

POSLEDICE KRITIČNIH RAČUNALNIŠKIH PROJEKTOV

Bojan Peček

1. VODENJE RAČUNALNIŠKIH PROJEKTOV

Veliko truda je bilo vloženega v zagotavljanje kakovosti razvoja sistemov. Pretežni del in učinkovitost lahko zaznamo na mikro nivoju kot npr. izpopolnjena programska orodja, vse boljša CASE orodja, itd. Ob vse bolj kompleksnih sistemih pa prihaja v ospredje skrb za izvedbo celotnega projekta, neke vrste makro politika kakovosti vodenja in upravljanja projekta.

Načela vodenja računalniških projektov so splošno znana. Vsi se strinjamo, da je pred začetkom dela na projektu potrebno izdelati uvodno študijo z določitvijo potrebnih resursov za izvedbo projekta, določiti realne plane izvedbe, definirati omejitve, postaviti realne cilje itd. Pri tem veljajo načela upoštevanja želja in mnenje končnega uporabnika, izdelava robustnega sistema, planiranje in načrtovanje testiranja, pravočasno šolanje končnih uporabnikov itd. Toda ali se teh preprostih in logičnih načel resnično vedno držimo?

Življenje nas pogosto sili, da sprejemamo odločitve izven strokovnih sfer. Določene sile pač pritiskajo tako, da sprejemamo odločitve, ki so v nasprotju z logiko, ki temelji na strokovnih argumentih. Žal je tak primer uvedba računalniško podprtega sistema Londonske reševalne službe, ki se je dogodil 26. in 27. oktobra ter 3. novembra 1992.

2. POČEK DOGODKOV V LONDONSKI REŠEVALNI SLUŽBI

Londonska reševalna služba pokriva področje veliko 600 kvadratnih milj in je na razpolago okoli 6,8 milijonu stalnih prebivalcev, kar se zaradi dnevne migracije še povečuje. Dnevno prejmejo okoli 2.000 do 2.500 klicev, od tega 1.300 do 1.600 klicev 'na pomoč'. Skupno prepeljejo dnevno 5.000 ljudi.

Tragična zgodba ima zametek v letu 1990, ko so opustili dotedanji osem let trajajoči projekt računalniške podpore razporejanja reševalnih vozil zaradi preslabih performans ob vzpostavitvi. 'Po zlu' je šlo 7,5 milijona funtov. Velika vsota? Morda, toda opustitev šestletnega projekta 'Taurus' za vzpostavitev brezpapirnega poslovanja Londonske borze je veljal celo 400 milijonov funtov, ampak to je druga zgodba. Če se vrnemo k Londonski reševalni službi, so finančne posledice še najmanj pomembne.

Torej po neuspelem lansiranju prvega projekta so razpisali ponoven projekt. Novi sistem je obsegal:

- sprejem klica,
- optimalno določitev reševalnega vozila za izvedbo intervencije,
- mobilizacijo voznika,
- strateško razporejanje opreme (vozil na najbolj optimalno mesto za hitro posredovanje).

Za realizacijo so potrebovali programsko opremo, strojno opremo, programsko opremo za geografski leksikon in mestni načrt, komunikacijski vmesnik, mobilni terminalski sistem ter sistem

za avtomatsko določanje lokacije vozila. Razvoj dogodkov (ne sistema) tako kompleksnega sistema je bil bliskovit: od jeseni '90 do februarja '91 opredelitev sistemskih zahtev, 7. februarja 1991 izide oglas za zbiranje ponudb v Journal of the European Communities, predvidena uvedba sistema planirana že za 8. januar 1992.

Seveda so bila predvidena testiranja. Sprva so celoten sistem aktiviranja vozil vodili ročno in računalniški sistem uporabljali paralelno. Poiskusni meseci so dokazovali ogromno napak. Stalno se je menjala, dograjevala ter izpopolnjevala oprema za javljanje, odpravljanje so se napake v programski opremi itd. V celoti z vsemi komponentami pa sistem ni bil testiran nikoli. Posebno ne pod največjimi obremenitvami. Kritična je bila zadnja faza projekta, ko je računalnik prevzel tudi kontrolo nad določanjem vozil za posamezno intervencijo.

Navkljub evidentiranim napakam in opozorilom, dejstvu, da večina osebja ni primerno izobražena ter da se celoten sistem ni nikoli povsem preverjen, se je vodstvo Londonske reševalne službe konec oktobra odločilo, da spravijo sistem v življenje brez klasičnega ročnega nadzora.

Odziv je bil katastrofalen. Sistem je temeljil na popolni informaciji, ki je v realnosti ni mogoče doseči - enostavno ni bil dovolj robusten. Prišlo je tudi do ozkega grla na radijski povezavi. Drobne napake, ki same niso bile usodne za delovanje sistema, so se medsebojno množile in naglo potencirale. Prišlo je do popolnega zastoja.

V praksi se je to odrazilo tako, da so ljudje dolgo čakali na rešilne avtomobile. Po dolgotrajnem čakanju so ponovno javljali isti nujni primer. To pa je le še dodatno zasitilo sistem, saj je razporedil novo vozilo za isti primer. Za nove primere pa je zmanjkovalo razpoložljivih vozil. Mnogi bolniki z infarktom so se zato raje odpravili v bolnišnice s taksijem. Enkrat pa je reševalni službi uspelo prispeti do kraja nesreče potem, ko je bil že na poti mrlški voz pogrebnega zavoda.

3. IZSLEDKI RAZISKOVALNE KOMISIJE

Dogodek je dobil seveda izreden odmev v medijih. Državna sekretarka je organizirala tričlansko preiskovalno komisijo. Slednja je februarja 1993 izdala poročilo o opisanih dogodkih. Obsega 80 strani, zajema tako napake pri razpisu natečaja, izboru izvajalcev, izvajanjem in testiranjem projekta kot tudi potrebne najbližje akcije za povrnitev ugleda in zaupanja v reševalno službo, kot tudi ideje pri nadaljevanju dela.

Ugotovitve?

Pravzaprav nič posebnega, česar ni mogoče prebrati že v strokovni literaturi. Popolna odtujenost računalniškega osebja od dejanskih uporabnikov.

V posebno frustrirani situaciji so se znašle reševalne ekipe.

Računalnik je brezkompromisno odredil za intervencije vedno najbližje vozilo. Posamezni vozniki so se zato vse bolj oddaljevali

od področja, ki so ga poznali, v nepoznane sisteme enosmernih ulic. Morda gre njihovemu revoltu pripisati marsikateri napačno aktivirani gumb na njihovih mobilnih terminalih, padanje v 'radijske tišine' itd.

Vsekakor so se vse drobne napake potencirale. Zaradi ponovnih klicev po izteku razumnega časa so imeli v kontrolnem centru občutek, da je bilo tisti dan enormno veliko klicev. Pogošto so na isto mesto razporejali več vozil. Slednjih je tako primanjkovalo za tekoče intervencije.

Čeprav je predmet študije odpoved sistema, pa sistem 26. in 27. oktobra ni odpovedal v klasičnem smislu. Samo odzivni čas sistema je bil tako problematičen, da se je odražal z enakimi simptomi kot da bi se to resnično dogodilo. Očitno sistem ni bil pripravljen za preživetje v prekomerno obremenjenem okolju. 3. novembra, ko je sistem odpovedal v klasičnem smislu, pa se je izkazalo, da preklon na rezervni sistem sploh ni bil stestiran.

Splošna ugotovitev preiskovalne ekipe je bila, da je "popolnoma jasno, da računalniško podprt dispečerski sistem, niti njegovi uporabniki niso bili pripravljeni 26. oktobra. Programska oprema ni bila celovita in nepopolno testirana. Obstajali so očitni problemi pri podatkovnem prenosu na mobilne terminale in nazaj. Obstajalo je nekaj skeptičnosti o natančnosti sistema avtomatskega določevanja pozicije avtomobila. Osebe tako v osrednjem kontrolnem centru kot v reševalnih ekipah ni imelo zaupanja v sistem in ni bilo dovolj izšolano in trenirano.

Fizične spremembe v kontrolni sobi so povzročile, da je osebe delalo v nedomačem okolju, brez papirnega back-upa. Noben poiskus ni bil napravljen za ugotovitev učinkov nepopolnih, napačnih ali nepravilnih podatkov sistemu. Vse te nepopolnosti so vodile v povečanje izrednih klicev, kar je potenciralo problem. Odločitev, da se tisti dan uporablja samo računalniško razporejanje virov, (kar je bilo dokazano manj kot 100% zanesljivo) je bil visoko rizičen korak".

Morda še kot zanimivost, da raziskovalna ekipa v svojem zaključku ugotavlja, da je problem medijsko prenapihnen. V predzadnjem odstavku študije ugotavlja, da "obstaja dejstvo,

da od 26 primerov proučenih od kronskega zbora niti za enega ni bilo ugotovljeno, da lahko Londonsko reševalno ekipo obtožimo za smrt pacienta".

4. ZAKLJUČEK

Nauk, ki ni posebno zapisan, vendar veje med vrsticami študije komisije je očitna odtujenost vseh vodstvenih struktur. Vodstvo Londonske reševalne službe je bilo odtujeno od realnosti izvedbe projekta. Stalno so imeli strogo pred očmi finančno katastrofo prvega projekta in so se zato toga držali finančnih okvirov. Za vodenje projekta in realizacijo so izbrali manjšo firmo, ki ni imela ustreznih izkušenj. Še posebno ne s tako kompleksnim problemom. Očitno je bila cena daleč najvažnejša postavka pri izbiri partnerjev.

Projektni team je bil vdan v usodo. Vodja projekta je bil tako npr. človek, ki je sprva delal v ekipi reševalnega vozila, kasneje je skrbel za komunikacije. Ni bil računalniško izšolan. Njegov predpostavljeni mu je dal jasno vedeti, da bo v kratkem zamenjan s primerno kvalificiranim delavcem. Lahko si je zamisliti njegovo voljo do dela.

Pod posebnim pritiskom je bilo tudi vodstvo dispečerske službe, saj si ni moglo privoščiti podaljšanja roka uvedbe sistema ali prekoračitve zneska dodatnih sredstev. Čeprav mnogih njihovih ukrepov preposto ni mogoče razumljivo opravičiti.

Nobene nove ugotovitve torej. Toda če pomislimo, da je veliko več prometnih nesreč povzročenih zaradi nepazljivosti in raztresenosti kot neznanja, potem velja snovalcem rizičnih sistemov opozorilo.

VIR:

REPORT OF THE INQUIRY INTO THE LONDON AMBULANCE SERVICE - Februar 1993

Robert Erskine: "QUALITY ASSURANCE DYNAMICS REQUIRED IN MISSION CRITICAL SYSTEMS", Software Quality Management Vol 1. - Computational Mechanics Publications 1994.

Podatkovne baze in koncept uporabnik - strežnik

Poročilo o konferenci v Bostonu, 13. do 15. junija 1995

Franco Kremžar

Prišel je čas, ko se poslovi pomlad in se spet pogovarjamo o stanju informatike na področju koncepta uporabnik-strežnik. Tak je bil morda malo romantičen moto enega največjih ameriških seminarjev s tega področja informacijske tehnologije pred nekaj dnevi v Bostonu, bolj konkreten je pa bil: prehod informacijske tehnologije od teorije k praksi.

Ključna spoznanja s tega posvetovanja so naslednja: arhitektura uporabnik-strežnik je arhitektura koncepta obdelave informacij na prehodu iz dvajsetega v enaindvajseto stoletje. Koncept skladiščenja podatkov v relacijskem modelu doživlja svojo potrditev in uporabniški programi, pisani v cobolu, so še vedno aktualni. Pričenja se pa obdobje skladiščenja specializiranih podatkov (data warehousing), ponovljenih podatkov (replication),