

Mrežna infrastruktura u energetici – primjeri iz prakse

Davor Janković



SCADA

- SCADA = Supervisory Control And Data Aquisition
- Računalni sustav za nadzor i upravljanje industrijskim sustavima
- Svaki industrijski sustav ili proces kojeg ima smisla automatizirati je dobar kandidat za primjenu SCADA sustava
- Široko područje primjene od jednostavnih nadzora (temperatura, tlak) do kompleksnih nadzora i upravljanja (proizvodni procesi, transport energije, regulacija prometa)



Važnost SCADA sustava

- SCADA se koristi za nadzor i upravljanje sustava kritičnih za društvo
 - Prijenos i distribucija električne energije
 - Prijenos i distribucija energenata
 - Upravljanje prometom
 - Prijenos i distribucija vode
- Gubitak komunikacije u tim sustavima za posljedicu može imati velike fizičke štete, prekide u radu i financijske gubitke u kompanijama
- Zbog toga je pouzdanosti i sigurnost takvih sustava kritična

Elementi SCADA sustava

- SCADA se sastoji od hardvera, softvera i komunikacijskih komponenti
- Osnovni elementi SCADA sustava su
 - Kontrolni centar – centralna stanica
 - Pretvornici i RTU jedinice
 - Komunikacijska infrastruktura

SCADA komunikacijska infrastruktura

- SCADA je u prošlosti za komunikaciju koristila legacy protokole kao što su Modbus, Profibus i Conitel
- Legacy protokoli nisu bili zamišljeni za rad preko korporativnih mreža ili čak IP protokola (npr. Modbus)
- Novije vrijeme donosi standarde kao što su IEC 60870-5-104 ili IEC 61850 koji rade preko TCP/IP-a
- Posljedično, dosta sustava koristi korporativne mreže za povezivanje SCADA sustava



SCADA komunikacijska infrastruktura

- Često je SCADA sustav raširen na značajnom broju međusobno geografski udaljenih lokacija
- Mrežna infrastruktura u takvim sustavima dolazi do izražaja
- SCADA inženjeri nemaju tehnološku pozadinu iz IP svijeta
- Drugačiji pogled na mrežu od mrežnih inženjera
- Mrežni dizajn može imati dva pristupa
 - Jednostavna mrežna infrastruktura
 - Sigurna i pouzdana mrežna infrastruktura



Elementi kompletne mrežne infrastrukture

Pouzdanost
i
proširivost

Kvaliteta servisa

Sigurnost

Nadzor
i
upravljanje

Pouzdanost komunikacijske infrastrukture

- Mrežnu infrastrukturu moguće je brzo i jednostavno postaviti korištenjem Layer 2 dizajna
 - Jednostavna logička shema
 - Malo posla sa definiranjem IP adresne sheme i plana VLANova
 - Tehnologija omogućuje povezivanje i uređaji rade “iz kutije”
- Takav sustav ima lošu skalabilnost, sporu konvergenciju – ali uglavnom rade
- Kad se pojavi problem – vidljiv je na cijeloj Layer 2 domeni
- Layer 3 bazirana infrastruktura je proširiva, brže konvergira, stabilnija i lakše upravljiva
- Potencijalni problemi imaju lokalni utjecaj, lakše se otkrivaju i otklanjaju
- STP vs. Routing protokoli OSPF ili ISIS



Pouzdanost komunikacijske infrastrukture

- Vrijeme konvergencije je kritično
Kako bi skratili vrijeme konvergencije mreže potrebno je podesiti praktički sve protokole
- Inicijalni tajmeri protokola usmjeravanja se godinama nisu mijenjali
Npr. OSPF ima DEAD timer 40 sekundi na ethernet vezama
- Potrebno je voditi računa o međuovisnosti protokola
HSRP i OSPF
OSPF i LDP
- BFD protokol može značajno smanjiti vrijeme konvergencije
Drugačiji tretman BFD paketa unutar mrežnih uređaja

Pouzdanost komunikacijske infrastrukture

- Primjer – upravljanje trafostanicom
- IED – kontroler elektroenergetske opreme sa mikroprocesorom
- Protokol IEC 61850 – definira model komunikacije IEDova
- GOOSE poruke – jezik kojim IEDovi komuniciraju
- Cijela transmisija mora se obaviti u pola ili četvrtini ciklusa
 $\text{Ciklus} = 1\text{s} / 50\text{ Hz} = 20\text{ milisekundi}$
- Industrija očekuje konvergenciju mreže u 4 milisekunde



Kvaliteta servisa

- U legacy mrežama je svaki servis bio na različitoj infrastrukturi
- IP donosi koncept jedna infrastruktura – više servisa
- Potrebno je kritičnim servisima osigurati dostupnost kapaciteta mreže

U graničnim slučajevima se postiže odvajanjem posebne infrastrukture za specifičan servis

Generalno rješenje je korištenje multiservisne mreže sa ispravno definiranim QoS modelom



Kvaliteta servisa

- Dobar QoS model je podloga za ispravnu implementaciju QoS mehanizama

Application	L3 Classification		Referencing Standard
	PHB	DSCP	
IP routing	CS6	48	RFC 2474-4.2.2
Voice	EF	46	RFC 3246
Interactive – Video	AF41	34	RFC 2597
Streaming Video	CS4	32	RFC 2474-4.2.2
Mission-Critical	AF31	26	RFC 2597
Call-Signaling	CS3	24	RFC 2474-4.2.2
Transactional Dana	AF21	18	RFC 2597
Network Mgmt	CS2	16	RFC 2474-4.2.2
Bulk Dana	AF11	10	RFC 2597
Scavenger	CS1	8	Internet 2
Best Effort	0	0	RFC 2474-4.1

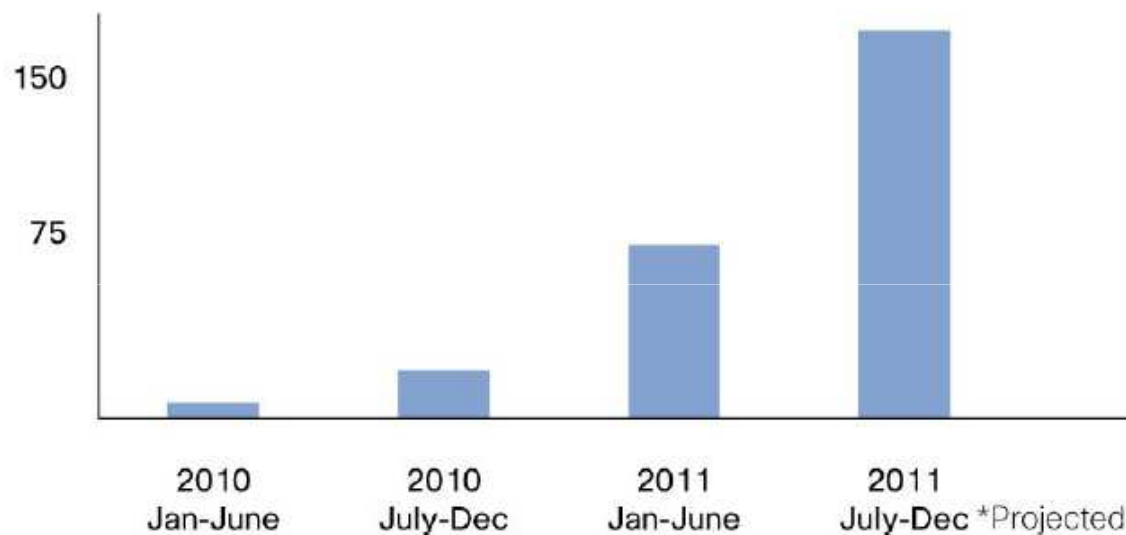
Sigurnost SCADA sustava

- Sigurnosni rizik uključuje dva elementa
 - Vjerojatnost da će se dogoditi sigurnosni propust
 - Utjecaj na sustav i servis
- Utjecaj može biti širok, osim gubitka servisa koji su često kritični za društvo, moguće su i katastrofalne posljedice
- Iako ima svoje specifičnosti, SCADA sustav sastoji se od poslužitelja i radnih koji imaju uobičajene operacijske sustave i podložni su sigurnosnim propustima kao i svi drugi sustavi



Sigurnost SCADA sustava

- Broj ranjivosti SCADA sustava raste gotovo eksponencijalno



- Umjesto dublje analize rizika i vjerojatnosti navest ćemo nekoliko primjera napada na SCADA sustave i njihove posljedice

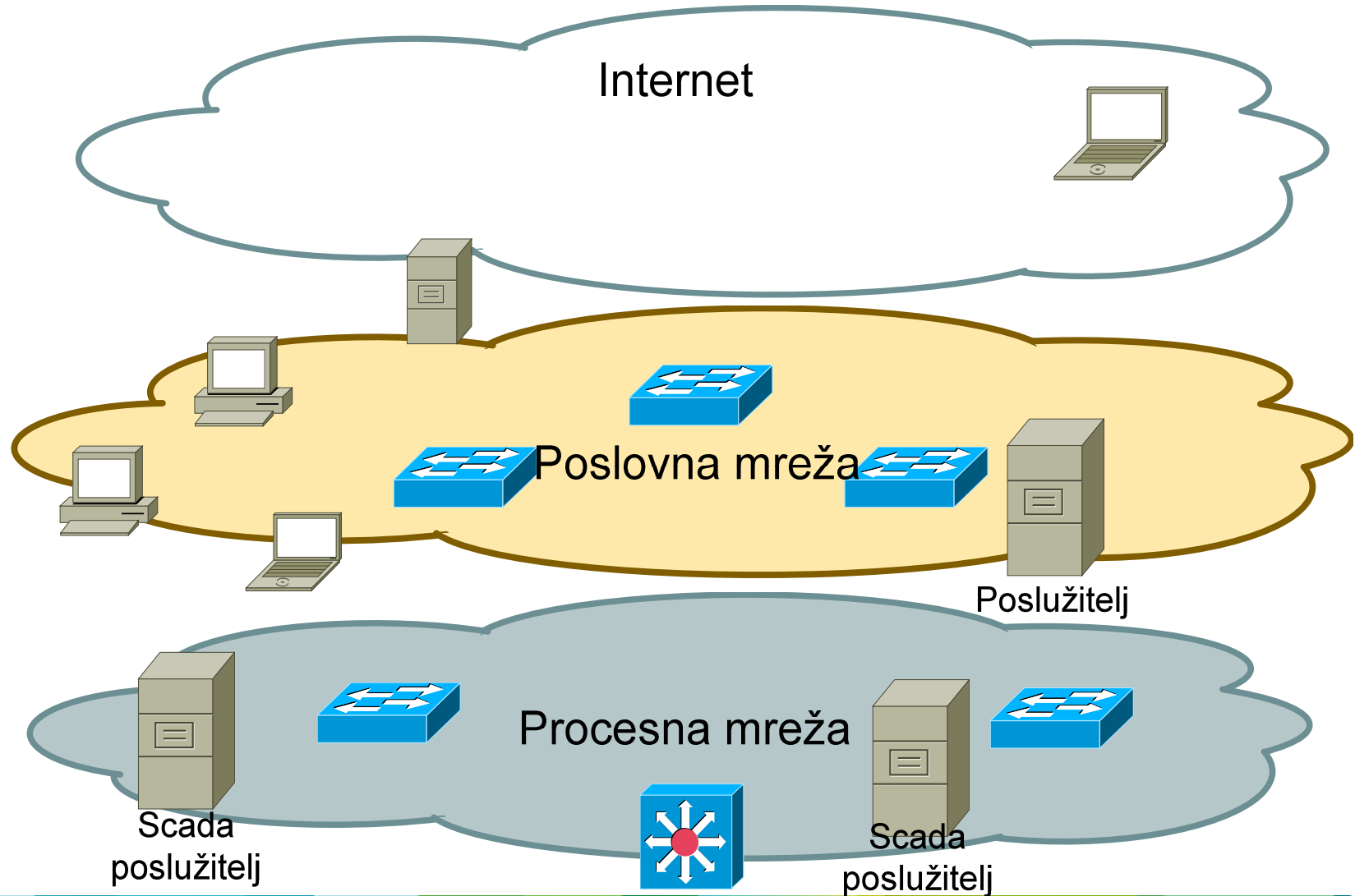
Sigurnost SCADA sustava

- Izljev kanalizacije u Maroochy Shire u Australiji
http://www.theregister.co.uk/2001/10/31/hacker_jailed_for_revenge_sewage/
- Još u 2002 godini pronađeni su dokazi da Al-Qaeda ima informacije o američkim SCADA sustavima i da posebnu pažnju posvećuju sustavima za vodoopskrbu
<http://news.bbc.co.uk/2/hi/science/nature/2070706.stm>
<http://www.pbs.org/wgbh/pages/frontline/shows/cyberwar/vulnerable/alqaeda.html>
- 2003 godine crv Slammer iz funkcije i nadzora je izbacio američku nuklearnu elektranu
http://www.theregister.co.uk/2003/08/20/slammer_worm_crashed_ohio_nuke/
Elektrana je bila zaštićena

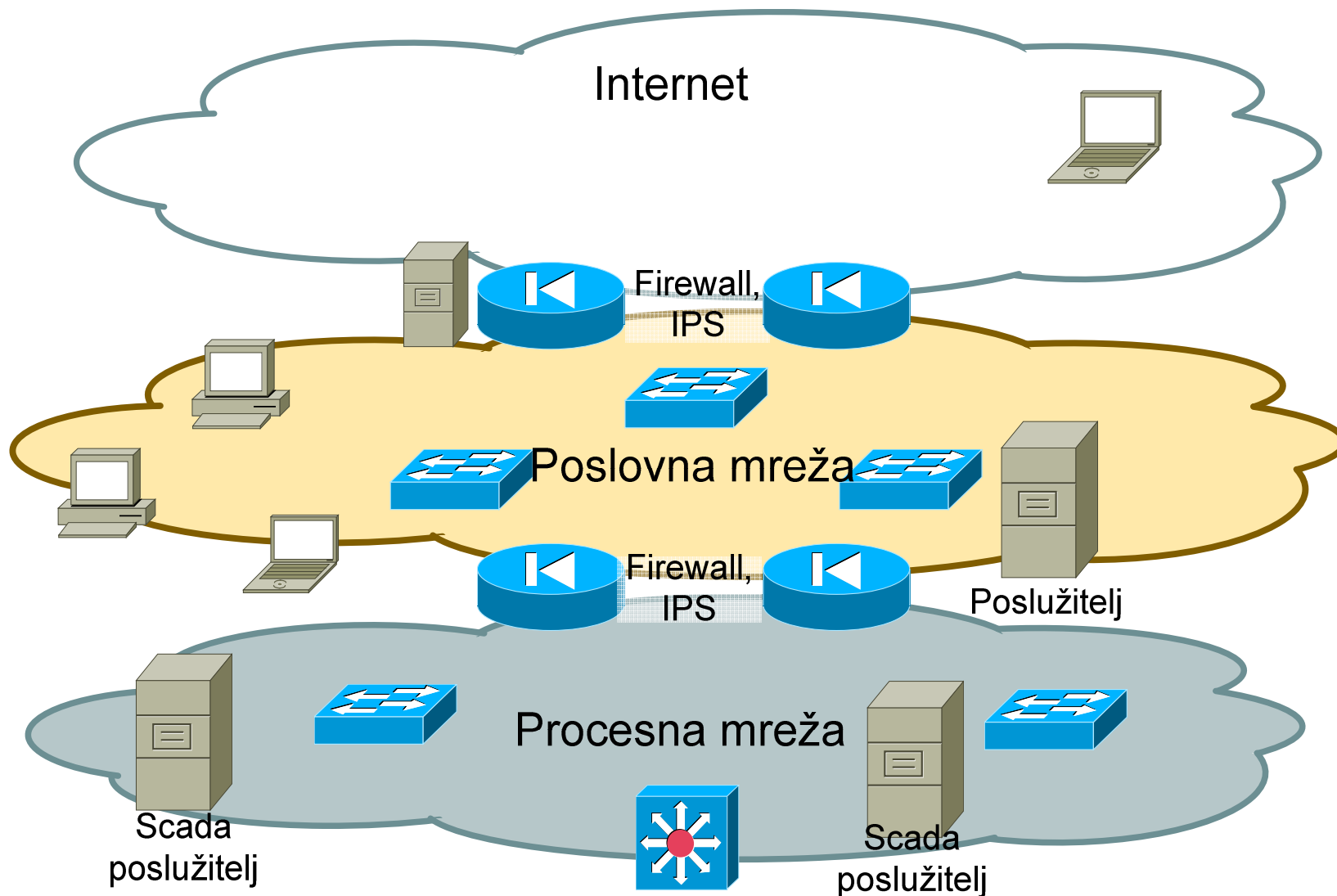
Sigurnost SCADA sustava

- Zagušena mreža ugasila Browns Ferry nuklearnu elektranu
<http://www.nrc.gov/reading-rm/doc-collections/gen-comm/info-notices/2007/in200715.pdf>
- Stuxnet virus zarazio iranska nuklearna postrojenja, ali i ostala širom svijeta (Indija, SAD, Pakistan, Indonezija...)
<http://en.wikipedia.org/wiki/Stuxnet>

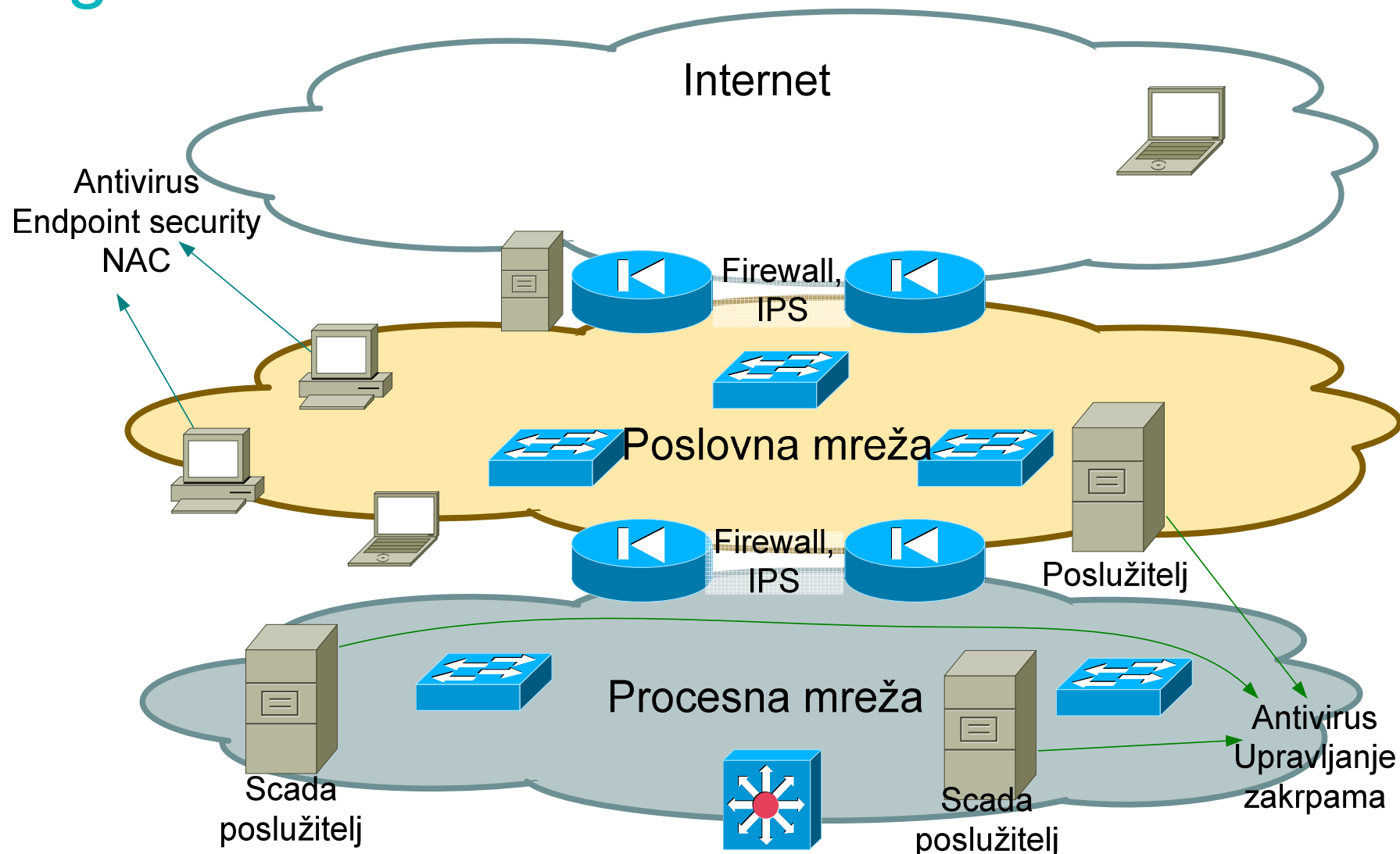
Sigurnost SCADA sustava – kako se zaštititi



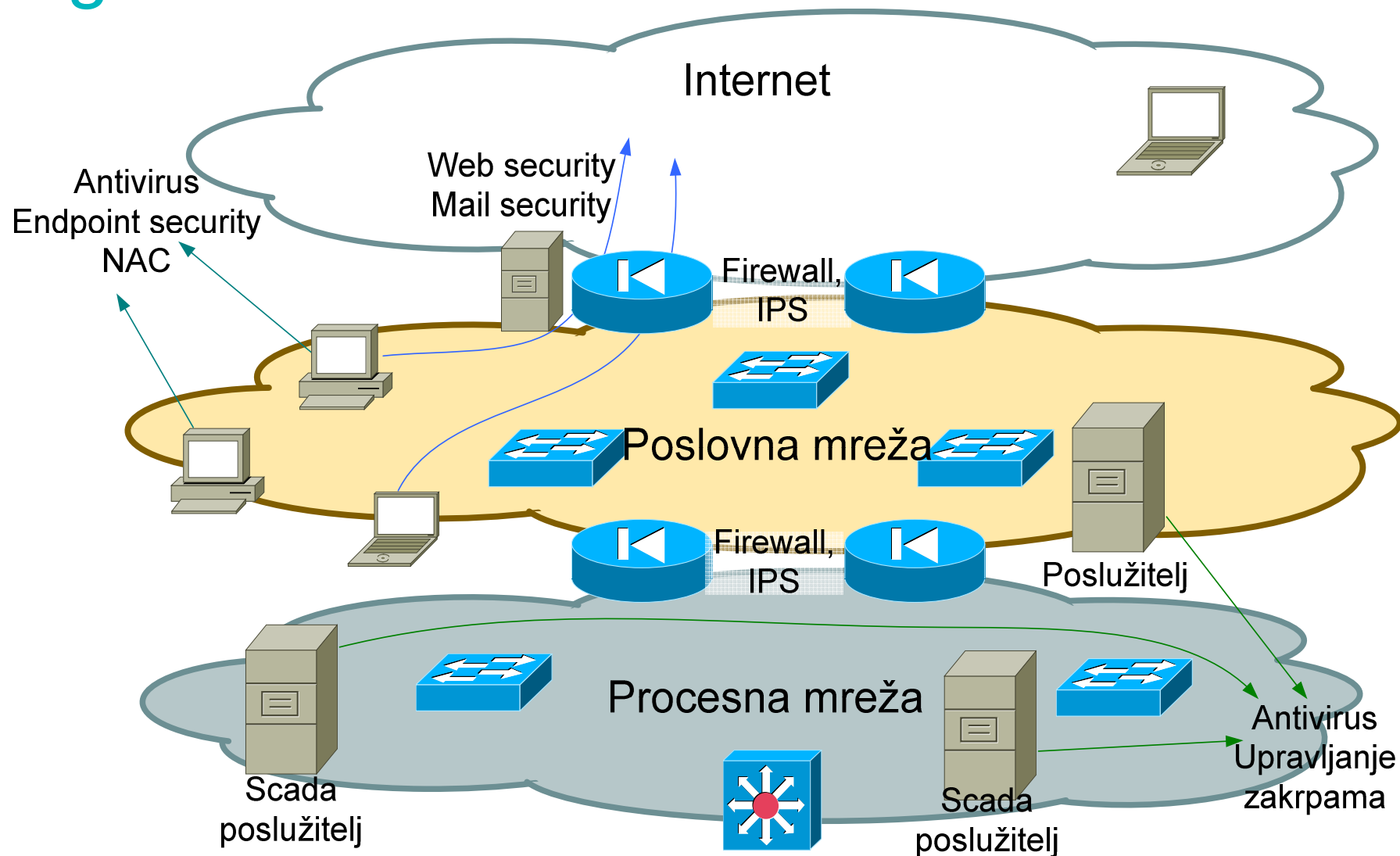
Sigurnost SCADA sustava – kako se zaštititi



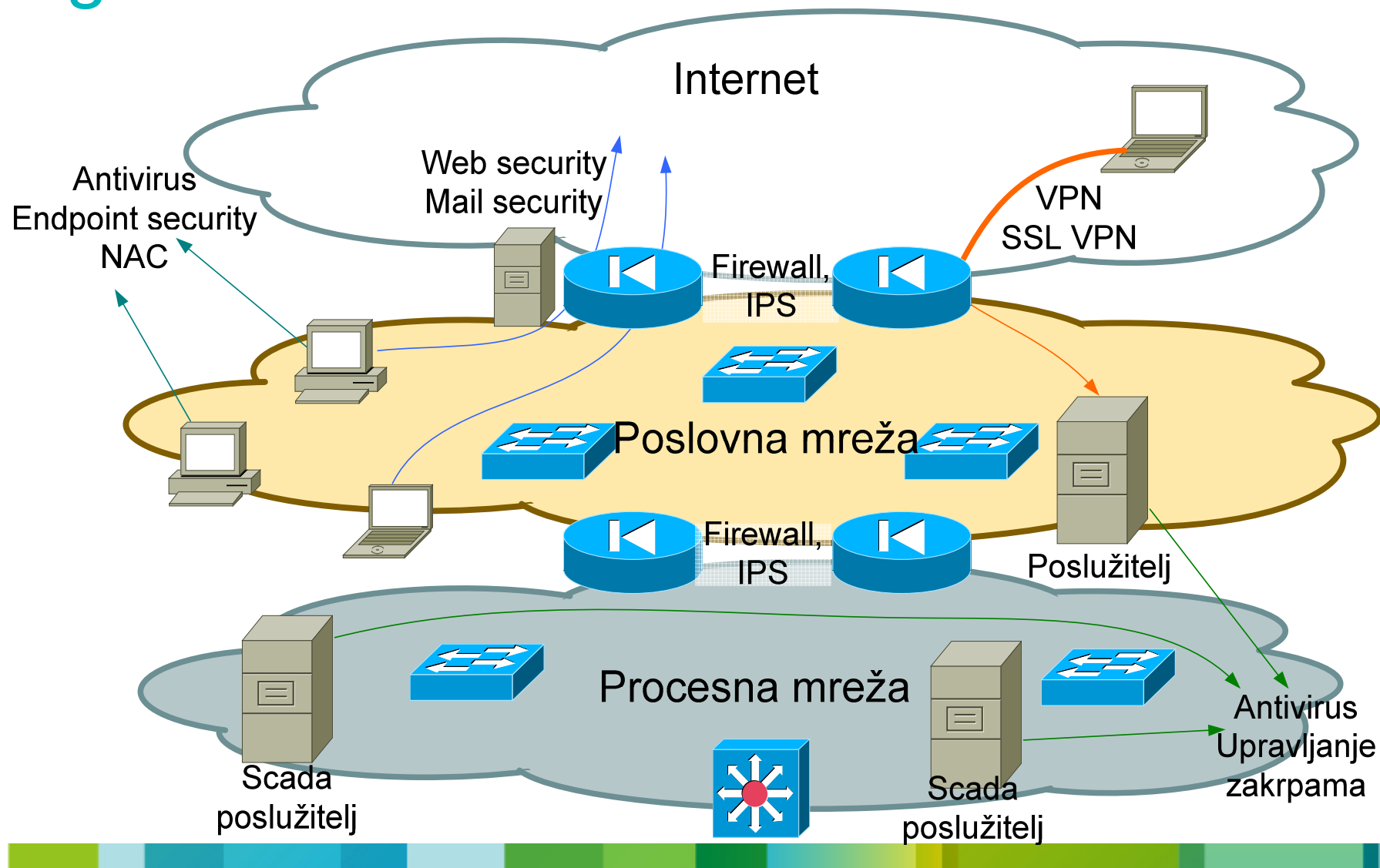
Sigurnost SCADA sustava – kako se zaštititi



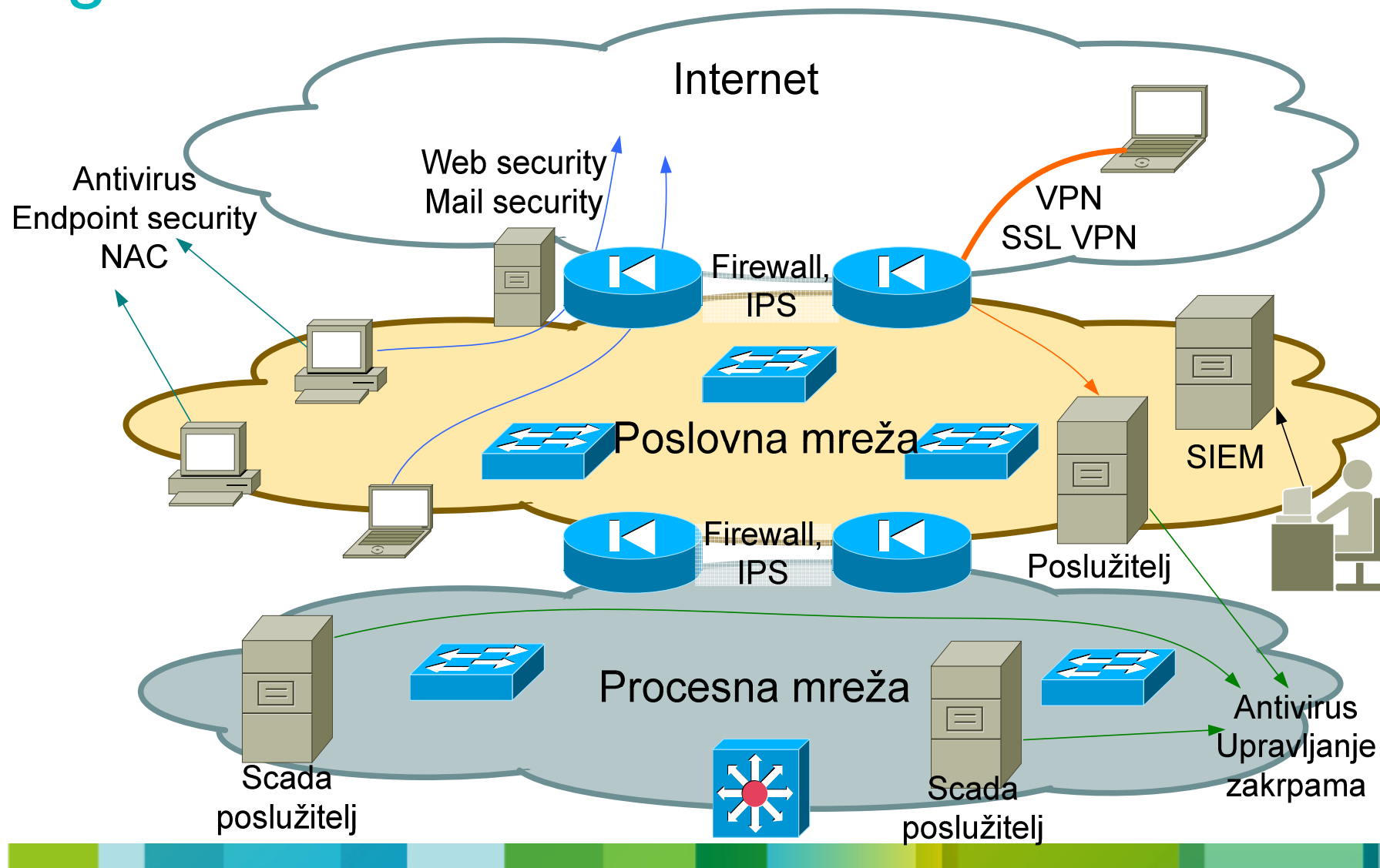
Sigurnost SCADA sustava – kako se zaštititi



Sigurnost SCADA sustava – kako se zaštititi



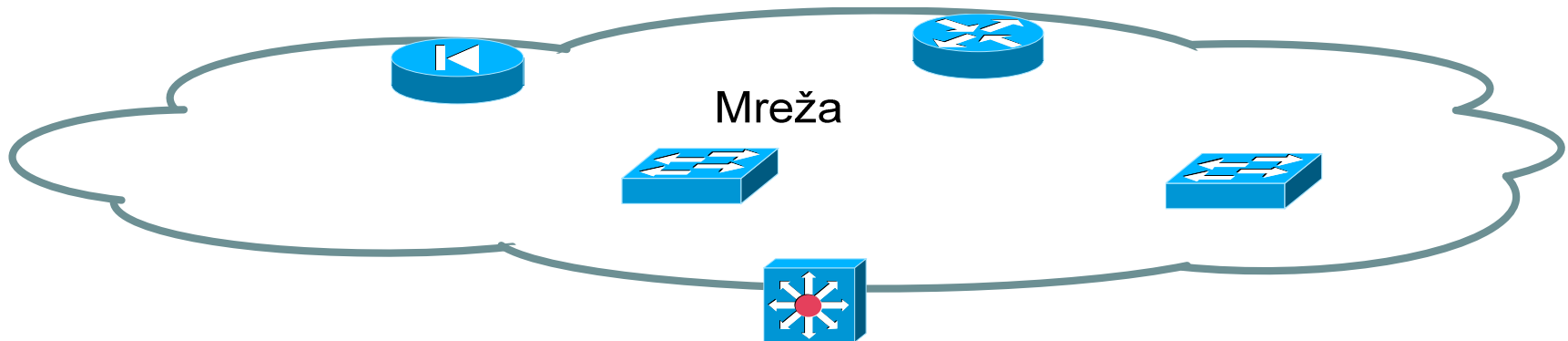
Sigurnost SCADA sustava – kako se zaštititi



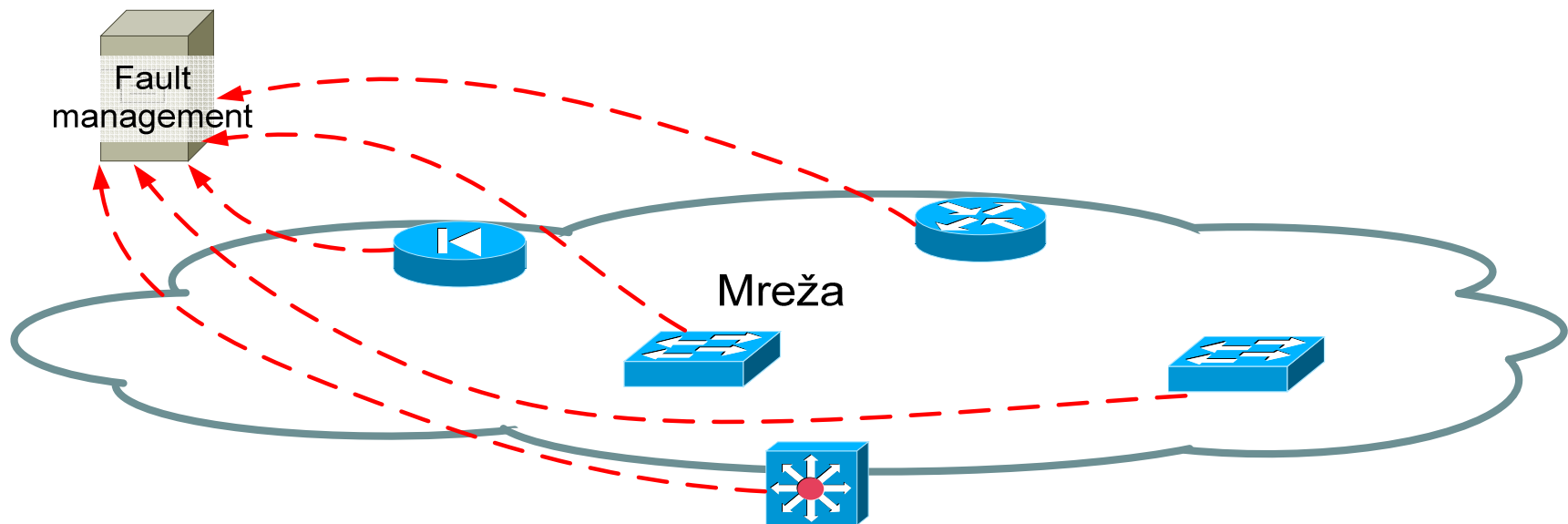
Sigurnost SCADA sustava – kako održati siguran sustav sigurnim

- Sveprisutnost mrežne infrastrukture u SCADA sustavima i primjeri katastrofa pokazuju koliko je sigurnost bitna
- Nije dovoljno jednom napraviti dizajn i postaviti mrežu – potrebna su kontinuirana unapređivanja i kontrole
- Zato treba sustav koji će unapređivati postavljenu infrastrukturu kroz različite procese
- ISMS – sustav u kojem pojedini procesi (Incident management, Risk mgmt itd., redovni godišnji audit i provjere, technical vulnerability checking itd.) kao zajednički cilj imaju sveobuhvatnu sigurnost informacijskog sustava i njegovih dijelova

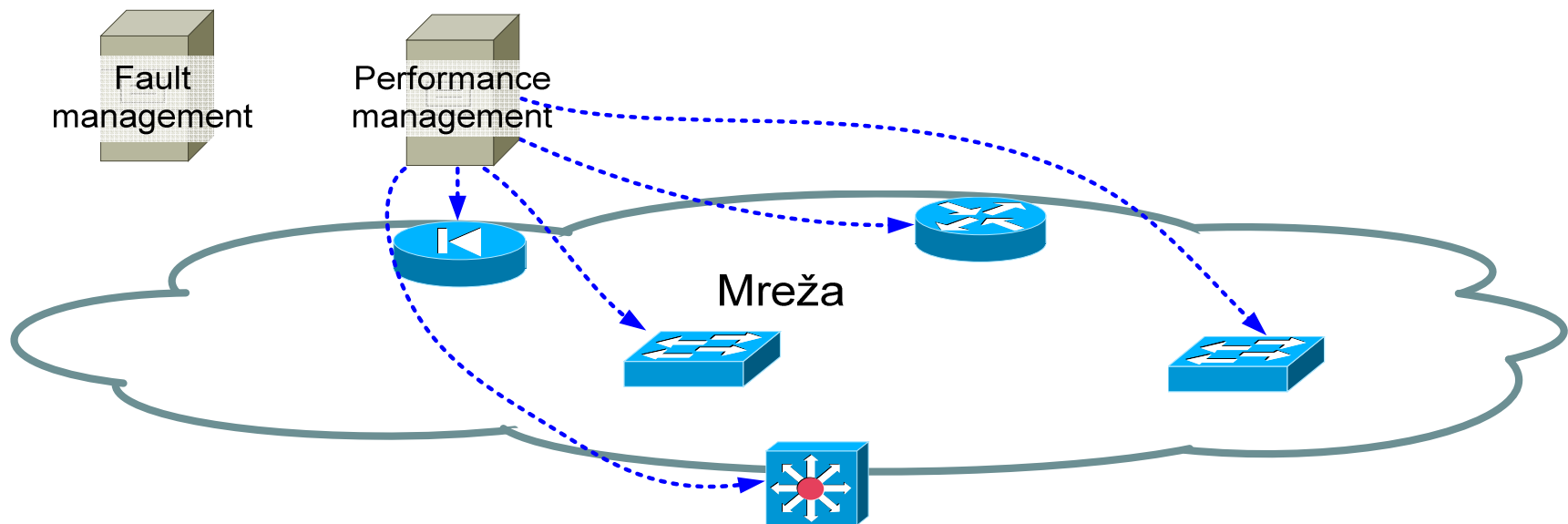
Nadzor i upravljanje mrežom



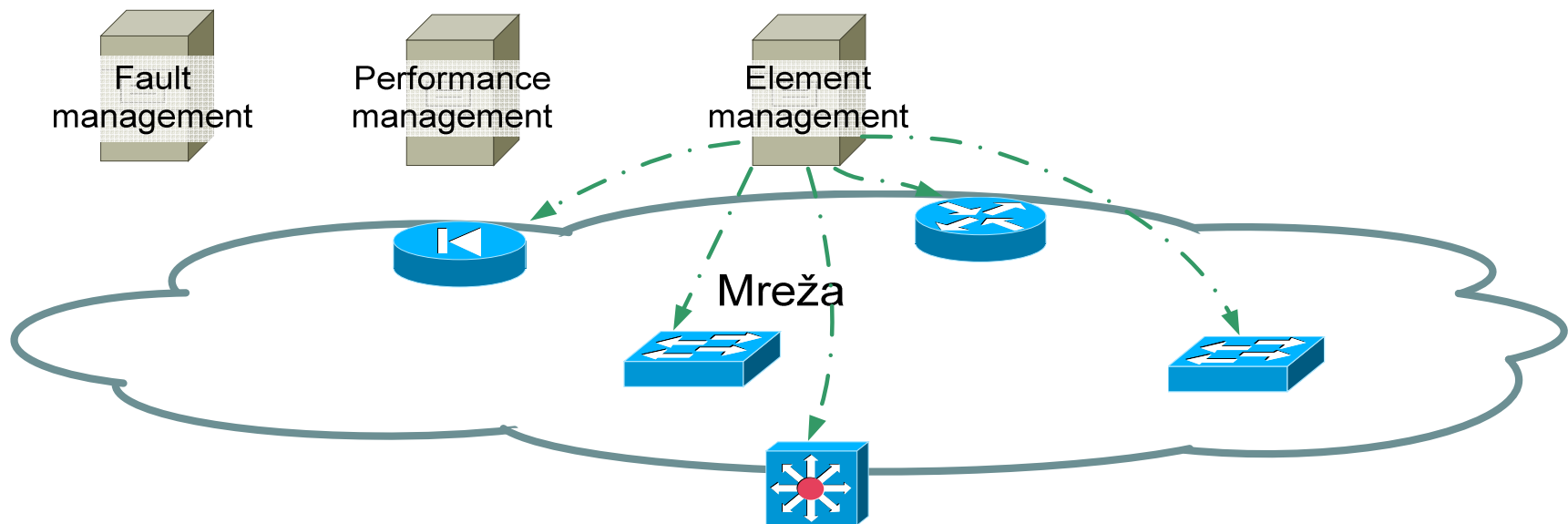
Nadzor i upravljanje mrežom



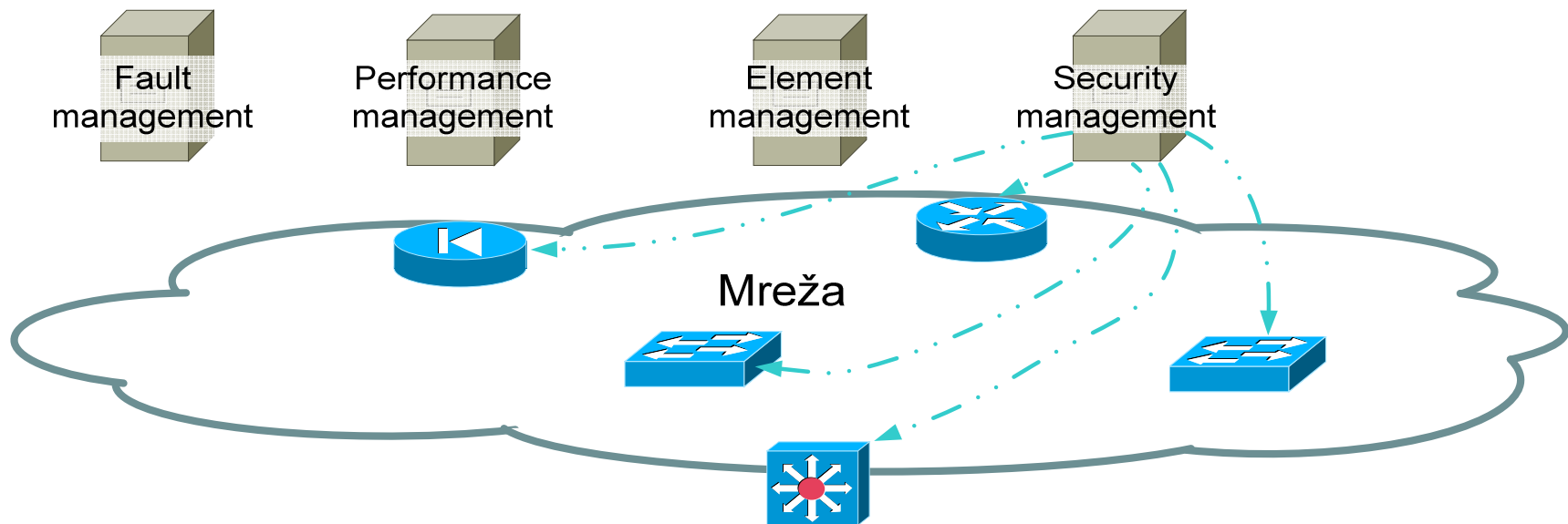
Nadzor i upravljanje mrežom



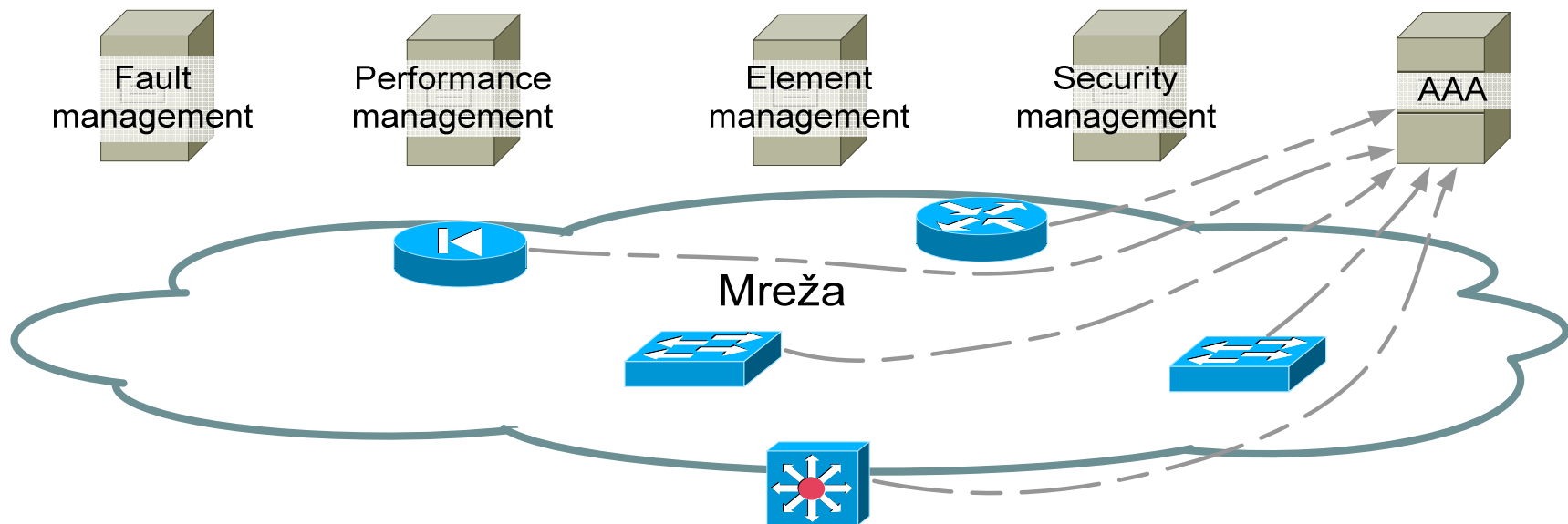
Nadzor i upravljanje mrežom



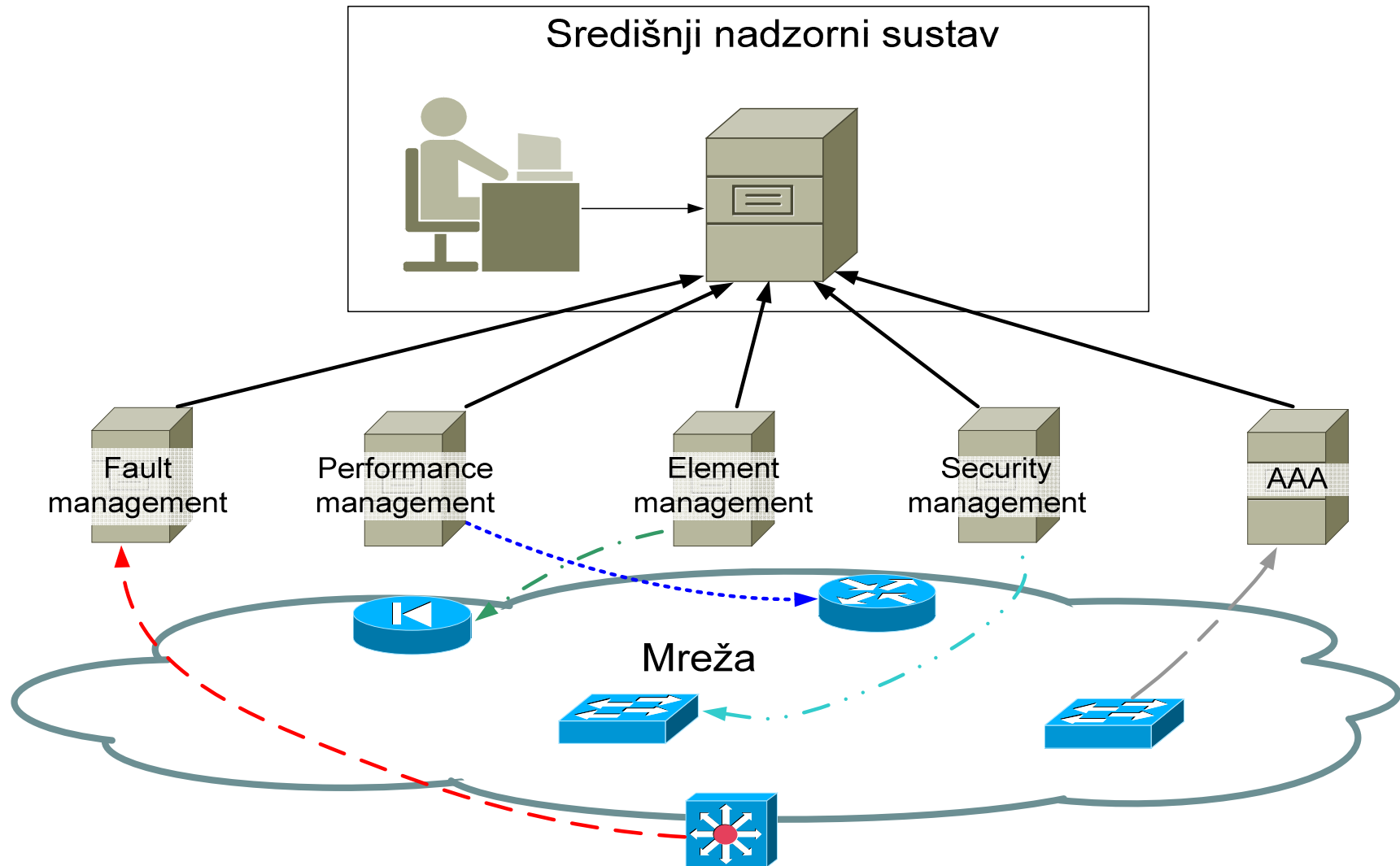
Nadzor i upravljanje mrežom



Nadzor i upravljanje mrežom



Nadzor i upravljanje mrežom



Pouzdanost i proširivost

Layer 3 infrastruktura
Redundancija
Konvergencija

Kvaliteta servisa

Garancija kvalitete
Prioritetni promet

Sigurnost

Izolacija
Kontrola krajnjih uređaja
Kontrola prometa
Kontrola servisa

Nadzor i upravljanje

Nadzor grešaka
Nadzor performansi
Nadzor pristupa
Nadzor sigurnosti

Pitanja i odgovori

