UDK 66.01.004.4

Študije nevarnosti v procesni industriji

Hazard Analysis in Process Industry

ĐORĐE VOJNOVIĆ — MITJA KOŽUH — JANEZ SUŠNIK

0. UVOD

Metode za vrednotenje tveganja in analizo nevarnosti postajajo v svetu zelo močno orodje za nadzorovanje varnosti v procesni industriji (kemijska, petrokemijska, naftna in sorodna industrija), ki uporablja škodljive in nevarne snovi. Metodološka zamisel varnostnih študij v procesni industriji je zelo podobna varnostnim študijam v jedrski tehniki, kjer se uporabljajo že 15 let. (Prva znana verjetnostna varnostna študija je »Reactor Safety Study« iz leta 1975). Kljub podobnostim obstajajo razlike, ki v glavnem izhajajo iz tega, da je proces v jedrski elektrarni en sam, medtem ko v procesni industriji teče več neodvisnih procesov, pri katerih osnovne snovi doživljajo fizikalne in kemične spremembe. Razlike nastajajo tudi zaradi različnih namenov in ciljev varnostnih študij. Metode se prenašajo s področja jedrske tehnike in prilagajajo posebnostim procesne industrije.

Ocenjevanje tveganja je obsežna naloga. Izvajamo jo po določenem postopku, ki ga razdelimo na več faz. Namen tega članka je predstaviti 1. fazo verjetnostne varnostne analize v procesni industriji — razpoznavanje nevarnosti in določanje izhodišč za logično modeliranje. Metodološke rešitve izhajajo deloma iz tujih izkušenj, deloma iz naših, ki smo jih pridobili pri verjetnostnih varnostnih študijah za jedrsko elektrarno Krško in posebej pri varnostni študiji sinteze smol v Colorju iz Medvod. V članku bomo definirali zamisel verjetostnih varnostnih študij, razsvetlili njihovo uporabnost in pojasnili varnostne kriterije, ki temeljijo na tej zamisli. V nadaljevanju se bomo zadržali pri metodi razpoznavanja nevarnosti in priprave izhodiščnih točk za logično modeliranje procesnega obrata. Metodološki prijem bomo pojasnili s primerom.

1. METODOLOŠKA ZAMISEL VERJETNOSTNE VARNOSTNE ŠTUDIJE

Vpliv industrije na okolje in ljudi je pomemben pri izbiri tehnologije v določenem primeru. Najbolj uveljavljena zvrst za oceno tega vpliva v svetu je tveganje. V zgodnjih časih je bilo tveganje čustvena opredelitev, ki je nastajala z oceno trenutnega stanja iz izkušenj. Brez matematičnega zapisa lahko tveganje opredelimo kot razmerje med nevarnostjo ali mogočo nevarnostjo in zaščito.

0. INTRODUCTION

Methods for risk evaluation and hazard analysis are becoming a very powerful tool for risk management in the process industry (chemical, petrochemical, oil and others), which uses dangerous and poisonous chemicals. The methodological concept of safety studies in the process industry is similar to probabilistic safety studies for nuclear power plants, where these studies have been intensively used for 15 years (the first known probabilistic safety study was »Reactor Safety Study« in 1975). In spite of the similarity there are differences which are caused by the fact that in nuclear power plants there is only one process while in the process industry there are several independent processes in which the basic substances suffer physical and chemical changes. Differences arise also because of different purposes and goals of safety studies. Methods are transferred from the nuclear field and are being adapted to the specific needs of the process industry.

Risk assessment is a huge task. It is performed according to a defined procedure, which is divided into several phases. The goal of this article is to show the first phase of safety analysis in the process industry - hazard identification and definition of starting points for logical modeling. Methodological solutions are based partly on experiences abroad and partly on our own, gained during probabilistic safety analyses for the Krško power plant and specially during a safety study for resin synthesis of Color Medvode. In this article definition of the concept of probabilistic safety analyses will be given and its applicability and safety criteria, based on this concept, will be explained. Attention will be concentrated on hazard identification methods and start point definition for logical modeling of process line. The methodological approach will be explained through an example.

1. METHODOLOGICAL CONCEPT OF PROBABILISTIC SAFETY STUDY

The impact of industry on the environment and people is important for the selection of technology in certain surroundings. The most commonly used term for estimating this impact is risk. In the past risk was an emotional category formed by judgement of the situation based on experience. Without the use of mathematical formulation we can define risk as the relation between hazard and protection. We are able to protect ourselves

Pred še tako veliko nevarnostjo se lahko zavarujemo tako, da tveganje zmanjšamo. Z razvojem verjetnostnih analiz tveganja se je izoblikoval izračun tveganja, in sicer kot seštevek verjetnosti pojava nezgode in njenih posledic, oziroma:

against a hazard in such a manner that the risk is low. With the development of Probabilistic Risk Analysis, calculation of risk was formalized in the form of a product between probability for an accident and its consequences, or:

$$Rc(x, y) = \sum_{a} Fa \times p(e/a) \times p(c/e) \quad (1)$$

kjer pomenijo: $Rc(x, y)$ — tveganje na lokaciji (x, y), Fa — ocenjeno pričakovano pogostost nezgode (a), $p(e/a)$ — pogojno verjetnost, da bo nezgoda (a) povzročila fizične učinke (e) na lokaciji (x, y), $p(c/e)$ pogojno verjetnost, da bodo fizični učinki (e) povzročili ljudem določene posledice (c).

Postopek ocenjevanja tveganja na splošno razdelimo v naslednje faze:

— razpoznavanje nevarnosti (kaj je morda narobe);

— ocena pogostosti (verjetnost pojava nezgode, verjetnost nezgodnega scenarija),

— izračun in ocena posledic (poškodbe ljudi, okolja, dobrin),

— ocena tveganja.

Razpoznavanje nevarnosti v procesni industriji pomeni sistematično opredelitev nevarnih dogodkov s poudarkom vzroka dogodka (odpoved, napaka) in neposredne posledice.

Metode, s katerimi analiziramo nevarnost, lahko razvrstimo v tri kategorije:

a) *Primerjalne metode*, kakor so kontrolni spiski procesov/sistemov, varnostni pregledi, pripravljalne analize nevarnosti itd.

b) *Temeljne metode*, kakršne so analiza obratovalne nevarnosti, analiza kaj-če, analiza načinov in posledic odpovedi.

c) *Logično-diagramske metode*, kakor so analiza z drevesi okvar, analiza z drevesi dogodkov, analiza zanesljivosti človeka itn.

Izbira metode je odvisna od namena in ravni nadrobnosti študije.

2. UPORABA VARNOSTNIH ŠTUDIJ

Študije za oceno tveganja kot orodja za nadzorovanje varnosti v procesni industriji naglo naraščajo, zlasti po razglasitvi t.im. smernic Post-Seveso (1982) in po nesrečah, ki so se zgodile v zadnjem desetletju (Bhopal). Obsežnost študij v državah Evropske skupnosti (EC) je različna, saj zajema vse od posebnega nadzora 178 kemičnih snovi ali kemičnih skupin do ocene ogroženosti celotnih regij in določanja krivulj z enako velikim tveganjem.

Sedanje študije tveganja so uporabne v procesni industriji, usmerjene pa so v glavnem v varnostne ocene projektov in v varnostne ocene obratovanja. Uporabniki navajajo, da so jim v veliko

Where: $Rc(x, y)$ — risk on location (x, y), Fa — estimated expected frequency of accident (a), $p(e/a)$ — conditional probability that the accident (a) will cause physical effects (e) on location (x, y), $p(c/e)$ — conditional probability that physical effects (e) will cause certain consequences (c) to the people.

The methodology of risk estimation is a huge and complicated task carried out for assessing and reducing risk from potentially dangerous technologies. The procedure for risk assessment can be generally divided into following phases:

— hazard identification (What can go wrong?)

— frequency estimation (accident probability, accident sequence probability)

— estimation and calculation of consequences (injuries to people, environmental impacts, damage of goods)

— risk assessment

Hazard identification in the process industry represents the systematical identification of dangerous events with emphasis on event cause (failure, mistake) and direct consequence.

Methods used for hazard analysis can be put in three categories:

a) *Comparative methods*, such as check-lists of processes/systems, Safety Audits, Preliminary Safety Analyses, etc.

b) *Fundamental methods*, such as HAZOP - Hazard and Operability Study, What if analysis, FMEA - Failure Mode and Effect Analysis,

c) *Logic—diagram methods*, such as Fault Tree Analysis, Event Tree Analysis, Human Factor Analysis etc.

Method selection depends on the purpose and resolution of the study.

2. USE OF SAFETY STUDIES

Risk assessment as a tool for risk management in process industry is becoming quite popular, especially following the so called Post—Seveso Directive (1982) and catastrophes in the last decade (Bhopal). The extent of the studies in EC countries differs from special control over 178 chemicals or chemical groups to risk assessment of whole areas and determining the isorisk curves.

Present risk assessment in the process industry is mainly oriented towards safety evaluation of projects and safety evaluation of operations. They are of great help to the users for efficient investigation into safety or during selection between different alternatives. This approach to the risk management and environmental protection

pomoč za učinkovito vlaganje v varnost oziroma pri iskanju ustrezne rešitve med različnimi možnostmi. Takšno stališče o nadzorovanju varnosti in odnosu do okolja dopušča upravnim organom in tudi javnosti, da ima večje zaupanje v ocenjeno varnost, ker so vsi varnostni kazalci pojasnjeni.

3. SPREJEMLJIVOST TVEGANJA IN KRITERIJEV

Vprašanji, kolikšna stopnja tveganja je sprejemljiva in kdo določa sprejemljivost, še vedno nista rešeni. Razprava je tesno povezana z zaznavanjem tveganja, ki se kaže v različni pripravljenosti za tveganje iz različnih virov in za sprejem različnih vrst tveganj med različnimi skupinami posameznikov.

Ljudje so v življenju izpostavljeni tveganju zaradi različnih vzrokov. Nekaterim tveganjem se lahko izognejo, druge pa trpijo zaradi koristi, ki se jim običajno nočejo odreči (sodelovanje v prometu itn.). Skupno ali celotno tveganje posameznika ali skupine je definirano kot vsota vseh tveganj, katerim so izpostavljeni.

Osnova ocenjevanja in nadzorovanja je domneva, da je neko stopnjo tveganja mogoče dopustiti. Brez tega so odločanje in oblikovanje strategije nadzorovanja tveganja, ocenjevanje uspešnosti nadzorovanja tveganja itn. brez pomena.

Merila za sprejemljivost ali odločanje v takih primerih so: velikost tveganja in doseženo zmanjšanje, cena zmanjševanja tveganja, kar zadeva družbo, gospodarstvo in okolje ter učinkovitost nadzornih meril. Meja med sprejemljivostjo in nesprejemljivostjo tveganja ni enopomenska, ampak je predvideno vmesno področje, kjer priporočajo posege za zmanjševanje tveganja. Poleg meril na ravni tveganja se hkrati postavljajo tudi merila ali zahteve na nižjih ravneh, npr.: verjetnost prevladujočih nezgodnih scenarijev ali zanesljivost izvajanja nekaterih funkcij, bistvenih za varnost.

Ker zamisel tveganja prinese povezavo med t.im. varnostnimi kazalci (odpovedi, nezanesljiva oprema, napake v postopkih, napačen odziv operaterja, učinkovitost in ustreznost vzdrževanja itn.) in tveganjem oziroma varnostnimi kriteriji, imamo možnost ocenjevanja obratovalnih izkušenj in nenormalnih dogodkov z vidika kriterijev, ki jih je postavila družba. Prav tako se lahko ugotovi težnja k spremembam varnosti oziroma obratovalnega tveganja.

4. ŠTUDIJA HAZOP

Razpoznavanje nevarnosti je zelo pomembna faza celotne študije tveganja, ker se lahko v naslednjih fazah obravnavajo samo ugotovljene nevarnosti ter učinkovitost zaščite proti njim. To lahko izvedemo z različnimi metodami, od katerih smo izbrali HAZOP.

allows the authority and the public great confidence in the estimated risk, because all safety indicators are explicit.

3. ACCEPTABLE RISK AND CRITERIA

The question of which risk level is acceptable and who is defining acceptability is still unanswered. Discussion is inherently connected with risk perception which is manifested through different preparation for tolerating risk from different sources and different preparation for different risk acceptance among different groups of individuals.

During their lifetime people are exposed to risks from different sources. They can avoid some of risks and tolerate others because of the benefits which they do not want to lose (car driving, traveling by plane etc.). The total risk of an individual or of the group is defined as the sum of all risks to which they are exposed.

The basis for risk assessment and risk management comes from the concept that certain risk levels can be tolerated. Without such a concept, categories like decision making and formulation of risk management strategies, evaluating success of risk management etc. are without any sense.

Acceptance and decision criteria which are set in these cases are: the level and achieved reduction of risk, the price of risk reduction expressed in social, economic and environmental terms and the effectiveness of management measures. What is acceptable or not is not separated by a uniform curve but there is a region in which the risk level should be reduced. Beside the criteria on the risk level at the same time, limits are put on the dominant sequence probability or on the reliability of certain essential safety functions.

The risk concept brings the connection between so called safety indicators (failures, unreliable equipment, errors within procedures, operator's wrong response effectiveness and the appropriateness of maintenance etc.) and risk or safety criteria, so we have the opportunity to evaluate operating experience and abnormal events from the point of the criteria set by the society. The trend of safety changes or operational risk can also be estimated.

4. HAZOP STUDY

Hazard identification represents a very important phase of complete risk assessment, as only identified hazards and protection against them can be analyzed later on. This can be carried out through different methods out of which we have chosen HAZOP (Hazard and Operability Study).

4.1 Kaj je HAZOP?

HAZOP je okrajšava, vpeljana za angleški zapis *Hazard and Operability Study*, kar lahko prevedemo kot *raziskavo, preučitev nevarnosti in razpoznavanje problemov, ki spremljajo obratovanje*. Pri tem preučimo vse mogoče načine, ki lahko pripeljejo do nevarnih stanj, do problemov obratovanja in ugotavljamo načine in ukrepe, kako bi zmanjšali verjetnost za pojav takih neugodnih neželenih stanj oziroma dogodkov. Dela se lotimo sistematično. Pri analizi mogočih odmikov od pričakovanega stanja uporabljamo značilne vodilne besede: *ni, več, manj, del(no)* itn.

4.2 Cilj izdelave HAZOP

Metodologijo HAZOP uporabljamo, kadar želimo poiskati varnostne in operativne probleme ob definiranih nenormalnih odmikih parametrov procesa. Tehnika HAZOP omogoča in spodbuja našo domišljijo, da svobodno poiščemo vse mogoče načine in poti, po katerih se lahko pojavijo nevarnosti ali operativni problemi. S tem zmanjšamo možnost, da kaj pomembnega izpustimo. S posebej pripravljenimi preglednicami sistematično zajamemo vsa mogoča neujemanja v procesu.

Če so stroški za odstranitev problemov oziroma obvladovanje preveliki in ne moremo najti cenejših rešitev, potem lahko sklenemo, seveda če želimo in če tveganje ni preveliko, da bomo s problemi živeli. Tudi tako ravnanje je lahko upravičeno. Vsekakor pa moramo probleme razpoznati, četudi nam povzročajo dodatno delo, nevšečnosti in stroške, da se lahko pripravimo nanje.

4.3 Postopek izdelave HAZOP

HAZOP izdela povezana skupina ljudi, rečemo jim lahko kar ekipa. Pri novem projektu običajno sodelujejo:

- projektant (navadno strojni inženir),
- tehnolog (navadno inženir kemije),
- vodja bodočega obrata (navadno inž. kemije),
- projektant instrumentacije (inženir ustrezne stroke),
- neodvisni moderator (izkušen pri uporabi tehnike HAZOP).

Moderatorjeva naloga je, da se ekipa drži postopkov, ki so priporočeni za izdelavo HAZOP. Primerno je, da podrobnostim posveča kar največjo pozornost.

Posamezni člani ekipe imajo isti cilj: varno, za obratovanje zmožno postrojenje.

Če gre za HAZOP že znanega postrojenja, bo sodelujoča skupina sestavljena nekoliko drugače.

4.1 What is a HAZOP?

Hazop is an abbreviation introduced for Hazard and Operability Study. In this study we assess all of the possible ways leading to dangerous situations, to operational problems and finding measures to reduce probability for undesired states and events occurrence. Approach or procedure is systematic. During analysis of possible deviations we use certain guide words such as: *none, more of, less of, part of, more than, other than* etc.

4.2 Why carry out a HAZOP?

We use HAZOP methodology when we want to identify safety and operational problems because of abnormal process parameter deviations. This technique enables us to stimulate our imagination in order to find out, without limitations, brainstormingly all possible ways and paths through which hazard and operational problems can occur. Thus we minimize the possibility of omission of anything important. With a specially designed table format we, in our analysis, assess all possible process deviations in a systematic way.

If the expenses for solving the problems or their mitigation are too high and we cannot find cheaper solutions, we can decide, if we want to, and if the risk is not too high, to live with them. This kind of attitude is possible. Nevertheless the problems should be identified, even though they give us extra work to do, annoyances and expenses. There is no exuse for not recognizing them. If we do not make an effort to identify them, we cannot prepare ourselves for them with special administrative measures nor with special emergency procedures.

4.3 HAZOP Procedure

HAZOP was made by a specially selected group of people. We can call them - the team. When a new project is being analyzed, the team consists of:

- project or design engineer (usually mechanical engineer),
- process engineer (usually cemical engineer),
- commissioning manager (usually chemical engineer),
- instrument design engineer (engineer of appropriate field),
- independent chairman (expert in the HAZOP technique).

The chairman's job is to ensure that the team follows procedure. The members of the team have the same objective: safe and operable plant.

VODILNA BESEDA	ODSTOPANJA	Št.	MOGOČI VZROKI	POKAZATELJ ODSTOPANJA	POSLEDICE	SEDANJA ZAŠČITNA DEJANJA		DODATNA POTREBNA DEJANJA	OPOMBA	ZD / GD / P	ZAČETNI DOGODEK / GLAVNI DOGODEK / POSLEDICA
						SAMO-DEJNA	ROČNA				
preveč	temperatura termalnega olja: -dovod olja v sintezo, -kroženje v grelni cevi	1.	odpoved regulacije temp. v kotlovnici; napaka kurjača; napaka v sistemu računalniškega vodenja; odpoved ventilov L in O v odprti poziciji (potenc. vzrok); odpoved omejilnika maks. temperature procesa; izguba napajanja ventilov z zrakom ?; ni dotoka hladilne vode ventil J zaprt (napačen položaj odpoved)	v kontrolni sobi: - temperatura (računalnik in komandna plošča) - položaj omenjenih ventilov	razpad vodenja procesa; poslabšanje kakovosti izdelka (motna barva izdelka, ...); možnost da pride do žeiliranja, itd.	alarm	akcija operaterja	izdelava navodil za ukrepe operaterja	regulacijska zanka vključuje: -temper. tipala - naprave za prenos in obdelavo signalov -sklop programske in aparaturne opreme (procesni računalnik)	ZD GD P	1*, 7* 1* 3*, 1*, 2*
preveč	temperatura hladilne vode	2.	hladilni stolpi v okvari; izpad obtočne črpalke; ni preklopa na vodovodno omrežje.	temp.hladilne vode; pretok hladilne vode; izpad hladilnih stolpov	razpad vodenja procesa; alarm	enako kakor (1)	enako kakor (1)			ZD GD P	6* 1* 3*, 1*, 2*
premalo	temperatura termalnega olja	3.	regulacija temperature v kotlovnici; regulacija temperature gretja reaktorja; okvara komponent v pretočnih linijah	procesne spremenljivke na računalniku	počasnejši proces	alarm ?	prehod na ročno vodenje procesa	usposabljanje za ročno vodenje procesa		ZD GD P	1*, 7* 1* 3*, 1*, 2*
ni	pretok termalnega olja: -dovod v sintezo:	4.	-izpad kotlovnice -pokanje cevovoda -zlom kompenzatorjev -zamašitev c; ventil O je neprehoden (odpoved zraka, napaka regulacije):	pretok in položaj zapornih organov (komandna soba)	zaustavitev proizvodnje; razlitje termalnega olja; možnost vnetja t. o.		delna zaščita; ročno se lahko odpre, če reg. odpove			ZD	1*, 2*, 3*
	-obtočna zanka:		-zlom cevovoda -pokanje spirale reaktorja -pokanje cevi v t. menjalniku K -neprehodnost: =zamašitev cevi in filtrov =ustavitev črpalke (odpoved el. napaj.) =neprehodnost ventila		požar; možnost požara; eksplozija; vdor termalnegal olja v hladilno vodo; zaustavitev procesa; izločanje šarže	ustavitev dotoka olja iz kotlovnice (1. faza alarma); izpraznitev sistema (2. faza alarma)		zmanjšati moč termošokov v topl. menjalniku: vzdrževanje potopljenega menjalnika	ali se prej lahko izprazni sistem ?	GD P	1*, 2*, 3* 4*, 5*, 1*, 2*
ni	pretok hladilne vode: hlajenje reaktorja (hladilnik termalnega olja)	5.	zamašitev; zaprt ventil; izguba hladilne vode (dovod)	temperature hladilne vode napačne	izguba kontrole reakcije (ni hlajenja); temperatura narašča; slaba kakovost; termični šok	izpust v razredčevalnik		predvideti programirano hlajenje za ponovno vzpostavitev hlajenja; meritev temperatur lokalno na komandni plošči		ZD GD P	1*, 7* 1* 3*, 1*, 2*
ni	dovod hladilne vode v obrat	6.	izpad črpalk hladilne vode; počena cev; človeška napaka; -ni preklopa na vodovod -zaprt ročni ventil -ustavljena črpalka	pretok; temperatura; alarm	dolgotrajno ustavljanje procesa	alarm	korekcijske akcije	usposobljenost za tak primer; načrtovanje zalog rezervnih delov		ZD GD P	6* 1* 3*, 1*, 2*
delno	olje v izolaciji reaktorja: - termalno olje, - hidravlično olje	7.	puščanje grelnih cevi reaktorja (mikro razpoke zaradi termalnih obremenitev in termičnih šokov); puščanje hidravlične instalacije mešalnika v reaktorju	ga ni, ali pa je nezanesljiv (vonj gorečega olja)	možnost požara	alarm; izpraznitev termalnega olja	po navodilih za primer požara	instaliranje sistema za sporočanje puščanja olja v izolacijo (po načelu spremembe el. upora v izolaciji), ali boljše rešitve	treba je poiskati načine rešitve tega problema drugje v svetu	ZD GD P	3* 1*, 2* 5*
delno	hladilna voda: - fosfati	8.	ob dodajanju polifosfatov	slab prenos toplote v menjalnikih	poslabšano hlajenje		redni pregledi toplotne opreme			ZD GD P	- - -
več ko	hladilna voda: -prevelika količina kisika	9.	kisik je zajet iz zraka zaradi odprtosti hladilnega sistema	ni direktnega pokazatelja	korozija cevi		redni pregledi toplotne opreme			ZD GD P	- - -

* *Definirano v tekstu*

Sl. 1. *Primer uporabe HAZOP preglednic v varnostni študiji sinteze smol.*

LEADING WORD	DEVIATION	No.	POSSIBLE CAUSES	INDICATION OF DEVIATION	CONSEQUENCES	EXISTENT PROTECTIVE MEASURES		ADDITIONAL NECESSARY MEASURES	COMMENT	IE / TE / C	INITIATING EVENT / TOP EVENT / CONSEQUENCES
						AUTO-MATIC	MANUAL				
more of	thermal oil temperature: -oil flow to synthesis -circulation in reactor spiral pipeheater	1.	heating station temperature control failure; stoker failure; computerized control system failure; valves L and O fail to open (potential cause); maximal process temperature restrictor failure; loss of air supply to valves; no flow of cooling water; valve J closed (wrong position - failure)	indication is in the control room: -temperature indication (computer and control table), -valves position indication	the process control collapse; worse product quality (unclean product colour, ...); possible congelation	alarm	operater action	instructions elaboration for operaters actions	control loop includes: -temper. sensors - signal transport and treatment devices -software and hardware (process computer)	IE TE C	1*, 7* 1* 3*, 1*, 2*
more of	cooling water temperature	2.	cooling tower failure; circulation pump failure; no switch on water supply	cooling water temperature and flow indication; cooling tower failure	the process control collapse; alarm	as (1)	as (1)			IE TE C	6* 1* 3*, 1*, 2*
less	thermal oil temperature	3.	heating station temperature control; reactor heating temperature control; flow loops components failure	computer indication of process variables	process is slower	alarm ?	switch to manual mode of process control	training for manual control of process		IE TE C	1*, 7* 1* 3*, 1*, 2*
none	thermal oil flow: -inflow to synthesis -recirculation loop	4.	heating station failure: -pipe line break -expansion break -pipe line plugging valve O impassable (air failure, control failure): -pipe line break -reactor spiral pipes break -heat exchanger tube break (K) -impassableness: =pipes and filters plugging =pump fails to run (el. supply failure) =valve impassable	flow indication; valve position indication	production interruption; thermal oil spilling; possible thermal oil ignition; fire; chances of fire; explosion; thermal oil irrupts into cooling water; process interruption waste of production	the heat station and oil pipeline isolation from resin synthesis (alarm 1st stage); system drainage (alarm 2nd stage)	partial protection; isolation by operator action in the case of automatic protection failure	reduction of thermal shocks intensity in heat exchanger: to keep the chiller thermal oil filled fully	is it possible to drain the system first ?	IE TE C	1*, 2*, 3* 1*, 2*, 3* 4*, 5*, 1*, 2*
none	cooling water flow: reactor cooling (thermal oil chiller)	5.	plugging; valve closed; loss of cooling water	cooling water temperatures are incorrect	loss of reaction control (no cooling); temperature is rising up; low quality; thermal shocks	release into dilution vessel		provide programed cooling for reestablish cooling temperature measuring: -on control table -local		IE TE C	1*, 7* 1* 3*, 1*, 2*
none	cooling water inflow to the plant	6.	cooling water pump failure; pipe break; human error: -no switch on water supply -manual valve closed -pump stopped	flow indication; temperature indication; alarm	slow process shut down	alarm	corrective actions	adequate trained personnel reserve parts store planning		IE TE C	6* 1* 3*, 1*, 2*
part of	presence of oil in reactor isolation: - thermal oil, - hydraulical oil	7.	reactor heater pipes cracks leakage (micro cracks because of thermal loads and thermal shocks); reactor mixer oil installation leakage	doesn't existing or unreliable (smell of burning oil)	fire possibility	alarm; thermal oil drainage	according to emergency procedures in case of fire	installation of system for indicating the oil release to thermal insulation (by changing of el. resistance in insulation)	we should find the ways of solving this problem by support of wider experience	IE TE C	3* 1*, 2* 5*
part of	cooling water: - phosphates	8.	adding of polyphosphates	poor heat conduct in exchangers	poor cooling	-	regular testing of thermal equipment			IE TE C	- - -
more than	cooling water: - too much oxygen	9.	oxygen is taken from the air because the cooling system is open	no direct indication	pipe corosion	-	regular testing of thermal equipment			IE TE C	- - -

* *Defined in text*

Fig. 1. *The example of HAZOP form use in resin synthesis hazard analysis.*

POSLEDICE / VZROK	IZPAD KOTLOVNICE, ODPOVED REGULACIJE, NAPAKA KURIŠČA	POKANJE CEVOVODA TERMALNEGA OLJA ZLOM KOMPENZATORJEV	ZAMAŠTEV CEVI TERMALNEGA OLJA	NEPREHODNOST, ODPOVED, NAPAČEN POLOŽAJ ZAPORNIH ORGANOV	NAPAČEN POLOŽAJ VENTILOV (PROCESNI RAČUNALNIK)	POKANJE SPIRALE V REAKTORJU	POKANJE CEVI V HLADILNIKU TERMALNEGA OLJA	ODPOVED ČRPALKE TERMALNEGA OLJA	ODPOVED ELEKTRIČNEGA NAPAJANJA	IZGUBA NAPAJANJA Z ZRAKOM	NI PRITOKA HLADILNE VODE; OKVARA HLADILNIH STOLPOV ALI VODNE ČRPALKE NI PRESKLOPA NA VODOVODNO OMREŽJE	MIKRO RAZPOKE GRELNIH CEVI (TERMOŠOKI TERMALNE CIKLIČNE OBREMENITVE)	SLABA KAKOVOST TERMALNEGA OLJA	ZAŠČITA	POKAZATELJ
USTAVITEV PROCESA	M	VH	H	H	M	VH	VH	VH	VH	M	M	VH	VL		
IZMET POLNITVE	M	M	M	L	L	H	H	H	M	H	M	H	VL	-IZDELANI POSTOPKI ZA REŠITEV POLNITVE -VNAPREJ PRIPRAVLJENE SUROVINE IN OPREMA	VZORČENJE
POSLABŠANJE KVALITETE	VH	VH	VH	H	M	VH	VH	H	VH	H	VH	M	VL	-IZDELANI POSTOPKI ZA REŠITEV POLNITVE -VNAPREJ PRIPRAVLJENE SUROVINE IN OPREMA	VZORČENJE
RAZPAD VODENJA ALI PODALŠANJE PROCESA	VH	VH	VH	VH	VH	VH	VH	VH	VH	VH	VH	M	L	-IZDELANI POSTOPKI ZA REŠITEV POLNITVE -VNAPREJ PRIPRAVLJENE SUROVINE IN OPREMA	VZORČENJE; REZULTATI ANALIZE PROCESA
RAZLITJE TERMALNEGA OLJA		VH	VL	VL		VH	H	VL				M		HITRA IZPRAZNITEV KINETE; ZAPIRANJE TEHNOLOŠKE KANALIZACIJE; SISTEM ZA INDIKACIJO PRISOTNOSTI OLJA V IZOLACIJI	ALARM 1. IN 2. STOPNJE ZARADI PADCA TLAKA TERMALNEGA OLJA
VNETJE TERMALNEGA OLJA, POŽAR, EKSPLOZIJA		H				VH	VH				L	VH	L	REDNA KONTROLA TOČKE VNETLJIVOSTI; IZDELAVA POSTOPKOV V SILI; INSTALIRANJE AVT. SIS. ZA GAŠENJE IN REDNO TESTIRANJE	ALARM 1. IN 2. STOPNJE ZARADI PADCA TLAKA TERMALNEGA OLJA
VDOR TERMALNEGA OLJA V HLADILNO VODO		VL				M	VH				M			ZAGOTOVITEV NENEHNEGA PRETOKA VODE SKOZI HLADILNIK; SIGNAL OB IZPADU PRETOKA	ALARM 1. IN 2. STOPNJE ZARADI PADCA TLAKA TERMALNEGA OLJA
ZAŠČITA	PREVENTIVNO VZDRŽEVANJE; PROGRAMI QA/QC USTREZANJE STANDARDOM IN KRITERIJEM ŠOLANJE	KVALIFIKACIJA OPREME, PREVENTIVNI PREGLED IN VZDRŽEVANJE, ZAGOTOVITEV ENAKOMERNEGA TLAKA, ZAMENJAVA KOMPENZAT; NA OSNOVI KRIT. DOBE TRAJANJA	REDNO VZORČENJE OLJA, UČINKOVITI FILTRI	PREVENTIVNO VZDRŽEVANJE	TESTIRANJE PROGRAMOV NADZOR OPERATERJA	DVOJNI PLAŠČ KVALIFIKACIJA OPREME, REDNI PREGLEDI	NEPRETRGANO POTOPLJEN MENJALNIK ZAGOTOVITEV USTREZNEGA MATERIALA CEVI HLADILNIKA	REZERVNA ČRPALKA PREVENTIVNI PREGLEDI	NEODVISNI VIR ELEKTRIČNE ENERGIJE	REZERVNI VIR; PREVENTIVNI PREGLED IN VZDRŽEVANJE	REZERVNI VIR; PREVENTIVNI PREGLED IN VZDRŽEVANJE, ZAGOTOVITEV USTREZNE KAKOVOSTI VODE, ZAPRT SISTEM	REDNI PREGLEDI KVALIFIKACIJA OPREME	REDNI NADZOR IN ZAMENJAVA KAKOVOSTNO OLJE		
POKAZATELJ	SPREMLJANJE PODATKOV O ODPOVEDIH IN NENORMALNIH DOGODKIH	SPREMLJANJE PODATKOV O ODPOVEDIH IN NENORMALNIH DOGODKIH SPREMLJANJE DEGRADACIJE	MERILNIK PRETOKA ALARM ZARADI NIZKEGA PRETOKA	MERILNIK PRETOKA ALARM ZARADI NIZKEGA PRETOKA	POVRATNA INFORMACIJA O POLOŽAJU VENTILA		POKAZATELJ PRETOKA HL. VODE ALARM ZARADI NIZKEGA PRETOKA	TEMPERATURNA RAZLIKA		ALARM ZARADI NIZKEGA TLAKA	ALARM ZARADI NIZKEGA PRETOKA	ODKRIVANJE MIKRO RAZPOK S PENETRANTI			

Sl. 2. *Primer matrike vzrokov in posledic.*

CAUSE / CONSEQUENCES	HEATING PLANT FAILURE, CONTROL FAILURE, STOKER ERROR	THERMAL OIL PIPE BREAKS, EXPANSION JOINTS BREAK	THERMAL OIL PIPE PLUGGING	IMPASSABILITY, FAILURE OR WRONG POSITION OF VALVES	VALVE IN WRONG POSITION BECAUSE OF PROCESS COMPUTER FAILURE	REACTOR SPIRAL HEATER BREAK	CHILLER THERMAL OIL PIPE BREAK	THERMAL OIL PUMP FAILURE	LOSS OF ELECTRICAL POWER SUPPLY	LOSS OF AIR SUPPLY	NO COOLING WATER SUPPLY; COOLING TOWER OR WATER PUMP FAILURE; NO SWITCH ON WATER WORK	HEATER PIPES MIKRO CRACKS (THERMAL SHOCKS, THERMAL CYCLIC LOAD)	QUALITY DEGRADATION OF THERMAL OIL	PROTECTION MEASURES	INDICATION
PROCESS SHUTDOWN	M	VH	H	H	M	VH	VH	VH	VH	M	M	VH	VL		
PRODUCTION LOSS	M	M	M	L	L	H	H	H	M	H	M	H	VL	-ELABORATION OF PROCEDURES FOR REACTOR FILLING SAVING -ADDITIONAL RAW MATERIAL AND EQUIPMENT PREPARING IN ADVANCE	PRODUCTION SAMPLING
LOW PRODUCTION QUALITY	VH	VH	VH	H	M	VH	VH	H	VH	H	VH	M	VL	-ELABORATION OF PROCEDURES FOR REACTOR FILLING SAVING -ADDITIONAL RAW MATERIAL AND EQUIPMENT PREPARING IN ADVANCE	PRODUCTION SAMPLING
COLLAPSE OF PROCESS CONTROL OR PROCESS PROLONGATION	VH	VH	VH	VH	VH	VH	VH	VH	VH	VH	VH	M	L	-ELABORATION OF PROCEDURES FOR REACTOR FILLING SAVING -ADDITIONAL RAW MATERIAL AND EQUIPMENT PREPARING IN ADVANCE	PRODUCTION SAMPLING PROCESS ANALYSIS RESULTS
THERMAL OIL SPILLING		VH	VL	VL		VH	H	VL				M		FAST CANAL DRAINAGE; CLOSING TECHNOLOGICAL CANALIZATION; INDICATION OIL PRESENCE ISOLATION SYSTEM	ALARM (IST IN 2ND STAGE) ON LOW PRESSURE THERMAL OIL
THERMAL OIL IGNITION, EXPLOSION, FIRE		H				VH	VH				L	VH	L	REGULARY TESTING OF INFLAMMABILITY POINT; ELABORATE EMERGENCY PROCEDURES AUTOMATIC SYSTEM INSTALATION FOR ESTINGUISHING AND REGULARY TESTING	ALARM (IST IN 2ND STAGE) ON LOW PRESSURE THERMAL OIL
THERMAL OIL IRRUPTION IN COOLING WATER		VL				M	VH				M			ASSURANCE CONTINIOUS WATER FLOW THROUGH CHILLER; SIGNAL AT LOSS OF FLOW	ALARM (IST IN 2ND STAGE) ON LOW PRESSURE THERMAL OIL
PROTECTION	-MAINTENANCE PREVENTION; QA/QC PROGRAMS -TO MEET THE NEEDS OF STANDARDS AND CRITERIONS -EDUCATION	EQUIPMENT QUALIFICATION, MAIN. PREV. AND TESTING, ASSURE PRESSURE EQUIVALENCE, EXCHANGE OF EXSPANSION JOINTS WITH REGARD ON CRITERIONS OF LIFE PERIOD AND DEG	REGULARILY OIL SAMPLING, EFFECTIVE FILTERS	PREVENTIVE MAINTENANCE	PROGRAMS TESTING OPERATER CHECKING	-VESSEL WITH DOUBLE WALL -EQUIPMENT QUALIFICATION, REGULARY TESTING	EXCHANGER IS CONTINUOSLY FILLED ASSURANCE OF PROPER MATERIAL FOR CHILLER PIPES	REDUNDANT PUMP PREVENTIVE TESTS	INDEPENDENT SOURCE OF ELECTRICAL ENERGY	BACK UP SOURCE, PREVENTIVE MAINTENANCE AND TESTING	BACK UP SOURCE, MAINTENANCE PREVENTING AND TESTING ASSURANCE OF PROPER WATER QUALITY; CLOSED SYSTEM	-REGULARY TESTS -EQUIPMENT QUALIFICATION	-REGULARY CHECK AND EXCHANGE -OIL QUALITY			
INDICATION	FOLLOWING OF DATA ABOUT FAILURES AND ABNORMAL EVENTS	FOLLOWING OF DATA ABOUT FAILURES AND ABNORMAL EVENTS FOLLOWING OF COMPONENT DEGRADATION	FLOW MEASURE ALARM ON LOW FLOW	FLOW MEASURE ALARM ON LOW FLOW	BACK UP INFORMATION (INDICATION) ABOUT VALVE POSITION		INDICATION FLOW COOLING WATER ALARM ON LOW FLOW	TEMPERATURE DIFFERENCE		ALARM ON LOW PRESSURE	ALARM ON LOW FLOW	SURVEILLANCE INSPECTION OF MICRO CRACKS (PENETRANTS)			

Fig. 2. *Cause — consequence matrix example.*

Sodelovali bodo:

– vodja postrojenja	odgovoren je za obratovanje postrojenja;
– vodja proizvodnje	ve, kaj se dejansko dogaja v praksi in ne le, kaj se lahko zgodi;
– tehnolog postrojenja	odgovarja za mehansko vzdrževanje; pozna številne napake, do katerih prihaja;
– vodja instrumentacije	odgovoren je za vzdrževanje instrumentacije, vključno s preizkušanjem alarmov in za nastavitve varnostnih sistemov;
– vodja raziskave	odgovoren je za raziskavo tehničnih problemov in za prenos laboratorijskih rezultatov v proizvodnjo.

Za izvajanje analize HAZOP se torej zahteva multidisciplinarno znanje, kar dosežemo s skupinskim delom strokovnjakov. V skupini so poleg moderatorja, dobrega poznavalca HAZOP, še specialisti s področij, ki so pomembna za obravnavani projekt.

Moderator organizira delovne sestanke in zastavlja vprašanja v zvezi z raznimi odstopanji od pričakovanih vrednosti parametrov procesa.

Osnovno vodilo moderatorjevih vprašanj so t.im. vodilne besede: *ni, preveč, premalo, več ko, delno* itn. v povezavi s parametri procesa kot so tlak, temperatura, koncentracija, vzdrževanje itn.

4. 4 Dokumentiranje študije — pregledniční prikaz študije HAZOP

Zaradi sistematičnosti in preglednosti izvajamo študijo HAZOP v praksi tako da izpolnjujemo pripravljene preglednice HAZOP (sl. 1), po informacijah, podanih na sestankihin po tehnični intehnološki dokumentaciji. Preglednice HAZOP so moderatorju pri vodenju delovnih sestankov v veliko pomoč.

5. POVEZOVANJE ANALIZE HAZOP Z LOGIČNIM MODELIRANJEM SISTEMA

Potem ko smo z analizo HAZOP razpoznali nevarnosti, ki najbolj ogrožajo okolje in ljudi, ali je zaradi njih mogoča gospodarska izguba, nadaljujemo študijo in logično povežemo zbrane informacije in spoznanja.

Naslednja faza pri izvajanju verjetnostnih varnostnih analiz je modeliranje obrata z metodami logičnih povezav vzrokov, zaščitnih ukrepov in posledic. Da bolj jasno podamo matrične povezave, ki se še vedno nanašajo na realni sistem, uporabimo obliko matrike, prikazane na sliki 2.

If an existing plant is being analyzed, the team will consist of different experts. The members of the team will be:

– plant manager	responsible for operation
– process foreman	he knows what actually happens rather than what is supposed to happen
– plant engineer	responsible for mechanical maintenance, he knows many of the faults that occur
– instrument manager	responsible for instrument maintenance including testing of alarms and trips
– process investigation manager	responsible for investigating technical problems for transfering laboratory results to plant scale operations

For HAZOP analysis a multidiscipline knowledge is needed; achieved through team effort of the experts. In the team, beside the independent chairman - expert in HAZOP, are also experts for the process.

The chairman organizes work meetings, asking questions related to different process parameter deviations.

The leading role of the chairman's questions have the so called guide words: *none, more of, less of, part of, more than, other than* etc. in connection with process parameters such as pressure, temperature, concentration, maintenance etc.

4. 4 Documenting of the study

For systematic reasons we perform HAZOP by filling in the gathered information in the predesigned forms (Fig. 1). Information is gathered at team meetings and from process documentation provided by the team members. Hazop forms are of great help to the chairman.

5. HAZOP AND SYSTEM LOGIC MODELING LINKING

After identification of hazard, with the help of HAZOP analysis, which potentially threatens the people and environment or its occurence can cause economic loss, we continue the study and logically connect all collected informations and findings.

The next phase in performing a probabilistic safety analysis is plant modeling by methods of logical connections of causes, protection features and consequences. In order to show the matrix connections refering to a real system more clearly, the shape of the matrix shown in figure 2 is used.

Po taki strnjeni predstavitvi nezgodnega zaporedja dogodkov kaza določimo izhodiščne parametre za logično modeliranje obrata. V stvarnem sistemu so nezgodni prikazi definirani s tremi parametri: odstopanje sistema-komponente, odstopanja procesne spremenljivke in učinki teh odstopanj. Z drugimi besedami, komponenta odpove na določen način in pri tem povzroči spremembo procesne spremenljivke v določenem delu sistema. V logičnem modelu sistema so scenariji definirani z naslednjimi tremi parametri: začetni dogodki, glavni dogodki in neželeni dogodki. Pri HAZOP se ukvarjamo s stvarnim sistemom in skušamo odkriti za dana odstopanja procesnih spremenljivk vzroke (odstopanja sistema-komponente) in posledice odstopanj (učinke odstopanj). Za izdelavo logičnega modela obrata se je treba omejiti na obvladljivo število izhodiščnih parametrov modela sistemov (začetni dogodki, glavni dogodki in neželeni dogodki).

Začetni dogodki so tisti dogodki, ki izzovejo spreminjanje fizikalnih in kemičnih parametrov v sistemu. Osnovni seznam začetnih dogodkov lahko oblikujemo po seznamu vzrokov iz preglednic HAZOP.

Glavni dogodki so odpovedi varovalnih zaščitnih ukrepov. Sem štejemo varnostne funkcije tehnološkega sistema in sistemov za vodenje procesa, še zlasti projektirane varnostne sisteme in posege operaterjev v sili. Začetni seznam glavnih dogodkov lahko oblikujemo po seznamu zaščitnih dejanj v preglednici HAZOP.

Neželeni dogodek je izid nezgodnega prikaza, ki ga označimo kot neuspeh. Glede na začetni dogodek in delovanje zaščite, so neželeni dogodki lahko sila različni. Take različne scenarije imenujemo sekvence, ki so definirane z omenjenimi tremi izhodiščnimi točkami logičnega modela. Spisek neželenih dogodkov delimo v dve skupini: na tisto z negativnim vplivom na okolje in ljudi ter škodo na objektu, opremi in v proizvodnji. Začetni seznam neželenih dogodkov lahko oblikujemo po seznamu posledic v preglednici HAZOP.

Iz izhodiščnih parametrov izdelamo logične modele, npr. drevesa dogodkov in drevesa okvar, ki jih kasneje ovrednotimo in podamo za že izdelani ali načrtovani stvarni sistem.

Potem ko razpoznamo nevarnosti in izdelamo logični model obrata, je mogoče ekonomsko učinkovito odločanje o zmanjšanju tveganja. Če upoštevamo stroške posegov za zmanjšanje tveganja, se utegne izkazati, da tveganje lahko zmanjšamo s kakšnim večjim (dražjim) posegom, lahko pa tudi z več manjšimi (cenejšimi) posegi, pri čemer je končni rezultat enak ali primerljiv. Tako postane tveganje merilo za učinke vlaganja v varnost.

After such a representation of an accident scenario, the basic parameters for plant logic modeling are determined. An accident scenario in the real world is defined by the triplet of *real system* parameters as a *system - component deviation*, *process variable deviation* and *system node effect*. Namely, the failure mode of the relevant component generates a deviation on one or more process variables at some particular points (nodes) of the plant. On the other hand, the triplet of safety *plant model* control points, or let us say modeling start points, is given by the *initiating events*, *top events* and *undesired events*. When we are carrying out a HAZOP study, we deal mainly with the first mentioned triplets, trying to discover for the given *process variable deviation* the cause (*system - component deviation*) and the consequences of deviation (*system node effect*). For the purpose of plant modeling, it is necessary to determine, by the selection process, the definitive number of plant modeling start points (*initiating events* and consequently *top events* and *undesired events*).

The initiating events are those events, which explicitly challenge the variation of system physical or chemical parameters. The specific initial list of *initiating events* can be made from the *feasible cause* of a process parameter deviation heading of the HAZOP form table.

The top events essentially represent the failure of protective measures. These protective measures or functions are performed by the control system, specific standby and protective system, and by specific operator action on the basis of emergency procedure. The initial list of *top events* can be drawn from the *existing protective measures* heading of HAZOP table.

Finally, *the undesired event* represents the accident scenario issue with undesired consequences. Generally, undesired event categories are: air pollution, water and earth pollution, explosion, fire, destroyed equipment, product low quality etc. The initial list of *undesired events* can be drawn from the *consequences* heading of HAZOP table.

The aim of this process is to develop logic models, event trees and fault trees for example, which are later to be evaluated and interpreted for an exsisting or planned real system.

The effective decision-making on risk reduction is possible after the hazard identification and plant logic model elaboration. The consideration of risk reduction cost can show that the same result could be reached by few large or by more minor interventions. Obviously, the cost-benefit ratio of investment into safety can be determined by risk reduction price.

6. PRIMER ŠTUDIJE HAZOP IN DEFINIRANJE IZHODIŠČ ZA LOGIČNO MODELIRANJE POSTROJENJA

V tem delu članka želimo na primeru študije HAZOP za Colorjevo sintezo smol iz Medvod predstaviti uporabo opisane metodologije. Na sliki 3 je prikazan del procesa z reaktorjem in hladilnikom termalnega olja, ki je namenjen za vzdrževanje želene temperature v reaktorju. Sinteza v reaktorju je krmiljena in ne regulirana, kar pomeni, da so vzorčenja med procesom in korekturo pri krmiljenju procesa ročna.

Pri projektu za Colorjevo sintezo smol smo uporabili kombinacijo obeh omenjenih načinov za izdelavo HAZOP, saj je v tovarni usposobljena strokovna ekipa za vodenje in vzdrževanje stare sinteze, ki jo je sicer uničil požar februarja 1990. Za izvedbo nove sinteze je skrbela investicijska skupina, projekte pa je izdelal neodvisni zunanji projektant.

6. 1 Izdelava študije HAZOP

Zbiranje za varnost pomembnih informacij je osnovna naloga HAZOP, od katere je odvisna kakovost raziskave.

V delovnih razgovorih so sodelovali naslednji profili strokovnjakov:

- vodja investicijskega projekta,
- tehnolog,
- vodja obrata,
- projektanti tehnologije in inštalacij,
- razvojni inženir,
- nadzorni inženir,
- dobavitelj opreme,
- ekolog.

Da bi zagotovili sistematičnost dela in popolnost analize, smo poprej izdelali pregled vseh tehnoloških funkcij (tehnološke komponente in tehnološki procesi) in ocenili pomembnost odstopanja procesnih parametrov za varnost in delovanje obrata. Po takem pregledu smo prišli do seznama komponent in procesov, v katerih smo odstopanja analizirali.

Značilnost obrata sinteze smole v Colorju je ta, da proces ni kontinuiren. Proces poteka v štirih fazah: polnjenje reaktorja, segrevanje do potrebne temperature in odvajanja reakcijske vode, pretakanje v razredčevalno posodo, razredčevanje in hlajenje oz. segrevanje v razredčevalni posodi. V obratu sinteze je postavljenih šest reaktorskih linij, ki se bistveno ne razlikujejo. Analizo HAZOP smo opravili za eno linijo, in sicer tako, da vsebuje vse elemente, ki se pojavljajo v vsem obratu.

6. EXAMPLE OF HAZOP ANALYSIS AND DETERMINATION OF STARTING POINTS FOR PLANT LOGIC MODELING

The second part of the paper deals with the HAZOP analysis of the Color Medvode resin synthesis. Through an example, the use of described methodology will be shown. The part of the technological process with the reactor and thermal oil heat exchanger is shown in Fig. 1. The heat exchanger is used for temperature control in the reactor. Synthesis process is not automatically controlled. Some manual corrections of temperature on the basis of sampling are required.

The HAZOP is performed by using the two mentioned approaches in combination. There is a team of experts for process managing and maintenance of »Old Synthesis«, destroyed in a fire in february 1990. The design of »New Synthesis« was performed by an outdoor designer. The building was managed by the Color investment team.

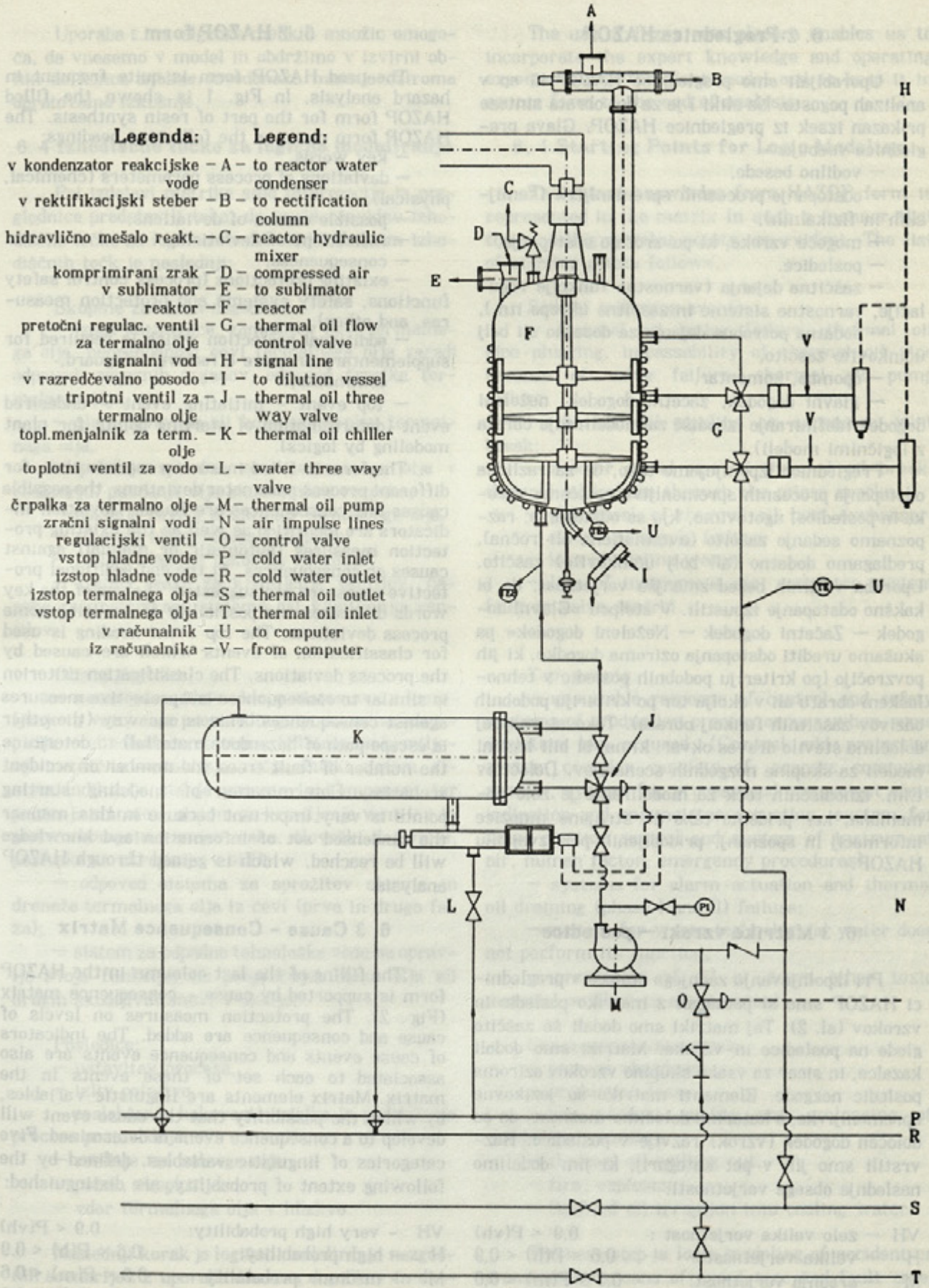
6. 1 HAZOP Performance

Collection of safety related information is the basic task, which influences the further quality of analysis. In working sessions the following profiles of experts were involved:

- head of investment project,
- technologist,
- works manager,
- designers of technology and installations
- R & D engineer,
- superintendent,
- plant vendor,
- ecologist.

The preliminary revision was performed in the form of tables of all technological functions (components and processes) and the importances of process parameter deviations for plant safety and operability were estimated. On the basis of this review the list of components and processes was defined for further analysis. This helped us to work systematically and to complete the analysis.

The characteristic of resin synthesis production in Color is batch process, which is composed of four phases: reactor charging, heating and maintenance of required temperature profile with simultaneous evaporation of reaction water, pouring from reactor to vessel for resin dilution and resin cooling. There are six production lines in the plant. The differences between them are not essential, so we have chosen one which includes all of the elements appearing in other reactor lines.



Sl. 3. *Sinteza smol Color Medvode: reaktor s sistemom za vzdrževanje temperaturnega profila.*
Fig. 3. *Color Medvode resin synthesis: reactor with temperature profile maintenance system.*

6. 2 Preglednica HAZOP

Uporabljali smo preglednice HAZOP ki so v analizah pogoste. Na sliki 1 je za del obrata sinteze prikazan izsek iz preglednice HAZOP. Glava preglednice vsebuje:

— vodilno besedo,
— odstopanje procesnih spremenljivk (kemijskih in fizikalnih),
— mogoče vzroke, ki povzročajo odstopanja,
— posledice,
— zaščitna dejanja (varnostne funkcije regulacije, varnostne sisteme in zaščitne ukrepe itn.),
— dodatna potrebna dejanja za dodatno ali bolj učinkovito zaščito,
— opombo, komentar,
— glavni dogodek, začetni dogodek, neželeni dogodek (definiranje izhodišč za modeliranje obrata z logičnimi modeli).

Preglednico izpolnjujemo tako, da za različna odstopanja procesnih spremenljivk poiščemo vzroke in posledice, ugotovimo, kje so odstopanja, razpoznamo sedanjo zaščito (avtomatična ali ročna), predlagamo dodatno (ali bolj učinkovito) zaščito. Uporaba vodilnih besed zmanjša verjetnost, da bi kakšno odstopanje izpustili. V stolpcu »Glavni dogodek — Začetni dogodek — Neželeni dogodek« pa skušamo urediti odstopanja oziroma dogodke, ki jih povzročijo (po kriteriju podobnih posledic v tehnološkem obratu ali v okolju ter po kriteriju podobnih odzivov zaščitnih funkcij obrata). Tako si vnaprej določimo število dreves okvar, ki naj bi bili logični modeli za skupine nezgodnih scenarijev. Določitev t.im. izhodiščnih točk za modeliranje je zelo pomembna, ker pridemo tako do strnjene množice informacij in spoznanj, pridobljenih pri izvajanju HAZOP.

6. 3 Matrika vzroki — posledice

Pri izpolnjevanju zadnjega stolpca v preglednici HAZOP smo si pomagali z matriko posledic in vzrokov (sl. 2). Tej matriki smo dodali še zaščito glede na posledice in vzroke. Matriki smo dodali kazalce, in sicer za vsako skupino vzrokov oziroma posledic nezgode. Elementi matrike so jezikovne spremenljivke, s katerimi določimo možnost, da se določen dogodek (vzrok) razvije v posledico. Razvrstili smo jih v pet kategorij, ki jim dodelimo naslednje obsege verjetnosti:

VH	— zelo velika verjetnost :	0,9 < P(vh)
H	— velika verjetnost:	0,6 < P(h) < 0,9
M	— srednja verjetnost:	0,3 < P(m) < 0,6
L	— majhna verjetnost:	0,1 < P(1) < 0,3
VL	— zelo majhna verjetnost:	0,0 < P (vl) < 0,1

6. 2 HAZOP form

The used HAZOP form is quite frequent in hazard analysis. In Fig. 1 is shown the filled HAZOP form for the part of resin synthesis. The HAZOP form contains the following headings:

— key words,
— deviations of process parameters (chemical, physical),
— possible causes of deviations,
— indications of deviations,
— consequences,
— existing protections (process control safety functions, safety systems and protection measures, and other),
— additional protection which is required for supplementary or more effective safeguard,
— comments,
— top event - initiating event - undesired event (determination of starting points for plant modeling by logics).

The form is filled in such a manner that, for different process parameter deviations, the possible causes and consequences are found. Deviation indicators are identified as well as the existing protection measures (automatic or manual) against causes or consequences. At the end additional protective measures are suggested. The use of the key words decreases the possibility of omitting some process deviations. The *top event* heading is used for classification of events which are caused by the process deviations. The classification criterion is similar to consequences and protective measures against consequences. This is one way (the other is escape path of hazardous material) to determine the number of fault trees and number of accident scenarios. Determination of modeling starting points is very important because in this manner the condensed set of information and knowledge will be reached, which is gained through HAZOP analysis.

6. 3 Cause - Consequence Matrix

The filling of the last coloumn in the HAZOP form is supported by cause - consequence matrix (Fig. 2). The protection measures on levels of cause and consequence are added. The indicators of cause events and consequence events are also associated to each set of these events in the matrix. Matrix elements are linguistic variables, by which the possibility that the cause event will develop to a consequence event is determined. Five categories of linguistic variables, defined by the following extent of probability, are distinguished:

VH	- very high probability:	0.9 < P(vh)
H	- high probability:	0.6 < P(h) < 0.9
M	- medium probability:	0.3 < P(m) < 0.6
L	— low probability:	0.1 < P(1) < 0.3
VL	- very low probability:	0.0 < P(vl) < 0.1

Uporaba t.im. algebre mehkih množic omogoča, da vnesemo v model in obdržimo v izvirni obliki do konca analize, izvedenska mnenja oziroma obratovalne izkušnje.

6. 4 Izhodiščne točke za logično modeliranje

Pri izdelavi matrike smo informacije iz preglednice predstavili tako, da so že razvidne izhodiščne točke za logično modeliranje. Seznam izhodiščnih točk je naslednji:

Skupine začetnih dogodkov:

— izpad kotlovnice, zamašitev cevi termalnega olja, neprehodnost cevi termalnega olja zaradi odpovedi zapornih organov, odpoved črpalke termalnega olja,

— zlom cevovoda ali kompenzatorjev termalnega olja,

— pokanje spiralne cevi termalnega olja v reaktorju, puščanje olja skozi mikro razpoke,

— pokanje cevi v hladilniku termalnega olja,

— odpoved električnega napajanja,

— izguba hladilne tekočine (hladiva),

— izguba zraka za krmiljenje ventilov, napaka računalniškega sistema pri krmiljenju ventilov.

Glavni dogodki:

— neustrezen odziv sklopa sistemov za krmiljenje in varovanje proizvodnega procesa na odstopanja v tehnološkem sistemu. (Sistem za krmiljenje in zaščito sestavljajo: računalniški sistem, sistem indikacije stanja procesa in komponent ter proženja alarmov, sistem za krmiljenje ventilov in sistem komprimiranega zraka, človeški dejavniki, postopki za ukrepanje v sili);

— odpoved sistema za sprožitev alarma in drenažo termalnega olja iz cevi (prva in druga faza);

— sistem za odpadne tehnološke vode ne opravlja svoje funkcije: ne preprečuje iztoka olja ali drugih škodljivih snovi v okolje;

Posledice:

— ustavitev procesa,

— izliv polnitve,

— poslabšanje kakovosti izdelka in podaljšanje procesa proizvodnje,

— razlitje termalnega olja,

— požar, eksplozija,

— vdor termalnega olja v hladivo.

Naslednji korak je logično modeliranje nezgodnih scenarijev z uporabo drevesa dogodkov in drevesa okvar. Ta dejavnost pa je že zunaj obsega razpoznavanja nevarnosti.

The use of fuzzy sets algebra enables us to incorporate the expert knowledge and operating experience into the plant model and to keep it in source form to the end of analysis.

6. 4 Starting Points for Logic Modeling

The gained knowledge from HAZOP form is represented in the matrix in such a manner that the modeling starting points are evident. The list of starting points follows.

Sets of initiating events:

— thermal oil boiler failure, thermal oil pipe plugging, impassability of thermal oil pipe because of valve failure, thermal oil pump failure;

— thermal oil pipeline or expansion joint break;

— reactor spiral pipe of thermal oil break, thermal oil leakage through the micro cracks.

— pipe break of thermal oil heat exchanger;

— electrical supply failure;

— loss of cooling water;

— loss of instrument air, computer system fault in valve control.

Top events:

— unsuitable response of control and safety systems of production process occurs when some deviation has occured. (Control and protection system complex consists of: process computer system, system for process and component state indication and annunciator actuation, system for valve position control and system of instrument air, human factor, emergency procedures).

— systems for alarm actuation and thermal oil draining (phase I and II) failure;

— system for waste technological water does not perform its function;

— prevention of oil or some other toxic material outflow to environment

Consequence categories:

— process shutdown,

— production loss,

— low product quality and prolonging of production process,

— thermal oil spilling out,

— fire, explosion,

— thermal oil irruption into cooling water.

The next step is logic modeling of accident or transient by means of event tree and fault tree. It is out of the scope of hazard identification and we call it HAZard ANalysis (HAZAN).

6.5 Povzetek ugotovitev iz preglednice HAZOP

V nadaljevanju povzemamo po naši oceni najbolj neugodne poteke, ki lahko pripeljejo do emisije nevarnih snovi v okolje, do škode na obratu in proizvodnji, do manj učinkovitega procesa ali do poslabšanja kakovosti izdelka.

1. *Temperaturni šoki v hladilniku termalnega olja in možnost pokanja cevi z izlitjem termalnega olja.*

Hladilnik termalnega olja je že v normalnem izdelovalnem procesu izpostavljen cikličnim toplotnim obremenitvam. V primeru izgube hladiva in ponovne napolnitve je ta temperaturni šok še ostrejši. Poleg tega se pri tem na začetku prehodnega pojava razvija večja količina pare, ki tlačno obremenjuje posodo. Načrtovana regulacija nima zaščitne funkcije, ki bi omilila ostre temperaturne prehodne pojave. Priporočili smo, da se pri regulaciji ventilov na oljni in vodni strani vgradi zakasnilni člen, ki bi upočasnil odpiranje ventilov in zagotovil najprej odpiranje vodnega ventila in šele potem oljnega.

2. *Mikro puščanje termalnega olja iz grelnih cevi v toplotno izolacijo*

Prav tako so cikličnim termičnim obremenitvam izpostavljene tudi grelne cevi okrog reaktorja. Poleg tega je dolžina zvarov izredno velika. V njih so lahko zaostale napetosti. Vse to povečuje verjetnost pojava mikro razpok v ceveh in zvarih. Pravočasna indikacija mikro puščanja nas lahko opozori na prisotno nevarnost. Predlagali smo, da se razišče možnost za vgradnjo sistema za sporočanje puščanja, ki bi deloval po načelu merjenja spremembe električnega upora toplotne izolacije. Nevarnost požara je manjša ob vzdrževanju inertne atmosfere v toplotni izolaciji.

3. *Izguba polnitve zaradi strjevanja ali poslabšanje kakovosti polnitve zaradi napake v računalniškem vodenju in slabi usposobljenosti operaterjev*

Če odpove računalnik ali se prekine računalniško vodenje, je treba zagotoviti varno nadaljevanje procesa ali njegovo varno ustavitev. Za uspešen prehod na ročno upravljanje mora biti osebje sinteze ustrezno usposobljeno. Osebje pri tem uporablja pripravljene postopke in se za ukrepanje v sili ustrezno uri, občasno pa mora na preizkus znanja.

6.5 Conclusions Resumed from HAZOP form

Listed below are some undesired scenarios which can result in emission of hazardous material to the environment, damage to production lines, less effective production process or in decrease of product quality:

1. *Temperature shocks in thermal oil heat exchanger and possibility of thermal oil leakage because of pipe cracks:*

Thermal oil heat exchanger in production process is normally exposed to cyclic thermal loads. In the case of loss of cooling water and a while after reestablishing it, there is a severe temperature shock. Besides, a large amount of steam developed at the beginning of the transient, additionally pressurizes the heat exchanger. The designed control system does not include protective functions which could mitigate the severe temperature transients. We have recommended to build up the delay device on oil and water side valves, which influences the valve opening regime. The valve on the cooling water side will be opened first and the thermal oil valve after that. The speed of valve position change should also be low.

2. *Thermal oil micro-eaks from heating spiral pipes to thermal isolation*

The heating spiral pipes around reactor vessel are also exposed to cyclic thermal loads. The length of the welds is substantial. The weld region is exposed to the residual stresses. All of these factors increase the probability of micro—cracks developing on pipes and welds. Timely indications of micro—leaks can warn of an existing hazard. We suggested the exploration of the possibility of using the system for leak indication, based on the measurement of electrical resistance changes of thermal isolation. The maintenance of inert atmosphere in thermal isolation decreases the fire hazard.

3. *Loss of reactor charge because of solidification or low quality caused by computer control faults and poor operator training*

In the case of computer failure or an event which causes the loss of computer control, it is required to provide safe prolongation of process or safe shutdown. Successful transition to manual control is assured by adequate training of plant personnel. The plant personnel use the emergency procedures and prepare for such situations by retraining and periodic knowledge and skill testing.

7. SKLEP

Študije tveganja v procesni industriji so se pokazale koristne predvsem na dveh ravneh uporabe. Ob izdelavi celotne raziskave tveganja je mogoče nadzorovati varnost na podlagi zamisli o celotnem tveganju z optimizacijo stroškov in sredstev, potrebnih za izboljšanje varnosti. Že izdelava študije HAZOP pomaga pri nadzorovanju obratovalne varnosti in preprečevanju nezgod brez nadrobne analize posledic.

Študija HAZOP sinteze smol za Color iz Medvod je prvi primer raziskav tveganja v procesni industriji v Sloveniji.

Izdelava HAZOP je omogočila razpoznavanje vzrokov, njihove posledice in zaščitne ukrepe. To so dogodki, ki definirajo nezgodno zaporedje dogodkov. S konstrukcijo matrike (vzroki — posledice) smo nadalje strnili vsebino preglednic HAZOP in s tem olajšali definiranje izhodiščnih točk (začetni, glavni, neželeni dogodki) za logično modeliranje nezgod. Prav tako smo z uporabo mehke verjetnosti definirali razmerje med vzroki in posledicami ter s tem omogočili uporabo te verjetnosti pri vrednotenju.

V študiji smo razpoznali verjetna kritična mesta in opozorili na mogoče človekove napake kot vire nevarnosti. Predlagali smo modifikacije opreme in priporočili izboljšave sedanjih oziroma izdelavo novih obratovalnih navodil, navodila za postopke v sili in preventivno vzdrževanje.

Prav tako smo z investitorjem dosegli soglasje glede rezultatov študije HAZOP in že dosežene ravni varnosti, ki je višja kakor v »stari sintezi«. Večino identificiranih kritičnih mest, posebej na področju izdelave navodil za postopke v sili ter navodil za preventivno vzdrževanje, je skupina Colorjevih strokovnjakov takoj začela obravnavati.

Nadaljnje faze študije bi z uporabo verjetnostnega modela pripeljale tudi do kolikostne ocene tveganja okolja in prebivalstva. Končna faza analize bi bilo nadzorovanje in upravljanje tveganja, ki bi temeljilo na logičnih in odločitvenih modelih. Celotna analiza tveganja omogoča ne samo racionalno in učinkovito ravnanje pri zagotavljanju *varnosti*, temveč tudi povečuje *razpoložljivost* tehnološkega postrojenja.

7. CONCLUSION

The risk analysis in the process industry showed its usefulness on two levels of use. The first is risk management on the basis of total risk concept, including the cost-benefit analysis of investment in risk analysis and safety improvements. The second is system analysis which helps us improve the operational safety and decreases the possibility of undesired consequences because of an accident without detailed consequence analysis. The HAZOP analysis supports this level to some extent.

The HAZOP study of resin synthesis for Color Medvode is the first case of risk investigation in the process industry in Slovenia.

HAZOP analysis enabled us to identify the causes, consequences and protective measures. By construction of the cause-consequence matrix, the contents of HAZOP form are condensed and in this manner make easier the definition of accident logic modeling starting points (initiating events, protective measures, undesired events). The relationship between the causes and consequences is defined by using the fuzzy probability (concept of possibility) on the basis of operational experience and expert knowledge. It enabled the use of the possibility concept in the quantitative evaluation.

The potential critical components and actions, possible human errors as hazard sources were identified and improvements were recommended. Some modifications and improvements of equipment, the operating procedures elaboration, emergency procedures elaboration and preventive maintenance elaboration were suggested.

An agreement with the investor concerning HAZOP study results and achived level of safety, which is higher than in the »Old Synthesis«, was reached. Most of the identified critical parts, especially in the field of emergency procedures and preventive maintenance, the Color experts started to react immediately.

Further phase of the study would be to use probabilistic models, carrying out quantitative estimation of environmental and social risk. This final phase of the analysis would be the risk management system which is based on the logical and decision models. Complete analysis of risk enables rational and effective *safety* management and increases technologic system *availability*.

8. LITERATURA
8. REFERENCES

[1] Kožuh, M.–Sušnik, J.–Vojnović, Đ.: Analiza nevarnosti med obratovanjem v obratu sinteza smol Color Medvode. Inštitut J. Stefan, Ljubljana, April 1991.

[2] Haddad, S.–Hirschberg, S.: PSA in the Nuclear and Process Industry: Opportunities for interchange of experience. International Symposium on the Use of Probabilistic Safety Assessment for Operational Safety. PSA '91, Vienna, Austria, 3–7 June 1991.

[3] Kletz, T.A.: HAZOP & HAZAN. Notes on the Identification and Assessment of Hazards. The Institution of Chemical Engineers, 1986.

[4] Amendola, A.–Bustamante, A.S.: Reliability Engineering – Proceedings of the ISPRA-Course. Madrid, September 1986.

[5] The 1988 European Summer School on Major Hazards. Christ's College, Cambridge, July 1988.

[6] Colombari, V.: Reliability Data Collection and Use in Risk and Availability Assessment. 6th Eurodata Conference, Siena, 1989.

[7] Summitt, R.L. et al.: Methodology for the Identification and Screening of Chemical and Petrochemical Initiating Events. PSA '89 Proceedings, Pittsburgh, 1989.

[8] King, R.: Safety in the Process Industries. Butterworth – Heinemann, 1990.

Naslov avtorjev: mag. Đorđe Vojnović, dipl. inž.
Mitja Kožuh, dipl. inž. in
dr. Janez Sušnik, dipl. inž.
vsi
Institut Jožef Stefan
Ljubljana
Jamova 39

Authors' Address: mag. Đorđe Vojnović, dipl. ing.
Mitja Kožuh, dipl. ing. and
dr. Janez Sušnik, dipl. ing.
all
Institut Jožef Stefan
Ljubljana
Jamova 39

Prejeto:
Received: 7.11.1991

Recenzirano:
Reviewed: 16.6.1992