumentoimaan prosessin käyttöön liittyvää tietoa ja siirtämään tämän tiedon käyttöohjeiden laadinnan pohjaksi. Käytön tukityökalun avulla on mahdollista kirjoittaa alustavat prosessin käyttöohjeet jo suunnitteluvaiheessa, jolloin jo suunnittelun yhteydessä syntyneet prosessiin käyttöön vaikuttavat seikat tulevat paremmin huomioiduiksi varsinaisia lopullisia laitoksen käyttöohjeita kirjoitettaessa. Työkalun tavoitteena on siis siirtää laitoksen suunnitteluvaiheessa syntyvää tietoa edelleen laitoksen lopullisia käyttöohjeita kirjoittaville henkilöille.

HAZID laatii poikkeamatarkastelun automaattisesti PI-kaaviotasoisien prosessikuvausten pohjalta. Sen toiminta perustuu yleiskäyttöiseen HAZOP-mallikirjastoon, joka sisältää eri prosessilaitteiden turvallisuusorientoituneet kvalitatiiviset mallit. Mallikirjastoa on tarpeen täydentää yrityskohtaisesti niin, että se kattaa kaikki analysoitavissa laiteyksiköissä esiintyvät laitetypit.

HAZIDin avulla on mahdollista nopeuttaa poikkeamatarkastelun suorittamista prosessikaavion alustavalle versiolle, jolloin prosessikaavioon vielä jääneet suunnitteluvirheet paljastuvat mahdollisimman aikaisessa vaiheessa.

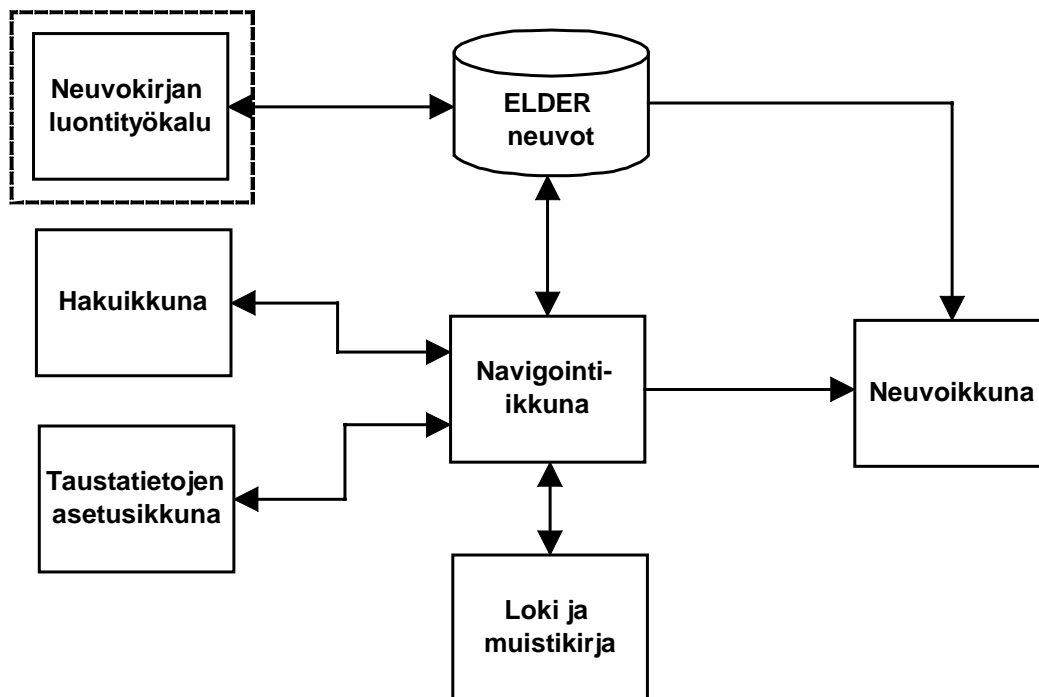
3. ELDER

3.1 ELDER-hyperkirjaohjelmiston osat

ELDER-hyperkirjaohjelmistossa on kuusi pääelementtiä:

- neuvot
- neuvoikkuna
- navigointi-ikkuna
- hakuikkuna
- taustatietojen asetusikkuna
- loki ja muistikirjajärjestelmä.

Järjestelmän osien liittyminen toisiinsa on esitetty kuvassa 2.



Kuva 2. ELDER-hyperkirjaohjelmiston osat.

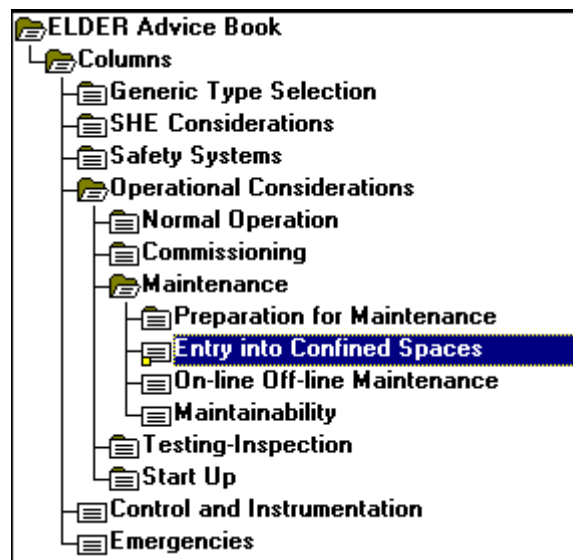
Käyttäjän kannalta kiinnostavinta on tutkia ELDER-hyperkirjan tarjoamia neuvoja. Neuvojen katselu tapahtuu neuvoikkunasta. Ikkunassa näkyvä neuvo valitaan joko valitsemalla otsikko sisällysluettelosta tai suorittamalla avainsanahaku hakuikkunassa. Taustatietojen asetusikkunan avulla on mahdollista estää epäoleellisten neuvojen esiintulo. Käyttäjä voi tallentaa laitoksen suunnitteluun liittyviä muistiinpanoja sekä katsella

aikaisemmin tehtyjä muistiinpanoja. Käyttäjän toimista pidetään lokia järjestelmän suunnittelun tarkistamiseksi myöhemmin. Uusien neuvojen luonti tapahtuu erillisellä kyseiseen tarkoitukseen tehdyllä ohjelmistolla.

3.2 Neuvot

Kunkin ELDER-hyperkirjan neuvokantaan tallennetun neuvon tulisi antaa käyttäjälle riittävästi tietoa päätöksenteon tukemiseksi ja suunniteltavan prosessin turvallisuus- ja ympäristönäkökohtien huomioonottamiseksi. Yksittäiset neuvot voivat sisältää esimerkiksi vastauksen ongelmaan tai kuvauksen tietystä laitteesta. Neuvoihin liitettävien määrittelysten avulla neuvoja voidaan luokitella asiasisältönsä mukaan ja etsiä haluttuun asiaan liittyviä neuvoja.

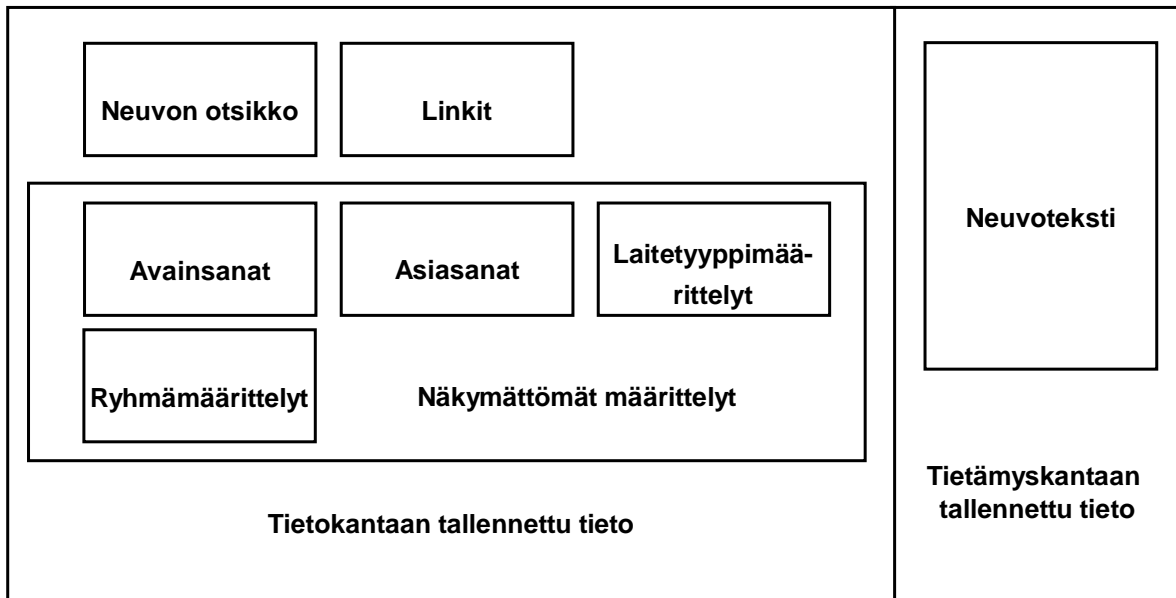
Kukin prosessiyksikkötyyppi, jonka ELDER kattaa, edustaa päätasoa neuvohierarkiassa. Kunkin pääotsikkotason alla on kaksitoista vakio-otsikkoa. Näiden vakio-otsikoiden (sääto ja instrumentointi, käyttönäkökohdat, lainsäädäntö, jne.) tavoitteena on varmistaa, että suunnittelijalle on tarjolla kattava valikoima neuvoja prosessin suunnittelemiseksi turvalliseksi ja ympäristölle vaarattomaksi. Neuvojen kirjoittajan on luotava vakio-otsikoiden alle määriteltujen alaotsikoiden hierarkia kullekin prosessiyksikkötyypille sopivaksi. Esimerkki tyypillisestä hierarkiasta on kuvassa 3.



Kuva 3. Esimerkki sisällysluettelon hierarkiasta.

Neuvot sisältävät tekstiä, kuvia ja yksinkertaisia laskentalomakkeita sekä linkkejä toisiin neuvoihin. Jotta järjestelmästä on saatu eri käyttötilanteisiin mukautuva, näkymät-

tömiä lisämääriytyksiä on liitetty kuhunkin neuvoon. Näihin näkymättömiin määriytyksiin kuuluvat avainsanat, asiasanat, laitetyyppimääriytykset sekä ryhmittelymääriytykset. Kuva 4 esittää ELDERissä käytettävien neuvojen rakenteen.



Kuva 4. Yksittäisen neuvojen rakenne.

Neuvon otsikko on teksti, joka näkyy ELDER-hyperkirjan sisällysluettelossa. Linkit ovat viitteitä neuvoihin, jotka sisältävät samaan aihepiiriin liittyviä neuvoja ja kiinnostavat siten kyseisen neuvojen tarvitsijaa.

Kutakin neuvokantaan tallennettua neuvoa luonnehtii joukko neuvoon liitettyjä määriytyksiä. Hakutoiminnoissa käytettäviä määriytyksiä ovat avainsanat ja asiasanat. Avainsanoja käytetään hakutoimintojen kohdistamiseen. Asiasanojen avulla luokitellaan karkeasti neuvojen asiasisältöä. Laitetyyppimääriytyksien avulla yksilöidään ne laitetyypit, joille kyseinen neuvo on voimassa.

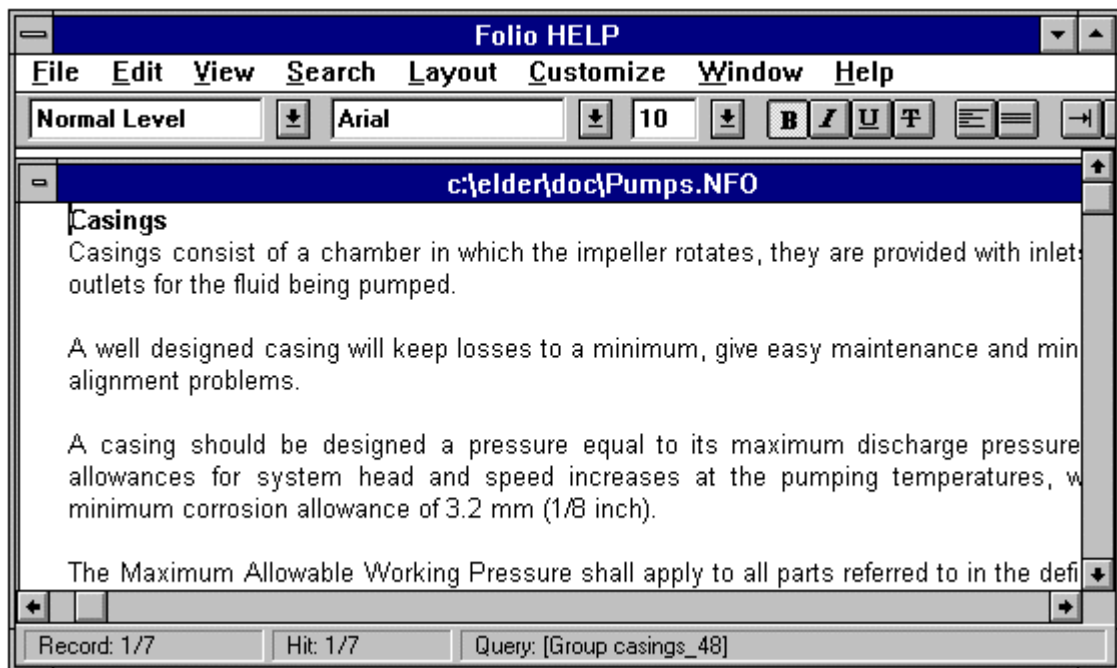
Neuvoteksti on neuvojen varsinaisen sisältö. Neuvotekstit on eroteltu neuvotietokannassa toisistaan ryhmittelymääriytyksin. Pelkän tekstin lisäksi neuvot voivat sisältää kuvien ja taulukkolaskentalomakkeiden lisäksi muita neuvotietokantaan liitettyjä objekteja.

3.3 Neuvojen katselu

Kaikki valitut neuvot näytetään neuvoikkunassa riippumatta siitä miten valittuun neuvoon päädyttiin. Neuvoikkunana käytetään Folio Views -ohjelmaa. Kyseisellä työkalulla on mahdollista katsella tekstiä ja kuvia. Skaalattavassa ikkunassa on tarjolla myös muita toimintoja kuten kirjanmerkit, popup-ikkunat ja korostus yliviivaamalla.

Kun neuvo valitaan katseltavaksi se näkyy neuvoikkunassa (kuva 5). Käyttäjä voi vapaasti säätää ikkunan kokoa siten, että se sopii hänen työpöytänsä. Ikkunaa voi vierittää, mutta ainoastaan yksi neuvo näkyy neuvoikkunassa kerrallaan.

Ponnahdusikkuna saadaan näkyviin linkkiä napsauttamalla. Niitä on käytetty osassa neuvoja viitteiden ja määritelmien esittämiseen neuvojenkirjoitusohjeissa annettujen sääntöjen mukaan, lähinnä isohkojen kuvien ja tekstikokonaisuuksien tallentamiseen. Ponnahdusikkunoihin viittaavien linkkien luonti tapahtuu neuvojen kirjoitusvaiheessa. Neuvojen käytön yhteydessä linkkejä voi ainoastaan käyttää muttei luoda uusia.



Kuva 5. Neuvoikkuna.

Grafiikkaikkunoita voidaan käyttää kuvien tai kaavioiden näyttämiseen. Tämä soveltuu silloin, kun kuvaa tarvitaan samanaikaisesti sitä tukevan tekstin kanssa. Pienikokoiset kuvat esitetään yleensä tekstin mukana, ja grafiikkaikkunoita käytetään ainoastaan erityisen suurikokoisten kuvien esittämiseen.

3.4 Navigointijärjestelmä

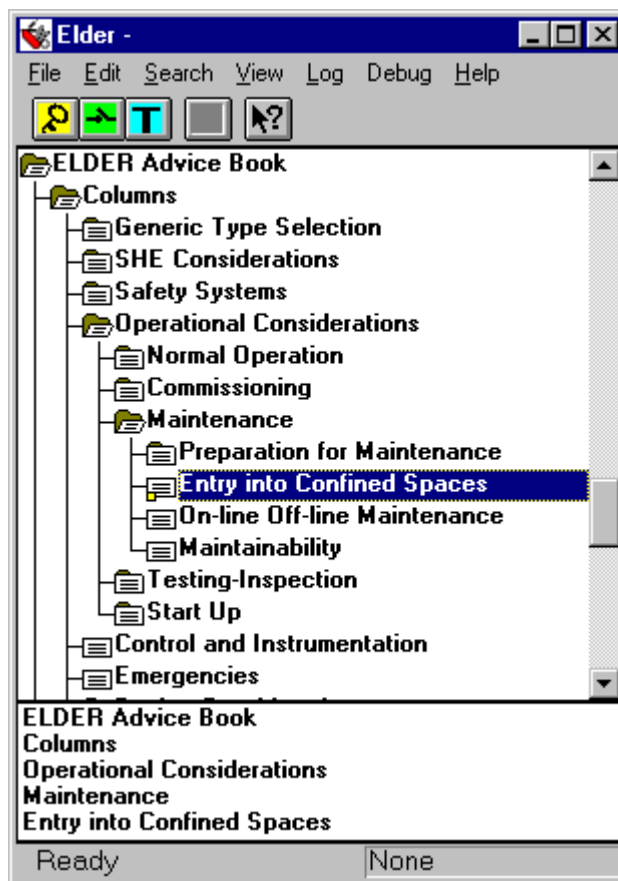
ELDER-hyperkirjan yleisin käyttötapa on neuvojen haku navigointi-ikkunaa käyttäen. Se näyttää neuvokirjan hierarkkisen sisällysluettelon. Tätä sisällysluetteloä käyttäjä voi selata ja katsella ELDER-neuvokannassa olevien neuvojen aihepiirejä. Halutessaan käyttäjä voi valita kiinnostavat neuvot katseltavaksi neuvoikkunaan.

Sisällysluettelon ulkoasun muoto on valittu siten, että käyttäjän on helppo hahmottaa neuvohierarkian koko rakenne. Eri tasot esitetään sisennysten lisäksi ikoneina, jotka on avattu tai suljettu. Tasojen riippuvuussuhteiden havainnoimisen selkeyttämiseksi eri tasojen välille on piirretty ikoneja yhdistävät viivat. Navigointi-ikkuna on täysin skaalattavissa käyttäjän mieltymysten mukaan. Ikkuna muistaa istuntojen välillä uudet asetukset esimerkiksi ikkunan sijainnin.

Sisällysluettelon ylimmän tason alapuolella on lueteltu prosessiyksiköt, joista neuvoja on olemassa. Kunkin prosessiyksikön otsikon alapuolella on seuraavat vakio-otsikot:

- General Information
- Generic Type Selection
- SHE Considerations
- Safety Systems
- Operational Considerations
- Control and Instrumentation
- Emergencies
- Design Considerations
- Codes of Practice
- Legislation
- Incidents.

Standardiotsikoiden alapuolella olevat otsikot on järjestelty kunkin prosessiyksikön tarpeen mukaan. Kuva 6 näyttää tyypillisen neuvohierarkian.



Kuva 6. Sisällysluettelon ulkoasu navigointi-ikkunassa.

Kun sisällysluettelo tulee käynnistyksen jälkeen esiin, siitä on näkyvissä kolme ensimmäistä tasoa, eli pääotsikko, laitetyyppien luettelo sekä laitetyyppien vakio-otsikot. Kaksoisnapsauttamalla otsikkorivillä olevaa ikonia seuraavan alatasen otsikot tulevat näkyviin. Jos kaikki otsikon alatasot halutaan saada näkyviin, se tapahtuu painamalla samanaikaisesti <ctrl> ja <shift> näppäimiä, kun ikonia kaksoisnapsautetaan. Vastavasti avointa ikonia kaksoisnapsauttamalla, kyseisen ikonin alatasot sulkeutuvat. Jos otsikon ikonin vasemmassa ylänurkassa ei ole ”kahvaa”, otsikolla ei ole alatasoja. Tällaisen ikonin napsauttaminen ei muuta sisällysluetteloa mitenkään.

Itse neuvon saa näkyviin kaksoisnapsauttamalla sisällysluettelossa neuvon otsikkotekstiä eikä ikonia. Haluttu neuvo ilmestyy napsautuksen seurauksena näkyviin neuvoikkunassa.

Ohjelman asetuksissa voidaan valita, mitä ikonin vihreä taustaväri kertoo neuvosta. Väriellä voi erotella ne neuvot, joita on katseltu nykyisen istunnon aikana tai vaihtoehtoisesti neuvot, jotka on luettu tarkasteltavan projektin aikana.

3.5 Asiayhteystietojen asettaminen

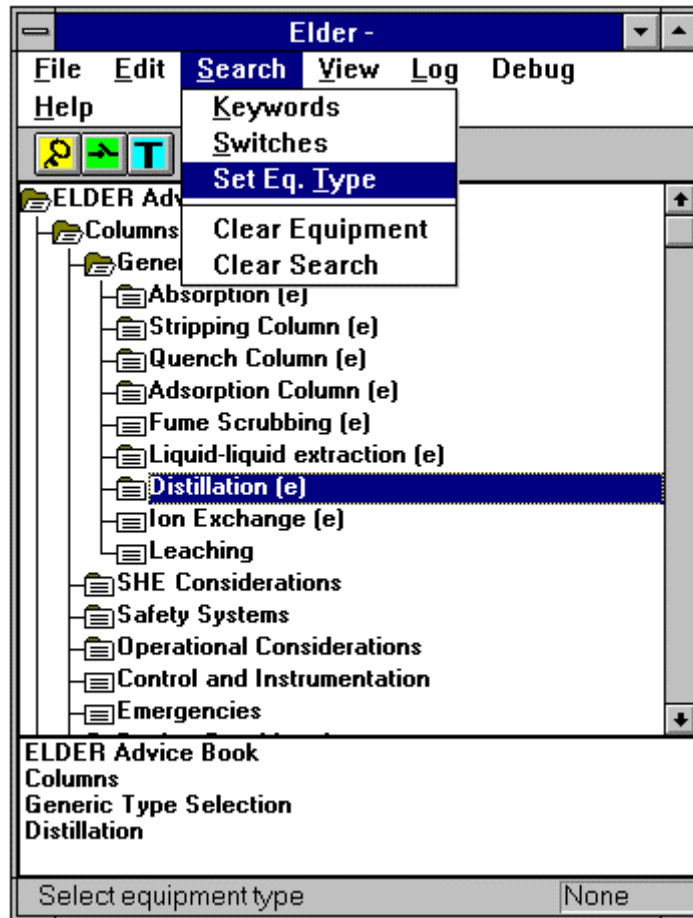
Asiayhteyttä käytetään vähentämään epäoleellisten neuvojen esittämistä käyttäjälle. Osa neuvoista on sovellettavissa ainoastaan erikoistilanteissa, esimerkiksi jos prosessilaitoksessa käsitellään erityisen tulenarkoja kemikaaleja. Tieto neuvojen voimassaolon rajoituksista lisätään neuvoihin niiden luontivaiheessa. Järjestelmää käytettäessä voidaan tehdä rajaavia valintoja, jolloin järjestelmä ei näytä epäoleellisia neuvoja. Tämä helpottaa käyttäjää löytämään halutun tiedon nopeasti samalla kun esitettävien neuvojen määrä pienentyy ja epäoleelliset neuvot jäävät pois.

ELDER sovittaa toimintaansa tutkittavan ongelman mukaan taustatietojen asettamisen avulla. Tämä tieto voi kuvastaa käyttäjän erityisiä mielenkiinnon kohteita (esimerkiksi saastuminen, materiaalit), yleisiä prosessin piirteitä (käytettävät kemikaalit, laitosympäristö) tai laitetyypin mukaisia ominaisuuksia (laitetyyppi, prosessiympäristö). Järjestelmässä voi antaa asiayhteystietoja kahdella eri tavalla, joko valitsemalla laitetyypin tai asettamalla asiasanojen tiloja.

3.5.1 Käytettävä laitetyyppi

ELDERin neuvoja luokitellaan sen mukaan, mille laitetyypille ne ovat päteviä. Olemassa olevat laitetyypit löytyvät sisällysluettelohierarkian ”Generic Types” -otsikon alta. Asiayhteystietojen asetus laitetyypin osalta tapahtuu siten, että laitetyyppiluettelosta valitaan haluttu laitetyyppi. Tämän jälkeen ainoastaan tälle laitetyypille ja laitetyypihierarkiassa ylempänä oleville laitteille pätevät neuvot jäävät näkyviin. Ne neuvot, joille ei ole määritelty, mille laitetyypille ne soveltuvat, tulevat aina näkyviin.

Käytettävä laitetyyppi asetetaan valitsemalla ”Generic Types” -otsikon alta jokin otsikko, joka on laitetyyppinen. Tämän näkee otsikon perässä suluissa olevasta e-kirjaimesta. Valinnan jälkeen valitaan valikosta ”Search” vaihtoehto ”Set Eq. Type”. Kuva 7 esittää laitetyypin valintaa.



Kuva 7. Laitetyypin valinta.

Vaikutus sisällysluetteloon on se, että kaikki ne otsikot, jotka eivät päde tälle käytettävälle laityypille tai sen alityypeille katoavat sisällysluettelosta. Toisin sanoen tarjolla on vain valitulle laityypille päteviä neuvoja samoin kuin yleisluontoisia neuvoja, jotka pätevät laityyppihierarkiassa ylempänä oleviin laityyppeihin.

Ohjelman asetuksissa on mahdollisuus saada myös valitun laityypin alityypeille pätevät neuvot näkyviin. Tämä on sikäli erilainen tila, että käsillä on edelleen tietoa myös valittua laityyppiä yksityiskohtaisemmista ratkaisuista.

3.5.2 Asiasanat

Asiasanat (switch) ovat avainsanoja, jotka kuvastavat neuvon sisältöä kokonaisuudessaan. Kuhunkin neuvoon voidaan määrittellä liittyväksi joukko asiasanoja.

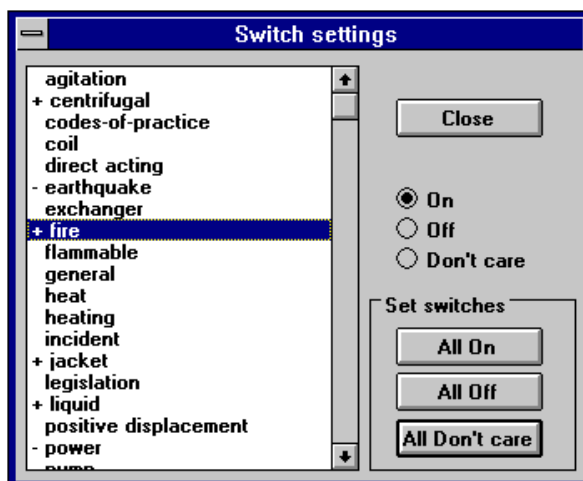
Asiasanoja voidaan käyttää muuttamalla niiden tilaa. Asiasanojen tiloilla on seuraavat vaikutukset sisällysluetteloon:

On: Ne neuvot, joihin tämä asiasana on liitetty, jäävät näkyviin.

Off: Ne neuvot, joihin tämä asiasana on liitetty, karsitaan pois.

Don't care: Eivät vaikuta neuvojen näkyvyyteen.

Asiasanojen asetuksia voi muuttaa valitsemalla valikosta ”Search” vaihtoehdon ”Switches”. Esiin tulevan valintaikkunan avulla on mahdollista muuttaa asiasanojen asetuksia. On-tila esitetään sanaa edeltävällä plusmerkillä ja off-tila miinusmerkillä. Kuvassa 8 on esimerkki asetuksien vaihdosta.



Kuva 8. Asiasanojen asetusten vaihto.

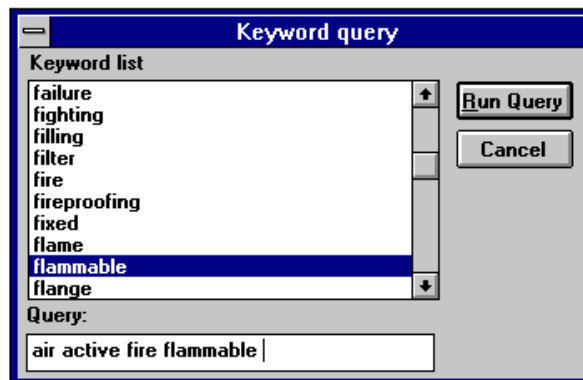
3.6 Avainsanahaku

ELDER-hyperkirjan hakujärjestelmä tarjoaa tavan päästä suoraan käsiksi neuvoihin. Haettaessa neuvoa jostain tietystä aihepiiristä käyttäjä antaa hakuikkunaan avainsanoja, jotka kuvaavat etsittävää tietoa. Avainsanojen perusteella ELDER hakee ne neuvot, jotka ovat oleellisia. Neuvojen otsikot kerätään listaksi, jota voi selailta ja itse neuvoja voi halutessaan katsella neuvoikkunassa.

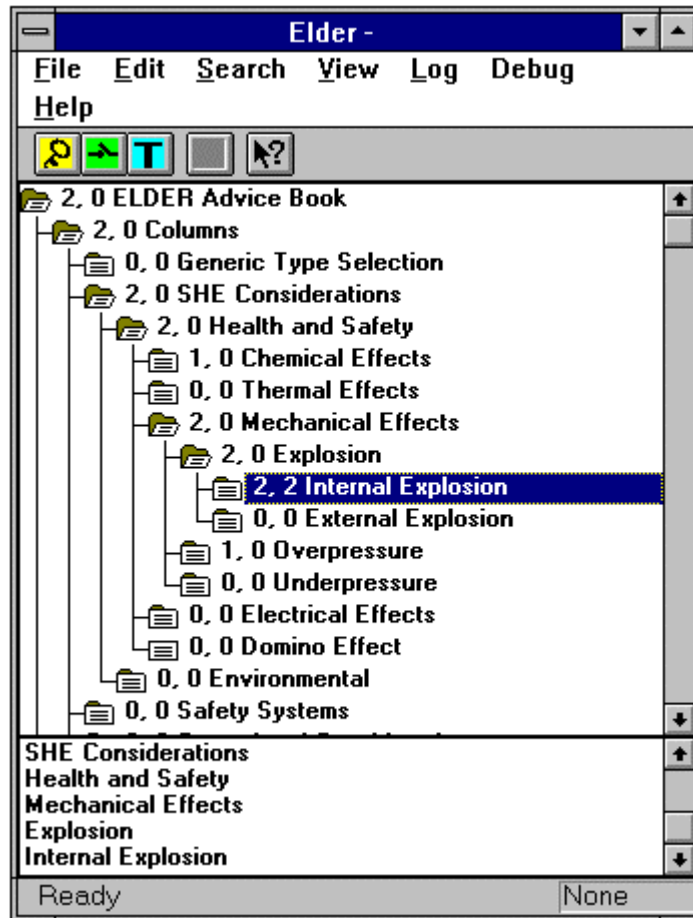
Avainsanahaun lisäksi käytössä on vapaa tekstihaku, joka hakee annettua merkkijonoa koko neuvokirjasta.

Avainsanahaun saa aloitettua valitsemalla valikosta ”Search” vaihtoehdon ”Keywords”. Esiin tulevasta valintaikkunasta voi valita haluamansa avainsanat. Kuva 9 näyttää

avainsanahaun suorittamisen. Avainsanoja voi valita kaksoisnapsauttamalla avainsanalistassa olevia sanoja tai kirjoittamalla avainsanat suoraan ikkunan alareunassa olevaan kenttään. Avainsanoja kirjoitettaessa avainsanalistasta yritetään samanaikaisesti hakea aakkosjärjestyksessä lähinnä vastaavaa avainsanaa. Lähimpänä oikeaa sanaa oleva sana avainsanalistassa näytetään korostamalla. Haku käynnistetään napsauttamalla "Run Query" -nappia. Avainsanalistassa on luetteloitu sellaiset avainsanat, joita on todella liitetty neuvoihin. Sellaisia sanoja, joita ei ole käytetty neuvoissa avainsanoina, ei huomioida avainsanahaussa.



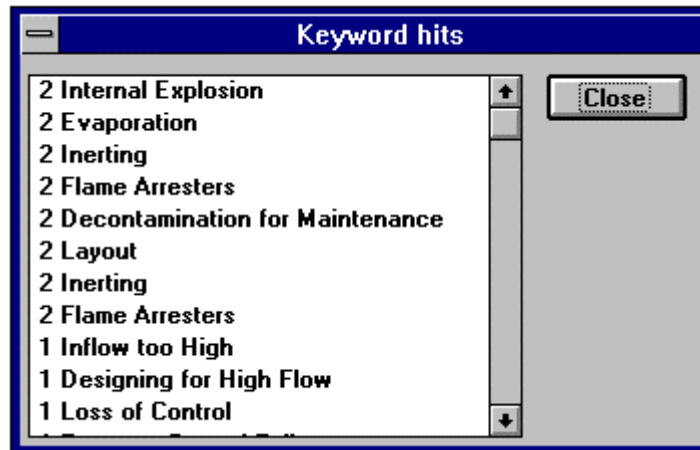
Kuva 9. Avainsanojen valitseminen.



Kuva 10. Avainsanahaun tulokset navigointi-ikkunassa esitettyinä.

Avainsanahaussa lasketaan osumat eli kuinka monta neuvoihin liitetystä avainsanoista esiintyi avainsanakyselyssä. Tällä perusteella kullekin neuvolle saadaan numeroarvo, jonka mukaan arvioidaan kuinka oleellista tietoa neuvossa esitetään. Kyselyn tulokset esitetään navigointi-ikkunassa (kuva 10). Kunkin otsikon eteen ilmestyy kaksi lukua, joista ensimmäinen kertoo suurimman löytyneen osumamäärän kyseisen otsikon kaikilla alitasoilla. Jälkimmäinen numero kertoo montako osumaa sattui kyseiseen otsikkoon.

Vaihtoehtoisesti avainsanahaun tuloksia voi katsella avainsanahaun tulosikkunassa, joka on valintaikkuna, jossa haussa osumia saaneet otsikot on lajiteltu osumien määrän mukaan laskevaan järjestykseen (kuva 11). Avainsanahaun tulosikkunaan pääsee valitsemalla valikosta ”View” vaihtoehdon ”Hits”. Myös tässä ikkunassa neuvon otsikkoa kaksoisnapsauttamalla saadaan itse neuvo näkyviin neuvoikkunassa. Tällöin navigointi-ikkunassa tehty valinta ei kuitenkaan muutu.



Kuva 11. Avainsanahaun tulokset avainsanahaun tulosikkunassa.

Käyttäjät voivat myös hakea neuvoja vapaalla tekstihaulla. Valitsemalla mitä tahansa sanoja hakuun, käyttäjälle näytetään ne kaikki neuvot, joissa teksti esiintyi. Neuvot näytetään neuvoikkunassa siinä järjestyksessä kun ne esiintyvät sisällysluettelohierarkiassa.

3.7 Loki ja muistiinpanot

ELDER-hyperkirjan käytöstä suunnittelun viimeistelyvaiheessa on kaksi etua tiedon hyvän saatavuuden lisäksi. Ensimmäiseksi järjestelmä tarjoaa mahdollisuuden tallentaa suunnittelutietoa, joka helpottaa muita samassa projektissa työskenteleviä ihmisiä. Toiseksi se kirjaa muistiin tietoa, kuinka suunnittelija käytti järjestelmää. Se luetteloi luetut neuvot ja tarjoaa siten mahdollisuuden tarkastella jälkepäin suunnitteluprosessin etenemistä.

Muistiinpanomekanismi kirjaa automaattisesti tilatietoja, joiden lisäksi käyttäjä voi kirjoittaa omia muistiinpanojaan. Tilatiedot sisältävät muistiinpanon tekijän nimen, laitoksen, käsiteltävän projektin sekä neuvon, joka oli näkyvässä kun muistiinpanoa kirjattiin. Muistiinpanoja voi lajitella ja lähettää eteenpäin. Kirjaukset voidaan tehdä pakollisiksi tai vapaaehtoisiksi.

Loki näyttää, mitkä neuvot on luettu ja milloin asetustiedot ovat muuttuneet. Näin suunnittelija voi varmistua, että kaikki näkökohdat on otettu huomioon. Myös laitoksen turvallisuudesta vastaavat saattavat haluta varmistaa, että suunnittelun yhteydessä kaikki potentiaaliset turvallisuusongelmat on käyty läpi.

3.7.1 Muistiinpanot

Käyttäjä voi halutessaan tehdä muistiinpanoja valitsemalla valikosta ”Edit” vaihtoehdon ”Note”. ELDER-hyperkirjan muistiinpanojen tarkoituksena on antaa prosessisuunnittelijalle mahdollisuus tallentaa ajatuksiaan suunnittelun kuluessa. Hän saattaa esimerkiksi tallentaa syyn, miksi jonkun neuvon antamaa ohjetta ei noudatettu, ja selvittää erityiset olosuhteet, joiden vuoksi tämä päätös oli perusteltu.

Muistiinpanoja voidaan tallentaa lyhyisiin ’muistilappuihin’. Leikkaa ja liitä -toimintoja voidaan käyttää liittämään muistiinpanoon osia ELDER-hyperkirjan neuvoteksteistä. Kun käyttäjä tekee muistiinpanon, vakiotiedot lisätään muistiinpanoon. Näitä ovat kirjoittajan tunniste, päiväys, kellonaika sekä neuvo, johon muistiinpano liittyy. Käyttäjä voi halutessaan liittää muistilappuun automaattisesti myös projektin ja laitteen nimen.

3.7.2 Loki

Lokitiedoston tarkoituksena on kirjata ELDER-hyperkirjan käyttäjän toimia käytön aikana. Tämä helpottaa käyttäjää tarkistamaan prosessin turvallisuuden, sekä helpottaa turvallisuudesta vastaavan henkilön tekemää suunnitelman tarkastusta.

Loki perustuu sisällysluetteloon ja aloittaa toimintansa, kun projekti on valittu. Projektin aikana luetut neuvot merkataan lokiin, jotta voidaan jälkikäteen tarkistaa, mitä neuvoja on luettu. Luetut neuvot näytetään käyttäjälle vaihtamalla sisällysluettelossa olevan ikonin taustaväri vihreäksi. Asetuksia muuttamalla on mahdollista tarkastella nykyistä istuntoa tai koko projektia. Lokia seuraamalla pystytään myös selvittämään, millaisia asetustietoja käytettiin istunnon eri vaiheissa.

Loki kirjaa tietoa seuraavista tapahtumista:

- projektin luonti, valinta ja tuhoaminen
- laitteen luonti, valinta ja tuhoaminen
- asiasanojen asetusten muuttuminen
- neuvojen lukeminen
- muistiinpanon luonti, muuttaminen ja tuhoaminen
- lokin käyttötilan muuttaminen.

Lokilla on kolme eri käyttötilaa. Lokin ollessa pois käytöstä kirjataan kuitenkin tiedot projektien luonnista ja poistamisesta, sekä laitteiden luonnista ja poistamisesta.

Käsitöissä tilassa kaikki muut tapahtumat tallentuvat automaattisesti paitsi neuvon luvun kirjaaminen. Halutessaan käyttäjä voi kirjata esillä olevan neuvon lokiin luetuksi painamalla navigointi-ikkunan työkalupalkissa olevaa lokin painiketta. Lokin automaattisessa tilassa järjestelmä tallentaa itsenäisesti kaikki lokitapahtumat.

3.8 Neuvokirjan luontityökalut

Jotta neuvoja attribuutteineen pystyttäisiin tuottamaan ja hallitsemaan, on toteutettu erityinen neuvon luonti- ja ylläpitojärjestelmä. Järjestelmän perustana on käytetty MultiDoc-dokumentinhallintatyökalua.

ELDERin neuvokirjan luonti tapahtuu kolmessa vaiheessa. Ensimmäisessä vaiheessa neuvon kirjoittaja luo neuvossa tarvitsemansa tekstin ja kuvat haluamallaan työkaluilla sekä valmistelee neuvoon liitettävät määrytykset. Toisessa vaiheessa neuvo siirretään MultiDoc-ohjelman alaisuuteen. Samalla neuvoihin liitetään niihin liittyvät määrytykset eli avainsanat, asiasanat ja laitetyypimäärytykset.

Kun neuvot on siirretty MultiDoc-ohjelman alaisuuteen ja tarvittavat määrytykset on tehty, tiedot voidaan muokata ELDERin ymmärtämään muotoon. MultiDoc-ohjelman avulla huolehditaan myös ELDER-hyperkirjan neuvon versionhallinnasta, version hyväksynnästä ja editoinnista. Koska neuvokirjan luomiseen osallistuu yleensä useita eri paikoissa työskenteleviä asiantuntijoita, syntyy tuloksena useita MultiDoc-tietokantoja, jotka on yhdistetään ELDERin neuvokirjan luonnin kolmannessa vaiheessa. Tätä tehtävää varten on neuvokirjan osien yhdistämistyökalu, joka käyttäjän ohjaamana luo ELDER-kirjan muodostavan Folio Views -tiedoston ja tietokannan. Neuvot, neuvohierarkia, asiayhteystiedot ja hakutiedot muodostetaan automaattisesti MultiDoc-ohjelmaan aiemmin syötetyn tiedon pohjalta, mutta sisällysluettelon järjestelyyn tarvitaan käyttäjän ohjausta.

4. HAZID

4.1 Tietokoneavusteinen poikkeamatarkastelu

Systemaattisten turvallisuusanalyysien merkitys ymmärretään prosessiteollisuudessa laajalti. Turvallisuusanalyysin menetelmät auttavat löytämään mahdollisia yhteyksiä syiden ja seurausten välille, mikä tarjoaa mahdollisuuden etsiä keinoja näiden yhteyksien aktivoitumisen estämiseksi [Hollnagel & Cacciabue 1992]. Poikkeamatarkastelun (HAZOP) tavoitteena on tunnistaa kaikki mahdolliset poikkeamat kohdejärjestelmän suunnitellusta toiminnasta ja niihin liittyvät vaarat [CIA 1977, Kletz 1983]. Poikkeamatarkastelu on muodostunut tavanomaiseksi turvallisuusanalyysin laadintamenettelyksi kemian prosessiteollisuudessa. [CCPS 1985], [Rouhiainen 1990] ja [Lees 1996] kuvaavat tarkemmin poikkeamatarkastelua ja muita vaarojen tunnistamismenetelmiä

Poikkeamatarkastelussa lähtöoletus on, että kohdejärjestelmä on turvallinen, kun kaikilla prosessia kuvaavilla parametreilla on normaali tai muutoin hyväksyttäväksi määriteltä arvo. Laittevat, inhimilliset virheet ja ulkoisesta ympäristöstä aiheutuvat häiriöt ilmenevät prosessia kuvaavien parametrien arvojen muutoksina. Kohdelaitoksen kuvausta, yleensä virtaus- tai PI-kaaviota, käytetään tarkastelun pohjana. Kohdejärjestelmän putkiliinat, säiliöt, reaktorit ym. keskeiset osat käydään läpi, kaikki mahdolliset poikkeamat kattavan avainsanalistan avulla. Tavoitteena on tunnistaa ne tapahtumaketjut, joiden ilmeneminen on tunnistettujen potentiaalisten syiden valossa mahdollista ja jotka voivat johtaa vaarallisiin seurauksiin.

Systemaattisen luonteensa vuoksi poikkeamatarkastelu soveltuu hyvin automatisoitavaksi erityisesti tietämyspohjaisia menetelmiä käyttäen [Venkatasubramanian & Vaidhyathan 1994]. Lisäksi Parmar & Lees [1987] toteavat, että kattavuus on hyvän vaarojen tunnistamismenetelmän oleellisin piirre. Poikkeamatarkastelu tuottaa rajatun poikkeamaluettelon pohjalta etukäteen rajaamattoman joukon syitä ja seurauksia ja soveltuu siksi paremmin vaarojen tunnistamiseen kuin logiikaltaan puumaiset tekniikat, jotka perustuvat siihen, että joko tarkasteltavien syiden tai seurausten joukko on etukäteen rajattu.

Poikkeamatarkasteluun ei sen puhtaasti kvalitatiivisen luonteen vuoksi sisälly tunnistettujen vaarojen laskennallista arviointia tai priorisointia. Tarkastelun lopputuloksena saadaan joukko tunnistettuja vaaroja ja niiden mahdollisiksi arvioituja syitä. Vakavuudeltaan merkittävät tapahtumaketjut löytyvät menetelmällä hyvin, mutta usein samalla tulee raportoiduksi paljon sellaista poikkeamiin liittyvää tietoa, joka on epäoleellista vakavimpien vaarojen tunnistamisen kannalta. Osa tästä epäoleellisesta tiedosta voi jopa

tarkemmassa kvantifiointia sisältävässä tarkastelussa osoittautua virheelliseksi tai täysin tarkasteltavaan tilanteeseen sopimattomaksi.

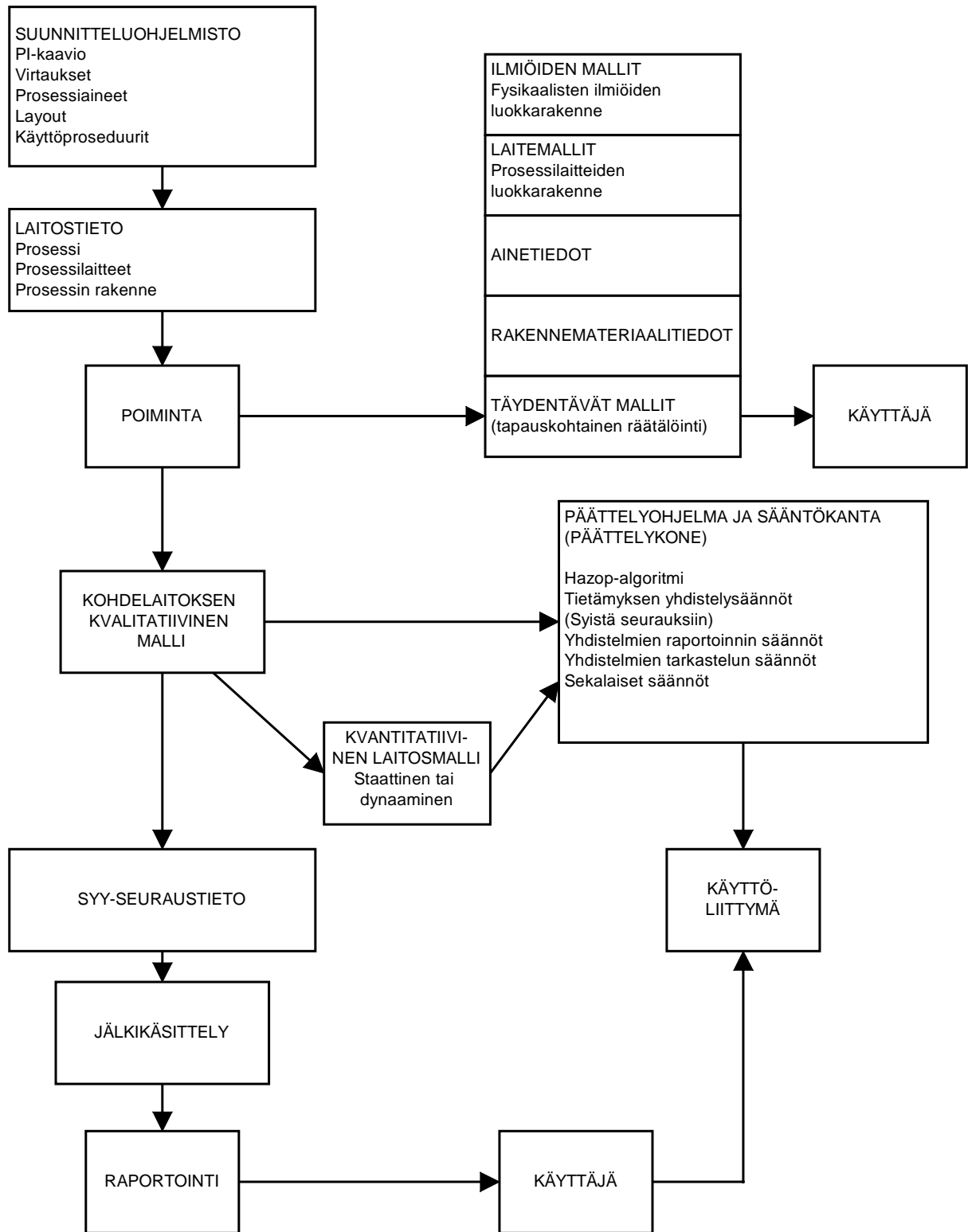
Huono epäoleellisen tiedon erottelukyky on poikkeamatarkasteluun ja muihin vastaaviin kvalitatiivisiin menetelmiin luontaisesti liittyvä ongelma, jota on vaikea täysin poistaa. Kokeneet poikkeamatarkasteluryhmän vetäjät pystyvät kuitenkin yleensä hyvin välttämään ryhmän ajan haaskaamista epäoleellisiin pohdiskeluihin. Vetäjä voi ohjalla poikkeamatarkastelun kulkua sopivasti ja saada ryhmän jäsenet nojautumaan omaan kokemukseensa ja keskittymään oleellisimpiin asioihin.

Kun poikkeamatarkastelua pyritään automatisoimaan, ongelmaa ei voida ratkaista edellä esitettyyn tapaan, vaan tietokoneohjelmistoa kehitettäessä on otettava huomioon tarve karsia epäoleelliset tiedot pois lopputuloksista. Karsinta on mahdollista toteuttaa kahdella tavalla:

- Annetaan ohjelmiston käyttäjän tehtäväksi arvioida ja hyväksyä tietokoneen ehdottamat tapahtumaketjut.
- Toteutetaan ohjelmistoon älykkäitä piirteitä, joiden avulla voidaan tarkistaa tunnistettujen tapahtumaketjujen merkitys.

Prosessivaarojen tietokoneavusteisen tunnistamisen lähtökohtana on tietämuspohjaisia tekniikoita käytettäessä kohdeprosessin rakenteen kuvaus. Päätelyprosessin tuloksena saadaan raportti potentiaaliin vaaroihin liittyen tunnistetuista syy-seurausketjuista.

Rushton [1997] on havainnollistanut tietämuspohjaista poikkeamatarkastelua käsittelevässä selvityksessään tämän sovellusalueen ohjelmiston tyypillistä rakennetta kuvassa 12 esitetyllä tavalla.



Kuva 12. Tyypillisen tietämyspohjaisen poikkeamatarkasteluohjelmiston rakenne [Rushton 1997]

Laitoskohtaisen tietämyksen pitäminen erillään laitosriippumattomasta on tietämuspohjaisen poikkeamatarkastelun oleellinen piirre. Tietämyksen laitoskohtainen osuus kuvaa kohdelaitoksen prosessilaitteita ja niiden ominaisuuksia, prosessilaitteiden liittymistä toisiinsa sekä prosessissa virtaavia aineita ja vallitsevia prosessiolosuhteita. Tätä osuutta tietämyksestä kutsutaan yleensä laitoskuvaukseksi.

Tietämyksen laitosriippumaton osuus koostuu prosessilaitteiden käyttäytymistä kuvaavista yleiskäyttöisistä malleista. Ne painottuvat epänormaaleihin oloihin liittyvien ilmiöiden kuvaamiseen. Koska erityyppisiä prosessilaitteita käsitellään malleissa irrallaan prosessiympäristöstä, ne ovat laitosriippumattomia ja soveltuvat siten erilaisten prosessien tarkasteluun. Todellisuutta vastaavan tarkastelun laatiminen edellyttää tietysti, että prosessissa esiintyvät laitteet sisältyvät mallikirjastoon ja ovat siten käytettävissä laitoskuvaukseen.

Tietämuspohjaisen ohjelman päättelykone soveltaa laitoskohtaista tietämystä mallikirjastosta valitsemiinsa yleiskäyttöisiin malleihin. Toisin sanoen laitoskuvaus ohjaa syy-seuraustiedon valintaa malleista. Valittu syy-seuraustieto raportoidaan laitoskohtaiseksi muokattuna.

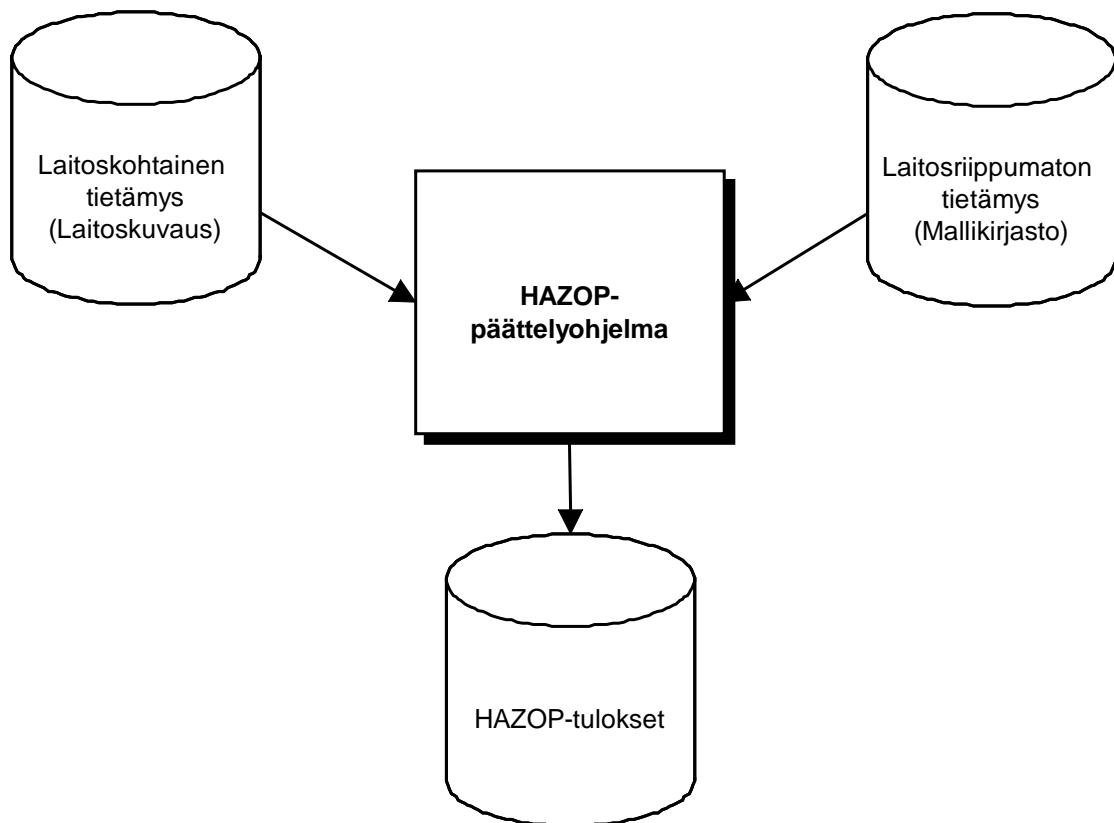
Riittävän yksityiskohtaisuuden saavuttaminen on vaikeaa yleiskäyttöisiin malleihin perustuvaa päättelytekniikkaa käytettäessä, koska malleihin täytyisi yksityiskohtien vuoksi sisällyttää runsaasti laitoskohtaisesta tiedosta riippuvia ehtoja. Ehtojen lisääminen tekisi mallintamisen liian monimutkaiseksi ja lisäisi myös käyttäjältä vaadittavien lähtötietojen määrää. Ehtoja ja niihin perustuvaa älykkyyttä on kuitenkin tarpeen lisätä, muutoin tietämuspohjaisen poikkeamatarkastelun tulokset jäävät liian yleiselle tasolle ollakseen käyttökelpoisia.

Tietämuspohjaisen poikkeamatarkastelun tyypillisiksi käyttäjiksi on arveltu suunniteluinsinöörejä, jotka haluavat tarkistaa laatimansa suunnitelman ennen varsinaista ryhmätyönä laadittavaa poikkeamatarkastelua. Suunnittelijat voisivat käyttää ohjelmaa potentiaalisten ongelmien tunnistamiseen myös suunnittelun aikaisemmissa vaiheissa, ennen kuin yksityiskohtaisia PI-kaavioita on käytettävissä. Tällöin ongelmien korjaaminen suunnitelmiin muutoksia tekemällä ei ole niin kallista kuin suunnittelun edettyä pitemmälle.

4.2 HAZID-ohjelmiston rakenne ja toiminta

4.2.1 Ohjelmiston perusrakenne

HAZID-ohjelmisto toteutettiin nojautuen Loughborough Universityn ja VTT:n aikaisempiin kokemuksiin tietämyspohjaisen poikkeamatarkastelun menetelmäkehityksestä. Kuvassa 13 on esitetty ohjelmiston perusrakenne, joka noudattelee edellä esitettyjä tyyppillisiä ratkaisuja.



Kuva 13. HAZID-ohjelmiston perusrakenne.

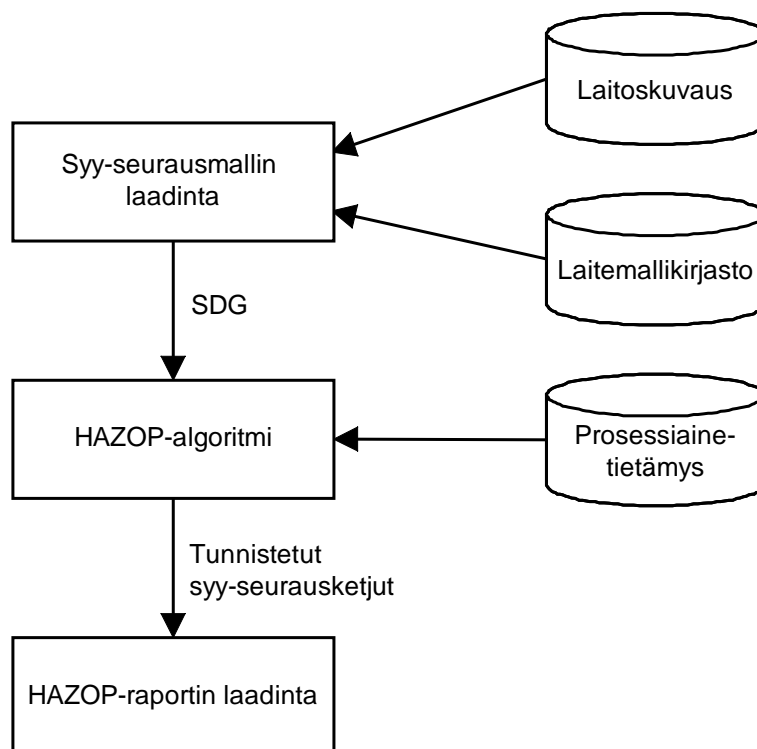
Prosessilaitteiden vikaantumista ja niistä aiheutuvien poikkeamien etenemistä kuvaavat kvalitatiiviset mallit ovat tietämyspohjaisen poikkeamatarkastelun perusta. Nämä laitosriippumattomat mallit on tallennettu mallikirjastoon, joka on täysin itsenäinen päättelyohjelmasta ja laitoskuvauksesta erillään oleva kokonaisuus.

HAZOP-päätelyohjelma sisältää poikkeamatarkastelun automaattiseen laadintaan vaa-
dittavat proseduurit. Se käyttää mallikirjastoa laitevikojen ja eri laitetyyppeihin liitty-
vien potentiaalisten vaarojen tietolähteenä.

Jotta voitaisiin soveltaa mallikirjaston yleiskäyttöisiä malleja kohteena olevaan laitok-
seen, ohjelmalle on annettava kuvaus kohdelaitoksesta. Se sisältää tiedot kohdelaitoksen
laitteista ja niiden välillä kulkevista virtauksista. Laitoskuvaukseen nojautuen HAZOP-
päätelyohjelma valitsee oikeat mallit mallikirjastosta ja laatii poikkeamatarkastelun.
Tulokset esitetään tavanmukaisten poikkeamatarkastelulomakkeiden muodossa.

HAZIDin päätelytoiminnot perustuvat Signed Directed Graph (SDG) -kuvaustekniikan
käyttöön. Se generoi laitoskuvausta ja mallikirjaston laitosriippumattomia malleja
käyttäen SDG-mallin, joka kuvaa laitevikojen ja muiden häiriöiden vaikutuksia proses-
sin eri osiin. HAZID käy tämän SDG-mallin läpi systemaattisesti HAZOP-algoritminsa
avulla.

Aineominaisuudet otetaan huomioon erityisen prosessiainemallin ja sitä käyttäen tehtä-
vien tarkistusten kautta. HAZOP-analyysin laadinta on toteutettu kuvassa 14 esitetyllä
tavalla.



Kuva 14. HAZID-ohjelman HAZOP-analyysitoteutus.

4.2.2 Laitemallikirjasto

Laitemallikirjasto kattaa niiden laitetyyppien kvalitatiiviset mallit, joita on HAZID-ohjelman avulla mahdollista tarkastella. Mallit muodostavat hierarkian, jossa osa laitetypille määritellyistä ominaisuuksista voi periä sen alityypeille.

HAZIDin päättelytoiminnot perustuvat SDG-esitystavan käyttöön. SDG:n ”kaaret” (arc) kuvaavat syy-seuraussuhteita. Laitemalleihin on SDG-muodossa koottu kullekin laitetypille yleisesti voimassa olevat syy-seurausketjut.

Mallien oliopohjainen toteutus tarjoaa mahdollisuuden käyttää toisia malleja uusien mallien määrittelyssä. Kun määritellään sellaisen laitetyypin mallia, joka on toisen alityyppi, syyseurausketjumäärittelyt voivat osaksi periä ylemmän tason mallista ja osaksi olla uusia laitetyyppien välisiä eroavaisuuksia kuvaavia määrittelyjä. Lisäksi on mahdollisuus määrittellä toistuvasti esiintyviä piirteitä kuvaavia apumalleja ja siten nopeuttaa varsinaisten laitemallien laadintaa.

Malleihin on myös mahdollista määrittellä ehdollisia osioita. Tällöin samaa laitemallia voi käyttää toisistaan tietyltä ominaisuudeltaan poikkeavien laitteiden tarkasteluun.

Laitemallien ensisijainen tarkoitus on määrittellä poikkeamien, vikojen ja seurausten kvalitatiiviset riippuvuudet kullekin laitetypille. Mallien tehtävänä on myös

- laitetypin sisään- ja ulosmenojen määrittely
- määrittelyt, mitkä sisään- ja ulosmenot on laitetta käytettäessä oltava yhdistettyinä toisiin laitteisiin
- laiteominaisuuksien oletusarvojen määrittely.

STOPHAZ-prototyypin osana julkistettu mallikirjasto sisältää yli 50 laitetypin mallit. Esimerkkejä kirjaston malleista ovat tislauskolonni, kaasu-neste-neste-erotin, mäntäpumppu ja signaalinjakaja. Yksityiskohtaiset laitemallit on ryhmitelty yhdeksään laiteryhmään, joita ovat mm. säiliö, paineenkorotus ja instrumentti.

4.2.3 HAZOP-algoritmi

Normaali poikkeamatarkastelun laadintamenettely perustuu kohdejärjestelmän systemaattiseen läpikäyntiin. Jokaista prosessiyksikköä tarkastellaan vuorollaan ja kaikki prosessisuureiden poikkeamat käsitellään. Tavoitteena on tunnistaa

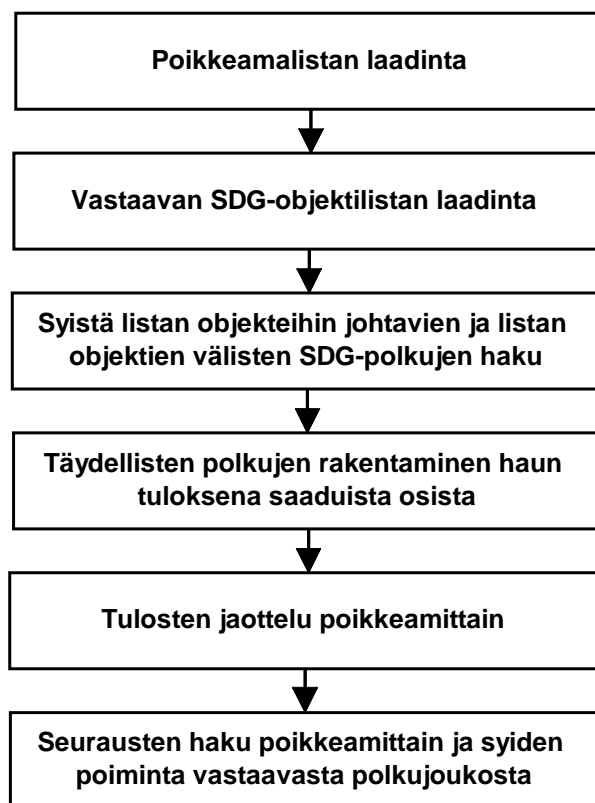
- poikkeamien mahdolliset syyt, esim. laiteviat tai muut häiriöt

- poikkeamien ja niiden syiden vaarallisiksi arvoidut potentiaaliset seuraukset.

Periaatteessa HAZID jäljittelee tätä normaalia analyysimenettelyä. On kuitenkin laskennallisesti epäkäytännöllistä suorittaa tarvittavat syy- ja seuraustietojen haut täsmälleen sen mukaisesti.

Yksinkertainen hakumenettely, joka perustuu SDG-aineiston läpikäyntiin poikkeama kerrallaan, poimii ensin kaikki kyseisen prosessisuureen muutokseen johtavat polut ja hylkää sitten ne, joiden muutos on väärän suuntainen. Turhaa työtä aiheutuu silloin, kun saman prosessisuureen vastakkaista poikkeamaa tarkasteltaessa poimitaan uudelleen samat tiedot. Toistuvaa saman tiedon hakua ilmenee myös silloin, kun SDG-malleissa on yhteyksiä eri poikkeamien välillä.

HAZID noudattaa tehokkaampaa hakumenettelyä, jossa kerätään kaikkiin poikkeamiin liittyvät tiedot kerralla. Haun jälkeen tiedot jaotellaan poikkeamittain. Tämän menetelmän mukaisesti toteutettu HAZIDin HAZOP-algoritmi on esitetty kuvassa 15.



Kuva 15. HAZIDin HAZOP-algoritmi.

4.2.4 Tulosten karsinta

Tietyn syy-seurausketjun merkitystä on mahdollista arvioida joko haun aikana tai sen päätyttyä. Haun päätyttyä tehtävä arviointi tähtää epäoleellisen tai virheellisen tiedon karsintaan lopullisista tuloksista.

HAZID:iin sisältyy kolme karsintaproseduuria:

- Samankaltaisten syy-seurausketjujen yhdistäminen yhdeksi syy-seurausketjuksi
- Eri poikkeamien yhteydessä toistuvasti raportoitujen syy-seurausketjujen poistaminen
- Toistuvasti esiintyvien syy-seurausketjujen korvaaminen viittauksella raportissa.

Karsinta on HAZIDin nykyisessä versiossa varsin rajoittunutta. Monia kontekstista riippuvia operaatioita olisi mahdollista toteuttaa karsintaproseduureina. Nämä proseduurit voisivat käyttää lähtöaineistonaan HAZOP-algoritmin tuottamaa alustavaa raporttia ja suorittaa monimutkaisia päättelyoperaatioita epäoleellisen tiedon tunnistamiseksi. Tällöin osa monimutkaisemmista päättelyoperaatioista voitaisiin siirtää HAZOP-algoritmin alaisuudesta jälkepäin tehtäviksi, ja HAZOP-algoritmin suoritus saattaisi nopeutua merkittävästi.

5. Käyttökokeilut

5.1 ELDER

5.1.1 Arvioinnin toteutus

ELDER-prototyypille järjestettiin käyttökokeilu, jotta saataisiin riittävää ja projektin toteuttajista riippumatonta palautetta. Tavoitteena oli löytää prototyypin puutteet ja parannuskohteita seuraavaa prototyyppiä varten. Tämä mahdollisti lopullisen version soveltamisen käyttäjien todellisten tarpeiden mukaiseksi.

Käytännön syistä testaus jaettiin kahteen osaan:

- 1) Ensimmäisessä vaiheessa projektitiimissä tarkisteltiin neuvojen sisällön laatua sekä sitä, kuinka hyvin ELDER täytti sille asetetut käyttäjävaatimukset.
- 2) Testauksen toisessa vaiheessa kerättiin loppukäyttäjiltä palautetta prototyypin soveltuvuudesta todellisiin suunnittelutilanteisiin.

Kaikille käyttötesteihin osallistuneille asiantuntijoille annettiin tehtäväksi selvittää seuraavia seikkoja:

- tarkistaa, että järjestelmä toimii määrittelyn mukaisesti sekä virheettömästi
- arvioida, oliko ELDER käyttökelpoinen ja miksi
- arvioida, olisiko ELDERistä edelleen kehiteltynä merkittävää hyötyä
- tunnistaa toiminnot, joita olisi edelleen kehiteltävä ja asettaa ne tärkeysjärjestykseen
- tunnistaa, minkä alan tietämystä olisi tärkeintä lisätä neuvoihin.

Testien aikana ELDERiä testasi 17 henkilöä. Projektiryhmälle palautetuista testilomakkeista saatiin 81 ELDERiin liittyvää havaintoa. Nämä käyttäjien tekemät havainnot ja huomiot käytiin läpi ja ryhmiteltiin sisältönsä mukaan tulevaa analyysiä varten.

5.1.2 Arvioinnin tulokset

Havaittiin, että ELDERin perusajatus oli käyttäjien mielestä hyödyllinen. Erityisesti käyttäjät pitivät valittua 12 pääotsikon käyttöä tehokkaana tapana turvallisuus-, terveys- ja ympäristövaatimusten läpikäymisen varmistamiseksi laitoksen perusratkaisujen suun-

nittelun aikana. Samoin ELDERin hakumekanismeja pidettiin helppokäyttöisinä ja nopeutta riittävänä.

Neuvojen hierarkkinen rakenne tunnustettiin tehokkaaksi tavaksi saada selkeitä, erilaisen yksityiskohtaisuustason neuvoja. Navigoimalla järjestelmässä käyttäjä saa esiin turvallisuuteen liittyvää tietoutta ja voi siten määritellä parhaan turvallisuusstrategian.

Järjestelmän heikkoudeksi koettiin prototyypiversiossa käytössä ollut neuvojen esitystapa sekä hakujärjestelmässä olevien avainsanojen vähäinen määrä. Siksi ELDERin hyödylliseksi koetun toiminta-ajatuksen toteutusta pidettiin puutteellisena.

Eri neuvojen kirjoittajilla oli erilaisia käsityksiä siitä, mikä oli turvallisuuteen liittyvää ja mikä ei. Tämä on ymmärrettävää, mutta se johti usein yksityiskohtaisuuden vaihteluun eri kappaleissa. Niinpä tarvittaisiin keino, jolla saataisiin yhdenmukaistettua neuvojen yksityiskohtaisuustaso neuvojen luontivaiheessa.

Useat käyttäjät kaipasivat neuvoissa enemmän havainnollistavaa materiaalia, kuten kaavioita, taulukoita ja esimerkkejä hyvästä suunnittelusta. Samoin taulukkolaskentalomakkeita ja laskentatyökaluja kaivattiin, jotta voitaisiin tehdä laskennallisia arvioita (quantitative assessment).

Kommenttien perusteella havaittiin, että jatkokehitystä tarvitaan erityisesti seuraavilla alueilla:

- Neuvojen kattavuutta tulisi parantaa.
- Järjestelmässä mukana olevien prosessiyksikkötyyppien määrää tulisi kasvattaa, jotta käyttäjien luottamus ohjelmiston kattavuuteen eri suunnittelutilanteissa kasvaisi.
- Neuvojen rakenne tulisi yhdenmukaistaa eli käytännössä tehdä neuvojen kirjoittajille yhtenäiset ohjeet neuvojen ulkoasusta ja asiasisällön tyylistä.
- Hakutoimintoihin käytettävien avainsanojen ja asiasanojen määritysten suunnitteluun tulisi keskittyä enemmän.

5.1.3 Johtopäätökset

Verkkoselaimet kehittyivät huomattavasti projektin aikana. Samoin WWW löi itsensä läpi. Siten neuvojen esittäminen html-muodossa olisi jatkossa mielekäs vaihtoehto, varsinkin kun samanaikaisesti selaimien lisäksi markkinoille ilmaantui helppokäyttöisiä html-editoreita, joilla neuvojen kirjoittaminen HTML-muotoon on yhtä helppoa kuin millä tahansa tekstinkäsittelyohjelmalla. Samalla päästäisiin eroon maksullisesta ja tällä

hetkellä ELDERissä välttämättömästä Folio Views -lisenssistä. Projektin alkuvaiheessa kyseisiä työkaluja kuitenkin ei ollut saatavissa, ja verkkoselainten käyttö ohjelmallisesti olisi ollut hankalaa.

HTML:n etuna on myös sen selväkielisyys. Avainsanat, asiasanat, linkit ja laitetyypin määritykset olisi mahdollista sijoittaa html:n kommenttikenttiin. Tämä edellyttäisi kuitenkin neuvokirjan luontityökalun täydellistä uudelleenohjelmointia.

Projektin loppuvaiheessa neuvojen esittämiseen käytettävän työkalun vaihtaminen ei ollut mahdollista, koska merkittävä osa hyperkirjasta oli jo kirjoitettu Folio Views:llä. Samoin projektissa mukana ollut ohjelmistotalo oli tehnyt merkittävästi töitä Folio Views -ympäristössä toimivan neuvokirjan luontityökalun valmistamiseksi. Html-kieleen siirtymisestä luovuttiin, koska asia tuli esiin, kun projektista oli enää vain neljännes jäljellä.

ELDER-hyperkirjan sisällön kehittämisen lisäksi ohjelman käynnistys tulisi saada nopeammaksi. Käynnistymisen yhteydessä ohjelma lukee muistiin kaikki neuvojen otsikot, mikä hidastaa merkittävästi ohjelman käynnistymistä. Projektin aikana käynnistymisen hitautta ei katsottu merkittäväksi ongelmaksi, kun sen avulla saatiin neuvokirjan sisällysluettelon käsittely käytön yhteydessä nopeaksi. Käynnistymisen nopeuttaminen olisi mahdollista muuttamalla tapaa, jolla sisällysluetteloä käsitellään ohjelmassa, mutta todennäköisesti käynnistymisen nopeuttaminen vaatisi runsaasti kokeiluja ja sisällysluettelon käsittelytavan perusteellista muutosta.

Haittana nykyisessä tietojen esittämisessä havaittiin laitetyyppien sisällyttäminen neuvojen otsikkotietojen joukkoon. Osa neuvojen kirjoittajista käsitti MultiDoc:ssa tehdystä neuvojen attribuuttien määrityksessä laitetyyppimerkinnän väärin, jolloin käytettävän laitetyypin valinta neuvokirjaa selatessa toimii virheellisesti.

Siksi laitetyyppilista tulisi irrottaa sisällysluettelosta erilliseksi etukäteen määriteltäväksi luetteloksi. Tämä selkiyttäisi käytettäviä käsitteitä. Samoin laitetyyppilista tulisi kiinnittää jo ennen varsinaista neuvojen kirjoittamista. Muutokset laitetyyppilistaan tulisi tehdä keskitetysti, jotta kaikilla kirjoittajilla olisi sama laitetyyppilista käytössään.

Neuvojen selauksessa kaivattiin verkkoselaimista tuttuja back- ja forward-nappeja, joilla pääsisi nopeasti katsomaan juuri hetkeä aikaisemmin katseltuja neuvoja. Tämä toiminto sopiikin hyvin yhden istunnon näkökulmasta katsottuna staattisena säilyviin html-sivuihin. ELDERin tapauksessa täytyy muistaa, että laitetyypin ja asiasanavalintojen vaikutuksesta sisällysluettelosta katoaa tai ilmestyy neuvoja. Jos toimintoa ei verkkoselainten toimintaan verrattuna muuteta, voidaan päätyä sellaiseen neuvoon, jota ei kyseisessä tilanteessa saisi näyttää. Yksinkertaisin tapa kiertää tämä ongelma on tyh-

jentää historiatieto selatuista neuvosivuista aina kun asiasana-asetukset tai komponenttityyppi vaihtuu.

Laitoksen suunnittelukäytössä erillisten työkalujen käyttöä vieroksutaan jossain määrin. Tämän vuoksi olisi käytännöllistä sisällyttää ELDERin kaltainen työkalu jo suunnittelijan muutoinkin käyttämään suunnittelutyökaluun.

ELDERin projektinhallinnassa oli vielä puutteita. Luetut neuvot tulisi olla nähtävissä myös laitteittain. Tarvittava tieto on jo tietokannassa, mutta esitystapa puuttuu. Lähinnä ongelmana on, miten kaikki tarvittava tieto saadaan esitettyä sisällysluettelossa siten, että se säilyy selkeälukuisena. Mahdollisena ratkaisuna voisi olla tekstimuotoisen raportin luominen halutusta osuudesta laitteita. Lisäksi projektihallintaan kaivattiin projektikohtaisia käyttörajoituksia. Kullekin projektille tulisi pystyä laatimaan lista käyttäjistä, jotka voivat lukea tai muuttaa projektiin liittyvää tietoa.

Käyttäjiltä lähtöisin ollut toive oli käyttäjien kirjaamien muistiinpanojen raportointi. Tämä on ilmeisestikin tarpeellista, sillä sisällysluettelosta on työlästä etsiä yksittäisiä muistiinpanoja. Toiminnon hyödyllisyys riippuu ratkaisevasti siitä, minkälaiseen tarkoitukseen ja miten muistiinpano-toimintoa käytetään suunnittelutyön aikana.

5.2 HAZID

5.2.1 Arvioinnin toteutus

STOPHAZ-projektin loppuvaiheessa suoritettiin viiden prosessilaitosesimerkin tarkastelu HAZID-ohjelman suorituskyvyn arvioimiseksi. Tarkastellut esimerkit eivät olleet täydellisiä prosessilaitoksia, mutta ne valittiin erityyppisiä prosesseja ja erilaisia vaaroja edustaviksi. Esimerkit olivat kooltaan samaa luokkaa kuin yhden HAZOP-ryhmätyöistunnon aikana tavallisesti läpikäytävät prosessilaitoksen osat.

Evaluointi toteutettiin ryhmätyömuotoisena. Kukin kolmesta rinnakkaisesta asiantuntijaryhmästä tarkasteli yhtä tai kahta esimerkkiä. Kuhunkin ryhmään oli kutsuttu 3 - 4 turvallisuusasiantuntijaa STOPHAZ-hankkeeseen loppukäyttäjinä osallistuneista yrityksistä.

Tarkastellut viisi prosessilaitosesimerkkiä olivat

- absorptiojärjestelmä
- bentseenivarasto
- erotusjärjestelmä
- trikloroetaanivarasto
- propaanin väkevöimistislaus.

5.2.2 Arviointimenetelmä

Kvantitatiivisen arvioinnin mahdollistamiseksi käytettiin tapausten luokitteluun perustuvaa järjestelmällistä menettelyä. Tavoitteena oli selvittää, kuinka hyvin HAZIDin tulokset vastaavat perinteisen manuaalisesti laaditun HAZOP-analyysin tuloksia.

Manuaaliseen HAZOP-raporttiin kirjatut tapahtumaketjut käytiin yksitellen läpi ja selvitettiin, oliko HAZID tunnistanut kyseisen tapahtumaketjun. Lopuksi käytiin yksitellen läpi ne tapahtumaketjut, jotka HAZID oli tunnistanut manuaaliseen HAZOP-raporttiin kirjattujen lisäksi. Tapahtumaketjuiksi luettiin kaikki raportoidut syy-seurausketjut sekä ilman seurauksia tunnistetut syyt.

5.2.3 Arvioinnin tulokset

Yhteenveto evaluoinnin tuloksista on esitetty taulukossa 1.

Taulukko 1. HAZIDin evaluoinnin tulokset.

	<i>HAZIDin tunnistamat oikeat tapahtumaketjut %</i>	<i>HAZIDin tunnistamat oikeat ja kiinnostavat tapahtumaketjut %</i>	<i>HAZIDin tunnistamat tapahtumaketjut HAZOP työryhmän tuloksista %</i>	<i>HAZIDin tunnistamat oikeat suojausjärjestelmät %</i>
Absorptio	49	10	36	10
Trikloroetaanivarasto	33	29	33	29
Propaanin väkevöimistislaus	69	24	60	NA
Betseenivarasto	83	27	50	77
Erotus	53	NA	53	NA

Prosessilaitosesimerkeistä bentseenivarasto osoittautui sellaiseksi, että manuaalisen HAZOP-analyysin laatinut työryhmä oli perustanut työskentelynsä merkittävästi toisenlaiseen laitoskuvaukseen kuin HAZIDin lähtöaineistona olleeseen. Kyseisistä esimerkeistä todettiin mahdottomaksi tehdä luotettavia johtopäätöksiä.

Evaluoinnin tuloksena todettiin, että HAZID löytää tapahtumaketjut kohtuullisen hyvin verrattuna perinteiseen työryhmämuotoiseen HAZOP-analyysiin. Tarkastelluissa esimerkkitapauksissa HAZID löysi työryhmän raportoimista tapahtumaketjuista 33 - 60%. HAZID-tyyppisen ohjelmiston kaupallista hyödyntämistä harkitsevan yrityksen edustaja on arvionaan esittänyt, että automaattinen poikkeamatarkastelutyökalu voisi olla kaupallisesti hyödynnettävissä, jos se kykenisi tunnistamaan 25 % asiantuntijaryhmän tunnistamista vaarallisista tapahtumaketjuista.

Kaupallisen hyödynnettävyyden esteeksi saattaisi muodostua se, että käyttökelpoisten tulosten ohella HAZID tuottaa suuren joukon epäoleellisia ja osittain jopa virheellisiä tuloksia. Teollisissa sovelluksissa vaadittaisiin parempaa suorituskkyä epäoleellisen tiedon karsimisessa.

Epäoleellista tietoa kertyy HAZIDin tuloksiin, koska HAZID ei kykene suuruusluokkaan liittyviin tarkasteluihin. Tämä on tyypillinen kvalitatiivisiin malleihin nojautuvan päättelyn ongelma. Evaluoinnissa yhtenä esimerkkinä tästä ilmenivät lämmönvaihtimen virtauspoikkeamat. Jos jäähdytysveden virtaus keskeytyy, prosessivirtauksen lämpötila nousee ja HAZID varoittaa lämmönvaihtimen ylikuumentumisesta. Varsinaista vaaraa ei kuitenkaan ole, koska jäähdytyksen keskeytyminen ei aiheuta lämpötilan kohoamista prosessisisääntulon lämpötilaa korkeammaksi.

6. YHTEENVETO

STOPHAZ-projektin lähtökohtana oli kehittää joukko työkaluja, joiden avulla prosessilaitosten suunnitteluvaihetta saataisiin nopeutetuksi ja samalla otetuksi huomioon rakennettavan prosessilaitoksen turvallisuus- ja ympäristönäkökohdat. Projektin alkuvaiheessa oletettiin, että tärkeimpänä tavoitteena tulisi olemaan automatisoidun poikkeamatarkastelun mahdollistava ohjelmisto (HAZID). Poikkeamatarkastelussa keskitytään jo olemassa olevan PI-kaavion tarkasteluun. Projektin alussa tehdyssä yli sadan prosessisuunnittelun ammattilaisen haastattelussa paljastui, että tukea kaivattiin enemmän prosessisuunnittelun aikaisempaan vaiheeseen. Tämän seurauksena STOPHAZ-projektin resurssit järjestettiin uudelleen siten, että suurempi osuus projektin resursseista käytettiin prosessin suunnittelua tukevan hyperkirjan (ELDER) toteuttamiseen.

ELDER koostuu joukosta neuvoja, joita hyväksikäyttäen on mahdollista huomioida suunniteltavan laitoksen turvallisuus- ja ympäristönäkökohdat. Tavallisesta hyperkirjasta poiketen ELDERin sisältöön sisällytettiin tietoa siitä, millaista tietoa sivu sisältää. Näitä lisämäärityksiä käytetään hyväksi tiedonhaussa, jotta käyttäjä löytäisi juuri haluamaansa aihepiiriä mahdollisimman tarkkaan kuvaavat tiedot. Toimiva ELDER-kirja saadaan, kun ohjelmarunkoon lisätään hyperkirjan sisältö: neuvokirjan luontityökaluilla tehty SQL-tietokanta ja Folio Views -tietämyskanta.

ELDER ei ole sellaisenaan käyttövalmis. ELDER-prototyyppi kattaa ainoastaan yleisimmät laitetypit, mikä ei riitä kaikkeen prosessisuunnitteluun. Siksi ELDERiä käyttävä organisaatio joutuu täydentämään tai muokkaamaan neuvokokoelmaa omiin tarpeisiinsa sopivaksi. Neuvokirjaa laadittaessa sopivien avainsanojen ja asiasanojen valinta on erittäin vaativa tehtävä. Neuvokirjan onnistunut käyttöönotto yrityksessä vaatii merkittävää panostusta kokeneilta asiantuntijoilta ja ELDERin viemistä kiinteäksi osaksi suunnittelijoiden työtä.

Neuvojen esittämiseen STOPHAZ-projekti valitsi Folio Views -ohjelman. Tällä hetkellä mielekkäitä neuvojen katseluun soveltuvia sovelluksia olisivat WWW-selainohjelmat tai Adoben Acrobat-ohjelma.

HAZID on pitkällisen menetelmäkehityksen tuloksena saavuttanut sellaisen tason, että on mahdollista laatia automaattisesti prosessilaitosten poikkeamatarkasteluja. HAZIDin mallikirjasto on varsin kattava ja korkealaatuinen. HAZID on hyvä lähtökohta turvallisuusanalyysin automatisoinnille.

Arvioinnit osoitti, että HAZID tunnistaa vaaralliset tapahtumaketjut kohtuullisen hyvin. Jatkokehitys on kuitenkin tarpeen ennen kuin tulokset saavuttavat teollisiin sovelluksiin

vaadittavan laatutason. Ongelmana on hyödyllisten tulosten ohella syntyvä suuri määrä epäoleellista tietoa

Lähdeluettelo

AIChE. 1992. Guidelines for Hazard Evaluation Procedures (2nd ed.) With Worked Examples. New York: American Institute of Chemical Engineers. 461 s.

CCPS. 1985. Guidelines for hazard evaluation procedures. Center for Chemical Process Safety (CCPS). AIChE: New York.

CIA 1997. A guide to hazard and operability studies. London: Chemical Industry safety and Health Council of the Chemical Industries Association Limited. 42 s.

Hollnagel, E. & Cacciabue, C. 1992. Reliability assessment of interactive systems with the system response generator. In: Petersen, K. E. & Rasmussen, B. (eds.). Safety and Reliability '92. London: Elsevier Applied Science. S. 140 - 150.

Kletz, T. A. 1983. HAZOP & HAZAN. Notes on the identification and assessment of hazards. Rugby: The Institution of Chemical Engineers. 81 s.

Knowlton, Ellis R. 1992. An Introduction to Hazard and Operability Studies. The Guide Word Approach. Vancouver: Chemetics International. 94 s.

Lees, F. P. 1996. Loss prevention in the process industries. Second edition. London: Butterworths.

Parmar, J. C. & Lees, F. P. 1987. The propagation of faults in process plants: Hazard identification. Reliability Engineering, vol. 17, s. 277 - 302.

Rouhiainen, V. 1990. The quality assessment of safety analysis. Espoo: Technical Research Centre of Finland. Publications 61. 133 p. + app. 30 s.

Rushton, A. G. 1997. Knowledge-based HAZOPs'. Part 2. European Process Safety Centre (EPSC). 18 s.

Venkatasubramanian, V. & Vaidyanathan, R. 1994. A knowledge-based framework for automating HAZOP analysis. AIChE Journal, Vol. 40, No. 3, s. 496 - 505.

Tekijä(t) Kotikunnas, Erkki & Heino, Perttu			
Nimeke Turvallisen prosessilaitoksen suunnittelu STOPHAZ-projektissa syntyneet työkalut			
Tiivistelmä EU:n ESPRIT-ohjelman tuella toteutetun STOPHAZ-projektin tavoitteena oli edistää turvallisten ja ympäristölle vaarattomien prosessilaitosten suunnittelua. Tietokoneavusteisia menetelmiä kehittämällä parannettiin prosessisuunnittelijan mahdollisuuksia tarkastella turvallisuus- ja ympäristönäkökohtia suunnittelun aikana. Tässä raportissa kerrotaan ELDER- ja HAZID-työkaluista, jotka muodostavat STOPHAZ-projektin keskeisimmät tulokset. ELDER on hyperkirja, joka sisältää neuvoja lähinnä turvallisuus-, terveys- ja ympäristönäkökohdista. Hyperkirja sisältää tavallisen kirjan sisällysluettelon kaltaisen navigointi-ikkunan, jossa eri prosessiyksiköistä kertovat neuvot on järjestetty ennalta määriteltyjen vakio-otsikoiden alle. Neuvot voivat sisältää tekstiä, laskentalomakkeita, kuvia ja linkkejä toisiin neuvoihin. Neuvoihin liittyy määrittämiä siitä, millaisille laitetyppeille ne ovat päteviä, sekä määrittämiä, jotka kuvaavat neuvon sisältöä. Neuvoihin liitettyjä määrittämiä käyttävien hakutoimintojen avulla käyttäjä pystyy poimimaan neuvokannasta käsillä olevan ongelman ratkaisemista helpottavat neuvot. Laiteympäristön, prosessiaineiden tms. vuoksi tilanteeseen sopimattomat neuvot karsiutuvat tällöin pois hakutuloksista. HAZID on työkalu vaarojen tunnistamiseksi automaattisesti poikkeamatarkastelua (HAZOP) käyttäen. Lähtökohtana on tieto prosessin laitteista ja kemikaaleista sekä prosessiolosuhteista, tyypillisesti esitettyinä PI-kaaviomuodossa. Tulokseksi saadaan luettelo syy-seurausketjuista, jotka saattavat johtaa vaaratilanteisiin. Tavoitteena on lopputulos, joka vastaa perinteisen ryhmätyönä laaditun poikkeamatarkastelun tulosta sekä laadultaan että kattavuudeltaan. Syy-seurausketjujen tunnistaminen perustuu yleiskäyttöisiin malleihin, jotka kuvaavat erityyppisten laitteiden vikaantumista ja käyttäytymistä häiriötilanteessa. HAZID yhdistelee näitä malleja annettuun laitoskuvaukseen nojautuen siten, että laitevikojen ja muiden häiriöiden vaikutukset kohdelaitoksen eri osien toimintaan tunnistetaan. Koska analyysi on laitoskuvauksen antamisen jälkeen täysin automaattinen, se on helppo toistaa suunnittelun edetessä tai prosessimuutoksia suunniteltaessa ja siten arvioida muutosten vaikutuksia kohdelaitoksen turvallisuuteen.			
Avainsanat plant design, quality assurance tools, hazard and operability studies, safety analysis, intelligent safe design kyberbook			
Toimintayksikkö VTT Automaatio, Riskienhallinta, Tekniikankatu 1, PL 1306, 33101 Tampere			
ISBN 951-38-5697-6 (nid.) 951-38-5698-4 (URL: http://www.inf.vtt.fi/pdf/)		Projektinnumero A9SU00585	
Julkaisu-aika Lokakuu 2000	Kieli suomi, engl. tiiv.	Sivuja 44 s.	Hinta A
Projektin nimi STOPHAZ		Toimeksiantaja(t) Teknologian kehittämiskeskus (Tekes)	
Avainnimeke ja ISSN VTT Tiedotteita – Meddelanden – Research Notes 1235-0605 (nid.) 1455-0865 (URL: http://www.inf.vtt.fi/pdf/)		Myynti: VTT Tietopalvelu PL 2000, 02044 VTT Puh. (09) 456 4404 Faksi (09) 456 4374	

Published by



Vuorimiehentie 5, P.O.Box 2000, FIN-02044 VTT, Finland
Phone internat. +358 9 4561
Fax +358 9 456 4374

Series title, number and
report code of publication

VTT Research Notes 2050
VTT-TIED-2050

Author(s) Kotikunnas, Erkki & Heino, Perttu			
Title Designing a safe process plant Tools created during STOPHAZ-project			
Abstract <p>The objective of the STOPHAZ project was to promote the safer and more efficient design of process plants through the use of a new generation of quality assurance tools. These tools include an intelligent safe design hyperbook ELDER (Engineering Line Diagram helpER) and HAZID (HAZard IDentification tool).</p> <p>ELDER is a hyperbook, which contains advice on SHE considerations and related issues. The advice in each chapter is organised under predefined standard headings. These headings (Control and Instrumentation, Operational Considerations, Legislation etc.) aim to guarantee that the advice covers all the considerations that are necessary for safer and more efficient design.</p> <p>Each piece of advice on a specific topic is called an advice note. These advice notes contain text, diagrams, simple calculation tools, and links to other advice notes. In order to make the system context sensitive, invisible definitions are associated with each advice note. These invisible definitions include query keywords, and the validity range of the advice in terms of topics and equipment subtypes.</p> <p>HAZID is an automated Hazard and Operability Study (HAZOP) tool based on a signed directed graph (SDG) representation of process equipment faults and their propagation. It accepts the description of the process as input and generates a HAZOP study report as output. This report contains the cause-consequence-chains associated with the identified hazards.</p> <p>A typical user of the tool is a design engineer who wishes to evaluate the plant design before commencing with a HAZOP study. Alternatively, it could be used at earlier stages of the design process, before detailed process and instrumentation diagrams (P&ID) are available, to screen for possible problems when the cost of design changes is not too high.</p> <p>HAZID uses process-independent unit models to create a model of fault propagation based on the given process-specific plant description. This SDG model is then examined by applying the HAZOP algorithm. Information on process conditions and the properties of the processed fluids is used for improving the performance of the knowledge-based hazard identification.</p>			
Keywords plant design, quality assurance tools, hazard and operability studies, safety analysis, intelligent safe design kyberbook			
Activity unit VTT Automation, Risk Management, Tekniikankatu 1, P.O.Box 1306, FIN-33101 TAMPERE, Finland			
ISBN 951-38-5697-6 (soft back ed.) 951-38-5698-4 (URL: http://www.inf.vtt.fi/pdf/)		Project number A9SU00585	
Date October 2000	Language Finnish, Engl. abstr.	Pages 44 p.	Price A
Name of project STOPHAZ		Commissioned by Technology Development Centre of Finland (Tekes)	
Series title and ISSN VTT Tiedotteita – Meddelanden – Research Notes 1235-0605 (soft back ed.) 1455-0865 (URL: http://www.inf.vtt.fi/pdf/)		Sold by VTT Information Service P.O.Box 2000, FIN-02044 VTT, Finland Phone internat. +358 9 456 4404 Fax +358 9 456 4374	