Univerza v Ljubljani

Fakulteta za računalništvo in informatiko

Tržaška 25, Ljubljana

Seminarska naloga

FMEA

Nenapovedan izpad računalniškega sistema v zdravstveni ustanovi

Računalniška zanesljivost in diagnostika

Ljubljana, 14. maj 2007

mentor:
prof. Miha Mraz

avtor:
Tine Lesjak
63030315

Kazalo

Kazalo 2
Uvod 3
FMEA 3
  Ozadje 3
FMEA postopek 4
  Korak 1: Izberemo proces 4
  Korak 2: Sestavimo večdisciplinsko ekipo 4
  Korak 3: Zapišemo korake v procesu 4
  Korak 4: Zapišemo seznam načinov odpovedi, njihovih vzrokov in posledic 5
    Načini odpovedi 6
    Vzroki odpovedi 6
    Posledice odpovedi 7
  Korak 5: Določimo RPN 7
  Korak 6: Določimo izboljšave 8
  FMEA tabela 9
Sklep 9
Viri 10

Uvod

Ta dokument naj bi predstavljal analizo enega procesa na primeru iz zdravstva. Zdravstvo je zelo širok pojem in kot takšen zajema vse od institucij (ministrstev, inštitutov itd.), prek ustanov (klinik, bolnišnic, zdravstvenih domov itd.), osebja (zdravnikov, sester itd.), pacientov, zdravil, do opreme, kot je računalniška.
Primer, ki ga bomo obravnavali, podaja analizo možnih problemov, njihovih vzrokov in posledic - FMEA - na primeru **nenapovedanega izpada računalniškega sistema**. Primer je resnično delo neke ameriške zdravstvene ustanove, ki se je odločila zmanjšati rizik izpada sistema za 50 odstotkov v šestih mesecih - to je cilj.

Analizo bom predstavil po korakih. Najprej se bomo seznanili z osnovami FMEA, nato bomo po bolj ali manj ustaljenih korakih skušali ovrednotiti proces, ki sledi ob nenapovedanem izpadu računalniškega sistema. Kot dodatek je priložena tudi tabela, ki opisuje vso FMEA analizo procesa v obliki pregledne tabele.

FMEA

Analiza načinov odpovedi in učinkov (failure modes and effects analysis - FMEA) je sistematična, proaktivna metoda za vrednotenje nekega procesa v smislu identificiranja, kje in kako lahko pride do odpovedi. Z njo ocenjujemo relativne posledice različnih odpovedi in tako odkrijemo dele procesa, ki so najbolj potrebni spremembe.

FMEA je pregled:
- korakov v procesu,
- načinov odpovedi (kaj lahko gre narobe),
- vzrokov odpovedi (zakaj lahko pride do odpovedi) in
- posledic odpovedi (kakšne so lahko posledice za vsako odpoved).

Ekipe uporabljajo FMEA, da vrednotijo možne odpovedi procesa in da jih preprečujejo tako, da popravljajo procese proaktivno namesto šele takrat, ko se odpoved že zgodi in že škodi. To lahko zmanjša rizik za poškodbe tako pacientov kot osebja. FMEA je zlasti uporabna pri vrednotenju novega procesa, ki še ni implementiran, in v ocenjevanju posledic predlaganih sprememb že obstoječega procesa.

Ali naredite kaj za to, da ne bi zamujali na delo?
Ali uberete drugo pot, kadar vidite gnečo na znanem mestu?
Ali skušate razlikovati med "velikimi" in "majhnimi" problemi?
Ali vidite rešitve za določene probleme, vendar potrebujete boljši način, da to pokažete ljudem?

Vaši odgovori kažejo na to, da že uporabljate nekatere principe FMEA, da bi preprečili probleme v vsakdanjem življenju.

Ozadje

FMEA je bila razvita zunaj zdravstvene stroke in se sedaj uporablja v zdravstvu za ocenjevanje rizikov odpovedi in posledic v procesih ter za odkrivanje najpomembnejših delov procesa, ki jih lahko izboljšamo. FMEA uporablja na stotine zdravstvenih ustanov.

FMEA uporabljajo inženirji po vsem svetu v:

- letalski industriji
- jedrski energiji
- vesoljski tehnologiji
- kemični industriji
- avtomobilski industriji
- ...

FMEA se uporablja že približno 30 let. Njen cilj je bil in ostaja še danes: preprečevanje nastanka nesreč.

FMEA postopek

Korak 1: Izberemo proces

Vrednotenje s FMEA deluje najbolje na procesih, ki nimajo preveč podprocesov. Namesto, da bi uporabljali FMEA na velikih in kompleksnih procesih, kakršen je vodenje zdravil v bolnišnicah, se FMEA uporablja na **podprocesih** ali njihovih variantah. Izvajati FMEA na celotnem procesu vodenja zdravil bi bila prevelika naloga. Namesto tega, izvajamo ločene FMEA analize na posameznih delih, kot so naročanje zdravil, razdajanje zdravil in administrativni postopki.

V našem primeru je proces že znan: Nenapovedan izpad računalniškega sistema v zdravstveni ustanovi.

Korak 2: Sestavimo večdisciplinsko ekipo

Prepričati se je treba, da so v ekipi vsi, ki so vpleteni v katerokoli točko v procesu. Nekaterim ljudem ni treba, da so prisotni v ekipi skozi ves čas analize, vendar nedvomno morajo sodelovati pri razpravi korakov, v katere so vpleteni. Na primer, da želi bolnišnica uporabiti kurirje za transport zdravil od farmacevtske tovarne do enote za bolniško nego. Tako je zelo pomembno vključiti kurirje v FMEA analizo korakov, ki opisujejo sam transport, kar morda ni znano osebam v tovarni ali enoti za bolniško nego.

Korak 3: Zapišemo korake v procesu

Naštejemo vse potrebne korake v procesu in smo pri tem čim bolj specifični. Za dokončanje seznama je morda treba organizirati več sestankov, odvisno od tega, kako kompleksen je proces. V pomoč je lahko tudi risanje diagramov poteka. Ko je seznam dokončan, se morajo vsi člani ekipe soglasno strinjati, da našteti koraki natančno opisujejo proces.

1. Prijava izpada računalniškega sistema nadzorniku
   Osebje, ki zazna, da računalniški sistem ne deluje po predvidevanjih ali se sploh ne odziva, prijavi opažanja nadzorniku.

2. Nadzornik prijavi izpad računalniškega sistema informacijskemu oddelku

Nadzornik ob pozivu osebja, ki je zaznalo izpad, opozori osebje v informacijskem oddelku (IO) tako, da pokliče telefonista in želi vzpostaviti telefonsko zvezo z osebjem v IO.

3. Telefonist prikliče informacijski oddelek
   Telefonist vzpostavi povezavo s kličočim nadzornikom in osebjem v IO.

4. Osebje informacijskega oddelka ovrednoti problem
   Osebje IO takoj ovrednoti in identificira problem. Osebje IO tudi čimprej ugotovi, če je problem sploh rešljiv.

5. Nadzornik razglasi uveljavitev "postopkov ob izpadu"
   Če je bilo ugotovljeno, da izpad sistema ne more biti rešljiv takoj, nadzornik razglasi, da mora vso osebje upoštevati tako imenovane postopke ob izpadu (downtime procedures).

   Postopki ob izpadu (downtime procedures) so množica posebnih vnaprej pripravljenih postopkov, ki se izvajajo takrat, ko računalniški sistem ne deluje. Postopki ob izpadu se lahko uveljavijo po vnaprej določenem urniku zaradi posodobitve opreme ali ob nepredvidenem izpadu.

6. Razglasi se "notranja katastrofa" in aktivira se primerno "telefonsko drevo"
   V primeru nerešljivega izpada računalniškega sistema, se razglasi tako imenovana notranja katastrofa (internal disaster). Obvesti se vse ljudi po načelu tako imenovanega telefonskega drevesa (phone tree).

   Notranja katastrofa (internal disaster) je stopnja, pri kateri stopi pod vprašaj varnost ali zdravje osebja. Od zunanje katastrofe se loči po tem, da nastane in preti samo določeni ustanovi. Med notranje katastrofe spadajo požar, grožnja bombnega napada, razlitje kemične snovi ali izpad pomembnih sistemov (voda, elektrika, ogrevanje, računalniki).

   Telefonsko drevo (phone tree) je predpripravljen, piramidno (hierarhično) zasnovan sistem za aktiviranje neke skupine ljudi prek telefona. Z uporabo telefonskega drevesa se lahko sporočilo razprši hitro in učinkovito velikemu številu ljudi.

7. Problem se odpravi in sistem je znova vzpostavljen
   Napake, ki je povzročila izpad računalniškega sistema, ni več in sistem znova teče.

8. Prekličejo se postopki ob izpadu
   Postopki ob izpadu, ki so se izvajali, medtem ko računalniški sistem ni bil na voljo, se prekličejo. Vzpostavijo se normalno stanje in normalni postopki.

Korak 4: Zapišemo seznam načinov odpovedi, njihovih vzrokov in posledic

Za vsak korak v procesu zapišemo vse možne načine odpovedi (failure modes) - to je vse, kar lahko gre narobe, vključujoč manjše in redke probleme. Za vsak način odpovedi identificiramo možne vzroke (causes). Nato zapišemo še vse potencialne posledice (effects, impacts), ki jih prinaša vsaka odpoved.
Lahko se zgodi, da ima več načinov odpovedi isti vzrok in podobne posledice.

Načini odpovedi

1. Prijava izpada računalniškega sistema nadzorniku
   - Osebje izpada ne prijavi takoj nadzorniku.

2. Nadzornik prijavi izpad računalniškega sistema informacijskemu oddelku
   - Nadzornik izpada ne prijavi takoj osebju IO.

3. Telefonist prikliče informacijski oddelek
   - Telefonist ne more vzpostaviti stika z osebjem v IO.

4. Osebje informacijskega oddelka ovrednoti problem
   - Osebje v IO ne more doseči sistema.
   - Osebje v IO ne more ugotoviti vzroka izpada v 30 minutah.

5. Nadzornik razglasi uveljavitev "postopkov ob izpadu"
   - Nadzornik ne razglasi in skupaj z upravniki ne pričnejo postopkov ob izpadu.

6. Razglasi se "notranja katastrofa" in aktivira se primerno "telefonsko drevo"
   - Notranja katastrofa se ne razglasi.
   - Nadzornik ne more doseči primernega osebja v IO po telefonskem drevesu.

7. Problem se odpravi in sistem je znova vzpostavljen
   - Problem izpada se ne razišče dovolj dobro ali sploh ne.

8. Prekličejo se postopki ob izpadu
   - Postopki ob izpadu so bili preklicani, vendar celoten sistem še vedno ne deluje po pričakovanjih.
   - Osebje ni dobilo sporočila o preklicu postopkov ob izpadu.

Vzroki odpovedi

1. Prijava izpada računalniškega sistema nadzorniku
   - Osebje, ki zazna nepredvideno obnašanje sistema, tega ne prijavi takoj, ker ne razume, kako pomemben je izpad oz. koliko zajema.

2. Nadzornik prijavi izpad računalniškega sistema informacijskemu oddelku
   - Nadzornik ne more prijaviti izpada takoj, ker telefonist ne more vzpostaviti povezave z osebjem v IO.

3. Telefonist prikliče informacijski oddelek
   - Osebje v IO ni na voljo, ker je odsotno (npr. so na izobraževanju). Rezervno osebje je bolno.
   - Še precej drugih potencialnih vzrokov, kot so izpad telefonskega omrežja, zunanje katastrofe itd.

4. Osebje informacijskega oddelka ovrednoti problem
   - Vse od izpada električnega omrežja, zunanje katastrofe ali sistemskih napak. Vse to je prek sposobnosti in izkušenj osebja v IO.

5. Nadzornik razglasi uveljavitev "postopkov ob izpadu"

- Ni možno najti postopkov ob izpadu. Stvari, ki se uporabljajo pri postopkih ob izpadu, niso pripravljene. Dodatno osebje za podporo pri postopkih ob izpadu ni na voljo.

6. Razglasi se "notranja katastrofa" in aktivira se primerno "telefonsko drevo"
   - Pri odločanju, ali se naj razglasi notranja katastrofa, lahko preteče precej časa. Notranja katastrofa je zato razglašena z zamudo ali celo prepozno.
   - Telefonske številke telefonskega drevesa niso ažurirane.

7. Problem se odpravi in sistem je znova vzpostavljen
   - Problem je lahko večjih razsežnosti: naravna katastrofa, izpad redundantnih sistemov, večja strojna napaka ali druge še neugotovljene okoliščine.

8. Prekličejo se postopki ob izpadu
   - Osebje v IO verjame, da je sistem ponovno vzpostavljen in delujoč, vendar sistem ne deluje pravilno oz. po predvidevanjih.
   - Osebje izvaja postopke ob izpadu, čeprav sistem že deluje.

Posledice odpovedi

Posledice vseh načinov odpovedi v našem primeru so bolj ali manj enake.
Vsaka sekunda, ko ni znano, kaj se dogaja, povzroči počasen oz. pozen prehod na postopke ob izpadu. To je potencialen vzrok za zamude pri kritičnem zdravljenju ali celo prekinitev stalne nege pacientov.

Korak 5: Določimo RPN

Za vsak način odpovedi določimo numerično vrednost (risk priority number - RPN) za pogostost pojavitve odpovedi, možnost pravočasnega zaznavanja in resnost posledic.

RPN nam pomaga prioritizirati področja, na katera se osredotočimo, in prav tako pomaga ocenjevati priložnosti za izboljšave.
Za vsak identificiran način odpovedi odgovorimo na naslednja vprašanja in tako določimo RPN (seveda se morajo vsi člani ekipe soglasno strinjati):

- Pogostost pojavitve (occurence): Kako pogosto se bo ta način odpovedi pojavljal?
  Določimo vrednost od 1 do 10, pri čemer pomeni 1 praktično nikoli in 10 zelo pogosto.

- Možnost zaznavanja (detection): Če se pojavi ta način odpovedi, kakšna je možnost, da bo pravočasno zaznan?
  Določimo vrednost med 1 in 10, pri čemer pomeni 1 zelo veliko možnost in 10 zelo majhno možnost zaznavanja.

- Resnost (severity): Če se pojavi ta način odpovedi, kakšna je resnost posledic?
  Določimo vrednost med 1 in 10, pri čemer pomeni 1 zelo majhno posledico in 10 zelo resno posledico. Vrednost 10 pomeni v primeru pacienta njegovo smrt.

Za izračun RPN-ja za vsak način odpovedi enostavno matematično zmnožimo med seboj vse tri vrednosti (vrednosti 1 do 10 za pogostost pojavitve, možnost zaznavanja in resnost posledic). Najmanjši RPN je lahko 1, največji pa kar 1000. Načine odpovedi, ki imajo

največji RPN, se najbolj splača **vzeti kot prve** pod drobnogled in jih skušati omiliti oz. odpraviti. Za izračun RPN-ja za celoten proces, enostavno seštejemo RPN-je posameznih načinov odpovedi.

$$\text{RPN} = \text{O (pojavitev)} \cdot \text{D (zaznavanje)} \cdot \text{S (resnost)}$$

Vse tri vrednosti smo določili in izračunali RPN v poglavju "FMEA tabela".

Korak 6: Določimo izboljšave

Načini odpovedi z visokim RPN-jem so verjetno najbolj pomembni deli v procesu, na katere se je treba osredotočiti. Načini odpovedi z zelo nizkim RPN-jem nimajo velikega vpliva na celoten proces, zato naj bodo na dnu prioritetne lestvice.

Vse načine odpovedi postavimo v **prioritetno lestvico** glede na njihov RPN. Na podlagi te lestvice se lotimo izboljšav, tako da določimo **dejanja** (actions), ki jih moramo vpeljati v proces, da bomo z razmeroma malo truda naredili čim večji učinek na bolje.

1. Prijava izpada računalniškega sistema nadzorniku
    - Direktor IO pripravi temo razgovora za osebje o postopkih, ki sledijo ob izpadu sistema.

2. Nadzornik prijavi izpad računalniškega sistema informacijskemu oddelku
    - Direktor IO z nadzorniki potrdi alternativni plan za takšne situacije. Primer za nadzornika bi bil, da osebno poroča problem telefonistu, ta pa bo neodvisno kontaktiral osebje v IO.

3. Telefonist prikliče informacijski oddelek
    - Nadzornik nemudoma razglasi uveljavitev postopkov ob izpadu.
    - Direktor IO poduči nadzornike in vodstvo.
    - Telefonisti vzdržujejo obsežen seznam klicnih številk za osebja v IO in višjih vodij. Direktorji pregledajo in popravijo seznam klicnih številk vsako četrtletje. Pregled tudi podrobno beležijo in si zapišejo vse posodobitve telefonskega sistema vsako četrtletje.

4. Osebje informacijskega oddelka ovrednoti problem
    - Nadzornik nemudoma razglasi uveljavitev postopkov ob izpadu.
    - Direktor IO poduči nadzornike in vodstvo.

5. Nadzornik razglasi uveljavitev "postopkov ob izpadu"
    - Direktor IO in inštitut pripravita izobraževanje za vodstveno ekipo o postopkih ob izpadu.
    - Direktorji in vodje izobražujejo zaposlene na sestankih.
    - Direktorji pregledajo postopke ob izpadu za morebitne izboljšave vsako četrtletje.
    - Inštitut in direktor IO organizirajo naključne revizije za povečanje natančnosti. Vsako četrtletje izvajajo revizijo zunanji izvajalci.
    - Uprava naredi načrt, kako pridobiti dodatno osebje, ko je potrebno. Uprava poduči nadzornike o tem načrtu.

6. Razglasi se "notranja katastrofa" in aktivira se primerno "telefonsko drevo"

- Direktor IO poduči vodstvo, da se izpad sistema (ko je ugotovljeno od osebja v IO, da ne more biti takoj odpravljen) smatra kot notranja katastrofa.
- Vpelje se komandni center za incidente.
- Direktor IO seznani vladne institucije o sredstvih ustanove in javi izvršnemu pomočniku predsednika Zdravstvenega informacijskega sistema.
- Telefonisti vzdržujejo obsežen seznam klicnih številk za osebja v IO in višjih vodij. Direktorji pregledajo in popravijo seznam klicnih številk vsako četrtletje. Pregled tudi podrobno beležijo in si zapišejo vse posodobitve telefonskega sistema vsako četrtletje.

7. Problem se odpravi in sistem je znova vzpostavljen
   - Direktor IO zagotovi, da ima osebje v IO vsa razpoložljiva sredstva za raziskovanje problemov in odpravljanje napak. Med sredstva so vključeni tako zdravstveno osebje kot osebje pri podpori prodajalcev naprav.

8. Prekličejo se postopki ob izpadu
   - IO bo v sodelovanju z oddelki opravljal revizijo, da zagotovijo povsem delujoče sisteme, preden prekličejo postopke ob izpadu.
   - Direktor IO in inštitut vodijo urjenje na celotnem procesu vsako četrtletje. Rezultate poročajo Komiteju za varnost pacientov.
   - O preklicu postopkov ob izpadu, gredo kurirji v vsak oddelek in kontaktirajo z vodjo. Direktor IO in inštitut o tem podučijo vodstveno ekipo.

FMEA tabela

FMEA tabela je bolj ali manj grafično ponazorjena FMEA analiza v obliki tabele. V tabeli so zbrani vsi koraki procesa, načini odpovedi, njihovi vzroki in posledice ter določeni pogostost pojavitve (O), možnost zaznavanja (D), resnost (S) in RPN. Poleg to tudi dejanja za izboljšave ter novi pogostost pojavitve, možnost zaznavanja, resnost in RPN. Na koncu sta seštet in izboljšan RPN za ves proces.

Tabela je zaradi velikosti priložena na koncu tega dokumenta kot dodatek.

Sklep

Sodeč po FMEA analizi, se da iz tabele prebrati, da se je rizik celotnega procesa (RPN) iz vrednosti 138 znižal na 58, kar je **58 odstotno izboljšanje**. To izboljšanje je zdravstveni ustanovi uspelo doseči v dobrih petih mesecih, kar je odlično - spomnimo se, da je bil njihov cilj 50 odstotno izboljšanje v šestih mesecih.

Če gledamo iz šolskega računalniškega stališča, se v analizi lepo vidi, kako odgovorno, prepleteno in zahtevno je imeti računalniški sistem v ustanovi, kot je zdravstvena, kjer lahko v najslabšem primeru stradajo ljudje ali pa je škoda na opremi ogromna. Dejstvo ob vsem tem pa je, da se nismo niti s kančkom dotaknili same računalniške tehnologije, saj smo obravnavali le proces ob izpadu. Smo pa ob vsem tem naleteli na zanimive, vsaj meni, stvari, kot so postopki ob izpadu, ko osebje še vedno zmore in mora negovati paciente tudi, če računalniški sistem ne deluje, vloga telefonskega drevesa in notranje katastrofe in ne nazadnje vloge pomembnih ljudi, kot so vodje oddelkov, direktor informacijskega oddelka, nadzorniki, telefonist ter morda predsedniki komitejev in komisij.

Pri vsem tem pa kot nalašč pridejo prav zanesljivostne analize, ki jih v svetu uporabljajo najrazličnejši inženirji tudi pri tako "tragičnih" zadevah kot je delovanje jedrske elektrarne in ne nazadnje bolnišnice. To pa potrjuje njihovo **uporabnost**. A njihova vrednost je zares velika le, če so tudi zelo strokovno izvedene - v vsakem koraku.

Viri

[1] Failure Modes and Effects Analysis Tool. Institute for Healthcare Improvement, IHI.org. 13. april 2007. http://www.ihi.org/ihi/workspace/tools/fmea/

[2] Hospital Community. Unscheduled Computer System Downtime. View FMEA Tool. Institute for Healthcare Improvement, IHI.org. 26. april 2007. http://www.ihi.org/ihi/workspace/tools/fmea/ViewTool.aspx?ToolId=2760

[3] Failure Modes and Effects Analysis (FMEA). Institute for Healthcare Improvement, IHI.org. 20. julij 2004. http://www.ihi.org/NR/rdonlyres/A52A0CC3-8938-4BAA-A203-92EC34A75A87/972/FailureModesandEffectsAnalysis_FMEA_1.pdf

[4] Healthcare Failure Mode and Effect Analysis (HFMEA). National Center for Patient Safety. United States Department of Veterans Affairs. 28. februar 2007. http://www.patientsafety.gov/SafetyTopics.html#HFMEA

[5] The Basics of Healthcare Failure Mode and Effect Analysis. Videoconference Course. VA National Center for Patient Safety. 11. september 2006. http://www.patientsafety.gov/SafetyTopics/HFMEA/FMEA2.pdf

[6] Bretschneider, L. FMEA – Web Application Security. 2007. http://lrss.fri.uni-lj.si/sl/teaching/rzd/tutorials/bretschneider2007_FMEA.pdf

[7] Huber, B.; Mraz, M. FMEA - FMECA. Ljubljana. 2005. http://lrss.fri.uni-lj.si/sl/teaching/rzd/tutorials/huber2005_FMEA.pdf

[8] Schlueter, M. Can Any Body Help Me for FMEA? Forum. iSixSigma.com. 14. julij 2003. http://www.isixsigma.com/forum/showthread.asp?messageID=30127

[9] Curtis, S. FMEA Severity, Occurrence, and Detection Definitions. Forum. iSixSigma.com. 24. junij 2002. http://main.isixsigma.com/forum/showmessage.asp?messageID=15024

[10] How to Build a Phone Tree; Activate local activists easily by phone. American Association of University Women. 11. maj 2007. http://www.aauw.org/issue_advocacy/phonetree.cfm

[11] Flipchart: Internal Disaster. EHS Department. Boston University, Medical Campus. 5. julij 2001. http://www.bu.edu/ehsmc/flipchart/intdis.htm

[12] Administrative Procedure for Downtime Procedures. Nursing. UNC Health Care. Januar 2005. http://www.unchealthcare.org/site/Nursing/nurspractice/policies/policies/policyd3.pdf

Korak	Način odpovedi	Vzroki	Posledice	O	D	S	RPN	Dejanja	O	D	S	RPN
1 - Prijava izpada računalniškega sistema nadzorniku	Osebje izpada ne prijavi takoj nadzorniku	Osebje, ki zazna nepredvideno obnašanje sistema, tega ne prijavi takoj, ker ne razume, kako pomemben je izpad oz. koliko zajema	Vsaka sekunda, ko ni znano, kaj se dogaja, povzroči počasen oz. pozen prehod na postopke ob izpadu. To je potencialen vzrok za zamude pri kritičnem zdravljenju ali celo prekinitev stalne nege pacientov	2	1	3	6	Direktor IO pripravi temo razgovora za osebje o postopkih, ki sledijo ob izpadu sistema	1	1	3	3
2 - Nadzornik prijavi izpad računalniškega sistema informacijskemu oddelku	Nadzornik izpada ne prijavi takoj osebju IO	Nadzornik ne more prijaviti izpada takoj, ker telefonist ne more vzpostaviti povezave z osebjem v IO		1	1	3	3	Direktor IO z nadzorniki potrdi alternativni plan za takšne situacije	1	1	3	3
3 - Telefonist prikliče informacijski oddelek	Telefonist ne more vzpostaviti stika z osebjem v IO	Osebje v IO ni na voljo, ker je odsotno (npr. so na izobraževanju). Rezervno osebje je bolno		1	1	9	9	Nadzornik nemudoma razglasi uveljavitev postopkov ob izpadu Direktor IO poduči nadzornike in vodstvo Telefonisti vzdržujejo obsežen seznam klicnih številk za osebja v IO in višjih vodij. Direktorji pregledajo in popravijo seznam klicnih številk vsako četrtletje. Pregled tudi podrobno beležijo in si zapišejo vse posodobitve telefonskega sistema vsako četrtletje	1	1	9	9
		Še precej drugih potencialnih vzrokov, kot so izpad telefonskega omrežja, zunanje katastrofe itd.		1	1	9	9		1	1	9	9
4 - Osebje informacijskega oddelka ovrednoti problem	Osebje v IO ne more doseči sistema	Vse od izpada električnega omrežja, zunanje katastrofe ali sistemskih napak. Vse to je prek sposobnosti in izkušenj osebja v IO		1	1	3	3	Nadzornik nemudoma razglasi uveljavitev postopkov ob izpadu	1	1	3	3
	Osebje v IO ne more ugotoviti vzroka izpada v 30 minutah			5	1	3	15	Direktor IO poduči nadzornike in vodstvo	2	1	3	6
5 - Nadzornik razglasi uveljavitev "postopkov ob izpadu"	Nadzornik ne razglasi in skupaj z upravniki ne pričnejo postopkov ob izpadu	Ni možno najti postopkov ob izpadu. Stvari, ki se uporabljajo pri postopkih ob izpadu, niso pripravljene. Dodatno osebje za podporo pri postopkih ob izpadu ni na voljo		5	1	7	35	Direktor IO in inštitut pripravita izobraževanje za vodstveno ekipo o postopkih ob izpadu Direktorji in vodje izobražujejo zaposlene na sestankih Direktorji pregledajo postopke ob izpadu za morebitne izboljšave vsako četrtletje Inštitut in direktor IO organizirajo naključne revizije za povečanje natančnosti. Vsako četrtletje izvajajo revizijo zunanji izvajalci Uprava naredi načrt, kako pridobiti dodatno osebje, ko je potrebno. Uprava poduči nadzornike o tem načrtu	1	1	7	7

6 - Razglasi se "notranja katastrofa" in aktivira se primerno "telefonsko drevo"	Notranja katastrofa se ne razglasi	Pri odločanju, ali se naj razglasi notranja katastrofa, lahko preteče precej časa. Notranja katastrofa je zato razglašena z zamudo ali celo prepozno		1	1	3	3	Direktor IO poduči vodstvo, da se izpad sistema (ko je ugotovljeno od osebja v IO, da ne more biti takoj odpravljen) smatra kot notranja katastrofa Vpelje se komandni center za incidente Direktor IO seznani vladne institucije o sredstvih ustanove in javi izvršnemu pomočniku predsednika Zdravstvenega informacijskega sistema	1	1	3	3
	Nadzornik ne more doseči primernega osebja v IO po telefonskem drevesu	Telefonske številke telefonskega drevesa niso ažurirane		1	1	3	3	Telefonisti vzdržujejo obsežen seznam klicnih številk za osebja v IO in višjih vodij. Direktorji pregledajo in popravijo seznam klicnih številk vsako četrtletje. Pregled tudi podrobno beležijo in si zapišejo vse posodobitve telefonskega sistema vsako četrtletje	1	1	3	3
7 - Problem se odpravi in sistem je znova vzpostavljen	Problem izpada se ne razišče dovolj dobro ali sploh ne	Problem je lahko večjih razsežnosti: naravna katastrofa, izpad redundantnih sistemov, večja strojna napaka ali druge še neugotovljene okoliščine		3	1	7	21	Direktor IO zagotovi, da ima osebje v IO vsa razpoložljiva sredstva za raziskovanje problemov in odpravljanje napak. Med sredstva so vključeni tako zdravstveno osebje kot osebje pri podpori prodajalcev naprav	1	1	7	7
8 - Prekličejo se postopki ob izpadu	Postopki ob izpadu so bili preklicani, vendar celoten sistem še vedno ne deluje po pričakovanjih	Osebje v IO verjame, da je sistem ponovno vzpostavljen in delujoč, vendar sistem ne deluje pravilno oz. po predvidevanjih		3	3	3	27	IO bo v sodelovanju z oddelki opravljal revizijo, da zagotovijo povsem delujoče sisteme, preden prekličejo postopke ob izpadu Direktor IO in inštitut vodijo urjenje na celotnem procesu vsako četrtletje. Rezultate poročajo Komiteju za varnost pacientov	1	1	3	3
	Osebje ni dobilo sporočila o preklicu postopkov ob izpadu	Osebje izvaja postopke ob izpadu, čeprav sistem že deluje		2	1	2	4	O preklicu postopkov ob izpadu, gredo kurirji v vsak oddelek in kontaktirajo z vodjo. Direktor IO in inštitut o tem podučijo vodstveno ekipo	1	1	2	2
RPN skupaj							**138**						**58**