INTERNET PAMETINIH UREĐAJA

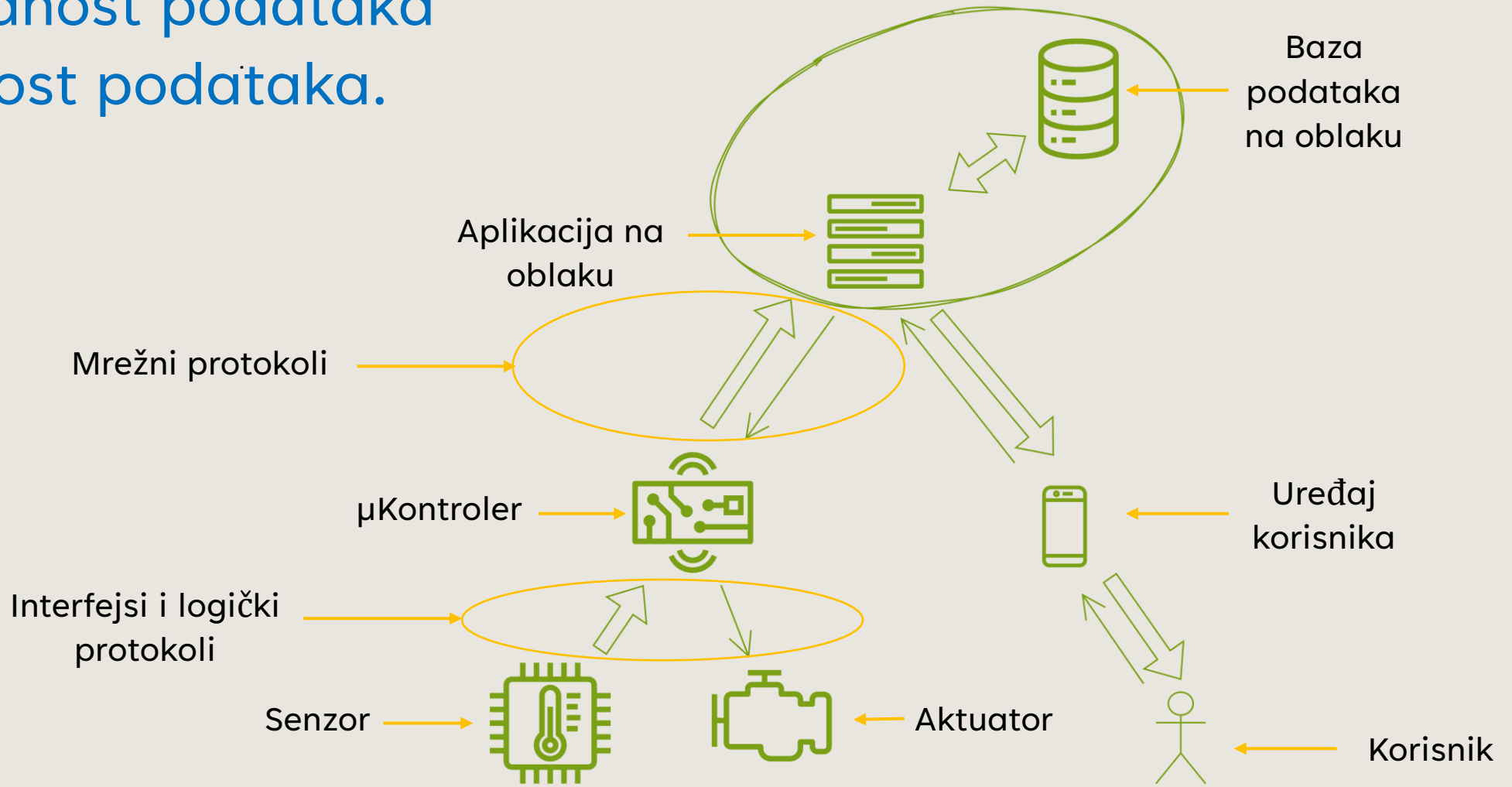
prof. dr Dejan S. Aleksić

Prirodno-matematički fakultet, Niš

07. SIGURNOST I BEZBEDNOST IOT

KLJUČNI ASPEKTI

- Pouzdanost podataka
- Sigurnost podataka.



KLASIFIKACIJA OTKAZA

Klasifikacija otkaza u sistemu

Otkaze u jednom IoT sistemu možemo klasifikovati:

- **Po mestu nastanka**
- **Po vrsti (hardverski ili softverski otkaz)**
- **Po tipu oporavka (moguć automatski oporavak, nije moguć automatski oporavak)**
- **Po ishodu (da li moguće premostiti otkaz kako bi sistem mogao ipak da funkcioniše ili je otkaz fatalan po funkcionisanje sistema)**

MESTO NASTANKA – SLOJ SENZORA.

- Sloj senzora cini mreža inteligentnih senzora zajedno sa linijama za njihovo povezivanje sa odgovarajućim IoT čvor.
- Otkaz na ovom nivou može da nastane na samom senzoru ili na komunikacionim linijama.
- Otkaze ove vrste možemo svrstati u hardverske otkaze kod kojih nije moguc automatski oporavak sto znaci da je nužno da se fizički izvrši njihova zamena sa ispravnim senzorom.
- Senzori povezani na IoT čvor imaju različit uticaj na pouzdanost sistema te ih možemo podeliti u dve grupe:
  - senzori čiji je otkaz fatalan po funkcionisanje sistema i
  - senzori čiji otkaz ne utiče značajno na pouzdanost sistema.

MESTO NASTANKA – SLOJ SENZORA.

- Kako bi se smanjio uticaj otkaza na pouzdanost sistema na najmanju moguću meru bilo je potrebno da se urade određene modifikacije kako u hardveru tako i u softveru.
- Intervencije u hardveru ogledaju se u udvajanju svih senzora i njihovih komunikacionih linija koji pripadaju prvoj grupi tj. čiji je otkaz fatalan za rad samog sistema.
- Ekonomski razlozi su uticali na odluku da se ne vrši udvajanje i senzora iz druge grupe.
- Ključne intervencije u softveru izvršene su kodu odgovarajućih IoT node taskova zaduženih za periodično očitavanje vrednosti senzora.
- U bazi podataka na cloud sistemu za svaki senzor postoji niz konfiguracionih podataka kao sto su njegova adresa, period očitavanja, granične (min i max) vrednosti, itd.
- Kopije ovih parametara nalaze se i u memoriji odgovarajućeg IoT noda na koji je povezan dati senzor.
- Otkazivanje senzora ili njegove komunikacione linije može se detektovati ili kao ne očitavanje bilo kakve vrednosti ili očitavanje vrednosti koja je izvan očekivanog opsega.

MESTO NASTANKA – SLOJ SENZORA.

- U slučaju otkaza senzora koji nije udvojen, IoT čvoru preostaje samo da generise alarm najvišeg nivoa i pošalje tu informaciju svom nadređenom edge računaru koji ovaj događaj prosleđuje do odgovarajućih komponenti sistema na cloudu.
- Kod udvojenih senzora stalno se vrsi očitavanje vrednosti sa oba senzora, upoređuju se očitane vrednosti sa njihovim graničnim vrednostima i ocenjuje se da li je došlo do otkaza nekog od ta dva senzora.
- U slučaju otkaza, njegova vrednost se odbacuje tj. usvaja se očitana vrednost sa ispravnog senzora a zatim se generise odgovarajući alarm i obaveštava se o tome nadređeni edge computer.
- Nakon otklanjanja uzroka otkaza (zamena senzora ili popravka komunikacione linije) sistem će automatski izvršiti proceduru oporavka tj. nisu potrebne nikakve intervencije u softveru na bilo kom layer-u.
- Na opisani način ostvarena zadovoljavajući nivo pouzdanosti sloja senzora sa ekonomski prihvatljivim posledicama.

MESTO NASTANKA – SLOJ SENZORA.

- Treba napomenuti da pouzdanost funkcionisanja sistema na ovom sloju nije 100% jer uvek postoji (mada vrlo mala) verovatnoća istovremenog otkaza oba udvojena senzora koji mere neku od kritičnih velicina.
- Naravno, sistem bi takav dogđaj automatski detektovao i generisao alarm najvišeg prioriteta u čitavom sistemu kako bi se sto pre otklonio uzrok otkaza.

MESTO NASTANKA – IOT ČVOR.

- Mogu se javiti dve vrste otkaza:
  - softverski otkazi
  - hardverski otkazi
- Softverski otkazi se odnose na softver u samom mikrokontroleru i pripadaju grupi otkaza koji se mogu automatski otkloniti.
- Mehanizmi za to su:
  - Interrupt Watchdog Timer (IWDT)
  - Task Watchdog Timer (TWDT).

MESTO NASTANKA – IOT ČVOR.

- Otkazi u hardveru odnose se na otkaz samog IoT noda tj. odgovarajućeg mikrokontrolera.
- Ovi otkazi spadaju u grupu hardverskih otkaza koji se mogu detektovati ali se ne mogu automatski otkloniti.
- Za njihovo otklanjanje potrebna je fizička zamena mikrokontrolera sto zahteva vreme i angažovanje stručnog osoblja.
- Da bi eliminisali negativan uticaj ove vrste otkaza na pouzdanost čitavog sistema vrsi se tkz. udvajanje IoT noda.
- Sada postoje dva IoT noda, jedan master i jedan slave.
- Oba IoT noda su povezana na komunikacione linije ka senzorima ali samo glavni IoT node vrši "prozivku" senzora.
- Slave IoT samo "sluša" saobraćaj komunikacionim linijama i prima podatke koje šalju senzori.

MESTO NASTANKA – IOT ČVOR.

- Dok radi u sniffer modu on ne šalje podatke ka nadređenom edge računaru.
- Sinhronizacija prelaska u hibernaciju.
- Onog trenutka kada izostane prozivka senzora od strane master IoT noda, slave IoT node vrđi prozivku master IoT noda preko posebne komunikacione linije i ako mu se master IoT node ne odazove on prelazi iz sniffer moda u master mode tj. preuzima u potpunosti ulogu master IoT noda.
- Naravno, u slučaju detekcije ovakvog otkaza IoT slave node generise i alarm visokog prioriteta ka ostatku sistema.
- Potrebno je naglasiti da se celokupna opisana procedura oporavka od ovakve vrste otkaza odvija potpuno automatski bez ikakve intervencije od strane operatera sistema.

MESTO NASTANKA –IOT NODE <-> EDGE COMPUTER

- komunikacija izmedju IoT noda i edge computera ostvaruje se preko LoRa protokola dok je kao logicki protokol upotrebljen MQTT protokol
- zbog ustede energije odlazak u hibernaciju moze da bude protumačen od strane MQTT servera kao otkaz - zato se i koristi SN-MQTT pod-verzija MQTT protokola.

- Ovde moze doci do tri vrste otkaza:

  - softverski otkaz taska koji se brine o LoRa komunikaciji
  - softverska otkaz taska kojim se realizuje SN-MQTT komunikacija
  - hardverski prekid bezzicne LoRa komunikacije
  - softverski otkaz SN-MQTT gateway-a na Edge computeru
  - hardverski otkaz samog Edge computera

MESTO NASTANKA –IOT NODE <-> EDGE COMPUTER

- Procedura oporavka od prve dve vrste otkaza već je obrađena na prethodnim slajdovima
- Poslednja dva će biti detaljno objasnjena u poglavlju pouzdanost Edge sloja.
- Dakle, ovde je paznja usmerena samo na prekid komunikacione linije izmedju IoT noda i Edge layer-a.
- Kod ove vrste otkaza nije moguc automatski oporavak ili ako se to i desi taj oporavak nije iniciran i kontrolisano izvršen od strane nekog elementa opisanog sistema.
- Moguc je privremeni i trajni prekid komunikacionog kanala izmedju IoT noda i edge Layer-a.
- Moze se desiti prekid bezžicne komunikacije na neko vreme usled neke spoljne smetnje i njeno ponovno uspostavljanje nakon nestanak uzroka prekida.
- Ovo ne moze biti kontrolisano od strane naseg sistema i ovakve vrste privremenih otkaza komunikacionih linija se tretiraju kao fatalan otkaz koji se ne može automatski otkloniti.

MESTO NASTANKA –IOT NODE <-> EDGE COMPUTER

- Bitno je naglasiti da nakon ponovnog upostavljanja prekinutog komunikacionog kanala, sistem ce automatski to prepoznati i ponovo poceti da isti koristi.
- Da bi eliminisali uticaj privremenog ili trajnog otkaza na komunikacionim linijama sistem automatski prelazi na rezervni komunikacioni kanal, u nasem slucaju koristi se GSM komunikacioni kanal.
- Zbog ovoga se ovakva vrsta otkaza može svrstati i u kategoriju otkaza sa automatskim oporavkom tj. ovakva vrsta otkaza, iako fatalna po svojoj prirodi, može se premostiti i time minimizirati njen uticaj na pouzdanost sistema.

MESTO NASTANKA –EDGE NIVO

- Otkaze na ovom nivou možemo grupisati u:
  - softverske otkaze
  - hardverske otkaze.
- Otkazi softverskih komponenti koje se izvrsavju na Edge computeru mozemo tretirati kao otkaze kod kojih je moguc automatski oporavak pa samim tim se eliminise i njihov fatalni uticaj na pozudanost sistema.
- Mehanizmi za eliminisanje softverskih otkaza na ovom sloju su primena Docker i Kubernetes tehnologije.

MESTO NASTANKA –EDGE NIVO

- U grupu hardverskih otkaza na ovom sloju spadaju:
  - otkaz LoRa modula
  - otkaz GSM modula
  - otkaz samog edgde computera
- U slucaju otkaz jednog od dva modula za komunikaciju sistem automatski prebacuje komunikaciju na drugi ispravan komunikacioni modul.
- Dakle, ova vrsta otkaza moze se svrstati u grupu otkaza koji se mogu automatski zaobici cime se i eliminise njihov uticaj na pouzdanost sistema.
- U slucaj otkaza samog edge computera situacija je mnogo ozbiljnija.
- Ovakav otkaz spada u grupu hardverskih otkaza bez mogucnosti automatskog oporavka koji su fatalni za funkcionisanje sistema.
- Eliminacija uticaja ove vrste otkaza na pouzdanost sistema realizuje se preko Kubernetes-a tako sto postoji jos jedan edge computer na kom će kubernetes uslucaju otkaza glavnog edge computera da "podigne" kopije svih softverskih komponenti kroz doker-e.

MESTO NASTANKA –EDGE NIVO

- Taj dodatni edge computer moze da bude computer namenjen samo za to a moze da bude i "susedni" edge computer koji ce, pored svojih redovnih funkcija, privremeno da preuzme sve funkcije edge computera kod koga je nastao otkaz.
- Pitanje: kako ce IoT nodovi znati da pocnu komunikaciju sa rezervnim tj. "susednim" edge računarom?
- Jedno od rešenja je da u svojoj konfiguraciji svaki IoT node ima i adresu rezervnog tj. "susednog" edge racunara pa kad ne moze da uspositavi komunikaciju niti sa LoRa niti sa GSM komunikacionim kanalom onda on zakljucuje da se desio fatalni otkaz glavnog edge computera i prebacuje komunikaciju na rezervni edge racunar.
- Bitno je da on stalno proverava dostupnost glavnog racunara na LoRa komunikacionom kanalu i ako se glavni edge racunar javi, verovatno nakon oporavka, on vraca nazad komunikaciju na glavni racunar.

- Procedura oporavka od otkaza ide Top Down Recovery algoritmom. Kubernetes sa cloud-a "nadizre" rad racunara na edge Layer-u i pokrece proceduru oporavka tj. pokrece nove instance sotverskih komponeti na nekom "susednom" edge computeru

MESTO NASTANKA –EDGE NIVO

- Procedura oporavka od otkaza ide Top Down Recovery algoritmom.
- Kubernetes sa cloud-a "nadizre" rad racunara na edge Layer-u i pokrece proceduru oporavka tj. pokrece nove instance sotverskih komponeti na nekom "susednom" edge computeru koji ispravno radi.
- Sa druge strane IoT nodovi se sami oporavljaju.

MESTO NASTANKA –CLOUD NIVO

- Cloud layer se generalno sastoji iz dva sublayer-a:
  - sloj aplikacije i
  - Sloj baze podataka.
- Kompletna funkcionalnost sloja aplikacije bazirana je na mikroservis arhitekturi i docker kontejnerima.