Poglavje 1

Analiza varnosti delovanja sistemov in FRAM metoda

V naslovu pričujočega poglavja prvič omenimo pojem *varnosti delovanja sistema* (angl. *system's operation safety*). Pri tem pojma varnosti ne smemo enačiti z informacijsko, podatkovno ali omrežno varnostjo, temveč imamo z njim v mislih varnost delovanja sistema z vidika posledic njegovega nepravilnega delovanja.

Soroden pojmu varnosti je pojem *inženirstva „odpornosti“* (angl. *resilience engineering*), ki vpeljuje metode, na osnovi katerih bi kompleksnejši sistemi, katerih deli so tudi računalniki, postali „odporni“ na variabilnosti in odpovedi posameznih sistemskih funkcij. Med omenjene metode spada tudi metoda FRAM, ki si jo bomo ogledali v nadaljevanju. V nadaljevanju navedemo definicijo „odpornosti“ sistema povzeto po [1].

Definicija 1 *Sistem je „odporen“ (angl. resilient), če je zmožen svoje delovanje prilagajati pričakovanim in nepričakovanim spremembam ter motnjam in s tem vzdrževati željene funkcionalnosti.*

Tretji novi pojem, s katerim se srečujemo v tem poglavju, je pojem velikih in kompleksnih *socio-tehničnih sistemov* (angl. *large-scale socio-technical systems*), s katerimi se soočamo v zadnjem desetletju. Slednji so postali tako kompleksni, da jih ne moremo več obravnavati samo skozi zanesljivosti posameznih sestavnih delov (npr. programske ali strojne opreme), temveč moramo v njihovo analizo vključiti tudi vidike njihove prepletenosti. Omenjeno analizo je mnogokrat nemogoče izvesti zaradi obsežnosti sistemov in zaradi njihove velike kompleksnosti. Na tem mestu sledi ugotovitev, da večine kompleksnih sistemov ne razumemo do te mere, da bi lahko predvideli vse možne neželjene dogodke.

1.1 Koncepta analize „Safety-I“ in „Safety-II“

Varnost delovanja sistema običajno enačimo z neko dovolj majhno intenzivnostjo porajanja neželjenih dogodkov kot so *nesreče* ali *incidenti*, ki ne sme biti presežena [1].

Klasično področje zagotavljanja varnosti delovanja sistemov je fokusirano na *neželjene dogodke* (angl. *adverse outcomes*) in si za cilj zadaja čim manjše število njihovih porajanj. Tovrstno gledanje na varnost poimenujemo s terminom „Safety-I“ [1]. Omenjeni pristop je *reakcijske narave* (angl. *reactive approach*), saj v večini primerov do ukrepanja pride po porajanju neželjenih dogodkov. Uporaben je le v primeru, ko je frekvenca porajanja neželjenih dogodkov izredno majhna.

Novoporajajoče področje zagotavljanja varnosti delovanja sistemov vzame v obzir našo nezmožnost razumevanja celotnega sistema, njegov fokus pa se preusmeri iz neželjenih dogodkov na normalno delovanje sistema, kjer se sistemske funkcije izvajajo pravilno. Tovrstno gledanje na varnost poimenujemo s terminom „Safety-II“ [1]. „Safety-II“ tako varnosti ne definira z odsotnostjo neželjenih dogodkov, temveč z razumevanjem vsakodnevnega normalnega funkcioniranja sistema. Osnova za normalno funkcioniranje sistema je po [1] vseskozno prilagajanje sistema (njegovih tehničnih, človeških in organizacijskih segmentov) na različne situacije in spremembe.

Več o konceptih „Safety-I“ in „Safety-II“ si bralec lahko prebere v delu [2].

1.2 FRAM metoda

FRAM metoda ali *analiza funkcijske resonance* (angl. *functional resonance analysis method* - FRAM) je ena od novejših metod za kvalitativno sistemsko analizo zanesljivosti, ki se trenutno (op.p. l.2019) vpeljuje v mnoge misijsko kritične sisteme, kot je npr. sistem DFS (Deutsche Flugsicherung Gmbh) - sistem nemške kontrole zračnega prometa. Avtor metode je Erik Hollnagel, primarno pa je bila razvita za potrebe analiz kliničnih obravnav pacientov v zdravstvu. Metoda služi tako za analize že minulih neželjenih dogodkov (angl. *retrospective analysis*), kot tudi za analize porajanja bodočih neželjenih dogodkov (angl. *prospecitve analysis*), do katerih lahko pride v opazovanem sistemu. Po izvedbi ene ali druge vrste analize naredimo sistemske popravke, ki število neželjenih dogodkov (angl. *adverse events*) minimizirajo. FRAM metoda je primarno namenjena področju analize velikih socio-tehničnih sistemov. Osnove metode so prikazane v javno dostopni elektronski knjigi navedeni v viru [1].

1.2.1 Osnove FRAM metode

FRAM metodo izvajamo v sledečih štirih korakih [1]:

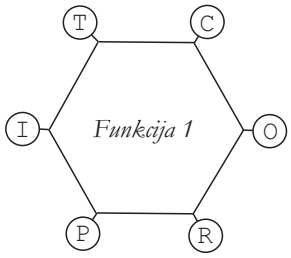
- identifikacija in opis pomembnih *sistemskih funkcij* ter okarakteriziranje teh funkcij glede na njihovih šest osnovnih *aspektov* (angl. *aspects*);

- identifikacija *potencialne variabilnosti delovanja* posameznih sistemskih funkcij;

- določitev možnosti *funkcijske resonance* na sistemskem nivoju glede na funkcijske soodvisnosti ali medsebojno povezanost funkcij;

- določitev *načina monitoriranja* ali *spremljanja variabilnosti* in *vplivanja* nanjo;

Z vidika zadnje alinee je naš cilj minimizirati ali celo popolnoma zadušiti variabilnost, ki vodi do neželjenih dogodkov in maksimizirati variabilnost, ki vodi do normalnega delovanja (željenih dogodkov). Na sliki 1.1 je predstavljena grafična ponazoritev posamezne sistemske funkcije. Ponazorjena je s šestkotnikom, katerega ogljišča predstavljajo *funkcijske aspekte*, ogljišča pa istočasno predstavljajo vozlišča funkcije, preko katerih opazovano funkcijo lahko povezujemo z aspekti ostalih sistemskih funkcij. Pomeni povezovalnih točk (vozlišč ali



Slika 1.1: Grafična ponazoritev posamezne sistemske funkcije z označbo njenih aspektov.

aspektov) so sledeči [1]:

- I - vhod v funkcijo predstavlja zahtevo za izvedbo funkcije in s tem posredno zahtevo za generiranje izhoda funkcije; v splošnem je vhod funkcije lahko materialna snov, energija ali informacija - podatek; vhod običajno poimenujemo s samostalniško besedo;

- O - izhod funkcije predstavlja rezultat izvedbe funkcije; v splošnem je izhod funkcije lahko materialni produkt, energija ali informacija - podatek; izhod funkcije običajno predstavlja vhod za neko drugo funkcijo; tudi izhod v večini primerov poimenujemo s samostalniško besedo;

- T - čas definira načine, kako lahko časovna dimenzija (npr. časovna relacija) vpliva na izvajanje funkcije; primera časovnih relacij bi bila npr. zahteva, da se mora neka funkcija do konca izvesti pred začetkom izvajanja neke druge funkcije, ali definicija, da se neka funkcija izvaja n časovnih enot;

- C - kontrolni vhod (angl. *control*) nadzira izvajanje funkcije, da se realizira ustrezen izhod; kontrolni vhod je lahko načrt, urnik, procedura, spisek instrukcij, program itd.; manj formalen kontrolni vhod (angl. *social control*) je npr. pričakovanje kako se naj funkcija - opravilo izvede; tudi kontrolni vhod v večini primerov poimenujemo s samostalniško besedo;

- P - predpogoj za izvedbo funkcije (angl. *precondition*) predstavlja pogoj, ki mora biti izpolnjen, preden se funkcija začne izvajati; narava pogoja je lahko logičnega tipa `True - False`, ali pa splošnega tipa (npr. primerjanje dveh števil); izpolnjenost predpogoja ni dovoljšnja za proženje funkcije, saj slednjo lahko dokončno sproži le vhod; predpogoj P mora biti vezan na izhod ene od preostalih funkcij, kar pomeni, da je predpogoj pogojen z izhodom neke druge funkcije; tudi predpogoj v večini primerov poimenujemo s samostalniško besedo;

- R - resurs (angl. *resource*) mora biti obvezno prisoten pri izvedbi funkcije; v splošnem je resurs funkcije lahko materialna snov, energija, informacija - podatek, kompetenca, programska oprema, orodje itd.; pomembna značilnost resursov je, da se lahko v času izvajanja funkcije *porabljajo* ali *ne porabljajo*; Hollnagel prve imenuje za prave *resurse* (angl. *resources*), druge pa za *izvajalne pogoje* (angl. *execution conditions*); za zgled navedimo primer povzet po viru [1]; krvna plazma pri operativnem posegu predstavlja pravi resurs (se skozi operacijo porablja), kompetenca ali znanje zdravstvenega delavca pa izvajalni pogoj (se skozi operacijo ne porablja); razlika med predpogojem in izvajalnim pogojem je v tem, da mora predpogoj biti izpolnjen le ob začetku izvajanja funkcije, izvajalni pogoj pa skozi celoten čas izvajanja funkcije; tudi resurs v večini primerov poimenujemo s samostalniško besedo;

Hollnagel funkcije deli na dve skupini in sicer na funkcije iz *ospredja* (angl. *foreground functions*) in na funkcije iz *ozadja* (angl. *background functions*). Delitev funkcij ne izhaja iz njihovega pomena, temveč iz njihove vloge v modelu. Funkcije iz ospredja so običajno v fokusu opazovanja vpliva njihove variabilnosti na delovanje sistema kot celote. Po dugi plati za funkcije iz ozadja smatramo tiste funkcije, za katere variabilnost ni možna in s tem ne vplivajo na resonanco funkcijskega sistema. Značilnosti funkcij iz ospredja so sledeče:

- funkcije morajo imeti definirane vhode;

- funkcije morajo imeti povezan vhod in izhod;

Značilnosti funkcij iz ozadja so sledeče:

- ni nujno, da imajo funkcije definirane vhode;

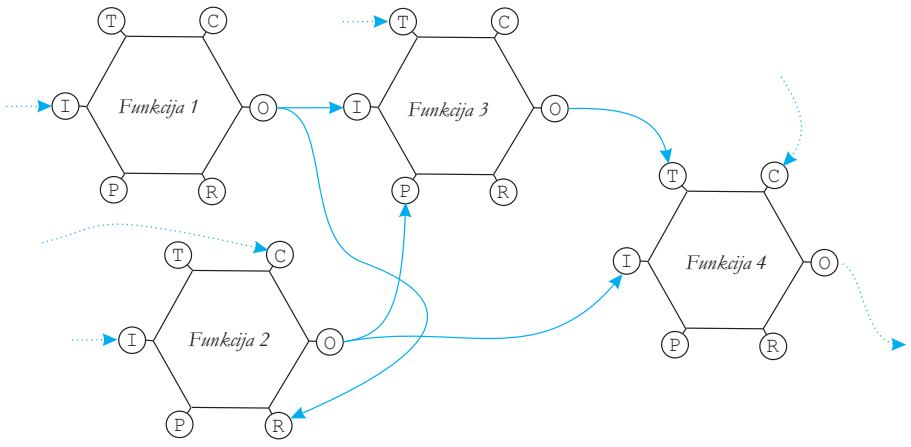
- funkcije morajo imeti definirane izhode, ki običajno vodijo na aspekte funkcij iz ospredja;

Druga delitev funkcij, ki jo vpelje avtor metode, je delitev funkcij na „upstream“ in „downstream“ funkcije. Predpostavimo, da je naš fokus usmerjen na dogajanje v eni od funkcij. V skupino „upstream“ funkcij sodijo vse tiste funkcije, ki so se izvedle pred njo, v skupino „downstream“ funkcij pa vse tiste, ki se bodo izvedle po njej. Iz povedanega je razvidno, da se klasifikacija funkcij po zadnjem kriteriju skozi čas spreminja - je relativna.

Tretja delitev sistemske funkcije razvršča na tri skupine in sicer na *tehnološke* (angl. *technological*), *človeške* (angl. *human*) in *organizacijske funkcije* (angl. *organisational*). Prav ta delitev je z vidika varnosti delovanja sistema izredno pomembna, saj običajno v analitični praksi premalo pozornosti posvetimo človeškim in organizacijskim funkcijam, ki nastopajo v večjih socio - tehničnih sistemih.

1.2.2 Povezovanje funkcij

Predpostavimo, da smo na prvem koraku FRAM analize identificirali n sistemskih funkcij. Na osnovi tega lahko narišemo graf z n vozlišči - šesterokotniki. Ključni korak k doseganju modela sistema za analizo je *povezovanje aspektov* med posameznimi funkcijami ali identifikacija njihovih medsebojnih relacij. Običajno to povezovanje izvedemo z neusmerjenimi povezavami, saj nam smer pretoka po povezavah odkrivajo aspekti, ki so povezani. Narava posamezne povezave je v splošnem tipa k_1:k_2 (angl. *many to many*) in ne nujno samo tipa 1:1 (angl. *one to one*). Primer povezane strukture povzet po [1] je prikazan na sliki 1.2, zaradi preglednosti medfunkcijskih relacij pa povezan z usmerjenimi povezavami.



Slika 1.2: Grafična ponazoritev povezanih sistemskih funkcij.

1.2.3 Princip resonance

Sovpadanje variabilnosti delovanja velikega števila sistemskih funkcij nas lahko občasno pripelje do vzajemnih vplivov med posameznimi funkcijami. Slednje lahko vodi v velike izhodne amplitude posameznih funkcij, ki se manifestirajo v pozitivnih ali negativnih (neželjenih) dogodkih. Omenjeni pojav poimenujemo za *fenomen resonance* [1]. V tem primeru so vzroki za povečano amplitudo (dogodek) težko določljivi in niso enostavno linearno izrazljivi. Poznamo tri osnovne tipe resonance in sicer

- *klasično resonanco* v fizikalnih sistemih: zanjo je tipično, da sistem lahko pri različnih frekvencah vzburjanja oscilira z različnimi amplitudami; prevelike amplitude oscilacij lahko vodijo do uničenja sistema; tipičen primer tovrstnega sistema je otroška gugalnica;
- *stohastično resonanco*: v primeru slednje zunanjo silo vzburjanja nadomesti naključni šum; rezultat stohastične resonance je nelinearen glede na vzburjevalni pulz;
- *funkcijsko resonanco*: slednja opisuje performančno variabilnost posameznih funkcij kot rezultat prilagajanja (angl. *adjustments*) socio-tehničnega sistema v okviru svojega delovanja; definiramo jo kot izhod ali signal nepričakovane - nepredvidene interakcije variabilnih, a sicer normalnih funkcijskih izhodov;

1.2.4 Avtomatizacija izvedbe FRAM analize

V kontekstu avtomatizirane analize modelov je na spletu javno dostopno programsko orodje „FRAM Model Visualiser“ (FMV). Slednje omogoča grafično postavitev modelov sistemskih funkcij in povezave njihovih aspektov, pri čemer trenutno (op.p. januarja l.2019) še ni razvit modul za avtomatizirano izvajanje analize funkcijske resonance. FMV model sistemskih funkcij shranjuje v standardizirani XML obliki in je trenutno v fazi razvoja.

Temeljitejši opis metode FRAM bralec najde v delu [3].

Literatura

[1] E. Hollnagel, J. Hounsgaard, and J. Colligan, *FRAM - the Functional Resonance Analysis Method*. Center for Quality in Southern Region of Denmark, 2014.

[2] E. Hollnagel, *Safety-I andf Safety-II: The Past and Future of Safety Management*. Ashgate Publishing Limited, 2014.

[3] E. Hollnagel, *FRAM: The Functional Resonance Analysis Method Modelling Complex Socio-technical Systems*. Ashgate Publishing Limited, 2012.