



METODE OPTIMIZACIJE SERVISA ZA UPRAVLJANJE ALARMIMA U PROCESNOJ INDUSTRIJI

OPTIMIZATION METHODS OF ALARM MANAGEMENT SERVICE IN THE PROCESS INDUSTRY

Aleksandar Duduković, *Fakultet tehničkih nauka, Novi Sad*

Oblast – ELEKTROTEHNIKA I RAČUNARSTVO

Kratka sadržaj – U radu je prezentovana ideja pametne alarmne supresije u elektroenergetskom sistemu kao i način primene veštačke inteligencije kao podrške operateru tokom ispada mreže

Ključne reči: Pametno alarmiranje, Alarmna supresija, Procesna industrija, Mašinsko učenje, Veštačka inteligencija

Abstract – The document presents the idea of smart alarm suppression in the electric power system as well as the method of applying artificial intelligence to support the operator during the failure of the network.

Keywords: Smart alarming, Alarm suppression, Process industry, Machine learning, Artificial intelligence.

1. UVOD

Rad će se bazirati na alarmiranju u procesnoj industriji, tačnije u elektroindustriji. Osvrnuće se i na sam posao operatera u elektrodistributivnoj SCADA (Supervisory Control and Data Acquisition) stanici koji nadgleda električnu mrežu i kako da se taj rad i olakša. Rad će takođe predstaviti primenu veštačke inteligencije u procesnoj industriji sa osvrtom na automatizaciju upravljanja prilikom ispada mreže iz normalnog radnog stanja.

Alarmi i sami alarmni sistemi su neophodni u svakom procesnom postrojenju kako bi se sprečio otkaz uređaja koji bi kasnije mogao kulminirati havarijom. Kako je tehnologija napredovala tako su i uređaji postali „pametniji“ i složeniji, dobili su više funkcionalnosti, fleksibilniji su, spram toga je i teže upravljati njima. Najveći prioritet što se tiče bezbednosti (eng. *safety*) u industriji je sačuvati ljudski život i prirodu, sprečiti ekološku katastrofu i oštećivanje kritičnih infrastrukture.

Havarija nije jedini razlog zašto se alarmi implementiraju u procesnim industrijama, iako predstavlja najprioritetniji, nego i da produži rok trajanja samom uređaju jer će se boljim uvidom u njegovo stanje optimizovanije rukovati samim uređajem pa i celokupnim sistemom. Oprema koja se koristi u elektroindustriji je veoma skupa, a nekad je i unikatno pravljena samo za projektovanu mrežu, tako da je optimalno upravljanje skupocenim uređajima veoma bitno.

NAPOMENA:

Ovaj rad proistekao je iz master rada čiji mentor je bio dr Darko Čapko, vanr. prof.

2. ANALIZA PROBLEMA

Da bi se objasnili problemi koji nastaju usled neadekvatno postavljenog alarmnog sistema i načini na koje ove probleme rešiti mora se prvo definisati šta je to alarm i alarmno stanje.

Po ISA-18.2 standardu [1] alarm je: zvučni i/ili vizuelni indikator operateru da postoji neispravnost u opremi, devijacije u procesima ili da su se pojavili abnormalni uslovi koji zahtevaju blagovremeni odgovor operatera.

Problemi se mogu javiti kada postoji premalo ili previše alarma. Kada postoji premalo alarma, operater nema pravi uvid u sistem koji nadgleda, a kada ih ima previše, dešava se pojava koja se naziva “alarm flood” (alarmna poplava) i tada je operater sprečen da odreaguje blagovremeno na trenutnu situaciju jer je vreme između prijave dva alarma veoma kratko. Realan problem loše postavke alarmnog sistema može se videti u eksploziji “Texaco” rafinerije (Milford Haven) 24. jula 1994. godine [2].

Dva operatera koja su radila na nadziranju sistema dobili su, pre same havarije, 275 različitih alarma u 11 minuta. EEMUA (Engineering Equipment and Materials Users Association) [3] je u svom dokumentu EEMUA 191 propisala *de facto* standard za broj alarma koji je prihvatljiv da se dogodi u sistemu za određen vremenski interval da bi operater mogao da ih isprocesuiru, a to je jedan alarm na svakih 10 minuta.

Iz njihovih podataka mogu se izvući zaključci da operateri u Texaco rafineriji nisu mogli brže i bolje da reaguju na toliko alarmnih događaja i da prepoznaju koji alarm je posledica, a koji je uzrok drugog alarma. Ranija mišljenja eksperata i ljudi u vladi bila je da je greška uvek u operaterima, tj. da je havarija posledica ljudskih grešaka, ali je EEMUA 191 jasno stavila do znanja da ako alarmna komponenta nije uspela da redukuje učestanost prijave alarma onda se operater ne može okriviti zato što je propustio važan alarm. Zbog toga je alarmna supresija veoma bitan faktor u alarmnoj komponenti, isto koliko i samo definisanje alarma.

3. METODE SUPRESIJE

Tipovi supresije koji mogu biti implementirani radi optimizacije alarmnog servisa su:

- Dinamička prioritizacija alarmnih stanja po njihovoj važnosti (eng. *importance*),
- *Out of service* supresija,

- Objedinjavanje različitih tipova alarma kreiranjem topoloških ostrva,
- Obeležavanje alarma po njihovom uzroku nastanka/posledica (eng. *root cause*),
- Ručna, kroz HMI (Human Machine Interface) i
- Supresija nivelacionih alarma.

Dinamička prioritizacija alarma omogućava da alarm koji već postoji u sistemu promeni njegovu važnost i ozbiljnost (eng. *importance and severity*) usled uticaja drugih akcija u sistemu koji direktno ili indirektno utiču na element i/ili povezane elemente na kojim se nalazi alarm. Kombinovanjem ove i metode koja objedinjuje alarme po uzroku nastanka/posledica najbolje se može pokazati na primeru kompresora u OGS industriji (Oil and Gas System). Kompresori imaju mnogo delova u sebi koji mogu da rezultuju alarmom i da ukažu na neke abnormalne uslove koji se dešavaju u njemu kao na primer nizak pritisak ulja, nizak pritisak usisavanja, temperatura ležaja itd.

Operater ne treba da vidi sve alarme u slučaju da kompresor počne da otkazuje i da na kraju prekine svoj rad kompletno. Ono što je tada bitno operateru je da ima alarm koji govori da je kompresor „ispao“ iz mreže bez pojedinačnih alarma elemenata koji se nalaze u kompresoru [4]. Ovim ne samo da se odradila supresija *root cause* metodom već alarmni servis može da promeni ozbiljnost (eng. *severity*) alarma i da je poveća, ukoliko ispad kompresora ugrožava postrojenje i ljude.

Out of service supresija bi trebala da postoji u svakom softveru koji nadgleda procesne sisteme. Kada se planira popravak jednog uređaja ili jednog dela sistema operater je skoro uvek obavešten o tome. Postavljanjem odgovarajućeg tag-a u softveru na uređaj ili deo sistema *Out of service* supresija može biti uključena. Tada operater, a i softver znaju da je uređaj odnešen na remont stoga alarmi za taj element operateru ne predstavljaju nikakvu novu informaciju i samo se gomilaju u listi alarma što otežava rad operatera.

Postoje događaji u sistemu koji nisu čisto alarmno stanje vezani za merenje, ali operateru itekako daju informacije sa terena. Jedan tip takvih događaja je i incident, koji pripada OMS-u (Outage Management System) i predstavlja planirane popravke, neplanirane i planirane ispade u sistemu i omogućava operaterima bolji pregled stanja na terenu i omogućava slanje ekipa za popravke (eng. *working crews*). Objedinjavanje više odvojenih sistema (SCADA i OMS u ovom slučaju) je moguće preko logičkog kreiranja topološko deenergizovanih ostrva kao elemenata u sistemu.

U elektroenergetskoj mreži ispadanjem jednog prekidača dobija se niz pojedinačnih alarma na elementima nizvodno od “problematičnog” prekidača ukazivajući na nedostatak napona, i tako se gomilaju isti alarmi u aktivnoj alarmnoj listi. Ako se uvede pojam topološko deenergizovanog ostrva, tada “problematični” prekidač usled ispada postaje koren novog stabla koje je deenergizovano. Pre prijave incidenta na sam prekidač kao izolovan objekat, treba se proveriti da li je taj element pripadnik nekog deenergizovanog ostrva, i ako jeste treba

naći njegov koren i tu napraviti uniju svih incidenata i alarma i označiti ga kao “Problem”. Problem bi tada bio kompleksan događaj koji u sebi sadrži više događaja, ali bi predstavljao čvorište svih problema koji su posledica ispada tog elementa i tako bi operater imao sažetiji pregled sistema. Logičkim dodavanjem topološkog deenergizovanog ostrva koje ne postoji kao fizički element u mreži, dobija se mogućnost klasterizacije pojava na pojedinačnim elementima u ostrvu.

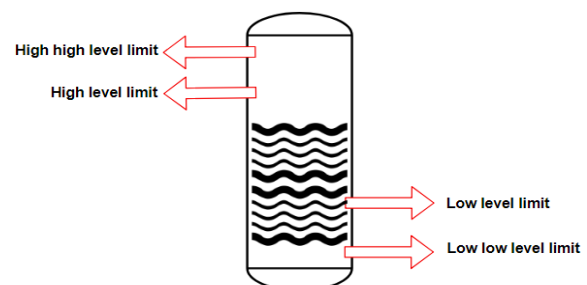
Ručan vid supresije je takođe bitan faktor u softveru koji omogućava operateru da definiše svoja pravila po kojima će se supresija dešavati. Kriterijumi u ovom vidu supresije mogu biti razni i zavise isključivo od sposobnosti operatera da primeni odgovarajuće filtere u datom trenutku.

U toku „alarmne poplave“ operater može da izabere da mu prvo stižu alarmi sa većim prioritetom, da vidi prvo alarme od prioritetnijih potrošača itd. Ovakav pristup bi se mogao i automatizovati ako je softver u stanju da prepozna kada je došlo do navale alarma, što može da se postigne merenjem učestanosti prijave alarma.

Da bi se smanjio broj nepotrebnih alarma bitno je da softver ima supresiju alarma koji su vezani za alarmna ograničenja na pojedinim senzorima/tačkama. U raznim OGS, vodovodnim, petrohemijskim industrijama postoje rezervoari koji rade sa tečnim sirovinama i u njih je zbog bezbednosti ugrađeno više bezbednosnih senzora za merenje nivoa tečnosti (Slika 1).

Ako se desi scenario gde će se nivo tečnosti kontinualno podizati jer se pumpa za punjenje zaglavila, prvo će se generisati High level limit alarm da upozori operatera na visok nivo tečnosti u rezervoaru. Ako se pumpa ne zatvori u neko predefinisano vreme, tečnost će nastaviti da raste i aktivirati *High high level limit* (Slika 1) da upozori na sada već kritičan nivo u rezervoaru i mogućnost izlivanja tečnosti u postrojenje.

U ovakvom scenariju operater ima dva aktivna alarma od kojih je jedan zastareo i podrazumevan jer postoji isti alarm većeg prioriteta koji nosi informaciju o dostizanju većeg alarmnog nivoa. U ovakvim situacijama mora se odraditi rekalkulacija alarma i skloniti podrazumevani alarmi da se slični njima ne bi gomilali u listi aktivnih alarma. U elektroindustriji je ovaj vid supresija takođe mnogo bitan jer tamo mogu biti definisani i po više od četiri alarmna nivoa za jedno merenje.

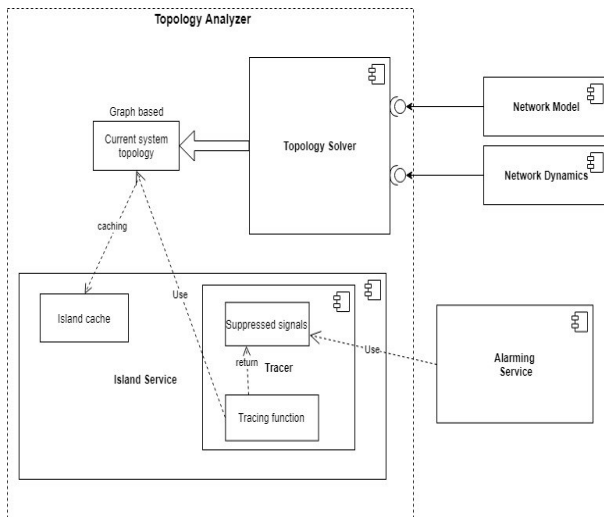


Slika 1 – Rezervoar sa definisanim alarmnim limitima

Softver sa automatskom supresijom ne bi smeo da sakrije supresovana alarmna stanja već treba da omogući operateru uvid u takve alarme ali tako da ta lista i/ili graficki prikaz ne bude u prvom planu.

4. ARHITEKTURA REŠENJA

Struktura rešenja prikazana je na slici (Slika 2).



Slika 2 – Arhitektura rešenja

Osnovne komponente od značaja za supresiju su:

1. Topology solver
2. Island service
3. Tracer
4. Alarming service

Topology solver komponenta prima statičke i dinamičke podatke o entitetima u mreži i na osnovu konektivnosti pravi graf o aktuelnom uklopnom stanju mreže. *Island service* koristi aktuelno stanje mreže i kešira podatke o deenergizovanim ostrvima pomoću *Tracer* komponente koja aktivira *Tracing* funkciju i popunjava ili pristupa *Island* keš podacima, koja potom pristupa svim deenergizovanim entitetima u ostrvu i kupi njihove signale, kao i signale opreme koja se nalazi u entitetima (npr. zaštitna oprema na prekidačima, rastavljačima, osiguračima itd.). Ti signali se šalju na *Alarming service* gde će posle biti supresovani.

5. PRIMENA VEŠTAČKIH NEURONSKIH MREŽA U PROCESNOJ INDUSTRIJI

Predstaviće se idejno rešenje i arhitektura restauracije mreže prilikom ispada korišćenjem neuronskih mreža. U ovom radu će se analizirati mogućnost primene *OpenAI Five* algoritma [5] koji je implementiran u video igri Dota 2.

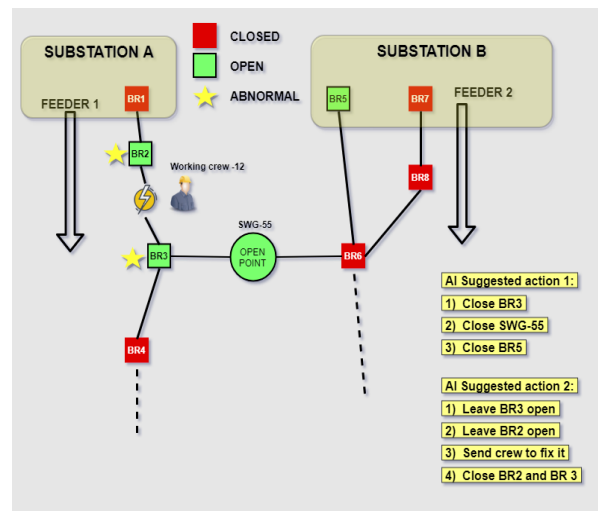
Krajnji, ultimativni cilj koji algoritam treba da održi, odnosno da ispuni je prazna lista alarma. Kada nema nijednog alarma to znači da je sistem, u ovom slučaju mreža, u normalnom radnom stanju. Supresijom je pokušano da se što manje nebitnih alarma pojavi u aktivnoj listi alarma ostavljajući samo one najprioritetnije. Ovo pomaže neuronskim mrežama da rade sa najprioritetnijim alarmima dajući im preciznije informacije o mestu i uzroku grešaka. Zatim treba definisati agente (igrače) koji treba da izvršavaju akcije u sistemu.

Ova stavka može da se mapira na više entiteta u mreži, a neki od primera su:

- Svaki glavni izvod je jedan agent,

- Svaka podstanica je jedan agent,
- Svaki region je jedan agent.

Ovo je moguće samo iz razloga što se pokazalo da agenti u *OpenAI Five*-u znaju da saraduju međusobno ka ispunjenju dugoročnog cilja. Ako se uzme slučaj da je svaka podstanica jedan agent u sistemu, tada bi svakoj podstanici dodelili upravljanje određenim brojem izvoda koji izlaze iz te podstanice. Kratkoročni cilj svake podstanice je da održava svaki izvod živim, odnosno energizovanim. Algoritam bi trebao da nauči, kao i heroji u Dota 2, da žrtvuju svoje akcije zarad konačnog cilja. Primer toga je ako se definišu neki izvodi kao pomoćni u podstanici i puštanjem u rad tih izvoda bi svakoj podstanici proizvodilo penale od sistema. Ali ako susedna podstanica prepozna da ima problem sa energizacijom jednog dela svog izvoda tada algoritam treba da prepozna da ako energizuje izvod prve podstanice i zatvori prekidače (koje inače ne bi smeo) tada bi se penali od sistema kompenzovali time što je glavni cilj algoritma ispunjen, tj. nema alarmnih stanja u aktivnoj listi alarma (Slika 3). Tada bi ta akcija dobila manje penale i ostala bi zapamćena kao jedan od koraka koji su proizveli kasnije dobitke.



Slika 3 – AI preporuke za reenergizaciju mreže

Slika 3 prikazuje jedan od načina kako bi AI (Artificial Intelligence) mogao da asistira operateru da što brže vrati mrežu u normalno stanje. Slika 3 prikazuje dva izvoda (FEEDER 1 i FEEDER2) koji pripadaju različitim podstanicama, A i B. Oba izvoda su energizovana pod normalnim uslovima rada, a prekidač BR5 je otvoren i on predstavlja pomoćni izvod podstanice B. Dešava se ispad na izvodu "FEEDER 1" između prekidača BR2 i BR3, prekidačka oprema se otvara i nizvodno od prekidača BR3 izvod je deenergizovan. Podstanica A javlja ostalim podstanicama da joj je potrebna pomoć jer ne može sama da energizuje izvod. Podstanica B prepoznaje da može da pomogne. Akcije koje algoritam može da izvrši mogu da budu samo preporuka operateru ako u softveru ne postoje kontrolne sekvence, ako postoje onda bi algoritam mogao i sam da izvrši korake koje je definisao u preporuci sa tim da bi izabrao povoljniju akciju.

Prva akcija bi se primenjivala ako se na prvom izvodu nalazi priključena bolnica jer je tada bitno odmah reenergizovati izvod u što kraćem roku. Prva akcija

