Poglavje 1

Uvod

Z vsesplošno vpeljavo *digitalizacije*[1] in *informatizacije*[2] upravljanje s svojim okoljem vse bolj prepuščamo avtomatiziranim sistemom, ki temeljijo na uporabi računalniških sistemov. Slednje vodi v eksplozijo števila tako večjih kompleksnejših, kot tudi manjših enostavnejših računalniških sistemov. Če smo bili do sredine 90-ih let prejšnjega stoletja priče predvsem masovni popularizaciji rabe osebnih računalnikov, smo danes priče poplavi pametnih mobilnih telefonov, digitaliziranih osebnih pripomočkov (npr. naprav za merjenje vitalnih življenskih funkcij), digitalizacije ambientalnega okolja na osnovi vgrajenih sistemov (npr. digitaliziranih naprav bele tehnike in upravljanja s prostori) itd. Še pestrejša bo prihodnost, saj so pred nami izzivi digitalizacije in informatizacije prometa, logistike, področij oblačil in prehrane, zdravstva, osebnega nadzora itd. V pričujočem delu vse navedene digitalizirane informacijske rešitve poimenujemo za *računalniške sisteme*.

Poleg *eksplozije števila računalniških sistemov* smo priče tudi *rasti kompleksnosti funkcij*, ki jih ti sistemi vršijo in *kompleksnosti njihove zgradbe*. Za ponazoritev kompleksnosti funkcije vzemimo samo navidezno lahek problem prepoznavanja osebe iz digitalne rastrske slike, za katerim se skriva procesno - računsko intenziven algoritem, ki od računalniškega sistema terja ustrezne sofisticirane rešitve že na nivoju strojne opreme.

Glede na povedano smo snovalci računalniških sistemov v prelomnem času, v katerem živimo, soočeni z naslednjimi dejstvi:

- število računalniških sistemov v eksploataciji[3] in njihova kompleksnost strmo naraščata;
- kompleksnost računalniških sistemov narašča hitreje, kot metode za njihovo verifikacijo[4];

[1] Digitalizacija - proces pretvarjanja analognih informacij v digitalne [1].

[2] Informatizacija - postopek vpeljave informatike in informacijskega sistema v ciljno poslovno okolje (npr. v bančništvo, zdravstvo, javno upravo, trgovino, policijo itd.).

[3] Eksploatacija sistema - uporaba sistema za reševanje nalog v realnem okolju.

[4] Verifikacija - postopek preverjanja pravilnosti delovanja sistema in njegove skladnosti s

- uporabniki računalniškim sistemom vse bolj zaupamo in smo od njihovih storitev vse bolj odvisni;
- globalnost trga računalniških rešitev zahteva vse krajše čase od idejne zasnove produkta do njegove pojavitve na trgu[5]; s tem se razpoložljivi čas za razvoj zanesljivih produktov iz leta v leto drastično krajša, posledično pa krajši časi ne zagotavljajo „zrelosti“ produkta ob njegovi pojavitvi na trgu;
- predvsem na področju razvoja programske opreme smo priče hitremu porajanju novih paradigem razvoja programske opreme in novih razvojnih okolij;
- na mnogih področjih razvoja računalniških rešitev smo snovalci ostali brez regulatornih normativov za njihovo realizacijo (pod regulatorne normative smatramo standarde, priporočila, certificiranje rešitev, nacionalne smernice in omejitve itd.);

Snovalci in razvijalci računalniških rešitev se moramo glede na predhodno naštete alinee zavedati svoje odgovornosti za zagotavljanje zanesljivega delovanja razvitih produktov in storitev. Pod besedno zvezo *zavedanja odgovornosti* smatramo razvijalčevo zavedanje in jasno opredelitev do rizikov in posledic (angl. *risk and effects*), do katerih lahko pripelje nepravilno delovanje ali nedelovanje razvite računalniške rešitve.

1.1 Odnos ponudnik - kupec v domeni računalniških rešitev

Na področju računalništva se zaradi njegovega *hitrega razvoja*, *nereguliranosti področja* in *globalnosti trženja* soočamo z množico problemov, ki izvirajo iz neurejenega ali (še) nedozorelega odnosa med *kupcem* računalniške rešitve in njenim *ponudnikom*, ki vrši bodisi funkcijo *snovalca* in *razvijalca* računalniške rešitve, ali zgolj funkcijo *integratorja* (povezovalca) množice že obstoječih rešitev v enoten računalniški sistem. V splošnem lahko ugotovimo, da smo kupci praviloma premalo kritični do ponujenih rešitev s strani ponudnikov. Slednjo ugotovitev lahko podpremo s ključnimi vprašanji v alineah v nadaljevanju, na katera si kupci pred nakupom neke računalniške rešitve običajno ne odgovorimo. Le ta so sledeča:

- Ali ponujena računalniška rešitev vrši samo željene - zahtevane funkcije, ali lahko ob določenih pogojih vrši tudi neželjene?
- Ali lahko ponujena računalniška rešitev ob prisotnosti posamezne odpovedi vodi do delovanja, ki je za uporabnika nesprejemljivo?

sistemskimi zahtevami.

[5] »Svet se spreminja zelo hitro. Veliki ne bodo več premagovali majhnih. Hitri bodo premagovali počasne.« (Rupert Murdoch) [1].

- Kakšne garancije za pravilno delovanje ponujene računalniške rešitve nudi ponudnik?
- Kakšne materialne škodne posledice je pripravljen nase prevzeti ponudnik ob neustreznem delovanju računalniške rešitve?

Poleg predhodno naštetih vprašanj, na katera si kupec običajno ne odgovori, obstaja še množica vprašanj, ki jih kupec običajno ne zastavi ponudniku, ali pa odgovori nanje vsaj niso pogodbeno dogovorjeni. Ta vprašanja so sledeča (navajamo le tista, ki se tičejo zanesljivosti delovanja sistema):

- Kakšne zanesljivostne analize je ponudnik izvedel za računalniško rešitev, ki jo ponuja?
- Kakšen je pričakovani čas do odpovedi ponudnikove računalniške rešitve?
- Kakšna je pričakovana življenska doba ponudnikove računalniške rešitve?
- Kakšna je dosegljivost[6] računalniške storitve ponudnika?
- Kako in koliko časa je potekalo testiranje ponudnikove računalniške rešitve?
- Kolikšen je čas popravila ponudnikove računalniške rešitve in kdo ter pod kakšnimi pogoji bo popravilo izvedel?

Pri opisih v pričujočem razdelku smo se sklicevali na pojem *računalniške rešitve*. Pomensko nam predstavlja kakršnokoli strojno in/ali programsko izvedbo reševanja nekega problema v realnem okolju. V nadaljevanju pričujočega dela se bomo na pojem računalniške storitve sklicevali z bolj razširjenim terminom *računalniškega sistema*.

1.2 Klasifikacija računalniških sistemov z vidika željene zanesljivosti

Z vidika namena eksploatacije in s tem posredno tudi z vidika željene zanesljivosti delovanja računalniške sisteme delimo po viru [2] na naslednje štiri skupine:

- *splošno namenski računalniški sistemi* (angl. *general purpose computers*): mednje sodijo osebni računalniki, pametni mobilni telefoni, tablični računalniki itd.;
- *visoko dosegljivi transakcijski sistemi* (angl. *on line transaction processing systems* - OLTP): mednje sodijo visoko dosegljiva „osrčja“ distribuiranih računalniških sistemov, kot so npr. bančni strežniki, strežniki za vodenje

[6] Dosegljivost (angl. *availability*) - kvantitativno jo izrazimo z razmerjem med časom pravilnega delovanja računalniške storitve in dolžino časovnega intervala opazovanja delovanja storitve.

prodaje letalskih kart, strežniki za vodenje transakcij plačilnih kreditnih kartic itd.; pri tem poudarimo, da v to skupino ne sodijo končne delovne točke (angl. *end points*) v tovrstnih sistemih; slednje sodijo v skupino splošno namenskih računalniških sistemov;

- *sistemi z dolgimi misijami* ali zahtevanimi *dolgimi življenskimi dobami* (angl. *long mission systems*, *long life systems*): mednje sodijo vsi tisti računalniški sistemi, ki morajo biti v eksploatacijski dobi vsaj do neke mere avtonomni[7]; v primeru željene avtonomnosti računalniškega sistema predvidevamo, da ne bomo imeli možnosti poseganj v obliki nadgradenj in servisiranj sistema v predvidenem času misije ali v predvidenem času življenske dobe sistema, ali pa bodo takšna poseganja cenovno izredno draga; v to skupino sodijo tako kompleksni računalniški sistemi na misijah v vesolju, kot tudi tako enostavne računalniške rešitve, kot so digitalizirani gospodinjski aparati stacionirani v domovih končnih uporabnikov;

- *misijsko kritični sistemi* (angl. *critical mission systems*, *life critical systems*, *critical computations*): mednje sodijo vsi tisti računalniški sistemi, ki bi s svojim nepravilnim delovanjem lahko neposredno ogrozili zdravje ali življenje človeka; tipični primeri tovrstnih rešitev so npr. digitalizirane rentgenske medicinske naprave, računalniško krmiljenje kompleksnih procesov (npr. jedrskega reaktorja), digitalizirani orožarski navigacijski sistemi, računalniški sistemi v potniških letalih, navigacijski sistemi itd.

Najmanj zanesljive računalniške naprave najdemo v prvi skupini, nato pa zanesljivost po skupinah narašča, kar vpliva tudi na ceno računalniških rešitev, ki po skupinah eksponentno narašča. Cenovni primerjalni vidik velja tako za strojno opremo (npr. cene posameznih vgrajenih strojnih komponent) in programsko opremo (npr. ceno na vrstico izvorne programske kode), kot tudi za izvajanje drugih faz življenskega cikla računalniškega sistema (npr. za testiranje računalniškega sistema pred fazo eksploatacije).

1.3 Vzorčni incidenti in nesreče z vpletenimi računalniškimi sistemi

V pričujočem razdelku predstavimo nekaj odmevnih vzorčnih incidentov in nesreč iz preteklosti, v katere so bili vpleteni računalniški sistemi. Na tem mestu najprej razložimo pomena besed *incident* (angl. *incident*) in *nesreča* (angl. *accident*). Opisana razlika med pomenoma besed je povzeta po semantiki terminologije področja zanesljivosti [3] in je sledeča:

- **incident** (angl. *near hit*, *near miss* - skorajšnja nesreča) predstavlja nepričakovan dogodek, ki prekine normalno delovanje sistema in rezultira v

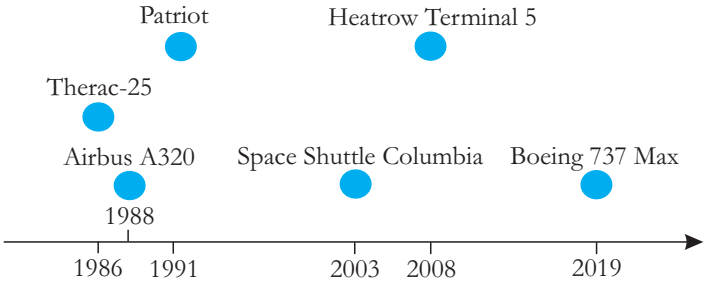
[7] Avtonomen sistem - sistem, ki deluje samostojno in neodvisno od drugih sistemov (Vir: SSKJ).

gospodarsko škodo (angl. *property damage*), ne rezultira pa v poškodbe ali bolezni ljudi;

- **nesreča** predstavlja nepričakovan dogodek, ki prekine normalno delovanje sistema in rezultira v poškodbe ali bolezni ljudi, lahko pa poleg tega rezultira tudi v gospodarsko škodo;

- vsako nesrečo smatramo tudi za incident, ne velja pa nasprotna posplošitev, da vse incidente smatramo za nesreče;

Časovna razporeditev v nadaljevanju opisanih incidentov in nesreč je predstavljena na sliki 1.1. Vzorčni incidenti in nesreče po eni strani poudarjajo



Slika 1.1: Časovno porajanje odmevnih vzorčnih incidentov in nesreč, v katere so bili v preteklosti vpleteni računalniški sistemi. Ker je izbira incidentov in nesreč izvedena po subjektivni presoji avtorja pričujočega dela, v prikazani časovni porazdelitvi ne iščemo nekih specifičnih zakonitosti njihovega časovnega porajanja.

pomembnost in izpostavljenost računalniških sistemov, ki nastopajo v misijsko kritičnih aplikacijah, po drugi strani pa izpostavljajo pomembnost področja zagotavljanja zanesljivosti. Kakršenkoli incident ali nesreča navkljub neljubim posledicam ne omogočata samo odprave eventuelnih napak v računalniških sistemih, temveč tudi razvoj *metod analize zanesljivosti* računalniških sistemov, njihove *standardizacije* in *certifikacije*.

1.3.1 Therac 25

Therac 25 je bil po napravah Therac 6 in Therac 20 tretji član produktne družine računalniško vodenih terapevtskih obsevalnih medicinskih naprav kanadskega proizvajalca Atomic Energy of Canada Limited (AECL, danes (op.p. l. 2016) Theratronics Ltd.), ki se je pojavil na tržišču leta 1983. Uporabljal se je za tretmaje rakastih tumorjev. Računalniški del sistema Therac 25 je temeljil na mikroračunalniku, sama programska oprema pa je imela približno 20.000 vrstic izvorne kode (angl. *lines of code* - LOC). Razvita je bila s strani ene osebe v nekaj letih razvoja. V letih od 1985 do 1987 je bila naprava vpletena v šest

nesreč, v katerih so pacienti prejeli prevelike, v večini primerov kar stokratne odmerke sevanja v primerjavi s predpisanimi.

Nesreča št.1

Do prve, nemudoma javno objavljene nesreče pride 21.marca 1986, v kateri pacient neposredno po prejeti dozi sevanja potoži o občutku prejetja elektrošoka, čeprav je imel predhodno dobre izkušnje z obsevanji. Operater - radiolog je z računalniškega krmilnega monitorja med obsevanjem uspel le prebrati sporočilo „`Malfunction 54`“, pri čemer je po proizvajalčevih navodilih to pomenilo bodisi predoziranje ali pa poddoziranje pacienta z obsevanjem. Napravo so po nesreči testirali, ker pa sistema niso uspeli spraviti v stanje, da bi se zopet odzval s sporočilom „`Malfunction 54`“, so napravo še istega dne vrnili v redno obratovanje in izvedli vse planirane obravnave. Še iste noči se je obsevani pacient zglasil v urgentni službi iste bolnišnice, kjer je na osnovi pordečelosti kože dobil diagnozo poškodb zaradi prejetja elektrošoka. Vsled temu je bolnišnica napravo umaknila iz rednega obratovanja in jo podvrgla intenzivnemu testiranju, ki je trajalo vse do 7.aprila 1986. Ker slednje naprave ni pripeljalo do odziva s sporočilom „`Malfunction 54`“, so napravo tega dne vrnili v redno obratovanje.

Nesreča št.2

Do druge, nemudoma javno objavljene nesreče pride 11.aprila 1986 na isti napravi v isti ustanovi. V tem primeru je po obsevanju pacient dobil vidne ožganine po obrazu. Da bi bila zgodba še bolj zapletena, je z napravo upravljal isti operater - radiološki inženir kot v prvi nesreči, kar bi lahko pomenilo tudi to, da je problem pri odzivanju naprave pogojen z načinom njegove interakcije s krmilnim računalniškim programom. Pacient z ožganinami je po treh tednih umrl. Avtopsija je pokazala, da je pacient resnično prejel prekomerno dozo sevanja, istočasno pa so se pojavili tudi podatki o tem, da se je s hudimi zdravstvenimi težavami, ki bi lahko bile posledice prekomernega obsevanja, soočil tudi pacient iz 1. nesreče. Slednji umre po šestih mesecih. Na osnovi ožganin drugega pacienta in zdravstvenih problemov prvega bolnišnica 11.aprila 1986 obvesti o problemih proizvajalca naprave, samo napravo pa izvzame iz rednega obratovanja in začne z njenimi intenzivnimi testiranji. Cilj slednjih je bil določiti robne pogoje, pri katerih se naprava odzove s predoziranjem, ki se manifestira s predhodno navedenim sporočilom.

Po ponovnih intenzivnih testiranjih bolnišnično osebje in strokovnjaki iz AECL 15.aprila 1986 pridejo do ugotovitve, da se v primeru prehitre interakcije s programom za vnos podatkov o obravnavi (vrsta in jakost sevanja itd.) računalniški program ne odziva več po vnešenih podatkih, temveč sam izbere stokratnik predvidene doze in sami napravi izda ukaz za izvedbo obsevanja. Vpletena bolnišnica in AECL o ugotovitvah seznanita FDA (Food and Drug Administration) in preostalih 10 bolnišnic v ZDA in Kanadi, ki so uporabljale enake tipe naprav. Temu priložita nova navodila za način vnosa podatkov o obravnavi. Navkljub temu FDA 2.maja 1986 do nadaljnjega prepove uporabo

naprav Therac 25 na celotnem področju ZDA. Razlog za prepoved je bil po argumentaciji FDA v nezadostni obrazložitvi AECL kaj je vzrok začasne odpovedi vnosnega dela programa, saj bi se omenjena anomalija lahko pokazala tudi v drugih režimih delovanja programa.

Po smrti obeh pacientov sorodniki proti AECL vložijo tožbe, sodišče pa kot ekspertnega izvedenca k obravnavi povabi prof. dr. Nancy G.Leveson, eno od pionirk raziskav na področju zanesljivosti programske opreme, ki začne preučevati dokumentacijo sistema. Do razsodbe ne pride, ker se stranke v sporu dogovorijo za poravnavo, dostop do dokumentacije pa se onemogoči. Navkljub temu Levesonova svojo raziskavo nadaljuje iz bolj ali manj javno dostopnih virov in svoje izsledke objavi v končnem poročilu l.1993. V njem opozori na splošni cilj raziskave, katerega namen ni bila očrnitev proizvajalca, temveč identifikacija napake pri zasnovi sistema, ker bi tovrsten tip napake lahko tako v prihodnje odpravili pri sorodnih misijsko kritičnih aplikacijah in tudi pri drugih proizvajalcih. V specifičnem opisanem primeru opozori na naslednje splošne pomankljivosti pri vodenju in izvajanju razvoja računalniškega sistema za krmiljenje naprave:

- identitete osebe, ki je razvijala programsko opremo ni bilo možno identificirati ne po imenu in priimku, ne po izobrazbi, ne po izkušnjah; AECL je uspel zagotoviti le podatek, da je oseba l.1986 zapustila delodajalca, pri čemer je bila pri AECL izvedena uradna policijska preiskava, a se identitete osebe skozi zgodovino zaposlitev ni dalo določiti;

- računalniški program in sistem kot celota sta šla skozi pomanjkljivo testiranje;

- računalniški program in sistem kot celota sta imela pomanjkljive specifikacije in dokumentacijo; programska oprema praktično ni bila niti komentirana, niti dokumentirana;

- programska oprema ni bila verificirana s strani neodvisne institucije;

- proizvajalec naprave do leta 1986 praktično ni vodil evidence nesreč in incidentov (angl. *hazard reports*) in temu primerno glede nanje tudi ni ukrepal;

Poleg tega je raziskava pokazala, da je bilo nesreč s prejetimi prevelikimi dozami sevanja več (skupaj 6), a štiri od njih niso bili javno objavljene. Zvrstile so se v obdobju od junija 1985 do januarja 1987, zaradi predoziranja pa so zahtevale 4 smrtne žrtve.

Primer je zanimiv zaradi njegove velike odmevnosti. Na osnovi izsledkov Levesonove so se tako v ZDA, kot tudi v drugih razvitih državah vzpostavili standardi, ustrezna telesa, postopki certificiranja in ostale regulative za misijsko kritične računalniške sisteme. Tipičen primer standarda, ki se je tokom desetletij po nesrečah razvil na področju medicinskih računalniških sistemov, je IEC 62304, ki definira življenski cikel programske opreme digitaliziranih medicinskih naprav.

Temeljit opis kronologije dogodkov povezanih z nesrečami naprave Therac 25 vključno z izvlečkom končnega poročila o opisanih nesrečah najdemo v delu [4], širše poročilo N.G. Leveson pa v [5]. V delu [6] je opisana tudi najdena sistemska napaka, ki bi lahko bila vzrok za predhodno opisane nesreče. V računalniški sistem je bil namreč vgrajen 6 bitni programski števec in venomer, ko je ta dosegel vrednost 0, so odpovedale določene I/O funkcionalnosti mikroračunalnika. Ta je v tem primeru zato izvedel obsevalni tretma, ni pa izvedel vseh predvidenih programsko vgrajenih varnostnih funkcij. V primeru hitrega in površnega vnosa predoziranja sistem tako prevelike vnešene doze ni zaznal (se nanjo ni odzval s korekturo) in enostavno izvedel obsevanje s predoziranjem.

1.3.2 Airbus A320

Letalo Airbus A320 evropskega proizvajalca Airbus, ki je v večinski lasti orožarskega koncerna EADS (European Aerospace and Defense Group), je bilo prvo civilno ozkotrupno (angl. *narrow body*, *single aisle*) potniško letalo, v katerega je bil l.1988 vgrajen „fly by wire“ koncept upravljanja s plovilom. Slednje pomeni, da se pilotovi ukazi za krmiljenje plovila do letalnih površin in motorjev ne prenašajo več preko mehanskih vodil, temveč preko računalniškega omrežja. Tovrstni koncept vpelje tudi računalnik (angl. *flight management system* - FMS), ki od pilota prejema upravljalske ukaze, jih analizira in eventuelno spreminja, ter nato preko omrežja pošilja do ciljnih točk upravljanja plovila.

„Fly by wire“ koncept tako po eni strani doprinese k zmanjšanju teže plovila na račun odprave mehanskih vodil, kar vodi do zmanjšanja stroškov poleta, po drugi strani pa omogoči analizo in popravke pilotovih ukazov, s čimer se poveča varnost plovbe na račun odprave eventuelnih pilotovih napak.

Od prihoda na tržišče je v letih 1988 (Air France Flight 296), 1990 (Indian Airlines Flight 605) in 1992 (Air Inter Flight 148) prišlo do treh strmoglavljenj plovil tega tipa. Vsem nesrečam je bila skupna prenizka višina leta pred vstopom v sklepno fazo pristajanja. Prvi sumi za vse tri nesreče so padli na FMS sistem (torej na računalnik), ki naj bi si podatke zajete preko sistema senzorjev plovila „napačno interpetiral“. Povedano drugače naj programska oprema ne bi opravila svoje funkcije korekcije upravljanja pristanka plovila.

Prvo od plovil strmoglavi po nizkem preletu na planirani višini 15 m na letalskem mitingu 26.6.1988 na letališču Mulhause Habsheim v Franciji. Plovilo je bilo v lasti družbe AirFrance, staro šest mesecev in dobro vzdrževano. Na plovilu je bilo 6 članov posadke in 130 potnikov, pri čemer 3 osebe nesreče niso preživele. Sum za nesrečo je padel na FMS in s tem posredno na krmilno logiko računalnika plovila, ki s preletne višine ni več uspel spraviti plovila v fazo vzpenjanja. Šele dokončno poročilo o nesreči objavljeno 29.11.1989 [7], je sume za krivdo računalniškega sistema ovrglo in nesrečo pripisalo spletu okoliščin prerizično načrtovane višine preleta (prvotna višina preleta je bila planirana na 35 metrov) ter nepredvidenih ovir na poti vzpenjanja plovila v obliki gozda na koncu pristajalne steze. V obdobju leta in pol po nesreči, ki je minilo do objave poročila o nesreči, je bil „fly by wire“ koncept javno smatran kot nezanesljiv in neustrezen za vodenje tako odgovornih misij kot je krmiljenje letalskega plovila.

Delno je bilo tovrstno javno mnenje tudi posledica tega, ker konkurenčni proizvajalec Boeing „fly by wire“ rešitve za svojo družino potniških plovil še ni imel razvite in je pred nesrečo začel izgubljati večinski tržni delež zaradi uspešne prodaje Airbusovih ozkotrupnih plovil.

Gledano z današnje časovne perspektive se izkaže, da je družina plovil Airbus A320 ena od najvarnejših družin plovil, pri čemer mnogo nesreč prepreči prav FMS. Nenazadnje smiselnost koncepta „fly by wire“ prizna tudi proizvajalec Boeing, ki začne računalniško vodeno krmiljenje v svoja civilna letala vgrajevati sredi devetdesetih let prejšnjega stoletja.

1.3.3 Patriot

V zalivski vojni l.1991 ZDA prvič uporabijo računalniško krmiljeni raketni sistem Patriot. Njegovi funkciji sta bili sledenje in uničevanje balističnih raketnih izstrelkov Scud, ki jih je proizvajala takratna Sovjetska zveza, v zalivski vojni pa jih je uporabljal Irak. Simulacijsko - testni rezultati sistema Patriot v idealnih razmerah so izkazovali 95% uspešnost uničenja sovražnega izstrelka. V praksi je uspešnost zadetkov padla na nizkih 13% [6]. Povhr vsega je ena od raket Patriot v misiji prestrezanja sovražne rakete Scud le to zgrešila za 678 metrov, slednja pa je nato v nadaljevanju zadela svoj cilj in porušila vojaški nastanitveni objekt pripadnikov članic organizacije NATO. Posledica zgrešenega cilja je bila 29 mrtvih in 97 ranjenih vojakov članic organizacije NATO. Po kasnejših temeljitih analizah sta bila za neustrezno navigacijo in s tem posledično za zgrešitev izstrelka Scud identificirana dva možna vzroka.

Prvi možni vzrok je tičal v primitivni napaki najdeni v programski opremi. Ena od potrebnih numeričnih konstant (konkretno število 0,1) za navigacijske izračune je bila hranjena v podatkovnem tipu dolžine 24 bitov, ena od spremenljivk pa v 48 bitnem. Ker se število 0,1 v dvovrednostnem bitnem zapisu zapiše z neskončnim zaporedjem ničel in enic, prihaja pri zaokroževanju tega števila, ki je odvisno od velikosti podatkovne strukture, do razlik. Pogramska oprema je v enem od navigacijskih modulov po prirejanju vrednosti spremenljivke preverjala njeno enakost s konstanto, zaradi različnosti podatkovnih tipov pa primerjava ni nikdar uspela in odtod je sledil napačen izračun potreben za navigacijo izstrelka [6].

Drugi možni vzrok je bil pogojen s kompleksnostjo celotnega računalniškega sistema, ki je temeljil na dveh podsistemih. Prvi se je nahajal na izstrelni ploščadi (lansirni rampi), drugi pa v samem izstrelku. Za normalno delovanje obeh podsistemov je bila ključna njuna časovna sinhroniziranost ali sinhroniziranost njunih realnih ur. Glede na stanje razvoja procesorjev začetkom devetdesetih let je bilo možno popolno sinhroniziranost na nivoju urinega takta doseči le za misijski čas 14 urne pripravljenosti na izstrelitev (angl. *max. duty cycle*). Po izteku tega obdobja je bilo potrebno oba sistema z resetiranjem ponovno časovno uskladiti, kar je zagotavljalo nov cikel 14 urne pripravljenosti na izstrelitev. Analiza po nesreči je pokazala, da upravljalsko vojaško osebje v danem primeru o potrebi po sinhronizaciji ni bilo obveščeno in je sistem brez sinhronizacije deloval že 100 delovnih ur [4]. Posledično je sledil napačen odziv enega

od podsistemov in kot končni rezultat zgrešitev izstrelka Scud.

1.3.4 Space shuttle Columbia

Space shuttle Columbia je bil prvi od petih ponovno uporabljivih (angl. *reusable*) vesoljskih raketoplanov, ki jih je NASA zgradila za potrebe prevoza astronavtov in tovora v nizko zemljino orbito (na vertikalno oddaljenost od 160 km do 2.000 km od zemlje) in za potrebe vračanja človeških posadk in tovora na zemljino površje. Raketoplan Columbia je bil dokončno zgrajen l.1980, l.1981 pa je bil kot prvi raketoplan prvič izstreljen na uradno misijo. Poleg plovila Columbia je NASA v nadaljevanju zgradila še štiri raketoplane z imeni Challenger (eksplodira 73 sekund po vzletu l.1986), Atlantis (danes razstavljen v letalskem oporišču Cape Canaveral), Discovery (danes razstavljen v muzeju v mestu Washington) in Endeavour (danes razstavljen v mestu Los Angeles). Petorica raketoplanov je od leta 1981 do leta 2011 opravila 135 misij v nizko zemljino orbito. Večina misij raketoplanov je imela za vmesni cilj obisk vesoljske postaje Mir (1986-2001), v nadaljevanju (1998-) pa obisk mednarodne vesoljske postaje (International space station - ISS) z namenom oskrbe, prevoza posadk, primarno pa je vsaka od misij imela tudi svoj raziskovalni in/ali servisni namen (npr. servisiranje Hubblovega teleskopa).

Space shuttle Columbia je bil l.2003 izstreljen na svojo 28. misijo s ciljem izvedbe specifičnih znanstvenih poizkusov v mikrogravitacijskem okolju, ki naj bi se opravile v zemljini orbiti. To je bila 113. misija raketoplanov po vrsti, NASA pa jo je vodila pod oznako STS-107. Pri izstrelitvi je prišlo do manjše fizične poškodbe krila raketoplana zaradi odpadanja zaščitne pene z rezervoarja za raketno gorivo. NASA je imela s tem probleme že pri predhodnih uspešnih misijah raketoplanov, zato ni sprožila temeljitejšega pregleda in eventuelnega popravila krila v zemljini orbiti na sami misiji. Po sedemnajstih dneh orbitalnega kroženja posadka Columbie zaključi z misijo in preko računalniškega krmilnega sistema plovilo usmeri v zemljino atmosfero. Manever vstopanja raketoplana v zemljino atmosfero (angl. *re-entry*) je pri vseh misijah vodil računalniški sistem, ker so izkušnje pokazale, da računalniški sistem manever vstopa izvede zanesljiveje, hitreje in natančneje, kot pilot. Ključni točki manevra sta vstopni kot v zemljino atmosfero na približni vertikalni oddaljenosti 100 km od zemlje, ki je določen z izredno majhnimi odstopanji in pa procedura nagibanja plovila po njegovi vzdolžni osi, ki omogoča časovno izmenično hlajenje površin kril ob vstopu v zemljino atmosfero. Do ekstremnega segrevanja kril in celotne zunanje površine plovila prihaja zaradi trenja. Dne 1.2.2003 po končani misiji ob vstopu v zemljino atmosfero Columbia razpade in delno zgori, umre pa vseh 7 članov posadke.

NASA takoj po nesreči vpelje preiskavo in prvi izsledki na osnovi telemetričnih podatkov in rekonstrukcije procedure upravljanja nagibanja plovila vržejo sum na neustrezno delovanje računalniškega krmilnega sistema, ki naj ne bi ustrezno nagibal plovila, kar bi lahko privedlo do pregrevanja letalnih površin in s tem posredno do njihove dezintegracije ali postopnega razpada. Šele končni izsledki raziskave [8] so pokazali, da je računalniški sistem ukrepal ustrezno glede

na podatke, ki jih je prejemal iz sistema senzorjev. Slednji je odpovedal zaradi temperaturno pogojene dezintegracije kril, to pa je povzročil vdor vročega zraka v krila zaradi njihove poškodbe pridobljene v fazi izstrelitve. Tako je računalniški sistem dobival neustrezne vhodne podatke in temu primerno neustrezno krmilil plovilo. S tem je NASA sicer nerada priznala krivdo za katastrofo, ki je izvirala iz mehanske poškodbe, katero bi posadka lahko na misiji celo popravila, ali pa bi po posadko poslali enega od ostalih raketoplanov. V kontekstu povedanega bi bilo vodstvu misije resnično lažje krivdo prenesti na nič hudega sluteči računalniški sistem.

NASA program misij z raketoplani julija 2011 ustavi, oskrbo delujoče mednarodne vesoljske postaje (ISS) pa še danes izvaja Rusija (Rossavia Kosmos) z družino raket Sojuz.

1.3.5 Heatrow Terminal 5

Londonsko letališče Heathrow je eno od največjih evropskih letališč, preko katerega letno potuje 80 milijonov potnikov[8]. Zaradi stalnega povečevanja števila potnikov so l.2002 začeli z gradnjo novega, po vrsti petega terminala. Gradnjo so zaključili v l.2007, od septembra tega leta pa vse do marca l.2008 pa je potekal prilagojevalni proces (angl. *operational readiness test*) na redno obratovanje terminala. Vanj je bilo vključenih 15.000 prostovoljcev v vlogi namišljenih potnikov, s katerimi so upravljalci skušali preveriti pripravljenost terminalske infrastrukture in osebja na realne letališke operacije (prijava na let, prevzem in izdaja prtljage, transport prtljage od terminala do letal in obratno, pregledovanje potnikov itd.). Končna cena terminala je znašala 8,5 milijarde USD, cena IT[9] infrastrukture pa 340 milijonov USD. Slednja je bila sestavljena iz 163 interoperabilnih[10] informacijskih sistemov, 9.000 povezanih naprav, 2.100 osebnih računalnikov, 5.000 km fiksnega računalniškega omrežja in 18 km informatiziranih transportnih trakov za prtljago. IT infrastrukturo je dobavilo 180 dobaviteljev. Dne 14.3.2008 terminal svečano otvori angleška kraljica Elizabeta II, kar dokazuje pomembnost investicije z nacionalnega zornega kota, dne 27.3.2008 pa terminal vstopi v redno eksploatacijo. Njegove predvidene zmogljivosti so bile ocenjene na 35 milijonov potnikov in 211.000 premikov letal (priletov in odletov) letno.

Dne 27.3.2008 ob začetku izvajanja rednih letaliških operacij je šlo na terminalu narobe vse, kar je narobe lahko šlo. Sosledje dogodkov, ki so vodili do incidentov, je bilo sledeče:

- na terminalu zaradi nedokončanih del še ni delovalo 28 od 275 razpoložljivih dvigal;
- letališki terminal bi moral začeti delovati ob 4:00; ob jutranjem prihodu

[8] Podatek glasi na leti 2018 in 2019 (Vir: Wikipedia).

[9] IT - informacijska tehnologija.

[10] Interoperabilnost informacijskega sistema - zmožnost opazovanega informacijskega sistema, da sodeluje z drugimi informacijskimi sistemi brez posebnega uporabnikovega posega-nja.

potnikov in zaposlenega osebja na terminalsko parkirišče je prišlo do popolnega avtomobilskega zastoja in osebje terminala je zamujalo na delovna mesta; posledično ob 4:00 tako ni delovalo niti eno prijavno (angl. *check-in*) mesto, zaradi česar je postajalo število čakajočih potnikov v vrstah za prijavo na let in oddajo prtljage vse večje;

- od 6:00 do 9:00 je v vrsti na prijavo in oddajo prtljage ves čas čakalo vsaj 300 potnikov, sortirni sistem prtljage pa v ozadju prijavnega procesa ni več zmogel pravočasno obdelati vseh zahtev (postane *ozko grlo*); do te ure je odletelo devet letal s potniki brez njihove prtljage, ker slednja ni bila pravočasno pripravljena za natovarjanje; zaradi obremenjenosti informacijskega in avtomatiziranega sortirnega sistema prtljage se je upočasnila tudi izdaja prtljage, na katero je bilo potrebno čakati v povrečju več kot dve uri in pol po pristanku letal;
- do 12:00 se je zaradi prevelikega števila potnikov na terminalu (čakajočih na prtljago ter čakajočih na prijavo in oddajo prtljage) odpovedalo 20 poletov;
- ob 17.00 je prtljažni informacijski sistem dokončno odpovedal in oddajanje prtljag ni bilo več mogoče; uporabnik terminala (letalski operater British Airways) se je odločil, da bo potnikom omogočil izbiro med potovanjem samo z ročno prtljago, možnostjo nakupa nove letalske karte z odhodom iz enega od preostalih terminalov ali povračilo denarja za nakup karte;

Posledice incidentov v prvem dnevu delovanja terminala so bile odpovedi 34 poletov, posledice podobnih incidentov v naslednjih 11 dneh delovanja terminala pa še odpovedi nadaljnjih 500 poletov. Obratovanje terminala se je normaliziralo šele 8.4.2008, v celotnem dvanajstdnevnem obdobju pa se je izgubilo 42.000 kosov prtljage, nastalo pa je za 60 milijonov USD gospodarske škode.

Kasnejše analize so pokazale, da je za množico incidentov kriv splet nesrečnih okoliščin oziroma zaporedje nepričakovanih oziroma nepredvidenih dogodkov (angl. *knock-on effect*). Pri tem analize razločujejo med *povodi*[11] in *vzroki*[12] za nastale incidente. Povodi za verižno porajanje incidentov so bili sledeči:

- prepozno odprtje prijavnih mest, ki so začela obratovati s prevelikim številom čakajočih potnikov;
- v prtljažnem informacijskem sistemu so bile še iz faze testiranja blokirana oziroma filtrirana vsa sporočila za izmenjavo informacij z prtljažnimi informacijskimi sistemi na preostalih terminalih letališča; tako je na terminal 5 prihajala prtljaga potnikov na povezovalnih letih, ki jo prtljažni informacijski sistem ni znal povezati z leti in potniki s tega terminala; omenjena prtljaga se je kopičila preko vseh razumnih meja in bila obravnavana kot izgubljena; opisani filtri so bili najdeni in izključeni šele po štirih dneh delovanja terminala;

[11] Povod - kar ima za posledico nek dogodek (Vir: SSKJ).

[12] Vzrok - kar utemeljuje nek dogodek (Vir: SSKJ). Vzrok je torej predpogoj za nek dogodek, povod pa ta dogodek sproži (op. a.).

- prtljažni informacijski sistem je bil z vidika zmogljivosti poddimenzioniran, zaradi česar je procesiranje prtljažnih transakcij potekalo močno upočasnjeno;

Vzroki za verižno porajanje incidentov so bili sledeči:

- slaba prometna signalizacija za usmerjanje zaposlenih in potnikov na letališče terminala;
- nedovoljšnja usposobljenost osebja za upravljanje s prtljago;
- slaba sistemska integracija informacijskih sistemov;
- prepozen začetek testiranja delovanja celotne IT infrastrukture zaradi zamud pri gradnji objekta; zaradi tega so bili obsegi testiranj in testni scenariji minimizirani;
- nedovoljšnje testiranje prtljažnega informacijskega sistema;

Dogodki na terminalu 5 sodijo v skupino incidentov in predstavljajo šolski primer delne odpovedi kompleksnega informacijskega sistema. Incidenti odprtja terminala 5 so relativno slabo dokumentirani, o njih ni javno dostopnega končnega poročila, večina informacij iz pričujočega razdelka pa je povzeta po virih [9], [10], [11], [12]. Del informacij o incidentih bralec najde tudi v prosto dostopnem angleškem dokumentarnem filmu „*A very British Airline*“.

1.3.6 Boeing 737 Max

Boeing 737 Max je pripadnik četrte generacije družine ozkotrupnih (angl. *single aisle*) dvomotornih potniških reaktivnih letal tipa „737“, ki ga na trg l.2017 dostavi ameriški proizvajalec Boeing. Osnovna konstrukcija letala izhaja iz predhodnih generacij letal tipa „737“, primarni predvideni cilji nove generacije letal pa so bili zmanjšanje porabe goriva, večji dolet[13] in njihovo lažje vzdrževanje.

Oktobra 2018 (Lion Air Flight 610) in marca 2019 (Ethiopian Airlines Flight 302) pride neposredno po vzletu (v prvem primeru po 13 minutah, v drugem primeru pa po 6 minutah) do dveh strmoglavljenj omenjenega tipa letala s skupno 346 človeškimi žrtvami. Oba dogodka sodita v skupino nesreč. Začetni indici[14] obeh preiskav vržejo sum za vzroka nesreč na nepravilno delovanje sistema MCAS. Posledično pride s strani letalskih regulatornih organizacij do prizemljitve vseh letal omenjenega tipa po celem svetu. V nadaljevanju preiskav Boeing prizna, da ima težave s konsistentnim delovanjem sistema MCAS, ki bo v bližnji prihodnosti po vsej verjetnosti tudi uradno potrjen kot „krivec“ za obe nesreči.

MCAS sistem (angl. *maneuvering characteristics augmentation system*) predstavlja programski segment računalniškega sistema plovila, ki skrbi za pozicioniranje horizontalnih stabilizatorjev in s tem posredno za prečni naklon

[13] Dolet - razdalja, ki jo lahko letalo prepotuje od vzleta do pristanka.
[14] Indic - kar omogoča sklepanje na kaj.

plovila pri njegovem vzpenjanju. Idealni prečni naklon plovila je bil pri letalih prejšnjih generacij samodejno zagotovljen na osnovi težiščnih značilnosti plovila, pri novi generaciji plovil pa je prišlo do sprememba težišča plovila, tako da je bilo popravke prečnega naklona na idealen kot vzpenjanja potrebno izvajati na „umeten“ način s pomočjo programsko izvajane regulacije horizontalnih stabilizatorjev oziroma vodoravnega dela repa letala.

Uradni izsledki obeh preiskav še niso dokončni, lahko pa pričakujemo, da bo neposredni krivec za obe nesreči neustrezno delovanje MCAS programskega modula, posredna krivda pa na strani proizvajalca, ki o režimih dela MCAS modula ni na ustrezen način (s šolanjem na simulatorjih) seznanjal pilotov.

1.3.7 Povzetek opisanih incidentov in nesreč

Iz opisanih primerov lahko pridemo do zaključka, da računalniški sistemi vršijo vse bolj odgovorne funkcije v misijsko kritičnih sistemih. Ob vsakem novem incidentu ali nesreči se običajno prvi sum za njun vzrok usmeri na računalniški sistem in v nekaterih primerih je ta sum tudi opravičen, kar dokazujejo nesreče in incidenti v katere so bili vpleteni Patriot, Therac - 25, Heathrow Terminal 5 in Boeing 737 Max. V vseh primerih incidentov in nesreč je potrebno opraviti temeljite analize, da se identificirajo pravi vzroki in povodi. Takšne analize lahko računalniški sistem krivde tudi razbremenijo, kar dokazujeta primera nesreč plovil Columbia in Airbus A320.

Literatura

[1] T. Gorenšek, "Digitalna transformacija." https://ipm.si/homopolitikus/digitizacija-digitalizacija-in-digitalna-transformacija/, Januar 2020.

[2] D. P. Siewiorek and R. S. Swarz, *Reliable computer systems - Design and evaluation*. A. K. Peters, Ltd., 1998.

[3] D. Zummack, "Defining accidents and incidents." https://blog.safetysync.com/whats-the-difference-between-incidents-and-accidents, Januar 2020.

[4] I. Peterson, *Fatal defect - chasing killer computer bugs*. Vintage Books, USA, 1996.

[5] N. Leveson and C. Turner, "An investigation of the Therac-25 accidents," *IEEE Computer, July*, pp. 18–41, 1993.

[6] P. Neumann, *Computer related risks*. Addison Wesley Publishnig Company, USA, 1995.

[7] "Mulhouse - Habsheim accident report." http://aviation-safety.net/database/record.php?id=19880626-0/, Februar 2016.

[8] R. Godwin, *Columbia accident investigation report*. Collector's Guide Publihsing, Inc., 2003.

[9] M. Krigsman, "IT failure at Heathrow T5: What really happened." https://www.zdnet.com/article/it-failure-at-heathrow-t5-what-really-happened/, Januar 2020.

[10] R. Thomson, "British Airways reveals what went wrong with Terminal 5." https://www.computerweekly.com/news/2240086013/British-Airways-reveals-what-went-wrong-with-Terminal-5, Februar 2020.

[11] P. Woodman, "Disastrous opening day for terminal 5." https://www.independent.co.uk/news/uk/home-news/disastrous-opening-day-for-terminal-5-801376.html, Marec 2008.

[12] BBC, "What did go wrong at Terminal 5?." http://news.bbc.co.uk/2/hi/uk_news/7318568.stm#graphic, Februar 2020.