UNIVERZITET CRNE GORE
ELEKTROTEHNIČKI FAKULTET

Igor Miljanić

SIGURNOSNE MJERE ZAŠTITE SADRŽAJA U SISTEMIMA PRENOSA TV SIGNALA U CRNOJ GORI

MAGISTARSKI RAD

Podgorica, 2018.

PODACI I INFORMACIJE O MAGISTRANTU

Ime i prezime	Igor Miljanić
Datum i mjesto rođenja	03.02.1981. godine, Podgorica
Naziv završenog osnovnog studijskog programa i godina diplomiranja	Elektrotehnički fakultet, smjer Primijenjeno računarstvo, 2005

INFORMACIJE O MAGISTARSKOM RADU

Naziv postdiplomskog studija	Studije Primijenjenog računarstva
Naslov rada	Sigurnosne mjere zaštite sadržaja u sistemima prenosa TV signala u Crnoj Gori
Fakultet na kome je rad odbranjen	Elektrotehnički fakultet, Podgorica

UDK, OCJENA I ODBRANA MAGISTARSKOG RADA

Datum prijave magistarskog rada:	10. 10. 2017
Datum sjednice Vijeća Univerzitetske jedinice na kojoj je prihvaćena tema:	23. 01. 2018
Komisija za ocjenu teme i podobnosti magistranta:	Prof. dr Vladan Vujičić, prof. dr Božo Krstajić, doc. dr Enis Kočan
Mentor:	Prof. dr Božo Krstajić
Komisija za ocjenu rada:	Prof. dr Vladan Vujičić, prof. dr Božo Krstajić, doc. dr Enis Kočan
Komisija za odbranu rada:	Prof. dr Vladan Vujičić, prof. dr Božo Krstajić, doc. dr Enis Kočan
Datum odbrane:	04. 04. 2018
Datum promocije:	

Sažetak:

Novi standardi za prenos multimedijalnog sadržaja doveli su do naglog razvijanja telekomunikacionih medija namijenjenih informativnom sadržaju. Većina takvih sistema prolazi dug put od momenta nastanka do perioda same realizacije i implementacije, što dovodi do situacija da se određeni sistemi, iako nikad realizovani, iskoriste za unapređivanje postojećih sistema. U ovom radu izvršena je analilza postojećeg sistema digitalne televizije TVCG, kao i analiza sigurnosnih zaštita digitalnih sistema za prenos multimedijalnog sadržaja.

Tokom analiziranja ovih sistema izvršen je detaljan pregled trenutno implementiranog sistema za prenos digitalnog signala u TVCG. Takođe, sagledan je svaki digitalni segment pojedinačno, ali je izvršena i analiza zaštite sistema. Izvršeno je poređenje novih tehnologija poput IP televizije analizirajući dalji razvoj digitalne televizije.

Komparativnim metodama analize postojećeg stanja digitalne televizije, kao i poređenjem sa aktuelnim tehnologijama iz ove oblasti dolazi se do rezultata koji mogu dovesti do implementiranja boljih mjera zaštite tokom prelaska na novi sistem digitalne televizije.

Kroz istraživanje i poređenje trenutnog sistema digitalne televizije TVCG sa ostalim sistemima potvrđena je potreba uvođenja novog tipa digitalne televizije prvenstveno baziranog na IP tehnologiji, zbog aspekta veće sigurnosti i mogućnosti konstatnog razvoja putem hardverske i sotverske implementacije.

Ključne riječi: digitalna televizija, IP televizija, analiza sistema, zaštita sistema, enkripcija signala.

Abstract:

Evolution of new standards for multimedia transmition made huge influence over news content and it's systems. Realization of most of those systems take much time, which leads to situations where systems, although never realized, found their way as a modules or upgrades for popular systems that are already in use. This work will analyze digital broadcasting system of TVCG and security systems for digital multimedia transmission.

Detailed analysis of currently implemented system for digital transmission in TVCG is available in this work, with each segment analyzed individually with a look at security measurements of overall system. Also, comparison between new technologies like IP TV and current system is analyzed.

Comparing those technologies, as well as comparing other available options for security and multimedia broadcast, lead to results which can be helpful when designing or implementing new systems for digital and multimedia broadcast.

Researching and evaluating results concludes that new digital broadcast system for TVCG has to be implemented, with strong tendencies to IP systems which provide better security and better implementation of hardware and software based solutions.

Key words: digital television, IP television, system analysis, signal encryption.

S A D R Ž A J:

1. UVOD

Tokom gotovo osam decenija postojanja, televizija predstavlja osnovni vid pružanja informacija, uselivši se u ogroman broj domova i istiskujući radio kao primarni vid informisanja. Međutim, i pored ogromne popularnosti televizije kao medijuma za prenos informacija, razvoj tehnologije omogućio je nove vidove pružanja informacija.

Internet kao jedan od glavnih medijuma prenosa informacija današnjice polako istiskuje televiziju kao primarnog informativnog medijuma sa trona. Logičan zaključak je, a i istorija je tako pokazala, da kada neki standard postigne veliki uspjeh i bude opšte prihvaćen od strane krajnjih korisnika, na toj poziciji ostaje dok se ne pronađe neko bolje rješenje. Većina korisnika nije sklona lakom prihvatanju bilo kakvih promjena, čak i ako te promjene unaprijeđuju bivše mehanizme rada. Internet je već prisutan nekih dvadeset godina i logičan je zaključak da ako televizija planira da ostane u vrhu informativnog trona mora prihvatiti nove standarde, i pružiti nove usluge kako bi zadržala postojeće korisnike. Televizija je prešla dugačak put od medija koji je služio za prikazivanje slika u boji, do popularizacije zabavnog sadržaja, ali taj napredak ne može trajati zauvijek. Nove tehnologije određuju nove standarde a novi standardi određuju nove tehnologije. Digitalna televizija treba da predstavlja hibrid između analogne televizije i Interneta, omogućavajući pristup informacijama na što brži i pristupačniji način, čuvajući onaj zabavni aspekt koji je televizija tokom decenija gradila.

Digitalna televizija predstavlja jedan od najvećih informativno-tehnoloških skokova još od pojave televizije sa slikom u boji. Jednostavno rečeno, digitalna televizija predstavlja budućnost. Da bi shvatili način funkcionisanja digitalnog televizijskog sistema, potrebno je analizirati sve njegove cjeline. Današnji operateri digitalnih televizija nude mogućnost prikazivanja programa po želji. Za krajnjeg korisnika bitan je isključivo kvalitet i sadržaj programa, dok sam tehnički aspekt vezan za digitalnu televiziju nije puno bitan. Ipak, kvalitet digitalnog signala vezan je za sam sistem, a srž samog digitalnog sistema za prenos čini skup raznih međusobno povezanih komponenti. U okviru televizije Crne Gore digitalni sistem podijeljen je na više segmenata, pri čemu svaki segment ima svoju značajnu ulogu

i kao takav predstavlja zasebnu cjelinu koju je potrebno nadgledati i eventulano zaštititi, u softverskom ili hardverskom smislu. Postojeći digitalni sistem u televiziji Crne Gore ne prati poslednje inovacije na polju digitalne televizije već predstavlja tranzicioni sistem zadužen za navikavanje prelaska iz analognog u digitalni domen. Predmet ovog rada jeste istraživanje primjena mjera sigurnosne zaštite sadržaja nad realnim sistemom prenosa televizije TVCG, kao i osvrt na trenutno implementirane segmente zaštite samog digitalnog sistema. Cilj istraživanja i analize digitalnog sistema u televiziji Crne Gore jeste davanje na važnosti i neophodnosti zaštite računarskih sistema.

2. DIGITALNA TELEVIZIJA

Televizija, nekada najpopularniji medijum za prenos informacija, emitovanje i primanje pokretnih slika i zvuka sa velikih daljina, predstavlja elektronski sistem pomoću koga optičku sliku i zvuk pretvaramo u električne signale, koji se prenošenjem do prijemnika pretvaraju u sliku i zvuk.

Prva javna upotreba riječi televizija datira iz 1900. godine, na međunarodnom kongresu u Parizu, pomenuta kroz članak 'Električna Televizija' tadašnjeg profesora elektronike Constantin Perskog. Prvi komercijalni TV prijemnik, predstavljen na Svjetskom sajmu 1939. godine polako je tokom idućih godina uspio da istisne radio prijemnike kao primarni izvor informacija. Iako su TV prijemnici bili monohromatski, prava revolucija je tek nastala 50-tih godina razvojem i pojavom televizije u boji. Razvoj tranzistora i integralnih kola 70-tih godina prošlog vijeka omogućuo je pretvaranje analognog u digitalni signal, sa ciljem poboljšanja kvaliteta TV prijema, čime se počinju javljati prve ideje o digitalnoj televiziji.

Iako je televizija sistem koji sadrži i zvuk i sliku, prenos analognog TV signala obavlja se identično kao i prenos radio signala - elektromagnetnim talasima. Kasnije pojavile su se varijante prenošenja signala kablovskom vezom što je u odnosu na prenos vazdušnim putem donijelo određene prednosti (poput kvaliteta slike), što će se kasnije i iskoristiti za razvoj digitalne televizije. Sam razvoj kablovskog prenosa i smanjenje njegove cijene tokom godina donosi sve pouzdaniji prenos uz sve viši kvalitet.

Ako posmatramo direktni prenos, na prijemnim uređajima audio i video signali se sinhronizuju i pretvaraju u elektronske signale u televizijskoj stanici. Ako uporedimo početni kablovski prenos televizijskog signala vazdušnom vezom vidi se da prenos kablovskom vezom nije mogao da dostigne efikasnost brzine prenosa signala vazdušnim putem.

Ukoliko posmatramo funkcionisanje analognog sistema prenosa možemo uvidjeti četiri faze:

• Pretvaranje optičke slike i zvuka u električne signale
• Kontrola, podešavanje i odabir signala
• Prenos signala do prijemnika
• Pretvaranje signala u optičku sliku i zvuk

Već je pomenuto da analogna televizija funkcioniše slanjem elektromagnetnih talasa u etar, što znači da je za razliku od radijskog signala gdje je potreban samo jedan signal radi prenosa zvuka, kod televizijskog signala potrebno poslati veliki broj električnih signala za prenos slike (jer ljudsko oko jednu sekundu statične slike registruje kao 25 pokretnih podslika). Da bi se ovo ostvarilo, televizijski prenos, odnosno predajnici iskoristili su istraživanja iz oblasti elektromagnetnih talasa. Električar Uilbi Smit je 1783. godine praktično dokazao da je selen kao gas fotoelektričan i da uz različite jačine struje daje i različite vrijednosti svjetlosti. Kao oca televizije možemo smatrati Paula Nipkova (nem. Paul Julius Gottlieb Nipkow), koji je 1884. godine napravio mehanički razlagač slike. Njegov pronalazak predstavlja spiralnu ploču koja se vrti ispred statične slike. Svjetlosna vrijednost svake tačke prenosi se na ćeliju selena i time stvara pulsirajuću jednosmernu struju, koja na strani prijemnika rotira ploču i tok struje pretvara u svjetlosnu vrijednost. Ovo se može smatrati začetkom televizije.

Ako posmatramo starije televizijske prijemnike najveći dio zauzimala je katodna cijev, koja se nastavljala na televizijski ekran. Početna slika prikazivana je u formatu 4:3, da bi tokom 90-tih godina prošlog vijeka primat televizijskog formata preuzeli formati 16:9. U zavisnosti od veličine ekrana postojali su TV prijemnici različitih dimenzija koji su se razlikovali po dužini, odnosno po dijagonali (37, 51, 56, 66, 69cm...). Sam ekran prijemnika bio je obložen najčešće fosforom, koji pod dejstvom mlaza elektrona prikazuje sliku. Kod televizije u boji princip finkcionisanja zasniva se na registraciji, prenosu i rekonstrukciji tri slike (crvena, zelena i plava , odnosno RGB).

Do pojave satelitske, kablovske i internet televizije, jedini način da se TV signal prenese bio je putem zemaljskih predajnika. Iako je ovaj vid emitovanja najstariji, njegova digitalizacija je počela najkasnije. Za razliku od analogne, digitalna televizija predstavlja veliko unapređenje u svim aspektima. Primljeni digitalni signal je identičan izvornom.

2.1. Istorijski razvoj slike i televizije

U zavisnosti od načina na koji se iz slike u boji dobija monohromatska, kao i nekih drugih tehničkih karakteristika, razvijeno je više nekompatibilnih standarda, kao što su NTSC, PAL i SECAM.

Prvi redovni televizijski program započeo je sa emitovanjem 1936. godine. Drugi svjetski rat stopirao je razvoj televizije, bar onog komercijalnog dijela. Međutim, nakon završetka rata, razvoj televizije je nastavljen, prije svega zahvaljujući tehnikama za prenos signala razvijenim u vojne svrhe. Značajnu prekretnicu predstavlja 1954. godina kada u SAD počinje emitovanje programa televizije u boji. Iako je postojao opravdani strah od nekompatabilnosti između dva različita načina prikazivanja, ta nekompatibilnost između monohromatskih i kolor televizora prevaziđena je tako što su monohromatski televizori mogli da iskoriste televizijski signal u boji na način što su koristili samo jednu komponentu slike (luma), dok su informacije o boji sadržane u ostalim komponentama odbacivali. Iako digitalna televizija uzima sve veći mah čak i na područjima Balkana, većina svijeta i dalje koristi analogne TV prijemnike. Već smo spomenuli neke od različitih vidova formata za prikaz slike:

NTSC - (*engl. National Television System Comittee*) razvijen je 1950. godine kao početni, prvi televizijski standard. Njegov prenos sadrži 30 slika (odnosno 60 poluslika) u sekundi koje imaju po 525 linija. Frekvencija osvježavanja slike (refresh rate) iznosi 60 Hz. Karakteristična je za SAD, Kanadu i Japan.

PAL - (*eng. Phase Alternating Line*). Karakteristike PAL sistema su da prenosi 25 slika (odnosno 50 poluslika) u sekundi sa po 625 linija, dok je frekvencija osvježavanja 50 Hz. PAL predstavlja detaljniji prikaz od NTSC zbog broja linija (100 linija razlike) ali je podložniji treperenju slike zbog nižeg frekvencijskog osvježavanja. Koristi 'interlace' za iscrtavanje slike i oslanja se na amplitudsko modulisani prenos (AM) slike i frekfencijsko modulisani (FM) prenos zvuka. Koristi se u većini Evropskih zemalja.

SECAM - (*fr. Séquentiel couleur avec mémoire*). SECAM sadrži 625 horizontalnih linija (od čega je 576 vidljivo) za iscrtavanje slike, sa frekvencijom osvježavanja od

50Hz. Za razliku od PAL sistema, njegov prenos slike i zvuka obavlja se FM modulacijom. U upotrebi je u Francuskoj, Grčkoj, Rusiji, nekim zemljama istočne Evrope i u Africi.

Standardan CRT (*eng. Cathode ray tube*) televizor predviđen za PAL standard prikazuje sliku rezolucije 768x576 piksela, SD (*eng. Standard-definition)* rezolucija. Ukoliko se na prijemniku pusti signal veće rezolucije u odnosu na SD neće se primijetiti poboljšanje, dok za materijal manje rezolucije od SD (npr. 640x480) i dalje ćemo imati sliku solidnog kvaliteta zbog fleksibilnosti katodne cijevi.

Sve popularniji LCD *(eng. liquid-crystal display)*, LED *(eng. light-emitting diode)* i Plazma televizori imaju fiksnu rezoluciju ekrana koja se naziva nativna (prirodna) rezolucija. Neke od standardnih rezolucija LCD/LED/Plazma televizora su:

- HD – (*eng. High Definition* - 1280x720)
- FHD – (*eng. Full HD* -1920x1080)
- QHD – (*eng. Quad HD* - 2560x1440)
- WQXGA – (*eng. Wide Quad Extended Graphics Array* - 3200x1800)
- UHD 4K – (*eng. Ultra HD* - 3840x2160)

Iako je FHD rezolucija standard zadnjih nekoliko godina, već u toku narednih par godina mogu se očekivati prenosi 4K rezolucije. Jedan takav 4K projekat bilo je prikazivanje Olimpijade u Londonu 2012. godine. QHD rezolucija, iako predstavlja logični naredni korak prikaza slike, nije zaživila, ali tokom poslednje dvije godine svoju primjenu nalazi na mobilnim platformama.

Ako se vratimo na analognu televiziju vidimo da standardi na kojima se zasniva današnja televizija postavljeni su prije skoro pola vijeka. Od tada pa do danas se skoro ništa nije promijenilo u smislu poboljšanja kvaliteta slike (ukoliko izuzmemo prenos kablovskim putem koji nam donosi određenu sigurnost po pitanju kvaliteta prenešenog signala). Ako sada uporedimo PAL rezoluciju od 768×576 piksela, vidimo da je to daleko ispod standarda koji danas preovladava. To se najbolje vidi kroz dijagonale televizijskih ekrana čija je rezolucija sve veća, dok rezolucija analognog prenosa ostaje nepromijenjena. Logičan zaključak je da digitalizacija predstavlja idući veliki korak u sferi televizije.

2.2. Standardi i rezolucije za digitalnu televiziju

Digitalna televizija predstavlja evolucionarni skok u proizvodnji i emitovanju radio i televizijskog programa. U zavisnosti od rezolucije slike (HD, FHD.... 4K) i tehnike skeniranja koja se koristi, digitalna televizija je standarizovana od strane Međunarodne unije za telekomunikacije.

Razvoj koncepta digitalne televizije, odnosno njene realizacije najviše je bio uočljiv tokom 90-tih godina prošlog vijeka. U okviru digitalne televizije postoje dvije grupe standarda, koje možemo razlikovati: evropski i američki. Ono što je karakteristično za oba standarda je da digitalna televizija donosi, prije svega, multimedijalne usluge.

Kodiranje i kompresija signala obavlja se preko MPEG-2 standarda [1]. Međutim sam digitalni signal možemo predstaviti, odnosno kodirati i kompresovati i uz pomoć generacije MPEG standarda (MPEG 1,2,3,4). Naravno tu su i transformacije signala: wavelet i diskretna kosinusna transformacija. Digitalni signal se može prenijeti kablovskim putem (eternet, optički kabal, bakarna parica ili radio talasima). U suštini standardi obuhvataju tri podsistema [18] [19]:

- Prvi podsistem definiše kompresiju i kodiranje, i to MPEG-2 za video kompresiju, odnosno Digital Audio Compresion (AC-3) za kodiranje zvuka.

- Drugi podsistem predstavlja multipleksiranje video, audio i pomoćnih informacija u jedan *stream* podataka, takođe koristi MPEG-2 kodiranje.

- Treći podsistem obuhvata prenos digitalno kodiranog *streama* bilo da je u pitanju kablovski prenos, preko satelita ili zemaljskim antenama.

Već su pomenute rezolucije digitalne televizije. Trenutno najpopularniji skup rezolucija slike sastoji se od:

- HDTV (*eng. High Definition TV*): HDTV nudi rezoluciju 1080 linija sa 1920 piksela po liniji (1920x1080), format slike je 16:9, i koristi se *interlaced*

scan. Za ovaj tip rezolucije potreban je kanal širine 6 MHz za prenos slike, dok *framerate* (broj slika u sekundi) ide do 60 fps (*frames per second*).

- *Medium resolution TVHD*: Rezolucija slike je 720x1280 (720 linija sa 1280 piksela po liniji), koristi se *progressive scan*, sa 24 ili 30 fps. Format slike je takođe 16:9, kao i širina kanala od 6MHz.

- SDTV (*eng. Standard Definition TV*): Ovaj standard podržava različite rezolucije, od kojih je najčešća rezolucija od 480x640 piksela. Format slike je 4:3 i može se prenijeti do 6 digitalnih kanala u osnovnom pojasu od 6 MHz. U tabeli 1 su prikazani standardi kako za SD tako i za HD standarde.

ATSC TABELA FORMATA ZA DTV PRENOS

Vertikalna vrijednost	Horizontalna vrijednost	Odmjer slike informacija	Okvir i skeniranje slike
(HD) 1.080	1.920	16:9	24p, 30p, 30i
(HD) 720	1.280	16:9	24p, 30p, 30p
(SD) 480	704	4:3	24p, 30p, 30i, 60p
(SD) 480	704	16:9	24p, 30p, 30i, 60p
(SD) 480	640	4:3	24p, 30p, 30i, 60p

Tabela 1 – Standardni formati digitalne televizije

SDTV u suštini predstavlja analognu televiziju standardne rezolucije koja se bežičnim putem distribuira kroz etar ili kablovske infrastrukture. U Evropi SDTV koristi PAL standard što povlači rezoluciju od 768x576 piksela.

DVB (eng. *Digital Video Broadcasting*) standard, odnosno digitalno emitovanje televizije, predstavlja skup internacionalno prihvaćenih standarda u domenu digitalne televizije. Projekat, nastao 90-tih godina prošlog vijeka, 1993. godine, sa sjedištem u Ženevi, osnovan je od strane 83 člana iz sfera radio difuzije, telekomunikacija, proizvođača digitalne opreme ali i regulatornih agencija.

Mnoge zemlje prihvatile su DVB standard kao zamjenu za PAL, SECAM i NTSC standard.

Grupa DVB standarda uključuje:

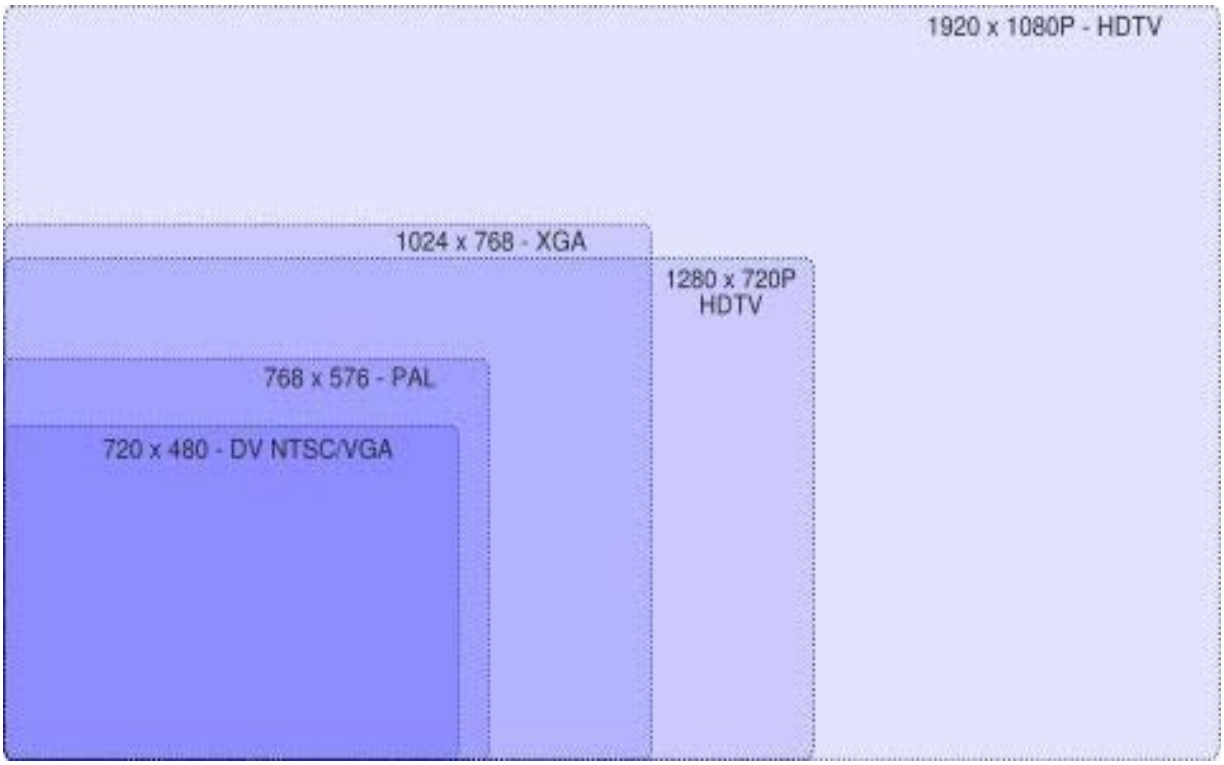
- DVB-S - digitalni satelitski sitem za frekvencije do 11/12 GHz.
- DVB-C - digitalni kablovski sistem kompatibilan sa DVB-S.
- DVB-CS - digitalni SMART TV sistem prihvaćen od DVB-C i DVB-S.
- DVB-MC - digitalni multipoint distribucioni sistem, (10GHz) baziran na DVB-C kablovskom sistemu.
- DVB-MS - digitalni multipoint distribucioni sistem, (10GHz) baziran na DVB-S satelitskom sistemu.
- DVB-T/T2 - digitalni sistem za zemaljske predajnike (8 MHz i 7 MHz).
- DVB-SI - servis IS, za DVB dekodere.
- DVB-TXT - DVB teletekst.
- DVB-CI - DVB za pristup drugim aplikacijama.
- DVB-IPI - transport DVB servisa preko IP adrese.

DVB-S predstavlja prvi standard koji je omogućio prenos HD slike. Kompresija je obavljena preko MPEG standarda i omogućavala je da se analogni materijal koji je zahtijevao veliki propusni opseg kompresuje tako da zauzima daleko manje prostora za vrijeme transmisije ali bez prevelikih gubitaka na kvalitetu. Prelaskom na DVB-C standard i kablovskim distributerima je omogućen prenos slike u HD rezoluciji.

DVB-T - *terrestrial* je standard koji je omogućio prenos digitalne slike u SDTV formatu. Očekivalo se da se upotrebom DVB-T standarda može prenijeti i HD format slike, ali ispostavilo se da je to mnogo složeniji proces u odnosu na prenos putem satelita ili kablovskog sistema. Tek uvođenjem DVB-T2 standarda omogućena je transmisija slike u 720p, 1080p formatu [14].
Što se tiče DVB-T standarda, upotrebljavana je MPEG-2 kompresija. Karakteristika DVB-T predajnika, odnosno mreže, pored znatno robusnije realizacije u odnosnu na analogni signal, je da je njegova mreža robusnija od analogne, odnosno ispad jednog od DVB-T predajnika u mreži neće uticati na prijem, jer je moguće da se signal primi od ostalih DVB-T predajnika.

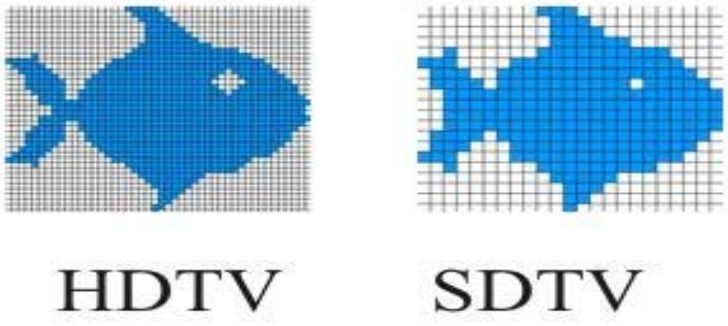
DVB-T2 standard predstavlja drugu generacija ovog standarda koja omogućava prenos slike u HD rezoluciji uz upotrebu MPEG-4 kodeka.

HDTV standard se definiše kao signal čija slika sadrži 1080 aktivnih linija, sa formatom slike 16:9 prema preporuci ITU-R BT.709. Za razliku od Evrope -SAD, Kanada i Južna Koreja HDTV standard definišu kao svaki digitalni signal čija je rezolucija veća od 720 aktivnih linija. Na slici 1 prikazano je nekoliko HDTV podstandarda.



Slika 1 – HDTV rezolucija

Naravno, HDTV nudi prikaz sa daleko većim brojem detalja u odnosu na SDTV, ali samim tim zahtijeva i veći prenosni opseg (*bandvith*). Na slici 2 je prikazano poređenje slike u HDTV i SDTV formatu.



Slika 2 - HDTV i SDTV, poređenje

2.3. Razlozi za digitalizaciju

Generalno posmatrano, digitalna televizija predstavlja pravu revoluciju za korisnike TV usluga. Analogna televizija čiji je razvoj popularizovao ovaj medijum, više ne može da ponudi ništa novo što može zadovoljiti korisnike. Naravno, digitalizacija neće preuzeti kompletno vođstvo u odnosu na analognu televiziju, bar ne neko vrijeme dok se ne ostvari skoro univerzalna pokrivenost digitalnim signalom. Postupak prelaska na digitalni sistem emitovanja znači preduzimanje mjera koje bi omogućile da građani prilagode postojeće TV prijemnike novim standardima, odnosno da se već postojeća oprema na neki način "osvježi", makar u vidu hardverskih dodataka.

Kao i svaka tehnološka revolucija i digitalizacija sa sobom donosi mnoge prednosti i otvara vrata novim mogućnostima. Proces digitalizacije počeo je još 90-tih godina prošlog vijeka ali su tek poslednjih godina ti standardi prihvaćeni u većini zemalja. Sa druge strane usvojeni su rokovi za finalizaciju u okviru međunarodne unije za telekomunikacije i evropske unije sa ciljem što bržeg prelaska na digitalne radio difuzne sisteme.

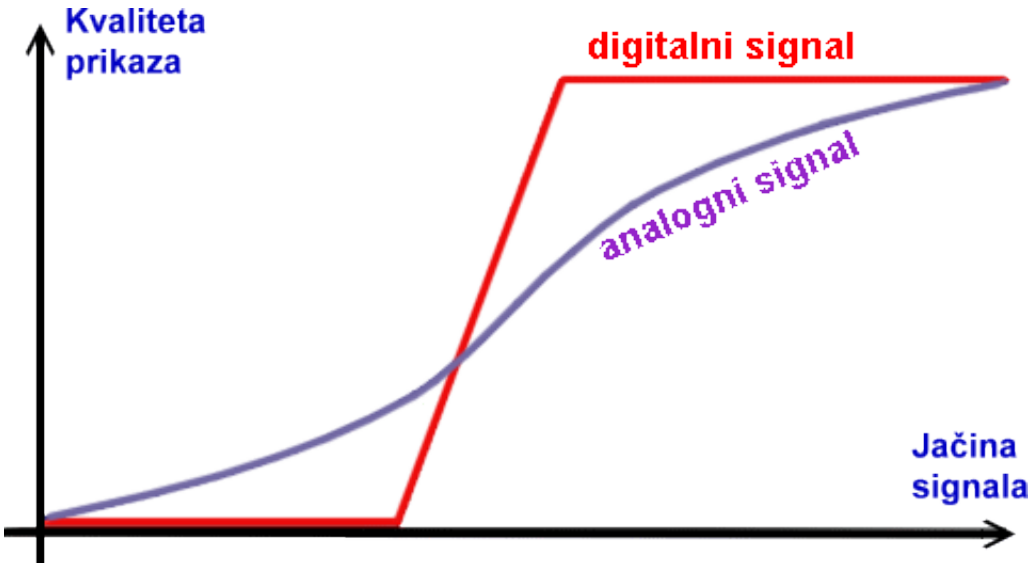
Naravno, proces prelaska sa analognih na digitalne radio difuzne sisteme je proces koji iziskuje vrijeme, kao i značajna finansijska sredstva ali i edukaciju građana da bi znali na koji način mogu da koriste digitalni signal, i prije svega, da li njihovi postojeći TV prijemnici mogu podržati novi format (DVB-T2). Analogni signali su zauzimali ogroman dio frekventnog opsega, tako da će digitalizacija omogućiti i oslobađanje radio frekventnog spektra, što se može iskoristiti za uvođenje novih servisa. Digitalna tehnologija omogućava bolji kvalitet slike, a sistem za prenos slike DVB-T2 mreže zemaljskih prijemnika omogućava prenos i emitovanje jednog ili više programa.

Naravno, razlozi za digitalizaciju su pored otpornosti na smetnje superiorni kvalitet slike, odnosno tona, bolji prenos radio signala, mnogo manja zavisnost od okoline, položaja antena i vremenskih uslova u odnosu na postojeći analogni signal. U nastavku su detaljno opisane najznačajnije prednosti digitalne televizije:

2.3.1. Otpornost na smetnje

Osnovna prednost digitalnog signala u odnosu na analogni je ta što na relativno jednostavan način veoma oštećen signal možemo regenerisati, odnosno rekonstruisati, što dovodi do situacija da kad čak imamo i ekstremno loše vremenske uslove (a signal šaljemo vazdušnim putem) taj signal možemo uspješno regenerisati na svakoj stanici između predajne i prijemne strane. To dovodi do situacije da skoro uvijek imamo zagarantovane visoko kvalitetne reprodukcije slika, odnosno zvuka. Ukoliko se ipak desi da smetnje prevazilaze graničnu vrijednost (vrijednost koju prijemna strana ne može regenerisati, odnosno rekonstruisati) slika se prikazuje kao zamrznut frejm, odnosno dolazi do odsustva slike.

Sama rekonstrukcija zavisi od kvaliteta primljenih impulsa, naime, digitalni signal je daleko otporniji na šum od analognog signala ali neprepoznavanje impulsa (impulsi se nikada ne mogu prenijeti od predaje do prijema u savršenom obliku zbog ne idealnosti sistema) kroz neadekvatne stanice dovešće do sigurnog gubitka.
U nekim granicama čak i izobličenje impulsa od preko 50% omogućava prepoznavanje impulsa na prijemnoj strani (u zavisnost od referentne vrijednosti potrebne za regeneraciju signala). Kvalitet prijemnog signala i otpornost digitalnog signala u odnosu na analogni prikazano je na dijagramu (slika 3).



Slika 3 - Otpornost digitalnog signala u odnosu na analogni

Ako je primljeni signal u odnosu na poslati signal slabiji i sklop za odlučivanje nije u stanju da odrediti šta je "0", a šta "1", već se pogrešno tumači sadržaj binarnih nizova, u tom slučaju dolazi do pada kvaliteta. Ovaj pad kvaliteta daleko je linearniji kod prijema analognog signala, slika je obuhvaćena šumom ali i dalje postoji, dok se kod digitalnog signala desi ili gubitak frejmova ili pikselizacija slike.

2.3.2. Više programa

Digitalni prenos signala koristi isti frekvencijski opseg kao analogni, ali sa tom razlikom da zahvaljujući savremenim metodama kompresije signala digitalni signal zauzima mnogo manji opseg u odnosu na analogni. To omogućava da u okviru jednog frekvencijskog opsega možemo emitovati istovremeno više TV kanala. U DVB-T2 standardu [5] koji je zastupljen kod nas, moguće je emitovati više TV programa u jednom kanalu.

Kao što je već rečeno, kompresija ovdje ima glavnu ulogu ali samim procesom kompresije dolazimo i do komplikovanosti hardvera na prijemnim stranama. Odnosno, jednostavnija predajna strana donosi jednostavniju i prijemnu stranu, ali ne može garantovati gubitke nastale tokom prenosa. Proces povećanja rezolucije trebao bi nuditi i nove vrste kompresije koje bi omogućile takođe vjeran prikaz originalne slike, uz što manju potrošnju raspoloživog opsega ali i komplikovanost u vidu tehničkih sposobnosti uređaja koji bi taj signal dekodirali. Digitalni signal takođe donosi mogućnost emitovanja programa na više jezika, mogućnost *surround* zvuka, EPG *(eng. Electronic program guides)*… Ovakva vrsta kompresije omogućava distributerima programa emitovanje više digitalnih kanala, koristeći pri tome isti frekvencijski opseg.

2.3.3. Jasnija slika i kvalitetniji zvuk

Ako govorimo o terminu jasnija slika, jedna od parametara jasnoće je, logično, slika visoke rezolucije. Iako visoka rezolucija konkretno ne garantuje jasnoću slike ona nudi daleko više detalja u odnosu na analognu odnosno SDTV televiziju. Ako uporedimo HDTV sa SDTV, posmatrajući samo rezoluciju oba signala, vidi se da

HDTV nudi sliku sa čak pet puta više piksela po liniji, što automatski povlači i činjenicu da se u prostoru 1920x1080 piksela može smjestiti daleko više detalja.

Slika 4 – SDTV i HDTV, poređenje

Nove generacije TV prijemnika podržavaju ekran formata 16:9 sto je približno širina perceptivne slike ljudskog oka. Čak novije generacije TV prijemnika razvijenih u poslednje dvije, tri godine nude mogućnost zakrivljenja ekrana, što ljudskom oku daje mogućnost realnijeg prikaza slike. Ovaj trend zasnovan na OLED *(eng. Organic Light Emitting Diode)* tehnologiji uvukao se i u sfere mobilne industrije.

Možemo smatrati da će sve više kako TV prijemnika tako i mobilnih aparata pribjeći ovom trendu u što skorijoj budućnosti. Ako pogledamo rezoluciju predviđenu za prikazivanje filmskog programa koja je već odavno u razmjeri 16:9, vidimo da nema potrebe za sužavanjem i izduživanjem slike kako bi film predviđen za bioskopsku projekciju mogao da se prikaže i na TV prijemniku.

Međutim, nije u pitanju samo kvalitet slike, digitalna televizija nudi mogućnost pristupa globalnim mrežama, odnosno polako postaje jedan pravi multimedijalni centar u okviru kućne varijante.

Glavne strategije u povezivanju interaktivne televizije i interneta su:

• Digitalni brodkasting (*eng .Digital Broadcast*)
• Pristup internetu putem TV-a (*Intercast, WebTV*)
• Fuzija ova dva slučaja

IPTV (*eng. Internet IP TV*) predstavlja jedan od najnovijih načina distribucije TV signala do krajnjih korisnika. Za prenos signala koristi klasične telekomunikacione sisteme, IP mrežu i postojeću infrastrukturu. Nudi interaktivnost kao i mnoge druge pogodnosti kao i neke od servisa poput snimanje programa, video na zahtjev, vremenska prognoza, elektronski vodič itd [19].

2.4. Razlike između DVB-T i DVB-T2 standarda

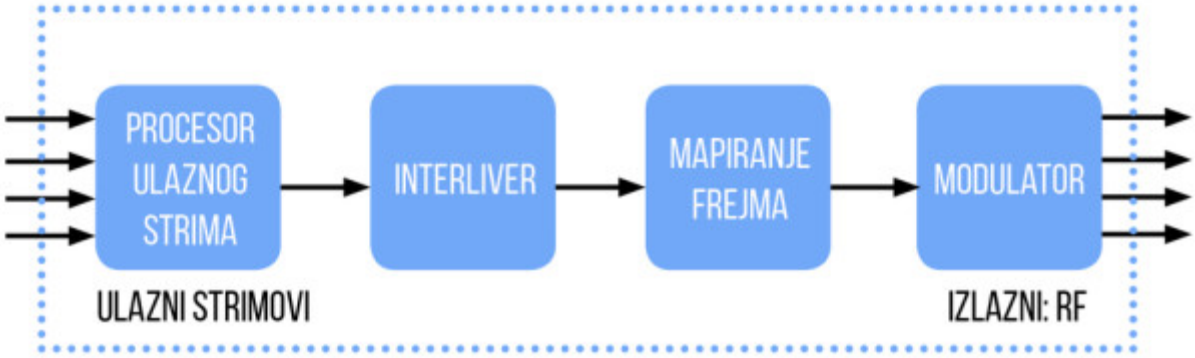
DVB-T, odnosno DVB-T2 [1], standardi predstavljaju prvu i drugu generaciju standarda, respektivno. Naravno razlika između generacija ova dva standarda postoji, a neki od najznačajnijuh su [20]:

- **Novija konstelacija (256-QAM - *Quadrature amplitude modulation*)**

DVB-T kao najvišu konstelaciju nudi 64-QAM, obezbjeđujući veoma veliku količinu podataka sa 6 bitova po simbolu po jednom nosiocu, dok DVB-T2, korišćenjem 256-QAM povećava efikasnost na 8 bitova po OFDM (*eng. Orthogonal Frequency Division Multiplexing*) ćeliji, što je povećanje od 33% u spektralnoj efikasnosti i kapacitetu kanala pri istom protoku bita. To znači da će biti neophodan znatno veći odnos signal šuma S/N (za 4-5dB veći) jer je prijem osetljiviji na šum.

- **Robustnost za servise i struktura DVB-T2 frejmova**

Fizički sloj DVB-T2 standarda prikazan na slici 5. Kao ulaz sistema može se dovesti jedan ili više MPEG transportnih TS strimova (*Transport stream*) i/ili jedan ili više GS (*eng. Generic stream*) strimova. Modifikacija strimova može se ostvariti kroz proces predprocesiranja. Na taj način ulazni strimovi imaju slaganje jedan-prema-jedan sa kanalima podataka PLP *(eng. Physical-Layer Pipes*) kanali u modulatoru.

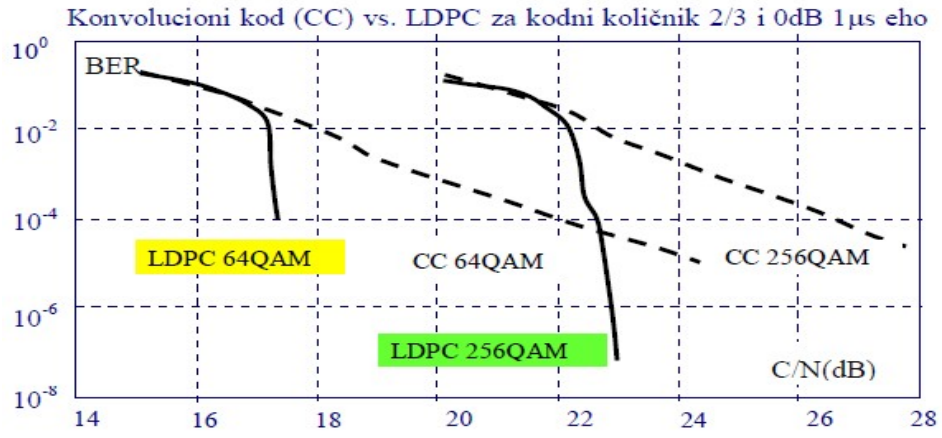


Slika 5 - Fizički sloj DVB-T2 standarda

Sa stanovišta komercijalne usluge T2 sistem predstavlja više različitih nivoa robusnosti za različite servise, u zavisnosti od načina modulacije, kao i servis korekcije grešaka (FEC). To se ostvaruje grupisanjem više OFDM (*eng. Orthogonal Frequency Division Multiplexing*) simbola u okviru jednog frejma. Nakon toga slijedi dodjeljivanje različitih servisa različitim slajsevima, koji predstavljaju djelove frejma.

- **Uticaj LDPC (*eng. Low Density Parity check Code*) kodovanja**

Posmatrajući prvu generaciju DVB standarda, slika 6 prikazuje dobitak prema klasičnom konvolucionom kodovanju. Uočava se nagli pad vjerovatnoće greške (*eng. BER, Bit Error Rate*) u slučajevima 64QAM i 256QAM QAM (*eng. Quadrature Amplitude Modulation*) [2]. Tačka QEF (eng. *Quasi Error Free*) koja se ima pri vjerovatnoći greške od oko 10-4, obezbjeđuje prenos bez gubitaka u televizijskom signalu.



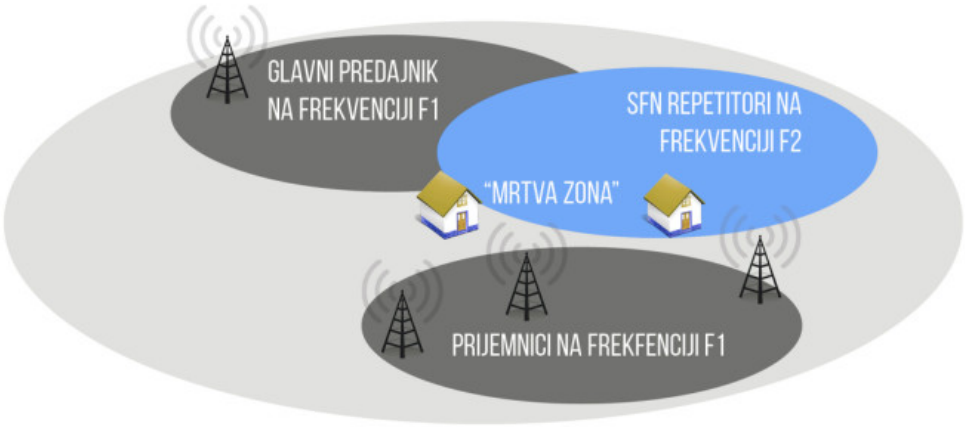
Slika 6 - Klasično konvoluciono kodovanje

- **Korišćenje više vrsta repetitora**

Pri korišćenju SFN (*eng. Single Frequcy Network*) mreža moguće je koristiti dvije vrste repetitora (slika 7):

- Regenerativne - sa ciljem demodulisanja DVB-T2 signala, regeneracije, ponovne modulacije i prenosa;

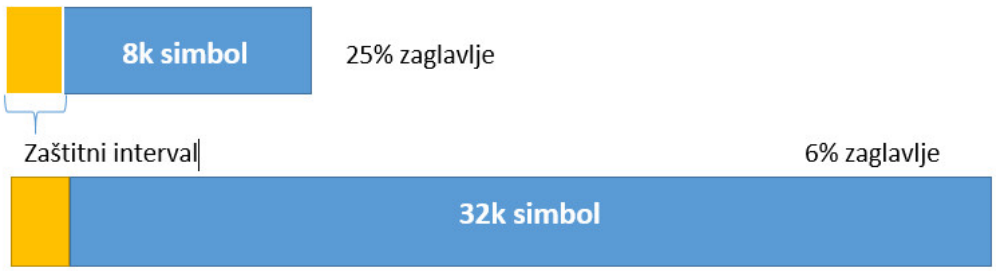
- Translatore - stanice sa ciljem pomjeranja i pojačavanja frekvencije, bez mogućnosti regeneracije odnosno bez mogućnosti remodulacije;



Slika 7 - Vrste repetitora

- **Zaštitni interval i broj nosilaca**

Povećanjem FFT (*eng. Fast Fouirier Transformation*), zaštitni interval smanjuje zaglavlje sa 25% (u slučaju 8k nosilaca) na 6%, u slučaju 32k nosilaca (slika 8).



Slika 8 - Smanjivanje gubitaka povećavanjem FFT

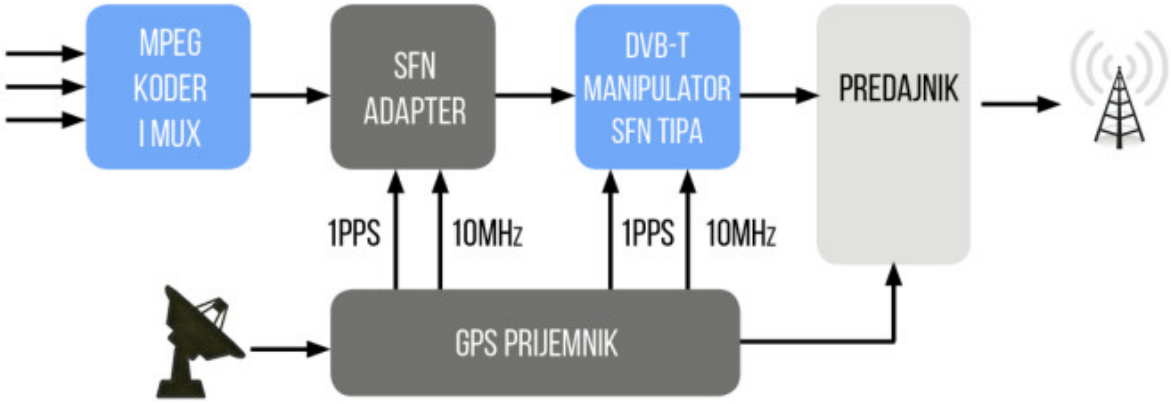
Veličine zaštitnih intervala u DVB-T2 standardu su: 1/128, 1/32, 1/16, 19/256, 1/8, 19/128, 1/4.

- **Frejmovi (BB)**

Interfejs na ulazu DVB-T2 modulatora obezbjeđuje BB frejmove (BaseBand frame) sa informacijom neophodnom za modulaciju, kao što su podaci za sinhronizaciju, format ulaznog strima i eventualna proširenja frejmova [6].

- **DVB-T2 sinhronizacija**

Ukoliko je potreban rad u jedno-frekvencijskim mrežama (SFN) DVB-T2 kao i DVB-T1 standard podrazumijevaju sinhronizaciju predajnika (slika 9).



Slika 9 - Sinhronizacija GPS predajnika

U realnim situacijama rad SFN mreže je moguć, ali je neophodno postići dobru sinhronizaciju među predajnicima.

U tabeli 2 prikazani su parametri DVB-T i DVB-T2 standarda.

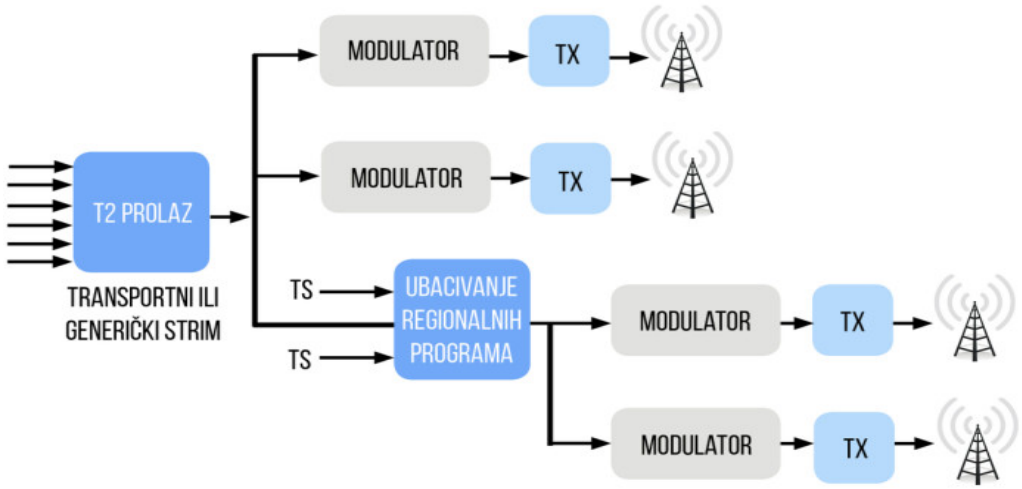
	DVB-T	DVB-T2
FEC	Conv. Coding + RS 1/2,2/3,3/4,5/6,7/8	LDPC + BCH 1/2,3/5,2/3,3/4,4/5,5/6
Modulacija	QPSK, 16QAM, 64QAM	QPSK, 16QAM, 64QAM, 256QAM
Zaštitni interval	1/4, 1/8, 1/16, 1/32	1/4, 19/256, 1/8, 19/128, 1/16, 1/32, 1/128
FFT veličina	2k, 8k	1k, 2k, 4k, 16k, 32k
Rasejani piloti	8% od ukupnog	1%, 2%, 4%, 8% od ukupnog
Kontinualni piloti	2,6% od ukupnog	0,35% od ukupnog

Tabela 2 – Uporedni parametri DVB-T i DVB-T2 standarda

- **Dodavanje lokalnih i regionalnih programa**

Prva generacija DVB standarda omogućavala je ubacivanje lokalnih programa u okviru multipleksera. To znači da svako novo ubacivanje programa zahtijeva kompletno dekodiranje signala, odnosno demultipleksiranje sadržaja. U slučajevima demutipleksiranja [6] nije potrebno vršiti dekodiranje signala, već se dekodira MPEG strim, što donosi mogućnost greške.

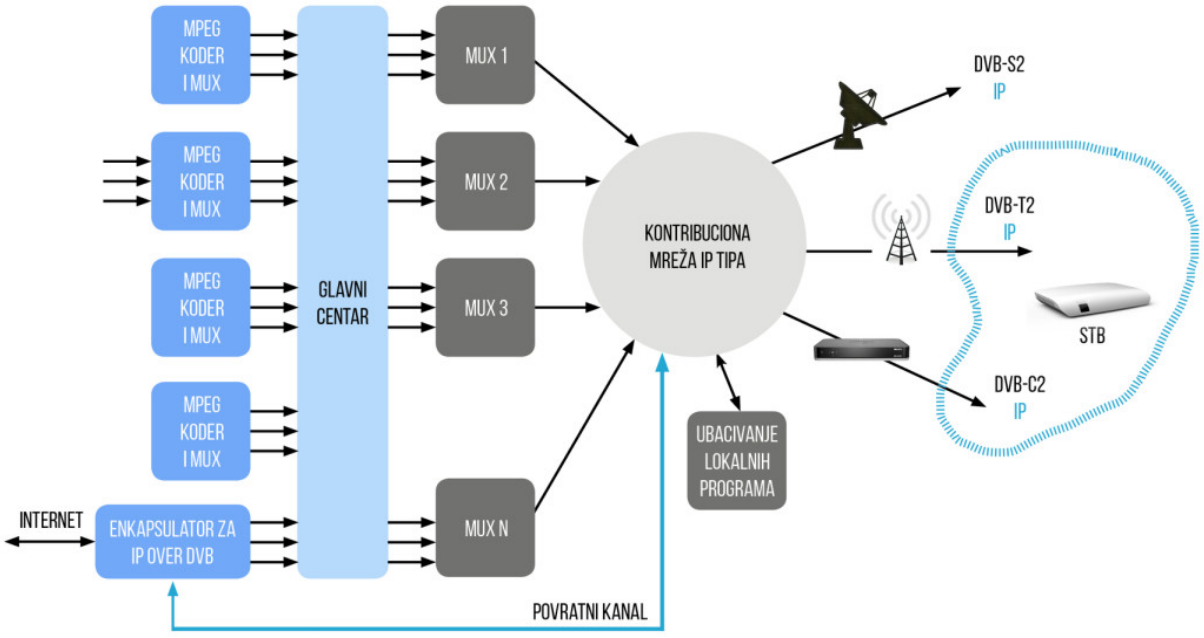
Druga generacija DVB standarda omogućava ubacivanje lokalnih i regionalnih programa bez dekodiranja, što je, u slučaju velikog broja programa prednost u odnosu na DVB-T1. Na slici 10 je data standardna DVB-T2 mreža.



Slika 10 – Standardna DVB-T2 mreža

DVB standard druge generacije [6] prije svega bio je zasnovan na razvoju interneta i njegovih standarda. Prva generacija DVB je za razliku od druge više bila multimedijski orjentisana.

Formiranje multipleksa vrši se u glavnom server centru i kroz njih kao ulaz dolaze programi generisani u produkcijskim centrima, VoD (*eng. Video on Demand*), eksterni signali. Mreža primarne distribucije je bazirana na IP protokolu i iz nje se vode signali na emitovanje (kablovski i/ili satelitski tip prenosa), uz istovremeno omogućavanje prenosa po DVB kanalima.



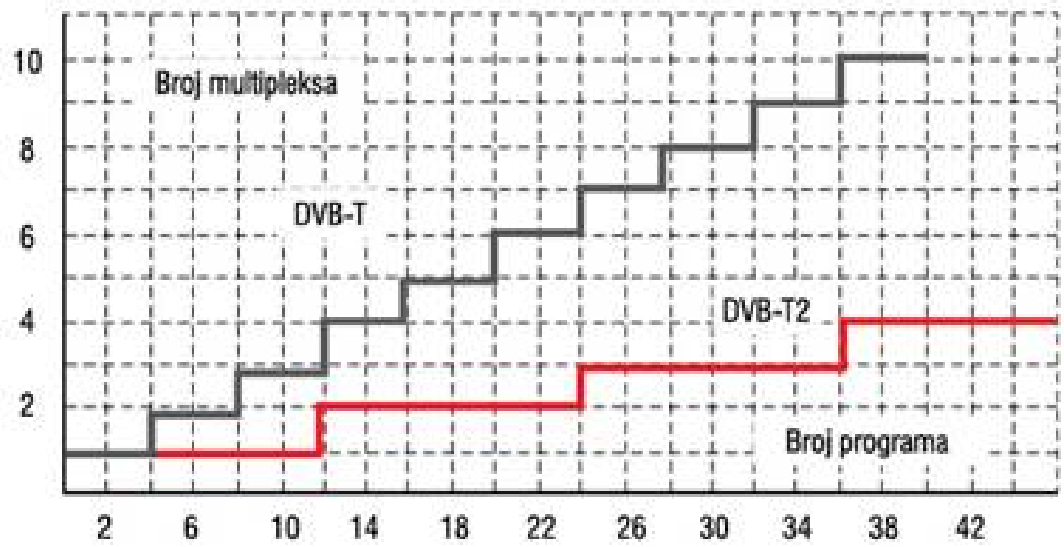
Slika 11 – Standardna IP/ DVB-T2 mreža

Zahvaljujući IP protokolima složenost ove mreže (slika 11) svedeno je na relativno jednostavan sistem što nam donosi mogućnost korišćenja jednog STB (*eng. set top box*) uređaja za različite medijume.

- **Kapacitet sistema**

Projektovanje mreže u SFN modu dodatno povećava kapacitet zahvaljujući velikom izboru i velikim iznosima zaštitnih intervala. Samo povećanje kapaciteta donosi veću uštedu u količini opreme, dok uz fiksirani broj programa potrebnih za prenos u nekoj mreži količina uređaja koji rade na DVB-T2 standardu je znatno manja u odnosu na DVB-T standard.

Na slici 12 uz pretpostavku da je program kodiran MPEG4 standardne rezolucije možemo grafički prikazati broj potrebnih multipleksa za prenos odgovarajućeg broja TV programa.



Slika 12 - Potreban broj multipleksa za prenos određenog broja TV programa

Slika dovodi do zaključka da uz kvalitetno planiranje uz korišćenje MPEG-4 kompresije DVB-T2 signala nosi značajnija i jeftinija poboljšanja u prenosu digitalnih televizijskih signala.

Neke od ključnih prednosti DVB-T2 standarda zasnovane su na sledećim činjenicama:

- bolji uslovi prenosa, što daje znatno veći protok u okviru istog opsega;
- manja osjetljivost na šum;
- izuzetno dobra zaštita signala, pogodna za prenose u slučaju kada su okruženja sa velikim šumom i smetnjama;
- kompatibilnost sa IPTV;
- mogućnost šireg izbora parametara pri kodiranju i modulaciji;
- veći broj programskih sadržaja u okviru jednog multipleksa i jednostavnost sistema;
- isplativost sistema;
- dovoljan protok za prenos HDTV signala.

2.5. Uslovi za prijem digitalnog signala

Budući da je digitalna televizija potpuno različiti koncept kodiranja, prenosa i prikaza od analogne televizije, potrebna su dodatna novčana ulaganja i na strani korisnika i na strani TV kompanija koji pružaju ove usluge.

Digitalizacija emitovanja TV programa kroz mrežu zemaljskih predajnika zahtijeva:

- odgovarajuću pripremu signala koji treba emitovati,
- zamjenu postojećih (analognih) predajnika novim digitalnim,
- prilagođavanje kućnih prijemnika.

Prijem slike kod TV prijemnika ostvaruje se na neki od četiri načina: satelitski, kablovski, internet i antenski prijem. U prva tri slučaja, po pravilu, sami provajderi (satelitski, kablovski ili internet) obezbjeđuju opremu za prijem digitalne TV.

Prijem digitalnog signala podrazumijeva prijemne antene, prateće instalacije i odgovarajući prijemnik. Prijem se može ostvariti: sobnom antenom, spoljnom antenom, zajedničkim antenskim sistemom, ali prijem prije svega zavisi od same lokacije tako da sama lokacija određuje način prijema signala. DVB-T2 nije isključivo vezan za televiziju, odnosno stacionarni prijem, već je svoju primjenu pronašao i u okviru mobilnih mreža.

Pored digitalne obrade slike proces digitalizacije podrazumijeva korišćenje digitalizovanih televizijskih prijemnika, odnosno prijemnika koji će moći da prihvate digitalno obrađeni televizijski signal.

Digitalni signal u sebi sadrži kompresovane podatke o TV slici koje prenosi sa predajnika na antenu. Uređaj koji omogućava da se ti podaci obrade, raspakuju i prilagode prikazivanju na TV prijemnicima naziva se Set-Top-Box ili resiver/tuner. Tuner je uređaj koji vrši demodulaciju i koji na svom izlazu daje MPEG-2 kodirani signal. Dekoder ima ulogu dekodiranja MPEG-2 *(eng. Moving Picture Experts Group)* strima u video signal, audio signal i pomoćne podatke. Tuner/dekoder kao uređaj koji na svom izlazu daje video signal koji se standardnim video priključcima vodi na TV prijemnik, a npr. optičkim kablom na Dolby Digital dekoder.

Digitalizacijom će se omogućiti da se u budućnosti bilo koji sadržaj emituje u bilo koje vrijeme i na bilo kom mjestu i prima na mnogim platformama.

Kraj ere emitovanja analognim putem onemogućiće prijem televizijskih programa bez digitalnog prijemnika. Što se tiče naše države televizijski prijemnik će morati da zadovolji sve postavljene standarde prijema: demodulacija DVB-T2 sa standardom ETSIEN302755 u jednofrekvencijskim SFN i višefrekvencijskim MFN (*eng. Multi Frequcy Network*) mrežama i prijem signala po svim kanalima u opsegu 174 MHZ do 230 MHZ i opsegu od 470 MHZ do 790 MHZ, i da bude otporan na moguće smetnje ostalih kanala. Takođe, neophodno je da prijemnik ima najmanje jedan ulazni RF konektor, a tip prijemnika STB mora da ima najmanje 1 SCART u skladu sa EN50049-1 i EN50157-2-1 standardom i jedan VCR Scart interfejs. Prijemnik mora imati optički ili koaksijalni interfejs za digitalni audio signal. Koliko različitih vrsta priključaka pojedini uređaj posjeduje će vrlo vjerojatno biti jedna od ključnih stvari pri odabiru među korisnicima.

Prijemnik treba da ima teletekst, svi jezici u službenoj upotrebi moraju biti podržani tako da korisnik može da izabere i memoriše svoj izbor. Digitalizacijom će biti omogućena i takozvana roditeljska kontrola.

Postojeći televizori mogu da se koriste za praćenje digitalno emitovanog programa, uz određene uslove. Tehnički uslov za prijem digitalnog signala na strani korisnika je neophodan Set-Top-Box uređaj. Uz povezivanje sa Set-Top-Box prijemnikom, može se pratiti program digitalne televizije koji se emituje u standardnoj (SDTV) rezoluciji. Slika formata 16:9 može se prikazati na ekranu analognog televizora, ali uz prilagođenja formata (izduživanje slike, smanjenje originalne slike i pojavu crnih štrafti ispod i iznad). Danas imamo savremenih televizora na tržištu TV prijemnika koji u sebi imaju već integrisan tuner za DVB-T2 prijem signala. U tom slučaju za prijem je potrebna samo antena.

Digitalizacija ne prestavlja trošak samo za krajnje korisnike već i TV emiteri moraju proći proces digitalizacije kroz ulaganja u studijske kamere sa digitalnim izlazom, odnosno kupovinom odgovarajućih adaptera za postojeće uređaje. Još jedan od preduslova je i neophodnost MPEG-2 enkodera. Za prenos slike među udaljenim studijima može se koristiti Internet.

2.6. Krajnji efekti digitalizacije

Da li je digitalizacija uopšte neophodna?
Jeste, u toku dosadašnjeg rada naveli smo sve pozitivne stvari digitalizacije, dok su negativne stvari reducirane, odnosno potpuno beznačajne. Sama digitalizacija predstavlja evolutivni skok u domenu televizijskog prenosa tako da sve negativne stavke su zanemarljive. Možda neki novi vid tehnologije ispravi postojeće greške digitalizacije, ali za sada digitalizacija je neophodna. Sa korisničke strane prednosti su očigledne:

- Kvalitetnija slika i zvuk
- Veći izbor televizijskih i radijskih progama
- Mogućnost titlovanja sa jezikom po izboru, audio komentara kao i specijalnih znakova potrebni licima sa specijalnim potrebama
- VoD (*eng. Video on Demand*) - krajnji korisnik može sam uređivati, pauzirati, preskakati, arhivirati i snimati program, omogućavajući korisniku potpunu slobodu kada je uređivanje programa u pitanju
- Aktivno pretraživanje programskih sadržaja po ključnim riječima, bilo da je u pitanju ime autora, emisije, nazivi emisije, datumi itd.
- Sa digitalnom televizijom samo potvrđujemo koncept *Internet-of-things* (IoT), gdje TV prijemnik postaje jedan pametan uređaj koji nam dozvoljava pristup globalnoj mreži
- Višejezična audio podrška za određene kanale

Slobodno možemo reći da tokom razvoja televizije upravo digitalna televizija po prvi put uspostavlja interaktivni odnos gledalaca i televizije.
Međutim, nisu samo prednosti digitalizacije na strani korisnika. Što se tiče provajdera, uvođenjem digitalizacije oni dobijaju:

- Smanjenje troškova prenosa (inicijalni gubici nastali zamjenom opreme mogu se nadoknaditi kvalitetom sadržaja i omogućavanjem VoD usluge)
- Interaktivnost servisa
- Uvođenje mogućnosti pružanja servisa na zahtjev
- Mogućnost usmjerene ponude sadržaja u skladu sa ciljnom publikom (krajnjim korisnicima)

Međutim, da bi sve ovo funkcionisalo potrebna je pomoć, odnosno saradnja sa državom iako EU forsira digitalizaciju, stvarajući ogroman trošak za države koje prihvate njihove standarde, država ipak ima određene koristi:

- Oslobađanje frekvencijskog spektra i njegovo efikasnije korišćenje
- Oslobođeni frekvencijski spektar može se iskoristiti za nove servise ili za iznajmljivanje stranim/domaćim investitorima
- Promocija novih tehnologija
- Konkurentnost među provajderima
- Lokalni sadržaj dobija ravnopravno mjesto sa ostalim sadržajem
- Smanjenje troškova prenosa

2.7. Digitalizacija u Crnog Gori

Na slici 13 je grafički prikazana podjela po zonama predajnika na teritoriji Crne Gore, na kojoj se vidi da su formirane četiri zone.

Slika 13 - Teritorija Crne Gore podijeljena u četiri zone

U zonama predajnika, sa objekata RDC-a, Lovćen (35. kanal), Podgorica (24. kanal), Bjelasica (43. kanal) i Tvrdaš (49. kanal), istovremeno se emituje analogni i digitalni TV signal. RDC posjeduje 42 lokacije na kojima uređaji rade kao predajnici (VHF i UHF) i 87 lokacija na kojima uređaji rade kao repetitori.

Objekat Lovćen je čvorna tačka za sve linkovske veze na prostoru centralne i južne Crne Gore, dok je objekat Bjelasica čvorna tačka za sve linkovske veze na prostoru sjevernog dijela Crne Gore. Na antenskom stubu na objektu Lovćen su instalirane ukupno 82 antene (48 UHF, 16 VHF i 18 FM antena), dok je na objektu Bjelasica instalirano 80 antena (40 UHF, 16 VHF i 24 FM antena).

Radio-difuzni centar (RDC) Crne Gore stekao je status operatora prvog multipleksa digitalne zemaljske radio-difuzije pokrivanjem cjelokupne teritorije Crne Gore i pravom da svoju uslugu pruža posredstvom radio-difuznih frekvencija u sve četiri zone za DVB-T/DVB-T2 koje su definisane planom raspodjele radio frekvencija za digitalnu zemaljsku radio-difuziju.

U sklopu prvog multipleksa će se, za početak, naći dva televizijska i dva radijska programa Javnog servisa Crne Gore, dok će ostali crnogorski kanali pravo pristupa moći ostvariti na javnom konkursu koji će biti raspisan.

Radio-difuzni centar Crne Gore koji se bavi prenosom i emitovanjem TV i audio signala u Crnoj Gori je zadužen za implementaciju ovog projekta. Taj projekat je podijeljen u dvije faze.

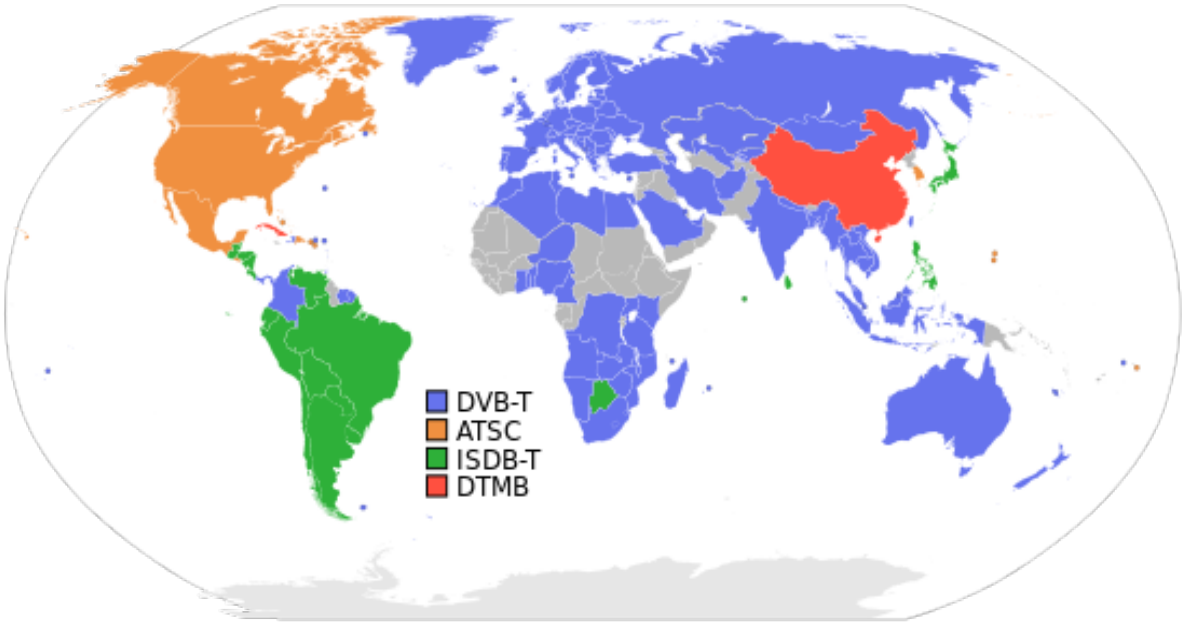
Prvu fazu, koju je finansirala delegacija Evropske unije, tokom koje su instalirana 43 predajnika i drugu fazu koju je finansirala Vlada Crne Gore, tokom koje je instalirano još 30 predajnika na objektima RDC-a širom Crne Gore. Sada postoje 73 predajnika i repetitora sa kojih se emituje digitalni signal zemaljske televizije i koji pokrivaju oko 90% stanovništva Crne Gore.

Pregled usvojenih parametara mreže koji će važiti za Crnu Goru možemo vidjeti u tabeli 3.

Modulaciona šema	256-QAM
Kompresioni standard	MPEG-4 (H.264/AVC)
Mod rada	32K
Nominalna širina kanala	8 MHz
Zaštitni interval	1/16
Kodni količnik	3/5
Pilot šema	PP2
Tip mreže	SFN
Vrsta prijema	stacionarni
Antenski mod	SISO
PLP mod	Single
Frekvencijski mod	Normalni
Procenjen bitski protok	31.1 Mbit/s

Tabela 3 - Parametri mreže

Sistem digitalne zemaljske televizije širom svijeta je prikazan na slici 14. Zemlje koje koriste DVB-T ili DVB-T2 su prikazane u plavoj boji.



Slika 14 - Zemlje koje koriste DVB-T ili DVB-T2 standard

3. DIGITALNI SEGMENT TEHNIKE U TVCG

Da bi shvatili način funkcionisanja televizijskog sistema, a samim tim i način funkcionisanja kao i radno okruženje EVS sistema, najbolje je napraviti uvod u funkcionisanje trenutno postojećeg analognog sistema. Sam proces digitalizacije obavlja se preko EVS sistema (*eng.* · EVS *Broadcast Equipment*). EVS sistem sastoji se iz više cjelina međusobno povezanih tako da omogućavaju realizaciju digitalnog signala integracijom svih tih cjelina u jedan *broadcast* sistem. Tako da te cjeline čine sistem koji sadrži montažerski dio (*Clean Edit*), unos materijala (*Ingest*), emitovanje programa (*Play Out*), centralnu memoriju (*Storage*), arhivu (*Archive*). Uporedo sa UTP i optičkim kablovima za transport materijala preko IP protokola sa ciljem povezivanja procesa montaže i Play Out stanice sa serverima (na kojima postoji protok materijala u obliku signala niske rezolucije protoka 1.5 Mbps, kao i signala visoke rezolucije protoka 15 Mbps). I dalje je dominatno prisutna mreža audio i video kablova koji vode i odvode signale do prostorije Glavne tehničke kontrole MCR (*eng. Master Control Room*). Uloga MCR-a je da kontroliše kvalitet eksternih i internih signala koji pripadaju analognom domenu i da ih prosleđuje na potrebne destinacije.

Generalno posmatrano, izvori signala koji imaju interno porijeklo su studijske režije, razni magnetoskopi, VTR-ovi (*eng. Video Tape Recorder*), DVD-ovi (e*ng. Digital versatile disc)*, *Play Out*-i… Kao signale eksternog porijekla mogu se navesti signali koji dolaze putem zemaljskih mikrotalasnih veza, optičkih mreža, satelitskih prijemnika, *LiveU* sistem transporta audio i video (AV) signala preko 3G mobilne mreže, kao i *live stream* sa Interneta. Svi ovi sadržaji transportnim mrežama prolaze kao digitalni signali, po protokolima koji su specificirani za određene medijume i određene generacije razvoja.

Ipak, da bi se signali mogli kontrolisati u MCR-u, kao i dalje proslijediti studijskim režijama kao i režijama dnevnog programa (Režija dnevnog programa je funkcionalno zadnja tačka emitovanja programskog signala, ali tehnički gledano, zadnja odlazna tačka je ista kao i prva, prijemna, dakle MCR), moraju se konvertovati u analogne, zbog analogne opreme koja je još uvijek u upotrebi. Signali koji dolaze u MCR iz spoljnjeg svijeta predstavljaju kontribucione signale, dok signale koje odlaze prema konzumentima programa nazivamo distributivnim

signalima. Nekadašnja praksa se sastojala od distribucije signala samo ka RDC-u (Radio Difuzni Centar), koji je preko radio mreže svojih primopredajnih stanica emitovao signal na teritoriji Crne Gore. Danas je situacija ipak drugačija. Signali oba programa (RTCG1, RTCG2) se distribuiraju novim operatorima, koji funkcionišu nezavisno od tradicionalnog RDC-a. Tako u MCR-u imamo kodere koji preuzimaju analogni signal i (uz upotrebu AD konvertora i električno-optičkog pretvarača) preko optičke IP mreže dovode signal do svojih tehničkih centara gdje u kombinaciji sa signalima drugih televizija formiraju razne komercijalne pakete (Extra TV, TOTAL TV, GO4YOU). Dakle, generalno govoreći, prisutnost na tržištu ne zavisi samo od jednog provajdera usluga prenosa. Nezavisno od svih pomenutih načina distribucije postoji i satelitski *up* link, preko kojeg smo prisutni na području Evrope, Bliskog Istoka i dijelu Sjeverne Afrike.

Udio analognog signala se vremenom smanjuje, ali je i dalje značajno prisutan. Tako, recimo, izlaz iz produkcionih kapaciteta je principijelno analogan. Kao sadržaj tog analognog signala možemo izdvojiti audio i video izlaz studija informativnog programa iz kojeg se realizuje veliki dio dnevne proizvodnje (Jutarnji program, sve dnevne informativne emisije, emisija Radni dan…). Takođe, emisije realizovane iz najvećeg studija, takozvanog velikog studija, koje se realiziju pomoću reportažnih kola (reportažna kola su resurs koji podrazumijeva svoju mobilnost u eksterijeru a sačinjen je od svih elemenata koji su prateći sadržaji svakog televizijskog studija) su analognog oblika. U formi analognog signala, mogu se pojaviti i izlazi sa satelitskih prijemnika. Tako se, recimo, Evrovizijski signal razmjene vijesti permanetno snima. Isto tako, snimaju se međunarodni sportski događaji.

Svi pomenuti analogni signali, po potrebi, mogu biti upućeni prema EVS sistemu. EVS sistem je sa ostatkom televizijskog sistema povezan preko digitalne (SDI - Serial Digital Interface, standard transporta podataka u digitalnom nekomprimovanom obliku protoka 270 Mbps) matrice - rutera, kapaciteta 16x16 (ulaza/izlaza). Ulazi su raspoređeni tako što je njih osam predviđeno za analogne signale, od kojih je pet rezervisano za signale proslijeđene iz MCR-a. Poseban oblik analognih signala koji se unose (importuju) u sistem je materijal snimljen na terenu. Naime, za akviziciju materijala na terenu koriste se različite generacije kamera. Tako u samom odeljenu Ingesta postoje magnetoskopi, VTR uređaje (Video Tape Recorder) koji služe za unošenje materijala snimljenog na terenu. Za taj vid unosa rezervisana su tri matrična ulaza. Obzirom da je matrica digitalna, svi

analogni signali, prije ulaska u nju, prolaze kroz AD konvertore, koji komponentni video konvertuju u MPEG2 *stream,* a analogni audio u AES/EBU standard *(eng. Audio Engineering Society Standard, Europian Broadcasting Union*), i embedere, u kojima se digitalnom videu dodaje digitalni audio. Naime, u procesu digitalizacije kompozitnog video signala pojavljuje se slobodan prostor, jer se digitalizuje samo aktivna linija, dok se za sinhronizaciju predajnika i prijemnika koriste kodne riječi pod imenima SAV (*eng. Start Active Video*) i EAV (*eng. End of Active Video*). U prostoru između EAV i SAV mogu se smjestiti odgovarajući dodatni podaci (*auxiliary data*), među kojima su najvažniji audio paketi. Uređaj koji omogućava tu operaciju zove se embeder. Konvertovani signali se zatim u obliku fajlova pohranjuju u sistem. Kada se, kao montažno obradjeni, ponovo koriste u svojstvu priloga u okviru emisija, oni se ponovo konvertuju u suprotnom smjeru, da bi se prilagodili analognim video miksetama. Izuzetak ove procedure predstavljaju *Sony*-jeva reportažna kola, koja imaju SDI internu komunikaciju (uređaji u kolima su digitalno spregnuti) i u kojima je implementiran Play Out Play Box uređaj, koji je *Ethernet*-om vezan sa EVS sistem, čime se izlazi iz digitalnog domena sve do izlaska iz reportažnih kola.

Kada su u pitanju pomenuti satelitski risiveri, možemo reći da je dio njih povezan direktno preko digitalnog SDI intefejsa, čime se postiže veći kvalitet signala za kasnije emitovanje i repriziranje. Pod SDI se obično podrazumijeva i embedovani audio signal, iako to nije obavezno. Preostali dio ulaza digitalne matrice rezervisan je upravo za ove digitalne signale, kao i unos materijala putem SX VTR-a koji je SONY-jev digitalni format.

U svrhu monitoringa snimanih signala signal mora biti obrađen u uređaju koji se zove de-embeder sa ciljem izdvajanja dodatih podataka iz video *stream*-a, nakon čega audio i video (AV) signal odvojeno prolaze kroz DA konvertore.
Ako je materijal snimljen na novijem medijumu – SD kartici ili optičkom disku, tada proces unošenja tog materija nazivamo import i on zapravo predstavlja klasično kopiranje fajlova. Ovdje treba napomeniti da unos materijala sa magnetnih traka, bilo da je u pitanju analogni ili digitalni standard, zahtijeva vrijeme unošenja koje je jednako vremenu trajanja sirovog materijala (sirovi materijal je ukupni materijal koji je snimljen na terenu koji procesom montaže tek treba da se pripremi za emitovanje). Takav pristup značajno usporava proces proizvodnje odnosno digitalizacije.

Televizija Crne Gore, kao članica EBU-a (*eng. European Broadcast Union*) ima mogućnost prijema i obavezu slanja svih aktuelnih, opšte značajnih i interesantnih događaja. To se obavlja u okviru Evrovizijske razmjene, na nivou razmjene živih signala i fajlova. U tom smislu, EBU je je uložio značajna finansijska sredstva da tu mrežu modernizuje i automatizuje. U pitanju je tkz. FNRMN (*eng. FUNA News & Radio Mandatory Network*) projekat. Taj projekat je još uvijek u fazi realizacije, iako je u nekim segmentima već upotrebljiv. Grubo govoreći, sastoji se od dva dijela: sistem za razmjenu živih signala i sistem za razmjenu fajlova. U upotrebi su najsavremenija rješenja za satelitsku komunikaciju, koja pripadaju takozvanom DVB-S2 (*eng. Digital Video Broadcasting-Satellite*) protokolu, koji predstavlja unapređenje DVB-S2 standarda [2]. Mreža je predviđena da prihvati budući prelaz na HD format razmjene. U planu je da sistem funkcioniše sa minimalnim učešćem lokalnih operatera. Dakle, procedura pristupa satelitu je delegirana na Ženevu, gdje je sjedište EBU-a. Sadašnji SD signal je 16:9 formata sa protokom 10,75 Mbps MPEG2 standarda.

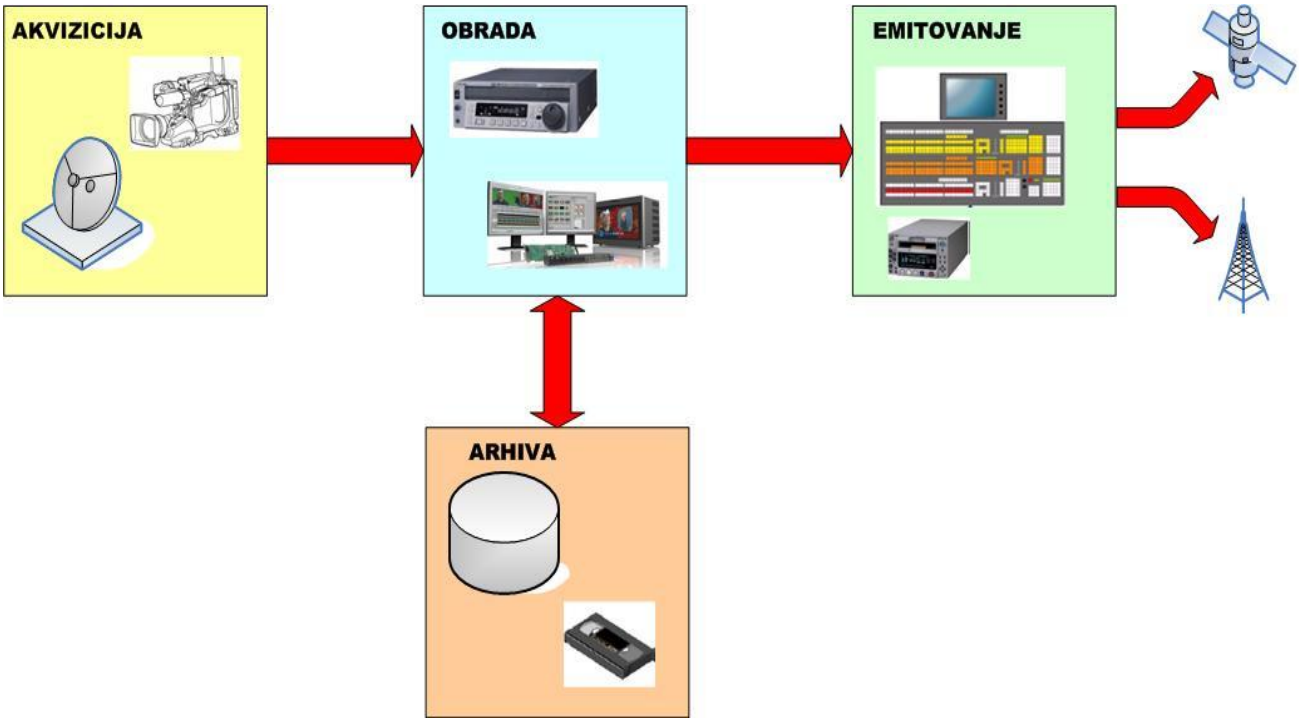
U nastavku ovog rada biće opisano trenutno stanje EVS sistema, sa osvrtom na sve funkcionalne cjeline, sagledavajući kompletnu sliku ovog sistema kroz njegove cjeline.

U savremenoj televizijskoj produkciji u upotrebi su različiti hardverski i softverski sistemi:

- Tapeless (*Digital*) *Newsroom Production* (TNP)
- *Newsroom Computer System* (NRCS)
- *Automation*
- *Media (Digital) Asset Management* (MAM, DAM)
- *Traffic system (software*)

Razvoj video servera, IT memorijskih kapaciteta, digitalne audio-video opreme stvorili su tehnološke uslove za razvoj TNP sistema. Sam razvoj je naravno praćen padom cijene komponenata i ekspanzijom jeftinijih rješenja.

Na slici 15 je dat jednostavan koncept rješenja uopštene televizijske produkcije.



Slika 15 – Koncept televizijske produkcije

U početku su video serveri bili „ostrva“ u televizijskom okruženju. Bili su zaduženi za emitovanje kratkih sadržaja, a nije postojao standardizovan način za razmjenu audio i video fajlova između montaže i servera za emitovanje.
Danas, video sistemi zasnovani na serverima obuhvataju funkcije kako playout-a tako i menadžmenta audio i video sadržaja u vidu fajlova.

Poslednjih godina trend je u konvergenciji tradicionalne televizijske i IT tehnologije. U upotrebi su standardna IT rješenja (ali poštujući izohronost, neophodnu za distribuciju video signala).

Proizvodnja informativnog programa je najzahtjevnija po pitanju brzine i potrebe da veći broj ljudi učestvuje u procesu realizacije programa. Logično je da su tapeless sistemi našli prvu primjenu u ovoj oblasti TV produkcije, direktno smanjujući potrebno vrijeme za proizvodnju programa, uz istovremeno poboljšanje kvaliteta samog programa upravo zahvaljujući značajnom vremenskom skraćivanju procesa montaže.

Da bi smo pravilno shvatili ulogu TNP sistema potrebno je sagledati sistem iz slijedećih uglova:

- Šta je cilj truda i ulaganja?
- Kako da obezbijedimo da svako u organizaciji shvati potrebu za promjenom i prihvati nov način rada?
- Da li potpuno razumijemo kako sada funkcioniše svaki segment organizacije?
- Kako će se novi sistem uklopiti u to i da li će dozvoliti proširenje u budućnosti?
- Da li želimo da sadašnji način proizvodnje vijesti uklopimo u novu tehnologiju ili da iskoristimo trenutak da izmijenimo cijeli postupak za potrebe budućnosti?

Potrebno je naobrojati sve procese neophodne u poizvodnji programa. Za svaki proces pojedinačno treba odgovoriti na pitanja koja se logično nameću (šta, ko, gdje, sa čim, kako...). Za uvođenje sistema u već postojeće TV stanice nije pitanje *da li?* Već kada i kako?

Iako se uvođenje tapeless sistema čini kao najidealnije dostupno riješenje, trake, kao primarni medijumi za snimanje televizijskog programa ipak imaju i neke dobre osobine. Neke od njih date su u nastavku:

- Traka je veoma pogodna za dodavanje dodatnog sadržaja na kaseti – ukoliko je u pitanju kraj postojećeg materijala.
- Kratak insert na traci može brzo da se prevrti i obilježi, nema potrebe da se promijeni ulazni port, izvrši trimovanje klipa i promijeni njegov naziv odnosno koristiti operacije karakteristične za serverski način rada.
- Traka je dosta spora kad treba startovati više klipova koji se brzo smjenjuju, kao hedovi, epp i sl.
- Traka, naročito analogna kao Betacam SP, je vrlo osetljiva na nove generacije. Gubi se kvalitet, javljaju se tzv. *drop-out* greške vrlo vidljive u gotovo svakoj našoj informativnoj emisiji.
- Trake moraju fizički da se premjeste iz kamere u montažu, iz montaže u emitovaje itd. Taj proces oduzima vrijeme, koje se tapeless sistemom djelimično riješavaju.

Iz svega navedenog vidi se da i pored korisnih osobina koje traka može da pruži, TNP sistem ipak nudi više:

- Veća efikasnost - isti proizvod sa manje ljudi ili veći proizvod sa istim brojem ljudi.
- Bolji kvalitet - smanjuju se gubici tehničkog kvaliteta u procesu od akvizicije do emitovanja.
- Odgovor na zahtjev tržišta za programom na televiziji, na više kanala, radiju, internetu, mobilnim telefonima.
- Bolje korišćenje audio i video materijala - proizvodnja novih izvora prihoda od postojećeg materijala.

Lako se da zaključiti da, posmatrajući trend modernizacije kvaliteta televizijskog kanala, kao glavni podsticajni faktori uvođenja TNP sistema presudni su:

- BRZINA, ubrzavanje procesa emitovanja vijesti korišćenjem prednosti produkcije zasnovane na video serverima.

- OVLAŠĆENJE, omogućavanje pristupa audio i video materijalu svakom pojedincu u produkcionom lancu (uz administratorsku mogućnost dodjele različitih prava u pogledu izmjene i/ili odobravanja) dozvoljavajući mu jednostavne ali i efektne alate za ispunjenje zadataka.

U ovom slučaju vidi se da autori dobijaju moć ali i odgovornost. Uvođenje TNP sistema, odnosno uvođenje sistema baziranih na IT tehnologiji ne umanjuje odgovornost, ne prebacuje je sa čovjeka na mašinu. Odgovornost se samo seli iz oblasti emitovanja u oblast obrade materijala.

Prije uvođenja sistema treba uzeti u obzir i navike novih gledalaca. Ipak, gledaoci bi trebali postaviti neke standarde programa. Analize pokazuju da većina gledalaca uglavnom želi češće emitovanje vijesti, detaljnije informacije o sportu i vremenskoj prognozi, promovisanje. Proces promjene je više vezan za promjenu ideja, koncepcija i radne prakse nego za instalaciju nove opreme i softvera.

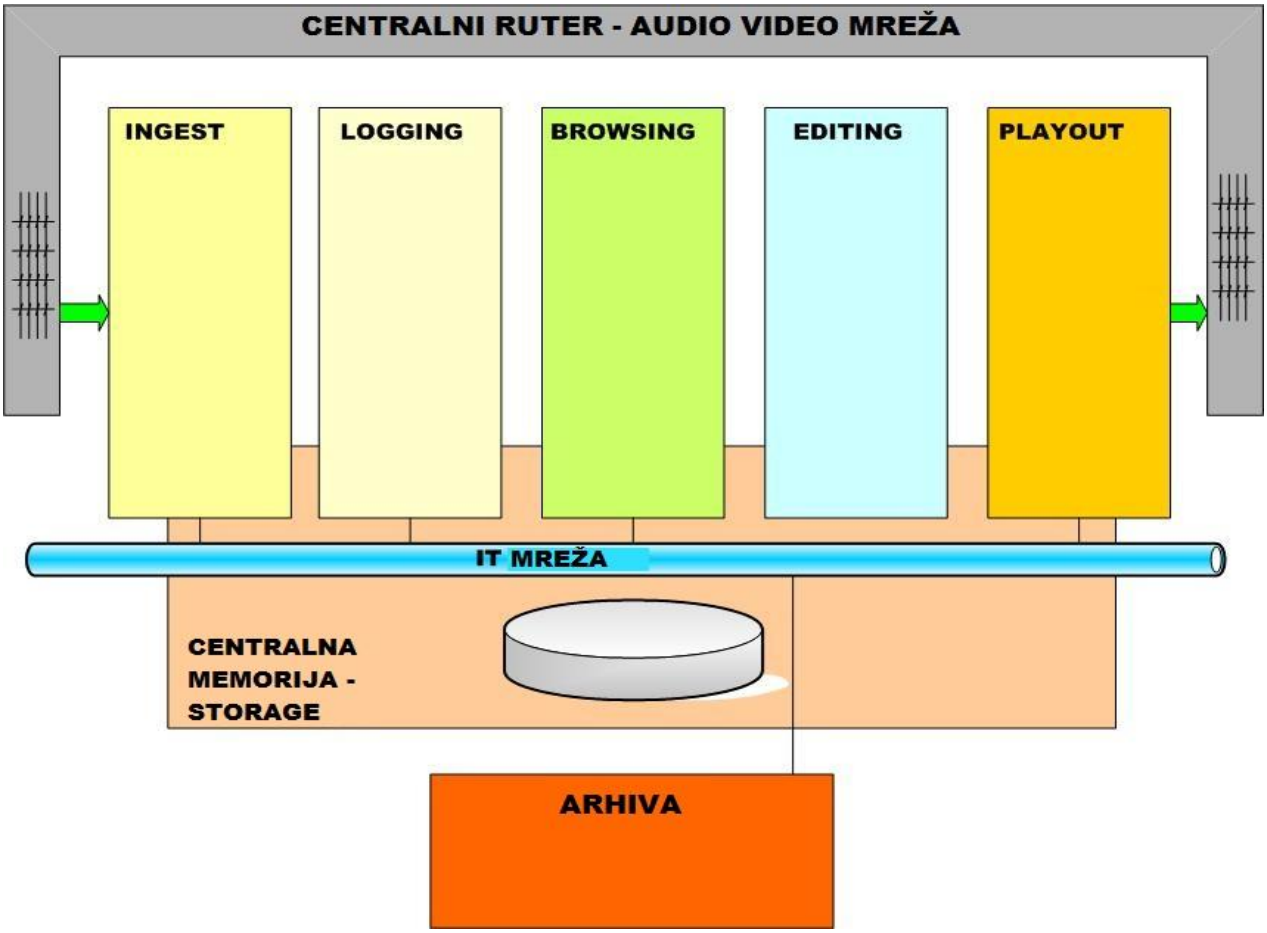
Motivacija za promjenu mora da postoji od vrha i svaki pojedinac treba da zna da menadžment potpuno vjeruje u projekat, kao i da će svako imati svoju ulogu u projektu.

3.1. Arhitektura TNP-a (Tapeless Newsroom Production)

Arhitektura TNP-a se sastoji od više elemenata:

- *Ingest* - unos materijala;
- *Logging and publishing* - indeksiranje materijala;
- *Browsing* - pregled materijala;
- *Editing* - montaža;
- *Central Storage* - centralna memorija;
- *Playout* - emitovanje;
- *Archive* - arhiva.

Na slici 16 je prikazana blok šema tapeless produkcionog sitema.



Slika 16 - Blok šema tapeless produkcionog sistema

3.1.1. INGEST - Unošenje AV materijala u sistem.

Audio i video materijal se unosi na jedan od dva načina:

1. Kao audio i video strim (video trake, satelitski eksternali, zemaljski linkovi, signali iz studija…) u sledećim formatima: SDI, embeded audio, analogni AV signali, firewire…

2. Kao media fajl (optički mediji - XDCAM , solid state memorije - P2, USB flash memorija, FTP transfer…). Media fajlovi mogu biti različitih ekstenzija, u različitoj kompresionoj šemi, različite rezolucije…

Tehnike koje se koriste prilikom unosa materijala:

- *video tape ingest (batch)* – unos materijala sa video traka,
- *scheduled ingest* – zakazivanje snimanja materijala,
- *crush recording* – unos po zahtjevu,
- *watch folder* – automatski unos video fajlova preko predhodno definisanog foldera.

Međutim, u najopštem slučaju:

1. Materijal se kodira odgovarajućom kompresionom šemom (MPEG ili DV) i upakuje u okviru odgovarajućih ekstenzija (fajl format: .avi, .mov, .mxf, .gxf, .aaf).

2. Pravi se proxy (Low-res) kopija materijala u čvrstoj relaciji (na nivou svakog frejma) sa Hi-res materijalom.

3. Materijal se smiješta na centralnu memoriju i postaje dostupan svima.

Audio i video materijal se prije unošenja u sistem odgovarajućim alatkama priprema u format koji sistem prihvata. To se radi sa aplikacijama za obradu i konvertovanje video i audio fajlova.

U okviru EVS sistema RTCG koriste se aplikacije poput Karbon Koder, TMPGEnc, Xilisoft. Za obradu audio fajlova koristi se aplikacija Easy CD-DA Extractor, koja sve audio fajlove konvertuje u format koji sistem prihvata, a koji nudi napredna podešavanja poput promjene kvaliteta enkodovanja, dodavanja ID3 tagova i promjene *bitrate*-a.

Profil za transkodovanje Hi-res video formata sadrži tehničke karektaristike (MPEG-2 PS SD@15):
Strim Format: Generic ISO MPEG strim Strim Tip: MPEG-1 sistem strim File Ekstenzija: mpg Frame rate (fps): 25.000 PAL sistem Video Bitrate: 150 000 Dimenzije: 720/576

Profil za transkodovanje Lo-res video formata sadrži tehničke karektaristike (MPEG-1 TS 1.5 Mbps):
Strim Format: Generic ISO MPEG strim Strim Tip: MPEG-1 sistem strim Fajl Ekstenzija: mpg Frame rate (fps): 25.000 PAL sistem Video Bitrate: 1500 Dimenzije: 720/576

Karakteristike audio profila koji se koristi za obradu audio materijala pilikom konvertovanja su:
Audio strim rate: MPEG-1 Audio Layer-2 Audio Bitrate (kbps): 192 kbps Sample Rate (kHz): 48.0

Sistem dozvoljava i unošenje slika ali one zahtijevaju prethodnu obradu. Sistem podržava providnost slika (*transparency*), pa tako podržava formate sa gubicima poput PNG (*eng. Portable Network Graphics)* i GIF *(eng. Graphic Interchange Format)*, kao i formate koje podržavaju kompresione metode bez gubitaka poput TIFF *(eng. Tagged Image File Format)* formata. Međutim, trenutno ograničenje sistema dozvoljava unos slike rezolucije 720x576 pixela.

3.1.2. LOGGING AND PUBLISHING - Indeksiranje materijala

Media fajl se sastoji od *metadata* podataka. Metadata zapravo predstavljaju podatke o podacima. Analogija u okviru audio domena bili bi ID3 tagovi. Metadata može da predstavlja: naziv, datum, vrijeme kreiranja, vrijeme modifikacije video fajla... Sistem omogućava hijerarhijsku podjelu metadata na kategorije koje olakšavaju pretragu. Metadata moraju biti transparentni kroz sistem i tako definisani da mogu da se filtriraju.

Osnovni element video signala je frejm. Frejmu je dodijeljen jedinstveni vremenski, tajm kod TC (*eng. Time code*). Pošto je u toku prelazni period, odnosno paralelna upotreba digitalnog sistema i video traka, *media* fajlova, word i excel dokumenata, tajm kod predstavljaju podatke koji se tretiraju na univerzalan i standardizovan način u okviru analognog i digitalnog domena.

Sistem omogućava logovanje i rad korisnika na video materijalu dok se materijal ubacuje u sistem, čime se dobija na brzini. Materijal se potom „siječe“ na manje klipove i opisuje radi lakšeg manipulisanja u kasnijem dijelu procesa, odnosno omogućavanja lakše pretrage. Za pregled materijala nije potreban VTR pregledač ili pregled u montaži, već se pregled vrši u novinarskom desku za računarom. Za efikasan rad u višekorisničkom okruženju neophodno je uvesti i poštovati izvjesne konvencije, poput pravilnog imenovanja fajla, ubacivanje metadata podataka...

3.1.3. BROWSING - Pregled materijala

Pregled i pretraga materijala vrše se nad proxy materijalom tj. materijalom koji je napravljen u niskoj rezoluciji – Lo-res fajl. Već smo spomenuli postojanje proxy-a,

najjednostavnije rečeno proxy predstavlja Lo-res repliku Hi-res klipova (800kb/s – 1.5 Mb/s).

U sistemu mora da postoji jednoznačna veza Lo-res klipa sa Hi-res verzijom materijala, odnosno svaki Lo-res klip mora sadržati istovjetni tajm kod Hi-res varijante originalnog materijala, u suprotnom sistem ne može na direktan način obraditi Lo-res fajl. Ukoliko se desi situacija da se Hi-res fajl greškom obriše ili ošteti, sistem nije u stanju da prepozna Lo-res fajl, onemogućavajući dalji rad sa Lo-res materijalom. U tom slučaju, postojanje Lo-res materijala može se iskoristiti kao novi unos kroz Ingest, naravno, sa daleko manjom rezolucijom i kvalitetom i uz učigledne gubitke nastale rekompresijom već kompresovanog materijala.

Lo-res kopije se uvode da bi se omogućio konkurentan pristup centralnoj memoriji, da bi materijal mogao da se pregleda od strane klijenata. Pristup materijalu u finalnoj rezoluciji zahtijevao bi veliku propusnu moć sistema.

Browser omogućava pretragu na osnovu metadata podataka, dodavanje ključnih (*key*) frejmova, dodavanje novih metadata (tekst za *off* komentar – potpis video materijala), jednostavna montaža i sl. Smisao uvođenja browsing podsistema je desktop pristup, odnosno omogućavanje daleko lakšeg pristupa informacijama (fajlovima) svim članovima u okviru EVS sistema.

3.1.4. EDITING – Montaža materijala

Glavne prednosti nelinearne montaže (NLE) i kolaborativnog rada u odnosu na klasičnu montažu su:

- Montaža postaje dostupna svima,
- Jednostavnost ponovnog korišćenja materijala,
- Razmjena EDL (*Edit Desicion List* - lista montažnih odluka) između montaža,
- Dodavanje off komentara.

Montaža koristi *Edit in place* tehnologiju, što znači da se proces montaže obavlja direktno na centralnoj memoriji, odnosno materijal se ne smiješta na lokalni hard disk radne stanice za montažu.

Može postojati više nivoa montaža - od *rough cut* do *craft editing*, omogućavajući brzo kreiranje klipova bez mogućnosti dodatnih tranzicionih efekata između frejmova ili klipova. Ipak, od ovakvog tipa montaže ne treba očekivati previše tj. mogućnost montaže na najvišem nivou, kao što to pružaju neki drugi profesionalni programi za montažu kao što su: FCP, Avid MC, GV Edius...

Međutim, upravo su te karakteristike one koje odvajaju ovaj proces montaže od ostalih u odnosu na profesionalne pakete za montažu, stavljajući akcenat na osnovnim karakteristikama poput:

- Brzine
- Jednostavnosti
- Opcija ograničenih za potrebe *news* produkcije

Rezultat montaže je potvrđena EDL razmjena ili nalog za eksport (konsolidaciju materijala). Izmontirana sekvenca se objavljuje tj. registruje u bazi podataka, i kao takva postaje dostupna za pregled, kontrolu, odobravanje i emitovanje.

3.1.5. PLAYOUT - Emitovanje

Playout aplikacija kontroliše izlazne A/V kanale sistema. Materijal se učitava iz centralne memorije ili lokalne memorije Playout servera, dekoduje i postaje AV signal – stream.
Aplikacija radi sa klipovima i plejlistama, odnosno skupovima klipova koji su u određenom odnosu (4:3 i 16:9) i mogu imati određena svojstva u vezi sa emitovanjem (crni ekran nakon završetka zadnjeg frejma klipa, prikaz narednog klipa, zaustavljanje na frejm narednog klipa itd.).

Osnovne mogućnosti playouta:

- Broj kanala koje kontroliše
- Mogućnost pregleda materijala
- Unošenje i kreiranje plejlista
- Pretraga i priprema klipova za emitovanje

- Kontrola toka emitovanja plejliste (osnovne kontrole, lančano emitovanje, naizmjenično, emitovanje u petlji, prozivanje eksternih uređaja...).

3.1.6. CENTRAL STORAGE - Centralna memorija

Centralna radna memorija predstavlja najbitniju stavku svakog velikog sistema. Njene karakteristike moraju biti takve da omogućava veliko skladištenje podataka, veoma brz odziv i veliku propusnu moć, tako da istovremeno omogućava što većem broju korisnika pristup sistemu.

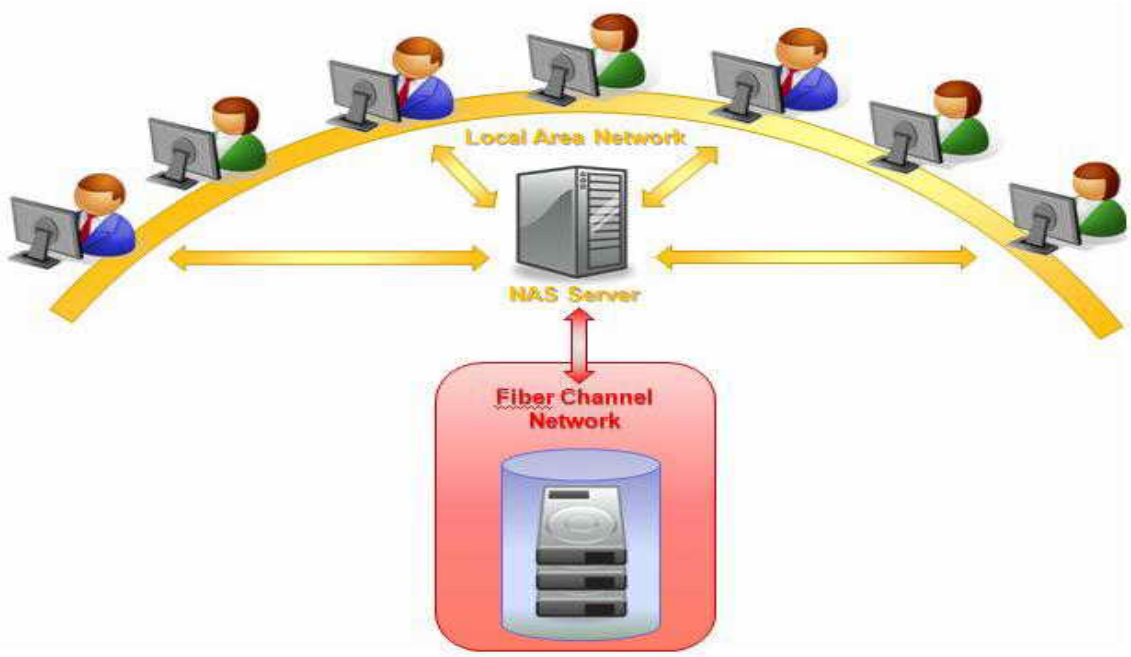
Trenutno stanje centralne memorije EVS sistema RTCG je kapacitet od 14 TB, što i neomogućava pretjerano veliko skladištenje materijala enkodovanih u HD formatu. Problem skladištenja bio je očigledan tokom prenosa Svjetskog prvenstva u Brazilu 2014, gdje se enkodovalo istovremeno par utakmica u HD formatu sa velikim *bitrate*-om.

Veliki skladišni kapacitet je dodat radnim stanicama preko:

- DAS (*eng. Direct Attached Storage*) – odnosi se na digitalni sistem koji je direktno zakačen na server ili radnu stanicu bez serverske mreže između. Uglavnom se koristi za razlikovanje neumrežene serverske veze iz koncepta SAN i NAS.

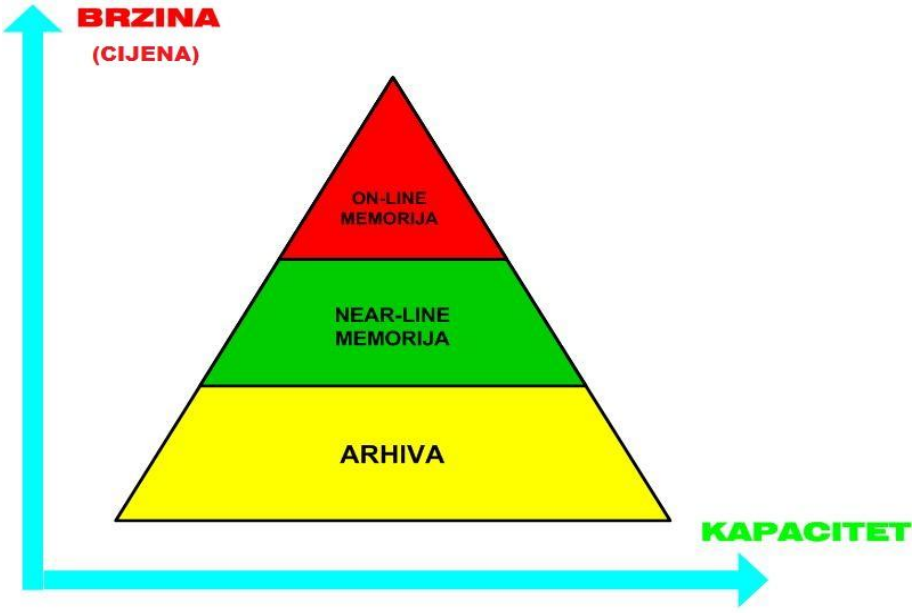
- NAS *(eng. Network Attached Storage)* - je baziran na fajl nivou skladištenja podataka. Server je povezan računarskom mrežom koja obezbjeđuje pristup podacima u heterogenoj grupi klijenata (slika 17). NAS je specijalizovani računar izgrađen u cjelini za skladištenje i serviranje fajlova. Povezan je sa mrežom koja samo pruža fajl servise drugim uređajima na mreži. Video materijalu na diskovima se pristupa direktno preko TCP/IP mreže.

- SAN *(eng. Storage Area Network)* - Svi diskovi su zasebna cjelina. Da bi se pristupilo diskovima, prvo se šalje zahtjev kontrolnoj stanici. Svi korisnici sistema vide centralnu memoriju kao jedan veliki lokalni disk. Povezivanje SAN uređaja sa serverima vrši se preko optičkog kabla.



Slika 17 – Pristup klijenata NAS serveru

Bitna napomena je da centralna memorija ne služi za trajno smještanje materijala već za istovremeni brz pristup većeg broja klijenata istim podacima, za skladištenje materijala upotrebljavaju se eksterni medijumi poput magnetnih traka, odnosno arhiva za materijale koji se u bliskoj budućnosti ponovo mogu pozvati.



Slika 18 - Hijerarhija memorijskih kapaciteta

Na slici 18 je prikazana hijerarhija memorijskih kapaciteta.

Osnove karakteristike centralne memorije su: kapacitet, održavanje, struktura (RAID) i skalabilnost.

3.1.7. *ARCHIVE* - Arhiva

U prošlosti, kada je arhiva bila zasnovana na video trakama postojale su police, naljepnice, prateće etikete i u boljim slučajevima bar kod oznake i baza podataka. Uvođenjem *tapeless* radnih procesa arhiva se može smjestiti u okviru lokalnog hard diska, eventualno na magnetnim trakama u digitalnoj formi, ćime se pristup digitalnim podacima znatno ubrzava, omogućavajući arhiviranje daleko većeg broja materijala.

Magnetne trake čine se kao najidealnije riješenje za skladištenje materijala jer se podaci na trakama zapisuju direktno u digitalnoj formi ali same trake zahtijevaju određene sobne uslove za dogutrajno skladištenje tih podataka. Pored toga veoma su osetljive na magnetno polje, a njihova cijena je veoma visoka.

Tipična arhitektura arhive:

- RAID array - nearline storage
- LTO biblioteka - offline storage.

Softver za upravljanje arhivom (*Archive Manager Software*) posreduje između medija centralne memorije i MAM (*eng. Media Asset Management*). Mogu postojati Lo-res kopije arhiviranog materijala dostupne preko MAM učesnicima u produkcionom procesu. U arhivi se nalaze i Hi-res verzije medija.

Razlikujemo dva procesa u arhiviranju materijala:

- Transkodovanje u odgovarajući fajl format;
- Premještanje fajlova.

Čuvanje podataka može se vršiti na različitom mediju:

- Magnetni (disk ili traka);
- Optički disk;
- Solid state memorije.

3.2. Konfiguracija rješenja TNP-a

U Radio Televiziji Crne Gore je implementirano EVS-ovo integrisano rješenje za TNP. U nastavku rada analiziraće se sistem sa stanovišta hardverske i aplikativne (softverske) platforme.

Slika 19 – Logo EVS kompanije

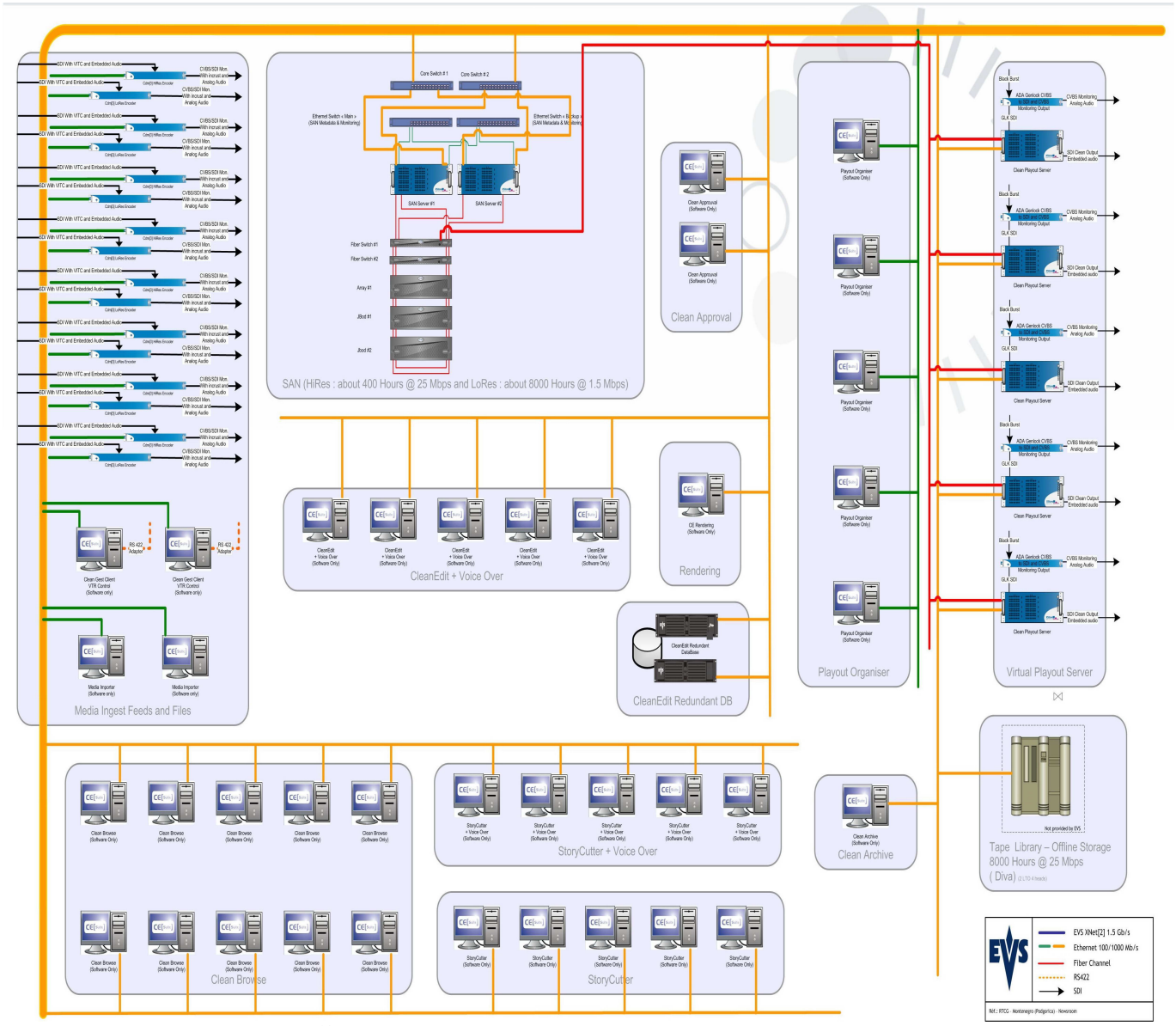
3.2.1. Hardverski sloj (platforma)

Hardverska platforma se zasniva na standardnoj IT tehnologiji i infrastrukturi i sopstvenom razvoju samo u dijelu platforme koja predstavlja vezu sa postojećom televizijskom video i audio infrastrukturom.

To praktično znači da je ovakav sistem veoma otvoren i da životni ciklus (implementacija, korišćenje, održavanje i nadogradnja) takvog sistema neće biti zavisan niti sputavan od trenutne sposobnosti razvoja spefičnih komponenti.
Sistem je zasnovan na jasno definisanim standardnim hardverskim komponentama, opšte prisutnim na IT tržištu i samim tim i lako dostupnim i zamjenljivim.

Trenutna konfiguracija sistema sadrži ukupno 65 računara, od čega 25 računara predstavljaju korisničke radne stanice a ostalih 40 računara su rezervisani za serverske potrebe.

Na slici 20 se nalazi šema hardverske konfiguracije sistema u RTCG.



Slika 20 – Šema hardverske konfiguracije sistema u RTCG

Sa slike 20 se vidi da je EVS sistem u RTCG podijeljen u različite cjeline:

- Centralna djeljiva memorija

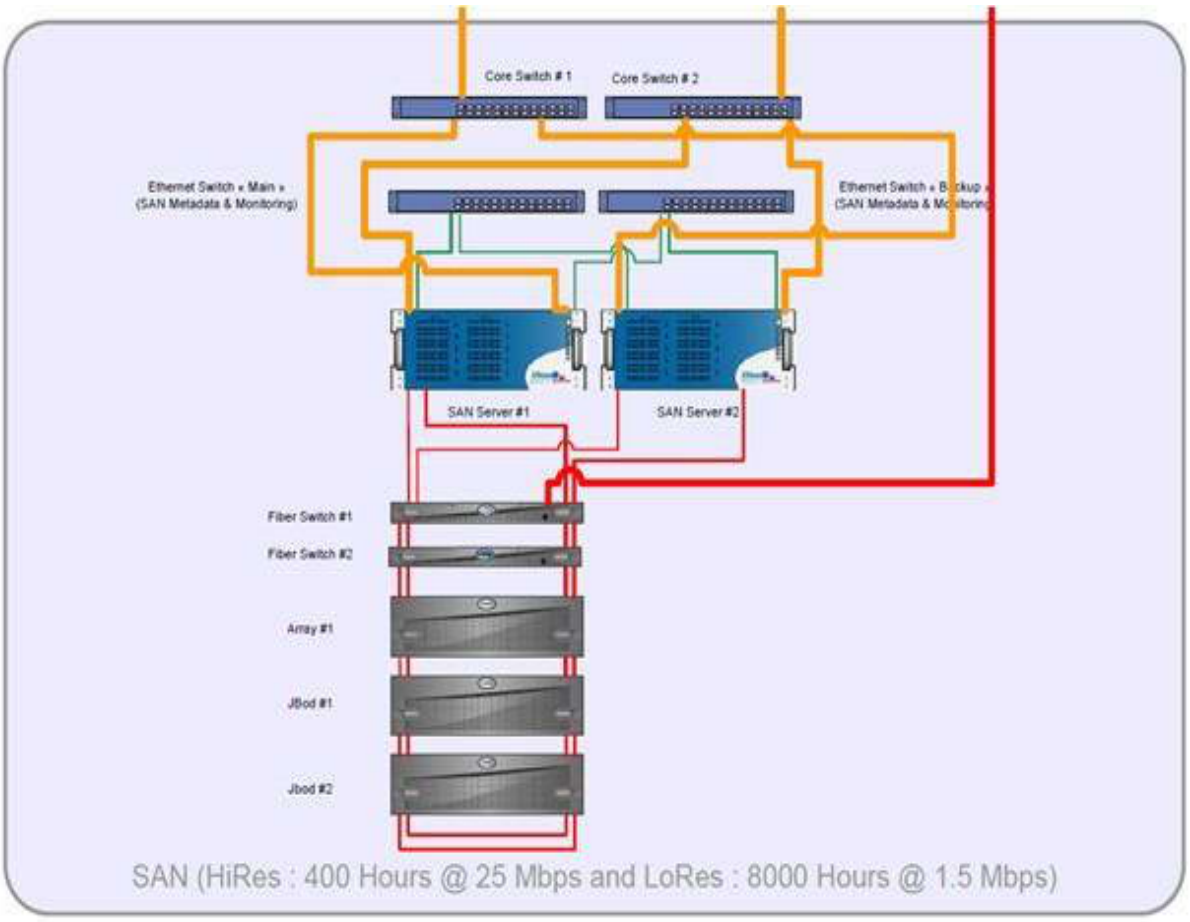
- Podsistem za unos audio i video materijala
- Podsistem za pregled i montažu materijala
- Podsistem za emitovanje
- Centralizovana arhiva audio i video materijala

Centralna djeljiva memorija je srce sistema i tehnološki je najzahtjevniji dio sistema. Baziran je na SAN tehnologiji i FC (eng. fiber channel) optičkom interfejsu.

Neke od prednosti SAN centalne memorije su:

- Velika pouzdanost hardvera
- Protok od 4Gbps po portu
- Mrežni protokoli su optimizovani za *streaming*
- Podržava više RAID nivoa
- Omogućava agregacije bez obzira na lokaciju diska
- Podržava različite disk tehnologije (SATA i FC) kao i veličine diska
- Podržava *HOT SPARE* sistem – jednostavno mijenjanje problematičnih diskova
- Podržava particioniranje

Na slici 21 prikazana je konfiguracija koja garantuje dodatnu pouzdanost u radu i sigurnost podataka.



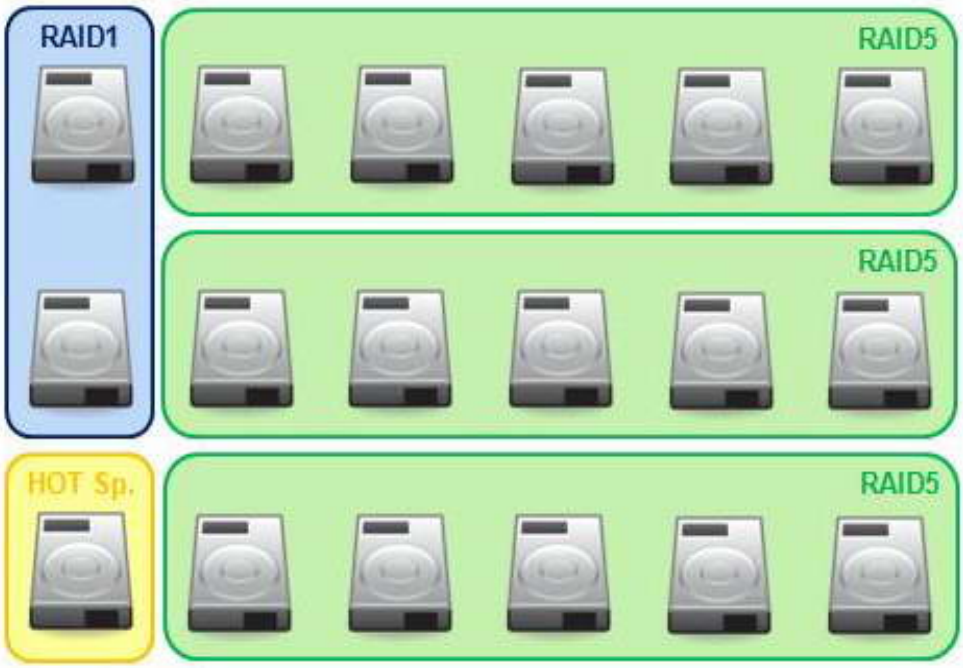
Slika 21 – Šema centralnog djeljivog storidža

Sistem se u ovom slučaju sastoji od tri reka sa diskovima. U jednom reku je postavljeno 16 diskova, što znači da ukupno u sistemu postoji 48 takvih diskova. Pojedinačni kapacitet jednog diska iznosi 300 GB, dok ukupan prostor na diskovima iznosi 14 TB.

Pomenuli smo da se u sistemu nalaze tri reka sa diskovima, od kojih je jedan onaj koji sadrži RAID *(eng. Redundant array of inexpensive disks)* kontrolere takozvani pametni rek. On je na slici 21 pikazan pod oznakom array1 i dva ostala *slave* reka pod oznakom *jbot*.

Diskovi su grupisani u RAID sistemu u više nivoa. RAID tehnologija skladištenja kombinuje više komponenti diskova u logičku jedinicu radi redudantnosti podataka i poboljšanja performansi. Podaci se distribuiraju preko diskova na više načina, koji se odnosne na RAID nivoe u zavisnosti od specifičnog nivoa

redudantnosti i željenih performansi. Na slici 22 su prikazani neki od tipova RAID nivoa koji se koriste u centralnoj memoriji.



Slika 22 – RAID nivoi

Konkretno kod RTCG sistema u upotrebi je RAID 0 nivo, sa ciljem združivanja diskova i pravljenja jednog diska velikog kapaciteta. RAID 0 ne doprinosi redudantnosti i ne doprinosi dodatnoj toleranciji na greške.

Osim RAID 0 koristi se RAID 4+1 nivo od 4 diska koji je zadužen za podatke, kao i petog diska koji je kontrolni disk. RAID 4 omogućava skladištenje parnosti podataka na jednom od dodijeljenih diskova. U sistemu je takođe prisutan i RAID 5+0 nivo. To je grupa od po 5 diskova i nula koja se koristi za spajanje. Suprotno od RAID 4, parnost informacija je distribuirana između diskova. On zahtijeva da svi diskovi sem jednog budu operativni, i ukoliko se desi kvar, odnosno otkazivanje jednog diska slijedeće se čitanje može izračunati iz distribuirane parnosti tako da nijedan podatak ne bude izgubljen. Podaci se upisuju na diskovima tako što se vrši fragmentiranje fajlova, tako da se na svaki disk upisuje blok podataka po jednoj iteraciji.

Pored RAID nivoa diskova koriste se i SPARE (rezevni) diskovi. Kada fizički disk otkaže rezevni disk preuzima sve podatke od otkazanog diska i u potpunosti preuzima njegovu ulogu. U tom slučaju od kontrolnog diska u RAID nizu dobija

informacije o pokvarenom disku, nakon čega regeneriše podatke i šalje na SPARE disk.

Rekovi su između sebe povezani optičkim kablovima na optičke svičeve. Veza SAN servera sa diskovima je takođe preko optike. Klijent stanice pristupaju video fajlovima koji se nalaze na diskovima kroz SAN server.

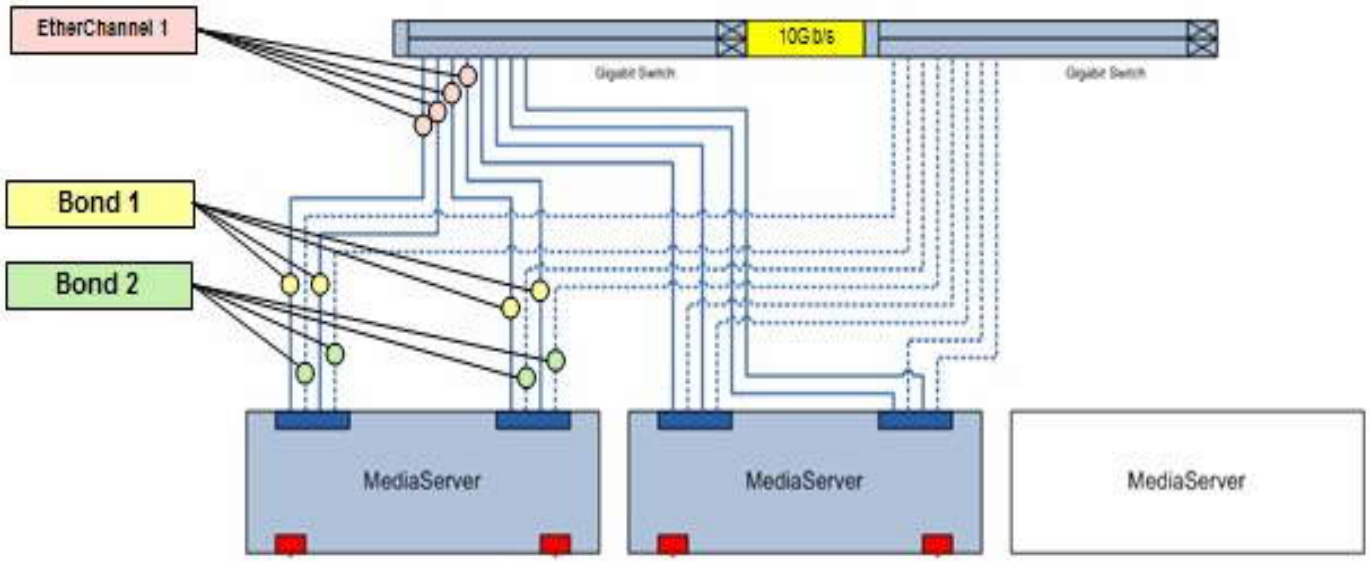
Pristup diskovima na SAN serveru se ostvaruje preko dva CORE sviča. Da bi se povećao propusni opseg, veza servera sa CORE svičevima je ostvarena preko osam gigabitnih mrežnih kartica. Druga dva sviča sa slike 21 su EDGE svičevi koji služe za kontolu i menadžment.

SAN server ima svoju bazu na nekom od hard diskova u kojoj se nalaze sve informacije o fizičkim lokacijama fajlova i oni se nalaze u RAID 1 nivou. Kod RAID 1 redudantnost se postiže jednostavnim dupliranjem svih podataka. Koristi se klasifikacija podataka tako da je svaka logička traka preslikana na dva posebna fizička diska, svaki disk u nizu ima svoj disk (MIRROR) koji sadrži iste podatke. Hard diskovi svih značajnijih uređaja u sistemu (uređaji za emitovanje, za snimanje materijala...) su duplirani tj. nalaze se u RAID 1 nivou.

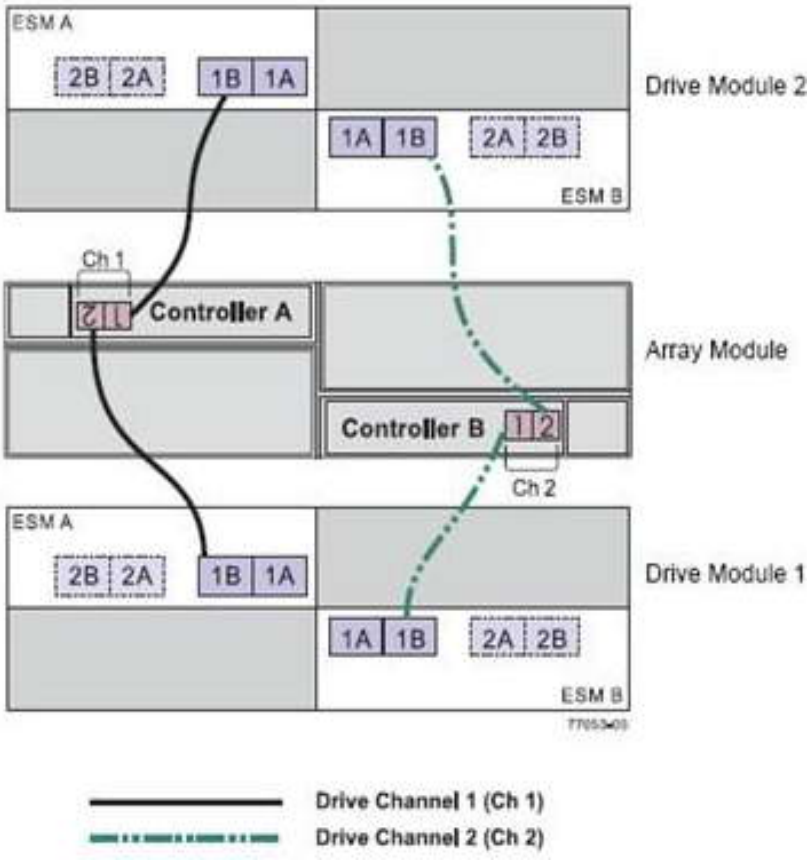
Cijeli sistem pa i SAN memorija je osmišljen da je redudantan, što znači da u slučaju otkaza ili kvara jednog medija servera saobraćaj će se prebaciti na sekundarni medija server. Sekundarni media server tada uz pomoć specijalnih algoritama dobija status primarnog servera i preuzima njegovu ulogu. CORE svič je zadužen za rutiranje, tj. promjenu rute u slučaju kvara primarnog media servera.

Na slici 23 i slici 24 se vidi kako je ostvarena redudantost sa SAN serverom. Oba media servera su duplim linijama povezana međusobno i sa jednim i sa drugim CORE svičem.

Media serveri su pod *Linux RedHat* operativnim sistemom. Servis *deamon* ima ulogu konstantnog provjeravanja dostupnosti primarnog media servera. Ako zaključi da je nedostupan, odmah odrađuje rezervnu konfiguraciju. U jednom trenutku se koristi samo jedan media server, dok je drugi uvijek u *stand by* modu.



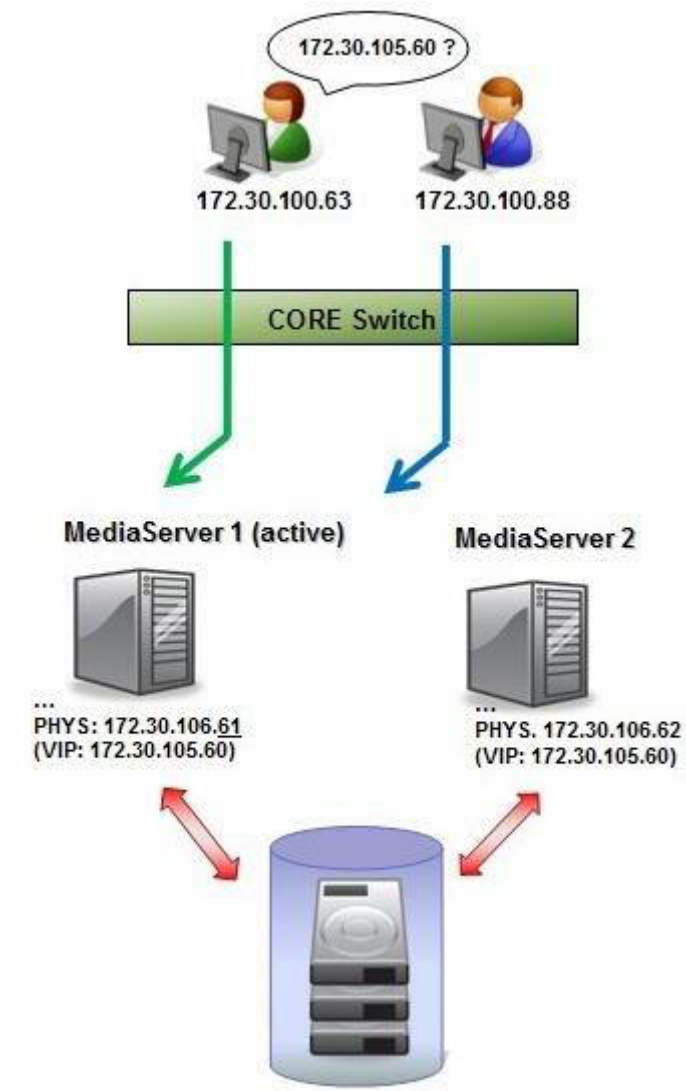
Slika 23 – Redudanta veza sa SAN serverom



Slika 24 – Redudantna veza sa SAN serverom

Medija serveri osim što imaju fizičke IP adrese, imaju i svoju virtualnu IP adresu, sto im omogućava da budu dostupni preko iste virtuelne IP adrese. Mreža je napravljena tako da omogućava raspodjelu opterećenja saobraćaja (*load balansing mode*).

Na slici 25 je prikazana ilustracija postavljanja virtuelne IP adrese na media serverima.



Slika 25 – Ilustracija postavljanja virtuelne IP adrese na media serverima

Neke od karakteristike Media Servera:

- 2 x 4 portni Eternet adapteri
- 2 x 1 port Host Bus adapter
- RAID 1 zaštita diskova + Hot Spare diskovi
- Redundanto napajanje i ventilatori za hlađenje
- Hot Spare RAM memorija

Neke od karakteristika kućišta za kontrolere (*Controller Enclosure*) - Dupli Kontroler:

- 2 x RAID kontroler
- I/O Zaštita lokacije podataka (*2 x Drive Loops + 2 x 4 Host Loops*)
- Direktna zamjena modula
- Zaštita baterija
- Redundantnost napajanja i ventilatora za hlađenje

Neke od karakteristika kućišta za diskove (*Disk Enclosures*):

- 2 x ESM
- 2 x Drive Loops
- RAID zaštita diskova + Hot spare diskovi
- Redundanto napajanje i ventilatori za hlađenje

Klijent - Server arhitektura omogućava ravnopravni i uniformni pristup podacima sa svih radnih stanica unutar sistema. Ovo je bitno sa stanovišta svih radnih procesa jer čini da su radne stanice unutar mreže (hardverski) ravnopravne, a da se vrsta procesa definiše na aplikativnom nivou. Takođe, sama SAN struktura, ima svoje servere koje čuvaju fajl sistem na dijeljenoj centralnoj memoriji, tako da svaki SAN klijent koji pristupa dijeljenoj memoriji, prvo mora da se „obrati“ za pristup serverima, pa tek onda može da preuzima fajlove sa same dijeljene memorije. Računarska mreža je standardna IT infrastruktura koja obezbjeđuje fizičku vezu između računara i servera. Zahtjevi koje ispunjavaju za uspešnu realizaciju mreže su sasvim jednostavni i na nivou su „običnih“ mreža koje nalazimo u drugim „kancelarijskim“ informacionim sistemima.

Podsistem za unos audio-video materijala (Ingest) je dio sistema koji se nalazi na početku radnih procesa za proizvodnju programa. Uslovno možemo ga podijeliti na tri dijela:

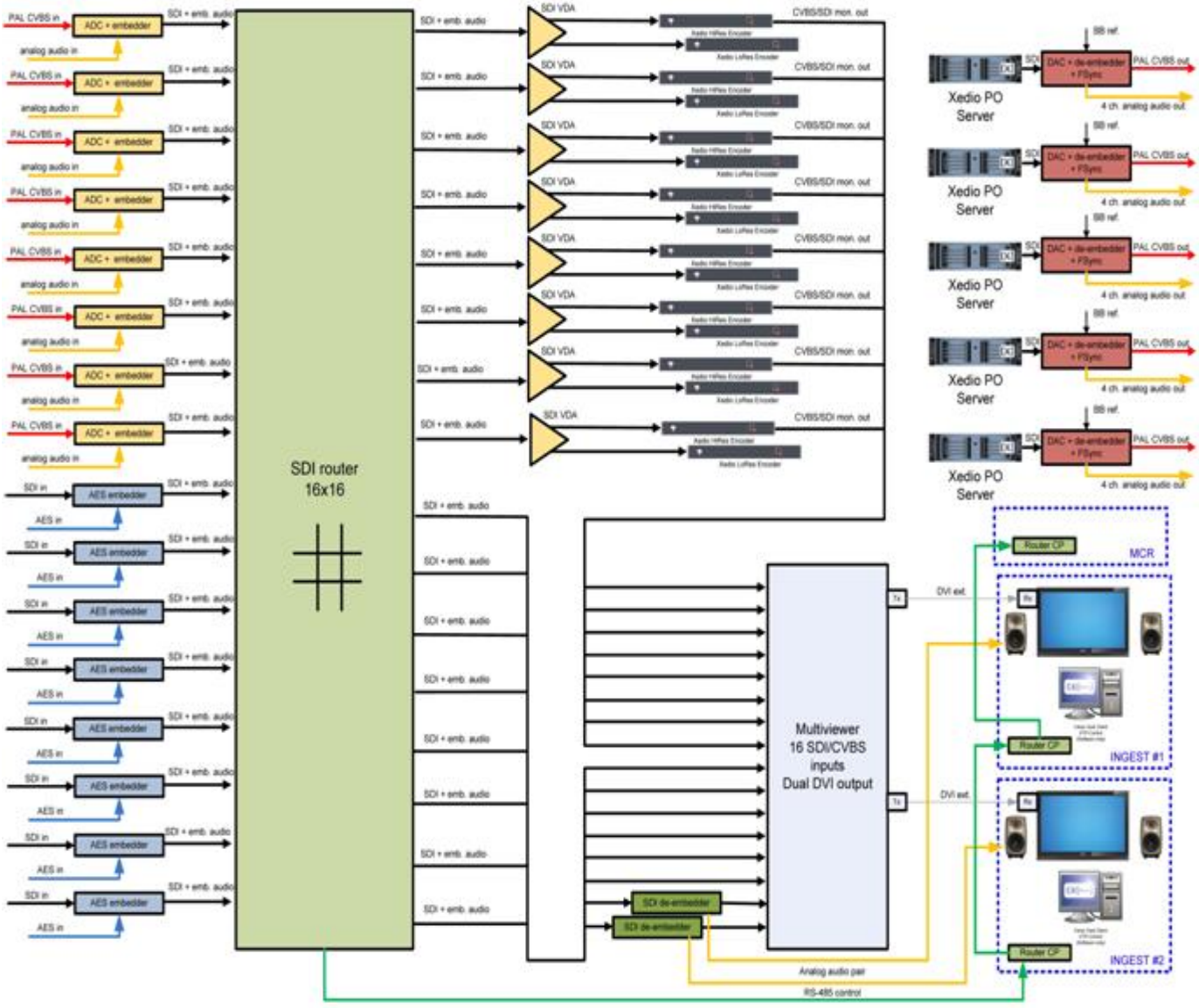
- Audio-video interfejs (enkoderi, matrica, izvori signala - VTR-ovi, sateliti, ostalo),
- Fajl sistem interfejs,
- Radne stanice za kontrolu procesa.

Na slici 26 je prikazana šema veze ingest podsistema, gdje su prikazani ruteri, konvertori i sistem za kontolu slike.

Postojeći analogni signali i njihova veza sa digitalnim enkoderima je ostvarena preko matrice tj. AD/DA konvertora marke Crystal Vision – Indigo 4. Na slici 26 je prikazan SDI ruter koji služi za rutiranje signala. Na ulazima i izlazima se nalazi SDI (*eng. Serial Digital Interface*). Na ulazima od rutera dolaze razne vrste video signala kao što su signali sa BETA mašina, satelitski signal i svi signali koji su potrebni sistemu.

Kod analognih signala video i audio se nalaze u odvojenim kanalima i da bi se na izlazima dobio digitalni signal SDI konvertori vrše njihovo spajanje. Primljeni digitalni signal koji se dobijaju na izlazima konvertora se dalje šalju na enkodere preko kojih se vrši unos materijala.

Na kraju procesa se uz pomoć konvertora odrađuje konverzija iz digitalnog u analogni signal, jer ostatak opreme u TVCG još uvijek nije digitalizovan. Sa *playout* servera se emituje digitalni signal, nakon čega se vrši njegovo konvertovanje u analogni signal radi dalje distrubucije u režijama.

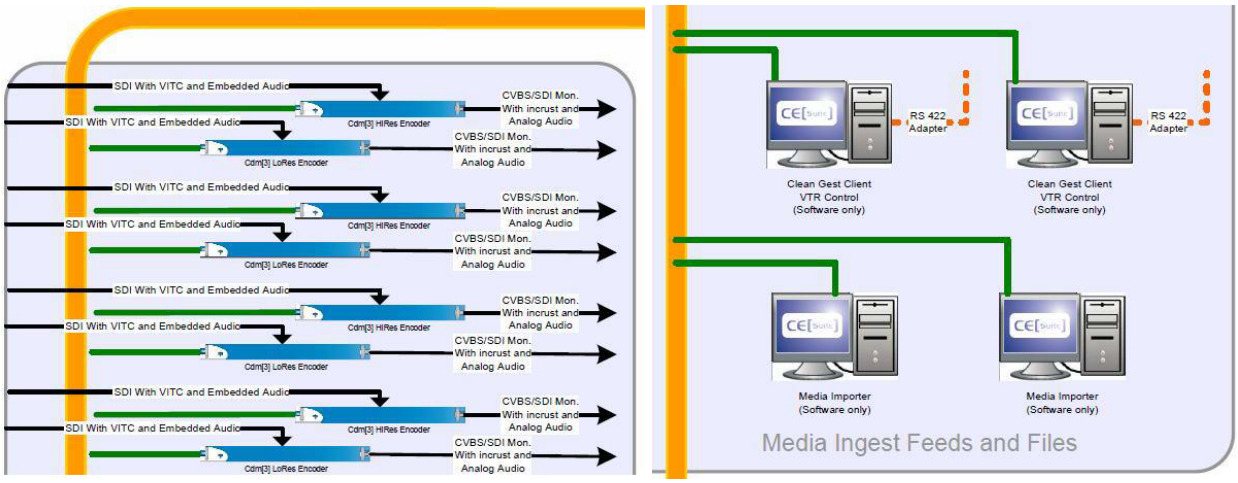


Slika 26 – Šema Ingest podsistema (ruter, konvertori i kontrola slike)

U sistemu se koristi uređaj Predator - Harris II, koji služi kao 'multiviewer' za kontrolu i monitoring slike. Uz njega je povezan i jedan kontrolni PC računar preko koga se sa odgovorajućom aplikacijom kontroliše sam rad i podešavanja

multiviewer-a. Na *multiviewer* tehnički mogu da se dovedu razni signali ali konkretno u ovom sistemu su dovedeni samo signali sa *playout*-a.

Na slici 27 je prikazan dio podsistema za unos audio-vido materijala (*ingest*). U sistemu postoji 16 enkodera. Od toga su 8 enkodera predviđeni za pravljenje Hi-res fajlova, a ostalih 8 za pravljenje Lo-res materijala.



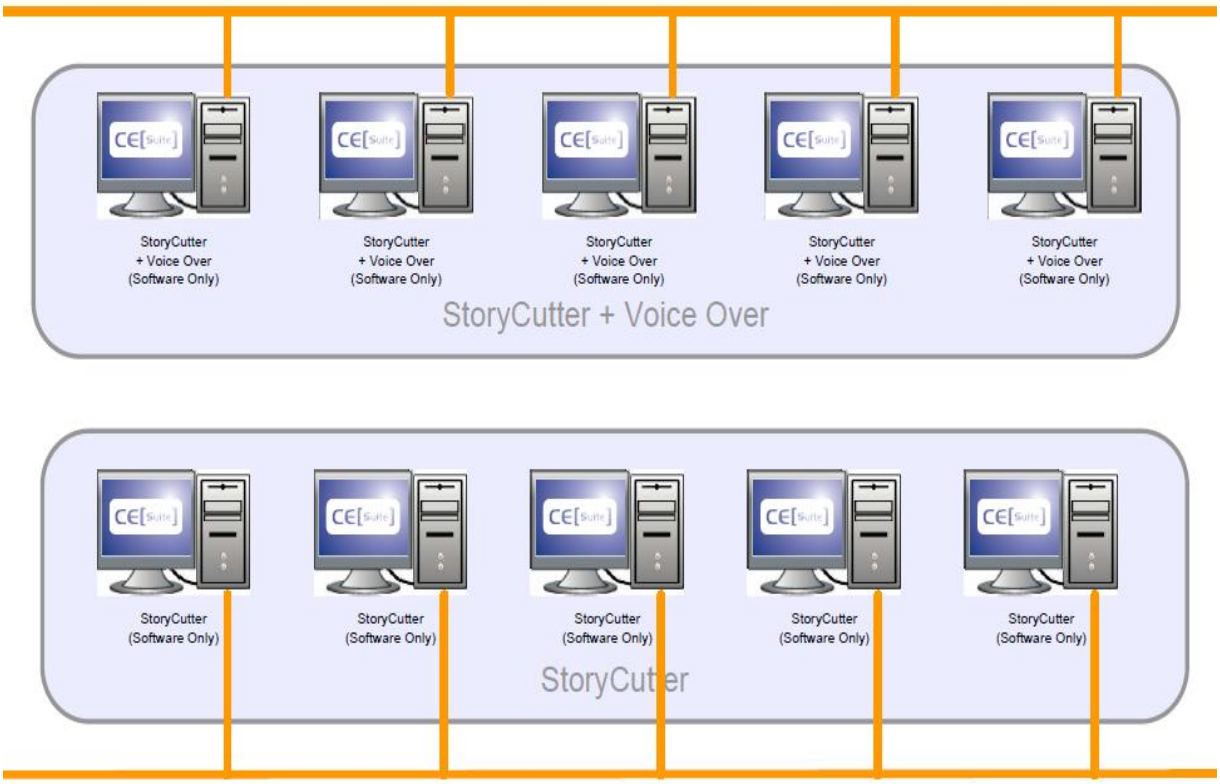
Slika 27 – Šema podsistema za unos audio-video materijala

Podsistem za pregled i montažu je dio sistema koji je zadužen za proizvodnju programskih sadržaja. Sastoji se iz nekoliko vrsta radnih stanica:

- Stanice za pregled materijala
- Stanice za pregledanje materijala i montiranje na bazi jednostavnih (osnovnih) softverskih mogućnosti
- Stanice za pregledanje materijala i montiranje na bazi jednostavnih (osnovnih) softverskih mogućnosti, uz mogućnost dodavanja glasovnih sadržaja (*voice over*)
- Stanice za montažu na bazi složenijih softverskih mogućnosti, uz mogućnost dodavanja glasovnih sadržaja (*voice over*)
- Stanice za pregled gotovih materijala i njihovo odobravanje za upotrebu

Na slici 28 je prikazan dio podsistema za pregled i montažu. U sistemu za video montažu postoji 10 korisničkih stanica koje mogu da se koriste istovremeno.

Sistem funkcioniše na principu dodijeljivanja tzv. licenci, pri čemu se jedna licenca istovremeno može iskoristiti samo na jednom računaru. Broj licenci kojima RTCG raspolaže je deset, što omogućava istovremeni rad na 10 računara.



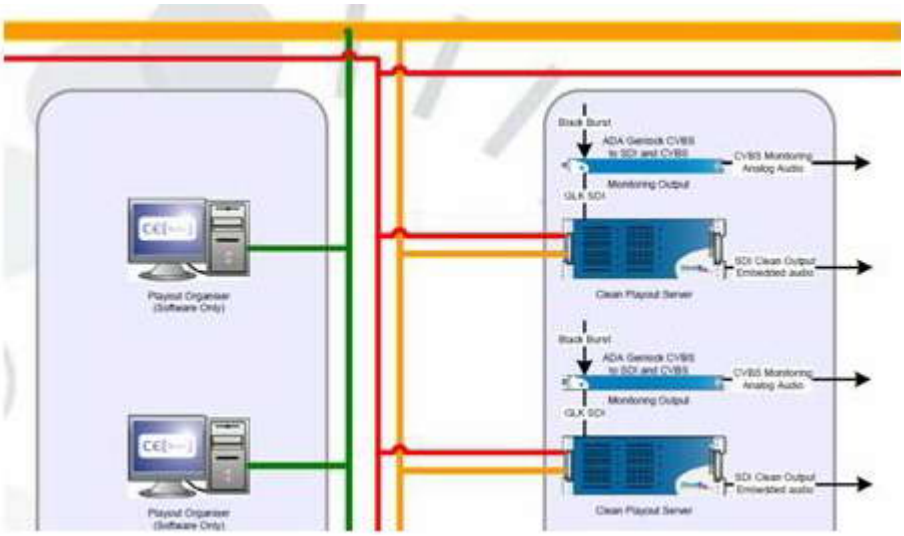
Slika 28 – Šema podsistema za pregled i montažu

Podsistem za emitovanje je dio sistema koji obezbjeđuje da se pripremljeni programski sadržaji pošalju na upotrebu (reprodukciju). Nije upotrijebljen izraz emitovanje, jer sadržaji najčešće i ne idu direktno u „etar“, već se šalju u video režije gde su samo jedan od mogućih izvora signala u produkciji informativnih emisija.

Ovaj dio se sastoji od dva dijela:

- *Playout* serveri,
- Radne stanice za kreiranje *play list*-i i kontrolu *playout* servera.

U sistemu postoje 5 *playout* servera i 5 *playout* korisničkih stanica.
Na slici 29 je prikazan dio podsistema za emitovanja.



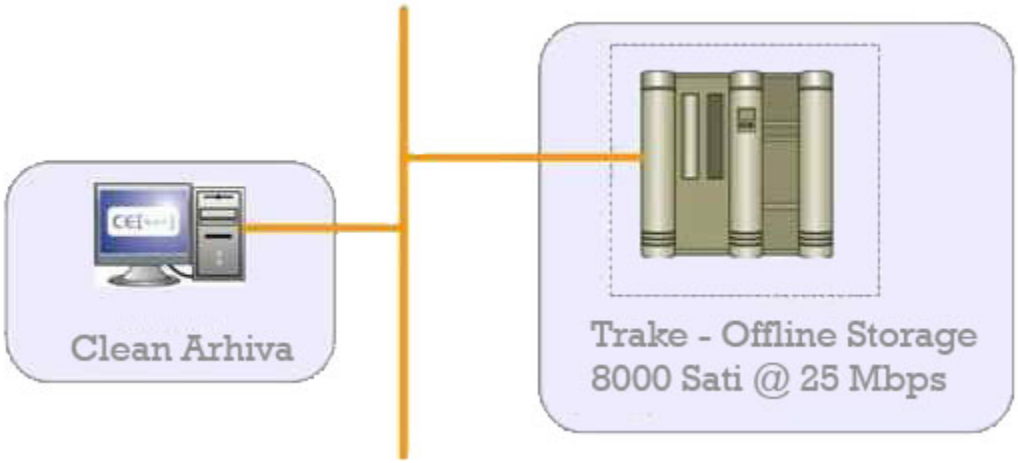
Slika 29 – Šema podsistema za emitovanja

Playouti su optikom direktno vezani na SAN centralnu memoriju i na taj način efikasno i brzo povlače video fajlove koje emituju.

Centralizovana arhiva audio-video materijala je dio sistema koji se nalazi na kraju, ali i na početku radnih procesa za proizvodnju informativnog programa. Osnovni zadatak koji treba da ispuni je da trajno sačuvaju audio, video i druge sadržaje koje mogu ponovo zatrebati u proizvodnji programa.

Hardverski gledano, ovo je IT baziran podsistem organizovan na skoro istovjetnoj topologiji kao i produkcioni dio.

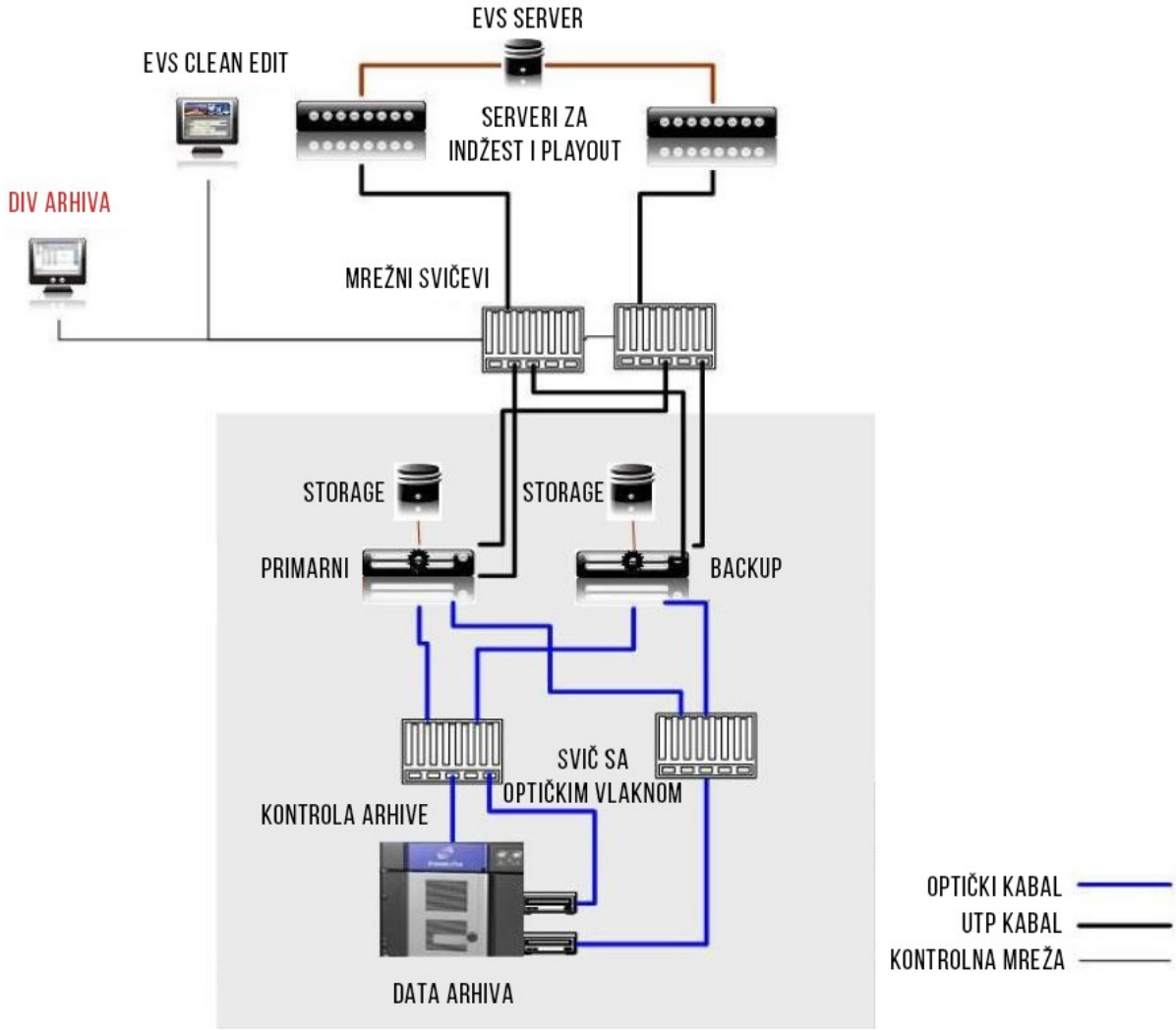
Na slikama 30 i 31 je prikazana šema centralizovane arhiva AV materijala.



Slika 30 – Šema centralizovane arhive AV materijala

Djelovi arhive su:

- Centralna biblioteka sa robotikom (*Data Archive Library*),
- SAN interfejs,
- Fajl serveri,
- Privremena memorija ubrzanje pristupa i snimanje podataka (*Nearline Archive*),
- Radna stanica za administriranje.



Slika 31 – Šema mreže centralizovane arhive

Tip traka koje se koriste u arhivi su LTO4 *(eng. Linear Tape Open)* digitalne trake. One se nalaze u kućištu kapaciteta do 100 traka. Veličina jedne trake je kapaciteta 800 GB. U kućištu postoje dva robota koji rade sa trakama (fizički uzimaju i

premještaju trake). Postoje i dva čitača traka tj. čitač video materijala koji se nalazi na LTO trakama.

Sa slike 31 se vidi da u sistemu arhive postoje dva server računara namijenjena arhivi, glavni i pomoćni server, koji uz pomoć posebnih aplikacija kontrolišu sam rad arhive. U reku osim LTO traka, čitača traka, robota za manipulaciju traka se nalazi i desetak hard diskova ukupnog kapaciteta 10 TB. To su 'offline' diskovi koji se koriste kao privremena arhiva. Služe za privremeno skladištenje fajlova koji se češće koriste u sistemu, a sve radi bržeg pristupa istim. Sistem omogućava automatsko prepoznavanje tih diskova.

Fajlovi se na trakama upisuju redom, jedna za drugom. U slučaju da dodje do brisanja nekog fajla između unešena dva fajla, nova informacija se ne može upisati između. Upisuje se jedino nakon upisa poslednjeg fajla. Takođe, sistem dozvoljava defragmentaciju. U tom slučaju se vrši proces preuređenja i objedinjavanja fragmentiranih fajlova.

Skalabilnost DIVA Arhive:

- Nema ograničenja u kapacitetu,
- Alarmi se generišu kada se dosegne kraj trenutne sposobnosti,
- Niz diskova (*array*) se može naknadno dodavati,
- Naknadno dodavanje trake - robot biblioteke,
- Nema ograničenja u propusnom opsegu,
- Dodavanje *Actor* servera ukoliko je potrebno bez zaustavljanja sistema,
- Dodavanje drajv traka ukoliko je potrebno,
- Filtriranje u aplikacijama se može primijeniti,
- Nema ograničenja u broju izvora/odredišta koji se mogu obratiti DIVA arhivi.

Veza sa produkcijskim sistemom na fizičkom nivou je e*ternet* mrežna konekcija. Mreža arhive je ostvarena preko optike i optičkih svičeva.

Arhiva ima mogućnost exporta i importa materijala. To je omogućeno preko robot biblioteke. Takođe arhiva ima mogućnost da se odgovarajući DIVA arhiv metapodatak izvozi u zasebnu datoteku.

U tabeli 4 je prikazana arhitektura DIVA Arhive.

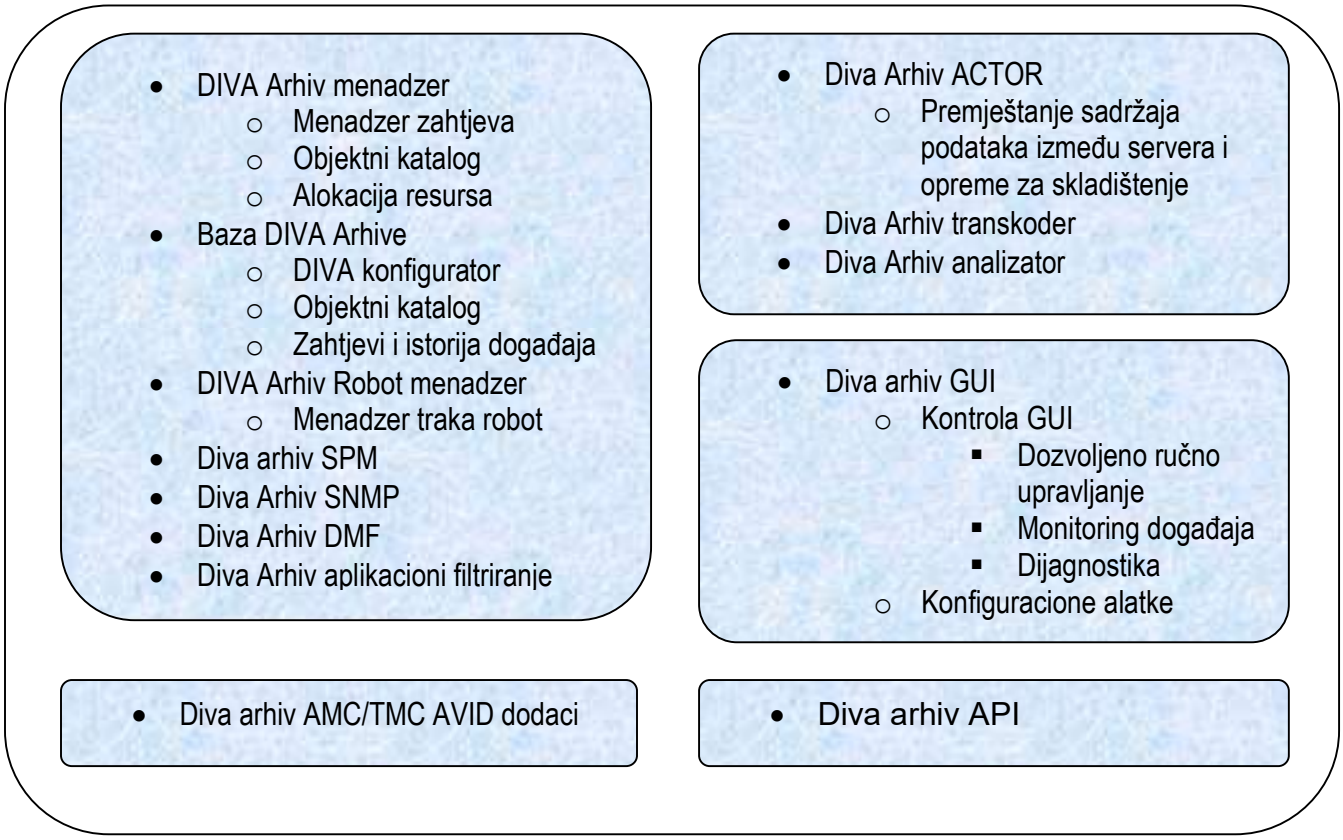


Tabela 4 – Glavniji elementi u arhitekturi DIVA arhive

3.2.2. Softverski sloj (platforma)

Softverska platforma se zasniva na setu aplikativnih rješenja - softverskih alata koji funkcionišu nad server - klijent arhitekturom i logičkom organizacijom podataka.

Same podatke možemo podijeliti na:

- Audio-video sadržaje visoke rezolucije (Hi-res fajlovi),
- Audio-video sadržaje niske rezolucije (Lo-res fajlovi ili proxy),
- Opisni podaci (metadata).

Centralizovane baze podataka su najvažniji (pred)uslov za pristup podacima. Sa porastom kapaciteta centralna memorija, raste i broj fajlova/dokumenata na samom storidžu, čime se gubi mogućnost „direktnog“ pristupa istim. Da bi se fajl/dokument lako i pouzdano locirao na storidžu, potrebno je imati dodatne

podatke tj. opise (metadata) koji će olakšati pristup materijalima niske i visoke rezolucije.

Audio - video sadržaji visoke rezolucije (Hi-res fajlovi) su sadržaji memorisani u fajlovima koji se koriste za finalnu proizvodnju, emitovanje i arhiviranje. Zbog logične relacije između kvaliteta i veličine fajlova, ovi sadržaji su veoma zahtjevni prema resursima sistema (veličina storidža, propusni opsezi mreže, snaga procesora koji ih obrađuju).
Audio - video sadržaji niske rezolucije (Lo-res fajlovi) su sadržaji memorisani u fajlovima koji su kopija fajlova (sadržaja) visoke rezolucije. Ovi fajlovi se dobijaju nekim od postupaka smanjenja količine informacija iz originalnih sadržaja čime im se smanjuje kvalitet, a samim tim se znatno smanjuje i potrošnja resursa u njihovom korišćenju. Time se omogućava većem broju korisnika da uz iste troškove (IT infrastrukturu, radne stanice, itd.) može da obavlja radne procese.

Osnovne karakteristike softverskih aplikacija:

Xedio Ingest

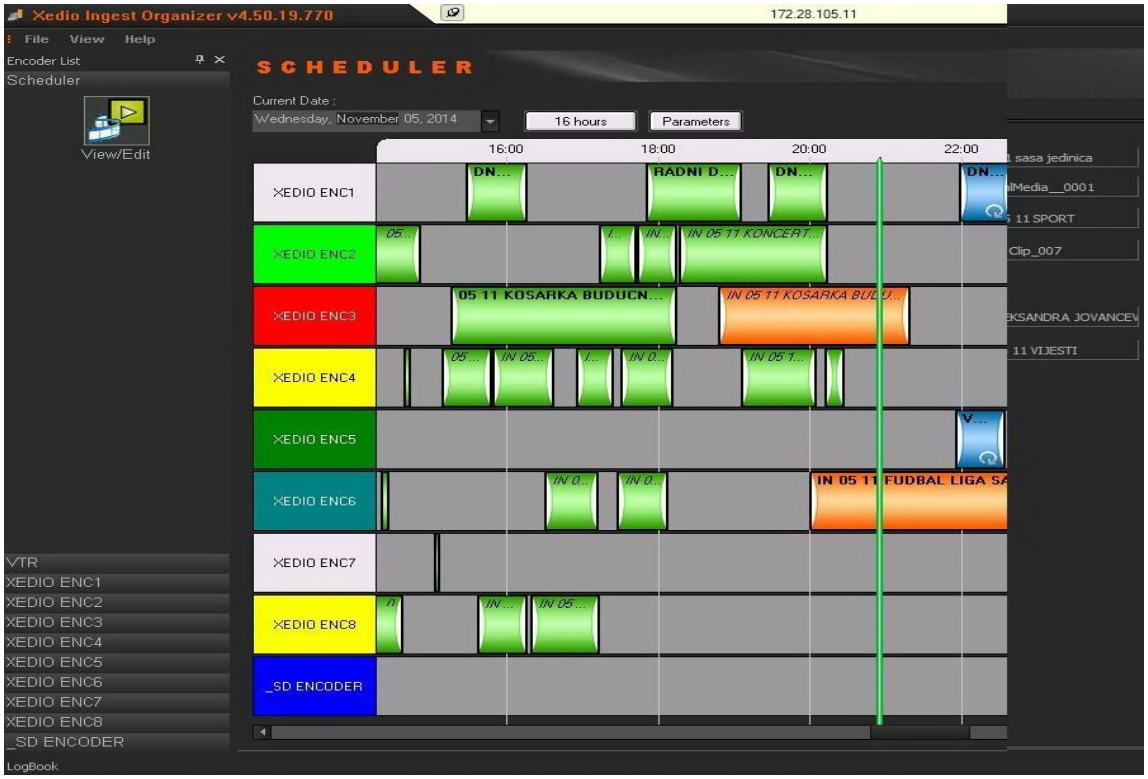
Osnovna namjena Xedio Ingest aplikacije je da kontroliše enkodere koji informacije iz dolazećih audio-video signala zapisuje u fajlove u odgovarajućem formatu.

Bitne karakteristike softvera su:

- Mogućnost kontrole više kanala (fidova) istovremeno
- Mogućnost gledanja tj. pretkontrole za izabrani kanal, šta se unosi (indžestuje) na VGA ekranu
- Fajlovi koji se zapisuju su dostupni za dalju obradu i prije nego što se proces unosa završi
- Mogućnost vremenski planiranog unosa (*scheduled ingest*) ili unosa po zahtjevu (*crush recording*)
- Mogućnost kontrolisanja VTR-ova

- Mogućnost vremenski planiranog unosa (*scheduled ingest*) ili unosa po zahtjevu (*crush recording*)
- Mogućnost kontrolisanja VTR-ova

Na slici 32 je prikazan interfejs Xedio Ingest Organiser aplikacije, u trenutku kad je aktivno svih osam enkodera.



Slika 32 – Interfejs Xedio Ingest Organiser aplikacije

AutoFileImporter

Namjena aplikacije je da obezbijedi unos audio-video sadržaja u domenu fajlova. Osnovna namjena mu je da skenira određene foldere i ukoliko prepozna nove fajlove u njima startuje proceduru enkodovanja i transfera zapisa na centralni storidž i unosa u bazu podataka.

MediaImporter

Namjena aplikacije je da obezbijedi unos audio-video sadržaja sa novih medija na kojima se vrši akvizicija slike i tona (XDCAM, P2 kartice, itd).

CleanBrowse

Namjena aplikacije je da omogući klijentima (novinarima) pregled medije raspoložive u CleanEdit integrisanom radnom okruženju.

Važnije karakteristike su:

- Rad sa Lo-res fajlovima
- Pretraga centralnog storidža i arhive. Pristup medijama se obavlja preko raspoloživih metadata informacija
- Unosi novih i izmena postojećih metadata
- Mogućnost kreiranja virtualnih klipova (virtualne medije),
- Pristup materijalu koji se još uvek unosi (indžestuje)
- Moguće je obaviti preselekciju i *publishing* materijala

Postoje i dvije aplikacije namijenjene montaži:

- **Story Cutter,**
- **CleanEdit**

Na slici 33 je prikazan interfejs CleanEdit montažerske aplikacije.

Zajedničke osobine softvera su:

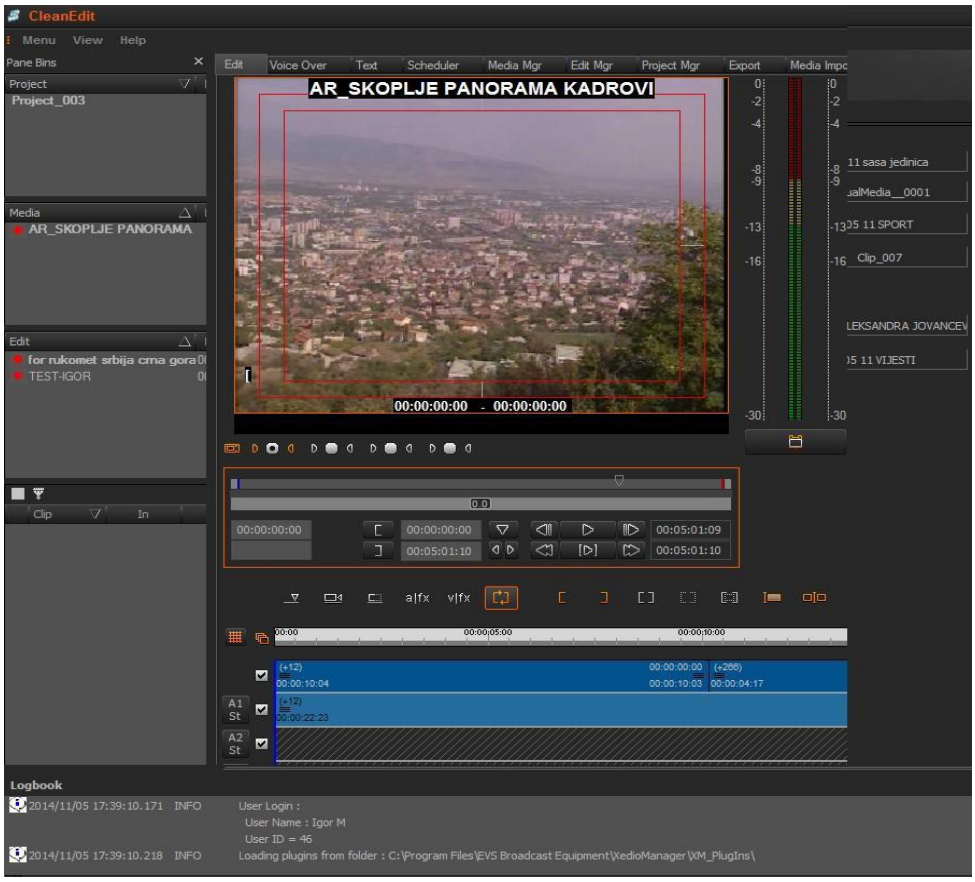
- Jednostavan i brz rad
- Mogućnost rada nad materijalom čiji unos još uvijek traje
- Mogućnost kreiranja virtuelnih klipova
- Mogućnost kreiranja finalnih projekata
- Mogućnost rada sa glasovnim zapisom (voice over)

Specifičnosti za Story Cutter aplikaciju:

- Namijenjen je novinarima
- Medije se preselektuju i raspoređuju u liste (storyboard-ove)
- Projekti mogu da se prenesu na montažu jačim alatima (CleanEdit)

Specifičnosti za CleanEdit:

- Namijenjen je i novinarima i montažerima
- Rad preko vremenskog (timeline) interfejsa (više video lejera, audio lejera)
- Mogućnost insertovanja grafičkih lejera
- Mogućnost primjene tranzicija i jednostavnih vizuelnih efekata
- Mogućnost finalnih provjera unutar projekta
- Rezultat montaže je trenutan, bez potrebe bilo kakvog rendera
- Omogućen rad i van sistema (na primjer na laptop računarima)



Slika 33 – Interfejs Clean Edit aplikacije

Xedio Approval

Namjena aplikacije je da kontroliše medije i projekte u bilo kojoj fazi produkcije.

Bitne karakteristike ove aplikacije su:

- Namjenjena je urednicima programa
- Mogu se gledati i Lo-res i Hi-res fajlovi
- Mogu se projekti odobravati za upotrebu ili se vraćati na doradu (*ready-to-broadcast*)

PlayoutOrganiser

Namijenjen je radu sa plej listama i kontroli emitovanja.

Osnovne karakteristike:

- Projekti se mogu reprodukovati u realnom vremenu
- Jedna aplikacija može da kontroliše jednu plej listu
- Plej liste se smještaju u bazu i dostupne su drugim instancama softvera u sistemu
- Aplikacija fizički može kontrolisati dva kanala emitovanja (*playout* servera), pa se ista plej lista može fizički emitovati na dva kanala (povećana pouzdanost)
- Medije se mogu pregledavati i trimovati
- U slučaju nedostupnosti Hi-res fajlova, emituje se Lo-res kopija
- Klipovi se mogu emitovati automatski (jedan za drugim) ili manuelno (pojedinačno)

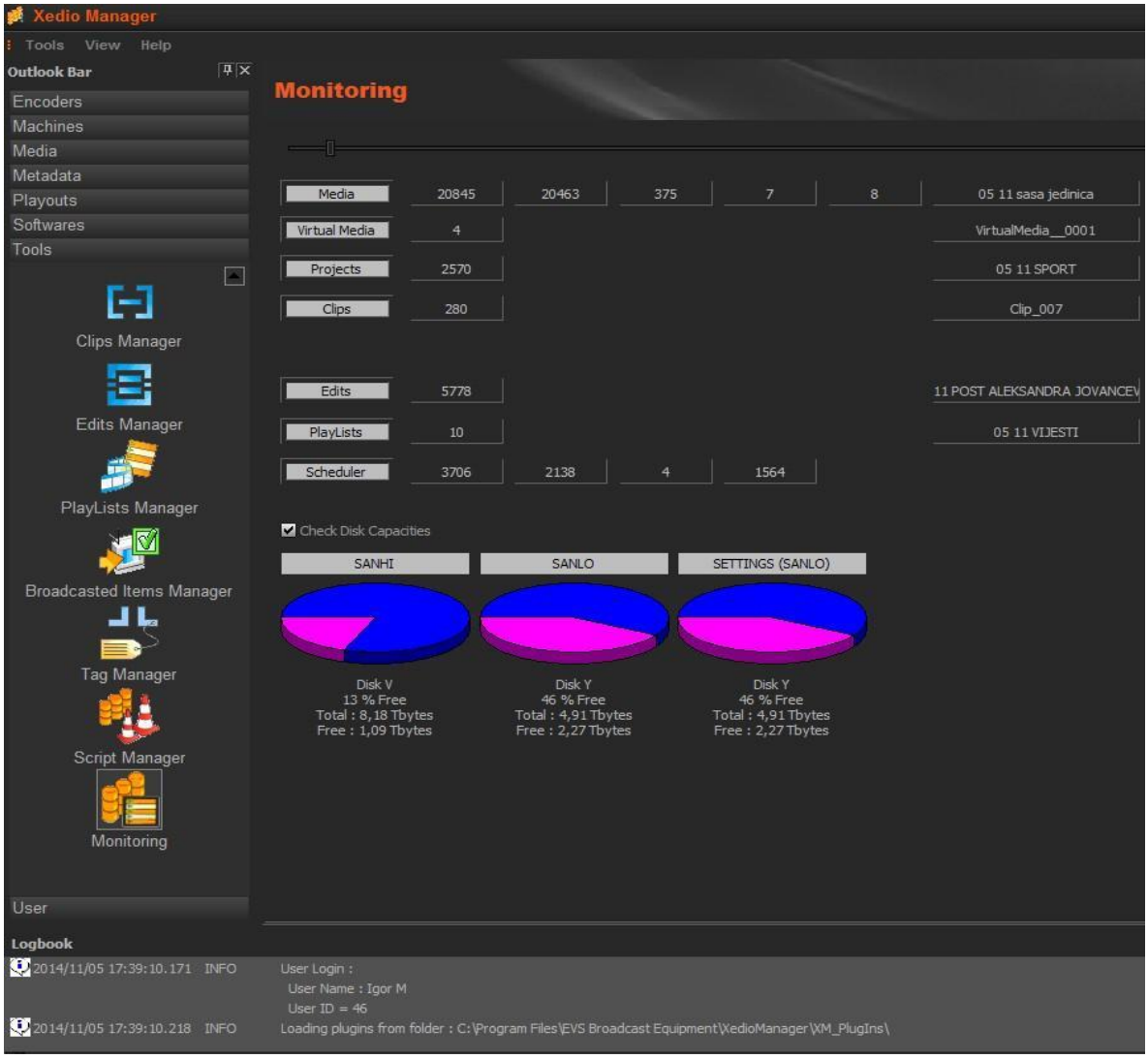
Xedio Manager

Ovo je centralizovana softverska aplikacija koja služi za konfiguraciju i održavanje cijelog sistema.

Ima sledeće karakteristike:

- Svi podaci o sistemu se memorišu u centralnu bazu podataka
- Konfiguriše i hardverske i softverske komponente sistema
- Definiše korisnike i grupe unutar sistema, definiše njihova korisnička prava
- Omogućava konfiguracije grafičkih interfejsa aplikacija
- Može da pretražuje medije prema unijetim metadata informacijama
- Kontroliše softverske servise i procese u sistemu
- Stara se o stanju sistema

Namijenjen je prije svega IT administratorima. Na slici 34 je prikazan interfejs Xedio Manager aplikacije.



Slika 34 – Interfejs Xedio Manager aplikacije

Aplikacije za rad sa Arhivom

Pristup dubokoj arhivi u sistemu je moguće ostvariti uz pomoć dvije aplikacije. To su: Clean Edit i Xedio Archive Organizer. Postoje dva načina vraćanja materijala iz arhive: kompletno i parcijalno. Aplikacija Xedio Archive Organizer je zadužena za slanje kompletne medije u duboku arhivu ali je zadužena i za ponovno vraćanje medija u sistem. Kada se medija pošalje na arhivu, pošalje se ustvari njen Hi-res fajl, dok njegova Lo-res kopija i dalje ostaje u sistemu. Informacije o toj mediji su i dalje dostupne svima kroz sistem i bazu, samo se status medije mijenja. Sa Clean Edit aplikacijom se vrši parcijalno vraćanje iz duboke arhive, ukoliko je to potrebno montažeru prilikom montiranja priloga. Parcijalno vraćanje je zapravo vraćanje dijela materijala iz medije koja se već nalazi na dubokoj arhivi.

3.3. Koncepti, analize konkretnih rješenja za TNP

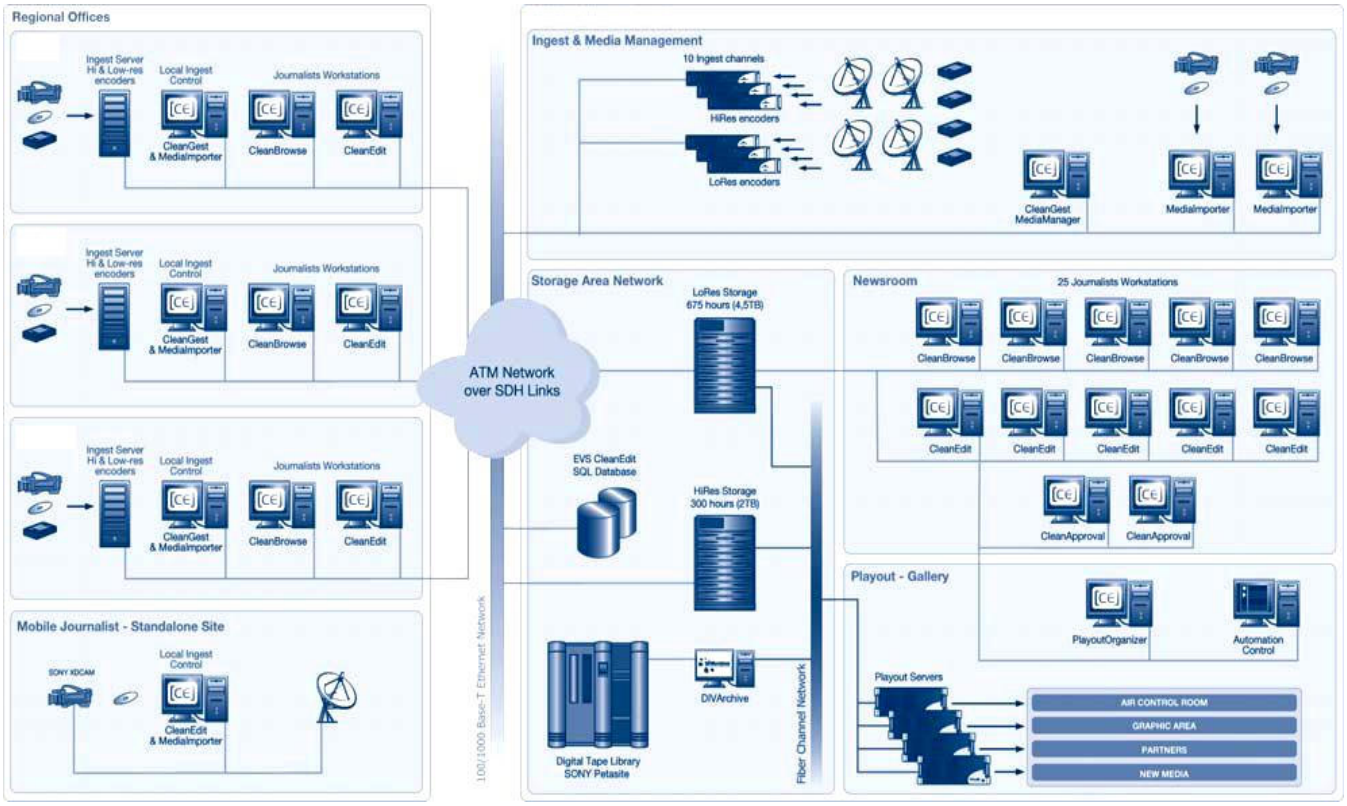
Polazeći od činjenice da je informativni program važan dio u programskoj strukturi u Televiziji Crne Gore, moguće je realizovati i drugačiji koncept od trenutno postojećeg cjelokupnog rešenja za TNP. Takvo rješenje se razlikuje i po hardverskoj i po softverskoj platformi.

Zahtjevi koje bi produkcijski sistem trebalo da ispuni su:

- Sistem mora da bude fleksibilan da bi se mogao integrisati u postojeći *workflow* kao i skalabilan da može da raste u skladu sa budućim zahtjevima,
- da se kao platforma koristi standardna IT tehnologija,
- da postojeća infrastruktura (prije svega IT) može biti iskorišćena,
- da se minimiziraju potrebe za tehničkom podrškom,
- da se omogući takvo okruženje koje će novinarima omogućiti, istovremeni rad na istim audio-video sadržajem i projektima,
- da je moguće uraditi izmjene na projektima neposredno pred emitovanje, uključujući i rad sa glasovnim zapisima (*voice over*) bez potrebe da se prave izmjene na plej listama,
- omogućiti urednicima programa uvid u projekte koji se rade ili koji su završeni,

- omogućiti novinarima korišćenje arhive koja je kreirana tokom 20-to godišnjeg rada,
- omogućiti novinarima pristup materijalu čim se on donese sa terena,
- korišćenje medije od strane više klijenata (novinara, urednika, montažera), bez njenog dupliciranja,
- omogućavanje ravnopravnog korišćenja medija u više regionalnih centara,
- mogućnost korišćenja materijala i novim formama - formatima (internet, 3G, 4G, etc.).

Na slici 35 je prikazana šema TNP sistema koji bi mogao da zamijeni i poboljša i unaprijedi postojeći sistem u TVCG.



Slika 35 – Šema mreže TNP sistema

Prednosti koje su ostvarene ovim sistemom su:

- Povećanje brzine emitovanja važnih vijesti (*breaking news*)
- Nema potrebe za namjenskim montažama i njihovim planiranjem
- Veća brzina upoznavanja radnog procesa (kraće vrijeme potrebno za obuku)

- Arhiva je dostupna cjelokupnoj produkciji
- Sistem je lako proširiv, dok su proširenja relativno jeftina
- Pregled i odobravanje materijala je trenutno
- Sistem je robustan i veoma pouzdan

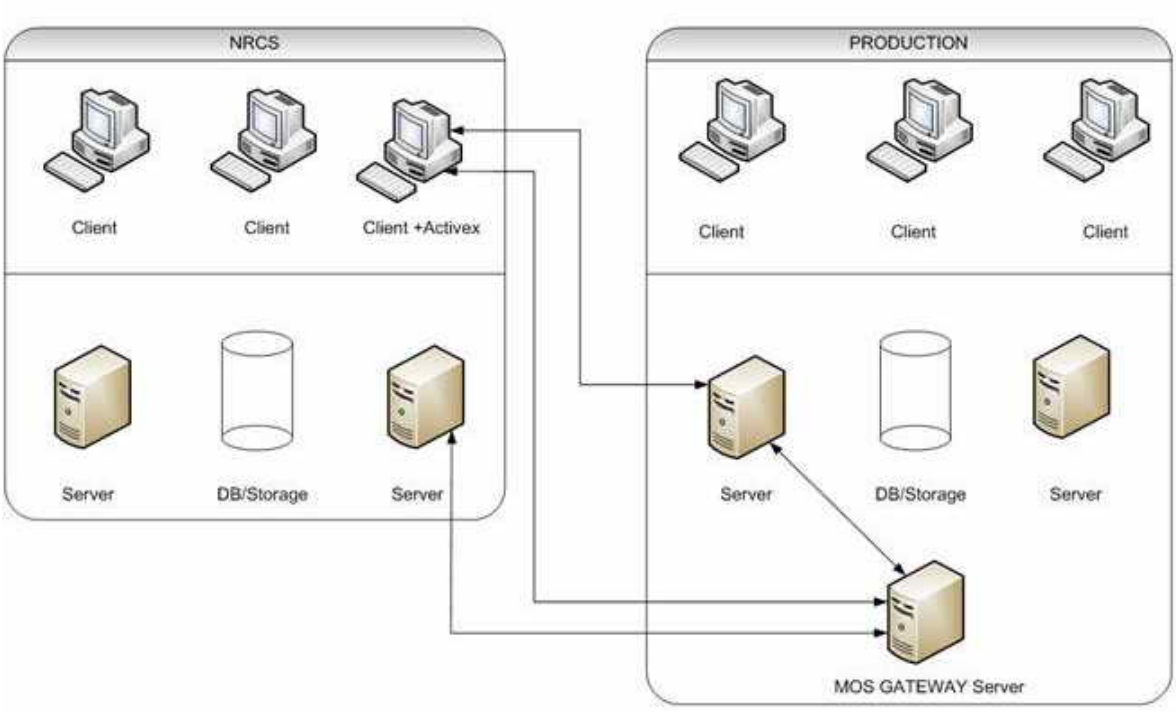
Integrisano radno okruženje informativne redakcije NRCS (*eng. News Room Computer System*) je sistem koji ima zadatak da centralizuje sve dnevne aktivnosti ljudi koje učestvuju u proizvodnji informativnog programa. Ti procesi počinju planiranjem tema i aktivnosti i to se dešava znatno prije od dana emitovanja. Zatim slijede dnevni procesi prikupljanja servisnih informacija (tekst, slika, zvuk, video), formiranje projekata/priča, dijeljenje radnih zadataka, pregled postojećeg materijala (arhiva), montaže, finalnog odobravanja, slanja na emitovanje itd. Cijelo vrijeme korisnici su u međusobnoj komunikaciji (interakciji), a istovremeno se na osnovu redosleda emitovanja kreiraju plej liste za sve integrisane produkcijske sisteme (prompter, karakter generator, montaže, video serveri, striming serveri, itd.).

Razmjena podataka između NRCS i integrisanih sistema produkcije treba da se obavlja industrijskim standardom poznatim kao MOS (*eng. Media Object Server*). Integracija može biti i dvosmjerna, tako da produkcija može mijenjati metadata NRCS-a od jednostavnih slanja poruka tipa “materijal je spreman” ili “materijal nije spreman” do unošenja opisa materijala ili poruka ostalim učesnicima u procesu. Praktično MOS protokol omogućava novinarima/producentima da kontrolišu produkcijske TV uređaje iz svojih softverskih alata, prevazilazeći barijeru tehničke obučenosti za rukovanjem istih.

Postoje dvije vrste komponenti:

- MOS *Gateway* server je most između NRCS i produkcijskih sistema. Njegova namjena je da stalno komunicira sa serverima NRCS-a u potrazi za izmjenama i zahtjevima koje treba opslužiti. Takođe ima zadatak i da proslijedi povratnu informaciju od strane produkcijskih servera, koje su relevantne za NRCS.

- *ActiveX* kontrole su klijentske komponente produkcijskog sistema koje se instaliraju da direktno rade kao jedan od prozora NRCS-a. Time praktično dobijamo sve mogućnosti produkcijiskih alata kao dio korisničkog interfejsa osnovnog klijenta NRCS-a.



Slika 36 – Šema mreže TNP-a

Na slici 36 su prikazani načini saznavanja sadržaja centralnog produkcijskog storidža bez dodatnih *ActiveX* kontrola. (NRCS -MOS *Gateway*). Na MOS serveru se definiše aktivni folder čiji se sadržaj (spisak fajlova) replicira u sadržaj lokacije unutar NRCS. To praktično znači da će svaki novinar/producent po nazivu fajla uvijek znati šta novo stiže na centralni storidž. U zavisnosti od konfiguracije to može biti samo dio koji sadrži gotove projekte ili cjelokupan storidž. Jedan od načina ubacivanja materijala je prevlačenje mišem imena fajla iz prozora lokacije u košuljicu. Tada se u košuljici pravi mjesto za klip (place holder) i automatski se vezuje za fajl čije se ime prebacilo u listu. Istovremeno, MOS server šalje produkcionom sistemu nalog da se taj klip uvrsti u određenu košuljicu.

Načini saznavanja sadržaja centralnog produkcijskog storidža:

- Klijent za pregled materijala (NRCS0-*ActiveX* klijent *CleanBrowse*).

Ako NRCS klijent ima *CleanBrowse* klijent, onda može duplim klikom miša na ime fajla ili na mjesto u košuljici rezervisano za klip (*place holder*) da dobije mogućnost pregleda klipa u nekom od prozora NCRS klijenta.

- Klijent za pregled i jednostavnu montažu (NRCS -*ActiveX* klijent *StoryCutter*).

Ovakva kontrola omogućava i pregled, ali i mogućnost montaže i slanja materijala na emitovanje (popunjavanjem neiskorišćenih rezervisanih mjesta za video u košuljici).

- Kontrola plejlisti (NRCS-MOS *Gateway* - aplikacija *PlayoutOrganizer*).

Principijelno postoje dva načina za slanje klipa na emitovanje iz NRCS:

1. Prevlačenjem imena gotovog klipa u košuljicu.
2. Pravljenjem (rezervisanog) mjesta za budući klip.

Spajanje rezervisanog mjesta i gotovog klipa se može izvršiti kasnije i to se može uraditi kroz montažne softvere ili kroz *PalyoutOrganizer*.

3.4. Realni sistemi zaštite pristupa multimedijalnom sadržaju digitalnog segmenta televizije Crne Gore

Razvoj računarskih sistema doveo je do lakšeg, bržeg i jednostavnijeg funkcionisanja velikih sistema namijenjenih prenosu multimedijalnog sadržaja. Svaki sistem bio on zatvorenog ili otvorenog tipa može imati probleme sa zaštitom samog sistema odnosno zaštitom sadržaja koji cirkuliše tim sistemom. U poslovnom sistemu pitanje zaštite postalo je jedno od najvažnijih pitanja svakog ozbiljnog sistema. Logično je da se apsolutna zaštita digitalnog sistema ne može ostvariti, kao i da su sistemi koji koriste mrežne protokole najranjiviji i najosetljiviji kada je u pitanju stepen zaštite. Visok nivo i pristup riješavanju problema zaštite mora biti sveobuhvatan sa stalnim razvijanjem novih mehanizama zaštite u skladu sa bezbjednosnim problemima koji nastaju.

U nastavku rada prikazan je aktuelni način administriranja računarskih stanica, koje čine dio digitalnog sistema televizije Crne Gore, pri čemu su računari namijenjeni korisnicima koji uz pomoć određenih aplikacija imaju mogućnost pregledanja digitalnog materijala, a sve u cilju mjera sigurnosne zaštite sadržaja koji se nalazi na serverima.

Sve stanice nalaze se u zatvorenom sistemu, sistemu koji nije povezan na internet. Stanice se nalaze u lokalnoj LAN mreži koja nema *Firewall* žaštitu, već je direktno povezana na svič. Vrsta komunikacionih medija sa kojima su povezane stanice su standardni UTP kablovi. Mrežni parametri lokalne mreže se ručno setuju na mrežnoj kartici računara u TCP/IP4 protokolu, ne dodjeljuju se preko DHCP servisa. Broj korisničkih računara koji su povezani na lokalnu mrežu sistema u ovom trenutku iznosi 40, dok ukupan broj korisničkih stanica zajedno sa serverima sistema iznosi 80.

Korisnički računari iz digitalnog segmenta podijeljeni su u dvije grupe. Prvu grupu računara čine računari koje koriste novinari i urednici za pregledanje materijala iz sistema. Drugu grupu računara čine računari namijenjeni montažerima i toncima koji pokrivaju radnje poput snimanje i obrade audio zapisa i napredniji stepen montaže (*voice over*). Jedno od najsigurnijih riješenja za uspješno održavanje funkcionisanja samog sistema jeste njegovo ažuriranje. Ažuriranja (zakrpe) skidaju se redovno, dok se samo ažuriranje sistema obavlja isključivo nakon nekih većih izmjena.

Korisničke radne stanice funkcionišu sa Windows operativnim sistemom, a sami korisnici ograničeni su po pitanjima prava i mogućnosti modifikovanja sistema odnosno sistemskih fajlova. Logično je da bi većina korisnika, ukoliko bi postojala otvorena mogućnost, instalirala razne softvere koji bi mogli da utiču na funkcionisanje i stabilnost samog operativnog sitema. Jedna od osnovnih stavki koja je implementirana u okviru zaštite TVCG sistema je onemogućavanje upisa podataka u Program Files i Windows direktorijume.

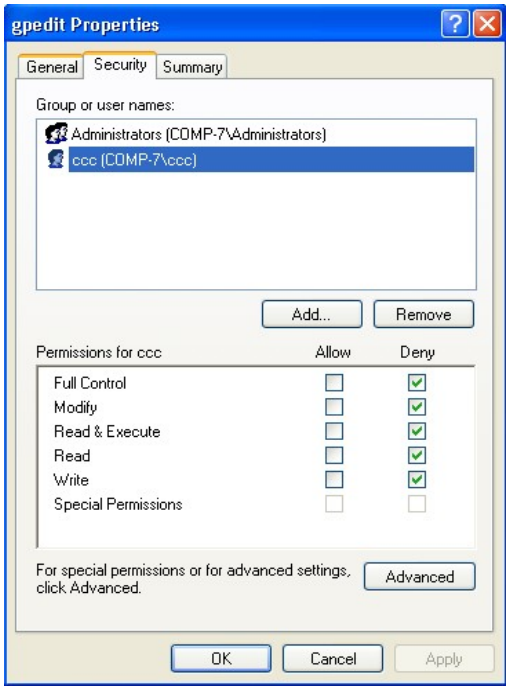
Programski kontrolisana upotreba USB portova treba da ima preventivni karakter i igra značajnu ulogu u sprečavanju krađe podataka od strane zaposlenih, a ujedno i predstavlja varijantu zaštite od neželjenog softvera, *autorun* skripti i sličnih programa - alata, koji mogu da naruše rad operativnog sistema. Da bi se omogućila razmjena podataka između korisnika koriste se specijalni dijeljeni folderi pri čemu su omogućena prava upisa i čitanja ali ne i brisanja podataka.

Da bi sistem bio što sigurniji svakom korisniku, prije nego što počne koristiti resurse sistema, obezbijeđeno je korisničko ime i lozinka. Ovi podaci dobijaju se otvaranjem naloga u glavnoj admin aplikaciji sistema *'Xedio Manager'* od strane administratora. Administrator treba da otvori nalog i smjesti korisnika u

predefinisanu grupu, čime je automatski dodijeljen set pravila za korišćenje određenih aplikacija. Na ovaj način, novinarima je omogućen pristup aplikaciji za pregledanje materijala *'Xedio Browser', urednicima i montažerima na raspolaganju stoji 'Xedio CleanEdit'* namijenjen montaži.

Sistem ne koristi enkripciju kao mogući način zaštite pristupu multimedijalnom sadržaju, već se zaštita vrši lokalno na svim stanicama uz pomoć grupnih polisa. U okviru Windows operativnog sistema računarskih stanicama dodijeljivani su parametri pristupa putem grupne polise (group policy).

U realnim sistemima mjere zaštite implementirane pomoću polisa vrše se preko poziva na komandu Gpedit.msc ili otvaranjem fajla sa lokacije *C:\WINDOWS\SYSTEM32\GPEDIT.MSC* pristupa se editoru grupnih polisa preko kojeg se vrši podešavanje svih naloga koji su potrebni. Na računaru su aktivna dva naloga, administratorski kojem su omogućena sva prava, i korisnički nalog nad kome se vrše podešavanja prava pristupa (slika 37).

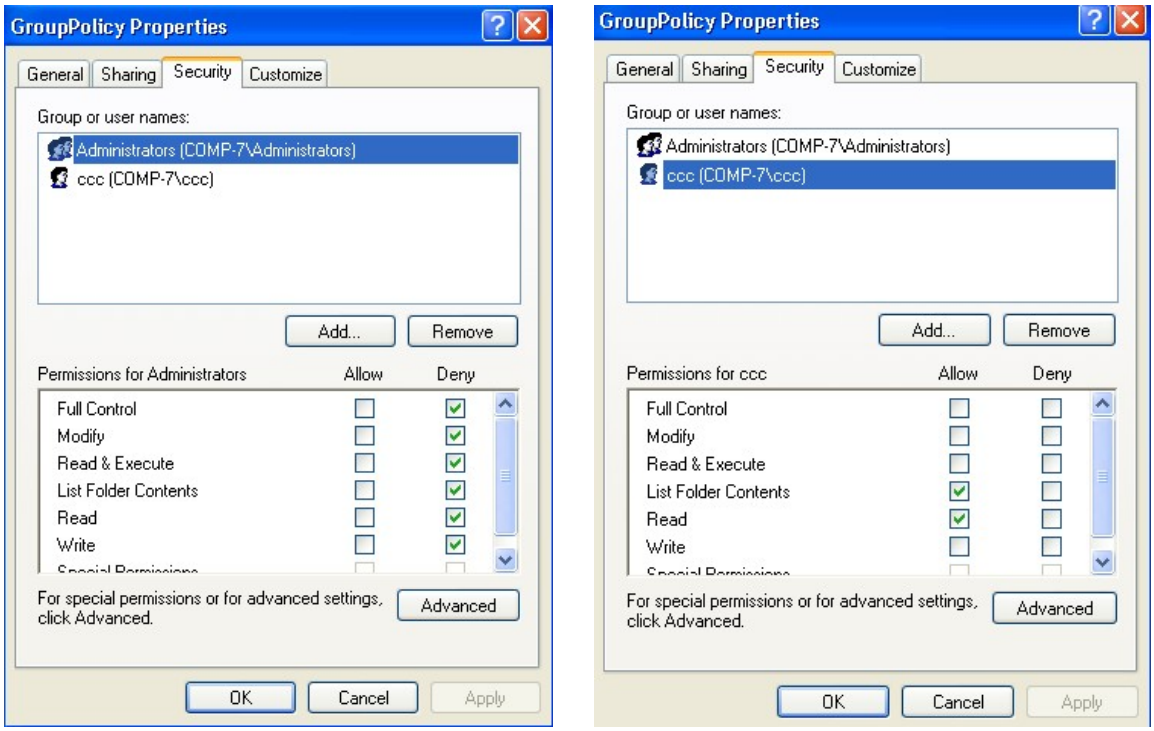


Slika 37 - Korisnički nalog

Ovim podešavanjima onemogućavamo otvaranje fajla *gpedit.msc* od strane korisnika i samim tim onemogućavamo mijenjanje samih polisa preko korisničkog naloga. Da bi se ova prava aktivirala potrebno je restartovati računar. Nakon onemogućavanja pristupa Gpedit.msc korisničkim nalozima, potrebno je

onemogućiti mijenjanje sadržaja samog foldera u kome se nalazi *gpedit.msc,* a čija se lokacija nalazi na *C:\WINDOWS\system32\GroupPolicy*.

Kao i za fajl *gpedit.msc* i ovdje se podešavaju dva naloga, administratorski i korisnički. U slučaju da želimo da se polise ne važe na administratorskom nalogu, a važe na korisničkom, tada se na administratorskom nalogu aktiviraju opcije za zabranu prava, a na korisničkom aktiviraju dozvole (slika 38).



Slika 38 – Podešavanje GroupPolicy foldera

Podešavanja polisa se uglavnom većinski nalaze i vrše na sledećim lokacijima:

- *'User Configuration/Administrative Templates/Windows Components/Windows Explorer ;*
- *'User Configuration/Administrative Templates/Windows Components/Desktop';*
- *'User Configuration/Administrative Templates/Control Panel';*
- *'User Configuration/Administrative Templates/System/Ctrl+Alt+Del Option/';*
- *'User Configuration/Administrative Templates/Start Menu and Taskbar';*

- *'User Configuration/Administrative Templates/System/Removable Storage Access';*
- *'Computer Settings/Windows Settings/Security Settings/Local Policies/User Right Assigment'.*

Dio zabrana i dozvola polisa koje su implementirane, kao i njihov opis i funkciju koju vrše prikazani su u nastavku rada:

- *Remove Change Password* – onemogućavanje korisnika da mijenja šifru računara.
- *Remove Lock Computer* – onemogućavanje korisnika da zaključa računar.
- *Remove Task Manager* – uklonjen Task Manager na korisničkom nalogu.
- *Remove Logoff* – uklonjena mogućnost korisnika da uradi Logoff računara.
- *Prohibit Access to the Control Panel - z*abrana pristupa Control Panel-u.
- *Hide and Disable all items on the desktop* – na Desktopu uklonjenje sve ikonice.
- *Hide Internet Explorer icon on Desktop* – uklonjenja ikonica explorera na Desktopu.
- *Prevent adding, dragging, dropping and closing the Taskbar toolbars – k*orisnicima uklonjenja opcija prevlačenja, dodavanja po taskbaru.
- *Do not keep History of recently opened documents* – uklonjena opcija za pamćenje zadnjih korišćenih fajlova.
- *Removable Disks Deny exetuce read write access* – zabrana korišćenja USB uređaja.
- *CD and DVD: Deny read write access* – zabrana korišćenja CD/DVD medija.
- *Add Search Internet link to Start menu* – zabrana korišćena pretrage računara.
- *Remove and prevent access to the Shut Down, Restart, Sleep, Hibernate* – zabrana korisniku da ugasi i resetuje računar.
- *Remove pinned programs list from the Start Menu* – zabrana dodavanja prečica u Start meniju.
- *Add the Run command to the Start Menu* – zabrana izvršavanja RUN komande.
- *Lock the Taskbar* – zabrana zaključavanja Taskbara.

- *Remove Favorites, Help menu from Start menu* – zabrana Favorites i Help menija u Start meniju.
- *Turn off user tracking* – isključivanje pravljenja logova na korisničkom nalogu.
- *Remove all program list from the start menu* – deaktivirana lista programa iz Start menija.
- *Remove network connection from start menu* – deaktivirana mrežna podešavanja iz Start menija.
- *Remove documents icon , music, network, pictures* – uklonjene prečice za dokumenta, muziku, mrežu i slike.
- *Remove search* – deaktivirana pretraga računara.
- *Hide the notification area* – sakriven notifikacioni prostor.
- *Prevent Access to the command prompt* – zabrana korišćenja DOS terminala.
- *Hide thes specified drives in My Computer* – zabrana pristupa lokalnom disku.
- *Display the menu bar in Internet Explorer* – deaktivirana meni opcija na Explorer-u.
- *Remove File menu from Windows Ecplorer* – deaktivirana File meni opcija na Windows Explorer-u.
- *Turn of Windows hotkey* – isključenje prečica na tastaturi.

U slučaju da postoji potreba za modifikacijom koja je vezana isključivo za korisnički nalog, poput instaliranja novog programa, pinovanja neke prečice, mapiranja mrežnog foldera itd, moraju se privremeno aktivirati prava nad polisama na administatorskom nalogu, kako bi se omogućio pristup polisama. Nakon urađenih promjena vrši se deaktivacija polisa na adminstratorskom nalogu i aktivacija već ranije definisanih dozvola na korisničkom nalogu.

Nakon implementiranja ovakvih mjera zaštite radne stanice pokazale su se kao stabilne i veoma pouzdane za rad, eliminisani su najčešći problemi koji su dolazili putem spoljnih medija poput USB uređaja, a samim tim obim intervencija kod samih korisnika i na samim radnim stanicama drastično je smanjena. Na ovaj način novinari, urednici, montažeri mogu koristiti samo ono što im je predefinisano. Takođe, postiglo se da je video server maksimalno zaštićen i da je svaka neovlašćena akcija onemogućena i ispraćena putem log fajlova, čime se

smanjuju problemi definisanja grešaka. Ranije intervencije nad digitalnim sektorom, zahtijevale su pronalaženje obrisanih fajlova, pri čemu se nije imalo na uvid šta, ko i kada je pobrisao sporni fajl, što se sada uspješno riješava preciznim monitoringom korisničkih naloga.

Međutim, treba napomenuti da ovakav sistem zaštite u TVCG, pored prednosti, vjerovatno posjeduje i svoje potencijalne nedostatke. Otkrivanje sigurnosnih problema u sistemu veliki je izazov za administratora računarskih sistema u bilo kojoj firmi. Blagovremenim djelovanjem može znatno da se spriječi ili uspori nastanak nekog problema. Zato je jako bitno da se postojeći sistem stalno analizira, testira, kako bi se našli problemi u sistemu i kako bi se na osnovu njih moglo blagovremeno reagovati i spriječiti negativne posledice pojavljivanja nekog problema.

4. MJERE SIGURNOSNE ZAŠTITE DIGITALNIH SISTEMA I IP TELEVIZIJE

Jedna od ključnih komponenti digitalne televizije je CA (*eng. Conditional Access*) sistem. CA sistemi omogućavaju operateru digitalne televizije enkriptovanje signala, čime se signal određenog TV sadržaja ili signal kompletnog kanala blokira. Naravno, ovakvi sistemi zahtijevaju posebne algoritme zaštite onemogućavajući krajnjem korisniku pristup blokiranom sadržaju.

Implementacija enkripcije u CA sistemima ključna je stavka koja određuje da li će se sadržaj prikazivati ili ne. Sam sistem funkcioniše putem servisa i namijenjen je i za prenos ostalih digitalnih tipova signala, digitalnih podataka, digitalnog radija ili interaktivnih servisa.

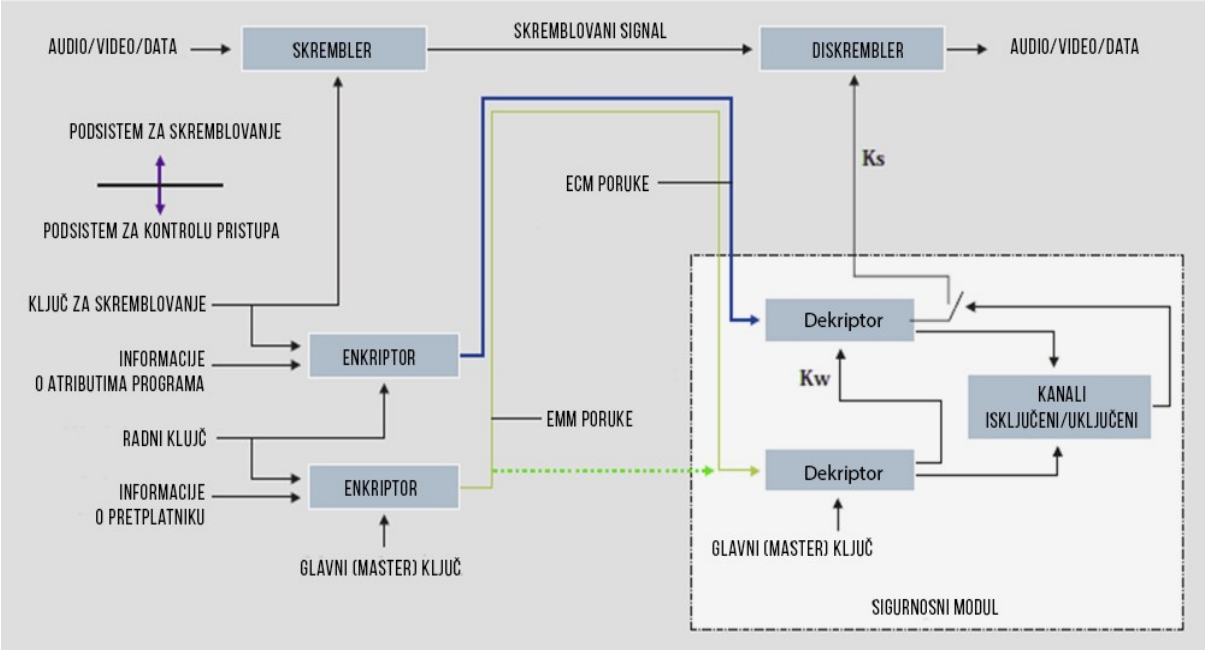
CA sistem možemo razložiti na par osnovnih komponenti:

SMS (eng. Subscriber Management System) – podsistem *CA* sistema koji se oslanja na korisničke informacije i zahtjeve EMM-a preko SAS-a. *EMM* (*eng. Entitled Management Message*) omogućava uvid u opšte informacije o korisniku i njegovoj pretplati. Bitan resurs *SMS* sistema je baza podataka svih korisnika i uređaja, kao i informacija o plaćenim servisima.
SAS (*eng. Subscriber Authorization System*) – predstavlja podsistem *CA* sistema čiji je zadatak prevođenje informacije o korisniku u *EMM* poruku na zahtjev *SMS* sistema. *SAS* takođe omogućava da zaštitni modul korisnika prihvati autorizaciju potrebnu za pregled programa, što *SAS* sistem pretvara u potrebni servis za pravljenje kopije u slučaju nepredviđene greške.
Sigurnosni modul – najčešće je predstavljen u vidu pametnih kartica, čiji je zadatak rad sa informacijama potrebnim za dekripciju signala. Ovaj modul je uglavnom hardverski vezan za *STB* uređaj ali može biti i u vidu eksterne kartice koja se povezuje na *STB* uređaj.

STB (*eng. Set Tob Box*) predstavlja hardverski uređaj koji obuhvata sve predhodno nabrojane module, odnosno uređaje koji se direktno vežu na TV uređaj, omogućavajući korisniku pristup digitalnoj televiziji.

Postoje dva *DVB* protokola koja koriste *CA* sistemi: *Simulcrypt i Multicrypt*. *Simulcrypt* protokol funkcioniše na sistemu istovremenog korišćenja višestrukih *STB* uređaja, od kojih svaki ima različit *CA* sistem radi autorizacije programa za isti zaštićen sadržaj [9]. Kod ovog protokala različite *ECM* i *EMM* poruke potrebne su za svaki *CA* sistem i šalju se simultano, a zadatak svakog *STB* uređaja je da prepozna i iskoristi odgovarajući *ECM* i EMM. *Multicryt* omogućava višestruke *CA* sisteme u okviru jednog *STB* uređaja koristeći PC karticu i pametnu (*smart)* karticu za svaki *CA* sistem koji se koristi. Svaka kartica stavlja se u poseban slot na *STB* uređaju čime se omogućava prepoznavanje ECM-a i EMM-a dozvoljavajući autorizaciju programa. Tipični *CA* proces uključuje tri osnovna elementa: opremu za prenos, *STB* uređaj i sigurnosni modul. Oprema za prenos generiše enkriptovani program namijenjen korisniku koji prilikom ulaska u *STB* uređaj mora da bude filtriran, nakon čega ide na sigurnosni modul. Sigurnosni modul obavlja autorizaciju programa za enkripciju u realnom vremenu i taj signal vraća *STB* uređaju koji sada dekriptovani signal šalje TV prijemniku.

Iako *CA* sistem nije unikatan već varira za različite servise osnovna konfiguracija sistema je prizakana za slici 39.



Slika 39 - Šema CA (Conditional Access) sistema

Posmatrajući analogne sisteme, skremblovanjem signala može doći do degradacije kvaliteta samog signala, i taj faktor zavisi isključivo od načina skremblovanja. Provajderi uglavnom biraju nivo skremblovanja na način da im je

najlakše obaviti obnavljanje kvaliteta signala, ostavljajući napredne nivoe enkripcije kao glavni zaštitni metod. U slučajevima digitalne televizije degradacija signala neće postojati kada je signal ispravno primljen.
Nivoi zaštite digitalne televizije zavise od kvaliteta enkripcije koja se obavlja nad skremblovanim signalom. Česte pojave poput poruka o nedostatku signala prave problem samom provajderu usluga od koga se očekuje odgovarajući nivo usluge koji može zadovoljiti krajnjeg korisnika. Prilikom pojave ovih problema operater ne može znati da li je u pitanju problem sa samim uređajem, odnosno resiverom, samom konekcijom ili možda CA sistemom. Problem je što su CA sistemi u tolikoj mjeri zatvoreni da otklanjanje ovakvih problema pravi poteškoće samim operaterima, što na kraju utiče na nezadovoljstvo krajnjih korisnika. Možda nezadovoljstvo krajnjih korisnika nije u toj mjeri izraženo u manjim sredinama poput Crne Gore, ali u sredinama u kojima se nalazi i po par stotina hiljada korisnika, ovakve stvari operateru donose određene neugodnosti koje mogu dovesti i do otkazivanja pretplate. Međutim, postoje neki relativno jednostavni koraci kojima je moguće osmotriti i detektovati najčešće probleme koji se javljaju prilikom prenosa digitalnog TV signala. Mnogi digitalni operateri u okviru različitih tehnologija za prenos signala koriste CA monitoring.

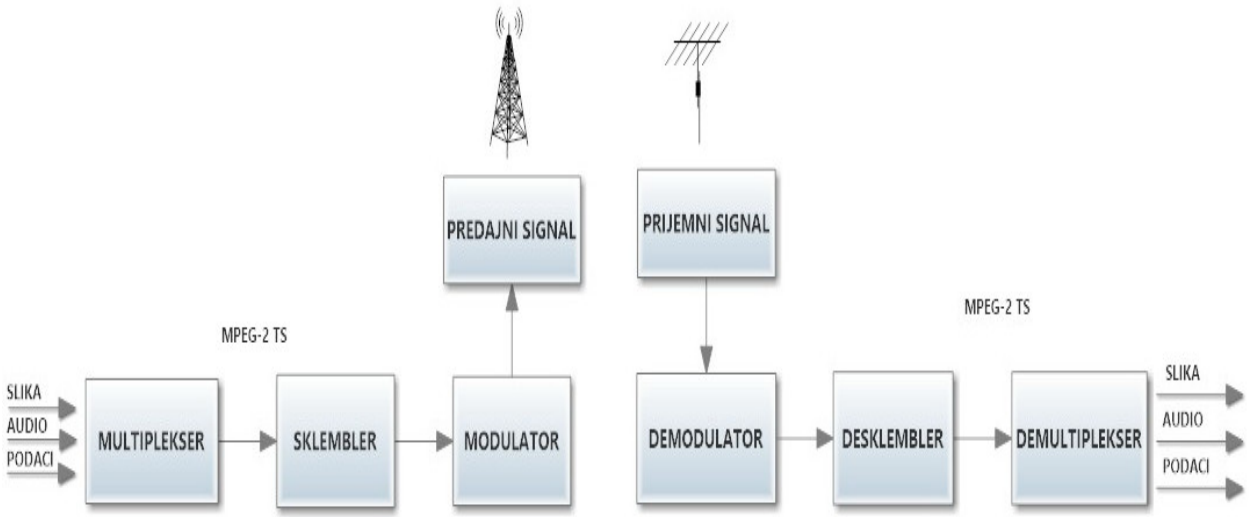
4.1. Princip rada CSA (Common Scrambling Algorithm)

CSA je algoritam enkripcije namijenjen prenosu digitalne televizije razvijen od strane *ETSI-a* (*eng. European Telecommunications Standards Institute*) tokom devedesetih godina. Do 2002. godine *CSA* je bio strogo čuvana tajna sa ciljem da se *CSA* implementira u okviru hardvera, čime bi se onemogućili napadi na sam sistem. Međutim, softversko rešenje je ipak predstavljeno omogućivši uvid u njegov način rada i implementiranje ispravki u cilju što bolje enkripcije, tako da trenutno već postoji *CSA* 3 enkripcioni sistem, baziran na 128 bitnoj *AES* (*eng. Advanced Encryption Standard*) enkripciji.
U Evropi *CA* sistemi za satelitski, zemaljski i kablovski broadcast koriste *CSA* algoritam za enkripciju i dekripciju TV signala. Pod *CSA* specifikacijama enkripcija i dekripcija signala naziva se skremblovanje (*eng. scrambling*) i deskremblovanje (*eng. descrambling*) signala [7]. Iako *CSA* algoritam predstavlja standard za

digitalni broadcast neki provajderi mogu iskoristiti različite varijante algoritama za enkripciju digitalnog signala.
CA sistem predstavlja kombinaciju skremblinga i enkripcije sa ciljem sprečavanja neovlašćenog pristupa sadržaju TV programa. Proces skremblovanja je proces pri kome zvuk, slika i generalno podaci postaju nečitljivi, i koji ima zadatak ograničavanja pristupa, odnosno onemogućavanje korisnicma pristup sadržaju za koji nemaju pretplatu. Enkripcija je proces zaštite sigurnosnog ključa kojeg šaljemo sa skremblovanim signalom, pri čemu je zadatak ključa da omogući deskremblovanje signala. Glavna uloga *CA* sistema pri *broadcast*-u jeste odlučivanje koji resiveri odnosno *STB* uređaji mogu primiti određene programske servise ili individualne programe.
Da bi sistem funkcionisao proces skremblovanja obavlja se kroz *CA* sistem. *CA* sistem uglavnom se sastoji od dva podsistema:

- Podsistema za skremblovanje, čija je funkcija skremblovanja signala i onemogućavnje neovlašćenog pristupa TV kanalima, kao i deskremblovanje signala u okviru korisničkog resivera.
- Podsistema za kontrolu pristupa koji obrađuje kontrolne pristupne poruke i određuje da li je potrebno obavljati deskrembovanje.

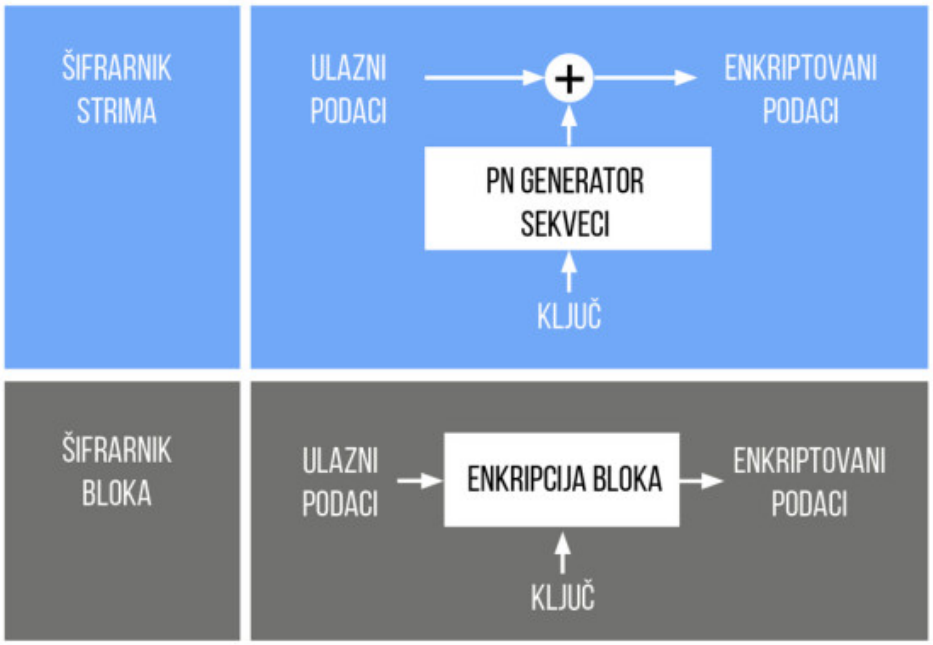
Na slici 40 je pojednostavljena šema skrembling sistema.



Slika 40 - Pojednostavljena šema skrembling sistema

Signal prolazi kroz *scrambler*, koder koji enkriptuje signal koristeći kontrolnu riječ - CW *(eng. Control Word),* enkripcioni ključ koji se generiše nasumično. Signal na izlazu iz kodera je nečitljiv dok se ne unese odgovarajući ključ. Dekoder dekriptuje kodirane signale takođe koristeći CW ključ da bi reprodukovao početni signal. U

normalnim *DVB* sistemima kodiranje se obavlja preko multipleksera ili IP *streamer*-a, dok se dekodiranje obavlja u samom *STB* uređaju. Već je naglašeno da se CW kontrolna riječ generiše kao slučajna promljenjiva i ovaj proces obavlja sam koder. Zbog sigurnosnih razloga kontrolna riječ se mijenja veoma često, uglavnom svakih 10 sekundi. Zaglavlje transportnog stima-TS (*eng. Transport Stream*) sadrži dva kontrolna bita koji definišu CW kontrolnu riječ koje treba dekodirati (parni i neparni bit).
Različiti nivoi enkripcionih tehnika mogu biti primijenjeni na skremblovani signal. Sama tehnologija za enkripciju digitalnih signala se sastoji od dva različita šifrarnika *(eng. cipher*), odnosno dvije različite šifre, šifra bloka i šifra strima (slika 41). Podaci se enkriptuju pomoću 64-bitne blok šifre u CBC (*eng. Cipher Block Chaining*) modu, počevši od kraja paketa. Strim šifra se implementira na početku *data* paketa.



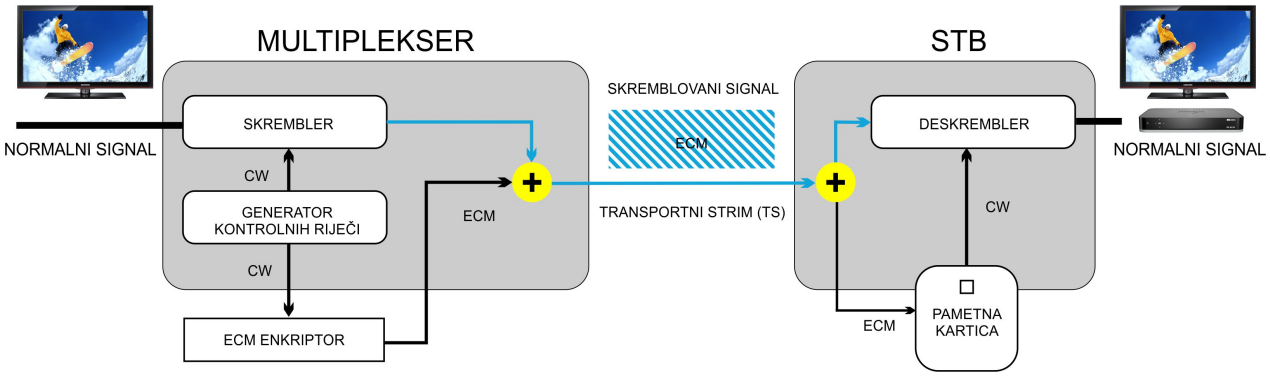
Slika 41 - Šema za skremblovanje digitalnih signala

Iako su signali poput video, audio i ostalih dodataka namijenjeni digitalnom prenosu i imaju različita svojstva, moguće ih je sastaviti u jedan digitalni signal olakšavajući proces prenosa podataka. Najčešći sistem koji bi obavljao sastavljanje svih signala baziran je MPEG standardu. Ovaj sistem sadrži dvije metode skremblovanja, pri čemu jedna metoda skrembluje trasportni strim paket, dok druga metoda skrembluje paketne elementarne strimove *PES (eng. Packetized Elementary Stream)*. U svakom slučaju metode skremblovanja nisu standardizovane, pa samim tim tip skremblovanja zavisi od provajdera, a u nekim

slučajevima i od same države. Evropa ima standardizovan skrembling sistem koji se zasniva na kombinovanju blok i strim šifrarnika.

4.1.1. ECM (Entitlement Control Message)

Najvažniji zadatak *CA* sistema je slanje ključa dekoderu na što sigurniji način. Ključ, odnosno kontrolna riječ smiješta se u kodiranoj *ECM* poruci implementiranoj u transportni strim. Većina *CA* sistema koristi sistem pametnih kartica radi sigurnosti, dok neki *CA* sistemi daju prioritet softverskim komponentama u odnosu na pametne kartice. Sama pametna kartica prima *ECM* u okviru signala, izvršava dekriptovanje a zatim šalje kontrolnu riječ *STB* resiveru radi dekodiranja signala.
Iako je kontrolna riječ veoma važna, njen vremenski rok trajanja je često ograničen od strane provajdera što dovodi do situacije da se kontrolna riječ mijenja i do nekoliko puta u minuti. Da bi resiver mogao da deskrembluje podatke on u svakom trenutku mora biti informisan o trenutnoj vrijednosti kontrolne riječi.



Slika 42 - Princip rada ECM-a

Za *CA* sistem slanje kontrolnih riječi ka *STB* resiveru veoma je zahtjevan zadatak. Na slici 42 ulazni signal ulazi u multiplekser, koji zatim dolazi do sklemblera, dok se iz generatora kontrolnih riječi generiše kontrolna riječ. Kontrolna riječ istovremeno šalje se skrembleru i *ECM* enktiptoru radi procesa enkripcije. Trenutna i sledeća kontrolna riječ šalju se *ECM* enkriptoru koji nakon enkripcije *ECM* šalje u multiplekser radi daljeg dodavanja u trasnportni strim. Sada TS ulazi na ulaz STB-a. Normalni signal bi išao direktno u deskrembler, dok *ECM* ide

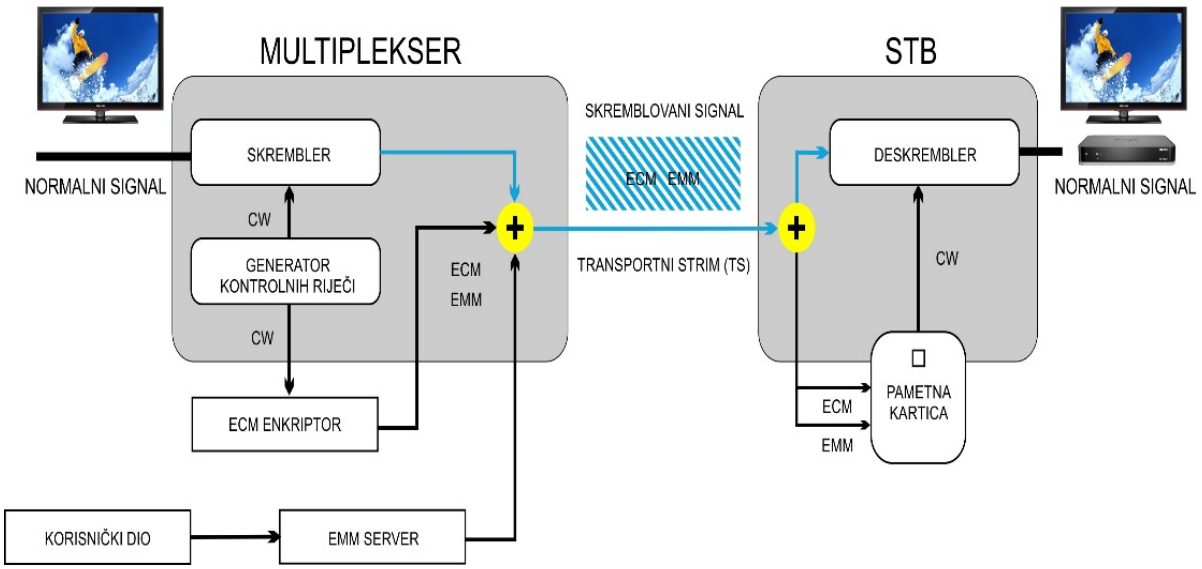
direktno na pametnu karticu. Pametna kartica čita ECM, dekriptuje ga i šalje kontrolnu riječ STB-u. *STB* uređaj prima kontrolnu riječ i vrši deskremblovanje signala što dovodi do izlaznog signala koji nije više enkriptovan i koji krajnjem korisniku daje regularnu sliku. *EMM* se uglavnom ponavlja svakih 100ms. Razlog za ovako često ponavljanje je omogućavanje *STB* uređaju deskremblovanje signala za što kraće vrijeme.

Sadržaj *ECM* poruke nije unikatan već može da varira od provajdera do provajdera, ali uglavnom sadrži sledeće informacije:

- Dvije kontrolne riječi – na ovaj način omogućava se slanje trenutne ali i sledeće ključne riječi radi lakšeg dekodiranja.
- Informacije o datumu i vremenu – pametne kartice na ovaj način mogu da odluče da li je korisniku omogućeno gledanje kanala ili ne.
- Indentifikacija kanala – može biti jedinstvena po kanalu ili dijeljena između svih kanala u okviru paketa pretplate. Indetifikator kanala omogućava pametnoj kartici da provjerava da li je kanal dostupan u okviru svoje tabele pristupa.

4.1.2. EMM (Entitled Management Message)

U *CA* sistemu *EMM* enkripcija se koristi radi slanja podataka pametnoj kartici, poput informacija da li je korisniku dozvoljeno gledanje određenog servisa, da li je korisniku dozvoljeno gledanje kanala idućeg mjeseca i slično. *STB* prima *EMM* i prosleđuje ih pametnoj kartici radi dalje obrade. Na taj način pametna kartica koristi informacije od EMM-a za ažuriranje internih pristupnih kontrola bazi podataka. Baza podataka sadrži listu kanala i video na zahtjev-*VOD* (*eng. Video on demand*) koji su dostupni korisniku. *EMM* može omogućiti pregledanje sadržaja *VOD*-a u vremenskim intervalima od nekoliko sati do nekoliko mjeseci, kao i omogućavanje gledanja sadržaja [9] na jednom ili više kanala. Kada pametna kartica primi *EMM* ona taj podatak upoređuje sa svojom bazom podataka čime odlučuje da li korisnik može pristupiti kanalu ili ne. Ukoliko korisnik ima pravo pristupa, dekodirana kontrolna riječ šalje se STB-u koja zatim deskrembluje signal.

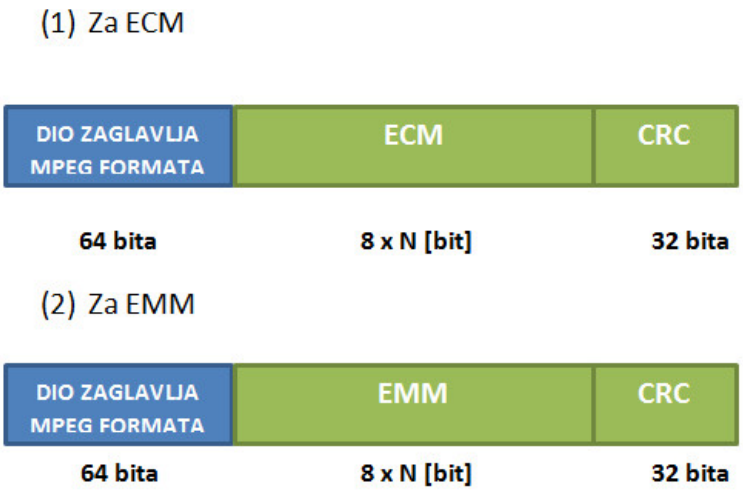


Slika 43 -Princip rada EMM-a

Kao što se vidi sa slike 43 ulazni signal ulazi u multiplekser i zatim se šalje skrembleru. Skrembler prima CW iz generatora kontrolnih riječi i skrembluje ga tako da su *ECM* i *EMM* importovane u trasportni strim. Kad god se dozvoli pristup krajnjem korisniku za novi servis *EMM* se generiše od strane CAS-a [4] i taj novi generisani *EMM* šalje se multiplekseru radi daljeg importa u transportni strim. Na drugom kraju pametna kartica prima *EMM* i *ECM* signal i šalje ga deskrembler. Pametna kartica dekriptuje *ECM* i *EMM* omogućavajući korisniku traženi servis, a zatim se kontrolna riječ šalje deskrembleru. Tek nakon što deskrembler primi kontrolnu riječ počinje deskremblovanje signala i na izlazu korisnik dobija traženi servis.

Za razliku od ECM-a, *EMM* poruke se ne mijenjaju toliko često, već se mijenjanju u mjesečnim intervalima. Naravno, ovaj način mijenjanja EMM-a može biti problematičan za provajdere, jer predstavlja vid zaštite koji može biti meta napada. Svaki provajder može izabrati svoj vremenski interval mijenjanja EMM-a. Sadržaji ECM-a i EMM-a nisu standardizovani i kao takvi zavise isključivo od *CA* sistema u upotrebi. Kontrolne riječi mogu biti prenošene i kroz različite ECM-ove odjednom, omogućavajući korišćenje različitih *CA* sistema u isto vrijeme, odnosno omogućavajući *Simulcrypt*.

Sistem koji koristi MPEG multipleksere šalje *ECM* i *EMM* poruke kroz konfiguracije signala poput one prikazane na slici 44.



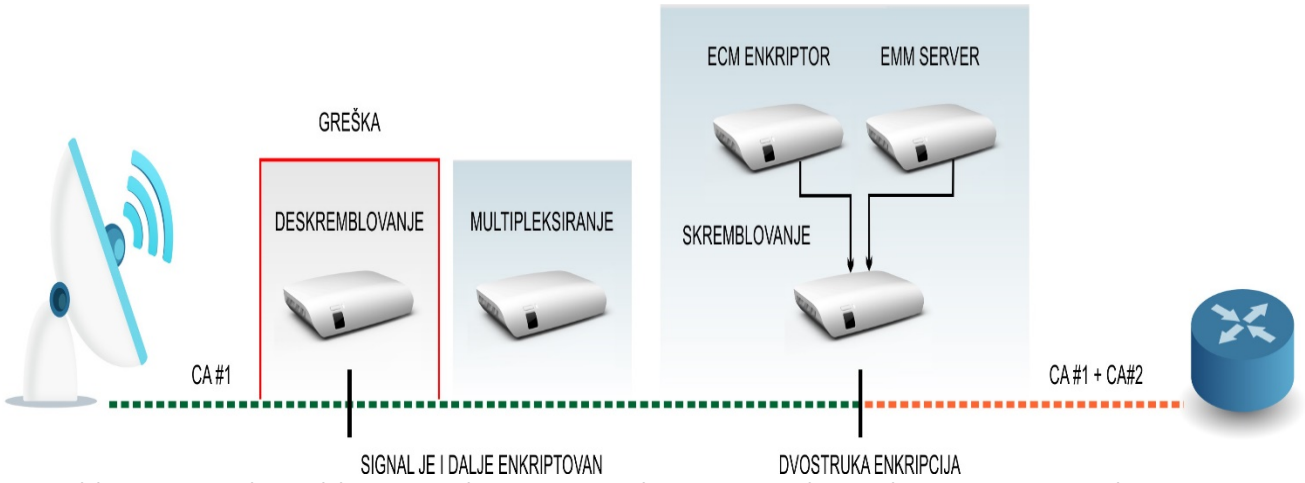
Slika 44 - Primjer konfiguracije signala potrebnom za slanje ECM i EMM poruke

EMM poruke enkriptovane su metodama poznatim isključivo *CA* provajderu, ali i pored ovog visokog stepena zaštite sadrže sledeće informacije:

- Dužinu polja EMM-a - podatak koji nije enkriptovan.
- Polje za adresu – podatak koji nije enkriptovan.
- Enkriptovani dio – adresno polje *EMM* dozvoljava STB-u filtriranje EMM-ova tako što šalje relevatne EMM-ove pametnoj kartici za obradu.

4.2. Kontrole grešaka ulaznog signala

Većina kablovskih i *IPTV* operatera prima značajni dio ulaznih signala u enkriptovanoj formi, najčešće preko satelita. To znači da će kanali dolaziti od različitih provajdera, pri čemu će svaki provajder imati različite *CA* sisteme.
Prvi korak pri radu digitalne televizije je dekodiranje ulaznih signala koje se uglavnom obavlja direktno u multiplekserima.
Ukoliko ulazni signal iz nekog razloga ne može biti deskremblovan, signal će i dalje biti enkriptovan ili kodiran *CA* sistemom. Tada, signal će ponovo biti enkriptovan operatorovim *CA* sistemom, što dovodi do situacije da je signal dva puta enkriptovan (slika 45). Korisnicima ovakav signal prikazuje se kao “crna slika”.



Slika 45 - Deskremblovanje ulaznog signala nije uspjelo i enkriptovani signal se dovodi do skremblera.

Problemi sa skremblingom najčešće se javljaju zbog:

- Hardverske greške deskremblera.
- Hardverske greške pametnih kartica.
- Pametne kartice nisu pravilno postavljene ili nepostoje.
- Nad pametnim karticama nije izvršena autorizacija (*EMM* nedostaje ili nije validan).
- Ulazni signal ima pogrešan ili nedostajući ECM.
- Postoje problemi sa autorizacijom na strani digitalnog TV provajdera.

Da bi se ovi problemi izbjegli poželjno je izvršiti monitoring signala nakon deskremblinga, u momentima prije nego što se signali enkriptuju. Najjednostavniji pristup bi bio provjera skremblovanih kontrolnih bita transportnih strim paketa. Da bi se ipak monitoring izvršio na što pravilniji način potrebno bi bilo detaljno analizirati dolazni signal, naročito video *PID (eng. Proportional Integral Derivativ)*. Najsigurniji način provjere bi bio sama provjera da li je omogućeno audio i video dekodiranje i u slučajevima kada je to moguće da se generiše kratak prikaz audio i video signala radi pravilne procjene. Pored ovog načina kontrole grešaka poželjna je i detekcija signala pri zamrznutoj slici ili detekcija problema poput “crnog ekrana” radi što preciznijeg monitoringa.

4.2.1. Kontrola i monitoring EMM-a i ECM-a

EMM poruke neprekidno se prenose od *CA* sistema prema multiplekseru koji *EMM* poruke unose u trasportni strim. Ovo se radi putem mrežnih protokola, preko IP adrese i UDP/TCP protokola. U slučajevima kada *EMM* poruke nisu prisutne problem može biti:

- Gubitak mrežne konekcije između *CA* sistema i multipleksera.
- Greška u serverima *CA* sistema.
- Greška u multiplekseru.

U realnim situacijama monitoring EMM-a koji može da detektuje sve probleme nije moguće isprojektovati. Dodavanje opreme koja generiše alarme u slučajevima kada *EMM bitrate* pada ispod određenog nivoa omogućiće značajniju zaštitu, samim tim detekciju i riješavanje grešaka prije nego što te greške dođu do krajnjeg korisnika. Računanje *bitrate*-a na intervalu od jedne sekunde dovešće do kreiranja lažnih alarma, što će dovesti do situacije da EMM-ovi nedostaju na par sekundi. Kao efikasno riješenje pokazalo se mjerenje bitrate u varijabilnom vremenskom periodu, odnosno vremenskim intervalima koji nisu standardni već zavise od same situacije.

Prilikom prebacivanja na kanal *STB* uređaju su potrebne kontrolne riječi radi deskremblovanja sadržaja određenog kanala ali i radi dekodiranja istog. Ovo znači da je transmisioni interval ECM-a veoma važan bez obzira na vrijeme prebacivanja između kanala. Netačan interval ponavljanja kod ECM-a uglavnom je uzrokovan netačnom konfiguracijom multipleksera ili internih problema u okviru rada multipleksera. Ukoliko *ECM* ne postoji *STB* će biti u nemogućnosti da deskrembluje signal čime se korisniku na prijemu prikazuje poruka tipa 'Nema signala'. Do greške nedostajućih ECM-ova uglavnom dolazi zbog greške *CA* sistema i *ECM* enkriptora, pogrešne konfiguracije multipleksera, mrežne greške između multipleksera i *CA* sistema.

Da bi se provjerilo *ECM* ponavljanje potrebno je pronaći sve ECM-ove za sve servise u signalu. ECM-ovi se uglavnom signaliziraju tako što ostavljaju *CA* dekriptor u program info sekciji *PMT* tabele (*eng. Program Map Table*). Ovo omogućava da se isti *ECM* prenese na *PID* komponente servisa. Kada se pronađe lista ECM-ova ona treba da primi sve podatke, različite vrste *ECM* PID-ova i da provjeri interval između različitih *ECM* paketa. Maksimalno dozvoljeno vrijeme između ECM-ova određuje sam provajder i najčešće iznosi 100ms.

4.2.2. Monitoring kontrolne riječi i PID-ova

Kontrolna riječ koja se koristi za enkripciju transportnih *stream* paketa konstantno se mijenja u vremenskim intervalima od 10ms. Ukoliko kontrolne riječi ne budu promijenjene *ECM* može iskoristiti postojeće kontrolne riječi radi dekripcije signala dokle god se ovaj problem ne riješi. U ovakvim situacijama krajnji korisnici mogu imati pristup kanalu čak iako im je operater zabranio pristup.
Gubitak kontrolnih riječi najčešće je prouzrokovan:

- Problemom između multipleksera, skremblera i *CA* sistema. Ovi problemi se najčešće dešavaju kad je *CA* sistem fizički udaljen od multipleksera, npr. prilikom *VPN* (*eng. Virtual Private Network*) konekcije ili prilikom obavljana enkripcije podataka na samoj ivici mreže (*eng. network edge*).
- Problemom sa *ECM* enkriptorom *CA* sistema. Ovo može biti prouzrukovano hardverskim i softverskim greškama, samim operativnim sistemom ili greškama *CA* aplikacija koje se nalaze na serveru.
- Problemom sa multiplekserom skremblera. Ovi problemi najčešće se javljaju progrešnom konfiguracijom uređaja ili softverskim problemima na samom multiplekseru.

Monitoring kontrolnih riječi, odnosno njegovog mijenjanja omogućava operateru detekciju ovih situacija čak i prije nego što se pojavi problem. U sistemima bez monitoringa ovi problemi mogu potrajati nedjeljama ili mjesecima.
Nakon što signal prođe multiplekser koji obavlja skremblovanje postavlja se set PID-ova koji moraju biti skremblovani u svakom trenutku kao i set PID-ova koji se ne skrembluje (čisti PID-ovi). Oprema za monitoring trebala bi da ima mogućnost za pregled PID-ova odnosno za deskremblovanje. Da bi se obavile ove promjene dovoljno je provjeriti kontrolne bite skremblovanja. Za skremblovanje operater može da izabere nekoliko opcija:

- PID-ovi uvijek moraju biti skremblovani. Ukoliko se desi da *PID* nije skremblovan aktiviraće se alarm. Ista ova situacija važi i u slučajevima kada očekujemo čiste, a dobijemo skremblovane PID-ove.
- *PID* nikad ne smije biti skremblovan. U tom slučaju će se takođe aktivirati alarm. Ova situacija se najčeše koristi kada sadržaj iz nekih razloga ne smije biti enkriptovan.

4.2.3. Monitoring EMM povratnog vremena

Parametar koji je od velikog značaja za provajdere je povratno vrijeme EMM-a. Provajder uglavnom želi da iskoristi što manje raspoloživog opsega za *EMM* saobraćaj. Veliki provajderi imaju oko 100 hiljada pametnih kartica, što povlači situaciju gdje je potrebno izvršiti autorizaiju EMM-ova za kanale za koji su korisnici prijavljeni. EMM-ovi se uglavnom šalju mnogo ranije tako da za *STB* uređaje koji su uvijek konektovani na mrežu povratno vrijeme EMM-a nije od velikog značaja. Međutim, povratno vrijeme EMM-a je bitno u situacijama kada je *STB* ugašen na duži vremenski period, jer tada pametna kartica mora biti ažurirana prije desklemblovanja signala. Ovaj vremenski period traje dosta dugo (ova procedura bi trebala najduže da traje oko 15 min), što dovodi do žalbi korisnika, što bi svaki provajder nastojao da izbjegne. *EMM* playout ima različite prioritete za EMM-ove, tako da u situacijama gdje korisnik kupi pristup novom setu kanala EMM-ovi se uglavnom stavljaju na veći prioritet i samim tim se ponavljaju češće. *CA* sistem provajderi ne žele da dijele detaljnije informacije o EMM-ovima, tako da je za monitoring povratnog vremena EMM-a potrebno znati njegov format bez enkripcije. To znači da ukoliko bi trebalo analizirati povratno vrijeme EMM-a potrebno je postići dogovor sa provajderom kao i doći do specifikacije *STB* uređaja koje provajder koristi.
Nakon što se saznaju ove informacije, povratno vrijeme treba izmjeriti na sledeći način:

- Izabrati broj *EMM* adrese za svaki različiti adresni tip
- Primiti sve EMM-ove za izabrane *EMM* adrese, izračunati i sačuvati *hash* enkriptovanog dijela *EMM-a*
- Kada se primi indentičan *EMM* moguće je izmjeriti povratno vrijeme

Nakon što se obavi dovoljan broj mjerenja statistička analiza se može izvršiti. Neki EMM-ovi se šalju samo jednom (prije nego što se promijene ili izbrišu) tako da se ne očekuje ponavljanje EMM-ova. Redosled će takođe biti različit za svaki *CA* sistem, ali će se uglavnom vidjeti povratno vrijeme. Grupisanjem sličnih mjerenja možemo dobiti povratno vrijeme za različite EMM-ove.
Za velike sisteme povratno vrijeme može biti do 30 minuta, ali može biti i duže ukoliko imamo *EMM* nižeg prioriteta, što dovodi do potrebe da se signal mjeri na veći vremenski period, radi što preciznijih informacija. Ukoliko su EMM-ovi indentični na svim trasportnim strimovima (kopiranje PID-a iz jednog multipleksera u drugi) dovoljno je izvršiti monitoring povratnog vremena jednog

povratnog strima. Međutim, ukoliko su EMM-ovi pušteni odvojeno za svaki TS poželjno je izvršiti monitoring svih raspoloživih frekvencija radi što preciznijeg vremena.

4.2.4. Provjera stanja ECM-a u odnosu na CW promjene

U svakom *PID* zaglavlju postoje dva bita koja dekoderu govore da li treba da koristi parne ili neparne kontrolne riječi. *ECM* uglavnom sadrži dvije kontrolne riječi, što mu omogućava da istovremeno nosi obje kontrolne riječi koje se trenutno koriste, kao i kontrolne riječi koje će se koristiti za skremblovanje prilikom iduće promjene kontrolne riječi. Ovo omogućava *STB* uređaju da uvijek ima na raspolaganju kontrolne riječi koje su potrebne za deskremblovanje sadržaja. Ukoliko promjene ECM-a nisu sinhronizovane sa promjenom kontrolnog ključa koji se koristi za enkripciju signala, može se desiti da *STB* uređaj neće biti u stanju da deskrembluje signal, čime dolazi do pojave „crne slike". Za promjene ECM-a važi da:

- *ECM* ne bi smio da se mijenja prerano, jer *STB* uređaj treba imati dovoljno vremena da deskrembluje sve TS pakete enkriptovane sa predhodnim skrembling ključem, prije nego sto se sam ključ promijeni.
- *ECM* ne bi smio ni da se mijenja prekasno, jer tada *STB* mora imati dovoljno vremena da dobije kontrolne riječi od pametne kartice i dovoljno vremena da ove informacije sačuva, prije nego što počne skremblovanje signala.

Neki *CA* sistemi za IPTV imaju ECM-ove koji sadrže samo jednu kontrolnu riječ. U ovim slučajevima *ECM* se mijenja prije promjene skremblovanja kontrolnih bita. Ukoliko bi izvršili monitoring ovog sistema oprema bi morala da isprati situaciju gdje se *ECM* mijenja i prije i poslije skremblovanja kontrolnih bita.

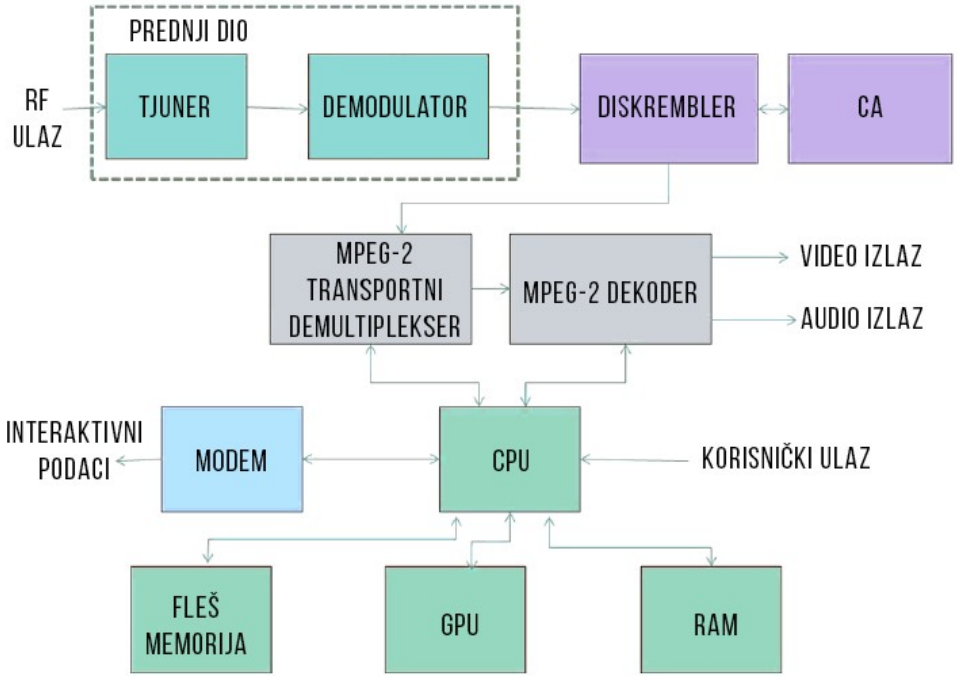
4.3. STB (Set Top Box) uređaj

Prenos digitalnih TV video signala može se obaviti preko različitih medijuma, bilo da je u pitanju prenos zemaljskim, kablovskim ili satelitskim putem. Digitalni TV signali koriste DVD-C standard za prenos kablovskim putem, DVD-T za zemaljski i

DVD-S za satelitski prenos. Poređenje TV signala može se obaviti preko MPEG2 kompresije u svim varijantama, iako je proces modulacije u svakom od ovih slučajeva drugačiji.
STB predstavlja uređaj čiji je zadatak pretvaranje prenošenog digitalnog signala u tip signala koji može biti prikazan na medijumima poput LED, LCD i analognim televizorima. Svaki *STB* prijemnik sadrži demodulator signala i *tuner.* Hardverska konfiguracija svih DVD resivera je indentična, osim u slučajevima demodulatora koji je različit za svaki tip *DVB* resivera. Arhitektura STB-a se može podijeliti na dva tipa, tip otvorene arhitekture i *interperablue*. Ako posmatramo *STB* kao skup funkcionalnih blokova odnosno modula, primijetićemo da svaki modul obavlja tačno definisanu funkciju, i kao takav može biti sastavljen isključivo od hardvera ili softvera, odnosno njihove kombinacije.

4.2.5. Funkcionalnost STB-a

Glavni moduli *STB* uređaja su: demodulator, deskrembler, *CA* modul, MPEG2 transportni demultiplekser, MPEG2 enkoder, CPU i modem (slika 46). Sam *STB* je podešen tako da od raznih frekvencija koje se nalaze u etru funkcioniše samo sa jednom dodijeljenom frekvencijom. Demodulator ima zadatak da konvertuje RF signal u orginalni signal, a njegov izlaz predstavlja MPEG2 transportni strim.



Slika 46 - Šema STB uređaja

Pored ulaznog i izlaznog signala *STB* uređaji uglavnom sadrže neku vrstu modema, namijenjenog za primanje i slanje interaktivnih podataka. Tradicionalni telekomunikacioni modemi su česta pojava u satelitskim i zemaljskim *STB* uređajima.
Provajderi digitalnih TV servisa najčešće enkriptuju svoj MPEG2 transportni strim. MPEG demultiplekser bira i dekriptuje audio i video signal za odgovarajući kanal kojeg krajnji korisnik želi da gleda, uz pomoć dekripcionih ključeva obezbijeđenih od strane *CA* sistema. MPEG dekoder kompresuje audio i video informaciju za izabrani program, dok CPU nadzire cijeli tok kodiranja. Ukoliko bi *STB* uređaj trebao da postane interoperabilan za sva tri prenosna medija (zemlja, kabal, satelit) tjuner i demodulator, koji čine *Front End STB* uređaja, moduli bi morali biti zamjenjivi. Kad god MPEG2 TS sadrži enkriptovan ili skremblovani podatak TS sadrži dva tipa skremblovanih poruka - *EMM* i ECM. *EMM* sadrži listu servisa kojima krajnji korisnik može da pristupi, kao i datum do kojeg im je dozvoljen pristup.
Kako se *ECM* i *EMM* podaci koriste radi kontrole servisa logično je da svaki *CA* sistem, odnosno svaki provajder koristi različiti algoritam enkripcije. Samim tim efikasnosti *ECM* i *EMM* enkripcije strogo se čuvaju od strane operatera, jer eventualna njihova dekripcija može dovesti do zloupotrebe komplentnog *CA* sistema. Da bi STB-u bio omogućen rad na različitim mrežama potrebno je iskoristiti sam *DVB* signal u vidu internacionalnog standarda *DVB* CI (*eng. Digital Video Broadcasting Common Interface*) .
Na slici 46 prikazana je verzija *STB* uređaja koji je u stanju da primi bilo kakav tip *broadcast* signala. U ovom slučaju *CA* sistem se posmatra kao odvojeni modul, koji komunicira sa *STB* uređajem preko *DVB Common Interface* konektora. Na ovaj način ukoliko korisnik želi da promijeni provajdera na svom *STB* uređaju *DVB* CI konektor omogućiće mu potrebnu interoperabilnost.

4.2.6. Softver STB uređaja

Svaki *STB* uređaj mora da sadrži odgovarajući softver koji omogućava pravilan rad sa hardverom kao i zakazivanje zadataka u realnom vremenu, pravilnu raspodjelu memorije, monitoring video i audio signala itd. Ovaj softver u vidu *STB* operativnog sistema smješten je u ROM memoriji u nivou kernela. Prilikom startovanja STB uređaja kernel se učitava i u memoriji ostaje dokle god je *STB* upaljen. Kernel je uglavnom zadužen za raspodjelu memorisjkih resursa, prenos *real time* aplikacija i *Hi-Speed* podataka, omogućavajući *multireading* i

multitasking, dozvoljavajući STB uređaju paralelno procesiranje različitih podataka ili sekcija. Postoje više različitih *STB* operativnih sistema, pri čemu većina velikih kompanija, odnosno provajdera u okviru *STB* uređaja implementira svoj OS-operativni sistem. Tako *STB* uređaj može da radi na operativnim sistemima poput: Power TV OS, Vx Works PSO System, Microware's DAVID OS-9, Microsoft Windows CE itd. Da bi cijeli proces funkcionisao kako treba, na softversko hardevskom nivou, potrebno je izvršiti i određena ažuriranja *STB* operativnog sistema. Da bi hardveru STB uređaja ažuriranje bilo omogućeno *STB* mora da sadrži tkv. *loader*, aplikaciju odnosno program koji će obaviti ažuriranje, a koji se nalazi u samoj memoriji STB-a. Hardver STB-a da bi funkcionisao ispravno potrebno je da sadrži odgovarajuće drajvere.

Svaki operativni sistem STB uređaja uglavnom se dizajnira da podrži određeni tip mreže, što znači da ukoliko se *STB* uređaj priključi na drugi tip mreže može doći do situacije da softver STB uređaja nije kompatabilan sa postojećim mrežnim zahtjevima, čime se automatski gubi interoperabilnost između STB-a i različitih mreža. Međutim, i ovaj problem se može riješiti korišćenjem MHP standarda (*eng. Multimedia Home Standard*) baziranom na nezavisnoj Java platformi (slika 47). Tada operativni sistem uz pomoć Java virtualne mašine konvertuje Java kod u kod razumljiv samom uređaju.

Slika 47 -MHP (Multimedia Home Standard) model

4.4. Nivo skremblovanja TS-a i kontrola polja skremblovanja

Glavna jedinica za skremblovanje i deskremblovanje je MPEG-2 transportni strim paket. Svaki paket se skrembluje nezavisno od ostalih paketa omogućavajući nasumičan pristup svakom od paketa. Sam paket sadrži zaglavlje i dodatna polja koja ostaju nepopunjena (slika 48). *AES* 128 koristi se za enkriptovanje blokova od 16 bajtova podataka od određenog TS paketa.

Slika 48 - Skremblovani TS paket

Metod *PES* (*eng. Packetized Elementary Stream*) skremblovanja zahtijeva da zaglavlje *PES* paketa nije skremblovano i da TS paket sadrži djelove skremblovanog *PES* paketa bez polja za adaptaciju. Zaglavlje skremblovanog *PES* paketa ne smije sadržati različite TS pakete. TS paket sadrži početak skremblovanog *PES* paketa i sadržan je u *PES* zaglavlju i prvom dijelu *PES* paketa. Na ovaj način prva cjelina *PES* paketa skremblovana je kao i TS paket sličnog sadržaja. Preostali dio *PES* paketa podijeljen je u super blokove od 184 bajta. Svaki super blok skremblovan je kao i sadržaj TS paketa od 184 paketa. Kraj *PES* paketa podudara se sa krajem TS paketa, tako što se na početku polja za adaptaciju dodaju određeni prazni bajtovi. Ukoliko dužina *PES* paketa nije 184 bajta, skremblovanje zadnjeg dijela *PES* paketa (1 do 183 bajta) indentično je TS paketu sličnog sadržaja. Dijagram skremblovanih *PES* paketa u TS paketima je prikazan na slici 49.

Slika 49 - Pregled PES skremblovanog paketa

MPEG2 sistemi sadrže skremblovanu kontrolu polja od 2 bita, oba u zaglavlju TS paketa i zaglavlju *PES* paketa (slika 50). Značenje ova dva bita je definisano MPEG2 standardom. Tabela 5 definiše skremblovane kontrolne bite i zaglavlja TS paketa.

Slika 50 – TS skrembling

TSC	Značenje
00	Bez skremblovanja
01	Rezervisano
10	Skremblovanje sa parnim ključem
11	Skremblovanje sa neparnim ključem

Tabela 5 - Kontrolne vrijednosti transportnog skremblinga

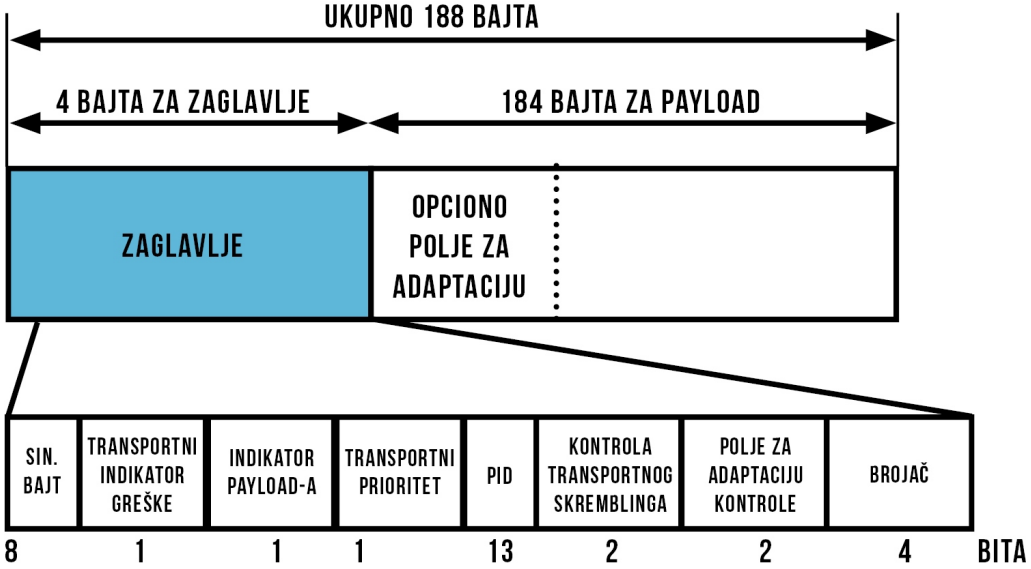
Prvi skremblovani kontrolni bit označava da li je sadržaj skremblovan, dok drugi kontrolni bit označava korišćenje parnog ili neparnog ključa. Ukoliko sadržaj TS paketa nije skremblovan na TS nivou skremblovanje podataka se i dalje može definisati na *PES* nivou. Tabela 6 označava skremblovanje kontrolnih bita u zaglavlju *PES* paketa koji su slični onima na TS nivou.

Bitska vrijednost	Značenje
00	Bez skremblovanja *PES* paketa
01	Rezervisano za buduce *DVB* korišćenje
10	*PES* paket skremblovan sa parnim ključem
11	*PES* paket skremblovan sa neparnim ključem

Tabela 6 - Kontrolne vrijednosti PES skremblovanja

Dva transportna skremblovana kontrolna bita prikazuju da li je TS paket skremblovan ili nije. Ukoliko oba bita imaju vrijednost nula, sadržaj podataka je poslat neskremblovan. Ako jedan od dva bita nije nula, sadržaj se šalje skremblovan i tada je potrebna *CA* tabela radi deskremblovanja sadržaja.

Ova dva bita impliciraju da li postoji zaglavlje produženog formata, poput polja za adaptaciju. Ukoliko su oba bita postavljena na vrijednost nula, polje za adaptaciju ne postoji, u suprotnom dio bita za prenos podataka se skraćuje čime zaglavlje postaje duže, dok ukupna veličina paketa i dalje ostaje 188 bajta (slika 51).



Slika 51 - Detalji MPEG-2 transportnog strima

Svaki TS paket sa istim PID-om šalje četvorobitni brojač. Ovaj brojač broji od 0 do 15 svaki TS paket, nakon čega se resetuje na nulu. Na ovaj način moguće je prepoznati TS pakete koji nedostaju i pronaći tokove podataka nad kojima je došlo do prekida brojanja.

Oprema u broadcast stanicama određuje konfiguraciju TS-a, tako da pored audio vizuelne komponente TS sadrži PSI (eng. Program Specific Information) i PSI tabele, PAT (*eng. Program Association Table*), *PMT* (*eng. Program Map Table*), CAT *(eng. Conditional Access Table).* PAT tabela sadrži listu svih trenutno dostupnih programa i prosljeđuje PIB vrijednosti programskoj tabeli PMT. Postoji samo jedan PAT, ali *PMT* tabela postoji koliko postoji i programa i svaki *PMT* omogućava uvid u informacije o samom strimu (audio i video data, ali sadrži i listu svih parametara potrebnih za dekodovanje). CAT tabela se koristi radi signalizacije, radi određivanja PID-ova koji će se u transportnom strimu koristiti za EMM. Postoji samo jedna CAT tabela po TS-u i ona sadrži spisak svih *CA* dobavljača koji rade sa servisima pronađenim u okviru TS-a. Jedinstveni identifikator *CA_System_ ID* prepoznaje *CA* dobavljače, dok CAT tabela dostavlja informacije o EMM-u i ECM-u. TS nosi odgovarajuće pakete skremblovanim signalima i nosi istovremeno pakete informacija o programima, kojima je pristup omogućen bez ograničenja.

4.5. Vrste enkripcija

Tokom razvijanja prenosa analogne televizije, korisnicima je omogućavan veliki broj kanala. Čak i u domenu analognih signala svi signali koje bi krajnji korisnici primili bili bi kodirani, onemogućivši ostalim korisnicima pristup plaćenim sadržajima. Veliki provajderi razvijali su sopstvene algoritme zaštite, a jedan od popularnijih algoritama zaštite bio je sistem kodiranja V*ideocrypt 1* i V*ideocrypt 2,* razvijen od kompanije 'News Datacom'. Ovi sistemi pružali su određeni stepen zaštite za obične korisnike, međutim, i pored ovih stepena zaštite sami sistemi su imali nedostatke koje su pojedine organizacije uspjele da eksploatišu. Prebacivanjem na digitalnu televiziju stepeni zaštite značajno su poboljšani, a jedna od najpopularnijih vrsta zaštite, koja se koristi i kod nas u Crnoj Gori, jeste *Videoguard* sistem kodiranja. Pored ovog sistema enkripcije digitalne televizije postoje i drugi sistemi poput *Mediaguard, PowerVU, Cryptoworks, Nagravison, CISCO Videoscape, Viacess* itd. Svi ovi sistemi pokrivaju najveći dio zaštite digitalne televizije i kao takvi često su meta hakerskih napada, ali i predmet akvizicije velikih kompanija poput CISCO-a. Neki od sistema zaštite su tokom vremena otkriveni, čime je dolazilo do njihovih zloupotreba, a samim tim i do definisanja novih standarda enkripcije digitalne televizije.

4.5.1. Cisco Videoguard (NDS) sistem enkripcije

Poznatiji svetski provajderi poput: TotalTV (Balkan), SBB (Serbia), DirecTV (Colombia), Sky Brazil (Brazil), ONO (Spain), China Central Television (China), koriste 'Video Guard' sistem kao svoj tip enkripcije.
Videoguard je metod enkripcije razvijen za prenos zaštićenog sadržaja digitalne televizije, omogućavajući prenos i drugih servisa poput interneta. Kako se digitalni signal prenosi preko razne opreme za emitovanje od satelita do radio tornjeva i sličnih uređaja za emitovanje signala, *NDS* omogućava prepoznavanje traženih servisa bilo da je u pitanju određeni kanal, internet ili neki drugi zahtjev od strane krajnjih korisnika. Indentični signal se šalje do svih krajnjih korisnika, što znači da NDC enkripcija mora biti ugrađena u okviru *STB* uređaja. Ovaj sistem funkcioniše tako što je jedan od čipova programiran u različitim enkripcionim nivoima, pri čemu je svaki nivo dizajniran da blokira određeni dio sadržaja koji primi. Kada

korisnik zatraži otključavanje ili zaključavanje novih servisa provajder promjenom podešavanja enkripcije može ispuniti korisnikov zahtjev.
Prednosti *NDS*-a ogledaju se u jednostavnoj intergraciji sa *STB* uređajima i mogućnosti zaštite *Pay-Per-View* sadržaja impementirajući geolokacijsku zabranu.
I pored svoje efikasnosti u kontroli sadržaja neki korisnici su uspjeli da iskoriste princip rada *NDS*-a u svoju korist, tako što bi implementirali enkripcioni čip na kome su omogućeni svi kanali u drugi *STB* uređaj koji nije imao pristup određenom sadržaju. Međutim, neki od *NDS* čipova su programirani za rad sa isključivo jednim *STB* uređajem, onemogućavajući bilo kakvo ažuriranje, čime krajni korisnik čak i nakon zamjene čipa gubi pravo gledanja sadržaja na određeni vremenski period.

4.5.2. Cisco Videoscape sistem enkripcije

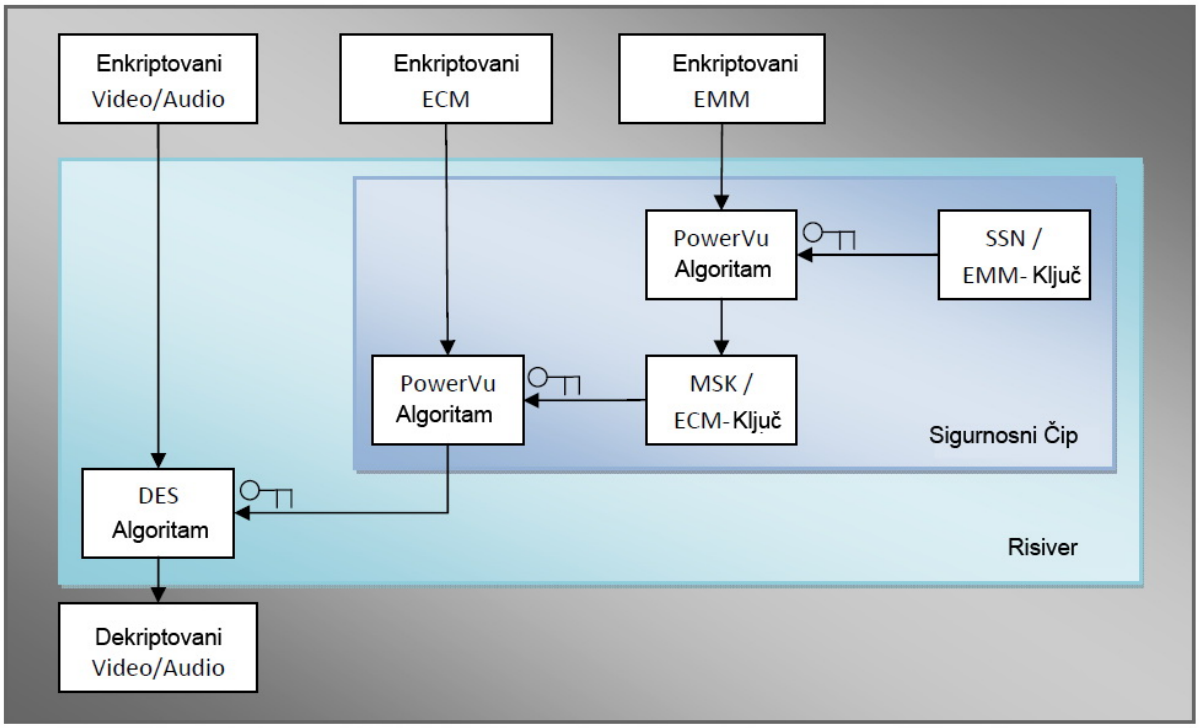
Još jedan od servisa vezanih za enkripciju koji CISCO omogućava je *Videoscape*, kupljen 2012. godine od strane CISCO-a. Pouzdanost *Videoscape-a* ogleda se u činjenici da ga koristi preko 85 TV provajdera širom svijeta, pri čemu sama tehnologija uključuje servise povezivanja za satelite Broat bend ATV, ERG, omogućavajući DRM *(eng. Digital Right Management*) zaštitu za plaćeni program.

4.5.3. Viacess sistem enkripcije

Viaacess je sistem zaštite digitalne televizije razvijene od strane Orange C.A. U upotrebi postoji šest različitih varijanti ovog sistema - *Viaccess* PC 2.3, 2.4, 2.5, 2.6 ,3.0, 4.0, 5.0, 6.0. *Viacces* PC 2.3 i 2.4 pokazali su se kao veoma neefikasni, jer su *STB* uređaji mogli biti modifikovani tako da prikazuju sadržaj koji ne bi trebao biti dostupan. Iako je verzija PC 2.3 prikazana kao neefektivna ona je koristila *TPS Crypt* sistem zaštite, sistem koji je *AS* (*eng. Advanced System*) ključeve mijenjao jednom nedjeljno, da bi nakon zaobilaženja PC 2.3 zaštite bio razvijen novi *TPS* sistem koji *AS* ključeve mijenja nakon svakih 12 minuta. Na ovaj način isključivo *TPS* resiveri mogli bi prihvatati *AS* ključ, dok bi ostali ključevi bili eliminisani. Ovo je dovelo do problema same zaštite jer su pojedine organizacije softverski mogli iskontrolisati predviđanja *AS* ključeva, praveći bazu aktivnih ključeva.

4.5.4. Power VU sistem enkripcije i analiza njegove zaštite

Power Vu spada u *CA* sistem enkripcije digitalne televizije, sa ciljem zaštite sadržaja kojem se može pristupiti nakon zadovoljavanja određenih kriterijuma postavljenim ovim standardom. Power Vu se smatra veoma sigurnim sistemom zaštite, zbog komplikovanog sistema autorizacije svakog *Power VU* resivera. Prednosti *Power VU* sistema obuhvataju jednostavna podešavanja, nepotrebnost internet konekcije i omogućavanje gledanja sadržaja bez čestih zamrzavanja slike. Međutim, kao i svaki sistem i *Power VU* ima i svojih mana. Sama kompleksnost njegove enkripcije dovodi do potrebe za što češćim mijenjanjem ključeva, što može dovesti do situacija da se ključevi mogu promijeniti u momentima kada to neodgovara krajnjem korisniku. I pored svoje kompleksnosti sistemi njegove zaštite su razotkriveni, čime su metode njegove dekripcije postale javno dostupne, od kojih će dio biti pokriven u nastavku ovog rada.



Slika 52 - Hijerarhija Power VU sistema za generisanje EMM ključeva

Sa slike 52 se vidi da se audio i video signali enkriptuju slučajnom promljenivom u vidu *DES (eng. Data Encryption Standard*) ključa. *DES* ključ se mijenja svakih par sekundi i enkriptuje preko *Power VU* algoritma i *ECM* ključa. *ECM* se uglavnom mijenja svakih par mjeseci. Sigurnosni čip od provajdera sadrži identični *ECM*

ključ. *ECM* ključ se enkriptuje preko *Power VU* algoritma i *EMM* ključa. Svaki sigurnosni čip ima pojedinačne *EMM* ključeve. Takođe, sigurnosni čip ima jedinstvenu adresu *UA (eng. Unicue Address*). Validan ključ uglavnom sadrži 7 nasumičnih bajtova, dok lažni ključevi u prva tri bajta sadrže sekvencu '00-00-000'. Po potrebi sam provajder može ubaciti lažni ključ umjesto validnog, ukoliko želi iz nekog razloga da učini sigurnosni čip neupotrebljivim. Da bi se otkrio *EMM* preko *brute force* napada nije dovoljno samo poznavati algoritam za generisanje ključa, potrebno je sadržati odgovarajuću šifru, odnosno kopiju *EMM* ključa, da bi se mogao otkriti EMM.

Primjer *EMM* sadržaja:
82 30 9B 10 99 01 0E 00 00 00 06 8F 00 5D 9C 8A 00 00 03
80 C2 72 68 28 3F F8 AF F8 16 13 FE D6 4D 95 32 AB 95 B2 F4 89 3F E8 62 3F 2B C3
80 C2 70 4B 2F 7F 5A 61 64 6B D0 D7 E7 24 B2 F7 F5 A6 16 46 BD 0D 7E 74 3F 34 61
80 C2 73 F6 BF 91 C9 F0 A1 25 40 EF 65 18 6D 52 66 62 C0 54 1C 0E F0 73 2E 3D 64
80 C2 71 EE 2F 4B D4 09 6C CD D0 67 6B 2E E2 F4 BD 40 96 CC DD 06 76 B4 FD 15 75
80 C2 76 DE 87 93 46 D1 7C 49 D6 0B E3 BD E8 79 34 6D 17 C4 9D 60 BE 3B B0 7B 66
5D F7 E4 01 (crc32)

Prva linija u okviru ove tabele (82) označava indentifikaciju tabele i prikazuje neenkriptovane informacije poput (UA 00 5D 9C 8A) od *ISE* (sigurnosnog) čipa koji obrađuje ovaj *EMM*. Svaka od narednih 5 linija je fiksne dužine i sadrži tekstualno zaglavlje (80), koje naznačava da je ostatak podataka enkriptovan preko *EMM* ključa i da mora biti proslijeđen od strane *ISE*-a. Na ovaj način *ISE* može da dekriptuje *EMM* i uskladišti podatke u internom *EEPROM*-u (*eng. Electrically Erasable Programmable Read-Only Memory)*. Poslednja linija *EMM*-a pokazuje četiri bajta i predstavlja *CRC-32* (*eng. Cyclic Redundancy Check*) *check* sumu predhodnih podataka. Međutim, *ISE*-u nije potrebno svih pet blokova iz zaglavlja za ažuriranje *ECM* ključa, zato što u zaglavlju nije sadržan samo jedan *ECM* ključ, već dva *ECM* ključa (parni i neparni ključ). Jedan ključ je u upotrebi, dok se drugi ključ može mijenjati. Ukoliko je parni ključ u upotrebi, provajder prilikom promjene ključa šalje isti parni, ali i novi neparni ključ.

Nakon *sto ISE* primi sve ključeve provajder će iskoristiti neparni ključ za enkripciju *ECM*-a. Zaglavlje *ECM*-a će otkriti da li je potrebno koristiti parni ili neparni ključ za dekripciju *ECM*-a. Ovo znači da je jedan blok dovoljan da ažurira parni *ECM* ključ, drugi blok služi za ažuriranje neparnog *ECM* ključa, treći blok se koristi da bi se aktivirali ključevi zaduženi za zatamljivanje slike kod parnih ključeva, jedna linija je zadužena za blokiranje slike kod neparnih ključeva i jedan od pet blokova koristiće

se za ažuriranje kodova zaduženog za prikaz tamnog ekrana. Ukoliko se posmatra prvih 5 blokova i ignorišu se prva tri bita koja izgledaju slično, može se primijetiti određena šema.

a) 80 C2 70 4B 2F 7F 5A 61 64 6B D0 D7 E7 24 B2 F7 F5 A6 16 46 BD 0D 7E 74 3F 34 61

b) 80C270**4B2F7F5A61646BD0D7E7**2**4B2F7F5A61646BD0D7E7**43F3461

Analizirajući dobijeni rezultat i koristeći mane *ISE*-a za svoju prednost došlo je do probijanja *Power VU* zaštite i do pojavljivanja softverskih rešenja za generisanje *EMM*-a odnosno ECM-a.

4.6. Algoritmi za kriptografiju i njihovo korišćenje u CA sistemima

U *CA* sistemima za kriptografiju uglavnom se koriste tri do četiri različite metode kriptovanja. Metoda ili tehnika simetričog ključa poput *DES* (*eng. Data Enryption Standard)* tehnike omogućava veoma brzu enkripciju, koja se može iskoristiti na pojedinačnim servisima. Međutim, problem ne leži u samoj brzini enkripcije već u distribuciji samog ključa. Sistemi javnog ključa poput *RSA* (*eng. Rivest-Shamir-Adleman)* algoritma rešavaju problem distribucije ključa ali su spori za dekriptovanje servisa. Algoritmi digitalnog zapisa mogu omogućiti ispravnu komunikaciju, dok sa *MAC* (*eng. Migration Authorisation Code*) kodovima možemo provjeriti samu ispravnost poruke [15] [16] [17].

***DES* algoritam** dizajniran je za enkripciju i dekripciju blokova podataka od 64 bita preko 64 bitnog ključa. Blokovi se sastoje od bitova numerisanih od lijeve strane prema desnoj, tako da je prvi bit sa lijeve strane bit 1. Dekripcija se može ostvariti samo ukoliko je poznat enkripcioni ključ, a proces prepoznavanja ključa obavlja se preko dekriptora.

***RSA* algoritam** predstavlja primjer algoritma namijenjenog za kriptografiju javnim ključem, kod kojeg su enkripcioni i dekripcioni ključevi različiti, uz mogućnost enkripcije bloka podataka.

MD5 *(eng. Message Digest Algorithm 5)* algoritam uzima dužinu poruke kao ulazni podatak, dok je izlaz 128 bitni „otisak“ samog ulaza. Njegova namjena je prije svega omogućavanje digitalnog potpisa podataka, u situacijama kada veliki fajl

mora biti kompresovan i provjeren na što sigurniji način, prije nego što se nad njim obavi enkripcija putem ključa.
Strukturne poruke *ECM* i *EMM* se prenose od početka do kraja procesa preko troslojne distribucije ključa. Ova tri sloja ključa obuhvataju kontrolni ključ, periodični ključ i distribucioni ključ. Svaki od ovih nivoa koristi se za enkripciju i prosleđivanje ključeva.
Periodični ključ koristi se za enkripciju kontrolne riječi i pristup *ECM*-u, pri čemu je svaki periodični ključ u kanalima različit. Kontrolne riječi kao i periodični ključ se ažuriraju u toku određenog vremenskog intervala i nikada nije javno dostupan samom korisniku. Distribucioni ključ koristi se isključivo za enkripciju periodičnog ključa i on je jedinstven za svakog korisnika. Njegovi podaci uglavnom se nalaze na pametnoj kartici i nisu javno dostupni korisniku. Enkripcija kontrolne riječi obavlja se preko periodičnog ključa i *DES* enkripcije.
Kontrolne riječi, periodični ključ i preostali broj bita od ukupnih 320 bitova kombinuju se u vidu poruke nad kojim se izvršava *MD5* autentifikacija koda poruke *MAC*. Sama poruka (*stream*) sadrži informacije o programskom broju, broju provajdera, blokiranju slike, preostalom vremenu programa, brzom pregledu sadržaja itd. Enkriptovana kontrolna riječ, *MAC* i bitovi podataka postaju *ECM*. Periodični ključ je vezan za digitalni potpis i enkodovanim javnim ključem preko *RSA* enkripcije. *EMM*-ovi se adresiraju ka određenim pretplatnicima radi autorizacije pristupa programima. Enkriptovani su putem distribucionog ključa vlasnika kartice. Ove poruke daju pretplatnicima pristup informacijama i pristup *ECM* porukama. Slanje ovih poruka obavlja se periodično, a broj pretplatnika i vrijeme ažuriranja određuju vremenski period transmisije.
Sigurnosni modul, najčešće u obliku pametne kartice, izvlači *EMM* i *ECM* radi procesa dekripcije. Sigurnosni modul je ili intergrisan u *STB* uređaju ili ugrađen u PC karticu. Dekripcija *EMM*-a obavlja se preko privatnog dijela *RSA* ključa i provjerava se digitalni potpis periodičnog ključa. Ukoliko je *ECM-MAC* validan informacija u podacima se čuva u okviru samog *STB* uređaja. Periodični ključ koristi se radi dekripcije kontrolne riječi, dok se za individulane servise koristi DES ključ.

4.7. Vrste napada na CSA sistem i njegove slabosti

Većina hakerskih napada na *CSA* sistem dovodio bi *DVB* signal, koji bi i dalje bio enkriptovan, a samim tim i nečitljiv, tako da za većinu napada meta nije bio *CSA* sistem, već sistemi zaduženi za razmjenu ili generisanje ključeva (*Conax, Irdeto, VideoGuard*...). Napadi su se sastojali od razbijanja algoritamskih sistema, presretanja generisanih ključeva u realnom vremenu i distribucije ključeva putem dijeljenja kartice (*Card Sharing*).
Dio vezan za šifru strima koristi tkz. *beat slicing*, softversku implementaciju tehnike koja omogućava dekripciju blokova ili dekripciju istog bloka, pomoću različitih ključeva istovremeno. Sa stanovišta zaštite ovaj sistem je podložniji *brute force* napadima, iako je u realnom vremenu teško za očekivati da će bilo koji *brute force* napad uopšte ugroziti ovaj dio *CSA* sistema. Sa druge strane šifrarnik bloka je kompleksniji za *beat slicing*.

4.7.1. Brute force napad

Podaci u *CS* sistemu istovremeno su zaštićeni i preko blok i preko strim šifrarnika. Prva 64 bita enkriptovani su preko blok šifre, dok su ostali biti enkriptovani preko strim šifre. Međutim, u *CBC* modu, blok šifra primijenjena je na kompletan *data* paket, od početka do njegovog kraja, čime je kompletan podatak enkriptovan.
Ukoliko bi se pokušao *brute force* napad na algoritam došlo bi do određenih poteškoća. Iako *CSA* algoritam koristi 64 bitne ključeve, samo 48 bitova ključa je nepoznato, jer se ostatak koristi za bitove parnosti u okviru *CSA* sistema. Ovo otvara mogućnost takozvanih *Knoun plain text napada.* Ukoliko bi prva tri bajta *PES* zaglavlja bila poznata, moguće bi bilo odraditi *brute force* napad. Takav napad mogao bi otkriti i do milion mogućih ključeva, a i u takvim situacijama bi samo mali dio ključeva možda bio pogodan za dekripciju drugih djelova padataka. Iako je zaštita od 48 bita u današnjem vremenu već prevaziđena ona i dalje predstavlja kvalitetnu zaštitu podataka. Ukoliko bi htjeli da otkrijemo ključ, morali bi imati softver koji bi svaki ključ detektovao prije njegove promjene. Kako se ključevi mijenjaju u različitim periodičnim vremenskim intervalima i ukoliko bi izvršili testiranje milion ključeva u sekundi bilo bi potrebno približno 8 godina da se skeniraju kompletni ključevi, čime *brute force* napad čini veoma nepraktičnim za obavljanje poslova veznih za probijanje zaštite. I u varijantama gdje bi hardver

mogao testirati sve varijante ključeva u vremenskom intervalu od dva minuta, bitovi parnosti mogli bi se zamijeniti pravim bitovima rezervisanim za ključeve, čime bi se enkripcija povećala sa postojećih 48 na punih 64 bita, što bi dovelo do 65536 puta većeg rečnika za ključeve.

4.7.2. Known plaintext napad

Jedna od varijanti napada na *CS* sistem objavljen je 2012. godine od strane njemačkih istraživača. Napad se sastoji u činjenici da MPEG-2 *padding* često zahtijeva veliki broj nula, čime se dolazi do sekvence, odnosno ključa čiji će određeni bajtovi biti enkriptovani sa nulama. Na osnovu ovog podatka moguće je pronaći ispravan ključ, ali pod uslovima da sam signal sadrži sve nule u okviru svojih blokova. Još jedna od tehnika napada objavljena 2004. godine, nazvan *fault* napad zasnivala se na namjernom dodavanju grešaka nad samim bitima u okviru hardvera dekodera koji sadrži ključ.

4.7.3. Open resiver napad

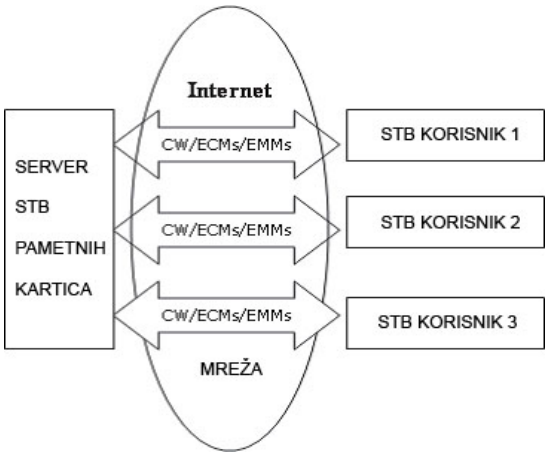
Korisnici digitalne televizije na raspolaganju imaju veliki broj različitih kanala, što je osnovna prednost u odnosu na analogni sistem prenosa. Međutim, svi kanali koji su dostupni krajnjem korisniku izabrani su od strane samog provajdera, a samim tim razlikuju se i po kvalitetu sadržaja. Uvijek se može desiti situacija da neki korisnik želi dio kanala koji nudi jedan provajder, ali i dio kanala koji nudi isključivo drugi provajder. Ovaj problem u okviru klasičnih *STB* uređaja nije rješiv. Tada korisniku preostaje mogućnost kupovine otvorenih resivera (*open receiver*). Otvoreni resiveri predstavljaju rekonfigurabilne satelitske resivere koji omogućavaju korišćenje različitih sadržaja od različitih provajdera u isto vrijeme. Da bi ovo sve funkcionisalo resiveri sadrže više *card smart* slotova. Problem sa ovakvom vrstom uređaja je vezan isključivo za njihovu sigurnost i zaštitu.
Hardverski posmatrano ovaj tip resivera se može više posmatrati kao računar sa ugrađenim *MPEG*-2 dekoderom. Operativni sistem ovakvih uređaja je uglavnom baziran na Linuxu ili nekom sličnom operativnom sistemu baziranom na jednostavnom grafičkom interfejsu, dok se podaci smještaju u *EEPROM* samog resivera. Najveće prednosti ovakvih uređaja predstavljaju i njihove najveće mane. Omogućavajući korisniku izbor provajdera stepen sigurnosti se znatno smanjuje i

samim tim ovakvi uređaji često predstavljaju metu napada sa ciljem omogućavanja otvaranja nedostupnih kanala.
Prednosti uređaja su više nego očigledne, i ogledaju se u samoj dostupnosti kanala i njihovom izboru. Pored toga u zavisnosti od tipa uređaja, ovakav tip resivera često omogućava nadogradnju različitih *firmware*-a, emulaciju pametnih kartica, omogućavanje dodataka (*plugin*), opciju umrežavanja, proširenje prostora putem USB periferija, omogućavanja ostalih periferija poput tastature i miša itd. Uređaji poput *DreamBoxa* predstavljaju najpopularnije *custom* varijante resivera, nudeći ogromnu funkcionalnost u odnosu na klasične resivere koje nudi sam provajder.

4.7.4. Card Sharing TV napadi

Svaki digitalni signal, prije ili kasnije, posmatrajući sferu digitalne televizije, postaje meta napada od strane onih koji mimo bilo kakve legalne procedure žele biti korisnici tog signala. Razvoj interneta doveo je i do okupljanja manjih zajednica (foruma) sa ciljem istraživanja određenih oblasti. Forumi su postali mjesto okupljanja raznih entuzijasta čiji je cilj istraživanje nedostataka *STB* uređaja kao i eksploatisanje njihovih mana. Najčešća vrsta napada zasniva se na *card- less* napadima, napadima bez kartice. CA sistem uglavnom se sastoji od *CAM* (*eng. Conditional Access Module*) i pametne kartice, mada *CA* može sadržati i samo jednu od ove dvije komponente. Da bi korisnici enkriptovali *DVB* signal potrebno je da njihov resiver sadrži oba ova elementa radi pravilnog dekodiranja. Dio vezan za pametne kartice može se softverski emulirati tako da oponaša pametnu karticu. Ovo je jedan od načina koji su uspješno bili implementirani dovodeći do kraha raznih *CA* sistema ali samim tim i njihovim jačanjem implementirajući kompleksne metode zaštite, sa ciljem zaustavljenja ovakvog tipa napada.
Da bi se efikasno izvršio napad na *DVB* odnosno *STB* uređaj potrebna je ogromna količina znanja o samom funkcionisanju sistema, pri čemu se informacije djelimično mogu pronaći na raznim forumima koji se bave ovom tematikom. Uglavnom, svi napadi obavljaju se preko otvorenih resivera, razlog za korišćenjem ovog tipa resivera je u činjenici da resiveri ne komuniciraju sa provajderom u koliko se nad njima vrši napad. Omogućavajući korisnicima da bezbjedno testiraju varijante napada bez straha da će provajder otkriti da je u toku pokušaj ilegalne radnje. Otvoreni resiveri su na ovaj način stekli ogromnu popularnost, omogućivši i manje naprednim korisnicima rekonfiguraciju resivera za testiranje *card-less* napada. Dream Box predstavlja jedan od najpopularnijih resivera za te svrhe, a

napad se vrši na način da se *custom* varijanta slike resiverskog hosta ubaci umjesto trenutno postojeće slike. Konfiguracije resivera je sada promijenjena i konfigurisanja da radi za određeni satelit, čime *DVB* programi postaju dostupni.
Napad koji podrazumijeva manipulaciju nad pametnim karticama predstavlja *Card Sharing* metodu napada (slika 53). Ova metoda dijeljenja kartice ne podrazumijeva rekonfiguraciju otvorenih resivera, već se zasniva na mogućnosti da jedan korisnik sa pravom karticom može omogućiti ostalim korisnicima pristup kodiranim kanalima.



Slika 53 - Kard šering napad

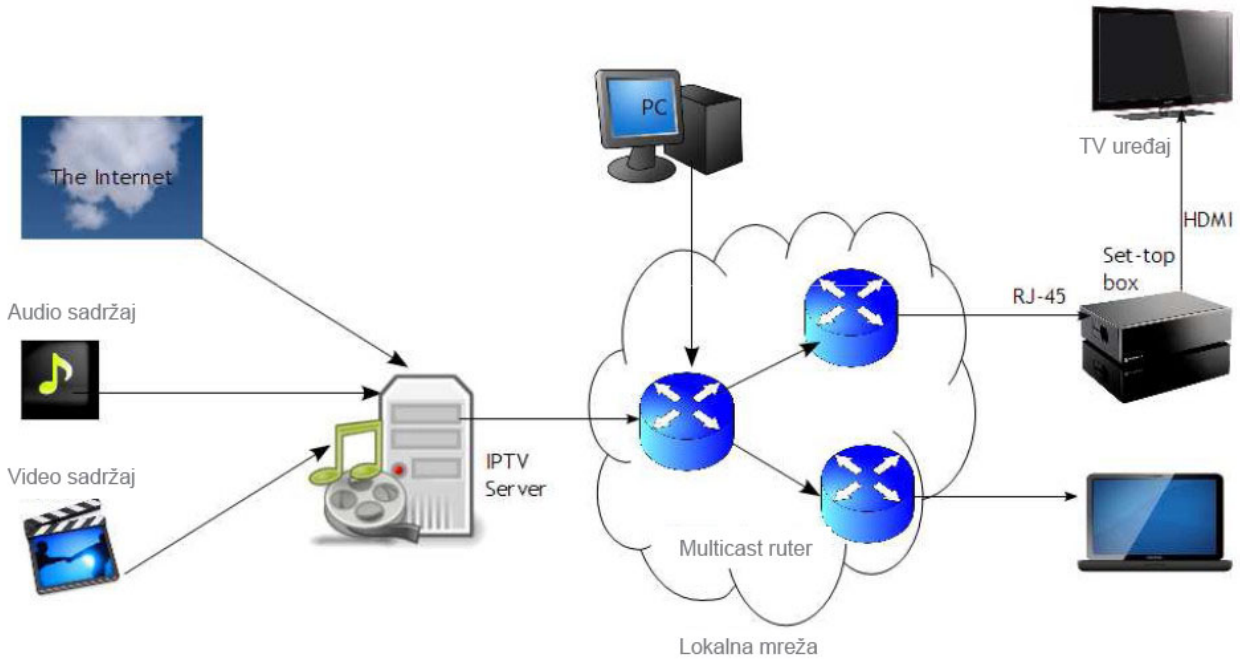
Princip rada dijeljenje kartica zasniva se na metodi da korisnik sa validnom karticom pravi server za kartice na rekonfigurisanom otvorenom resiveru i prisluškuje klijentsku komunikaciju na određenim portovima. U procesu slanja podataka od klijenta do servera, nalaze se *EMM* i *ECM* poruke koje se dekritptuju, čime vraćaju kontrolne riječi koje se koriste za skremblovanje sadržaja. Server za napade obavlja autentifikaciju klijenta koristeći regularnu karticu i nastavlja da razmjenjuje *ECM* i *EMM* poruke, omogućavajući klijentima pristup enkodovanom *DVB* programu bez pretplate. Server može podržati onoliko klijenata koliko sama kartica dozvoljava, a kako su kartice ograničene svojim resursima postoji različiti konačni broj mogućih korisnika koje je moguće priključiti i on zavisi od samog tipa kartice.

4.8. IP televizija

U sistemima digitalne televizije internet se može iskoristiti kao tehnološka inovacija sa ciljem pružanja što kvalitetnijeg digitalnog signala, omogućavajući protoke velikih brzina. IP (*eng. Internet Protocol*) televizija predstavlja telekomunikacionu infrastrukturu čiji je cilj pružanje najboljih mogućih servisa u okviru digitalne televizije uz što veću interaktivnost između korisnika i televizije. IPTV je u stanju da primi i prikazuje video strimove koji su enkodovani kao IP paketi, čime simultano omogućava prenos audio, video i data paketa.

Mreža kroz koju se prenose podaci može se razdvojiti u dvije funkcionalne cjeline, jezgro mreže *(core)* i pristupna mreža *(access network)*. Jezgro mreže predstavlja set uređaja namijenjenih organizaciji IP protokola i implementiranju različitih transportnih tehnika.

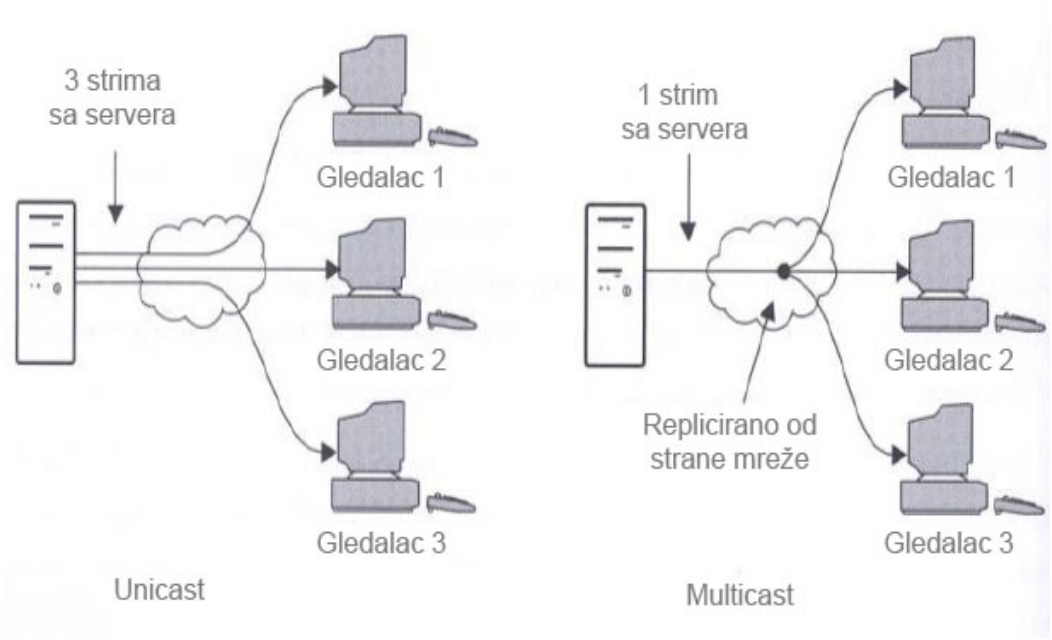
Cilj IP televizije u realnim sistemima je omogućavanje prenosa digitalnog signala, servisa poput VOD (*eng. Video on Demand*), VOIP (*eng. Voice over IP*), kao i web servisa koji postaju dostupni samom korisniku. U literaturi ova tri servisa zovu se *triple play* servisi. Sama IP televizija ne predstavlja standard emitovanja signala, što dovodi do činjenice da provajderi IP televizije mogu implementirati svoju IPTV mrežu i distribuirati signal u skladu sa zahtjevom tržišta. U odnosu na kablovsku televiziju IP televizija ima omogućene iste servise uz mogućnost implementiranja i korišćenja *triple play* servisa. Korisnici IPTV-a u svakom trenutku mogu pauzirati živi prenos programa i odložiti njegovo gledanje za kasnije. U suštini, bilo koji program može da se snimi i kasnije reprodukuje u okviru IPTV sistema. Problem ovakvog vida prenosa digitalne televizije leži u samom *bandwidth-u*. Naime, sam kvalitet internet konekcije određuje kvalitet prenosa audio i video signala. Ovaj princip donosi sigurnost u pogledu prenosa signala, jer signal biva prenešen dok konekcija postoji, ali degradacija kvaliteta signala može uticati na kvalitet usluge i zadovoljstvo korisnika. Sa obzirom da je internet glavni medij u prenosu signala vremenski uslovi ne utiču na IPTV. Na slici 54 prikazana šema osnovne arhitekture IP televizije.



Slika 54 – Osnovna arhitektura IPTV-a ili IPTV sistem

IP protokol omogućava mehanizam prenosa paketa između uređaja povezanih na internet. Pod pojmom paket podrazumijeva se skup informacija u predefinisanom formatu namijenjenom za prenos preko IP mreže. Video i audio signali se u okviru IP televizije dijele na više paketa i kao takvi se proslijeđuju IP mreži.
Postoje tri različita procesa prenosa paketa: unicast, multicast, broadcast (slika 55).
Unicast predstavlja tip transmisije gdje jedan pošiljalac i jedan primalac međusobno komuniciraju u okviru mreže, čime se paket informacija šalje isključivo između ova dva čvora (krajnje tačke prenosa i primanja podataka u okviru mreže).

U okviru multicast prenosa informacija sa jednog izvora šalje se grupi primalaca, čime se paketi podataka šalju sa jednog uređaja na više drugih uređaja istovremeno. Ukoliko bi grupisali više multicast grupacija dobili bi IP broadcast, čime bi se istovremeno slalo više različitih paketa kroz multicast grupe, omogućivši istovremeni prenos različitih tipova podataka kroz IPTV mrežu. Naravno, prenos multicast podataka najefektivniji je kada se istovjetni paketi šalju na više korisnika istovremeno. Ovo donosi određene probleme prilikom implementacije multicast prenosa, u vidu dodavanja ili brisanja korisnika iz multicast grupa u zavisnosti od tipa sadržaja koji se šalje.



Slika 55 – Unicast i Multicast prenos paketa

Kada analogni video signal dođe na ulaz MPEG enkodera njegov izlaz sastojaće se iz različitih audio i video *data* strimova koji se nazivaju elementarni strimovi. Svaki od ovih strimova dijeli se na manje pakete koji se nazivaju PES paketima (*eng. Packetized Elementary Stream*), koji mogu biti fiksne ili varijabilne dužine, pri čemu svaki PES sadrži zaglavlje radi indetifikacije i sinhronizacije.

Kao i kod kablovskih digitalnih sistema kvalitet slike zavisi od metoda kompresije koja se obavlja nad audio i video signalom. Kompresija videa omogućava smanjenje potrebnog *bandwidth* za slanje podataka i samim tim utiče na kvalitet sadržaja koji korisnik dobija. U zavisnosti od tipa kompresije kroz isti *bandwidth* moguće je prenijeti više različitih video kanala čime se smanjuju finansijski troškovi samog provajdera. Za razliku od nekompresovanih strimova internet konekcija ne mora biti previše brza jer se podaci kodiraju, samim tim i kompresuju.

Najveći dio protoka u IPTV sistemima odlazi na prenos multimedijalnih aplikacija, odnosno aplikacija koje uključuju audio, video i grafiku. Jedna od povoljnosti ovakvih sistema je i mogućnost korišćenja video konferencija pri čemu se prenos podataka obavlja u realnom vremenu i sa oba kraja. Da bi sve ovo funkcionisalo u realnim situacijama potrebno je imati i video servere čiji je zadatak čuvanje digitalnih video fajlova na svojim hard diskovima. Iako je ovo jedna od bitnijih

funkcija video servera, njihov primarni zadatak je dostavljanje i prenos kompletnog multimedijalnog sadržaja preko mreže. Video serveri najćešće se prave tako da čuvaju kopije podataka na svojim rezervnim hard diskovima, pri čemu se kopije i *mirroring* fajlova obavlja putem RAID tehnologije.

Kao i kod kablovskih sistema namijenjenim za prenos digitalne televizije, sistemi IP televizije sastoje se i od dodatnih servera namijenjenih raznim zadacima poput čuvanja fajlova, montaže, arhive itd.

Ingest (indžest) serveri koriste se za prikupljanje podataka sa različitih medijuma, bilo da su u pitanju video kasete, hard diskovi, USB podaci, video signali itd. Tek nakon što se video fajl indžestuje, moguće ga je proslijediti kroz sistem radi dalje obrade. Fajl serveri koriste se radi čuvanja multimedijalnih sadržaja na određeni vremenski period, prije nego što se materijali proslijede radnim stanicama. Serveri namijenjeni produkciji koriste se za pregled finalnih obrada indzestovanih materijala i kao takvi šalju se provajderima radi daljeg emitovanja ka korisnicima. Sadržaj koji je od bitnog značaja uglavnom se arhivira kroz servere namijenjene za arhivu. Takvi serveri uglavnom raspolažu velikim brojem medija za skladištenje. Često korisnici zahtijevaju da određeni multimedijalni sadržaji budu dostupni u što kraćem roku. Rješenje takvih zahtjeva ogleda se u implementiranju posebne vrste VOD servera (*eng. Video on Demand*). VOD serveri su pored servera za arhivu, najskuplji djelovi opreme koje bi provajder IPTV usluga trebao da posjeduje, prije svega zbog količine prostora kao i zbog činjenice da VOD servisi zahtijevaju veliki protok za nesmetano funkcionisanje. VOD serveri predstavljaju vrstu servisa za strimovanje podataka, a njihova namjena je ograničena samo za zahtjeve korisnika, ali ne i za *live* striming. Za svrhu *live* striminga koristi se poseban tip servera sa ciljem generisanja višestrukih kopija strimova preko jedne konekcije. Za razliku od VOD servera, njima nije potreban prostor za skladištenje, ali im je potrebna ogromna količina kapaciteta za generisanje velikog broja IP paketa.

4.8.1. IPTV protokoli

IPTV tehnologija zasniva se na određenim protokolima. RTP (*eng. Real-time Transport Protocol*) omogućava format paketa namijenjenog za slanje audio i video sadržaja. Ovaj protokol koristi se za striming kanala i kontroliše se putem RTSP protokola (*eng. Real-time Striming Protocol*). RTP i RTSP protokoli zajedno

čine jednu cjelinu namijenjenu za omogućavanje servisa poput video konferencija i pomenutog strimovanja audio i video sadržaja. U tim slučajevima RTSP protokol se oslanja na statistiku prenosa i kvalitet servisa QoS (*eng. Quality of service*) pri čemu pomaže procesima sinhronizacije tokom višestrukih strimova. RTSP protokol koristi se za kontrolu servera namijenjenog za strimovanje, odnosno kontrolisanje prenosa podataka kao i za kontrolisanje *unicast* i *multicast* strimova, pri čemu se striming obavlja isključivo u jednom pravcu od servera do korisnika. RTSP je protokol nivoa aplikacije koji kontroliše tok VOD strimova. Sadrži funkcije za početak, zaustavljanje, premotavanje i pauziranje multimedijalnog sadržaja koji se prenosi preko RTP protokola. RTSP omogućava sesije, ne konekcije, tako da prenos podataka ne mora da bude kontinualan da bi se održala veza između pošiljaoca i primalaca. Komunikacija se obavlja uz pomoć *setup* poruka koje omogućavaju početak i kontrolu sesije.

U IPTV tehnologiji PIM (*eng. Protocol-Independent Multicast*) protokol predstavlja set protokola namijenjen multicast rutiranju, koji omogućavaju distribuciju podataka preko IP mreža [10].

RTP protokol predstavlja protokol nivoa sesije, definisan tako da omogućava transportne funkcije preko mreža, poput dostavljanja data audio i video paketa u realnom vremenu. Njegova najznačajnija funkcija je mogućnost prenosa informacije bez obzira na vremenski život paketa, čime se omogućava da se STB uređaj precizno sinhronizuje sa izvornim signalom. TP uključuje seriju brojeva u svojim paketima pomoću kojih risiver određuje koliko je i koji paketi su izgubljeni tokom prenosa. Ovaj protokol koristi se i za transport do 7 MPEG2 TS paketa i vezan je za UDP transportni protokol.

Mana RTP protokola je nemogućnost izvještaja statusa o konekciji tako da se uglavnom oslanja na RTCP. RTCP *(eng. Real-time Transport Control Protocol)* protokol omogućava kontrolu informacija vezanih za RTP paketni strim u okviru određene sesije. Sa ovim protokolom primalac i pošiljilac u toku jedne sesije razmjenjuju poruke paralelno sa prenosom multimedije. Glavna funkcija RTCP protokola je omogućavanje povratnih informacija bez obzira na kvalitet veze između početne i krajnje tačke neke mreže.
IGMP *(eng. Internet Group Management Protocol*) koristi se za određivanje članstva u okviru multicast grupa i najviše je iskorišćen u okviru video striminga. U

okviru IPTV ovaj protokol se koristi za konekciju ka TV kanalima i promjenu TV kanala.

U okviru prenosa multimedijalnih sadržaja na nivou transporta koristi se UDP protokol kao optimalnije rješenje u odnosu na TCP protokol. Problemi sa multimedijalnim sadržajem vezani su za UDP protokol i javljaju se u vidu gubljenja paketa, oštećenja paketa, što može dovesti do grešaka u audio i video komponenti ili do njenog kašnjenja *(delley)*.

4.8.2. Karakteristike IP televizije

Triple play sistem namijenjen je za prenos audio, video i data podataka preko jedne pretplate. U okviru *triple play* sistema najpopularnije aplikacije su vezane za internet pretraživanje, televiziju i telefoniju. Telefonija u ovom slučaju omogućava servise poput prosleđivanja poziva, informacije o dolazećim pozivima, konferencijske pozive i slične stavke koje nisu ili su djelimično dostupne u klasičnoj telefoniji. Telefonska veza obavlja se preko IP protokola i omogućena je za sve fizičke medijume popup optičkog kabla, kablovskog i satelitskog predajnika. U sistemima kablovske digitalne televizije prijemna strana imala je specijalnu vrstu uređaja namijenjenu prijemu poslatih signala. STB uređaj obavljao je sve funkcije vezane za dekodiranje i autorizaciju korisnika. IPTV sistemi na prijemnoj strani, takođe, moraju posjedovati STB uređaje čiji je zadatak, takođe, dekodiranje digitalnog TV signala [21].

QoS servis predstavlja kombinaciju mrežne tehnologije i mrežne tehnike. U slučajevima IPTV televizije QoS razdvaja audio i video komponentu i određuje audio i video kvalitet zasebno. Audio kvalitet predstavlja audio signal koji treba rekreirati na strani prijema tako da su njegove karakteristike što bliže predajnom audio signalu. Prenos signala obavlja se putem raznih medija i to može uticati na prijemni audio signal. Sama kompresija omogućava prenos što kvalitenijih audio signala ali kao takva nije imuna na greške. Loša transmisija audio signala najčešća je pojava gubitka paketa ili prijema oštećenih paketa. Gubici paketa se dešavaju kada predajna strana nije uspjela da prenese pakete u određenom vremenskom intervalu. U realnim situacijama ovo znači da je audio signal na prijemu bez tona. Oštećeni paketi predstavljaju modifikaciju poslatih paketa i najčešće su pojava uslijed loše telekomunikacione mreže. U slučajevima oštećenih paketa audio signala na prijemu neće zvučati kao i predajni audio signal.

Video kvalitet definiše se kao odnos video kvaliteta na prijemnoj strani i video signala na predajnoj strani. Kao i kod audio signala, takođe se mogu desiti gubici paketa i oštećeni paketi, koji će se na korisničkoj strani pojaviti u okviru šuma, zamrzavanja slike ili nestanka kompletne sekcije.

Mobilna IP televizija predstavlja tehnologiju koja koristi mobilne uređaje za prijem i prenos multimedijalnog sadržaja putem žičnih ili bežičnih IP mreža. Cilj ove tehnologije je da IP televiziju omogući u svakom trenutku i na svim lokacijama u koliko je to moguće. Tehnologija iza ovog servisa bazirana je na 3G i 4G mrežama i polako pronalazi put ka krajnjim korisnicima. U Crnoj Gori 3G mreža je dostupna već par godina, dok su 4G mreže i dalje u fazi testiranja i omogućene su samo na određenim lokacijama.

4.8.3. Mehanizmi zaštite IP televizije

Prenos IP podataka putem IP infrastrukture veoma je lak za implementiranje i veoma je pouzdan. Kablovska televizija probleme zaštite signala riješavala je kombinacijom softverskih i hardverskih rješenja pri čemu je softversko rješenje podrazumijevalo skremblovanje i enkodovanje signala, dok je hardverski sistem zaštite bio baziran na pametnim video karticama. IPTV svoje mehanizme zaštite ostvaruje kroz tri tipa tehnologija [11] [13]:

1. CPS (*eng. Content Protection System*) - sadržaj se šalje kroz mrežu u enkriptovanoj formi radi zabrane neovlašćenog pristupa.
2. CAS (*eng. Conditional Access System*) - omogućava pristup sadržaju samo autorizavanim korisnicima.
3. DRM (*eng. Digital Rights Management*) - omogućava način pristupa sadržaju od strane korisnika, pri čemu je pristup ograničen uslovima koje je odredio sam provajder.

CPS sistemi pružaju sigurnost korisnicima u vidu osiguravanja dostupnosti podataka. Cilj CPS-a je da se neautorizovanim korisnicima onemogući dekodiranje sadržaja, a samim tim i zabrani redistribucija strimova. Ova zaštita ostvaruje se putem enkripcije zaglavlja sadržaja nakon što je sadržaj bio enkodiran. Postoje različite implementacije i opcije zaštite, a jedna od popularnijih zaštita je korišćenje slučajnog simetričnog ključa. Ovaj ključ koristi se za cijeli sadržaj od

strane provajdera ali može se implementirati i samo na određenim kanalima. Radi sigurnije zaštite ovaj ključ trebao bi da se mijenja što češće i praksa je da se ključ mijenja minimum jednom dnevno. Ključ na prijemnoj strani autorizovani korisnik dobija od strane provajdera. Tek nakon prijema ključa korisniku je omogućena dekripcija signala. Dodatne sigurnosne mjere uključuju mijenjanje simetričnog ključa tokom prenosa čime se povećava kompleksnost zaštite i smanjuje šansa pronalaska odnosno otkrivanja ključa. Procesi zaduženi za nadzor ključeva zaduženi su za provjeravanje stanja o slanju ključeva.

CA sistemi koriste se radi kontrole pristupa sadržaju i kao takvi predstavljaju jedan od ključnih sistema funkcionisanja ne samo IPTV-a već i digitalne kablovske televizije.
Sami počeci CA sistema vezani su za frekvencijska pomjeranja da bi se kasnije ovi sistemi pretvorili u moćne sisteme zaštite, čiji je osnovni zadatak enkripcija sadržaja. U hijerarhiji IPTV sistema CA sistem zauzima veoma važnu poziciju, jer ukupan sadržaj koji se prenosi putem mreže mora biti zaštićen od strane provajdera. Kao i kod CPS sistema, nakon enkripcije podataka CA sistem je zadužen za određivanje i kontrolu ključeva koji se moraju dostaviti odgovarajućim korisnicima.

Iako je IPTV tehnologija novijeg datuma svi podaci se nalaze u digitalnoj formi i kao takvi daleko su podložniji napadima u odnosu na ostale tipove signala odnosno podataka. P2P (*eng. Peer to peer*) mreže omogućile su nagli razvoj mehanizama za razmjenu podataka što direktno može uticati na sadržaj koji provajder dostavlja korisnicima. Upravo iz takvih razloga provajderi se okreću što snažnijim sistemima zaštite podataka koji mogu iskontrolisati po želji, sa ciljem totalnog distanciranja od svih neželjenih distribucija. Problemi zaštite javili su se na samom početku razvijanja IP tehnologije, korisnicima je omogućeno snimanje i skladištenje fajlova radi ponovnog pregleda. Upravo je to skladištenje podataka, tj. njegova kasnija distribucija postala osnova razvoja što sigurnijih ulaganja u zaštitu takvih sistema. DRM kodiranje postalo je *de-facto* standard zaštite distribuiranog sadržaja. U slučajevima VOD (*eng. Video on Demand*) sadržaj se segmentira i enkriptuje pomoću simetričnog ključa. Sam ključ mijenja se nekoliko puta u određenim vremenskim intervalima, radi što sigurnije zaštite. Svaki STB uređaj sadrži svoj privatni ključ i na osnovu tog ključa VOD server šalje enkriptovani sadržaj i enkriptovane simetrične ključeve radi dalje dekripcije i omogućavanja pregleda VOD sadržaja. Situacija je slična i u *broadcast* mrežama,

gdje se sadržaj takođe enkriptuje uz pomoć simetričnih ključeva, pri čemu STB uređaj šalje zahtjev trenutnim ključevima i na osnovu njegovog privatnog ključa sam server određuje koji je sadržaj namijenjen kojem korisniku.
DRM zaštita podrazumijeva da DRM-om zaštićene informacije postaju nečitljive za bilo koga osim za onoga kome su namijenjene, odnosno da u slučajevima dijeljenja fajlova sa ostalim korisnicima, sami fajlovi postaju nečitljivi. Dekripcija bi se obavljala tek nakon prijema informacije na korisničkoj strani. Metode kodiranja poput H.264 ili MPEG-4 [3], Advanced Video Coding (MPEG-4 AVC) moraju biti podržane od strane DRM aplikacija, da imaju mogućnost implementiranja AES (*eng. Advanced Encryption Standard*) [12] standarda.
Kao i u kablovskim sistemima, veći stepeni zaštite otežavaju neželjeni pristup samim fajlovima, tako da se AES enkripcija obavlja sa 128 bitova, iako se ta granica pomjera ka enkripciji od 256 bitova. Još jedna otežavajuća okolnost kada je u pitanju probijanje DRM zaštite leži u činjenici da je DRM zaštitu moguće implementirati na način da se određene hardverske komponente vežu za prijemni signal, poput čipova koje bi bile unikatne za svakog korisnika. Za samu enkripciju sadržaja DRM server mora je obavljati u realnom vremenu, dok u slučajevima VOD zahtjeva DRM enkripcija može se obaviti nakon primanja kompletnog sadržaja, odnosno prije njegovog emitovanja. Svi ovi stepeni zaštite čine da se težište zaštite mijenja sa softverskog nivoa ka transportnom nivou. Jedan od problema DRM zaštite može predstavljati distribucija ključeva, jer najefikasniji metod distribucije bio bi slanje ključeva direktno za korisnika. Ovaj metod predstavlja najsigurnije rješenje, jer se tada ključ šalje isključivo na određenu adresu i bez odgovarajućeg hardvera nemoguće bi bilo probiti zaštitu. Iako je ovaj metod najsigurniji on može dovesti do raznih problema u realnim situacijama gdje se broj korisnika mjeri u desetinama hiljada.

Broadcast televizija takođe mora biti zaštićena od neovlašćenog pristupa pri čemu se zaštita obavlja po određenim fazama:

1. Enkripcija sadržaja preko ključeva - DRM sistem je odgovoran za enkripciju kompletnog sadržaja i kao takav treba da traži ključeve od servera namijenjenog za generisanje istih ključeva. Ovi ključevi biće dodijeljeni STB uređaju, čime će im se omogućiti pregled odgovorajućeg sadržaja. Sam provajder određuje da li će isti ključ biti vezan za sve kanale ili će svaki kanal imati svoj sopstveni ključ.

2. Enripcija sadržaja slanja preko video striming servera.

3. DRM server pronalazi enkriptovani sadržaj - Nov enkriptovan sadržaj mora biti omogućen svim korisnicima preko posebnog elektronskog vodiča za program. Ovo znači da DRM server mora poslati tačno određeni sadržaj svim korisnicima koji žele da iskoriste mogućnost gledanja ili poručivanja novog sadržaja.

Pametne kartice *(Smart Card)* [8] predstavljaju element zaštite koji se najčešće implementira u kablovskoj digitalnoj televiziji, ali i pored toga svoju svrhu pronašle su u IP televiziji zbog kompatabilnosti sa DRM zaštitom. Današnje pametne kartice u sebi sadrže posebne čipove ali i manje procesore koji omogućavaju zaštitu samih ključeva. Preko pametnih kartica proizvođači STB uređaja mogu ponuditi dodatne stepene zaštite primjenog sadržaja. Čak i u slučajevima da napadi uspiju da uđu u sam operativni sistem STB-a pronalaženje ključeva za pametne kartice predstavlja vremenski zahtjevan zadatak. Tada se stepen zaštite, ukoliko bi sigurnost sistema bila ugrožena, može povećati jednostavnim prosljeđivanjem novih pametnih kartica.

Z A K LJ U Č A K:

DVB-T2 signal omogućio je brojne prednosti u odnosnu na postojeće, analogno stanje. Da bi sistem digitalizacije funkcionisao kako treba i pružio sve bitne funkcije koje digitalna televizija donosi, potrebno je ispoštovati određene standarde koje zahtijeva Evropska Unija, a sve u cilju što lakše globalne razmjene podataka i pružanja što kvalitetnije usluge građanima Crne Gore i Evrope. Kompletna tranzicija iz analognog u digitalni domen zahtijeva ulaganje u što kvalitetniju opremu, kao i osvrt na neke tehnologije koje bi mogle zaživjeti u ne tako dalekoj budućnosti, a koje mogu poremetiti planove vezane za proces digitalizacije. Jasno je da analogni sistemi više nemaju budućnost, bar kada je televizija u pitanju, a novi digitalni sitemi bazirani na *Internet-of-Things* doživjeće još veću ekspanziju u bliskoj budućnosti. Što se tiče emitovanja radio signala, oni će i dalje funkcionisati u analognom domenu iako će se sama oprema kretati ka trendu digitalizacije.

Digitalna televizija omogućavaće spregu između radija i televizije pružajući usluge prenosa radio kanala u okviru TV programa. Međutim, da bi sve ovo funkcionisalo kako treba i da bi se omogućile sve bitne funkcije koje digitalna televizija donosi potrebno je ispoštovati određene standarde i procedure zaštite signala, a sve u cilju što sigurnije razmjene podataka između provajdera i krajnjeg korisnika. Kontrolom i monitoringom CA sistema provajderi mogu omogućiti što kvalitetnije usluge digitalne televizije svojim korisnicima. Iako sistemi kontrole i monitoringa zahtijevaju određene resurse, prije svega finansijske, njihova implementacija, dugoročno gledano, može doprinjeti razvijanju kvalitetnijih provajderskih servisa koje mogu prevazići trenutno dostupne okvire digitalne televizije. Sam monitoring može se implementirati nad svim sistemima, ali kontrolisanje sistema uvijek predstavlja problem tehničke prirode. Otkrivanje sigurnosih problema u sistemima digitalnog prenosa predstavlja veliki izazov za administratora računarskih sistema, bilo da je u pitanju sam provajder ili omanji emiter digitalnog signala. Nijedna mreža, ma koliko god bila obezbijeđena, nije u potpunosti sigurna. Posmatrajući realnu situaciju u okviru sistema televizije Crne Gore, mjere zaštite odrađene su kroz softversku platformu. Iako softverska zaštita nije najidealnije rješenje, ona je u trenutnoj mjeri dovoljna da sistem funkcioniše nesmetano. Trenutni problemi koji se javljaju na poljima žaštite i sigurnosti mogu

se razriješiti prebacivanjem na IPTV tehnologiju, koja već u startu donosi sve poznate protokole i koja je hardverski jednostavnija u odnosu na digitalnu opremu namijenjenu kablovskim operaterima. Problem i dalje predstavljaju same finansije jer obezbijeđivanje kvalitetne veze između korisnika i provajdera zahtijeva dosta ulaganja u mrežnu infrastrukturu, ukoliko ona ne postoji ili nije adekvatnog tipa. Iz svega navedenog zaključuje se da digitalna televizija već predstavlja budućnost dostupnu širokom spektru građana, ali da će njen tok razvoja težiti ka implementiranju IP protokola kao glavnog medijuma za prenos informacija.

Analogijom između postojećeg aktivnog sistema TVCG i neimplementiranih digitalnih tehnologija koje se koriste u svijetu dat je uvid na neophodnost zaštite računarskih sistema kao i na pregled vrsta enkripcija digitalnog signala. Analizom trenutnog sistema dolazi se do zaključka da će digitalna televizija u bliskoj budućnosti biti jedan od glavnih medija za prenos informacija bazirajući se na tehnologijama koje pružaju adekvatnu sigurnost i zaštitu. Digitalni sistem Crne Gore tek očekuju brojna unaprijeđenja koja se neće bazirati na trenutno implementiranom hardveru i softveru, već će biti bazirane na novijim tehnologijama, sa ciljem pružanja što kvalitetnijeg sadržaja, bilo da je u pitanju tehnički ili informativni aspekt.

L I T E R A T U R A:

[1] Walter Fischer. (2008) - “Digital Video and Audio Broadcasting Technology”, Springer-Verlag, Berlin Heidelberg, ISBN 978-3-642-11612-4, strana 440-460 strana.

[2] Charles Poynton (2003) - “Digital Video and HDTV, Algorithms and Interfaces”, Morgan Kaufmann Publishers, San Francisco, ISBN 978-1558607927, strana 736.

[3] lberto Morello (2006) - “DVB-S2: The second generation standard for satellite broad-band services”, Proc. IEEE, vol. 94, SSN: 0018-9219, strana 210–227.

[4] Reimers Ulrich (1998) - “Digital Video Broadcasting”, IEEE Communication, Magazine, Tech. Univ. Braunschweig, Germany, ISBN 978-3-642-07807-1, strana 104-109.

[5] Aleksandar Sugaris (2009) - “DVB standards development”, Proc. Telsiks, vol. 1, ISBN 978-1-4244-4382-6, strana 263-272.

[6] Irini Reljin. (2008) - “DVB second generation of digital standards”, in Proc. POSTEL, strana 145-154.

[7] ETSI TS 102 367 (2005, januar). DAB Conditional access. Dostupno: http://www.etsi.org/deliver/etsi_ts/102300_102399/102367/01.01.01_60/ts_102367v010101p.pdf

[8] F. Miller, A.Vandome, J. McBrewster (2010) - “Downloadable Conditional Access System,” Alphascript Publishing, ISBN 6131781524, strana 10–78.

[9] T. Jiang (2004) - "Key distribution based on hierarchical access control for Conditional Access System in DTV broadcast", IEEE Trans. on Consumer Electronics, vol. 50, ISBN 0-7803-8549-7, strana 185-205.

[10] Lawrence Harte (2007) - "IPTV Basics Technology, Operation, and Services", Althos Publishing, Fuquay-Varina USA, ISBN 9781932813562, strana 299-355.

[11] David H. Ramirez (2008) - "IPTV Security: Protecting High-Value Digital Contents", Wiley & Sons, Chichester, England, ISBN 9780470519240, strana 180-211.

[12] Borko Furht, Darko Kirovski (2006) - "Multimedia Encryption and Authentication Techniques and Applications", Auerbach Publications, Boca Raton, New York, ISBN 9780849372124, strana 330-360.

[13] S. Lian, Z. Liu, Z. Ren, H. Wang (2006) - "Secure Advanced Video Coding Based on Selective Encryption Algorithms ", IEEE Transactions on Consumer Electronics, Vol. 52, ISSN 0098-3063, strana 521-581.

[14] Marković Dušan P. (2008) – "DVB-T : Terestrička Digitalna Televizija", Akademska Misao, Beograd, SR, ISBN 10: 8674663354.

[15] William Stallings, (2016) - "Cryptography and Network Security: Principles and Practice Autor William Stallings", Pearson Education, U.S.A, ISBN 9780134484525.

[16] Behrouz A. Forouzan (2008) – "Introduction to Cryptography and Network Security", McGraw-Hill, ISBN-13: 978-0073327532.

[17] Douglas R. Stinson (2006) – "Cryptography: Theory and Practice, Third Edition", Chapman & Hall/CRC, ISBN 9781584885085.

[18] Jian Song, Zhixing Yang, Jun Wang (2015) – "Digital Terrestrial Television Broadcasting: Technology and System", John Wiley & Sons, New Jersey, CA, ISBN: 978-1-118-13053-7.

[19] Roland Beutler (2011) – "The Digital Dividend of Terrestrial Broadcasting", Springer, Stuttgart, Germany, ISBN: 9781461415688.

[20] Marković Dušan P. (2014) – "Sistemi Digitalne Televizije i radija", Akademska Misao, Beograd, SR, ISBN: 978-86-7466-515-2.

[21] E. Tews, J. Walde, M. Weiner (2011) – “Breaking DVB-CSA,” in Proceedings of West European Workshop on Research in Cryptography, Weimar, Germany, ISBN: 0302-9743.

[22] H, Greenfield, W. Simpson (2009) – “IPTV and Internet Video: Expanding the Reach of Television Broadcasting”, 2nd Edition, Focal Press, Burlington, MA, ISBN: 024081245X.

[23] Gerard O'Driscoll (2008) – “Next Generation IPTV Services And Technologies”, A John Wiley & Sons, New Jersey, CA, ISBN: 978-0-470-16372-6.