© Strojniški vestnik 48(2002)8,418-437
ISSN 0039-2480
UDK 66.012.004.64:614.8
Izvirni znanstveni članek (1.01)

© Journal of Mechanical Engineering 48(2002)8,418-437
ISSN 0039-2480
UDC 66.012.004.64:614.8
Original scientific paper (1.01)

Sinteza orodij za analizo človeške napake po metodi analize spoznavne zanesljivosti in napak ter analize drevesa odpovedi

The Synthesis of Human-Error Analysis Using the Cognitive Reliability and Error Analysis Method and Fault-Tree Analysis

Janja Zupančič - Jure Marn

V pričujočem prispevku je bila obravnavana sinteza orodij, ki so uporabljana za oceno človeških napak (analiza spoznavne zanesljivosti in napak - ASZN - CREAM) in tehničnih odpovedi (drevo napak) na tak način, da je moč dobljene rezultate smiselno primerjati. Sinteza je bila opravljena za obstoječo rektifikacijsko kolono. Predlagane in predstavljene so izboljšave na osnovi dobljenih rezultatov.

(Ključne besede: metode CREAM, verjetnost napak, verjetnost okvar, drevo odpovedi)

In this paper we have looked at the synthesis of tools used for human-error analysis (Cognitive Reliability and Error Analysis Method - CREAM) and technical error or device error (fault tree) in such a way that a comparison between the results is possible. The synthesis was performed for an existing rectification system (column). Possible improvements are shown and suggested.

(Keywords: CREAM methods, human probability, failure probability, fault tree analysis)

0 UVOD

Optimizacija procesov, povečevanje dobička, manjšanje stroškov, zlasti stroškov dela, so povzročili umik običajnih pripomočkov, ki so prispevali k zmanjšanju ali odpravi vplivov pomanjkljivega znanja. Na drugi strani je razvoj svetovno nevarnih sistemov za proizvodnjo energije in objektov procesne tehnike, zlasti s področja kemije, povzročil potrebo po manjšanju verjetnosti nezgod na človeštvu še sprejemljivo raven, ki se pogosto bliža frekvenci 1×10^{-5} dogodka na leto, kar prevedeno pomeni eno nezgodo v 100.000 letih obratovanja posameznega objekta. Za uporabnika ali operaterja pomeni taka verjetnost zanemarljivo tveganje.

V tem prispevku želimo prikazati možnost povezave med metodologijo ovrednotenja verjetnosti napake kot človekovega prispevka k odpovedi zahtevnega procesnega sistema in metodologijo ovrednotenja verjetnosti okvare kot tehnološkega prispevka k odpovedi procesnega objekta. Prednost prikazane metode je v enakovredni obravnavi nezgod in okvar ter v številski oceni verjetnosti odpovedi zahtevnega procesnega sistema.

Verjetnostna varnostna analiza na področju tehnoloških sistemov[1] v procesnem strojništvu je dobro razvita. Na tem področju je tudi pri nas moč najti več prispevkov, ki sodijo v zakladnico svetovne

0 INTRODUCTION

The optimization of processes, the increase of profit, and the decrease of costs, in particular labor costs, have resulted in an end to classical ways of decreasing or eliminating effects that occur due to a lack of knowledge. In addition, the evolution of globally dangerous systems for energy production and process engineering installations, in particular in the area of chemistry, caused the drive toward a lower accident probability that was at a level acceptable to the public, usually of the order of 1×10^{-5}, i.e. one accident in 100,000 years of operation for a particular installation. For both user and operator such a low frequency usually amounts to a negligible risk.

This paper deals with the possibility of a connection between the methodology of the accident probability evaluation of the human contribution to the failure of a complex-process installation, on the one hand, and the methodology of the evaluation of the technological contribution to failure of the same installation. The advantage of the method presented below is in the transformation of both types of information into comparable quantities, and the better assessment of complex-process system failure.

The probabilistic safety analysis of technological systems[1] in process engineering is well established. There are several studies in this area available in Slovenian professional literature: works

znanosti, zlasti deli Kožuha ([1] in [2]). Večje težave pa so pri opredelitvi vpliva, ki ga imajo na delovanje kompleksnih sistemov ljudje.

V pričujočem prispevku zato poskušamo dvoje: ponoviti verjetnostno varnostno analizo odpovedi z uporabo analize dreves dogodkov, dobro znanih iz številnih del ([3] in [4]), najti je moč še številne druge avtorje in nadalje, to analizo nadgraditi z uporabo sodobne metodologije na področju analize vpliva človeških napak. Pri tem nimamo namena zadovoljiti zgolj z opisom mogočih posledic, temveč želimo vpliv človeških napak tudi številsko izraziti, s tem pa prepričati morebitne uporabnike[2], da bi predstavljeno metodologijo pričeli rutinsko uporabljati za svoje redno delo.

1 TEORETIČNA IZHODIŠČA

Človeške napake pomenijo 60 do 90 odstotkov vseh sistemskih napak.V zadnjih 40 letih se delež nezgod, katerih vzrok je človeška napaka, zvečuje. To ne pomeni, da povzročamo ljudje čedalje več napak, ampak da prihajajo s tehnološkim razvojem vedno bolj do izraza. Soodvisnost je prikazana na sliki 1 po [5]. Z uvajanjem sistemov nadzora kakovosti vse do sistema popolne kakovosti namreč prihaja do redkejših lomov strojev, človeška zanesljivost pa je ostala približno nespremenjena[3].

To spoznanje lahko spreminja žarišče dosedanjih verjetnostnih varnostnih analiz na področju zahtevnih tehnoloških sistemov iz analiz, ki so se zlasti ukvarjale z verjetnostjo odpovedi posameznega dela sistema, v analize, ki se ukvarjajo z verjetnostjo napačnih odločitev vpletenih na vseh stopnjah procesov (oz. organizacijski faktor). Poglobljena analiza zahtevnih tehnoloških sistemov

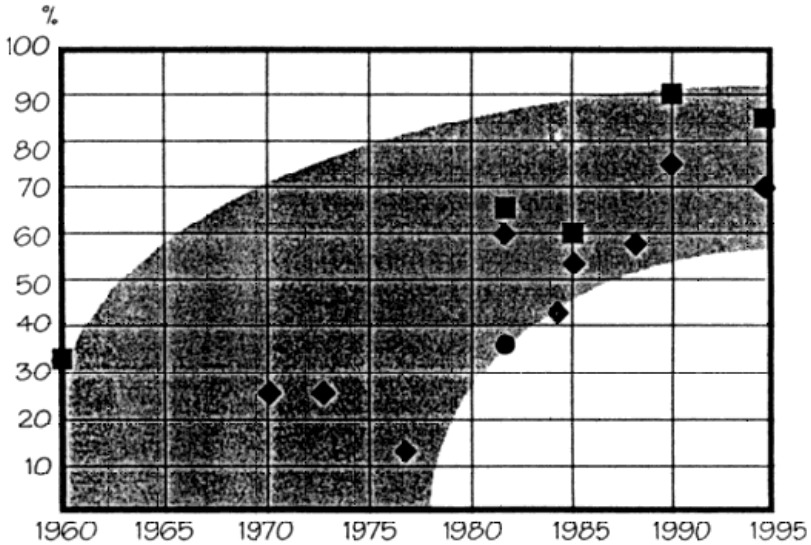
such as Kožuh ([1] and [2]). However, it is harder to find such contributions in the area of human-error analysis effecting complex engineering systems.

In this contribution we have tried to achieve two objectives: first, to repeat a well-established probabilistic safety analysis using the fault-tree-analysis method known from several contributions ([3] and [4]), and several other authors and second, to augment this analysis with a human-error analysis using modern methodology in this area. Further more, in addition to qualitatively describing possible consequences we have strived to quantify the effects of these errors, thereby convincing the users[2] of this information to start using such a methodology in their day-to-day operations.

1THEORETICAL BACKGROUND

Human errors represent 60–90% of all system failures. Over the past 40 years the ratio of accidents caused by human factors to all accidents has steadily increased. This does not mean that people are less careful, rather it means that technological progress is eliminating mechanical errors. This codependency was shown by [5], whose figure is reproduced as Figure 1. Modern quality systems such as Total Quality Management (TQM) have resulted in a reduction of mechanical failures, while human reliability has tended to stay constant unless influenced by training or other methods[3].

This conclusion can change the focus of to-date probabilistic safety analyses in the area of complex technological systems from analyses mainly dealing with the probability of failures to particular parts of a system to analyses dealing with the probability of erroneous decisions of all those involved in various levels of processes (the so-called organizational factor). The in-depth analysis of



Sl. 1. *Delež nezgod, katerih vzrok je človeška napaka* [5]
Fig. 1. *Fraction of human-error-induced accidents [5]*

tako še naprej ostaja v osti varnostnih analiz, zlasti na področju latentnih in zato premalo opazovanih napak [6]. Avtorja ugotavljava, da je bilo v začetku veliko zanimanje za tehnološko zanesljivost (v 70.), potem so spoznali, da je ključen človek (v 80.), in nato, da je pomembna organizacija (v 90 letih prejšnjega stoletja).

V nadaljevanju je najprej opisan problem, nato pa prikazana uporaba metodologije drevesa odpovedi (znane tudi pod imenom drevo napak), zatem uporaba metode spoznavne (oz. miselne) zanesljivosti in analize napak [5] na sistemu rektifikacijske kolone in nazadnje sinteza obeh metod ter primerjava med verjetnostjo nezgode in okvare s predlogom odprave.

2 OPIS PROBLEMA

Poglavitni namen dela je določitev verjetnosti tehnične (mehanske) in človeške napake rektifikacijskega sistema, katere posledica bi bil trenutni oziroma stalni izpust tekočinske mešanice. Obe vrsti izpusta bi bili iz vidika ekonomike procesa in parametrov okoljske varnosti nesprejemljivi, zato je treba določiti ne le verjetnost odpovedi temveč tudi posamezne vplivne parametre, ki na morebitno napako vplivajo. Številska vrednost prispevka napake posameznega vplivnega parametra, v okviru predpostavk, podaja tudi vrstni red, ki ga je smiselno upoštevati pri odpravi napak. Tako je moč v okviru prispevkov tehničnih napak ugotoviti potrebo po zamenjavi posameznih kritičnih delov in smiselno frekvenco preventivnih pregledov, v okviru prispevkov človeških napak pa tista področja, na katerih je primerno izvesti dodatno izobraževanje ljudi, ki so neposredno vpeti v proces obratovanje rektifikacijske kolone. Pri tem je smiselno poudariti še, da imata izobraževanje in trening omejitev in verjetnosti napake ne moremo poljubno zmanjšati [11].

Za določitev verjetnosti tehnične napake rektifikacijskega sistema je bila uporabljena metoda drevesa napak. Verjetnost človeške napake je bila vrednotena z osnovno in razširjeno metodo ASZN. Verjetnost človeške napake je bila vključena v drevo napak za trenutni in stalni izpust in hkrati opravljena analiza vpliva verjetnosti človeške napake na skupno verjetnost napake pri obeh izpustih.

2.1 Opis delovanja sistema

V rektifikacijski koloni, osrednji napravi rektifikacijskega sistema, poteka postopek ločevanja zmesi aceton - izopropanol - voda na podlagi različnih hlapljivosti navzočih sestavin. Ločevanje komponent poteka pri temperaturah vrelišča, pri čemer slika 2 prikazuje shemo rektifikacijskega sistema, ki je sestavljen iz rektifikacijske kolone, uparjalnika in kondenzatorjev.

complex technological systems still remains at the cutting edge of safety analyses, in particular for latent and therefore not-enough-observed errors [6]. The authors note that interest has shifted from an initial interest in technological reliability (1970s) to human-error analysis (1980s), and finally to organizational aspects of reliability (1990s).

The problem will be briefly discussed below, and this will be followed by the use of the methodology of failure-tree analysis, and then the use of [5] applied to the system of a rectification column, and finally the synthesis of both methods and a comparison between the probability of error and accident with a suggestion for system remedies.

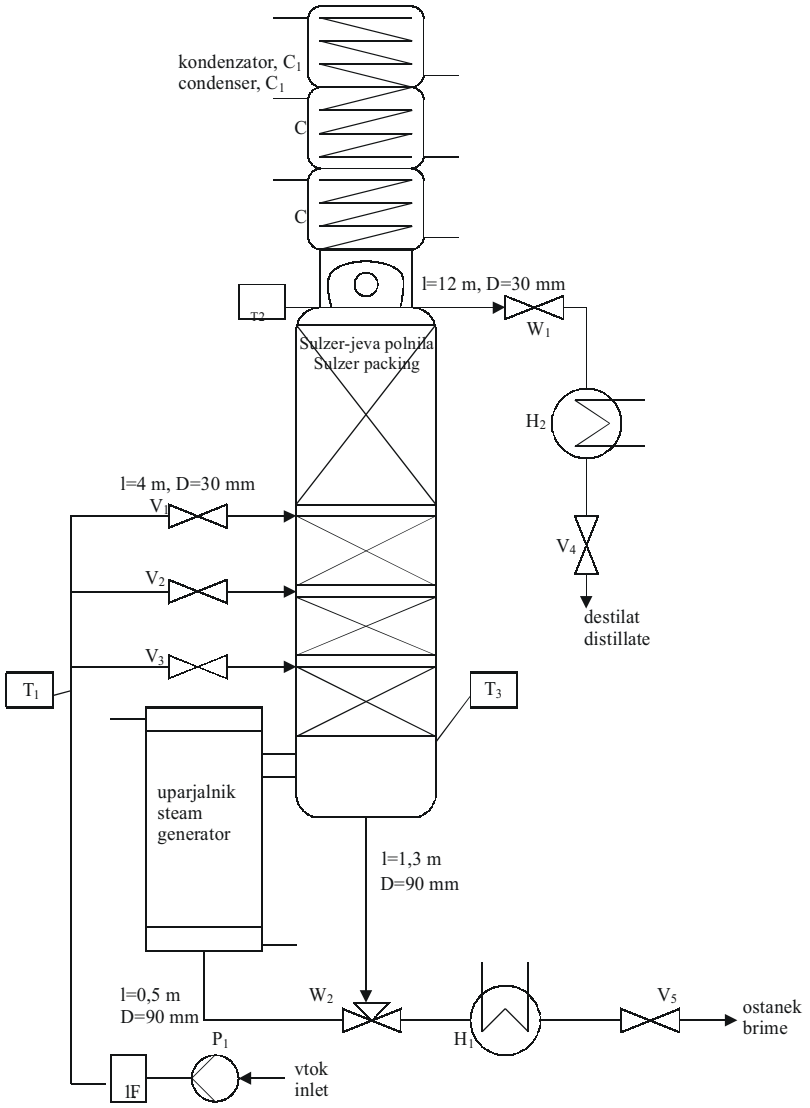
2 PROBLEM DESCRIPTION

The basic goal of this work is the quantification of technical (mechanical) and human error during the continuous operation of a rectification system that causes instantaneous and continuous releases of a fluid mixture. Both types of leaks are unacceptable from the viewpoint of the economy of the process and ecological safety parameters; therefore, not only the probability of failure needs to be assessed but also the important parameters influencing the failures. A quantitative assessment of a particular failure mode also forms the basis for the mitigation of the factors leading to this failure: first the parameters leading to the most probable failure mode need to be investigated, followed by the second most probable, etc. given that the damage to life, people, and property is similar. This methodology enables one to establish which parts of the machinery are most likely to fail and therefore schedule preventive maintenance; and which areas should be addressed when training people involved in the operation of the rectification system. At the same time it should be noted that the effects of education and training are limited and that the probability of human error cannot be lowered indefinitely [11].

Fault-tree analysis was used for the evaluation of the technical error of the rectification system. The probability of human error was assessed using the basic and extended CREAM method. Then, the probability of human error was included in the fault trees for instantaneous and continuous releases and analyses of human-error influence on the total probability for both cases was performed.

2.1 Description of system operation

The process of separating acetone-isopropanol-water occurs within a rectification column forming the main part of a rectification system. The process is based on the different volatilities of the individual components. The separation occurs at the boiling temperatures of the components. The system is comprised of the rectification column, an evaporator and a condenser, and is shown in Fig. 2.



Sl. 2. *Shema rektifikacijskega sistema*
Fig. 2. *Schematic of the rectification system*

S črpalko napajalno zmes doziramo s strani v kolono. Z merilnikom pretoka uravnavamo pretok napajalne zmesi.

V koloni zmes ločujemo v lažje hlapni aceton in težje hlapno zmes izopropanol - voda. Ta se nabira na dnu kolone, kjer intenzivno vre. Za razvoj hlapov skrbi uparjalnik, skozi katerega kroži težje hlapna zmes. Hlapi iz uparjalnika se dvigujejo po koloni navzgor in na svoji poti prihajajo na površini polnil v stik s padajočo napajalno zmesjo. Zaradi intenzivnega stika med dvigajočimi hlapi in padajočo zmesjo pride do intenzivne toplotne in snovne izmenjave med njima. Iz padajoče zmesi se uparja del lažje hlapne komponente, iz dvigajočih hlapov kondenzira del težje hlapne komponente. Težje hlapljiva zmes se nabira na dnu kolone. Aceton se dviga proti vrhu kolone skozi refluksno glavo v kondenzator.

V kondenzatorju aceton kondenzira. Nastali destilat se zbira v refluksni glavi kolone. Del destilata se kot refluks preliva nazaj v kolono,

The mixture is introduced into the system using the pump. The flow into the system is adjusted in accordance with the flowmeter reading.

Inside the column the mixture is separated into acetone, which boils at a low temperature, and a mixture of isopropanol and water. The latter accumulates at the bottom of the column, where it boils intensively. The vapors are primarily formed within the evaporator, through which the heavier mixture circulates. The vapors from the evaporator rise through the column and are brought into contact with the falling input mixture. Due to the intensive contact between both flows an intensive heat and mass transfer takes place. As a result, the most volatile compound evaporates while the heavier compounds condense and flow back to the bottom of the column. The acetone rises to the top of the column through the reflux head into the condenser.

The acetone condenses inside the condenser. The resulting condensate accumulates in the reflux head of the column. Part of the liquid flows back into the column while

del pa odteka iz kolone skozi regulacijski ventil za uravnavanje refluksnega razmerja skozi hladilnik destilata v rezervoar. Pretok destilata uravnavamo z regulacijskim ventilom tako, da temperatura v glavi kolone ne naraste nad nastavljeno vrednost, ki je tik nad vreliščem acetona. Pretok težje hlapne zmesi iz dna kolone kot destilacijski preostanek krmilimo z odjemnim regulacijskim ventilom, tako da je nivo nespremenljiv. Temperatura vrelišča lažje hlapne sestavine - acetona je 56,5 °C, težje hlapne - izopropanola pa 80,3 do 82 °C.

- Sestava vhodne zmesi: aceton (75 ut. %), izopropanol (15 ut. %), voda (10 ut. %).
- Ciljna sestava destilata: aceton (95,0 ut. %), izopropanol (3,0 ut. %), voda (2,0 ut. %).
- Sestava destilacijskega preostanka: aceton (največ 5,0 ut. %), izopropanol - voda (95,0 ut. %).

Iz dolgoletnih izkušenj operaterja so v obratu, kjer obravnavana kolona deluje, postavili naslednje delovno pravilo: najmanj 95 ut. % acetona v destilatu je zagotovljeno s stalnim vzdrževanjem temperatur T_2=56-57 °C v refluksni glavi kolone in T_3=80 °C na dnu kolone. Dejavnosti operaterja pri pripravi, vklopu, obratovanju in izklopu rektifikacijske kolone so opisane v preglednici 3.

3 IDENTIFIKACIJA TEHNIČNIH ODPOVEDI IN ANALIZA Z METODO DREVESA ODPOVEDI

V literaturi [7] je moč tehnične odpovedi razdeliti na tiste, ki imajo za posledico trenutni izpust (zaradi sesutja oziroma porušitve uparjalnika/kolone/kondenzatorja, prelom cevi) in tiste, katerih posledica je stalni izpust (poškodba plašča uparjalnika/kolone/kondenzatorja, poškodba cevi). To razdelitev smo upoštevali tudi v pričujočem prispevku. V nadaljevanju tako najprej identificiramo in analiziramo odpovedi s posledico trenutnega izpusta in nato odpovedi s posledico stalnega izpusta.

Uporaba in izdelava drevesa odpovedi je dobro znana. Najti je moč več avtorjev, v konkretni analizi pa smo se naslonili na delo [8]. Izračun verjetnosti za vmesne in glavni dogodek so za vse primere izračunani s t.i. Booleanovo algebro:

vezje ALI:

$\lambda_G=\lambda_1+\lambda_2-(\lambda_1 x\lambda_2)$ … če vezje povezuje dva dogodka (1)

$\lambda_G=1-[(1-\lambda_1)x\ldots x(1-\lambda_n)]$ … če vezje povezuje *n* dogodkov (2)

vezje IN:

$\lambda_G=\lambda_1 x\lambda_2 x\ldots x\lambda_n$ (3).

λ_x … verjetnost dogodka

Verjetnosti osnovnih dogodkov za rektifikacijski sistem ločevanja mešanice aceton-izopropanol - voda, ki smo jih povzeli po [7], so bile

another part of the liquid flows from the column through the control valve enabling the control of the reflux ratio through the condensate cooler into the reservoir. The actual flow of the liquid is controlled in such a fashion that the temperature within the reflux head does not rise above a preset value that is just above the acetone's boiling point. The flow of the heavier compound from the bottom of the column (bottom product) as well as the distillation bottom product is manipulated by the control valve in order to obtain an approximately constant level. The boiling point of the lighter compound, acetone, is 56.5°C, the boiling point of the heavier isopropanol is 80.3–82 °C.

- The input fluid is comprised of acetone (75% w.), isopropanol (15% w.), and water (10% w.).
- The desired distillate contains acetone (95% w.), isopropanol (3 % w.), water (2% w.)
- The distillation bottom-product contains acetone (5% w. max.), isopropanol-water (95% w.)

To achieve the best result the following rule has been established, based on several years' worth of observation: a minimum of 95% w. of acetone in the distillate is ensured with a constant temperature T_2=56–57 °C in the reflux head of the column and T_3=80 °C in the bottom of the column. The activities of the operator during preparation – turning on and turning off the rectification column – are described in Table 3.

3 IDENTIFICATION OF TECHNICAL FAILURES AND THE FAULT-TREE ANALYSIS

The literature [7] distinguishes between technical failures that result in an instantaneous release as a result of evaporator, column, condenser, or tube failure, and technical failures that result in a continuous release (damage to the shell of the evaporator, column, condenser, or tube). This division was also used in this study. Below, we identify and analyze the failures that result in an instantaneous release, and then the failures that result in a continuous release.

The use of a failure tree is well known. There are several authors who have explored this method in detail; however, this analysis was based on work by [8]. The computation of the probability for the top and intermediate events are calculated using the so-called Boolean algebra, as follows:

OR gates:

$\lambda_G=\lambda_1+\lambda_2-(\lambda_1 x\lambda_2)$ … if the gate connects two events (1)

$\lambda_G=1-[(1-\lambda_1)x\ldots x(1-\lambda_n)]$ … if the gate connects several (*n*) events (2)

AND gates:

$\lambda_G=\lambda_1 x\lambda_2 x\ldots x\lambda_n$ (3).

λ_x … probability of event

The probabilities of the top events for the rectification system for separating acetone-isopropanol-water were taken from [7] and adjusted

Preglednica 1. *Verjetnosti osnovnih dogodkov opisanega rektifikacijskega sistema*
Table 1. *Basic events probability of described rectification system*

DOGODEK EVENT	VERJETNOST DOGODKA PROBABILITY OF EVENT
prelom napajalne cevi uparjalnika (D=90 mm, l=0,5 m) reboiler feed line rupture (D=90 mm. l=0.5 m)	$1{,}3\times10^{-7}$ /leto (year)
puščanje napajalne cevi uparjalnika (D=90 mm, l=0,5 m) reboiler feed line leak (D=90 mm. l=0.5 m)	$2{,}7\times10^{-6}$ /leto (year)
prelom napajalne cevi kolone (D=30 mm, l=4 m) column feed line rupture (D=30 mm. l=4 m)	$3{,}5\times10^{-6}$ /leto (year)
puščanje napajalne cevi kolone (D=30 mm, l=4 m) column feed line leak (D=30 mm. l=4 m)	$3{,}5\times10^{-5}$ /leto (year)
prelom odvodne cevi iz dna kolone (D=90 mm, l=1,3 m) column bottom discharge line rupture (D=90 mm. l=1.3 m)	$3{,}4\times10^{-7}$ /leto (year)
puščanje odvodne cevi iz dna kolone (D=90 mm, l=1,3 m) column bottom discharge line leak (D=90 mm. l=1.3 m)	$6{,}9\times10^{-6}$ /leto (year)
prelom odvodne cevi iz vrha kolone (D=30 mm, l=12 m) column top discharge line rupture (D=30 mm. l=12 m)	$1{,}0\times10^{-5}$ /leto (year)
puščanje odvodne cevi iz vrha kolone (D=30 mm, l=12 m) column top discharge line leak (D=30 mm. l=12 m)	$1{,}0\times10^{-4}$ /leto (year)
sesutje uparjalnika/kolone/kondenzatorja column/reboiler/condenser rupture	$6{,}5\times10^{-6}$ /leto (year)
puščanje plašča uparjalnika/kolone/kondenzatorja column/reboiler/condenser shell leak	$1{,}0\times10^{-5}$ /leto (year)

preračunane glede na dolžine dejanskih cevi in so prikazane so v preglednici 1.

3.1 Trenutni izpust

Shema drevesa odpovedi za trenutni izpust je prikazana na sliki 3. Na vrhu je glavni dogodek ("top event"), katerega verjetnost ocenjujemo, pod njim pa tisti dogodki, ki na verjetnost odpovedi vplivajo. Z vezjem ALI poudarimo, da se dogodek (odpoved) nad vezjem ALI zgodi, če se zgodi katerikoli od dogodkov, ki jih vezje ALI povezujejo, z vezjem IN pa, da se dogodek nad vezjem IN zgodi, če se zgodijo vsi dogodki, ki so med seboj povezani z vezjem IN.

Že ta del kaže, da rektifikacijski sistem ni v zadostni meri opremljen z varnostnimi sistemi, če seveda so verjetnosti odpovedi posameznega podsistema nesprejemljive, saj bo verjetnost odpovedi celotnega sistema kvečjemu višja od verjetnosti odpovedi posameznega podsistema.

3.2 Stalni izpust in rezultati analize drevesa odpovedi

Shema drevesa odpovedi za stalni izpust je prikazana na sliki 4. Preglednica 2 kaže rezultate za verjetnost trenutnega in kontinuiranega izpusta v obeh primerih, izračunane z enačbama (1) in (2) za posamezne primere s slik 3 in 4.

4 IDENTIFIKACIJA ČLOVEŠKIH NAPAK Z UPORABO OSNOVNE IN RAZŠIRJENE METODE CREAM

V nadaljevanju prikazujemo identifikacijo človeških napak in njihovo analizo z uporabo

for the actual lengths of the pipes. The results are shown in Table 1.

3.1 Instantaneous release

The failure-tree schematic for an instantaneous release is shown in Fig. 3. On the top there is an event, the probability of whhich one wishes to estimate. Below the top event there are events that influence the top event. An OR gate connects events where each event connected occurring causes the event above the gate to occur while an AND gate connects events where all events connected occurring causes the event above the gate to occur.

The rare use of AND gates in the presented case shows that the rectification system is not sufficiently equipped with safety features (provided that failures of subsystems are not acceptable) as the probability of failure of the total system could only be higher than the probability of failure of a particular subsystem.

3.2 Continuous release and the results of the fault-tree analysis

The fault-tree schematic for a continuous release is shown in Fig. 4. Table 2 shows results for the probability of instantaneous and continuous releases in both cases calculated using Eqs. (1) and (2) for the cases in Figs. 3 and 4.

4 IDENTIFICATION OF HUMAN ERRORS USING BASIC AND EXTENDED CREAM METHODS

Below, we examine the identification of human errors and their analysis using the basic and extended

osnovne in razširjene metode ASZN, ki jo povzemamo po [5], in sicer najprej z osnovno metodo, ki jo dogradimo še z razširjeno metodo.

4.1 Analiza po osnovni metodi ASZN

Osnovna metoda sestoji iz naslednjih treh stopenj:

- opis naloge ali dela naloge, ki ju analiziramo in opravimo tako, da posamezno nalogo razčlenimo na njene sestavne dele, podobno kakor je to za verjetnost odpovedi, opravljeno z uporabo drevesa odpovedi (preglednica 3),
- ocena splošnih pogojev dela[4], pri čemer za vsakega od predstavljanih pogojev dela izberemo primerno vrednost (preglednica 4),
- določitev verjetnega načina nadzora[5] (preglednica 5).

CREAM methodology by [5].

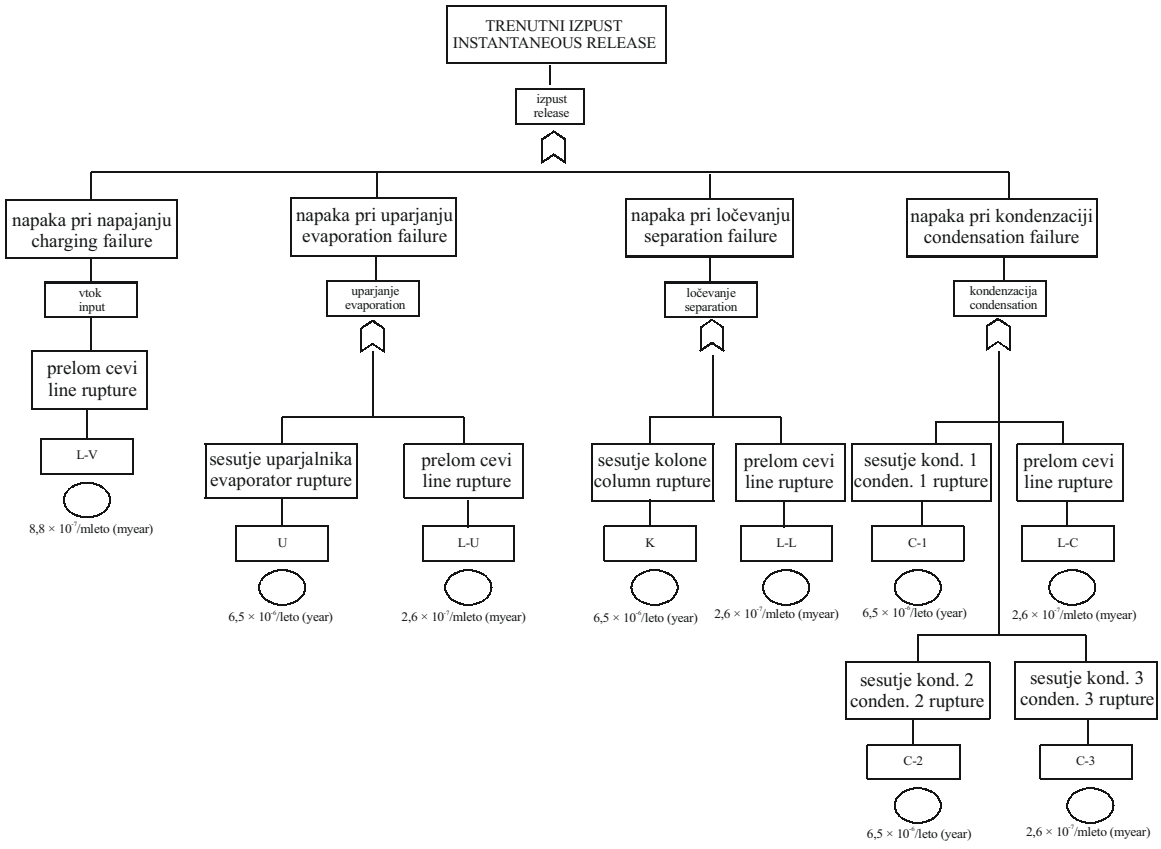
4.1 Analysis using the basic CREAM method

The basic method comprises the following three levels:

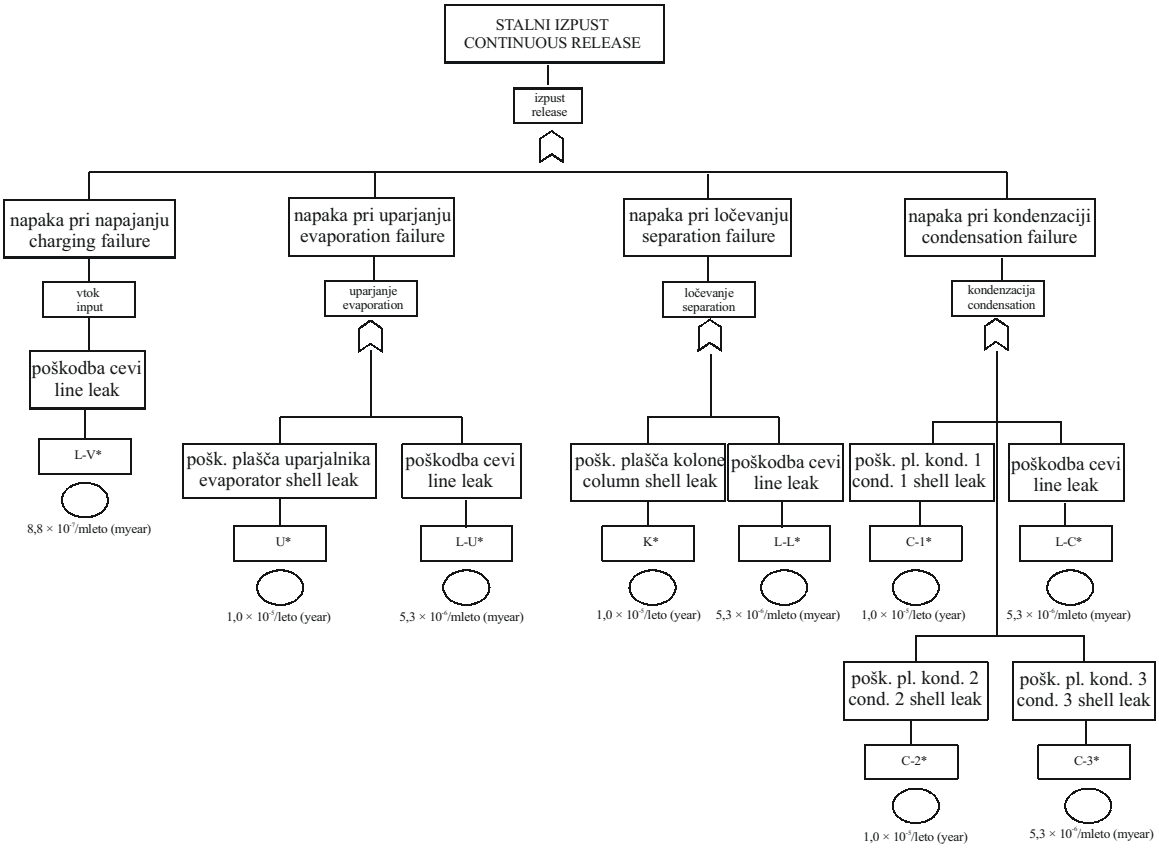
- description of the task or part of the task subject to analysis which is performed by breaking down particular tasks into their components in a similar fashion as done with failures using the fault-tree analysis, Table 3,
- assessment of common performance conditions[4] where a suitable value for each of the conditions of work is selected, Table 4,
- selection of probable control mode[5] , Table 5.

Preglednica 2. *Rezultati analize za trenutni in stalni izpust*
Table 2. *Results of analysis for instantaneous and continuous release*

NAPAKA FAILURE	VERJETNOST NAPAKE - p PROBABILITY OF FAILURE - p
trenutni izpust instantaneous release	$4{,}6x10^{-5}$
stalni izpust continuous release	$2{,}0x10^{-4}$



Sl. 3. *Drevo napak - trenutni izpust*
Fig. 3. *Fault tree – instantaneous release*



Sl. 4. *Drevo napak - stalni izpust*
Fig. 4. *Fault tree – continuous release*

V preglednici 3 je prikazano zaporedje dejavnosti pri pripravi, vklopu, obratovanju in izklopu rektifikacijskega sistema. Vidimo lahko, da so identificirane zlasti aktivnosti, katerih odsotnost bi povzročila napake v delovanju (primer: če so povezave med kolono in rezervoarji za destilat in destilacijski ostanek odprte, ima to negativne posledice za končni rezultat procesa). Iz navedenega je jasno razvidna potreba po obstoju tehnoloških postopkov, ki se jih operaterji zahtevnih procesnih sistemov držijo pri nadzoru delovanja teh sistemov.

Splošni pogoji dela dajo obširno in dobro strukturirano bazo za karakterizacijo razmer, v katerih izvajamo določeno nalogo. Za vsako vrsto delovnih pogojev je treba določiti ustrezno stopnjo. Vsaki stopnji ustreza pričakovan vpliv na zanesljivost dela, kakor je določeno v preglednici 4, povzeti po [5]. Pri tem so s krepkim tiskom označene vrednosti, ki smo jih upoštevali za izračun obravnavane rektifikacijske kolone.

Verjeten način nadzora določimo z oceno splošnih pogojev dela in določitvijo pričakovanega vpliva na zanesljivost izvedbe. Oceno splošnih pogojev dela prikažemo kot trojico [∑zmanjšan, ∑brez posebnosti, ∑izboljšan]. Slika 5 prikazuje povezavo med splošnimi pogoji dela in načinom nadzora. Način nadzora določimo glede na polje, v katerem je presečišče vrednosti ∑izboljšan in ∑zmanjšan [5].

Table 3 shows activities during the preparation, operation, and turning off of the rectification system. We see that the activities, the lack of which could cause errors during the operation, are noted (i.e. if the connections between the column and reservoirs for distillate remain open this is detrimental to the final result of the process). Therefore, a need for clearly defined guidelines for system control is shown.

Common performance conditions give a broad and well-structured basis for the characterization of conditions under which a particular task is performed. For each type of performance conditions one needs to define an appropriate level. Each level is associated with performance reliability, as defined in Table 4, according to Hollnagel [5], 1998. In Table 4 the conditions used for the actual calculations are written in bold.

The probable control mode is defined using an assessment of common performance conditions and selecting the expected influence on the reliability of performance. Common performance conditions are shown as a triplet [Σreduced, Σnot significant, Σimproved]. Fig. 5 depicts the relationship between the common performance conditions and the control mode. The control mode is defined according to the intersection of Σreduced and Σimproved [5].

Preglednica 3. *Zaporedje dejavnosti pri pripravi, vklopu, obratovanju in izklopu rektif. sistema*
Table 3. *Sequence of activities for preparing, start, operation and stopping of the rectification system*

OZNAKA MARK	CILJ GOAL	DEJAVNOST ACTIVITY
1.0	Priprava sistema Preparing of the system	
1.1		Preverimo, ali so odprte povezave med kolono in rezervoarji za destilat in destilacijski ostanek. Check if connections between column and tanks of destillate and distillatory residue are open.
1.2		Zapremo ventile za odvzem destilata in destilacijskega ostanka. Close valves for destillate and distillatory residue taking away.
2.0	Vklop sistema Start of the system	
2.1		Vključimo črpalko za kroženje glikola v kondenzatorjih. Start the pump for glycol circulation in condensers.
2.2		Vklopimo napajalno črpalko in napolnimo uparjalnik z mešanico topil. Start the feeder pump and fill up reboiler with components mixture.
2.3		Ko mešanica topil prekrije grelnik uparjalnika, odpremo ventil za gretje uparjalnika. When components mixture cover reboiler heater, open valve for reboiler heating.
3.0	Obratovanje sistema Operation of the system	
3.1		Kolona mora vsaj 30 min delovati pri popolnem refluksu brez napajanja. The column has to operate at least 30 minutes by full reflux without feeding.
3.2		Odpremo ventil za odvzem destilata in destilacijskega ostanka. Open valves for destillate and distillatory residue.
3.3		Napajalno črpalko naravnamo na pretok 300 l/h. Feeder pump set for flow 300 l/h.
3.4		Temperaturo v refluksni glavi uravnavamo z ventilom za odvzem destilata na 56 °C. Control temperature in reflux head with valve for destillate taking away at 56°C.
3.5		Temperaturo na dnu kolone uravnavamo z ventilom za odvzem destilacijskega ostanka na 80 °C. Control temperature in column bottom with valve for distillatory residue taking away at 80 °C.
4.0	Izklop sistema Stopping of the system	
4.1		Izklopimo napajalno črpalko. Stop feeder pump.
4.2		Zapremo ventil za gretje uparjalnika. Close valve for reboiler heating.
4.3		Zapremo ventil za odvzem destilacijskega ostanka. Close valve for distillatory residue taking away.
4.4		Odpremo ventil za odvzem destilata. Open valve for destillate taking away.
4.5		Izklopimo črpalko za kroženje glikola v kondenzatorjih. Stop pump for glycol circulation in condensers.

Ob koncu osnovne metode je treba določiti območje zanesljivosti za vsakega od načinov nadzora, ki so uporabni v primeru obravnavanega rektifikacijskega sistema.

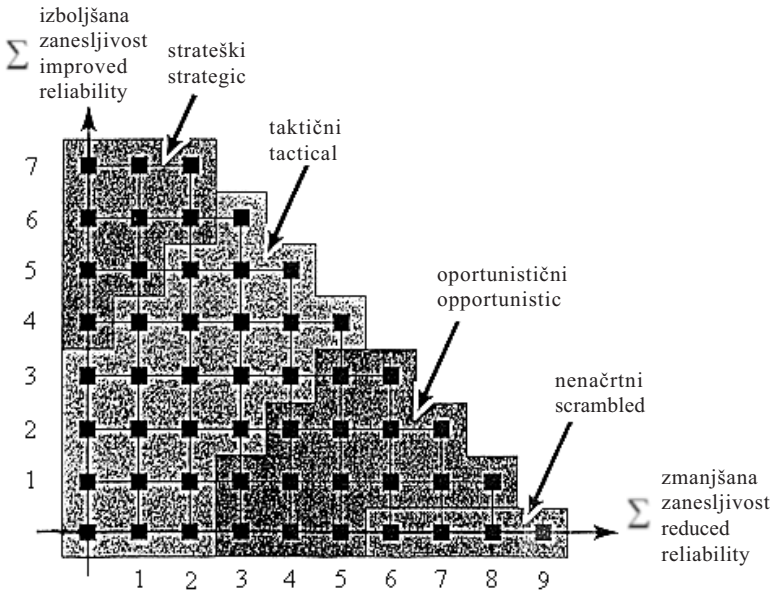
Za obravnavani sistem smo ugotovili, da zanj velja trojka [∑zmanjšan, ∑brez posebnosti, ∑izboljšan] = [0,5,4]. Ugotovimo lahko, da je presečišče vrednosti ∑zmanjšan in ∑izboljšan v polju, kjer je način nadzora strateški. Preglednica 5 kaže zanesljivostno območje za strateški način nadzor:

The final result of the basic method is the interval of reliability for each of the control modes used in the case of the rectification system as analyzed in this contribution.

For the system analyzed in this contribution we found the triplet [Σreduced, Σnot significant, Σimproved] = [0,5,4] to be valid. This gives a strategic control mode area of intersection between Σreduced and Σimproved. Table 5 presents the reliability interval for the strategic control mode as:

Preglednica 4. *Splošni pogoji dela in pričakovan vpliv na zanesljivost dela za obravnavani sistem*
Table 4. *Common performance conditions and expected effect on performance reliability for relevant system*

VRSTA DELOVNIH RAZMER COMMON PERFORMANCE CONDITIONS	OPIS EVALUATION	STOPNJA LEVEL	PRIČAKOVAN VPLIV NA ZANESLJIVOST DELA EXPECTED EFFECT ON PERFORMANCE RELIABILITY
Primerna organiziranost	kakovost podpore in namenjena sredstva organizacije, za opravljanje naloge; vključujoč komunikacijski sistem, sistem varstva pri delu	zelo učinkovit	izboljšan
		učinkovit	**brez posebnosti**
		neučinkovit	zmanjšan
		pomanjkljiv	zmanjšan
Adequacy of organisation	The quality of the support and resources provided by the organisation for the task being performed. This includes commu. system, Safety Management System.	very efficient	improved
		efficient	**not significant**
		inefficient	improved
		deficient	improved
Delovne razmere	osvetljenost prostora, bleščanje na zaslonih, hrup alarmov, motnje iz procesa, …	ugoden	izboljšan
		znosen	**brez posebnosti**
		neznosen	zmanjšan
Working conditions	Ambient lighting, glare on screens, noise from alarms, interruptions from the task, etc.	advantageous	improved
		compatible	**not significant**
		incompatible	improved
Primerna zaščita človeka pred strojem in operativna podpora	kakovost zaščite človeka pred strojem, informacije, dosegljive na nadzornih ploščah, računalniško vodenje	v pomoč	izboljšan
		primeren	brez posebnosti
		znosen	**brez posebnosti**
		neprimeren	zmanjšan
Adequacy of MMI and operational support	The quality of of the MMI, control panels, workstations.	supportive	improved
		adequate	not significant
		tolerable	**not significant**
		inappropriate	improved
Razpolaganje s postopki	razpolaganje s postopki in načrti, ki vključujejo operativna in nepričakovana stanja	**primeren**	**izboljšan**
		sprejemljiv	brez posebnosti
		neprimeren	zmanjšan
Availability of procedures/planes	The availability of prepared guideance for the work to be carried out, emergency proced..	**appropriate**	**improved**
		acceptable	not significant
		inappropriate	improved
Število hkratnih nalog	število nalog, ki jih mora delavec opraviti ali biti pozoren v istem času	pod zmožnostmi	brez posebnosti
		primerno zmožnostim	**brez posebnosti**
		nad zmožnostmi	zmanjšan
Number of simultaneous goals	The number of tasks or goals operators must attend to.	fewer than capacity	not significant
		matching curr. capacity	**not significant**
		more than capacity	improved
Razpoložljiv čas	čas, ki je na voljo za izvedbo naloge	**primeren**	**izboljšan**
		začasno neprimeren	brez posebnosti
		stalno neprimeren	zmanjšan
Available time	The time available to complete the work.	**adequate**	**improved**
		temporarily inadequate	not significant
		continuously inadequate	improved
Čas dneva	čas, v katerem je naloga opravljena	**dnevni čas**	**brez posebnosti**
		nočni čas	zmanjšan
Time of dav	The time at which the task is carried out.	**dav-time**	**not significant**
		night-time	improved
Primerna usposobljenost in izkušnje	raven in kakovost usposobljenosti operaterja, seznanitev z novo tehnologijo, ponavljanje starih spretnosti, stopnja operaterjeve izkušenosti	**primeren, zelo izkušen**	**izboljšan**
		primeren, omejeno izk.	brez posebnosti
		neprimeren	zmanjšan
Adequacy of training and preparation	The level of readiness for the work. Includes familiarisation to new technology, refreshing old skills, the level of operational experience.	**adequate, very experience**	**improved**
		adequate, lim. experience	not significant
		inadequate	improved
Kakovost sodelovanja v skupini	kakovost sodelovanja članov skupine, stopnja zaupanja, splošno počutje članov v skupini	**zelo učinkovit**	**izboljšan**
		učinkovit	brez posebnosti
		neučinkovit	brez posebnosti
		pomanjkljiv	zmanjšan
Crew collaboration quality	The quality of the collaboration. between crew members, the level of trust, the general social climate among crew members.	**very efficient**	**improved**
		efficient	not significant
		inefficient	not significant
		deficient	improved



Sl. 5. *Povezava med splošnimi pogoji dela in načinom nadzora [5]*
Fig. 5. *Relations between common performance conditions and control modes by [5]*

Preglednica 5. *Način nadzora in zanesljivostno območje [5]*
Table 5. *Control modes and probability intervals [5]*

NAČIN NADZORA CONTROL MODE	ZANESLJIVOSTNO OBMOČJE (VERJETNOST NAPAKE) RELIABILITY INTERVAL (PROBABILITY OF ACTION FAILURE)
strateški strategic	$0{,}5x10^{-5} < p < 1{,}0x10^{-2}$
taktični tactical	$1{,}0x10^{-3} < p < 1{,}0x10^{-1}$
oportunistični opportunistic	$1{,}0x10^{-2} < p < 0{,}5$
nenačrtni scrambled	$1{,}0x10^{-1} < p < 1{,}0$

$$0{,}5x10^{-5} < p < 1{,}0x10^{-2}$$

Ker je verjetnost človeške napake reda velikosti verjetnosti odpovedi rektifikacijskega sistema oz. je večja, je bilo treba analizo nadaljevati z razširjeno metodo CREAM.

4.2 Analiza z razširjeno metodo ASZN

Namen razširjene metode ASZN [5] je, da natančneje ovrednotimo posamezne prispevke k skupni človeški napaki in jo uporabimo takrat, ko je človeška napaka enakovredna ali pomembnejša od tehnične napake, ovrednotene po osnovni metodi ASZN.

V postopku izvedbe razširjene metode ASZN opravimo naslednje dejavnosti:

- določimo poznavalne dejavnosti[6], preglednica 6,
- identificiramo najverjetnejše napake poznavalne funkcije[7], preglednica 7,
- določimo verjetnost napake za vsako verjetno napako poznavalne funkcije za rektifikacijski sistem, preglednica 8,

As the probability of human error exceeds that of technical failure we continued the analysis with the extended CREAM methodology.

4.2 Extended CREAM methodology analysis

The extended Cognitive Reliability and Error Analysis Method (Extended CREAM) was designed by Hollnagel [5] as a tool to improve quantification of particular contributions to common human error and is used when the human-error probability assessed with basic CREAM equals or is greater than the technical failure probability.

In order to perform the extended CREAM the following activities should be undertaken:

- define cognitive demands[6], Table 6,
- identify cognitive function failures[7], Table 7,
- define cognitive failure probability, Table 8,

- določimo uravnane verjetnosti napak poznavalnih funkcij[8] za rektifikacijski sistem, preglednica 10.

Tako določeno vrednost napake lahko nato vključimo v drevo odpovedi in jo obravnavamo enako kakor smo obravnavali verjetnost okvare (napake iz tehničnih vzrokov).

Najprej smo na podlagi generičnih poznavalnih dejavnosti definirali poznavalne dejavnosti z zahtevami poznavanja za rektifikacijski sistem. Ugotovimo lahko, da je za rektifikacijski sistem največja zahteva po izvajanju, temu pa sledita opazovanje in razlaga. Preglednica 6 prikazuje poznavalne dejavnosti z zahtevami poznavanja za rektifikacijski sistem.

V nadaljevanju določimo najverjetnejše napake poznavalnih funkcij, uporabljenih za obravnavani rektifikacijski sistem, kar je prikazano v preglednici 7.

V nadaljevanju določimo še nominalne verjetnosti napak poznavalnih funkcij. Te lahko določimo na temelju lastnih opazovanj ali na temelju dosegljivih podatkov iz literature. V konkretnem primeru smo verjetnosti povzeli po [5], ki podaja osnovne vrednosti ter skrajne meje območij.

Iz vpliva splošnih delovnih pogojev na nominalno verjetnost napake poznavalne funkcije za rektifikacijski sistem določimo splošni uravnalni faktor (SUF) kot zmnožek posameznih uravnalnih faktorjev (UF[9]), kar storimo na podlagi utežnih količnikov uravnalnih faktorjev v skladu z razširjeno metodologijo ASZN. Izračun SUF je prikazan v preglednici 9.

Končna vrednost uravnane verjetnosti napake poznavalnih funkcij (UVNPF) je zmnožek skupnega uravnalnega faktorja in nominalne verjetnosti napake poznavalnih funkcij (NVNPF). Uravnane verjetnosti napak poznavalnih funkcij za rektifikacijski sistem so prikazane v preglednici 10.

V drevesi odpovedi za trenutni (sl. 3) in stalni izpust (sl. 4) so vključeni osnovni dogodki, ki so posledica človeških napak. Drevo odpovedi s tehničnimi in človeškimi napakami za trenutni izpust je na sliki 6. V drevesi odpovedi so vključene samo človeške napake, ki imajo za posledico trenutni ali stalni izpust tekočinske mešanice iz rektifikacijskega sistema.

5 SINTEZA VERJETNOSTI NEZGODE (ČLOVEŠKE NAPAKE) IN OKVARE (TEHNIČNE NAPAKE) V DREVESU ODPOVEDI

Na obravnavani način smo dobili vrednosti za verjetnosti človeških (nezgod) in mehanskih (okvar) napak, ki jih je moč uvrstiti v drevo odpovedi. Na sliki 6 je prikazano drevo odpovedi za trenutni izpust, na sliki 7 pa drevo odpovedi za stalni izpust. Prednost prikazanega je prav v uravnoteženju (deanimaciji[1]) objektivnih dogodkov (okvar) in subjektivnih dogodkov z objektivnimi posledicami (nezgod).

Zdaj je mogoče z uporabo že prikazane Booleove algebre ponovno ovrednotiti vse rezultate z upoštevanjem in brez upoštevanja človeških napak,

- define adjusted cognitive failure probability[8], Table 10.

The final result is a quantified human-error probability, which can be included in a fault tree and treated as any other failure probability to arrive at a final combined value for failure probability.

In order to arrive at the final result, we first define the cognitive demands based on generic cognitive demands. For our case, the execute cognitive demand was most frequently followed by observation and interpretation. The demands are summarized in Table 6.

Then we defined the cognitive function failures most likely to occur in the system at hand.The results are summarized in Table 7.

Further, we define the nominal cognitive failure probability. This can be defined based on our own observation or on published results. In our case we relied on the values of [5] who published basic values and upper and lower limits.

Based on the effect of common performance conditions on cognitive function failures for the rectification system under observation we can define a common weighting factor as a product of weighting factors[9] using the process shown in Table 9.

The final value of the adjusted cognitive failure probability is the product of a common weighting factor and the nominal cognitive failure probability. These values are shown in Table 10.

As a result, we have modified the fault trees for instantaneous (Fig.3) and continuous (Fig. 4) releases to include adjusted cognitive failure probabilities for both cases, shown in Fig. 6 for the instantaneous release case, and Fig. 7 for the continuous release case.

5 SYNTHESIS OF HUMAN-ERROR AND TECHNICAL FAILURE PROBABILITIES IN A FAULT TREE

In the preceding sections we have shown the process of obtaining human-error and technical failure probabilities. The results can be inserted in a fault tree in order to compare the influence of either component. Fig. 6 shows a fault tree for instantaneous release, and Fig. 7 for continuous release. The advantage of the presented synthesis is in the deanimation[10] of the objectively perceived events and the subjectively perceived human errors resulting in objectively perceived consequences of human errors (i.e. accidents)

Now, we can re-evaluate the results already

Preglednica 6. *Poznavalne dejavnosti z zahtevami poznavanja rektifikacijskega sistema*
Table 6. *Cognitive activity with cognitive demand for rectification system*

#	DEJAVNOST ACTIVITY	POZNAVALNA DEJAVNOST COGNITIVE ACTIVITY	O	IN	N	I
1.1	Preverimo, ali so odprte povezave med kolono in rezervoarji za destilat in destilacijski ostanek. Check if connections between column and tanks of destillate and distillatory residue are open.	Preveri Verify	*	*		
1.2	Zapremo ventile za odvzem destilata in destilacijskega ostanka. Close valves for destillate and distillatory residue taking away.	Izvedi Execute				*
2.1	Vključimo črpalko za kroženje glikola v kondenzatorjih. Start the pump for glycol circulation in condensers.	Izvedi Execute				*
2.2	Vklopimo napajalno črpalko in napolnimo uparjalnik z mešanico topil. Start the feeder pump and fill up reboiler with components mixture.	Izvedi Execute				*
2.3	Ko mešanica topil prekrije grelnik uparjalnika, odpremo ventil za gretje uparjalnika. When components mixture cover reboiler heater, open valve for reboiler heating.	Krmili Control	*			*
3.1	Kolona mora vsaj 30 min delovati pri popolnem refluksu brez napajanja. The column has to operate at least 30 minutes by full reflux without feeding.	Nadzoruj Monitor	*	*		
3.2	Odpremo ventil za odvzem destilata in destilacijskega ostanka. Open valves for destillate and distillatory residue.	Izvedi Execute				*
3.3	Napajalno črpalko naravnamo na pretok 300 l/h. Feeder pump regulate at flow 300 l/h.	Izvedi Execute				*
3.4	Temperaturo v refluksni glavi uravnavamo z ventilom za odvzem destilata na 56 °C. Control temperature in reflux head with valve for destillate taking away at 56°C.	Krmili Control	*			*
3.5	Temperaturo na dnu kolone uravnavamo z ventilom za odvzem destilacijskega ostanka na 80 °C. Control temperature in column bottom with valve for distillatory residue taking away at 80 °C.	Krmili Control	*			*
4.1	Izklopimo napajalno črpalko. Stop feeder pump.	Izvedi Execute				*
4.2	Zapremo ventil za gretje uparjalnika. Close valve for reboiler heating.	Izvedi Execute				*
4.3	Zapremo ventil za odvzem destil. ostanka. Close valve for distillatory residue taking away.	Izvedi Execute				*
4.4	Odpremo ventil za odvzem destilata. Open valve for destillate taking away.	Izvedi Execute				*
4.5	Izklopimo črpalko za kroženje glikola v kond. Stop pump for glycol circulation in condensers.	Izvedi Execute				*

Oznake: O – opazovanje, IN – interpretacija, N – načrtovanje, I – izvedba
Mark: O – observation, IN – interpretation, N – planning, I – execution

prikazanih v preglednici 2. Rezultati so prikazani v preglednici 11.

Ugotovimo lahko, da človeške napake v mejah postavljenih predpostavk ne vplivajo na verjetnost trenutnega izpusta, skoraj za faktor 25 pa povečajo verjetnost stalnega izpusta.

shown before with and without the human errors shown in Table 2. The results are shown in Table 11.

We deduce that human errors do not influence (within the limits of the assumptions) instantaneous release while they increase the probability of continuous release almost 25 fold.

Preglednica 7. *Verjeten način napak poznavalnih funkcij rektifikacijskega sistema*
Table 7. *Potential cognitive function failures for rectification system*

#	POZNAVALNA DEJAVNOST COGNITIVE ACTIVITY	opazovanje observation			razlaga interpretation			načrtovanje planning		izvedba execution				
		O1	O2	O3	IN1	IN2	IN3	N1	N2	I1	I2	I3	I4	I5
1.1	Preveri Verify			*										
1.2	Izvedi Execute									*				
2.1	Izvedi Execute													*
2.2	Izvedi Execute										*			
2.3	Krmili Control			*										
3.1	Nadzoruj Monitor			*										
3.2	Izvedi Execute										*			
3.3	Izvedi Execute			*										
3.4	Krmili Control									*				
3.5	Krmili Control									*				
4.1	Izvedi Execute													*
4.2	Izvedi Execute													*
4.3	Izvedi Execute												*	
4.4	Izvedi Execute												*	
4.5	Izvedi Execute											*		

Ob analizi verjetnosti stalnega izpusta ugotovimo, da z vidika človeške napake nanjo vplivajo naslednje vrste napak poznavalne funkcije:
- brez izpolnitve
- napačna izpolnitev (2x).

Bistveno vprašanje, ki se zastavi operaterju rektifikacijskega sistema, je tedaj, kako napake zmanjšati ali odpraviti. Kar se tiče okvar, so postopki znani in preskušeni ter zaobseženi v načelih obvladovanja kakovosti. Glede nezgod pa bi bilo najprej smiselno ugotoviti, ali bi bilo nezgode moč omejiti tako, da bi jih iz potencialnih nezgod prekvalificirali v potencialne okvare, da bi torej razosebili njihov vir. To bi bilo najpreprosteje moč storiti z avtomatizacijo posameznih elementov delovanja rektifikacijskega sistema - torej zamenjavo človeške podpore s strojno podporo. Ker pa namen tega prispevka ni predlagati dejanske izvedbene tehnike, temveč le prikazati orodje in metodologijo za objektivno analizo sicer subjektivnih vprašanj, se s tem nismo bolj poglobljeno ukvarjali.

Glede same verjetnosti človeške napake pa menimo, da jo bo brez prekvalifikacije oz. zamenjave človeka z napravo moč najbolj zmanjšati v primeru

Further analysis of the continuous release shows that the following cognitive function failures are the main contributors to the human error:
- missed action
- action of the wrong type (2x)

The main question which the operator needs to answer is how to reduce or eliminate failures. As far as technical failures are concerned there are a number of procedures that are known under the umbrella of quality management. As far as human errors are concerned they should first be deanimated by switching them (conceptually and actually) from potential accidents into potential failures. This can be achieved by changing the human involvement with devices such as the automation of elements of the rectification system. As this is beyond the scope of this study we did not further explore the actual switch but it should, in our opinion, be performed at some point in the future.

Regarding human error itself, and short of changing the human operator with a device, the following actions should be performed to reduce failure rates:
- produce and use quality procedures and technical guidelines for operation,

Preglednica 8. *NVNPF osnovnih napak poznavalnih funkcij rektifikacijskega sistema*
Table 8. *Nominal Cognitive Failur Probabilities (NCFP) of basic cognitive function failures for rectification system*

#	DEJAVNOST ACTIVITY	VRSTA NAPAKE ERROR MODE	NVNPF NCFP
1.1	Preverimo, ali so odprte povezave med kolono in rezervoarji za destilat in destilacijski ostanek. Check if connections between column and tanks of destillate and distillatory residue are open.	O3 brez opazovanja observation not made	$7{,}0x10^{-2}$
1.2	Zapremo ventile za odvzem destilata in destilacijskega ostanka. Close valves for destillate and distillatory residue taking away.	I1 napačna izpolnitev action of wrong type	$3{,}0x10^{-3}$
2.1	Vključimo črpalko za kroženje glikola v kondenzatorjih. Start the pump for glycol circulation in condensers.	I5, brez izpolnitve missed action	$3{,}0x10^{-2}$
2.2	Vklopimo napajalno črpalko in napolnimo uparjalnik z mešanico topil. Start the feeder pump and fill up reboiler with components mixture.	I2 nepravočasna izpolnitev action at wrong time	$3{,}0x10^{-3}$
2.3	Ko mešanica topil prekrije grelnik uparjalnika, odpremo ventil za gretje uparjalnika. When components mixture cover reboiler heater, open valve for reboiler heating.	O3 brez opazovanja observation not made	$7{,}0x10^{-2}$
3.1	Kolona mora vsaj 30 min delovati pri popolnem refluksu brez napajanja. The column have to operate at least 30 minutes by full reflux without feeding.	O3 brez opazovanja observation not made	$7{,}0x10^{-2}$
3.2	Odpremo ventil za odvzem destilata in destilacijskega ostanka. Open valves for destillate and distillatory residue.	I2 nepravočasna izpolnitev action at wrong time	$3{,}0x10^{-3}$
3.3	Napajalno črpalko naravnamo na pretok 300 l/h. Feeder pump set for flow 300 l/h.	O3, brez opazovanja observation not made	$7{,}0x10^{-2}$
3.4	Temperaturo v refluksni glavi uravnavamo z ventilom za odvzem destilata na 56 °C. Control temperature in reflux head with valve for destillate taking away at 56°C.	I1 napačna izpolnitev action of wrong type	$3{,}0x10^{-3}$
3.5	Temperaturo na dnu kolone uravnavamo z ventilom za odvzem destilacijskega ostanka na 80 °C. Control temperature in column bottom with valve for distillatory residue taking away at 80 °C.	I1 napačna izpolnitev action of wrong type	$3{,}0x10^{-3}$
4.1	Izklopimo napajalno črpalko. Stop feeder pump.	I5, brez izpolnitve missed action	$3{,}0x10^{-2}$
4.2	Zapremo ventil za gretje uparjalnika. Close valve for reboiler heating.	I5, brez izpolnitve missed action	$3{,}0x10^{-2}$
4.3	Zapremo ventil za odvzem destilacijskega ostanka. Close valve for distillatory residue taking away.	I4, napačno zaporedje izpolnitev action out of sequence	$3{,}0x10^{-3}$
4.4	Odpremo ventil za odvzem destilata. Open valve for destillate taking away.	I4, napačno zaporedje izpolnitev action out of sequence	$3{,}0x10^{-3}$
4.5	Izklopimo črpalko za kroženje glikola v kondenzatorjih. Stop pump for glycol circulation in condensers.	I2, nepravočasna izpolnitev action at wrong time	$3{,}0x10^{-3}$

upravljanja rektifikacijske kolone:
- z izdelavo kakovostnih tehničnih navodil za delo in
- občasnim usposabljanjem upravljalca.

V navodila in usposabljanje je treba vključiti tudi neobičajne dogodke, katerih posledice so odvisne predvsem od hitre in prisebne reakcije upravljalca. Tudi sestava takih scenarijev je zunaj želenega dometa tega prispevka in pravzaprav spada v študij dela.

- education and training of the operator.

Procedures and guidelines should include unusual events, the consequences of which are primarily dependent on the rapid reaction of the operator. The scenarios, however, which could be included in this venue is outside of the scope of this study and should be performed by people involved in human-resources management.

Preglednica 9. *Vpliv splošnih delovnih razmer na nominalno verjetnost napake poznavalnih funkcij rektifikacijskega sistema*
Table 9. *Effects of common performance conditions on cognitive function failures for rectification system*

VRSTA DELOVNIH RAZMER COMMON PERFORMANCE CONDITION	STOPNJA LEVEL	1.1	1.2	2.1	2.2	2.3	3.1	3.2	3.3	3.4	3.5	4.1	4.2	4.3	4.4	4.5
Primerna organiziranost Adequacy of organisation	učinkovit efficient	1,0	1,0	1,0	1,0	1,0	1,0	1,0	1,0	1,0	1,0	1,0	1,0	1,0	1,0	1,0
Delovne razmere Working conditions	znosen compatible	1,0	1,0	1,0	1,0	1,0	1,0	1,0	1,0	1,0	1,0	1,0	1,0	1,0	1,0	1,0
Primerna zaščita človeka pred strojem in operativna podpora Adequacy of MMI and operational support	znosen tolerable	1,0	1,0	1,0	1,0	1,0	1,0	1,0	1,0	1,0	1,0	1,0	1,0	1,0	1,0	1,0
Razpolaganje s postopki Availability of procedures/planes	primeren appropriate	0,8	0,8	0,8	0,8	0,8	0,8	0,8	0,8	0,8	0,8	0,8	0,8	0,8	0,8	0,8
Število istočasnih nalog Number of simultaneous goals	primerno zmožnostim matching curr. capacity	1,0	1,0	1,0	1,0	1,0	1,0	1,0	1,0	1,0	1,0	1,0	1,0	1,0	1,0	1,0
Razpoložljiv čas Available time	primeren adequate	0,5	0,5	0,5	0,5	0,5	0,5	0,5	0,5	0,5	0,5	0,5	0,5	0,5	0,5	0,5
Čas dneva Time of day	dnevni čas day-time	1,0	1,0	1,0	1,0	1,0	1,0	1,0	1,0	1,0	1,0	1,0	1,0	1,0	1,0	1,0
Primerna usposobljenost in izkušnje Adequacy of training and preparation	primeren, zelo izkušen adequate, very experience	0,8	0,8	0,8	0,8	0,8	0,8	0,8	0,8	0,8	0,8	0,8	0,8	0,8	0,8	0,8
Kakovost sodelovanja v skupini Crew collaboration quality	zelo učinkovit very efficient	0,5	0,5	0,5	0,5	0,5	0,5	0,5	0,5	0,5	0,5	0,5	0,5	0,5	0,5	0,5
SKUPNI URAVNALNI FAKTOR TOTAL INFLUENCE OF CPC		0,16	0,16	0,16	0,16	0,16	0,16	0,16	0,16	0,16	0,16	0,16	0,16	0,16	0,16	0,16

Preglednica 11. *Primerjava rezultatov analiz drevesa odpovedi z upoštevanjem in brez upoštevanja človeških napak*
Table 11. *Comparision of Fault-Tree Analyse results with and without including human errors*

KRITERIJ CRITERION	VERJETNOST DOGODKA PROBABILITY OF FAILURE	
	TRENUTNI IZPUST INSTANTANEOUS RELEASE	STALNI IZPUST CONTINUOUS RELEASE
TEHNIČNE NAPAKE TECHNICAL FAILURES	$4{,}6\times10^{-5}$	$2{,}0\times10^{-4}$
TEH. IN ČLOVEŠKE NAPAKE TECHNICAL AND HUMANS FAILURES	$4{,}6\times10^{-5}$	$4{,}9\times10^{-3}$

6 SKLEP

V pričujočem delu smo na kratko predstavili metodologijo, ki jo je po našem mnenju primerno upoštevati pri analizi delovanja zahtevnih sistemov. Najprej smo analizirali verjetnost napake trenutnega in stalnega izpusta iz rektifikacijskega sistema zaradi tehnične (mehanske) napake, kar smo storili z uporabo metode drevesa odpovedi in Booleove algebre.

Nato smo obravnavali sistem z vidika človeških napak ter ga analizirali z metodologijo ASZN.

Bistveni prispevek tega dela je v sintezi obeh vplivov, to je vpliv nezgod (človeške napake) in odpovedi (tehnične napake) v drevesu odpovedi. Po sintezi smo ugotovili, da človeška napaka na trenutni izpust bistveno ne vpliva (da je torej dominantna tehnična napaka), pač pa lahko bistveno vpliva na stalni izpust.

Analiza je pokazala še na glavne vire človeške napake, in sicer na napako, ki se pokaže kot neizpolnitev naloge in napačno izpolnitev naloge. Te napake je moč odpraviti z izdelavo dobrih tehničnih navodil za delo in občasnim usposabljanjem operaterja. Druga možnost je avtomatizacija tistih ponavljajočih se dejavnosti, ki bistveno prispevajo k verjetnosti nezgode.

6 CONCLUSION

This study deals mainly with methodology, which should, in our opinion, be used for an analysis of complex-system operation. First, the probability of technical failure for instantaneous and continuous releases was analyzed using fault-tree analysis and Boolean algebra.

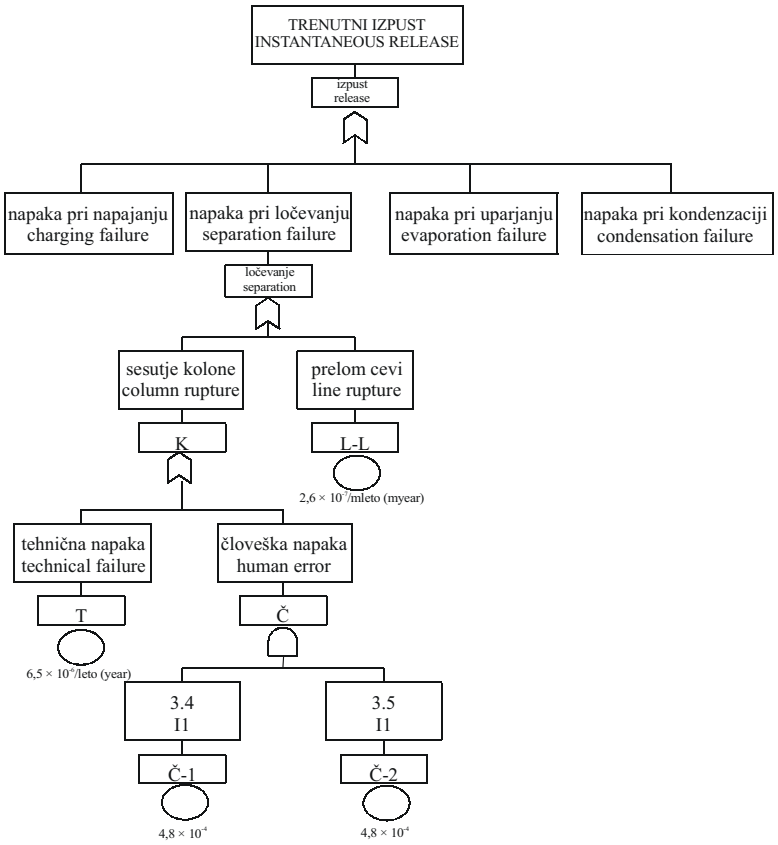
Then, the same system was presented from the human-error perspective and analyzed using CREAM methodology.

The main thrust of this work was in the synthesis of both methodologies, i.e. the influence of human errors and technical failures within the framework of the fault-tree analysis. The results have shown that human failure is almost negligible for instantaneous release, and of significance for continuous release.

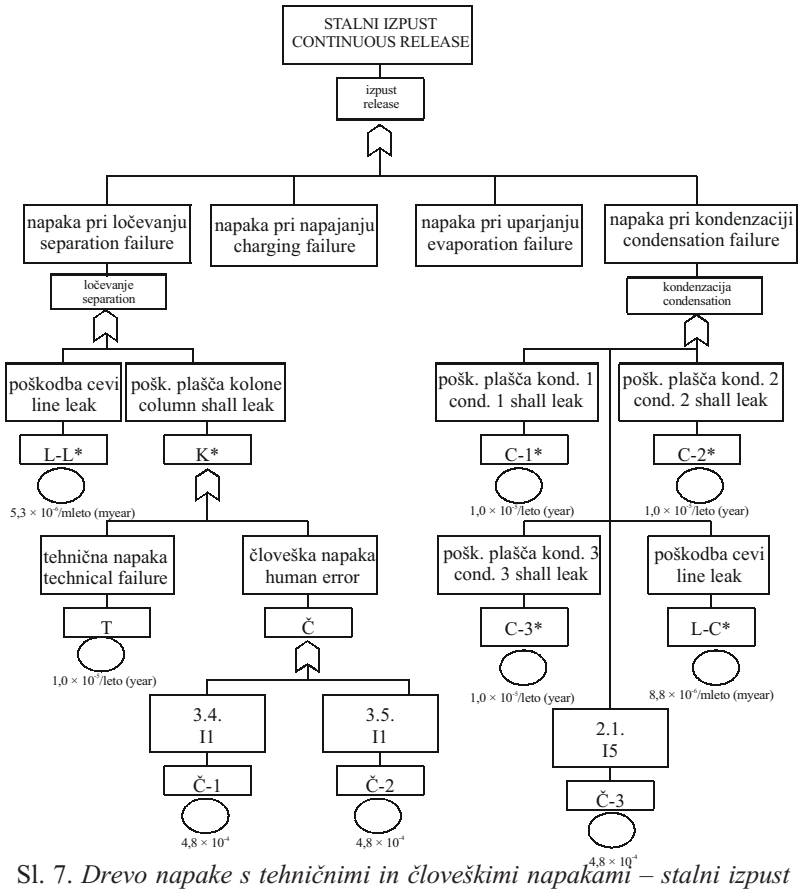
The analysis further identifies the main sources of human error as missed action and action of the wrong type. These errors could be mitigated using technical guidelines of sufficient quality and the periodic training of operators. The second possibility is switching the operations from human operator to activities operated using devices for those repetitive activities which could be the main contributors to the accidents as analyzed.

Preglednica 10. *Uravnane verjetnosti napak poznavalnih funkcij za rektifikacijski sistem*
Table 10. *Adjusted CFPs (ACFP) for rectification system*

#	DEJAVNOST ACTIVITY	VRSTA NAPAKE ERROR MODE	NVNPF NCFP	SUF WF	UVNPF ACFP
1.1	Preverimo, ali so odprte povezave med kolono in rezervoarji za destilat in destilacijski ostanek. Check if connections between column and tanks of destillate and distillatory residue are open.	O3 brez opazovanja observation not made	$7{,}0\times10^{-2}$	0,16	$1{,}1\times10^{-2}$
1.2	Zapremo ventile za odvzem destilata in destilacijskega ostanka. Close valves for destillate and distillatory residue taking away.	I1 napačna izpolnitev action of wrong type	$3{,}0\times10^{-3}$	0,16	$4{,}8\times10^{-4}$
2.1	Vključimo črpalko za kroženje glikola v kondenzatorjih. Start the pump for glycol circulation in condensers.	I5 brez izpolnitve missed action	$3{,}0\times10^{-2}$	0,16	$4{,}8\times10^{-3}$
2.2	Vklopimo napajalno črpalko in napolnimo uparjalnik z mešanico topil Start the feeder pump and fill up reboiler with components mixture.	I2, nepravočasna izpolnitev action at wrong time	$3{,}0\times10^{-3}$	0,16	$4{,}8\times10^{-4}$
2.3	Ko mešanica topil prekrije grelnik uparjalnika, odpremo ventil za gretje uparjalnika. When components mixture cover reboiler heater, open valve for reboiler heating.	O3 brez opazovanja observation not made	$7{,}0\times10^{-2}$	0,16	$1{,}1\times10^{-2}$
3.1	Kolona mora vsaj 30 min delovati pri popolnem refluksu brez napajanja. The column have to operate at least 30 minutes by full reflux without feeding.	O3 brez opazovanja observation not made	$7{,}0\times10^{-2}$	0,16	$1{,}1\times10^{-2}$
3.2	Odpremo ventil za odvzem destilata in destilacijskega ostanka. Open valves for destillate and distillatory residue.	I2 nepravočasna izpolnitev action at wrong time	$3{,}0\times10^{-3}$	0,16	$4{,}8\times10^{-3}$
3.3	Napajalno črpalko naravnamo na pretok 300 l/h. Feeder pump set for flow 300 l/h.	O3 brez opazovanja observation not made	$7{,}0\times10^{-2}$	0,16	$1{,}1\times10^{-2}$
3.4	Temperaturo v refluksni glavi uravnavamo z ventilom za odvzem destilata na 56 °C. Control temperature in reflux head with valve for destillate taking away at 56°C.	I1 napačna izpolnitev action of wrong type	$3{,}0\times10^{-3}$	0,16	$4{,}8\times10^{-4}$
3.5	Temperaturo na dnu kolone uravnavamo z ventilom za odvzem destilacijskega ostanka na 80 °C. Control temperature in column bottom with valve for distillatory residue taking away at 80 °C.	I1 napačna izpolnitev action of wrong type	$3{,}0\times10^{-3}$	0,16	$4{,}8\times10^{-4}$
4.1	Izklopimo napajalno črpalko. Stop feeder pump.	I5, brez izpolnitve missed action	$3{,}0\times10^{-2}$	0,16	$4{,}8\times10^{-3}$
4.2	Zapremo ventil za gretje uparjalnika. Close valve for reboiler heating.	I5, brez izpolnitve missed action	$3{,}0\times10^{-2}$	0,16	$4{,}8\times10^{-3}$
4.3	Zapremo ventil za odvzem destilacijskega ostanka. Close valve for distillatory residue taking away.	I4, napačno zaporedje izpol. action out of sequence	$3{,}0\times10^{-3}$	0,16	$4{,}8\times10^{-4}$
4.4	Odpremo ventil za odvzem destilata. Open valve for destillate taking away.	I4, napačno zaporedje izpol. action out of sequence	$3{,}0\times10^{-3}$	0,16	$4{,}8\times10^{-4}$
4.5	Izklopimo črpalko za kroženje glikola v kondenzatorjih. Stop pump for glycol circulation in condensers.	I2, nepravočasna izpolnitev action at wrong time	$3{,}0\times10^{-3}$	0,16	$4{,}8\times10^{-4}$



Sl. 6. *Drevo napake s tehničnimi in človeškimi napakami – trenutni izpust*
Fig. 6. *Synthesis of human error and fault-tree analysis – instantaneous release*



Sl. 7. *Drevo napake s tehničnimi in človeškimi napakami – stalni izpust*
Fig. 7. *Synthesis of human error and fault-tree analysis – continuous release*

[1] Z mehanskimi sistemi imamo v mislih vse sisteme, ki niso odvisni od človeškega odziva, ne glede na to, za kakšne sisteme gre - sem spadajo npr. cevi, ventili, tlačne posode, zvari ipd.

[2] Med uporabnike štejemo menedžerje, zavarovalnice, sodne izvedence, tehnologe in druge, ki za svoje odločitve uporabljajo podatke o verjetnosti ali možnosti okvare ali porušitve posamezne naprave.

[3] Glede na krajšanje dobe, ki je potrebna za doseganje družbeno sprejemljive spretnosti pri ravnanju s stroji in višanje števila nosilcev tako pridobljene izobrazbe je ta predpostavka konzervativna.

[4] Z izrazom splošni pogoji dela po [5] označujemo obširen in dobro strukturiran temelj za označevanje pogojev, pri katerih naj bi se delo izvajalo. Osnovna predpostavka njihove uporabe je, da so medsebojno odvisni in da zato preprost seštevek ne pomeni še skupne ocene splošnih pogojev dela. V posledici medsebojne odvisnosti mora biti skupna ocena izračunana tako, da upošteva način medsebojne odvisnosti.

[5] Sklepni korak osnovne metode je določitev verjetnega načina nadzora na podlagi kombinacije števila posameznih vplivnih parametrov (od 9 skupnih), ki so bodisi zmanjšani, niso spremenjeni, ali izboljšani ([Σ zmanjšan, Σ brez posebnosti, Σ izboljšan]), pri čemer trojka [9,0,0] opiše najmanj zaželeno stanje, trojka [0,2,7] pa najbolj želeno stanje.

[6] Z izrazom poznavalne dejavnosti [5] označujemo posamezne poznavalne (prepoznavalne, kognitivne) dejavnosti, ki so značilne za vsakega od korakov iz osnovne metode. Te posamezne dejavnosti so uporabljene za gradnjo poznavalnega profila (*Cognitive Profile*) za bistvene segmente opravila, osnovane na funkcijah (t.i poznavalnih funkcijah), ki so opisane s poznavalnim (kognitivnim) modelom. Poznavalne funkcije so uporabljene za prepoznavanje posameznih poznavalnih dejavnosti (npr. z opazovanjem kot funkcijo opravimo dejavnost verifikacije ali dejavnost spremljanja).

[7] Z izrazom napake poznavalne funkcije so [5] označene napovedane napake, do katerih lahko pride pri izvedbi poznavalnih funkcij (npr. pri opazovanju kot funkciji lahko pride do napak opazovanja, ki imajo lahko neposredni vpliv na poznavalne dejavnosti, npr. na spremljanje).

[8] Različne napake poznavalnih funkcij imajo različen učinek na končni rezultat, zato je posamezne napake poznavalne funkcije treba primerno utežiti.

[9] Uravnalni faktor po [5] iz [9], ki za učinek posamezne poznavalne funkcije na posamezno poznavalno aktivnost določa utež. Ta izvira iz izkušenj in znaša za nevtralni položaj 1.0, za položaj, ki izboljšuje stanje manj ko 1 in za položaj, ki stanje slabša, več ko 1. Tako npr. primerna dostopnost načrtov in postopkov pomeni 20% zmanjšanje verjetnosti napake (uravnalni faktor 0,8), sprejemljiva dostopnost pomeni nevtralno stanje (UF=1,0), neprimerna dostopnost pa 100% povečanje verjetnosti napake (UF=2). Značilna za tako porazdelitev je penalizacija, ki kaznuje slabšanje položaja in posledično vnaša konzervativnost v določanje UF.

[10] *Deanimation*, po Raven, J., osebna komunikacija.

[1] With mechanical or technological systems one describes all systems that are not directly dependent on human response without regard to actual systems - such as piping, valves, pressure vessels, welds etc.

[2] Such as insurance companies, managers, court experts, system engineers and others on a need-to-know basis regarding the probability of failure.

[3] This is a conservative assumption given the reduction in time needed for qualification as a machinist and inflation in the number of graduates of technical schools.

[4] Common performance conditions were suggested by Hollnagel [5] to describe well-structured foundation for description of conditions for work performance. The basic assumption of their use is common interdependence and the fact that a simple sum does not equal common performance conditions. Interdependence also requires taking into account its mode.

[5] The final step of the basic method is the evaluation of a probable control mode based on the combination of a number of important parameters (numbering 9) which can either be reduced, are not significant, or are improved [Σ reduced, Σ not significant, Σ improved] where the triplet [9,0,0] stands for least-desirable situation, and the triplet [0,2,7] for most-desirable situation.

[6] Hollnagel [5] defines the cognitive demands that are characteristic for each of the basic method steps. These demands are used to build a cognitive profile for important segments of a particular action and are based on a cognitive function. These functions are used for either recognizing a particular cognitive demand (e.g. with observation as a function the activity of monitoring is made).

[7] Cognitive function failures Hollnagel [5] describes potential failures that can occur during the execution of cognitive functions (i.e. observation as a function can result in observation failures, and these failures may directly influence execution).

[8] Different cognitive failures may have a different influence on the final result, which requires different weights to be applied to cognitive functions.

[9] Hollnagel [5] has adopted weighting factors from Williams [9] who defines the weight for the effect of each particular cognitive function on cognitive demand. The weight (weighting factor) is based on experience and equals 1.0 for neutral (not significant) position, less than 1 for improvements, and more than 1 for reduction. For example, good access to plans and procedures means a 20% reduction in probability of error (i.e. weight of 0.8), while adequate access means not significant position with a weight of 1.0, and inadequate access increase for 100%, i.e. a weight of 2.0. This method means penalization of worsening of position and results in a conservative weight definition.

[10] From Raven, J., personal communication.

7 LITERATURA
7 REFERENCES

[1] Kožuh, M. (1999) Odkrivanje in vrednotenje latentnih pomanjkljivosti v kompleksnih tehnoloških sistemih, *Fakulteta za strojništvo*, Ljubljana, Doktorska disertacija, 207.

[2] Jordan Cizelj, R. (2001) Ocena stanja komponent jedrskih sistemov z uporabo teorije verjetnosti in teorije mehkih množic, *Fakulteta za matematiko in fiziko*, Ljubljana, Doktorska disertacija.

[3] Kožuh, M., B. Mavko (1994) Comparing different system configurations and success criteria by the use of Fault tree technique for Instrument Air System. V: STRITAR, Andrej (ur.). *International Meeting PSA/ PRA and Severe Accidents '94*, Ljubljana, Slovenia, 17.-20. April.

[4] Čepin, M., R. Jordan-Cizelj, M. Kožuh (1994) AC/DC power supply system fault tree analysis". V: Thermal Reactor Safety Assessment: *Proceedings of the conference organized by the British Nuclear Energy Society*, Manchester, 23-26 May.

[5] Hollnagel, E. (1998) Cognitive reliability and error analysis method, *Institutt for Energiteknikk Halden,* Norway, ISBN 0-08-0428487.

[6] Kožuh, M., J. Peklenik (1999) A method for identification and quantification of latent weaknesses in complex systems, *Cognition, Technology & Work,* vol. 1, no. 4, 211-221.

[7] Center for chemical process safety*:* Guidelines for chemical process quantitative risk analysis, *American Institute of Chemical Engineers*, 1989.

[8] Sutton, I.S. (1992) Process reliability and risk management, *Van Nostrand Reinhold New York*.

[9] Williams, J.C. (1988) A data-based method for assessing and reducing human error to improve operational performance, *Proceedings of IEEE 4th Conference on Human factors in Power Plants*, Monterey, CA 6-9 June.

[10] Zupančič, J. (2001) Analiza tehničnih in človeških napak rektifikacijskega sistema, poročilo o individualnem raziskovalnem delu (IRD), *Fakulteta za strojništvo Univerze v Mariboru*.

[11] Bainbridge, L., *Ironies of automation,* http://www.bainbrdg.demon.co.uk/index.htm

[12] Zupančič, J. (2002) Varnost in zanesljivost rektifikacijske kolone, magistrska naloga, *Fakulteta za strojništvo*, Maribor.

Naslova avtorjev: mag. Janja Zupančič
Krka, d.d., Novo mesto
Šmarješka c. 6
8000 Novo mesto

prof.dr. Jure Marn
Fakulteta za strojništvo
Univerza v Mariboru
Smetanova 17
2000 Maribor
jure.marn@uni-mb.si

Authors' Addresses: Mag. Janja Zupančič
Krka, d.d., Novo mesto
Šmarješka c. 6
8000 Novo mesto, Slovenia

Prof.Dr. Jure Marn
Faculty of Mechanical Eng.
University of Maribor
Smetanova 17
2000 Maribor, Slovenia
jure.marn@uni-mb.si

Prejeto: 18.1.2002
Received:

Sprejeto: 20.9.2002
Accepted: