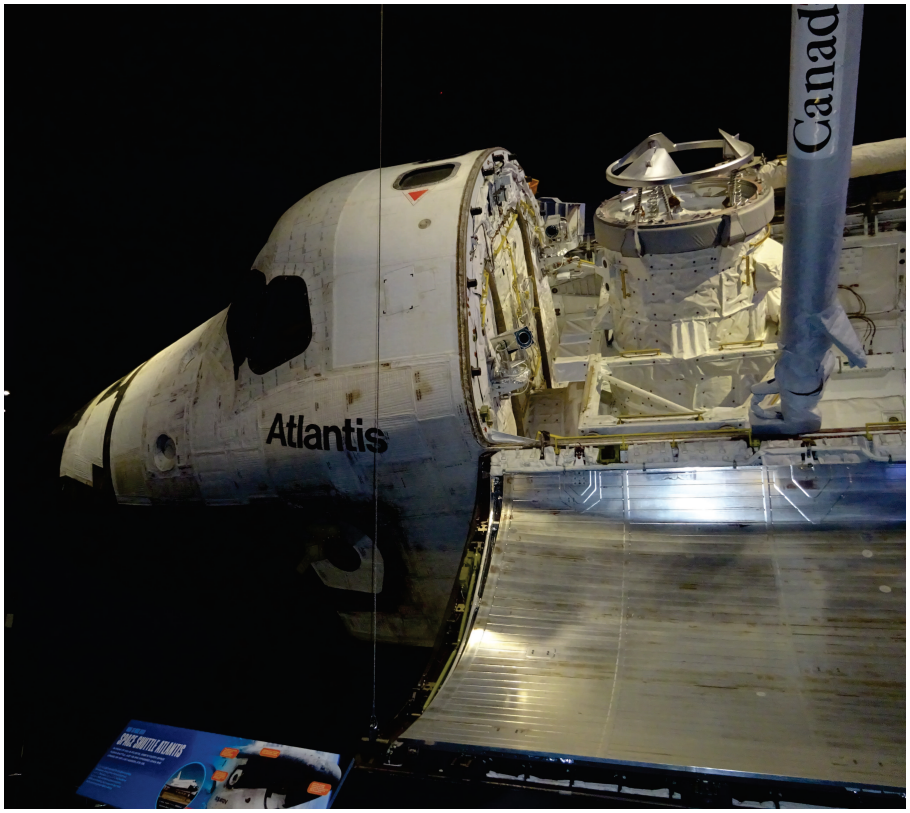
Poglavje 1

Zgledi realizacij misijsko kritičnih računalniških sistemov

V pričujočem poglavju si bomo ogledali nekaj vzorčnih primerov pristopov in realizacij računalniških sistemov za nadzor misijsko kritičnih procesov. Omenjene primere bomo povzeli s področij vesoljskih misij, civilnega zračnega prometa (civilne aviacije) in nadzora železniškega prometa. Vsem primerom bo za doseganje željene zanesljivosti skupna uporaba redundance.

1.1 Redundančni sistem krmiljenja vesoljskega plovila Space Shuttle

Raketoplan Space Shuttle je NASA (angl. *National Aeronautics and Space Administration*, ZDA) uporabljala za potovanja v nizke zemljine orbite in je od l. 1981 do l.2011 predstavljal poleg sovjetskega (od l.1990 naprej ruskega) vesoljskega programa edino možnost za gradnjo in oskrbovanje vesoljske postaje Mir in Mednarodne vesoljske postaje (angl. *International space station* - ISS) ter posledično raziskave v zemlji bližnjemu vesolju. Raketoplan je bil v svoji zasnovi načrtovan kot ponovno uporabljiv in 5 raketoplanov iz te družine je v 30 letih opravilo 135 misij v nizke zemljine orbite. Program Space Shuttle je bil po dveh katastrofalnih nesrečah v letih 1986 (eksplozija raketoplana Challenger pri vzletu) in 2003 (razpad raketoplana Columbia pri vstopanju v zemljino atmosfero) l.2011 ustavljen, preostali trije raketoplani pa so danes razstavljeni na različnih lokacijah v ZDA. Na sliki 1.1 je predstavljen raketoplan Atlantis z odprtim tovornim prostorom.



Slika 1.1: Raketoplan Atlantis z odprtim tovornim prostorom razstavljen v muzeju v vesoljskem oporišču Cape Canaveral na Floridi (foto: M.Mraz, 2019).

1.1.1 Značilnosti in funkcije računalniškega sistema

Vseh pet raketoplanov je uporabljalo „fly by wire“ koncept upravljanja s plovilom, ki smo ga opisali že v uvodnem poglavju pričujočega dela. Osnovo za izvedbo koncepta „fly by wire“ na plovilu je predstavljal *sistem za procesiranje podatkov* (angl. *Data Processing System* - DPS) s sledečimi značilnostmi povzetimi po viru [1]:

- DPS sistem je bil sestavljen iz petih splošno namenskih računalnikov (angl. *general purpose computers* - GPC); posamezen GPC je predstavljal IBM 4Pi/AP-101S računalnik, med seboj pa so bili povezani z ločenim sistemom vodil; posamezen računalnik je imel ob začetku programa dinamični pomnilnik sestavljen iz 106.496 32-bitnih besed v feritni izvedbi zaradi eliminacije vpliva sevanja; procesne zmogljivosti posameznega GPC-ja so bile v začetku programa omejene na 0,4 MIPS-a (angl. *million instructions per second*), z nadgradnjami sredi devetdesetih let pa na 1 MIPS;

- za potrebe trajnega pomnjenja podatkov sta bili v sistem vgrajeni dve magnetni tračni enoti (*magnetic tape mass memory units* - MMU) s kapaciteto 134 megabitov;
- GPCji so bili razporejeni v različnih delih plovila in so imeli zagotovljeno redundančno hlajenje iz dveh neodvisnih virov; v primeru odpovedi obeh virov hlajenja je bila predvidena doba normalnega delovanja posameznega GPC-ja od 17 do 25 minut po odpovedi zadnjega delujočega vira v odvisnosti od zračnega tlaka na lokaciji posameznega GPC-ja;
- deklarirani MTBF (angl. *mean time between failure*) za posamezni GPC (AP-101S) računalnik je bil 6.000 delovnih ur;
- GPC-ji so preko senzorike prejemali podatke zajete na več kot 2.000 vitalnih točkah plovila;
- programska oprema je bila napisana v prevajanem jeziku HAL/S (angl. *High-order Assembly Language/Shuttle*) razvitem zgolj za namene vesoljskih misij;
- programska oprema posameznega GPCja se je imenovala PASS (angl. *Primary Avionics Software System*), izdelana pa je bila v podjetju IBM; obsegala je približno 500.000 vrstic izvorne kode, zajemala pa je vse potrebno funkcionalnosti za izvedbo misije; poleg PASS verzije programske opreme je obstajala tudi tako imenovana BFS (angl. *Backup Flight System* - BFS) verzija programske opreme, v kateri so bile samo nujne funkcionalnosti, ki so omogočale varno prekinitev misije v poljubni fazi in povratek plovila ter posadke na zemljo; slednja je bila razvita v podjetju Rockwell Inc.;

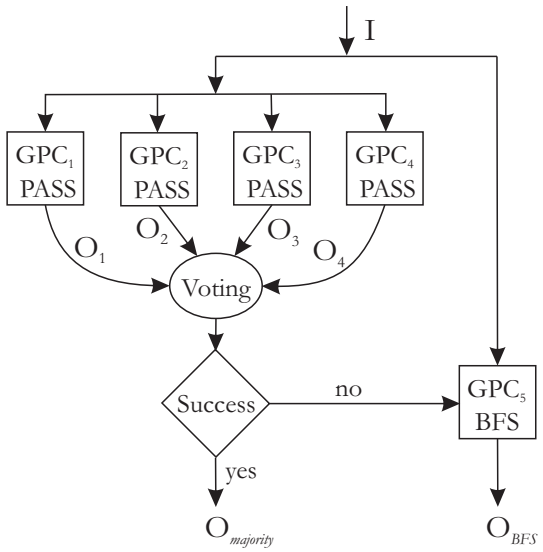
Osnovni namen PASS programske opreme je bilo izvajanje dveh skupin funkcij. Le ti sta sledeči:

- GNC funkcije (angl. *Guidance, Navigation, Control*): funkcije potrebne za izstrelitev, dostop do orbite, manevriranje v orbiti, vstopanje v orbito in pristajanje;
- SM funkcije (angl. *System Management*): funkcije za monitoriranje vitalnih delov plovila (preko 2.000 nadziranih točk plovila), zagotavljanje življenskih pogojev (vzdrževanje tlaka, koncentracije kisika, temperature itd.), upravljanja s tovornim delom ter robotsko roko itd.;

Glede na majhne kapacitete resursov (npr. procesne moči in dinamičnega pomnilnika) in različne zahteve po zanesljivosti v različnih fazah posamezne misije, so bile možne konfiguracije DPS sistema sledeče:

- v *kritičnih fazah* poleta (angl. *critical flight phahes*) je posadka štiri GPCje povezala v redundantno glasovalno konfiguracijo, s čimer je bila dosežena večja zanesljivost delovanja sistema kot celote in odpornost na odpovedi (angl. *fault tolerant*) posameznih GPCjev; v kritičnih fazah tako konfiguriran DPS prevzame funkcije vodenja, navigacije in krmiljenja plovila

(GNC funkcije); kritični fazi poleta sta primarno vzlet (angl. *ascent*) in pa vstop v zemljino atmosfero (angl. *reentry*) s pristankom (angl. *landing*); na omenjenih štirih GPCjih je v tem primeru tekla identična verzija PASS programske opreme, peti GPC pa je imel naloženo BFS verzijo programske opreme; nadzor nad plovilom je v tem primeru vršila glasovalno redundantna konfiguracija, vse do odpovedi treh od štirih sistemov; po odpovedi treh sistemov glasovanje ne uspe več in popoln nadzor nad plovilom se prepusti GPCju z BFS verzijo programske opreme, ki nemudoma prekine misijo in plovilo usmeri v fazo vstopa v zemljino atmosfero; BFS je ves čas nameščen v enega od GPCjev in ga praviloma ni potrebno nalagati iz MMU pomnilnih enot, če ne pride do odpovedi dotičnega GPCja; iz slednjega lahko sklepamo, da je BFS sistem v „hot standby“ konfiguraciji; da dosegamo konsistentnost glasovanja med štirimi GPCji je le to realizirano tako, da se GPC, ki sprocesira drugačen odziv od večine GPCjev izloči iz glasovalne konfiguracije; na tak način preidemo iz konfiguracije štirih glasovalcev na konfiguracijo s tremi, v nadaljevanju pa na konfiguracijo z dvema GPCjema; v misijah od l.1981 do l.1996 delujoča redundantna konfiguracija nikdar ni padla pod število treh GPCjev, kar pomeni, da v časovnem intervalu misijsko kritične faze v navedenem obdobju nikdar ni odpovedal več kot en GPC; na sliki 1.2 je prikazana shema konfiguracije DPS sistema v misijsko kritični fazi z alternativnima izhodoma DPS sistema $O_{majority}$ in O_{BSF};



Slika 1.2: Shema konfiguracije DPS sistema plovila „Space shuttle“ v misijsko kritični fazi.

- v *nekritičnih fazah* poleta se funkcije porazdelijo med GPCje in delovanje

ni več redundantno; tako npr. eden od GPCjev skrbi za GNC funkcije, preostali pa lahko vršijo druge funkcije (npr. upravljanje s tovornim delom plovila, njegovo robotsko roko itd.) ali pa so celo deaktivirani (v „cold standby“ konfiguraciji);

1.1.2 Izračun zanesljivosti redundančne konfiguracije

Na tem mestu si oglejmo, kolikšno je zvišanje zanesljivosti z vpeljavo redundance v DPS sistem. Pri izračunu zanesljivosti bomo izhajali iz sledečih predpostavk:

- predhodno smo omenili, da je predviden MTBF za posamezni GPC računalnik 6000 delovnih ur; ob predpostavki, da je intenzivnost odpovedovanja GPC sistema v eksploatacijski dobi konstantna, se MTBF izraža kot inverzna vrednost λ_{gpc}; tako lahko predpostavimo, da je intenzivnost odpovedovanja GPC sistema 1 odpoved na $6*10^3$ delovnih ur ($\lambda_{gpc} = \frac{1}{6*10^3}$);
- odpovedi posameznih GPC računalnikov so med seboj neodvisne (odpoved posameznega GPCja ne vpliva na odpoved drugega GPCja);
- glasovalni sistem je idealno zanesljiv (ne vpliva na zanesljivost redundančnega glasovalnega sistema);

Ob upoštevanju predpostavk lahko najprej izračunamo zanesljivostno funkcijo posameznega GPC računalnika $R_{gpc}(t)$ po izrazu (1.1), v nadaljevanju pa še zanesljivostno funkcijo redundantne glasovalne konfiguracije $R_{sys}(t)$, ki jo obravnavamo kot sistem „*2 out of 4*“ (glej izraz 1.2). V nadaljevanju podamo izračun obeh zanesljivostnih funkcij z izrazoma

$$R(t)_{gpc} = e^{-\lambda_{gpc}*t}, \tag{1.1}$$

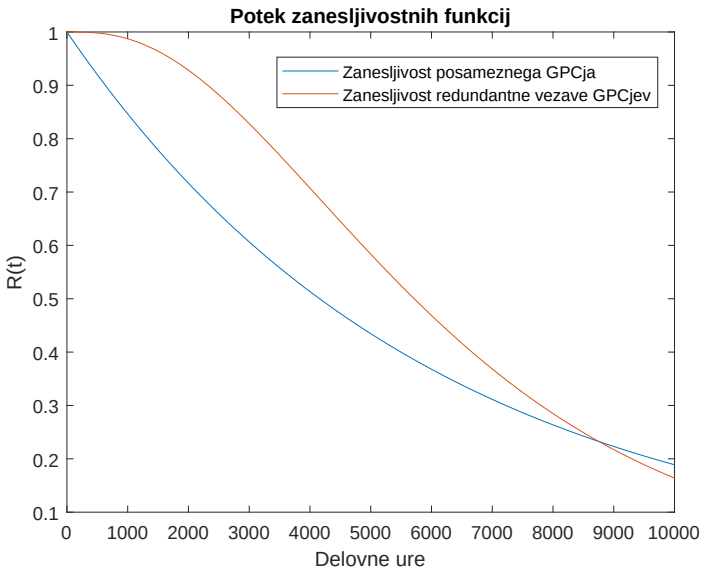
$$R_{sys}(t) = \sum_{i=2}^{4} \binom{4}{i} (R_{gpc}(t))^i * (1 - R_{gpc}(t))^{4-i} = \tag{1.2}$$

$$= \binom{4}{2} (R_{gpc}(t))^2 * (1-R_{gpc}(t))^2 + \binom{4}{3} (R_{gpc}(t))^3 * (1-R_{gpc}(t)) + \binom{4}{4} (R_{gpc}(t))^4 =$$

$$= 6*(R_{gpc}(t))^2*(1-2*R_{gpc}(t)+(R_{gpc}(t))^2)+4*(R_{gpc}(t))^3(1-R_{gpc}(t))+(R_{gpc}(t))^4 =$$

$$= 6 * (R_{gpc}(t))^2 - 8 * (R_{gpc}(t))^3 + 3 * (R_{gpc}(t))^4$$

Na slikah 1.3 in 1.4 sta po vrsti istočasno prikazana poteka zanesljivostnih funkcij $R_{gpc}(t)$ (za posamezen GPC) in $R_{sys}(t)$ (za redundančno vezavo) za 10.000 delovnih ur in 500 delovnih ur. S prvo sliko ponazorimo potek obeh funkcij v daljšem časovnem obdobju s predhodno že omenjenim križanjem po približno 8.500 delovnih urah, ko redundantna konfiguracija postane manj zanesljiva od neredundantne. Na drugi sliki upoštevamo čas trajanja misije posameznega plovila. Najdaljša misija plovila Space Shuttle z oznako STS-80 je trajala približno 18 dni ali 432 ur. Iz te slike razberemo evidentno prednost redundantne konfiguracije v časovnem intervalu trajanja misije.

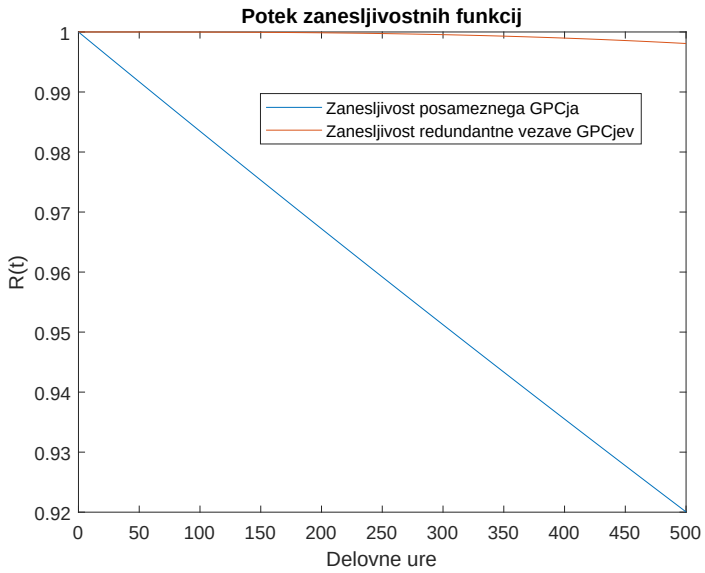


Slika 1.3: Poteka zanesljivostnih funkcij posameznega GPCja (modra barva) in redundančne vezave štirih GPCjev (rdeča barva) v 10.000 delovnih urah.

Še enkrat poudarimo, da sta bila razloga za rekonfiguriranje DPS sistema v zvečanju njegove zanesljivosti delovanja v kritičnih fazah in maksimalno izkoriščanje sicer relativno majhnih sistemskih resursov (npr. procesne moči in hitro dostopnega pomnilnika) v misijsko nekritičnih fazah. Rekonfiguriranje DPS sistema se je izvajalo v dveh fazah s strani posadke. V prvi fazi je posadka najprej resetirala in časovno sinhronizirala posamezne GPCje, v drugi fazi pa je naložila predefinirane memorijske konfiguracije in programe z MMU enot.

O vrstah redundančnega konfiguriranja DPS sistema najdemo v različnih virih mnogo med seboj nasprotujočih si informacij. Pričujoči opis redundančne konfiguracije temelji na virih [1] in [2]. Razlog različnim opisom tiči v tem, da je NASA glede na veliko število opravljenih misij (preko 130), razvoj strojne opreme od l.1981 do l.2011, različne naloge in cilje misij ter glede na različne dolžine trajanja misij uporabljala različne koncepte konfiguriranja in različno strojno opremo. Nenazadnje moramo komentirati tudi na prvi pogled okorno inicializacijo redundance, ki temelji na ročnem rekonfiguriranju sistemske spojenosti. Ta deloma izhaja iz stanja računalniške tehnologije izpred tridesetih let, deloma pa tudi iz konzervativnosti računalniških rešitev v podporo vesoljskim misijam. Tako je tak način upravljanja z DPS sistemom bil „podedovan“ iz predhodnega programa Apollo.

Nekaj zanimivih komentarjev o pionirskih časih razvoja programske opreme za program Space Shuttle najdemo na spletni strani [3], zgodovinsko dokumentacijo o zanesljivosti prvih načrtovanih DPS sistemov za program SpaceShuttle



Slika 1.4: Poteka zanesljivostnih funkcij posameznega GPCja (modra barva) in redundančne vezave štirih GPCjev (rdeča barva) v 500 delovnih urah.

pa v viru [4]. V delih [5] in [6] najdemo opise „porodnih“ problemov in incidentov do katerih pride pri vpeljevanju računalniškega vodenja vesoljskih poletov v programih Apollo in SpaceShuttle.

1.2 Redundančni sistem krmiljenja letala Airbus A340

V pričujočem razdelku predstavimo konfiguracijo redundančnega računalniškega sistema za krmiljenje širokotrupnega (angl. *wide body*, *twin aisle aircraft*) štirimotornega potniškega letala Airbus A340. Tudi v tem primeru računalniški sistem predstavlja osnovo za implementacijo „*fly by wire*“ koncepta.

Običajno se v kontekstu „*fly by wire*“ sistemov na njihovo elektronsko realizacijo sklicujemo s terminom *avionike* (angl. *avionics*). Ker je večina današnje elektronike digitalne in programirljive narave, lahko pojem avionike na letalu enačimo s pojmom kompleksnega distribuiranega računalniškega sistema. Osnovne funkcije avionike so sledeče:

- pozicioniranje in navigacija plovila;
- nadziranje vitalnih funkcij in stanj plovila (npr. višine in hitrosti leta, potisne moči motorjev, lege letalnih površin itd.);

- upravljanje s poletom (angl. *flight management*), ki ga vrši sistem za kontrolo letenja (angl. *flight control system* - FCS); le ta vključuje funkcijo prenosa ukazov od pilota do letalnih površin in motorjev preko računalniškega omrežja, funkcijo avtomatskega pilota in funkcijo analize in eventuelnega preprečevanja prenosa situaciji neprimernih ukazov s strani pilota in kopilota, ki bi lahko ogrozili strukturalno zasnovo plovila ali njegove letalne zmožnosti; tipičen primer takšnega neprimernega ukaza je vklop „*reverse thrust*“ funkcije na potovalni višini letala, ki bi letalu odvzela njegovo zmožnost letenja zaradi hitrega padca hitrosti in s tem posledično padca vzgona pod nek minimalen zahtevan nivo za normalno letenje;
- upravljanje z gorivom (nadzor nad količino goriva, izračunavanje potrebnega goriva za posamezen polet, spreminjanje težiščne točke letala glede na spreminjajočo se količino goriva itd.);
- izogibanje trkom (angl. *collision avoidance system* - CAS);
- beleženje podatkov o letu (angl. *fligh recorder*);
- pridobivanje in obdelava vremenskih podatkov;
- upravljanje letala z vidika vzdrževanja; v to skupino funkcij sodijo identifikacije odpovedi, beleženje preletenih ciklov, opozarjanje na potrebne preventivne servisne preglede itd. (angl. *aircraft management system*);

Med naštetimi funkcijami avionike ne najdemo funkcij predvajanja multimedijskih in interaktivnih vsebin (npr. filmov) ter komunikacijskih storitev (storitev omogočanja komunikacij mobilnim telefonom in ostalim osebnim digitalnim napravam), ki se postopoma vgrajujejo v vsa potniška letala. Omenjene funkcije so primarno namenjene potnikom, ne sodijo v domeno avionike in jih iz varnostnih, zmogljivostnih in zanesljivostnih razlogov običajno izvaja fizično popolnoma ločen računalniški sistem na letalu.

Zgodovinsko gledano sta za začetek in v nadaljevanju hiter razvoj avionike pomembna dva časovna mejnika in sicer

- vpeljava elektronskih navigacijskih sistemov za potrebe vodenja letal preko Atlantika med II. svetovno vojno in
- vpeljava "*fly by wire*" koncepta v upravljanje s potniškimi letali proizvajalca Airbus v osemdesetih letih prejšnjega stoletja.

V primeru iz prve alinee se je avionika pokazala kot izjemno koristna, saj so letala s pomočjo avionike lahko začela prečkati Atlantik po najkrajši možni poti navkljub slabim vremenskim razmeram. Do II. svetovne vojne je letalstvo namreč temeljilo na tako imenovanem *vizualnem letenju* (angl. *visual flight rules* - VFR). Slednje je temeljilo na *prepoznavnih vizualnih referencah* (npr. rekah, gorah, mestih itd.), ki jih je pilot videl iz letala. Ob slabi vidljivosti (oblačnosti, megli, dežju, sneženju in v nočnih razmerah) je bilo VFR letenje močno otežkočeno ali celo praktično nemogoče. Z vpeljavo elektronskih navigacijskih

sistemov na zemlji in v letalih se omogoči t.i. *instrumentalno letenje* (angl. *instrument flight rules* - IFR), ki temelji na uporabi elektronskih instrumentov na letalu. Slednji v domeni pozicioniranja lege letala in njegove navigacije nadomestijo predhodno omenjene vizualne reference.

V primeru iz druge alinee je avionika, ki je nadomestila težke, obrabljive in manj zanesljive mehansko-hidravlične sisteme, doprinesla k velikemu zmanjšanju teže letal, slednje pa do večje ekonomičnosti letov. Letalski operaterji so tako bodisi porabili manjše količine goriva, ali pa letala prilagodili za večje število potnikov, oboje pa je vodilo v zmanjšanje cen letalskih kart. Primer mehansko-hidravličnega sistema so bili npr. vzvodi, ki so vodili od pilotske kabine bodisi do letalnih površin (angl. *flight control surfaces*) kot so zakrilca, rep itd., ali motorjev letala, po katerih so se prenašali ukazi pilota.

Danes je avionika v civilnem letalstvu zaradi misijske kritičnosti izredno razvito področje, tako z vidika posameznih sestavnih delov (strojne in programske opreme), kot tudi s sistemskega vidika. Delež *cene razvoja* avionike za novo civilno potniško letalo se giblje pri okoli 80%, pri helikopterjih pa pri 60% celotne razvojne cene plovila. Glavni razvojni akterji na trgu avionike so Honeywell, Thales Group, BAE systems avionics, Aérospatiale itd.

1.2.1 Sestavni deli FCS sistema

FCS računalniški sistem plovila A340 je sestavljen iz sledečih sedmih računalniških enot [7] (vsi tehnični podatki glasijo na l.1996):

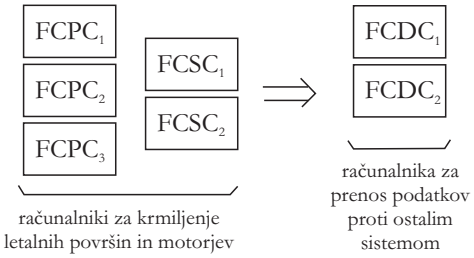
- treh redundančno realiziranih FCPC računalnikov (angl. *flight control primary computer*); vsak FCPC računalnik je realiziran v obliki 2 modularne glasovalne redundance dveh podsistemov, kar pomeni, da posamezen FCPC deluje vse dotlej, dokler delujeta oba računalnika; vseh šest podsistemov temelji na Intlovem 80386 procesorju s taktom ure 16 MHz; prvi podsistem v posameznem FCPCju je sprogramiran v zbirnem jeziku, drugi pa v PL/M jeziku; programska oprema ima približno 800kB; strojno in programsko opremo proizvaja Aérospatiale;

- dveh redundančno realiziranih FCSC računalnikov (angl. *flight control secondary computer*); tudi vsak FCSC računalnik je realiziran v obliki 2 modularne glasovalne redundance dveh podsistemov; vsi štirje podsistemi temelji na Intlovem 80186 procesorju s taktom ure 12 MHz; prvi podsistem v posameznem FCSCju je sprogramiran v zbirnem jeziku, drugi pa v jeziku Pascal; programska oprema ima približno 300kB; strojno in programsko opremo proizvaja Aérospatiale;

- dveh FCDC računalnikov (angl. *flight control data contentrators*);

Prvih pet računalnikov (FCPC, FCSC) je namenjenih krmiljenju letalnih površin in motorjev, zadnja dva (FCDC) pa sta namenjena zbiranju (funkcija koncentratorja) in prikazovanju podatkov na prikazovalnikih, opozarjanju in

alarmiranju. Podatke FCDC računalnika prevzemata od prve skupine petih računalnikov, posredujeta pa jih tudi sistemu za upravljanje letala z vidika vzdrževanja in sistemu za beleženje podatkov o letu (angl. *flight recorder*). Na sliki 1.5 je predstavljena simbolična shema opisanega sistema.



Slika 1.5: Simbolična shema funkcionalnosti sedmih računalnikov, ki tvorijo FCS sistem na letalu Airbus A340 delno povzeta po viru [7].

1.2.2 Uporaba redundance pri upravljanju A340

V predhodnem razdelku smo že omenili redundančno glasovalno izvedbo treh FCPC in dveh FCSC računalnikov. Proizvajalec se odloči še za vpeljavo dodatnih redundanc. Preden si jih ogledamo, navedimo osnovne sisteme, na katerih temelji krmiljenje plovila. Le ti so sledeči:

- *računalniški FCS sistem*: o njem smo govorili v prejšnjem razdelku;
- *računalniško omrežje*: realizirano je z množico žičnih povezav, katerih skupna dolžina na posameznem plovilu je velikostnega razreda 100 km; povezave vodijo od FCS sistema do posameznih aktuatorjev, ki so locirani neposredno pri letalnih površinah in motorjih;
- *aktuatorji*: pod pojmom aktuatorja smatramo pretvornik, ki neko vrsto signala pretvori v fizično dejavnost (npr. premik, obrat itd.); v večini primerov aktuatorji na A340 pretvarjajo ukaze prejete iz računalniškega omrežja (torej elektronske signale) v mehansko dejavnost premikov letalnih površin in ventilov na motorjih s pomočjo hidravličnih sistemov; večina aktuatorjev na A340 nastopa redundantno (če odpove eden iz redundančne množice, njegovo funkcijo opravijo drugi, ki še delujejo);
- *hidravlični sistemi*: slednji predstavljajo vire moči, s katerimi upravljajo aktuatorji; na plovilu A340 so nameščeni trije redundančni med seboj neodvisni hidravlični sistemi, označeni z oznakami Y, B in G (angl. *yellow, blue* in *green*);
- *senzorika*: predstavlja množico senzorjev, ki zajemajo vhodne podatke in jih preko računalniškega omrežja posredujejo proti FCS sistemu; na osnovi

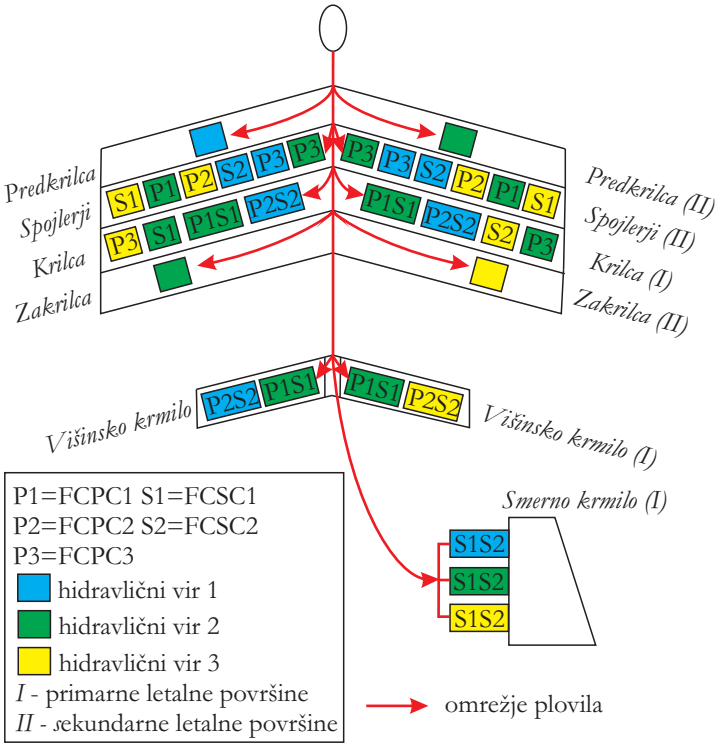
teh vhodnih podatkov FCS procesira svoje odločitve; večina senzorjev je redundantnih;

Uporabo redundance FCS, hidravličnih virov in aktuatorjev si bomo ogledali na primeru konfiguracije za krmiljenje *letalnih površin*. Slednje razdelimo na *primarne* in *sekundarne* na naslednji način:

- *primarne letalne površine* (angl. *primary flight control surfaces*):
  - *krilca* (angl. *ailerons*) so aerodinamične kontrolne površine za krmiljenje letala po nagibu okoli vzdolžne osi; nameščena so na zadnjem skrajnem robu krila [8];
  - *višinsko krmilo* (angl. *elevator*) je aerodinamična krmilna površina za krmiljenje letala po višini - okrog lateralne (prečne) osi; običajno je nameščeno na vodoravnem delu repa letala [9];
  - *smerno krmilo* (angl. *rudder*) je aerodinamična krmilna površina za krmiljenje letala po smeri glede na vzolžno os letala; po navadi je nameščeno na navpičnem delu repa letala;
- *sekundarne letalne površine* (angl. *secondary flight control surfaces*):
  - *zakrilca* (angl. flaps) so strukture na zadnjem robu kril, ki služijo spreminjanju ukrivljenosti profila krila, s čimer vplivajo na silo vzgona; omogočajo pristajanje in vzletanje pri manjših hitrostih in s tem skrajšajo potrebno vzletno in pristajalno pot [10];
  - *spojlerji* (angl. *spoilers*) so strukture na osrednjem delu kril, ki v dvignjenem stanju bistveno zmanjšajo razmerje med vzgonom in uporom in pomagajo pri zaviranju letala ob pristajanju [11];
  - *predkrilca* (angl. *slats*) so strukture na sprednjem delu kril, ki v izvlečenem stanju omogočajo letenje z manjšimi hitrostmi in večjimi vpadnimi koti (angl. *angle of attack*) [12];

Na sliki 1.6 je predstavljena redundančna konfiguracija krmiljenja primarnih letalnih površin na plovilu A340. Aktuatorji na posameznih krmiljenih letalnih površinah so označeni s četverokotniki. Z različnimi barvami četverokotnikov so označeni različni hidravlični viri, s črkami v četverokotnikih pa računalniki, ki krmilijo posamezno letalno površino. V primeru, da imamo v četverokotniku navedena dva računalniška sistema slednje pomeni, da delujeta v „*1 out of 2*“ konfiguraciji. Iz slike 1.6 je razvidno sledeče:

- ob odpovedi posameznega hidravličnega vira odpovesta največ dve od štirih razpoložljivih krilc na posameznem krilu, največ dva segmenta od štirih razpoložljivih pri višinskem krmilu, smerno krmilo pa s tem ni prizadeto; pregledali smo zgolj odpovedi segmentov primarnih letalnih površin;
- ob odpovedi enega od primarnih računalnikov odpove največ eno od štirih razpoložljivih krilc na posameznem krilu, ter največ dva segmenta od štirih razpoložljivih pri višinskem krmilu, smerno krmilo pa s tem ni prizadeto; pregledali smo zgolj odpovedi segmentov primarnih letalnih površin;



Slika 1.6: Redundanca krmiljenja primarnih letalnih površin na plovilu Airbus A340 povzeta po viru [7].

Glede na povedano lahko ugotovimo, da je redundančna arhitektura krmiljenja visoko odporna na posamezne odpovedi (angl. *single point of failure tolerant*).

1.2.3 Preventivne vzdrževalne procedure v letalstvu

Preventivno vzdrževanje letal (angl. *airplane maintenance check*) je eno od najbolj dodelanih *proceduralno opredeljenih področij* za doseganje čimvečje sistemske zanesljivosti. S terminom proceduralnosti imamo v mislih predvsem časovno in vsebinsko predoločenost preventivnega preverjanja delovanja in menjavanja sestavnih delov letal. Mednje kot pomemben segment sodi tudi avionika. Preventivno preverjanje se na področju letalstva izvaja ciklično na osnovi treh časovnih kriterijev. Le ti so sledeči:

- pretečeni absolutni čas od izvedbe predhodnega pregleda (angl. *calendar time*),
- število preletenih ur od predhodnega pregleda (angl. *flight hours*) in

- število naletov ali ciklov (vzletov in pristankov) od predhodnega pregleda (angl. *flight cycles*);

Ciklični pregledi se delijo na štiri vrste in so pogojeni s predhodno navedenimi tremi časovnimi metrikami. Omenjene vrste pregledov so sledeče:

- A poseg : izvaja se približno enkrat na mesec ali na 500 preletenih ur (angl. *flight hours*); prostor izvedbe preverjanja je običajno na samem letališkem dovozu (angl. *gate*);
- B poseg: izvaja se enkrat na približno 3 mesece na samem letališkem dovozu, pri čemer traja dlje (npr. celo noč);
- C poseg: izvaja se na vsakih 12 do 18 mesecev ali na 2.500 preletenih ur v hangarju;
- D poseg (angl. *heavy maintenance visit* - HMV): izvaja se na 4 do 5 let; letalo se pri tem praktično v celoti razstavi in nato ponovno sestavi; vrši se v pooblaščeni vzdrževalni ustanovi; za trenutno drugo največje potniško letalo Boeing 747 to pomeni v številkah 15.000 do 35.000 opravljenih delovnih ur, na letalu se tokom dela v treh izmenah v 24 urah zvrsti preko 1.000 izvajalcev, v časovnem smislu traja tudi več kot mesec dni, cena posega pa se meri v nekaj milijonih USD; od tega je 70% cene vezane na samo delo, 30% odstotkov cene pa na materialne stroške;

Termin "približnosti" v gornjih navedbah izhaja iz različnih tipov letal in njihove namembnosti. Z vidika ekonomije letalskih prevoznikov so ciklična preverjanja s predvidenimi menjavami sestavnih delov obvezna, a neželjena, ker v času servisiranja plovilo ne more vršiti svoje poslovno - tržne funkcije.

1.2.4 Komunikacijski protokoli v domeni avionike

Za potrebe „*fly by wire koncepta*“ so se razvili posebni protokoli, ki definirajo naravo podatkov in način njihovega prenosa po omrežju plovila ter med plovilom in zemeljsko infrastrukturo. Družina omenjenih protokolov nosi ime po enem od pionirskih podjetij s področja avionike in sistematizacije področja avionike ARINC (angl. *Aeronautical Radio INCorporated*), najpomembnejši od njih pa so sledeči:

- Aircraft Data Network (ADN), ARINC 664, Avionics Full-Duplex Switched Ethernet (AFDX): protokoli definirajo različico "Ethernet" omrežja za komercialna letala;
- ARINC 629: specializiran protokol za prvo Boeing-ovo "*fly by wire*" plovilo Boeing-777; protokol omogoča na podatkovno omrežje plovila priključiti 128 terminalnih enot, ki imajo možnost tako oddajati, kot tudi sprejemati sporočila; hitrost prenosa podatkov po omrežju je 2Mbit/s;
- ARINC 708: specializiran protokol za prenos vremenskih podatkov;

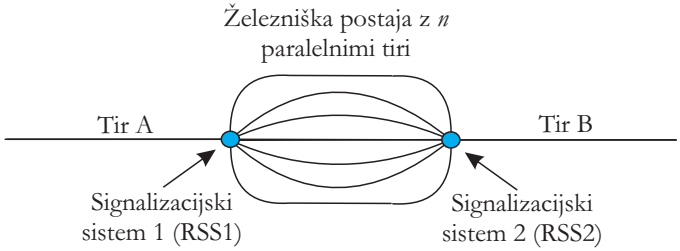
- ARINC 717: specializiran protokol za beleženje podatkov o letu (angl. *Flight Data Recorder*) za komercialna plovila;
- IEEE 1394b, MIL-STD-1553, MIL-STD-1760: specializirani protokoli za vojaška plovila;

Osnovni opis področja ARINC protokolov bralec najde v viru [13], kjer je kot izhodišče opisa družine ARINC protokolov povzet protokol ARINC 429, ki je predhodnik ARINC 629 protokola.

1.3 Redundančne konfiguracije signalizacijskih sistemov v železniškem prometu

Nadzor nad železniškim prometom je eno od misijsko kritičnih področij, ki je danes v razvitem svetu že močno informatizirano in digitalizirano. Ključni temelj digitalizacije so *železniški signalizacijski sistemi*, ki omogočajo vstopanje železniških kompozicij na posamezne *tirne odseke*.

Za boljše razumevanje zadnjega stavka predpostavimo, da imamo na neki železniški postaji n paralelnih *postajnih tirov*, do postajnih tirov pa je možno dostopati preko dveh dvosmernih *prometnih tirov*, kot je prikazano na sliki 1.7. Iz varnostnih razlogov moramo pri menjavanju tirnega odseka (vstop iz pro-



Slika 1.7: Simbolična shema železniške postaje s paralelnimi tiri in dvema vhodno-izhodnima tiroma.

metnega tira na postajnega in obratno) posameznim vlakovnim kompozicijam zagotoviti mehanizem signaliziranja, ki v poljubni časovni točki dovoljuje ali prepoveduje vstop iz enega tirnega odseka na drugega. V ta namen so železnice opremljene z digitaliziranimi železniškimi signalizacijskimi sistemi, ki vršijo sledeči funkciji:

- signalizirajo vlakovni kompoziciji dovoljenje ali prepoved za vstop na posamezen tirni odsek;
- posredujejo preko različnih komunikacijskih povezav podatke o vstopu ali izstopu vlakovne kompozicije s posameznega tirnega odseka *centralnemu nadzornemu sistemu*;

Za doseganje zanesljivosti delovanja celotnega sistema nadzora prometa morajo delovati posamezni digitalizirani signalizacijski sistemi čimbolj zanesljivo. Področje doseganja zanesljivosti nadzora železniškega prometa pokrivajo mnogi standardi (npr. EN 50126, EN 50128, EN 50129). Z našega zornega kota je zanimiv posamezen signalizacijski sistem, ki ga lahko pojmujemo kot računalniški sistem lociran na neki geografski točki v nadzorovanemu železniškemu omrežju. Dve takšni enoti (dva signalizacijska sistema) sta predstavljeni na sliki 1.7. V nadaljevanju se bomo na posamezen signalizacijski sistem sklicevali s kratico RSS (računalniški signalizacijski sistem). Več osnov o delovanju signalizacijskih sistemov v železniškem prometu bralec najde v delu [14].

Upoštevajoč standarde za doseganje zanesljivosti delovanja posamezne RSS enote, morajo biti slednje realizirano redundančno s čimer maksimiziramo *dosegljivost* in *zanesljivost* delovanja posamezne RSS enote. Tipične vrste uporabljene redundance v RSS sistemih so sledeče:

- 2oo2 konfiguracija: sistem je sestavljen po načelu „*2 out of 2*“;
- 2x2oo2 konfiguracija: sistem je sestavljen po načelu sklopljenosti dveh „*2 out of 2*“ podsistemov;
- 2oo3 konfiguracija: sistem je sestavljen po načelu „*2 out of 3*“;

Najvidnejši proizvajalci in integratorji RSS sistemov na evropskem tržišu so Alstom, AŽD Praha, Bombardier, Siemens in Thales.

Literatura

[1] D. Jenkins, *Space Shuttle: The History of the National Space Transportation System.* by Dennis R.Jenkins, USA, 2001.

[2] M. L. Shooman, *Reliability of computer systems and networks: fault tolerance, analysis, and design.* J.Wiley and Sons, 2002.

[3] "What operating system(s) were used in the space shuttle?." `https://space.stackexchange.com/questions/19006/what-operating-systems-were-used-in-the-space-shuttle`, Marec 2019.

[4] J. R. Sklaroff, "Redundancy Management Technique for Space Shuttle Computers," *IBM Journal of Research and Development*, vol. 20, no. 1, pp. 20–27, 1976.

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

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

[7] N. Storey, *Safety critical computer systems.* Addison Wesley Longman, 1996.

[8] "Krilca." `https://sl.wikipedia.org/wiki/Krilca`, Marec 2019.

[9] "Višinsko krmilo." `https://sl.wikipedia.org/wiki/Vi%C5%A1insko_krmilo`, Marec 2019.

[10] "Zakrilca." `https://sl.wikipedia.org/wiki/Zakrilca`, Marec 2019.

[11] "Zaviranje letala." `https://sl.wikipedia.org/wiki/Zaviranje_letala`, Marec 2019.

[12] "Podaljšano sprednje krilo." `https://sl.wikipedia.org/wiki/Podalj%C5%A1an_sprednji_rob_kril`, Marec 2019.

[13] "ARINC Protocol Tutorial." `http://leonardodaga.insyde.it/Corsi/AD/Documenti/ARINCTutorial.pdf`, Maj 2019.

[14] L. Tang, "Reliability assessments of railway signaling systems: A comparison and evaluation of approaches," Master's thesis, Norwegian University of Science and Technology, Norveška, 2015.