# Študija ustreznosti implementacije sistema za nadzor kritičnih aplikacij v bančnem sistemu

[1]Simon Sirc, [2]Jože Zupančič
[1]NLB, d. d., Šmartinska cesta 130, 1000 Ljubljana
[2]Univerza v Mariboru, Fakulteta za organizacijske vede, Kidričeva 55 a, 4000 Kranj
simon.sirc@nlb.si; joze.zupancic@fov.uni-mb.si

## Izvleček

V prispevku je prikazana študija ustreznosti sistema za nadzor kritičnih aplikacij v bančnem informacijskem sistemu NLB, d. d. Sistem za nadzor smo proučevali z namenom nadgradnje obstoječega nadzornega sistema, s katerim ne moremo nadzorovati delovanja kritičnih aplikacij oz. transakcijskih tokov v realnem času. Cilj novega nadzornega sistema je, da omogoča stalno spremljanje delovanja sistema in kritičnih aplikacij, alarmiranje in v določenih primerih celo avtomatizirano odpravljanje napak. Naš namen je zgraditi čim bolj avtonomen informacijski sistem, kar pa na vseh področjih ni mogoče. Preučevani nadzorni sistem z zmožnostjo sledenja transakcijskim tokovom omogoča tudi odkrivanje ozkih grl v delovanju aplikacij, zato bi z njegovo uporabo lahko optimizirali marsikateri proces, za katerega sedaj niti ne vemo, da obstaja oz. da nam povzroča težave. Predlagani pristop je bil implementiran in preizkušen na kritični aplikaciji, ki podpira plačilne transakcije v državi in skrbi za izmenjavo plačilnih transakcij med notranjimi in zunanjimi sistemi. Podana je tudi ocena implementiranega dela nadzornega sistema in predlogi za nadgradnjo oz. implementacijo preostalih komponent nadzornega sistema.

**Ključne besede:** informacijski sistem, nadzorni sistem, kritične aplikacije, transakcije, IBM Tivoli, strateški cilji, analiza ustreznosti.

## Abstract

**The Study of the Implementation of Monitoring System for Critical Applications in the Banking System**

This paper presents a feasibility analysis of a system for monitoring of critical applications in the NLB bank. The monitoring system was investigated with the intention to upgrade the existing application of the monitoring system, which doesn't support real-time monitoring of critical applications and transaction flows. The proposed system has the capability to continually monitor the functioning of the entire information system and critical applications, and warn the operators; in some cases even an automated recovery from failure is possible. The capability to monitor transaction flows enables the system to reveal bottlenecks in the existing processes and identify and optimise critical or failure prone processes within critical applications. Although the goal of the study was to propose a widely autonomous system, the monitoring system still requires intervention of IS personnel. The proposed approach was implemented and evaluated on a critical application, i.e., the central application which supports payment transactions within the country and manages exchange of payment transactions between internal and external systems. An evaluation of the implemented monitoring system is presented and proposals for further upgrade and development of the system are given.

**Keywords:** information system, monitoring system, critical application, transaction, IBM Tivoli, strategic goal, feasibility analysis.

## 1 UVOD

**Z razvojem novih storitev in z njimi povezanih uporabniških rešitev v NLB, d. d., se hitro povečuje tudi kompleksnost informacijskega sistema podjetja, ki ga je vse težje nadzorovati. Čeprav sta zanesljivost in razpoložljivost informacijskega sistema že več let visoki, podjetje stremi k doseganju še boljših rezultatov na tem področju.**

**Poslanstvo oddelka za informacijsko tehnologijo v NLB je vzpostaviti okolje, v katerem je informacijska tehnologija glavni temelj poslovanja banke in eden od gonilnih sil razvoja. Širše gledano je poslanstvo skupine NLB biti zanesljiv dolgoročni partner, na katerega se stranke lahko zanesejo. NLB hoče svojim strankam zagotavljati prvovrstne in celovite finančne storitve in rešitve, ki jih potrebujejo za doseganje svojih ciljev (NLB, 2011a). Eden od ciljev oddelka za informacijsko tehnologijo v tem letu je zmanjšati število dni z motnjami za uporabnike in s tem zagotoviti, da uporabniki v prihodnje sploh ne bodo zaznavali nepredvidenih motenj delovanja informacijskega sistema.**

Glede na heterogenost informacijskega sistema in veliko število sprememb, ki se izvedejo vsako leto, to pomeni zelo velik izziv (NLB, 2011b).

Da bi dosegli omenjene cilje, je treba najprej izpostaviti, da je trenutno največji problem zagotovitev natančnega, hitrega, zanesljivega in celovitega sprotnega pregleda nad delovanjem celotnega informacijskega sistema, kakor tudi pregled nad medsebojno povezanostjo komponent, na katerih se izvajajo poslovne aplikacije oz. transakcije.

Nadzor in spremljanje transakcij z obstoječim načinom nadzora ni mogoč, zato se velikokrat spopadamo z napakami v delovanju kritičnih aplikacij, ko se te že razširijo na druge komponente informacijskega sistema. Takrat je odprava napak zahtevnejša, saj je vzrok oz. mesto nastanka težje odkriti, napake pa se kopičijo. Za nadzor informacijskega sistema trenutno uporabljamo več različnih produktov, ki niso povezani v celoto. Ker nimamo celovitega pregleda nad informacijskim sistemom na enem mestu in ker ne znamo povezovati soodvisnih podatkov, tudi ne moremo razpolagati s podatki o transakcijskih tokovih. Potrebujemo nadzorni sistem, ki bi informacije o sistemu in transakcijskih tokovih prikazoval v dejanskem času na uporabniškem vmesniku, katerega bi uporabljali vsi skrbniki.

Da bi rešili omenjeno težavo, smo v banki izvedli študijo ustreznosti nadzornega sistema IBM Tivoli, ki naj bi omogočal tako nadzor sistema, kakor tudi nadzor nad transakcijami. Ker je celoten nadzorni sistem preobsežen, se je bilo treba odločiti, kateri deli nadzornega sistema so nujno potrebni, katere bi še radi implementirali ter katerih ne potrebujemo.

Glede na visoko stopnjo zanesljivosti in razpoložljivosti bančnega informacijskega sistema bi na prvi pogled lahko sodili, da je obstoječi način nadzora povsem zadosten, saj tudi v praksi uspešno deluje že od vsega začetka. Z njim smo lahko zadovoljni in ga ocenjujemo kot zanesljivega. Spoznanja o zmožnostih naprednih tehnologij nadzora pa kažejo, da z naprednim nadzornim sistemom lahko tudi optimiziramo poslovne procese in dvignemo poslovanje na višjo raven, informacijskemu sistemu pa znižamo obratovalne stroške in stroške, povezane s pojavom in odpravo napak. To pa seveda še ne pomeni, da bi tako lahko odpravili vse napake v delovanju informacijskega sistema in poslovnih aplikacij, vsekakor pa bi bili zmožni nadzorovati transakcijske tokove in celotno delovanje informacijskega sistema z enim samim uporabniškim vmesnikom.

## 2 KRATKA PREDSTAVITEV INFORMACIJSKEGA POSLOVNEGA OKOLJA BANKE IN NADZORNEGA SISTEMA

Arhitektura informacijskega sistema banke je kompleksna, heterogena in večnivojska. Tvori ga skupek različnih medsebojno prepletenih komponent na različnih ravneh, ki uporabljajo različne tehnologije. Glavni del informacijskega sistema banke je velik osrednji računalnik (angl. host, mainframe) IBM Z196. Na tem sistemu ter podsistemih, kot so CICS TS (angl. Customer Information Control System Transaction Server), DB2 (angl. Database 2), WebSphere MQ (angl. WebSphere Message Queue) idr., se izvajajo programi s poslovno logiko. Predstavitvena logika, torej uporabniški vmesniki, ki v glavnem zajemajo in prikazujejo podatke, pa so ločeni od osrednjega računalnika. Nameščeni so na različnih distribuiranih okoljih, v katerih se tudi izvajajo.

Poleg vmesnih ravni, ki se navezujejo na varnost, prenos podatkov itn., sta z vidika zanesljivosti delovanja najbolj pomembni predstavitvena raven in raven obravnavanja poslovnih podatkov, saj so spremembe (in s tem posledično tudi napake) na teh dveh ravneh najbolj pogoste, poleg tega pa sta za uspešno in pravilno delovanje poslovno kritičnih aplikacij tudi najbolj pomembna. Z vidika zanesljivosti delovanja poslovno kritičnih aplikacij so najbolj izpostavljene transakcije, saj morajo nemoteno delovati ravno tisti trenutek, ko se izvajajo.

V slovenski literaturi opisa termina kritična aplikacija ne zasledimo, tudi slovar informatike (http://www.islovar.org/) ga ne pozna, čeprav se o tem zadnje čase vedno več govori in se to tako rekoč tiče skoraj vsakega podjetja z informacijskim oddelkom. Zato navedbe o kritičnih aplikacijah, ki so predvsem v bančnem poslu nekaj vsakdanjega, povzemamo iz tuje literature.

Tradicionalno so bile poslovno kritične aplikacije opredeljene kot aplikacije, ki so za poslovne procese bistvenega pomena. Podatkovno usmerjeni aplikaciji, kot sta bančni transakcijski sistem ali letalski rezervacijski sistem, sta že od nekdaj ključni za ta dva poslovno kritična procesa. Njuno nedelovanje se običajno pokaže kot izguba dohodkov ali zmanjšanje produktivnosti zaposlenih. Zadnje čase uporabljajo vse več aplikacij, ki veljajo za poslovno kritične. Ta realnost je v velikem številu podjetij spremenila vlogo in funkcijo informacijske tehnologije. V splošnem kot poslovno kritične aplikacije še vedno

lahko označimo tiste, katerih sistemske napake pri uporabniških rešitvah vodijo v izgubo prihodkov, nezadovoljstvo strank in/ali upad produktivnosti. Vendar pa je meja med aplikacijami, ki so kritične za poslovanje, in drugimi aplikacijami vedno bolj zamegljena. Drugačne storitve, pa četudi znotraj enega podjetja, zahtevajo različna merila za opredelitev, kaj je poslovno kritično (Hicks, 2004).

Poslovanje banke temelji na plačilnem prometu, plačilni promet pa na finančnih transakcijah. Transakcija je postopek, ki ga sproži posamezna zahteva in jo izda operater oz. uporabnik. Postopek, izveden glede na podano zahtevo, sproži akcije enega ali več medsebojno povezanih aplikacijskih programov, ki izpolnijo podano zahtevo. Poti transakcij skozi programe in sisteme poznamo le opisno. Nekateri skrbniki aplikacij imajo v dokumentaciji celo izrisane transakcijske tokove skozi sisteme na principu procesnih slik. Kako transakcije določen trenutek dejansko potekajo, kje so ozka grla, kakšni so odzivni časi med posameznimi komponentami informacijskega sistema itn., pa ne znamo spremljati oz. nadzirati. Možnosti boljših načinov nadzora upravljavci informacijskih sistemov iščejo že od vsega začetka informatizacije poslovanja. Skrbniki posameznih področij informacijskega sistema in poslovnih aplikacij so pogosto sami izdelali svoje nadzorne rešitve ali pa so implementirali v okolje kupljene produkte različnih proizvajalcev.

## 3 PREGLED OBSTOJEČE LITERATURE IN DOKUMENTACIJE

Pregled raziskovalne literature je pokazal, da je se objave v zvezi z nadzorom (kritičnih) aplikacij večinoma nanašajo na lastne rešitve in specifične vidike, npr. na preprečevanje in odkrivanje vdorov v sistem, pa tudi na razvoj algoritmov, postopkov in splošnih rešitev pri nadzorovanju informacijskih sistemov. Abdul-Malek (2010) je v svoji doktorski disertaciji predlagal model in izdelal od računalniškega okolja neodvisno aplikacijo, ki poleg nadzorovanja tekočih in končanih poslov omogoča tudi nadzor napak in alarmiranje operaterjev. Agarwala idr. (2010) so predstavili idejo in praktično rešitev za vmesno programje (angl. middleware), namenjeno nadzorovanju računalniške konfiguracije, ki temelji na najboljših industrijskih standardih in praksah. Izboljšanje učinkovitosti nadzornega sistema na podlagi analize karakteristik aplikacij je poglavitni cilj modela, ki je opisan v Wang idr. (2008). Paxton idr. (2011) predlagajo model za zaščito in nadzorovanje napadov na računalniški sistem »botnet«,[1] Veyard (2003) opisuje aplikacijo za nadzor informacijskega sistema za odkrivanje transakcij, ki so sumljive z vidika pranja denarja. Sengupta idr. (2008) predlagajo od računalniškega okolja neodvisen in »neinvaziven« pristop, ki temelji na analizi vzorcev transakcij izhajajoč iz dnevnikov transakcij (angl. log files). V referatu Yang idr. (2010) avtorji predstavljajo pregled, kako v nekaterih vodilnih azijskih bankah pristopajo k nadzorovanju tveganj, povezanih z informacijsko tehnologijo. Haberkorn in Trivedi (2007) opisujeta metodo za nadzor in prikaz razpoložljivosti računalniškega sistema v realnem času.

Ker nismo uspeli najti ustreznih virov v znanstveni literaturi, ki bi obravnavali praktično implementacijo nadzornega sistema, smo se pri našem delu opirali predvsem na nekatere strokovne članke in na proizvajalčevo dokumentacijo.

Ker se bančno poslovanje neprestano širi, je treba uvesti prožen nadzorni sistem, ki se bo z lahkoto prilagajal razširjenemu ali spremenjenemu poslovanju. Da bi bili stroški čim manjši, mora biti način prilagajanja nadzornega sistema enostaven in ne sme zahtevati stalne pomoči zunanjih svetovalcev. Praviloma bi komercialno dostopen transakcijsko nadzorni sistem moral biti pripravljen za integracijo v bančno okolje, vendar v večini primerov ni tako. Zato lahko pričakujemo, da bosta implementacija in natančno nastavljanje nadzornega sistema tekla uspešno le, kadar je vzpostavljeno tesno sodelovanje med ponudnikom nadzornega sistema in informacijskim oddelkom. Nujna je pogosta fizična navzočnost ponudnika med implementacijo in je priporočljiva tudi kasneje – pri dopolnitvah in nadgradnjah. Zato je izbira ponudnika ključnega pomena. Zaposleni v informacijskem oddelku morajo biti s temi dejstvi dobro seznanjeni in morajo biti pripravljeni sodelovati s ponudnikom (Veyder, 2003).

Če zaposleni niso pripravljeni sodelovati, lahko pričakujemo, da bo njihova absorpcijska sposobnost zelo nizka. Kot ugotavlja Mulej (2003:1), absorpcijska sposobnost pomeni sposobnost in voljo sprejeti in ustvarjalno ter koristno uporabiti znanje, vednost in

[1] Po slovarju informatike (http://www.islovar.org/) pomeni »botnet« večje število računalnikov, nad katerimi napadalec brez vedenja skrbnikov na daljavo pridobi nadzor z namenom izvajanja zlonamernih dejanj; sin. omrežje robotskih računalnikov.

vrednote, ki se ne razvijajo neposredno v praksi, bi pa naj jih tam uveljavili.

Pri izbiri nadzornega sistema je bila zato pomembno merilo tudi združljivost nadzorne tehnologije z obstoječo informacijsko tehnologijo. Ker osrednji del informacijskega sistema banke predstavlja IBM-ov računalnik Z196, je na odločitev o izboru ponudnika najbolj vplivala preprosta združitev nadzorne tehnologije z obstoječo informacijsko tehnologijo. Banka se je odločila za nadzorni sistem IBM Tivoli Monitoring tudi zaradi njegovih karakteristik, saj omogoča podroben nadzor osrednjega računalnika in njegovih sistemskih ter podsistemskih komponent. S tem je mogoče pokriti nadzor skoraj celotnega dela poslovne logike, ki se izvaja na osrednjem računalniškem delu, omogoča pa tudi podroben nadzor logike predstavitvenega dela (uporabniški vmesniki), ki se izvaja na različnih distribuiranih okoljih.

Nadzorni sistem IBM Tivoli Monitoring je kompleksen sistem, sestavljen iz več komponent – tako strojnih kot tudi programskih –, ki omogoča nadzor strojnih in aplikativnih programskih delov (transakcij) poslovnoinformacijskega sistema. Programska oprema Tivoli deluje kot možgani v ozadju osrednjega računalnika. Omogoča performančni in aplikativni nadzor, sistemsko in aplikativno avtomatiko, nadzor omrežja, podatkovni, finančni in varnostni nadzor, omogoča izdelovati finančna poročila in poročila o izvajanju aplikacij, procesov in še več drugih funkcij (IBM Plans New Tools to Support Tivoli System z Management Software, 2007).

V študijah primerov, ki so dosegljivi na IBM-ovih spletnih straneh, avtorji večinoma pišejo o nadzornem sistemu IBM Tivoli za sistemske komponente, bolj malo pa o nadzorni tehnologiji transakcij; italijansko borzno podjetje Consip SpA npr. uporablja Tivoli Business Service Manager za boljše razumevanje odvisnosti in povezave med infrastrukturnimi deli ter poslovnimi storitvami, kar jim omogoča boljši vpogled v dejavnosti in boljše razumevanje vpliva, ki ga problem lahko povzroči uporabnikom (IBM, 2011a). V nemškem podjetju BG-Phoenix GmbH, ki se ukvarja s prodajo strojne in programske opreme socialnovarstvenim ustanovam in strokovnim združenjem, uporabljajo Tivoli Monitoring za zagotavljanje kakovosti njihovih storitev, saj spremljajo celotno informacijsko infrastrukturo vključno z distribuiranimi strežniki zunaj njihove osrednje računalniške infrastrukture (IBM, 2011b).

Sistemski nadzor z uporabo produktov Tivoli Monitoring je torej že dokaj razširjen, medtem ko sam nadzor transakcij ni. Sledenje transakcijam je za banko najbolj zanimivo področje, predvsem pa je povsem novo. Nadzor nad samim sistemom sicer že obvladujemo z drugačnimi prijemi in produkti. Tudi prehod oz. implementacija proizvodov IBM Tivoli za sistemski nadzor ne bi bila problematična, zahtevno pa je uvesti tehnologije nadzora transakcij. Po besedah enega izmed največjih specialistov za to področje in soavtorja članka Hu idr. (2008), Richarda Macklerja, s katerim smo imeli priložnost sodelovati, smo v banki na področju implementacije v tako kompleksen, predvsem pa realen poslovni sistem v svetovnem merilu naredili velik korak v tej smeri.

IBM je že leta 2004 naznanil novo verzijo programa Tivoli Monitoring for Transaction Performance, ki naj bi zelo povečala možnosti sledenja transakcij z različnimi aplikacijami. Ta zmožnost je bila mišljena predvsem za velika okolja, v katerih nadzorujejo več sto različnih transakcij (Musich, 2004).

Zadnje čase se poleg nadzora veliko govori tudi o avtonomnih računalniških sistemih. Avtonomno računalništvo, kot pove že ime, je metafora, ki temelji na biologiji. Avtonomni živčni sistem v telesu je osrednjega pomena za veliko nezavednih dejavnosti, ki nam omogočajo, da nadaljujemo z višjo stopnjo aktivnosti v našem vsakdanjem življenju. Tipični primeri, ki izstopajo, so bitje srca, utrip, dihanje, refleksni odziv po dotiku ostrega ali vročega predmeta itn. Namen uporabe te metafore je izraziti vizijo, da bi nekaj podobnega morali doseči tudi na področju računalništva, tj. ustvariti samodejno upravljanje znatnih količin računalniških funkcij in s tem razbremeniti uporabnike na nižji stopnji upravljanja, da se bodo lahko posvečali skrbi za upravljanje na višji ravni, preizkušanju novih stvari ali zabavi (Sterritt, 2005; Huebscher in McCann, 2008).

Za avtonomno in uporabno delovanje računalnikov stranke potrebujejo zmožnost merjenja, kako se aplikacije obnašajo na sistemu in kako se transakcije izvajajo prek informacijske infrastrukture. Tivoli Monitoring za spremljanje transakcijskih zmogljivosti je korak v tej smeri, saj so za avtomatizacijo popravkov v IBM-u načrtovali sisteme, ki znajo sami skrbeti zase. Tudi programska oprema nadzornega sistema mora zato najprej »razumeti«, kako aplikacije komunicirajo z infrastrukturnimi komponentami na ravni transakcij (Dubie, 2004).

Po trditvah proizvajalca (IBM, 2011c) nadzorni sistem za nadzor transakcij omogoča visoko zanesljiv nadzor transakcij za spletne in organizacijsko-informacijske infrastrukture ter pomaga uporabnikom, da se izognejo kritičnim performančnim problemom. Tako omogoča, da operacije za stranke in končne uporabnike tečejo gladko. Ilog JViews[2] uporabljajo stranke Tivoli, kot so transakcijski ponudniki, da lahko od začetka do konca spremljajo tok in učinek individualnih ali skupnih vplivov transakcij, ugotavljajo transakcijske odzivne čase in vire zakasnitev. Ko nadzorni sistem locira problem, spoznavni grafični model Ilog JView pomaga uporabniku, da s pomočjo vizualizacije locira komponento, ki povzroča zaostanke in s tem pripomore k hitri odpravi problema. Ilog JViews interaktivni prikazi z naprednimi podatkovnimi tehnikami, kot je avtomatsko razvrščeni tokovni diagram, omogočajo uporabnikom lažje razumevanje kompleksnega toka podatkov, ki se pretaka skozi njihove procese.

Ker je IBM Tivoli Monitoring za nadzor transakcij dokaj nov proizvod, ki se v takšnem obsegu, kot ga želimo uporabiti v banki, skorajda ni uporabljal, se je postavilo vprašanje, ali je nadzorni sistem sploh dovolj izpopolnjen in ali sploh stabilno deluje. Zanimalo nas je, ali je glede na heterogeno informacijsko okolje banke res primeren oz. zmožen kakovostno in zanesljivo opravljati funkcijo nadzora transakcijskih tokov poslovno kritičnih aplikacij skozi kompleksno informacijsko omrežje in jih tudi izrisati.

Glede na predstavljena dejstva iz literature in zaradi preproste združljivosti nadzorne tehnologije z obstoječo informacijsko infrastrukturo smo se odločili, da nadzorni sistem IBM Tivoli Monitoring implementiramo in preizkusimo, ali je primeren za NLB. Opravili smo študijo, v kateri so sodelovali zunanji strokovnjaki in naši strokovnjaki za različna področja znotraj banke, kakor tudi skrbniki za posamezne sistemskoaplikativne dele poslovno kritičnih aplikacij. Študija je bila opravljena z namenom, da bi skupaj postavili oceno ustreznosti nadzornega sistema za NLB, d. d.

## 4 POSTAVITEV KRITERIJEV IN CILJ ŠTUDIJE

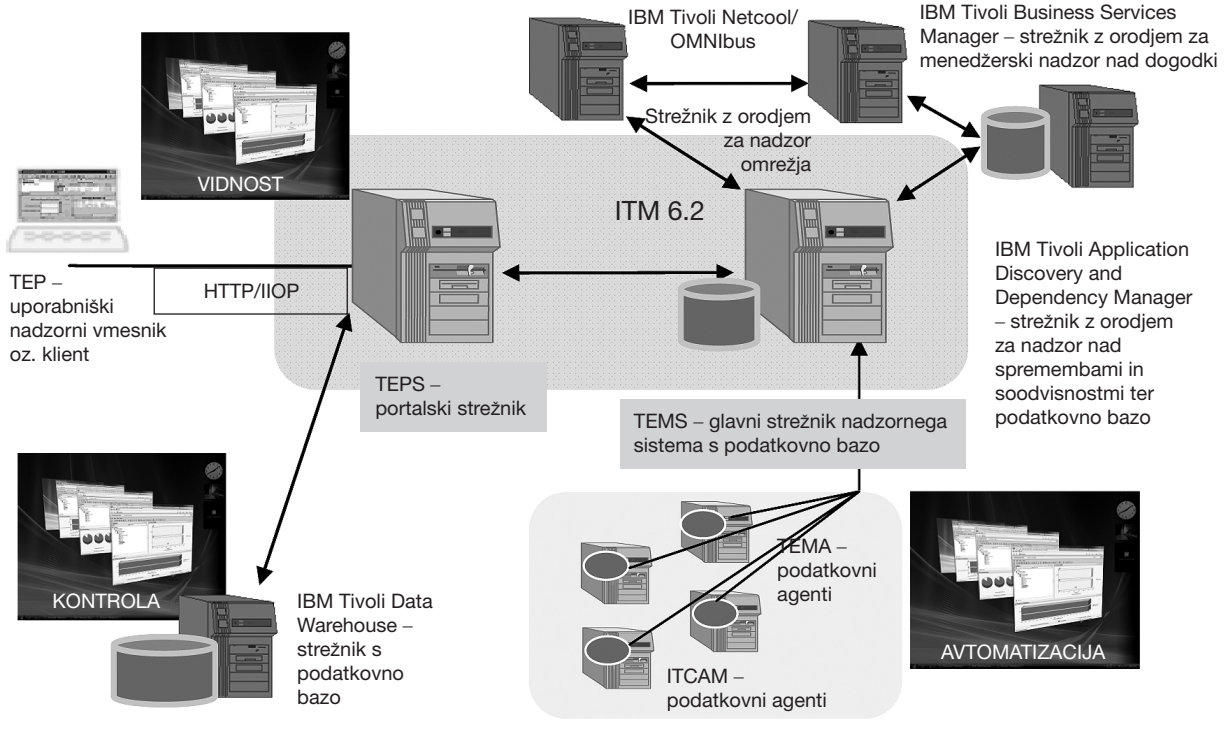
Cilj študije je bilo opraviti analizo ustreznosti sistema za nadzor informacijskega sistema banke, na katerem se izvajajo kritične aplikacije. Prav tako je bil cilj preučiti tudi nadzor kritičnih aplikacij in spremljanje toka transakcij v realnem času. Upoštevali smo, da sam informacijski sistem znamo nadzorovati že dokaj natančno, ne znamo pa nadzorovati toka transakcij. Za oceno primernosti oz. ustreznosti nadzornega sistema smo na podlagi zmožnosti nadzornega sistema, opisanih v proizvajalčevi spletni literaturi (http://www-01.ibm.com/software/tivoli/products/monitor/), določili glavne kriterije, katere mora izpolnjevati nadzorni sistem. Kriterije smo postavili v obliki vprašanj, s pomočjo katerih smo kakovostno ocenili ustreznost nadzornega sistema.

- Ali nadzorni sistem omogoča nadzor celotnega informacijskega sistema in poslovno kritičnih aplikacij na enem uporabniškem vmesniku?
- Ali omogoča sledenje in vizualizacijo celotnega toka transakcij ne glede na heterogenost našega informacijskega sistema?
- Ali nadzorni sistem omogoča spremljanje končnih in vmesnih odzivnih časov transakcij in s tem tudi odkrivanje ozkih grl?
- Ali je nadzorni sistem na podlagi postavljeni pravil zmožen zaznavati, alarmirati, locirati, diagnosticirati in avtomatsko odpravljati napake v doglednem času, ki je v večini primerov krajši od 5 minut (toliko časa navadno traja, da problem zaznajo uporabniki)?
- Ali je poraba sistemskih resursov osrednjega računalnika za izvajanje nadzora manjša od 15 odstotkov celotne porabe resursov?
- Ali so za upravljanje (namestitev, uporaba, nadgradnja) nadzornega sistema dovolj trije skrbniki?
- Ali nadzorni sistem v primerjavi z obstoječim načinom nadzora omogoča lažje obvladovanje informacijskega sistema banke?

Da smo lahko odgovorili na zastavljena vprašanja oz. da bi nadzorni sistem omogočal funkcionalnosti, katere smo preizkušali, smo morali zagotoviti, da je bila na vsaki komponenti informacijskega sistema, ki jo nadzorujemo, nameščena ustrezna komponenta nadzornega sistema. Bolj podrobna arhitekturna slika sestavnih delov nadzornega sistema po komponentah informacijskega sistema, na katerih temelji naš nadzorni sistem, bo predstavljena v nadaljevanju. Na sliki 1 pa je razvidna tipična

[2] Ilog JViews je IBM-ova blagovna znamka za vizualizacijo. Nanaša se na celovito zbirko programskih orodij in knjižnic, ki so namenjeni razvijalcem uporabniških vmesnikov in omogočajo izdelavo interaktivnih grafičnih prikazov. Uporabiti jih je mogoče v različnih razvojnih okoljih in omogočajo izdelavo kompleksnih grafičnih vmesnikov za zahtevna poslovna okolja (http://www.ibm.com/developerworks/offers/lp/demos/summary/ilog-jviews-maps.html).

oz. osnovna zgradba nadzornega sistema, kot so si jo zamislili IBM-ovi strokovnjaki, ki so zasnovali nadzorni sistem. Na sliki je še nekaj gradnikov oz. komponent, katerih funkcionalnosti nismo uspeli preizkusiti, niti jih nismo nameščali, jih pa načrtujemo za prihodnost. Osredinili smo se na osrednji del, ki omogoča nadzor sistema in sledenje transakcijam, in tako izpustili orodja za nadzor omrežja (IBM Tivoli Netcool/OMNIbus), za nadzor nad spremembam in soodvisnostmi (Change and Configuration Management Database in IBM Tivoli Application Discovery and Dependency Manager) in orodju za menedžerski nadzor nad dogodki (IBM Tivoli Business Services Manager).




Slika 1: **Arhitekturna slika – nadzorni sistem IBM Tivoli Monitoring** *(Vir: Implementacija IBM Tivoli Monitoring v NLB)*

Ker je ves nadzorni sistem IBM Tivoli izredno kompleksen, smo sprva za potrebe analize ustreznosti izbrali komponente, ki bodo nadzorovale najpomembnejše dele bančnega informacijskega sistema. Sproti smo dodajali posamezne dodatne dele in tako postavili nadzorni sistem, ki naj bi glede na kriterije odgovoril na naša vprašanja oz. zadostil našim potrebam. Predstavljeni nadzorni sistem sicer temelji na prikazu nadzora ene same poslovno kritične aplikacije in njenih sistemskih komponent, vendar zajema ravni poslovne logike, ki se odvija na osrednjem računalniku, kakor tudi ravni predstavitvene logike iz distribuiranega okolja.

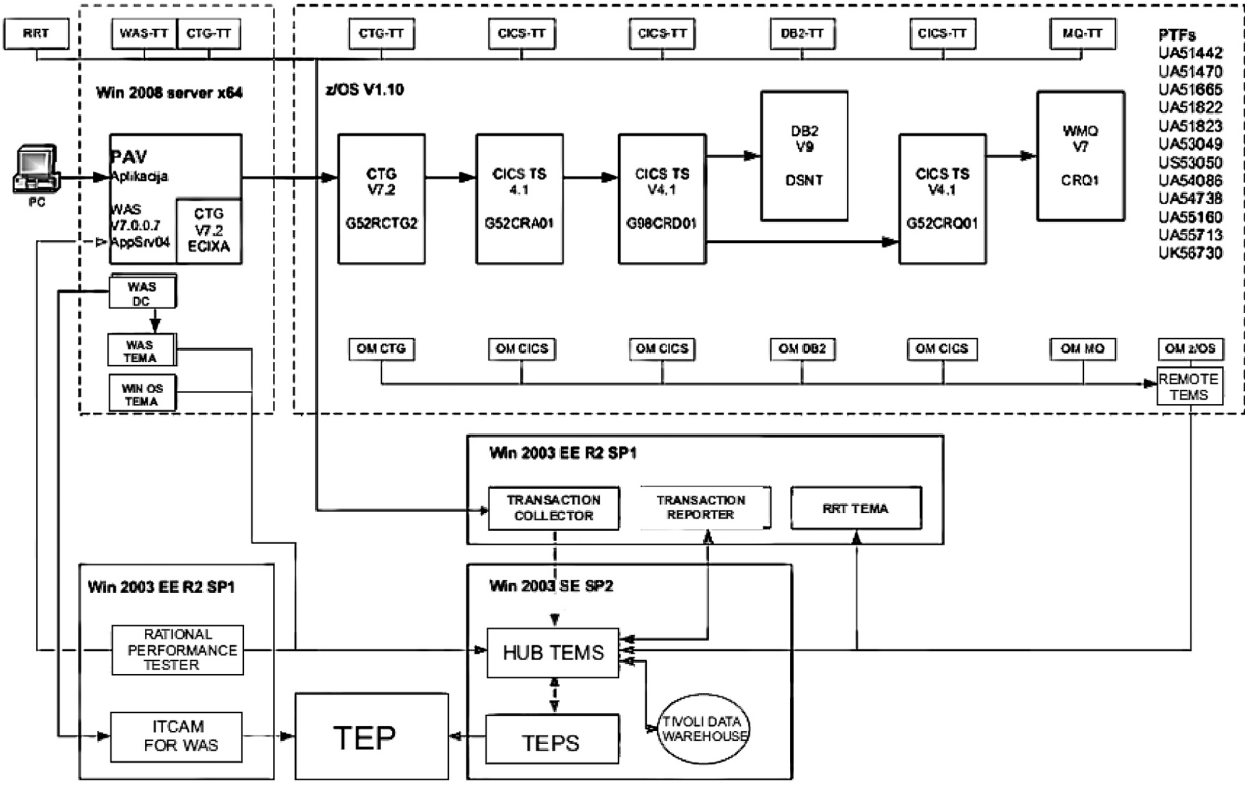
## 5 PREDSTAVITEV NADZORNEGA SISTEMA

Ker večina aplikacij v plačilnem prometu deluje na podobnem principu (več o tem v nadaljevanju), smo uporabili večino najpomembnejših delov nadzornega sistema, ki bodo podlaga nadaljnjemu razvoju oz. implementaciji nadzornega sistema v informacijskem okolju banke. Nadzorni sistem smo preizkusili na aplikaciji PAV (ime PAV ima po projektu Prenova aplikacije in vmesnika). PAV je osrednja aplikacija za podporo plačilnemu prometu v domovini in skrbi za izmenjavo plačilnih transakcij med internimi in eksternimi sistemi. Večnivojska arhitektura sistemskega dela aplikacije, prikazana na sliki 2, kaže vpletenost te aplikacije v heterogeno informacijsko okolje. Uporabniški vmesnik s predstavitveno logiko

aplikacije PAV oz. klient je na WAS-u (angl. Websphere Application Server), ki je nameščen na strežniku windows. Klient je napisan v programskem jeziku java. Samo izvajanje v okolju windows omogoča javin navidezni stroj, s katerim razpolaga WAS. WAS je preko CICS TG (angl. CICS Transaction Gateway) povezan z aplikativnim CICS TS, ki je nato naprej povezan z drugimi CICS TS, s podatkovno bazo in sporočilnim sistemom WebSphere MQ, ki se nahajajo na osrednjem računalniku z operacijskim sistemom Z/OS (angl. Z Series Operating System). CICS TG je nameščen na USS (angl. Unix System Services), ki je integriran v Z/OS. Na osrednjem računalniškem delu se izvaja poslovna logika. Programi s poslovno logiko so napisani v programskem jeziku cobol.

Za popoln nadzor aplikacije PAV je treba na vsaki sistemski komponenti namestiti po dve komponenti nadzornega sistema: eno za spremljanje sistemskih komponent, drugo za spremljanje transakcij. Slika 2 prikazuje arhitekturo sistemskih in nadzornih komponent, potrebnih za izvajanje in nadzor aplikacije PAV. Komponente za nadzor sistemskih komponent, kot so rešitve Omegamon XE, pokrivajo samo osrednji računalniški del in vsebujejo tudi orodja za poglobljene analize. Posamezni Omegamon s svojimi agenti zbrane podatke pošilja prek oddaljenega TEMS-a (angl. Tivoli Enterprise Management Server) na glavni TEMS, od tu pa na TEPS (angl. Tivoli Enterprise Portal Server), kot je to razvidno s slike 2. TEMS je glavni strežnik nadzornega sistema, njegova naloga je zbiranje, filtriranje, koreliranje, analiziranje itn, TEPS pa je strežnik, namenjen za prenos podatkov do TEP-a (angl. Tivoli Enterprise Portal) in za povezovanje s podatkovnim skladiščem (angl. Data Warehouse). TEP je skupen uporabniški vmesnik za nadzor nad celotnim informacijskim sistemom in kritičnimi aplikacijami.

Z orodji Omegamon XE (na sliki 2 so označeni s kratico OM) pokrivamo osrednji računalniški sistemski del, ki je potreben za delovanje aplikacije PAV. Za spremljanje transakcij na osrednjem računalniškem delu potrebujemo še komponente Transaction tracking, to so komponente za sledenje transakcij. Enako kot za sistemski del je tudi za transakcijski del treba namestiti posamezne dele nadzornih komponent oz. podatkovne zbiralnike na vsako sistemsko komponento. Postaviti je treba še strežnike (v našem




Slika 2: **Arhitektura aplikacije PAV, nadzornega sistema za osrednji računalniški in distribuirani del ter orodja za spremljanje transakcij** (Vir: Implementacija IBM Tivoli Monitoring v NLB)

primeru so to strežniki windows), na katerih so nameščene druge komponente, potrebne za zbiranje in povezovanje podatkov, katerih skupek imenujemo Agregation Agent. Agregation Agent je sestavljen iz sklopa Transaction Collector in agentov, imenovanih Web Response Time Agents. Na sliki 2 je ta skupek prikazan kot Transaction Collector. Komponenta za prikazovanje podatkov v obliki grafov in topologij je na sliki prikazana kot Transaction Reporter.

Vsi podatki se prek TEMS-a stekajo v TEPS, pregledujemo pa jih na TEP-u, ki je dejansko glavni nadzorni uporabniški vmesnik. Z TEMS-i, TEPS-om, Omegamoni, komponentami Transaction Tracking, agenti Agregation Agents in transaction reporterjem smo pokrili nadzor osrednjega računalniškega dela informacijskega sistema, ne pa distribuiranega, v katerem se nahaja uporabniški klient za delo z aplikacijo PAV. Za nadzor sistema distribuiranega dela moramo pokrivati strežniško okolje windows (operacijski sistem – na sliki 2 prikazano kot WinOS TEMA), v katerem je aplikativni strežnik (WAS), na katerem se izvaja klient aplikacije PAV, katerega je tudi treba nadzorovati (s pomočjo nadzorne komponente, ki je na sliki prikazana kot WAS TEMA). Uporabili smo še WAS Data Collector, ki pošilja podatke svojemu strežniku (na sliki ITCAM for WAS Managing Server) in omogoča poglobljene analize in grafične prikaze uporabe resursov, s katerimi razpolagata WAS in aplikacija, ki je nameščena na WAS-u (npr. povezava do baze podatkov, povezava do CICS TS prek CICS TG s pomočjo klicev ECI[3]). Za podatke o transakciji in za končni izris distribuiranega dela transakcijske topologije skrbijo komponente ITCAM, ki so na sliki 2 prikazane v kvadratkih pod zgornjim robom slike (WAS-TT, CTG-TT, CICS-TT, DB2-TT in MQ-TT). Te komponente Transaction Tracking pa zbrane podatke pošiljajo neposredno Transaction Collectorju.

Ves nadzorni sistem za aplikacijo PAV, tj. distribuirani in osrednji računalniški sistemski del, je prikazan na sliki 2. Na sliki je prikazana tudi vpletenost testerja Rational Performance (označen z RRT), ki je popolnoma samostojno orodje za performančno testiranje aplikacij na podlagi posnetkov akcij. Tako lahko posnetek uporabnikovega dela na klientu prenesemo v AMC (angl. Application Management Console) in z njegovo pomočjo simuliramo delo uporabnikov na sistemu, tudi ko noben uporabnik ni aktiven (na sliki 2 je simulirani uporabnik razviden kot RRT). S tem pridobimo nadzor nad delovanjem sistema, tudi ko ta miruje in nihče ne uporablja njegovih virov oz. razpoložljivosti. To je tudi eden izmed načinov, kako nadzorovati informacijski sistem, ko na njem ni aktivnosti.

S pomočjo nameščenih komponent nadzornega sistema na vseh komponentah informacijskega sistema pridobimo polno funkcionalnost nadzornega sistema, vključno z orodji za poglobljeno analizo. Ta orodja nam omogočajo hitre detajlne vpoglede v prav vsak del sistema.

## 6 PRIKAZ UPORABE IN TESTIRANJE V PRAKSI

Pri analizi ustreznosti nadzornega sistema smo testirali uporabnost z vidika nadzora sistemskih komponent nadzornega sistema, kakor tudi nadzor kritičnih aplikacij oz. transakcij na primeru aplikacije PAV. Za nadzor sistema uporabljamo grafični vmesnik TEP (slika 3), pri čemer lahko uporabimo različne tipe pogledov. Najbolj osnovni je pogled Query-based, ki v tabeli in grafih prikazuje posamezne atribute in njihove vrednosti. Poglede lahko potem, ko iščemo oz. najdemo vzrok problema, prilagodimo zahtevam, npr. atribut, ki nas zanima, prikažemo v obliki grafa.

Nadaljnji tip pogledov so pregledi dogodkov. V teh pogledih sledimo dogodkom, ki nas zanimajo. Ti dogodki so lahko splošni dogodki, ki se dogajajo na sistemu in se zapisujejo v sistemske dnevnike (»loge«), lahko pa se osredinimo na natančno določene dogodke in prednastavimo situacije. Izberemo atribute sistemskih komponent, na katerih pogosto prihaja do odstopanj, in jim določimo zgornje in spodnje meje odstopanj. Na podlagi teh meja oz. stopenj doseganja dogodka (alarmiranje) obveščamo skrbnike.

Alarmiranje je že eden izmed prispevkov nadzornega sistema. Poleg alarmiranja v določenih situacijah je velik doprinos tudi samodejni zagon procesov (preventivni ukrep), ki se izvede kot odziv na prednastavljeno pravilo. Pravila sproti dopolnjujemo in sčasoma jih lahko postavimo toliko, da sistem skorajda skrbi sam zase. Seveda obstajajo situacije, katerih odprave ne moremo avtomatizirati. Preventivne ukrepe določimo na podlagi preteklih situacij, ki jih poznamo, jih predvidimo ali o katerih imamo podatke v podatkovnem skladišču.

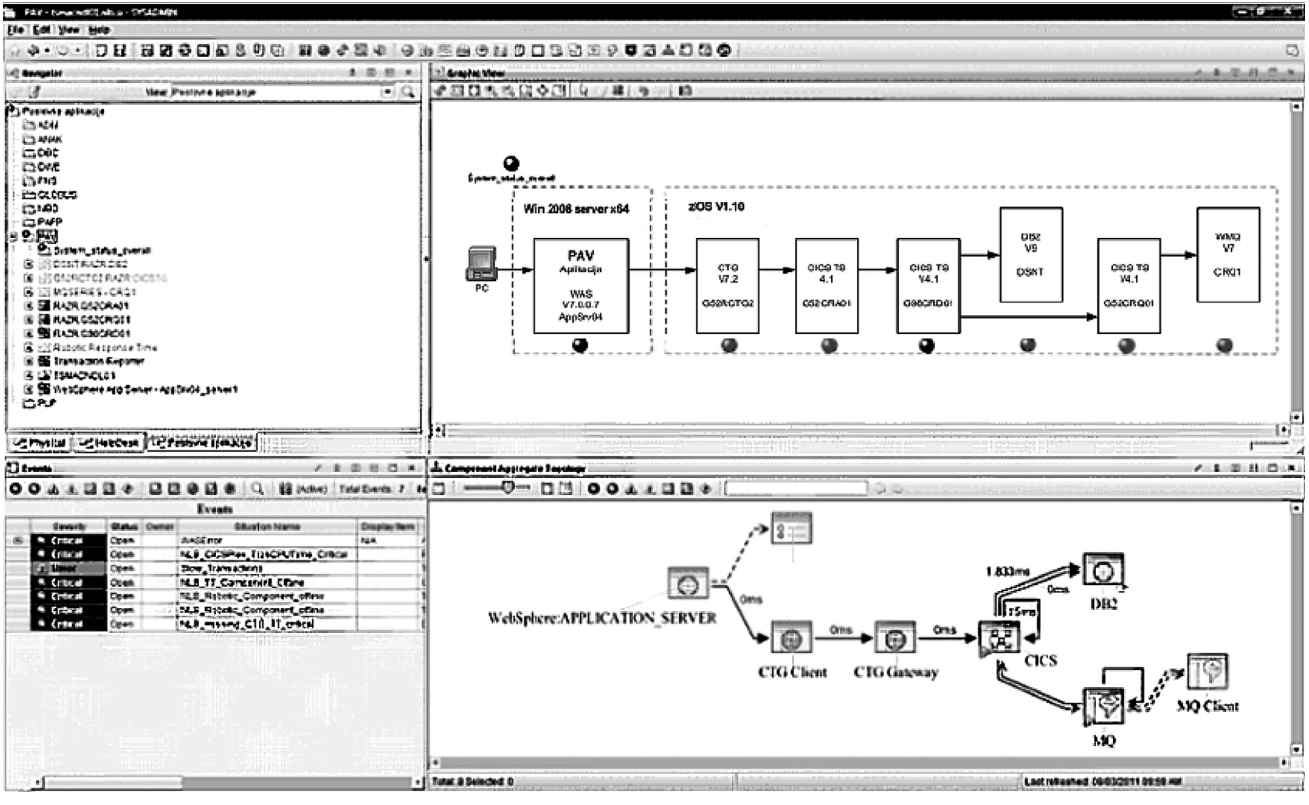
Velik prispevek nadzornega sistema IBM Tivoli je pregled ne le nad celotnim informacijskim sistemom, temveč tudi nad poslovnimi aplikacijami v realnem

[3] ECI (angl. External Call Interface) so klici programov CICS TS iz distribuiranih okolij ali iz paketnih programov osrednjega računalniškega okolja.

času, kar pri obstoječem načinu nadzora ni bilo mogoče. V veliko pomoč pri odpravi napak je tudi samodejno povezovanje in prikazovanje podatkovnih tokov, za katere sploh ne vemo, da obstajajo, ali pa ne vemo, kako potekajo. Na podlagi povezovanja podatkov lahko napako odkrijemo bistveno hitreje. Če bi implementirali še nadzorna orodja za dogodke (Event Management System), kot je Omnibus, bi pridobili še pri t. i. analizi vzroka (Root Cause analysis), ki lahko drastično zmanjša poprečni čas do odprave napake (MTTR – Mean Time To Repair), saj na podlagi zbranih podatkov zna ugotoviti vzrok napake oz. primarno napako, ki je povzročila sekundarno oz. vse ostale napake.

Na sliki 3 v spodnjem desnem okencu je grafični prikaz, na katerem je razviden dejanski transakcijski tok nad njim narisane sheme (skrbniška procesna slika za lažjo predstavnost), na kateri so ob posamezni sistemski komponenti tudi alarmi. Alarmi so v obliki krogcev in prikazujejo, da je napaka na dveh komponentah (na distribuirani WAS, na kateri je nameščena aplikacija PAV, in na osrednji računalniški CICS TS – krogca sta dejansko rdeče barve, na črno-beli sliki pa sta razvidna kot temnejše sive barve, medtem ko so ostali zeleni oz. na sliki svetlo sivi). Napaki sta kritični, sistemski komponenti nista aktivni. Krogci oz. lučke predstavljajo alarme v obliki semaforjev. Kritičnost posamezne napake pa označujejo barve: zelena označuje normalno stanje, modra sporočilo, rumena in oranžna opozorilo, rdeča in črna kritično napako (slika je črno-bela, na sliki so zajete samo zelene – svetlo sive – in rdeče – temno sive – lučke, op. avt.). Alarmi so glede na posamezno komponento tudi opisani v spodnjem levem okencu. V spodnjem desnem okencu pa je razviden realen transakcijski tok v dejanskem času. Med posameznimi komponentami so prikazani tudi odzivni časi (v milisekundah). V tem okencu lahko vidimo, da problematične komponente niso aktivne in so bledе oz. svetlo sive barve.

S klikom na posamezni alarm oz. na povezavo preidemo globlje v prikaz problema, torej na natančno določeno komponento ali sistem in razpolagamo z bolj detajlnimi podatki, ki jih lahko prikažemo tudi v grafih oz. tabelah. Podrobnosti delovanja posameznih sistemskih komponent aplikacije si lahko ogledamo kadar koli.




Slika 3: **Primer nadzora transakcijskega toka** (Vir: Implementacija IBM Tivoli Monitoring v NLB)

## 7 REZULTATI OZ. UGOTOVITVE

Po uspešni implementaciji nadzornega sistema do stopnje, ki že zagotavlja dejansko uporabno vrednost, kot jo je obljubljal ponudnik nadzornega sistema, smo prišli do spoznanj, da učinki uporabe v primerjavi z obstoječim načinom nadzora pričajo o velikem preskoku k lažjemu zagotavljanju nemotenega delovanja informacijskega sistema banke. Če se sklicujemo na postavljene kriterije, lahko podajamo oceno primernosti kot odgovore na zastavljena vprašanja.

- Nadzorni sistem nam omogoča pregled nad delovanjem celotnega informacijskega sistema banke in poslovno kritičnih aplikacij na enem uporabniškem vmesniku. S tem je poenoten način nadzora, saj vsi skrbniki uporabljajo isti uporabniški vmesnik (TEP), poglede pa si priredijo po svojih potrebah.
- Ne glede na heterogenost informacijskega sistema nadzorni sistem omogoča sledenje transakcijam od začetka do konca in njihovo vizualizacijo.
- S pomočjo vizualizacije in prikaza odzivnih časov je lažje odkrivati ozka grla in locirati mesta napak. Ko je napaka locirana, jo lahko odpravimo – problem lahko odpravimo, preden se razširi še na druge komponente informacijskega sistema. Širjenje problema na več komponent informacijskega sistema po navadi pomeni najdaljše prekinitve v delovanju bančnega informacijskega sistema, saj je težko odkriti vzrok problema in ga ustaviti. Ko poznamo vzrok za nastanek oz. širjenje problemskega stanja, lahko akcijo reševanja problema tudi avtomatiziramo.
- Na podlagi postavljenih pravil je mogoče spremljati določene dogodke in zaznati odstopanja ter alarmirati skrbnike oz. izvajati avtomatske akcije odprave problema. Za večino sistemskih napak imamo na razpolago tudi diagnostiko napake in predlagano rešitev, ki jo izvedemo z nekaj kliki z miško. Sam čas zaznavanja napak je odvisen od nastavitev časa osveževanja podatkov, katere pridobivamo iz posameznih komponent prek podatkovnih zbiralnikov.
- Ravno od časa osveževanja podatkov in od števila atributov, katerih podatke zbiramo oz. osvežujemo, je odvisna tudi poraba resursov osrednjega računalnika, na katerem so nameščene komponente nadzornega sistema. Pri uporabi nadzornega sistema smo večinoma uporabljali osnovne nastavitve, pri katerih smo zbirali podatke o vseh atributih posameznih komponent, čas osveževanja podatkov pa je bil nastavljen na 5 do 15 minut. Povprečno se je poraba resursov osrednjega računalnika za potrebe nadzora gibala okoli 15 odstotkov, ob večji obremenitvi osrednjega računalnika oz. ob nastavitvi hitrejšega osveževanja podatkov pa ta naraste tudi do 20 odstotkov in več. Vsekakor bo treba opraviti več testov v predprodukcijskem okolju, v katerem je število transakcij oz. količina podatkov in obremenitev osrednjega računalnika večja. Porabo resursov osrednjega računalnika za potrebe nadzora bo nujno treba zmanjšati. Omejiti bo treba število nadzorovanih podatkov na tiste, ki indicirajo kritičnost. Tudi čas osveževanja podatkov bo treba nastaviti glede na zahteve nadzora posamezne komponente informacijskega sistema. Nekatere komponente potrebujejo bolj pogost nadzor (npr. CICS TS), druge manj (npr. Websphere Q-ji), torej bomo nekatere podatke osveževali na pet minut ali manj, druge pa na petnajst minut. Obstaja še rešitev, da bi oddaljeni TEMS premaknili iz osrednjega računalnika na distribuirano strežniško okolje.
- Prvi vtisi pri upravljanju (namestitvi, uporabi in nadgradnji) nadzornega sistema niso bili najboljši. Orodje je izredno obsežno. Soočali smo se s težavami pri nameščanju komponent nadzornega sistema zaradi nezdružljivosti z različnimi verzijami komponent informacijskega sistema. Sčasoma so zadeve postale bolj razumljive in lažje obvladljive. Vsekakor nam je primankovalo znanja oz. izkušenj. Brez strokovnjakov IBM bi bila zadeva skorajda neizvedljiva. O tem pričajo tudi številni PTF-ji (angl. Program Temporary Fix), nameščeni na različne komponente informacijskega sistema (gl. sliko 2 za seznam). Začasne rešitve in nasvete so strokovnjaki IBM iskali od svojih kolegov po vsem svetu. Ocenjujemo, da bo za upravljanje nadzornega sistema sprva potrebna večja skupina ljudi, pa tudi stalna navzočnost dobavitelja. Sčasoma se število skrbnikov lahko zmanjša na celo manj kot tri osebe. Za nadzor sistema in kritičnih aplikacij bo potrebno občasno sodelovanje skrbnikov nadzornega sistema s sistemskimi tehniki, pa tudi s skrbniki aplikacij. Takšna je bila tudi praksa pri preizkušanju nadzornega sistema.

- K sodelovanju smo povabili skrbnike posameznih sistemskih in aplikativnih sklopov aplikacije PAV. Posamezni skrbniki so izpostavili najpogostejše težave, s katerimi se soočajo. Skušali smo jih simulirati in odpraviti z novim nadzornim sistemom. Ker se težave nanašajo na sistemske in aplikativne dele informacijskega sistema ter zaradi večje obsežnosti in tudi težje razumljivosti simuliranih primerov, so v tabeli 1 združeni splošni primeri reševanja tako sistemskih kot tudi aplikativnih problemov po starem načinu in po načinu z uporabo nadzornega sistema IBM Tivoli Monitoring.

Tabela 1: **Primerjava starega načina nadzora z novim**

| Obstoječi način nadzora | Uporaba nadzornega sistema IBM Tivoli |
|---|---|
| O napaki v delovanju poslovnih storitev nas preko help deska obvestijo uporabniki. | Sistemske napake v delovanju poslovnih storitev oz. njihov nastanek zaznamo pred uporabniki. |
| Za pregled nad delovanjem informacijskega sistema uporabljamo več različnih orodij, ki imajo različno urejene dostope in poglede. S celovitim pregledom nad informacijskim sistemom in povezanostjo komponent ter aplikacijami ne razpolagamo. Slika o trenutnem dogajanju na sistemu oz. o stanju delovanja aplikacij ni jasna, odstopanja ne zaznamo najhitreje. | Kljub uporabi različnih nadzornih orodij znotraj celotnega sklopa nadzornega sistema imamo ves pogled združen na enem mestu – portalu (TEP). Razpolagamo s celovitim pregledom in nadzorom nad informacijskim sistemom in aplikacijami. Natančno vemo, kaj se trenutno dogaja na sistemu ali z aplikacijami, hitro zaznamo že najmanjša odstopanja. |
| S podatki o odzivnih časih razpolagamo le, če smo spremljanje časov programirali v aplikacije oz. opravljali meritve na komponente oz. med njimi. | Nadzorni sistem omogoča spremljanje odzivnih časov med strežniki, aplikacijami, transakcijami. |
| Napako je treba locirati glede na uporabniške razlage iz logov, iz sistemskih izpisov itn. Izkušnje pri delu in pri uporabi različnih orodij so pomemben dejavnik za hitro lociranje napake. | Nadzorni sistem omogoča hitro lociranje napake in pohitritev postopka odprave napake. Dejansko napako lahko zaznamo, tudi če nismo skrbnik oz. strokovnjak na tem področju. |
| Napak na sistemu ne znamo predvideti, razen če jih prej nismo izkusili ali namerno povzročili. | Nastanek napake znamo predvideti v dejanskem času, npr. s pomočjo pregleda nad odzivnimi časi, ki se povečajo, ter tako v delovanju opazimo odstopanja od normalnega stanja. (Višja stopnja uporabe orodja nam ob implementaciji podatkovnega skladišča na podlagi povezovanja pretekih dogodkov zna predvideti napako, ki se je v preteklosti že zgodila.) |
| Ozka grla odkrivamo na podlagi izkušenj, meritev in analiz posameznih sklopov aplikacije oz. komponent informacijskega sistema. | Odkrivanje ozkih grl aplikacij je preprosto, s pomočjo grafičnih prikazov hitro vidimo, kje je treba optimizirati procese, in s tem posledično že lahko zmanjšamo stroške za analizo in načrtovanje za pripravo na povečani obseg poslovanja v prihodnosti. |
| Za predstavnost aplikacij smo skrbeli s procesnimi slikami, narisanimi s procesnimi orodji, kot sta npr. erwin in visio. | Rešitve Tivoli omogočajo lažjo predstavnost, odkrivanje detajlov v delovanju, povezanosti ter lociranja nameščenih sklopov aplikacije po komponentah informacijskega sistema. |
| Za izvajanje ukazov na posameznih komponentah moramo poznati veliko število sistemskih ukazov. | Posamezno orodje nadzornega sistema že vsebuje velik nabor sistemskih ukazov za posamezno komponento. |
| Za nadzor osrednjega računalniškega informacijskega sistema uporabljamo uporabniku oz. skrbniku ne preveč prijazen terminal, grafični prikazi in poročila so redkost. Distribuirana okolja imajo svoje nadzorne produkte. | Uporabniku prijazen vmesnik, poročila so v grafični in tabelarični obliki ter v obliki topologij. Na enem vmesniku nadzorujemo tako osrednji računalniški informacijski sistem, kakor tudi distribuirana okolja. |
| Prehod med komponentami za različne poizvedbe je počasen, potrebne so večkratne prijave v različne sistemske komponente (npr. v vsak CICS TS se je treba posebej prijaviti, prav tako za delo na produkcijskem LPAR-u,[4] administratorski konzoli za WAS itn.). | Za prehod iz pogleda ene komponente na drugo je potreben le klik, avtorizacija se izvede ob prijavi v TEP. |

Iz tabele 1 lahko povzamemo, da je obladovanje informacijskega sistema banke z novim nadzornim sistemom lažje kot z obstoječim načinom nadzora.

Za vodstvo smo sestavili razpredelnico (tabela 2), ki prikazuje prispevek k hitrejši oz. lažji realizaciji strateških ciljev z uporabo nadzornega sistema IBM Tivoli.

[4] LPAR (angl. Logical Partition) – logična enota, navidezno ločevanje strojnih komponent na več logičnih enot, particij.

Tabela 2: **Prispevek k doseganju strateških ciljev po področjih**

| **Strategija informacijske tehnologije v NLB** (Vir: Strategija informacijske tehnologije 2011—2014, interni dokument) | | **Prispevek nadzornega sistema k lažjemu doseganju ciljev** |
|---|---|---|
| **PODROČJE** | **CILJ** | |
| **FINANCE** | *Optimizacija poslovnih procesov, izboljševanje kakovosti, učinkovitosti ter zanesljivosti izvajanja storitev informacijske tehnologije* | S pomočjo sprotnega spremljanja tako sistemskih komponent kot tudi aplikacij ter z vizualnim pregledom nad ozkimi grli bomo zmanjšali stroške poslovanja in stroške, ki nastanejo ob izpadu v delovanju informacijskega sistema oz. aplikacij. Poznavanje problemov je prvi korak pri optimizaciji procesov. Že z odpravo manjših težav lahko prispevamo k izboljšanju učinkovitosti in zanesljivosti storitev informacijske tehnologije. Z uporabo orodij in novosti, ki jih prinaša nadzorni sistem, bomo dolgoročno zagotovo izboljšali stopnjo zanesljivosti informacijskega sistema. |
| **STRANKE** | *Zagotavljanje učinkovite informacijske podpore poslovanju banke, ki bo omogočala uresničevanje ciljev po poslovnih področjih* | Z izboljšanjem zanesljivosti in z optimizacijo procesov bo tudi informacijska podpora poslovanju veliko bolj učinkovita, strankam in poslovnim partnerjem pa bomo ponudili še bolj zanesljive storitve, za katere bomo natančno vedeli, kako delujejo tisti trenutek. |
| **ZAPOSLENI** | *Uporaba orodij, ki zagotavljajo hitro in učinkovito delo, vzpostaviti okolje, ki omogoča razvoj zaposlenih in v katerem so zaposleni temeljni vir* | Nadzorni sistem s pomočjo svojih orodij in napredno tehnologijo na področju sprotnega nadzora in vizualizacije pomaga izboljšati predstavnost in s tem hitrost odpravljanja težav ter optimizacijo delovanja. Tudi avtomatizacija odprave težav bo prispevala k skrajševanju časa za odpravo težav in s tem posledično prispevala, da bodo imeli zaposleni več časa za spremljanje novosti in inovativnih pristopov na svojem področju dela. |
| **PROCESI** | *Povečevanje stroškovne učinkovitosti informacijske in komunikacijske tehnologije* | S poznavanjem procesnih problemov in ozkih grl ter tudi z odpravo le-teh bomo povečali stroškovno učinkovitost informacijske in komunikacijske tehnologije, poleg tega pa se bomo lažje pripravili na povečan obseg dela v prihodnosti, s katerim se že soočamo ob določenih dnevih. |

Dejansko ni nič nenavadnega, da predstavljeni nadzorni sistem posega na vsa področja strateških ciljev. To dokazujejo dejstva, da so si prakse in menedžerski pristopi k izboljšavam strategij informacijske tehnologije pravzaprav zelo podobni. Ustvarjeni so bili različni okviri, da bi pomagali strokovnjakom informacijske tehnologije optimizirati uporabo tehnologije in izboljšati opravljanje procesov informacijske tehnologije. Infrastrukturna knjižnica informacijske tehnologije (angl. Information Technology Infrastructure Library – Itil) zagotavlja nabor najboljših praks, ki pomagajo organizacijam doseči visokokakovostne poslovno usklajene storitve. Osredinja se predvsem na to, kaj je treba storiti, da se zagotovi vrednost storitev informacijske tehnologije, ne razlaga pa, kako to efektivno doseči. To pomanjkljivost lahko premostimo z drugimi pristopi upravljanja storitev (Kastelic in Peer, 2012). Če se vrnemo na ugotovitve v prejšnem odstavku omenjene IBM-ove knjige, pa IBM Service Management in programska oprema IBM Tivoli (ta koncept je prikazan na sliki 1) pomagajo organizacijam, da je opravljanje storitev in ITIL procesov izvedljivo. Rezultat prikazujemo v tem prispevku z opisanim pristopom, ki pomaga izboljšati servisne storitve z izboljšano vidljivostjo, kontrolo in avtomatizacijo.

Tako vodstvo kot tudi skrbniki posameznih področij so bili nad predstavitvijo navdušeni, nekoliko manj pa so bili navdušeni nad kompleksnostjo nadzornega sistema in dokaj veliko porabo virov (CPU) osrednjega računalnika.

Poleg potrebne optimizacije TEMS-a bo moral biti nadzorni produkt nameščen tudi v predprodukcijskem okolju, v katerem bomo v času testiranja aplikacij poleg nadzora delovanja nadzornega sistema, informacijskega sistema in poslovnih aplikacij odkrivali ozka grla, katera naj bi odpravili pred prenosom programske kode in/ali sistemskih nadgradenj v produkcijsko okolje. Informacijski sistem banke naj ne bi dosegel stoodstotne obremenjenosti v produkcijskem okolju, saj bi nas nadzorni sistem na povečanje porabe resursov in/ali na odstopanja od normalnega delovanja opozarjal že veliko prej. Celo več, določene težave bi lahko reševal sam, ko bi nastopile oz. še pred tem.

Seveda pa je pri zaznavanju povečane porabe resursov informacijskega sistema treba ločevati, ali gre za performančne probleme zaradi aplikativnih oz. sistemskih nadgradenj ali je vzrok težav v povečanem obsegu količine podatkov. Ne glede na vrsto težave je treba v takšnih primerih ukrepati zelo hitro. Po Cherkasova idr. (2009) je treba ukrepati takrat, ko uvedemo

posodobitev aplikacije, in/ali takrat, ko se pojavijo nepričakovani performančni problemi. Pomembno je ločiti performančne probleme, katerih vzrok so večje količine podatkov, od performančnih problemov, katerih vzrok so morebitne napake ali neučinkovitosti pri nadgrajeni programski opremi. Po Ganek idr. (2008) so rešitve Tivoli v pomoč pri avtomatiziranem izvajanju korektivnih ukrepov, kakor tudi pri analizi temeljnih vzrokov, saj zagotavljajo korelacijo več informacijskih sistemov na strežniški ravni.

Nekaj komponent nadzornega sistema za potrebe nadzora sistemski komponent smo že namestili v produkcijsko okolje. Uporabljamo jih za zaznavanje odstopanj od normalnega delovanja CICS TS ter za avtomatizirano vključujevanje in izključujevanje obsežnega in potratnega beleženja sistemskih zapisov v primeru povečanega obsega prometa.

Prav tako smo na produkcijskem okolju že avtomatizirali zaznavanje, obveščanje in ponovni zagon enega izmed procesov kupljenega programa ter obsežen ročni poseg, ki ga je treba izvesti ob izpadu delovanja procesa, in tako dosegli, da je ta proces poleg alarmiranja in obveščanja tudi popolnoma avtonomen.

S tem je tudi dokazano, da je vključitev katerega koli produkta pod nadzor pravzaprav mogoča in dokaj preprosta glede na to, za kakšen proizvod gre (lastni razvoj, neki specifični kupljeni proizvod ali prvotni proizvod IBM), pomembno je le, da je nameščen v okolju, ki je pod nadzorom nadzornega sistema IBM Tivoli. Ne moremo se izogniti dejstvu, da je končna rešitev nadzornega sistema velikokrat kombinacija uporabe nadzornega sistema IBM Tivoli Monitoring in programiranih rešitev lastnega razvoja.

Trenutno še nerealizirana naloga in največji izziv bo implementacija nadzornega sistema za potrebe spremljanja transakcijskih tokov v produkcijskem okolju, saj bo transakcijska slika zelo razvejena in prepletena, treba bo odstraniti posamezne, predvsem nepomembne gradnike in narediti sliko pregledno in razumljivo, kar pa ni vedno popolnoma izvedljivo. Tudi z vidika porabe resursov osrednjega računalniškega sistema, velik delež CPU-ja porabi ravno del nadzornega sistema za nadzor transakcij in ga bo nujno treba optimizirati.

Glede na omenjena dejstva iz študije ob uporabi oz. primerjavi nadzornega sistema z obstoječim načinom dela ter skladno s strategijo informacijske tehnologije banke smo opravili analizo SWOT.

### Prednosti

- Celovit nadzor informacijskega sistema banke na enem mestu
- Spremljanje oz. nadzor nad sistemom, aplikacijami in transakcijami
- Izris strežniško-sistemske in transakcijske topologije
- Spremljanje in nadzor povezav med osrednjimi računalniškimi in distribuiranimi sistemi.
- Stalen in sproten performančni nadzor v dejanskem času in prikaz odzivnih časov medsebojne komunikacije med programi, aplikacijami oz. strežniki
- Dvig razpoložljivosti infrastrukture informacijske tehnologije in aplikacij
- Hitra izolacija, diagnostika in odprava nastale težave
- Zgodnje odkrivanje težav
- Možnost zaznave nastanka težave, preden ta nastopi oz. se razširi na ves sistem
- Samodejna odprava težave na podlagi prednastavljenih pravil
- V IBM Tivoli vgrajeni nasveti (najboljša praksa), razširljivi z lastno bazo znanja
- Zmanjševanje poprečnega časa odprave napak (MTTR – Mean Time To Repair) in povečanje poprečnega časa med pojavi napak (MTBF – Mean Time Between Failures)
- Večje zadovoljstvo končnih uporabnikov bančnih storitev (večja zanesljivost in razpoložljivost storitev)

### Slabosti

- Velika poraba resursov osrednjega računalnika CPU (v produkcijskem okolju je ocenjeno na najmanj 15–20 %)
- Draga in dolgotrajna implementacija
- Dokaj nova tehnologija in s tem povezane napake v novih komponentah nadzornega sistema
- Počasno dobavljanje popravkov
- Potrebno je veliko ljudi za upravljanje in vzdrževanje.
- Ni zadosti znanja za samostojno upravljanje sistema nadzora.
- Nadzor in samodejna odprava težav kupljenih specifičnih programskih produktov znata biti težavna, saj v nadzornem sistemu rešitve niso povsem implementirane in zahtevajo razvoj lastnih dopolnilnih rešitev.

### Priložnosti

- Uveljaviti NLB kot sinonim zanesljive banke, ki vedno ve, kaj se dogaja na informacijskem sistemu
- Ponudba zanesljivega informacijskega sistema obstoječim poslovnim partnerjem oz. potencialnim novim
- Uporaba dodatnih orodij za menedžerski nadzor, izdelavo poslovnih poročil
- Nadzor in odkrivanje performančnih problemov kupljenih produktov in specifičnih programskih rešitev zunanjih izvajalcev, ki smo jih doslej lahko obravnavali le kot črno škatlo
- Izboljšanje produktivnosti in stroškovne učinkovitosti z racionalizacijo obstoječih poslovnih procesov (npr. enkratna kontrola nalogov na vhodu in ne večkratna na posameznih podprocesih)

### Nevarnosti

- Ob implementaciji na produkcijsko okolje so lahko slike topologij zaradi velikega števila prikazanih podatkov nejasne.
- Morebitna nezmožnost pokrivanja celotnega informacijskega okolja
- Vzdrževanje nadzornega sistema je drago in zahtevno.
- Vpleteni ne bodo sprejeli novega načina dela, ne bo prave motivacije za delo in uporabo.
- Več stroškov z uporabo nadzornega sistema kot z odpravo težav
- Velika stroškovna in časovna izguba v primeru opustitve programa nadzora

Zaradi kompleksnosti nadzornega sistema v testiranje in analizo nismo uspeli namestiti nekaterih komponent in zato tudi nismo mogli preskusiti teh funkcionalnosti:

- predvidevanja in avtomatizacije odprave napak na podlagi pravil iz preteklih dogodkov z uporabo skladišča podatkov (Data Warehousea); dejansko je to ena izmed rešitev, ki omogoča vzpostavitev avtonomnega sistema;
- nadzora omrežja in delovnih postaj;
- menedžerskega pregleda nad dogodki;
- uvedbe produktov za ekološki menedžment (angl. Green Management).

Bistvo celotnega nadzornega sistema ni več samo nadzor, je tudi zmožnost optimizacije informacijskega sistema, predvidevanja nastanka napak, nižanja stroškov poslovanja itn. Nadzorni sistem je zmožen nadzirati tako rekoč vse, tudi porabo energije, in tako tudi spodbuja oz. pripomore k hitri realizaciji ciljev ekološko usmerjenega menedžmenta.

Kot piše Kovačič (1998: 62), mora načrtovanje informatike izhajati iz strateškega načrtovanja potreb podjetja, ki se zrcalijo v smotru poslovanja, ciljih in strategiji podjetja, opredeljenih v strateškem načrtu podjetja. Ker je informacijska tehnologija eden najpomembnejših delov podjetja, moramo za doseganje poslanstva skupine NLB najprej dosegati strateške cilje informacijske tehnologije. Po dosedanjih spoznanjih bi po mnenju avtorja zastavljene cilje veliko lažje in hitreje dosegli z uporabo novega nadzornega sistema, saj je z njim mogoče poseči v vsa najpomembnejša področja strateških ciljev.

## 8 SKLEP

Implementacija celotnega nadzornega sistema, predvsem nadzor transakcijskih tokov, je zahtevna naloga, za kar potrebujemo razmeroma veliko časa. Na podlagi spoznanj, do katerih smo prišli pri uporabi nadzorne tehnologije, ki smo jo prikazali v članku, ugotavljamo, da je banka naredila korak v pravi smeri. Celovita rešitev pa bo zahtevala še veliko testiranja, nadgrajevanja in optimizacije.

Implementacija predstavljenega nadzornega sistema, predvsem nadzor toka transakcij na produkcijskem okolju banke bo zahtevala tudi strokovno usposobljene in motivirane zaposlene. Usposabljanje in izpopolnjevanje zaposlenih na različnih delovnih področjih že poteka, od ustrezno usposobljenih in motiviranih ljudi pa je odvisna absorpcijska sposobnost. Pomembno je, da gradimo na prednostih in izkoristimo priložnosti, ki nam jih ponuja nadzorni sistem, obenem pa se moramo zavedati nevarnosti in se pripraviti na morebitne negativne scenarije, ki nas čakajo v primeru neuspešne implementacije.

## 9 LITERATURA

[1] Abdul-Malek, A. (2010). Development of system automation and monitoring tool for heterogeneous platforms. Doktorska disertacija. Tennessee State University. ProQuest Dissertations and Theses, pridobljeno 20. 6. 2012 s http://search.proquest.com/docview/516421401?accountid=28931.

[2] Agarwala, S., Bathen, L. A., Jadav, D. & Routray, R. (2010). Configuration discovery and monitoring middleware for enterprise datacenters. *Network Operations and Management Symposium (NOMS)*, 19–23 April 2010 (2010 IEEE), str. 639–646. DOI: 10.1109/NOMS.2010.5488423.

[3] Cherkasova L., Ozonat K., Mi, N., Symons, J. & Smirni, E. (2009). Automated anomaly detection and performance modeling of enterprise applications. *ACM Transactions on Computer Systems*, 27(3), Article No. 6, DOI: 10.1145/1629087.1629089.

[4] Dubie, D. (2004). IBM Tivoli digs deeper into app transactions. *Network World*, 21(40):72.

[5] Ganek, A. G., Hilkner, C. P., Sweitzer, J. W., Miller, B. & Hellerstein, J. L. (2004). The response to IT complexity: autonomic computing. V: *Network Computing and Applications, 2004. (NCA 2004). Proceedings. Third IEEE International Symposium*, 30 Aug.–1 Sept. 2004, str. 151–157. DOI: 10.1109/NCA.2004.1347772.

[6] Haberkorn, M. & Trivedi, K. (2007). Availability Monitor for a Software Based System. *High Assurance Systems Engineering Symposium, 2007. HASE '07*. Dallas, Texas, 14–16 Nov. 2007, str.321–328. DOI: 10.1109/HASE.2007.49.

[7] Hicks, M. (2004). *Optimizing Applications on Cisco Networks*, Cisco Press.

[8] Hu, Y. B., Feng, F., Gucer, V., Huang, J., Jiang, B. & Mackler, R. (2008). Monitoring the IBM Tivoli Composite Application Management Server V6.1, IBM Corp. Redpaper, 24 januar 2008, pridobljeno 20. 6. 2012 s http://www.redbooks.ibm.com/redpapers/pdfs/redp4353.pdf.

[9] Huebscher, M. C. & McCann, J. A. (2008). A survey of autonomic computing-degrees, models, and applications. *ACM Comput. Surv*., 40(3), 7–1 – 7–28. DOI: 10.1145/1380584.1380585.

[10] IBM (2011a). Simplifying administration with IBM Integrated Service Management, (22. 3. 2011), pridobljeno 20. 3. 2012 s http://www-01.ibm.com/software/success/cssdb.nsf/CS/LWIS-8LXG57?OpenDocument&Site=tivoli&cty=en_us.

[11] IBM (2011b). BG-Phoenics extends the benefits of mainframe computing, With the world's first production deployment of IBM zEnterprise with the zBladeCenter Extension, (8 december 2011), pridobljeno 20. 3. 2012 s http://www-01.ibm.com/software/success/cssdb.nsf/CS/STRD-8PBJCA?OpenDocument&Site=tivoli&cty=en_us.

[12] IBM (2011c). Tivoli Monitoring for Transaction Performance (12. 11. 2011), pridobljeno 5. 3. 2012 s https://www.ibm.com/developerworks/wikis/display/tivolidoccentral/Tivoli+Monitoring+for+Transaction+Performance.

[13] IBM Plans New Tools to Support Tivoli System z Management Software (2007). Wireless News (5. december 2007), pridobljeno 10. 4. 2012 s http://business.highbeam.com/165048/article-1P1-146775679/ibm-plans-new-tools-support-tivoli-system-z-management.

[14] Kastelic M. & Peer, P. (2012). Managing IT Services: Aligning Best Practice with a Quality Method. *Organizacija*, 45: 31–37. DOI: 10.2478/v10051-012-0004-6.

[15] Kovačič, A. (1998). *Informatizacija poslovanja*. Ljubljana: Ekonomska fakulteta.

[16] Mulej, M. (2003). Mehanizmi in ukrepi za prenos znanja iz akademske in raziskovalne sfere v gospodarstvo v luči novih inovacijskih paradigem – stanje in trendi razvoja v Sloveniji glede na razvite države EU – absorpcijska sposobnost. Skrajšana verzija raziskovalnega poročila, 5. avgust 2011, pridobljeno 20. 6. 2012 s http://leonardopublic.innovation.si/9.Innovation%20and%20R&D%20support%20system/Mulej-za%20LdV-03Povzetek-absorbSpos%20(Slovenian).doc.

[17] Musich, P. (2004). IBM Broadens Tivoli Tracking; IBM is launching a new version of its IBM Tivoli Monitoring for Transaction Performance software that will greatly expand the range of application transactions it can track. *eWeek*, 21(41): 32, pridobljeno 20. 12. 2011 s http://www.highbeam.com/doc/1P3-712996261.html.

[18] NLB (2011a). Strategija informacijske tehnologije 2011–2014. Nova Ljubljanska banka, interni dokument, 23. 2. 2011.

[19] NLB (2011b). Novice informacijske tehnologije: Predstavitev Oddelka za razvoj upravljanja s podatki in integracijo informacijskega sistema banke. Nova Ljubljanska banka, interni dokument, 20. 7. 2011.

[20] Paxton, N. C., Ahn, G. & Shehab, M. (2011). MasterBlaster: Identifying In»uential Players in Botnet. *Transactions. 35th IEEE Annual Computer Software and Applications Conference*, München, 18–20 July 2011, str. 413–419. DOI: 10.1109/COMPSAC.2011.61.

[21] Sengupta, B., Banerjee, N., Bisdikian, C. & Hurley, P. (2008). Tracking transaction footprints for non-intrusive, end-to-end monitoring. *Cluster Computing*, 12: 59–72, DOI 10.1007/s10586-008-0066-7.

[22] Sterritt, R. (2005). State of the art: Autonomic computing. *Innovations Syst Softw Eng,*1, 79–88, DOI 10.1007/s11334-005-0001-5.

[23] Veyder, F. (2003). Case study: Where is the risk in transaction monitoring? *Journal of Financial Regulation and Compliance*, 11(4): 323–328. DOI: 10.1108/13581980310810606.

[24] Wang, K., Wu, Z., Luan, Z. & Qian, D. (2008). Reducing the Cluster Monitoring Workload by Identifying Application Characteristics, *GCC '08 Proceedings of the 2008 Seventh International Conference on Grid and Cooperative Computing*, IEEE Computer Society Washington, DC, USA, str. 525–531. DOI: 10.1109/GCC.2008.56.

[25] Yang, F., Shao, P., Le, Q., & Li, D. (2010). Commentary on the Supervision of Foreign Banking IT Risks. *International Conference on E-Business and E-Government (ICEE)*, Guangzhou, 7–9 May 2010, str. 2026–2028. DOI: 10.1109/ICEE.2010.512.

▪

Simon Sirc je zaposlen kot samostojni sistemski analitik v NLB, d. d., v sektorju za razvoj informacijskega sistema banke, kjer skrbi za razvoj in nemoteno delovanje sklopa poslovno kritičnih aplikacij plačilnega prometa v domovini. Leta 2006 je diplomiral na Fakulteti za organizacijske vede Univerze v Mariboru. Na isti fakulteti končuje magistrski študij.

▪

Jože Zupančič je upokojeni redni profesor na Fakulteti za organizacijske vede Univerze v Mariboru. Njegovi raziskovalni interesi so razvoj in uvajanje računalniških rešitev in informacijskih sistemov.