FFI-RAPPORT

20/01320

Moderne løsninger for management av sammensatte kommunikasjonsinfrastrukturer

Anders Mykkeltveit
Anders Fongen

Moderne løsninger for management av sammensatte kommunikasjonsinfrastrukturer

Anders Mykkeltveit
Anders Fongen

Forsvarets forskningsinstitutt (FFI) 13. august 2020

Emneord
Kommunikasjonsinfrastruktur
Kommunikasjonsnettverk
NFV (Network Functions Virtualisation)
SDN (Software Defined Networking)
Styring og kontroll

FFI-rapport
20/01320

Prosjektnummer
1398

Elektronisk ISBN
978-82-464-3279-3

Engelsk tittel
Management solutions for military communications networks

Godkjennere
Åshild Grønstad Solheim, *forskningsleder*
Jan Erik Voldhaug, *forskningssjef*

Dokumentet er elektronisk godkjent og har derfor ikke håndskreven signatur.

Sammendrag

Forsvaret er i økende grad avhengig av informasjons- og kommunikasjonsteknologi (IKT) for å få utført sine oppdrag. For at IKT-tjenester skal virke, må det finnes en kommunikasjonsinfrastruktur som står for overføring av informasjon mellom de ulike systemene brukerne benytter. Et velfungerende kommunikasjonsnettverk fordrer både prosesser og tekniske løsninger for styring og kontroll (management) av nettverket.

Gode tekniske løsninger for management bidrar til at nye kommunikasjonstjenester kan etableres raskt, at kommunikasjonstjenestene kan tilpasses endrede behov, at det løpende kan holdes god oversikt over tjenestekvaliteten og at tiltak for å rette opp i problemer som oppstår, kan settes inn effektivt. Alt dette er nødvendig for at IKT-tjenestene skal kunne understøtte Forsvarets evne til å utføre sine oppdrag i fred, krise og krig.

Om vi betrakter alle kommunikasjonsnettverk Forsvaret benytter seg av for å levere kommunikasjonstjenester til sine brukere, ser vi at disse nettverkene utgjør en sammensatt kommunikasjonsinfrastruktur som

- består av komponenter som benytter både nyere og eldre teknologi,
- inneholder flere sikkerhetsdomener som må isoleres,
- består av både stasjonære og mobile kommunikasjonsnettverk, og
- er bygget opp av nettverk som eies av ulike organisasjoner.

Disse forholdene bidrar til at det er utfordrende å etablere systemer som muliggjør effektivt og enhetlig management av hele kommunikasjonsinfrastrukturen. Denne rapporten vurderer på et overordnet nivå hvordan tekniske løsninger for management av Forsvarets kommunikasjonsinfrastruktur kan bygges opp med utgangspunkt i eksisterende og kommende standarder og rammeverk som utvikles i sivil sektor. Rapporten er i hovedsak basert på litteraturstudier og kontakt med aktører i privat sektor og forsvarssektoren.

Et viktig moment i denne diskusjonen er valg av ambisjonsnivå for management. Det kan være behov for mange ulike systemer som tar hånd om ulike aspekter ved management. Hvert system kan være dyrt, og det kan være krevende å få de ulike systemene til å fungere samlet. Denne rapporten har tatt utgangspunkt i et forholdsvis høyt ambisjonsnivå.

Rapporten finner at det i dag er vanskelig å oppnå helhetlig management i sammensatte kommunikasjonsinfrastrukturer, men at det ser ut til at teknologiutviklingen vil føre til at dette kan bli enklere i fremtiden. Rapporten anbefaler at Forsvaret velger et ambisjonsnivå for management og deretter etablerer et målbilde ut i fra det valgte ambisjonsnivået. For de utfordringene som ikke kan løses i dag anbefales det å følge med på teknologiutviklingen innen managementløsninger. I dag anbefaler vi at når det anskaffes nytt nettverksutstyr, må Forsvaret sørge for at dette utstyret har grensesnitt som gjør at de kan styres av de managementløsningene som kommer i fremtiden.

Summary

The Norwegian Armed Forces are increasingly dependent on Information and Communications Technology (ICT) to be able to succeed in their missions. For ICT services to work, a communications infrastructure able to transmit information between the users of the service must be in place.

Management of a communications infrastructure includes a series of tasks with the common goal to ensure that the services produced on the communications infrastructure perform as expected over time. Adequate technical solutions for management of the infrastructure enable rapid delivery of new services, rapid reconfiguration to meet changed requirements, provide good situational awareness of the quality of the services' performance and enable the proper troubleshooting actions to be taken. All of these properties are necessary in order to support the Norwegian Armed Forces in their missions in peace, crisis and war scenarios.

When one observes the totality of communications networks the Norwegian Armed Forces use to deliver services to their users, it is evident that this infrastructure is far from uniform since it

- consists of elements from both newer and older technology generations,
- contains networks belonging to multiple classification levels,
- consists of both stationary and mobile communications networks, and
- consists of networks owned by different organizations.

These issues all make the task of designing systems to effectively manage the entire communications infrastructure challenging. This report contains high level suggestions to how technical management systems for the composite communications infrastructure of the Norwegian Armed Forces may be built. The suggestions are based on frameworks and standards under development in the civilian sector.

An important part related to the topic of network management is to choose the level of ambition for management. There may be many different systems needed to handle different aspects of network management. Each system may be expensive and it can be challenging to integrate all these systems to an overall satisfactory solution. In this report, a relatively high level of ambition is assumed.

The report concludes that it is challenging today to achieve unified management of composite communications infrastructure. However, recent developments in technologies and emerging frameworks and standards can simplify this challenge. The report recommends the Norwegian Armed Forces first choose a level of ambition for management and thereafter define a target architecture based on their level of ambition. For the challenges that cannot be overcome with today's systems, it is recommended to monitor closely the development of management systems. When acquiring network equipment today it is recommended to ensure this equipment has interfaces that allow them to be monitored by future management systems.

Innhold

Forord

Arbeidet med denne rapporten inngår i en delaktivitet som studerer management av Forsvarets kommunikasjonsinfrastruktur i FFI-prosjekt 1398 «Forsvarets fremtidige kommunikasjons-infrastruktur». Delaktiviteten er finansiert av Cyberforsvaret. Arbeidet bygger i stor grad videre på FFI-rapport 17/01692 «Management av Forsvarets kommunikasjonsinfrastruktur» som tidligere har blitt utarbeidet i samme delaktivitet.

Arbeidet er utført som et samarbeid mellom Anders Mykkeltveit ved FFI og Anders Fongen ved Forsvarets Høgskole, Cyberingeniørskolen. Fongen har høsten 2019 hospitert ukentlig ved FFI.

Forfatterne ønsker å takke FFI-kollegaene Petter Kristiansen og Ingar Bentstuen for gode diskusjoner og nyttige innspill til rapporten.

Kjeller, 17. juni 2020

Anders Mykkeltveit

Lillehammer, 17. juni 2020

Anders Fongen

1 Innledning

Forsvaret er i økende grad avhengig av informasjons- og kommunikasjonsteknologi (IKT) for å få utført sine oppdrag. Gjeldende Langtidsplan for forsvarssektoren fastslår at «anvendelse av IKT er en forutsetning for å etablere situasjonsforståelse, lede militære styrker og bruke moderne våpen» [1]. For at IKT-tjenester skal virke må det finnes en kommunikasjonsinfrastruktur som står for overføring av informasjon mellom de ulike systemene brukerne benytter.

For at en kommunikasjonsinfrastruktur skal fungere som ønsket, er det ikke tilstrekkelig å bygge den – den må også driftes og utvikles. Alt som skal til av aktiviteter, metoder, prosedyrer og tekniske løsninger for å holde en kommunikasjonsinfrastruktur ved like, kalles *network management* eller rett og slett *management* [2]. Management av en kommunikasjonsinfrastruktur innebærer blant annet å overvåke den for å oppdage feil og ytelsesproblemer samt å kunne styre den for å utbedre problemer. Utvikling av kommunikasjonsinfrastrukturen må gjøres for å møte endrede krav til kapasitet og for å møte nye behov.

Forsvaret drifter per i dag en kommunikasjonsinfrastruktur kalt Forsvarets kommunikasjonsinfrastruktur (FKI). FKI består av flere ulike kommunikasjonsnettverk og inngår i Forsvarets informasjonsinfrastruktur (INI). INI omfatter også avanserte samhandlingstjenester og informasjonssystemer som muliggjør samhandling på tvers i Forsvaret. Denne rapporten fokuserer hovedsakelig på management av en kommunikasjonsinfrastruktur og fokuserer ikke spesielt på informasjonssystemer. For økt lesbarhet forkorter vi noen ganger begrepene kommunikasjonsnettverk og kommunikasjonsinfrastruktur til henholdsvis nettverk og infrastruktur.

Forsvarets nettverk skiller seg fra sivile nettverk på flere områder, noe som gjør management ekstra utfordrende:

1. Anskaffelsessyklusen for IKT-materiell har tradisjonelt vært lengre enn for sivile nettverk. Dette skyldes faktorer som krav til sikkerhetsgodkjenning, bruk av skreddersydd materiell som oppfyller militære krav til robusthet. I tillegg har forsvarssektoren i liten grad utfaset eldre systemer og ender opp med en stor portefølje av utstyr [3]. Lang anskaffelsessyklus innebærer at moderne teknologi ikke kan innføres under ett, men at man i alle endringsprosesser må regne med en lang periode hvor gammel og ny teknologi vil sameksistere.

2. Nettverket er delt opp i domener ut i fra hvilket graderingsnivå de befinner seg på. Regler for å håndtere informasjon i de ulike domenene er regulert av sikkerhetsloven og sammenkopling av slike domener er gjenstand for streng regulering og kontroll. Typisk tillates kun datatrafikk i retningen mot domenet med den «strengeste» reguleringen.

3. Deler av nettverket består av mobilt utstyr. Det benyttes radiokommunikasjon også for lange avstander (ikke bare til lokal distribusjon). Radiolinker kan ha lav overføringshastighet og dermed være mindre egnet for mediastrømmer (f.eks. videokonferanser) og andre krevende overføringstjenester.

I tillegg til de tre problemstillingene ovenfor, vil det fremover trolig bli endringer i tilknytning til eierskapet til nettverkene Forsvaret benytter seg av. Dette tas med som en fjerde problemstilling vi ser nærmere på i denne rapporten:

4. Det totale nettverket som leverer kommunikasjonstjenester til Forsvaret forventes fremover i større grad enn i dag å være satt sammen av egen infrastruktur og infrastruktur fra kommersielle leverandører. Dette er i tråd med mål om strategisk samarbeid innen teknologi generelt og innen cyberforsvaret spesielt [4]. Dette medfører at det er nødvendig å vurdere management på tvers av eierskap i større grad enn i dag.

Disse fire problemstillingene bidrar alle til at Forsvaret må utføre management av en *sammensatt infrastruktur*. Målet med rapporten er å fremme forslag til en helhetlig managementløsning for Forsvarets sammensatte kommunikasjonsinfrastruktur og foreslå tilhørende teknologikomponenter som kan støtte management av sammensatte kommunikasjonsinfrastrukturer bygget med moderne tekniske løsninger.

Denne rapporten er hovedsakelig basert på studier av åpent tilgjengelig litteratur og inntrykk fra deltakelse på SDN NFV World Congress i 2018 [5]. Vi har i tillegg diskutert problemstillinger og muligheter innen management med ansatte i Forsvarsmateriell (FMA) og Telenor. Vi har tilegnet oss kunnskaper om management i deployerte nettverk gjennom implementasjon og testing av Protected Core Networking (PCN) under interoperabilitetsøvelsen CWIX [6]. Som bakgrunn for kapittel 3.2 har vi eksperimentert noe med verktøyet Open Source MANO [7].

Vi har valgt å beholde noen engelske begreper i teksten, ettersom disse er innarbeidet både i dagligtale og i mye av litteraturen og begrepsapparatene som allerede brukes. Vi har brukt det engelske begrepet management i stedet for det norske begrepet styring og kontroll fordi begrepet kontroll kan assosieres med nettverkets kontrollplan som ikke er relatert til management men til ruting.

1.1 Ambisjonsnivå for management

For å vurdere tilnærming til management er det viktig å ha avklart ambisjonsnivået. Dette ambisjonsnivået vil være førende for hvilke krav som settes til de tekniske managementløsningene som velges. Er managementløsningene utviklet for et lavt ambisjonsnivå, kan det gi seg utslag i at:

- Management er fragmentert, idet tekniske domener er utstyrt med separate managementløsninger som i liten grad samarbeider, og hvor informasjonen de inneholder ikke kan settes sammen til et aggregert helhetsbilde av status for kommunikasjonsnettverket og tjenestene nettverket leverer.

- Management har fokus på tekniske komponenter, ikke på tjenesteproduksjon. Dette innebærer at det er lite fokus på hvordan konfigurasjon av én komponent påvirker tjenestene som beror på denne komponenten.

- Manglende helhetsbilde av status for komponenter gjør feilsøking tid- og personell-krevende.

- Endringer i konfigurasjonen eller strukturen utover det grunnleggende og dagligdagse er en krevende prosess, og det oppstår lett ikke-forvaltede ad hoc-løsninger for endringer.

I denne rapporten legges det til grunn at Forsvaret ønsker et forholdsvis høyt ambisjonsnivå for management. Til grunn for dette legger vi Forsvarets økte avhengighet til IKT som beskrevet i LTP. Et høyt ambisjonsnivå innebærer at vi forventer at det skal være kontroll på tilstanden i hele nettet, og det skal være mulig å utføre management av hele nettet. Det bør også være mulig å gjennomføre endringer raskt, gjerne gjennom ett enkelt grensesnitt i stedet for å måtte konfigurere gjennom mange uavhengige systemer.

Ved bruk av moderne managementløsninger ønskes et sterkt *operativt fokus*, dvs. fokus på egenskapene i nettverket som avgjør om det kan støtte planlagte og pågående operasjoner. For å for eksempel kunne gjennomføre en videokonferanse, må nettverket tilby overføringstjenester med de nødvendige egenskaper langs den trafikkerte stien av linker, men ikke nødvendigvis utenfor denne. Å styre nettverket med et detaljnivå ned på enkelttjenester, som videokonferanse i eksempelet, kalles tjenesteorientering. Tjenesteorientering skiller seg fra en grovere og mer tradisjonell tilnærming til management, som for eksempel å operere med en gjennomsnittlig overføringskapasitet for alle linkene i nettverket. Tjenesteorientering innebærer at andre og mer sammensatte måledata må innhentes, og at et sett av spesifikke operasjoner må gjøres på teknologikomponentene for å gi den planlagte videokonferansen de nødvendige ressurser, samtidig som man er klar over hvilke andre tjenester som berøres og hvilke operative konsekvenser dette får.

Vi forstår at det er sterkt ønskelig for Forsvaret å ha et oppdatert situasjonsbilde over nettverkets helsetilstand, såkalt Recognized Cyber Picture (RCyP). Dette begrepet er ikke presist definert, og forventningene til hva slags informasjon et RCyP inneholder, varierer sterkt. Det legges i denne rapporten til grunn at RCyP har et operativt fokus og viser hvilke tjenester som kan tilbys i forskjellige deler av nettet, pågående trusler, feilsituasjoner og trafikkstatistikk, og at alle slike opplysninger kan vises i en historisk sammenheng.

Videre legger vi til grunn at det med moderne managementløsninger er mulig å gjennomføre en konstant migrasjon mellom teknologigenerasjoner, dvs. at utstyr skal kunne moderniseres og fortsatt delta i den samlede verdikjeden uten at andre deler av systemet blir nevneverdig påvirket.

Det er fremfor alt ønskelig å realisere managementløsninger som skaper færre feilsituasjoner, gir raskere endringer til lavere kostnader, gir bedre situasjonsoversikt og muliggjør raskere feil-søking.

1.2 Avgrensninger

Rapporten fokuserer hovedsakelig på tekniske systemer og løsninger for management av kommunikasjonsnettverk. De tekniske løsningene skal støtte opp under operativ drift, men prosedyrer for, og organisering av, drift er ikke hovedfokus i rapporten.

Når det gjelder selve kommunikasjonsnettverkene som det skal utføres management av, ligger fokus på den logiske delen av infrastrukturen, det vil si konfigurasjon av nettelementer som svitsjer, rutere og brannmurer og høyere ordens tjenester i infrastrukturen. Management av de fysiske komponentene og kommunikasjonslinjene i infrastrukturen gjennom f.eks. inventardatabaser ansees som et dekket behov og er ikke omtalt i rapporten.

Rapporten fokuserer ikke bare på stasjonær kommunikasjonsinfrastruktur, men også på mobil og deployerbar infrastruktur som ikke er konstant operativ, men som er i bruk i forbindelse med militære operasjoner.

1.3 Tidligere arbeid

FFI-rapport 17/01692 [8] etablerer begreper for å snakke om management i Forsvaret. Den beskriver hvordan to aktører som har lignende nettverk som Forsvaret har innrettet seg og anbefaler at Forsvaret studerer tekniske løsninger for å automatisere management.

En rapport Analysis Mason har levert til Forsvarsmateriell [9] gir oversikt over status og utfordringer i forbindelse med management av Forsvaret sine IKT-systemer i dag samt en gjennomgang av dagens beste praksis og trender fra industrien.

De to rapportene [8] og [9] går ikke inn på spesielle utfordringer som Forsvaret har i forbindelse med sammensatte kommunikasjonsinfrastrukturer, slik som flere graderingsnivåer eller at deler av infrastrukturen er mobil.

1.4 Oppbygning av rapporten

Resten av rapporten er bygget opp som følger. I kapittel 2 forklares det i mer detalj hva som menes med sammensatte kommunikasjonsinfrastrukturer. I kapittel 3 gis en oversikt over standarder og rammeverk for management. I kapittel 4 presenteres noen teknologikomponenter som kan anvendes for å bygge opp en helhetlig løsning for management. I kapittel 5 gis det innspill til en helhetlig løsning for management for Forsvarets kommunikasjonsinfrastruktur basert på foregående kapitler. I kapittel 6 avsluttes rapporten med noen vurderinger og anbefalinger om management.

2 Sammensatte kommunikasjonsinfrastrukturer

Med Forsvarets kommunikasjonsinfrastruktur (FKI) mener vi i denne rapporten summen av alle stasjonære, deployerbare og mobile kommunikasjonsnettverk som Forsvaret benytter. FKI er i hovedsak sammenhengende, i den forstand at alle endesystemer kan kommunisere med hverandre. FKI kan betegnes som en sammensatt infrastruktur, hvor de tekniske komponentene skiller seg fra hverandre på ulike måter. Figur 2.1 viser et eksempel på en sammensatt kommunikasjonsinfrastruktur som Forsvaret kan benytte seg av for å levere sine kommunikasjonstjenester. Den midterste delen av figuren viser eksempler på ulike teknologier som benyttes – fiber, satellitt, radiolinje og mobilnettverk. Den nederste delen av figuren viser eksempler på ulike eiere som denne sammensatte kommunikasjonsinfrastrukturen kan ha.

Figur 2.1 Eksempel på sammensatt kommunikasjonsinfrastruktur som Forsvaret benytter seg av for å levere kommunikasjonstjenester [10].

I dette kapittelet trekkes det fram fire måter som FKI er oppdelt på. I tillegg til de allerede nevnte aspekter teknologi og eierskap, diskuteres også sikkerhetsdomener samt det forhold at av Forsvarets nettverk består av både stasjonære, deployerbare og mobile nettverk i dette kapittelet.

2.1 Ulike teknologier

Komponenter i nettverket som skal tilby tjenester i ulike aktuelle omgivelser (utendørs/innendørs) og under ulike forhold (stasjonært/mobilt), vil ha ulike egenskaper knyttet til strømforbruk, modulasjonsformer, fysisk robusthet og tilleggstjenester (rutingprotokoller, kontrollgrensesnitt, kryptering, etc.).

Enkelte av de tekniske egenskapene kan knyttes til et generasjonsbegrep: Komponenter med nye tjenester og protokoller blir gradvis innført i markedet, men mulighetene disse nye komponentene gir blir ikke unyttet fullt ut med mindre de omkringliggende komponentene også støtter de samme tjenestene og protokollene. Mellom gamle og nye komponenter eksisterer det dermed en generasjonskløft som forhindrer en effektiv utnyttelse av det nyeste utstyret.

I dag er det meste av nettverksutstyret tilpasset IP-ruting. Tjenestene i nettet produseres tradisjonelt enten på spesialisert maskinvare (for eksempel ved hjelp av rutere og brannmurer), eller ved hjelp av programvare som kjører på hver sin egen servermaskinvare (for eksempel navnetjenere). To sentrale nye teknologier innen kommunikasjonsinfrastrukturer er *Network Functions Virtualisation* (NFV) og *Software Defined Networking* (SDN), og disse teknologiene vil endre hvordan managementløsninger er bygget opp.

NFV består i utgangspunktet av at den spesialiserte maskinvaren nettelementene er bygget på byttes ut med rene programvarebaserte løsninger realisert som *virtuelle nettverksfunksjoner* (VNFer). VNFene kjøres i datasentre bygget opp av standard server-maskinvare, men med noen tilpasninger for kommunikasjonstjenesters behov. Datasentrene kan være forholdvis store og være plassert sentralt i nettet eller de kan være mindre datasentre plassert i «kanten» av nettet. Ved å bruke standard servermaskinvare, kan operatøren spare utgifter, og NFV gir økt fleksibilitet ved at kapasiteten i VNFene enkelt kan tilpasses behovet. NFV gjør det også mulig å lansere nye tjenester raskere enn tidligere, siden det vanligvis er raskere å utvikle ny programvare enn å utvikle og anskaffe nye maskinvarebaserte nettelementer.

SDN er en nettverksteknologi som introduserer programmerbare svitsjekomponenter i infrastrukturen. Programmerbarheten gjør det langt mer fleksibelt å bygge nettverk med SDN enn med tradisjonell teknologi. Én enkelt SDN-svitsj vil ha begrenset nytte – det er først når SDN-svitsjer danner sammenhengende strukturer at potensialet ved SDN vil kunne utnyttes optimalt. Open Networking Foundations definisjon av SDN er at nettverkets kontrollplan er fysisk skilt fra ressursene (svitsjene) som håndterer trafikk i nettverket[1]. I de fleste løsninger for SDN benyttes det én sentral node kalt *SDN controller* som styrer alle ressursene i nettet.

Vi tror at kommunikasjonsnettene Forsvaret benytter seg av i fremtiden i større grad vil være en blanding av nettverk med tradisjonell IP-ruting og SDN. Det vil også bli en blanding av tradisjonelle komponenter basert på spesialisert maskinvare og nye komponenter basert på NFV. Det er viktig at managementløsninger støtter opp om disse ulike teknologiene og teknologier som vil bli introdusert lengre fram i tid.

2.2 Sikkerhetsdomener

Forsvarets informasjonssystemer og kommunikasjonsnettverk er godkjent for å behandle informasjon opp til en bestemt sikkerhetsgradering, og data i et system skal behandles i henhold til reglene for det høyeste graderingsnivået som systemet er godkjent for. Slik oppstår begrepet

[1] https://www.opennetworking.org/sdn-definition

partisjonert operasjonsmåte som sikrer tilstrekkelig beskyttelse av gradert informasjon, men gjør det komplisert å behandle lavere gradert informasjon fra dette systemet. For eksempel vil varslinger generert i ett nettverk måtte behandles som informasjon av høyeste tillatte gradering hvis all varsling er samlet i samme managementløsning, noe som kompliserer samordnet management med nettverk for lavere graderte informasjonssystemer.

Gradert informasjon vil kunne overføres i nettverk godkjent for det aktuelle graderingsnivået, eller gjennom lavere gradert nettverk dersom det er kryptografisk beskyttet. Et ugradert nettverk kalles ofte «sort nettverk». Skillet mellom nettverk tilhørende ulik gradering skal være robust, og sammenkopling mellom dem, f.eks. i den hensikt å overvåke en sti av svitsjer under ett, er gjenstand for streng regulering. Generelt er det grunnlag for å anta at overvåking av nettverk vil måtte foregå separat for hvert sikkerhetsdomene.

2.3 Stasjonære, deployerbare og mobile kommunikasjonsnettverk

Hos kommersielle nettverksoperatører er stort sett hele kommunikasjonsinfrastrukturen stasjonær. De kommersielle mobilnettene er stort sett bygget opp med stasjonære basestasjoner, mens kun brukerne er mobile. Forsvarets kommunikasjonsinfrastruktur (FKI) har én stasjonær del bygget opp med kommunikasjonslinjer av fiber og radiolinje og i tillegg finnes andre stasjonære nettverk. I tillegg har Forsvaret nettverk som er deployerbare og nettverk som er mobile hvor selve infrastrukturen flytter på seg.

Deployerbare nettverk opererer fra samme sted over noe tid og har ofte relativt god kapasitet. Det er ofte planlagt på forhånd når disse nettene skal etableres og når de skal tas ned. For bruk under øvelser og operasjoner på landjorda har Forsvaret mobile taktiske noder [11]. Nodene benytter ulike bærere, for eksempel satellitt for å koble seg til stasjonær infrastruktur. De taktiske nodene leverer en utvidelse av den ugraderte delen av FKI og kan brukes av flere lokalnettverk (informasjonsdomener) som opererer på ulike graderingsnivåer.

Mobile nettverk er oftere i bevegelse enn deployerbare nettverk, og ofte må mobile nettverk levere kommunikasjonstjenester mens nettelementene er i bevegelse, for eksempel hvis nettelementer er montert i kjøretøy. Mobile nettverk er ofte graderte og tilegnet en avdeling. I mobile nettverk benyttes ofte radioløsninger som gjør at tilgjengelig overføringskapasitet er langt lavere enn i stasjonære og deployerbare nettverk. Det kan være vanskelig å prioritere mellom nyttetrafikk og managementtrafikk i de mobile nettverkene.

Mobile nettverk vil, som en del av normalsituasjonen, kunne bli utilgjengelige både for ordinær kommunikasjon og for management. I den stasjonære infrastrukturen vil derimot et utilgjengelig endesystem representere en feilsituasjon. Dette innebærer at det kan være behov for spesialtilpassede managementløsninger for mobile nettverk.

Vi finner dynamikk i trafikkmønsteret så vel som i infrastrukturen. Det er grunn til å anta at Forsvarets nettverk utviser større variasjon i trafikkmønsteret enn nettverk i en sivil bedrift. Dette er knyttet til den utstrakte øvingsaktiviteten og pågående militære operasjoner.

Dynamikk i nettverksstrukturen representerer en utfordring for driftspersonell, delvis fordi stadige endringer i infrastrukturen skaper mye managementtrafikk og kan føre til mange unødvendige alarmer i driftssenteret, men også fordi isolerte deler av infrastrukturen bør kunne operere autonomt, uten å ha kontakt med det sentrale systemet for management.

2.4 Eierskap

Forsvaret har hittil selv vært eier av de fleste nettverkskomponentene (svitsjer, linker, mm.) i FKI, med unntak av satellittlinker og linker gjennom offentlige mobilnettverk (4G). Dette bildet er i endring i retning av å kjøpe kommunikasjonstjenester fra kommersielle leverandører. En leverandør som leverer en driftet kommunikasjonstjeneste kalles en (kommersiell) operatør. En situasjon hvor Forsvaret produserer deler av en kommunikasjonstjenester selv og kjøper resten av tjenesten fra en kommersiell operatør innebærer at verdikjeden, som resulterer i kommunikasjonstjenester til endesystemene, vil være en blanding av egen produksjon og innkjøpte tjenester. Dette er en stor endring fra dagens situasjon, hvor Forsvaret ofte leier «mørk fiber» og produserer hele tjenesten ende-til-ende ved hjelp av disse.

Det ligger både tekniske, juridiske og administrative utfordringer i en slik situasjon. Fra et teknisk perspektiv reiser deg seg problemstillinger knyttet til management av ressurser i en verdikjede som spenner over flere foretak. Utfordringene er blant annet knyttet til at oppgaver må gjøres manuelt når det ikke finnes protokoller og grensesnitt som kan brukes for management på tvers av eget og andre leverandørers nettverk.

Det vil være ønskelig at Forsvarets leverandører tilbyr grensesnitt hvor Forsvaret kan disponere de innkjøpte kommunikasjonsressursene i henhold til egen prioritering. Mulighetene for dette undersøkes i denne rapporten.

3 Standarder og rammeverk for management

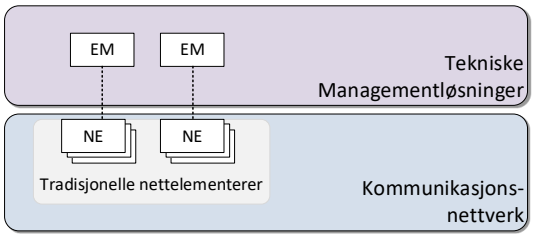
Dette kapittelet inneholder en oversikt over ulike standarder og rammeverk som kan benyttes som utgangspunkt for å implementere managementløsninger. Det fokuseres på standarder og rammeverk med bred oppslutning i industrien fremfor proprietære løsninger fra enkeltleverandører. Begrepene som brukes er ikke enhetlig standardisert, og ulike definisjoner kan forekomme i ulike modeller. Her brukes en enkel kategorisering basert på rammeverk som enten er etablert eller under utvikling i ulike standardiserings- og bransjeorganisasjoner.

3.1 Management av tradisjonelle nettverk

Forenklet kan det sies at et kommunikasjonsnettverk er bygget opp av nettelementer og linker mellom disse. I tradisjonelle nettverk er nettelementene fysiske «bokser» som ofte har en definert funksjonalitet slik som en IP-ruter, Ethernet-svitsj eller brannmur. Linkene mellom nettelementene kan for eksempel være fiberkabler eller luftstrekk (i forbindelse med radiolinjer).

Den internasjonale teleunionen, ITU-T, definerer rammeverk for management av tradisjonelle telekommunikasjonsnettverk i *recommendation M.3010* [12]. ITU-T bruker en lagdelt modell hvor det nederst skilles mellom *element management* og *network management*. Element management dreier seg om å styre et sett av enkeltkomponenter i nettet, og programvareløsninger på dette nivået kalles Element Managere (EMer). En EM kan være begrenset til én type utstyr fra én enkelt leverandør, eller løsningen kan støtte noe flere typer utstyr og/eller flere leverandører. Hovedpoenget er at løsningen har fokus på management av individuelle nettelementer.

I mindre nettverk er det vanlig å kun benytte EMer for management av nettverket. Et forenklet oppsett med kun to typer nettelementer som er koblet til hver sin EM er vist i Figur 3.1. Her er det ingen integrasjon mellom EMene, og driftspersonell må derfor manuelt logge seg på begge EMene for å utføre management av tjenester som leveres av kommunikasjonsnettverket.



Figur 3.1 Management ved hjelp av Element Managere (EM) – brukt i mindre kommunikasjonsinfrastrukturer.

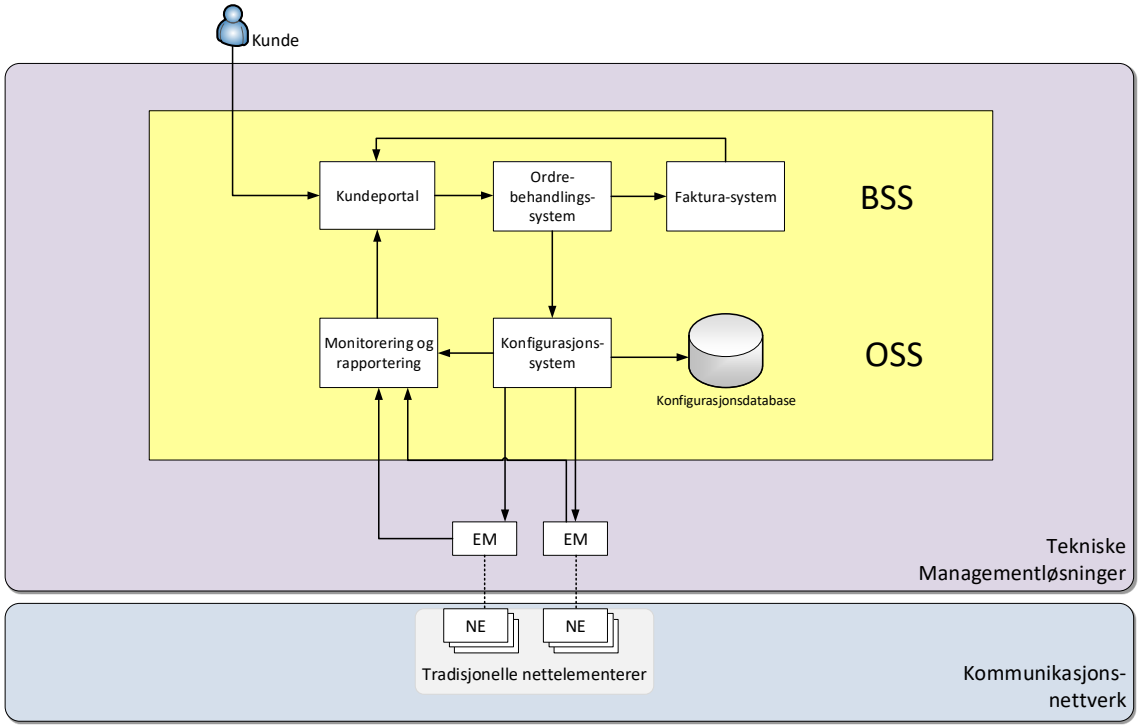
Network management dreier seg om å styre nettverket som helhet. Programvareløsninger innenfor network management kalles ofte for Operations Support Systems (OSS). Begrepet Network Management System (NMS) brukes noen ganger også som et alternativ til OSS

og/eller EM. OSS-systemene inneholder konfigurasjonen til alle nettelementer fra alle leverandører og de kan overvåke ytelsen til alle nettelementene. OSS muliggjør dermed konfigurasjon og overvåking av *tjenester* heller enn enkeltkomponenter.

På laget over network management har ITU-T definert et lag som kalles *service management layer*. Dette laget er ansvarlig for ordre og kontraktsmessige forhold til kunder. Systemene i dette laget kalles for Business Support Systems (BSS).

OSS- og BSS-systemer er generelt større og mer komplekse enn EM-systemer og er oftere brukt i større nettverk, for eksempel hos tjenesteleverandører som Telenor og Broadnet.

Figur 3.2 viser et forenklet eksempel på managementsystemer som må kommunisere når en kunde bestiller en løsning via en kundeportal hos en operatør og tjenesten skal leveres. I eksemplet legger kunden inn en bestilling via en kundeportal som kan være en webside. Bestillingen sendes til et ordrebehandlingssystem som videre kaller opp andre systemer. Ordren sendes til et konfigurasjonssystem som vil kunne omforme ordren til konfigurasjon som kan utføres av EM. Konfigurasjonssystemet må også sørge for at konfigurasjonsendringene blir lagret i en konfigurasjonsdatabase samt at det blir gjort klart for monitorering og rapportering av hvordan den oppsatte tjenesten fungerer. Rapporter kan igjen bli tilgjengelige for kunden i kundeportalen. Når ordren er ferdigbehandlet vil det legges til avregning i fakturasystemet.



Figur 3.2 Eksempel på BSS- og OSS-komponenter involvert i en kundeleveranse.

I virkeligheten vil det kunne være langt flere systemer som er involvert i en slik ordreprosess hos en teleoperatør. For eksempel kan det være mange ulike nettelementer som må konfigureres. Disse kan potensielt være knyttet til ulike ordrebehandlingssystemer og konfigurasjonssystemer. Informasjon må kanskje hentes inn fra eksterne datakilder og kanskje må det også bestilles montør for å utføre kabling eller utplassering av utstyr.

Tradisjonelt har OSS og BSS vært adskilte systemer, men i dag brukes gjerne begrepet BSS/OSS samlet siden de henger tett sammen. BSS/OSS kan være satt sammen av mange systemer som kan være til dels overlappende.

Leveranse av en tjeneste er bare ett eksempel på hva BSS- og OSS-systemene skal håndtere. De skal for eksempel også håndtere feilhendelser, endring av trafikk og utvidelser av nettet. Når man tar i betraktning at en teleoperatør leverer mange tjenester over mange slags underliggende kommunikasjonsinfrastrukturer, vil antallet systemer innen BSS/OSS kunne bli svært høyt. Det nevnes for eksempel i [13] at den britiske operatøren BT har klart å redusere antallet systemer fra 4500 til 1798 gjennom et konsolideringsprosjekt det tok syv år å gjennomføre. Norske forhold er noe mindre, men antallet systemer vil likevel være høyt for norske operatører.

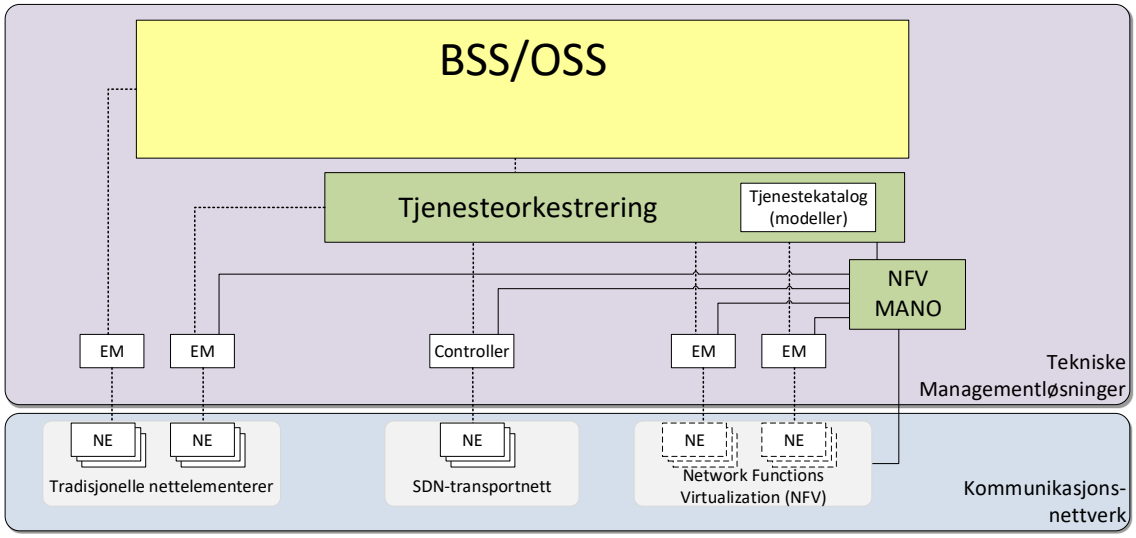
Det å få en rekke komponenter i BSS/OSS til å fungere sammen, har tradisjonelt krevet at det lages spesialtilpassede grensesnitt mellom komponentene. Når det ikke finnes standarder som beskriver disse grensesnittene ender man fort opp med at hver operatør må utvikle grensesnittene selv.

Teleoperatørene har gjennom organisasjonen TMForum arbeidet med å utvikle standardiserte grensesnitt mellom komponentene i BSS/OSS. Slike grensesnitt kalles vanligvis *Application Programming Interface* (API). I dag finnes det over 50 APIer for BSS/OSS definert av bransjeorganisasjonen TMForums *Open API-rammeverk* [14]. Ved anskaffelse av BSS/OSS-systemer kan det være lurt å forsøke å velge systemer som støtter Open API for å redusere utfordringer med integrasjon av ulike systemer.

3.2 Management av fremtidige nettverk

Som beskrevet i kapittel 2.1, forventer vi at fremtidens kommunikasjonsnettverk vil inneholde stadig større innslag av NFV og SDN. Med NFV blir det nødvendig å håndtere det som kalles *livssyklusen* til VNFene. Dette innebærer å opprette nye VNFer og terminere VNFer når de ikke lenger skal brukes. Gjennom levetiden kan kapasiteten til en VNF justeres opp og ned ved behov ved at de tildeles mer eller mindre prosessorkapasitet, lagringsplass og minne. Det blir også mulig å flytte VNFer rundt i nettet, fra ett datasenter til et annet, noe som kan være nyttig for å optimalisere tjenestene. Et eksempel på slik optimalisering kan være å flytte VNFer nær brukerne for å redusere forsinkelsen når de kommuniserer med hverandre. VNFer inngår som byggeklosser i nettverkstjenester. En nettverkstjeneste kan for eksempel være et lukket virtuelt nettverk for et sett brukere, som inneholder VNFer som tilbyr byggeklosser som adressetildeling (DHCP), navnetjenester (DNS) og en brannmur som begrenser forbindelse mot andre nettverk.

Figur 3.3 viser en oversikt over komponenter som forventes å inngå i tekniske management-løsninger for et typisk kommunikasjonsnettverk noen år fram i tid. Nettet vil da bestå av tradisjonelle fysiske nettverkselementer, VNFer og SDN-nettelementer. I figuren indikerer heltrukne linjer mellom komponenter at management er relatert til NFV, mens stiplede linjer er relatert til tjenestelogikk.



Figur 3.3 Oversikt over managementløsninger for moderne kommunikasjonsnettverk.

Standarder for management innenfor NFV utvikles av organisasjonen ETSI. ETSI bruker begrepet NFV Management and Orchestration (MANO) om systemet som utøver management over både nettverkstjenester og VNFene nettverkstjenestene inneholder. Den overordnede standarden fra ETSI for NFV MANO er [15]. Her spesifiseres grensesnittene mellom NFV MANO og BSS/OSS samt mellom NFV MANO og underliggende NFV-infrastruktur.

Det må bygges opp modeller av hver nettverkstjeneste før man oppretter én eller flere instanser av nettverkstjenestene. Det finnes ulike språk som er egnet for å beskrive tjenestemodeller. To språk som ofte benyttes er YANG [16] og TOSCA [17]. YANG er et språk som er utviklet med tanke på å beskrive nettelementer eller nettverkstjenester mens TOSCA [17] er utviklet med tanke på å beskrive skytjenester for IT.

NFV MANO dekker ikke den delen av tjenesteorkestrering som er knyttet til å styre selve oppførselen til nettverkstjenestene, det vil si tjenestelogikk. Tjenestelogikken kan være hvilke regler en brannmur forholder seg til eller hvilke IP-adresser en DHCP-server skal dele ut til klientdatamaskiner. Managementsystemet som håndterer tjenestelogikken kalles gjerne *ende-til-ende tjenesteorkestrering* eller bare *tjenesteorkestrering*. Tjenesteorkestratorer kan gjerne styre både virtualiserte nettelementer, tradisjonelle nettelementer og SDN-elementer. SDN er en teknologi som kan inngå på flere måter i relasjon til NFV. Internt i datasentrene som kjører NFV brukes det nær sagt alltid SDN for å koble sammen VNFer som kjører på ulike fysiske servere. SDN

kan også brukes i transportnettet mellom datasentrene samt ut mot sluttbrukere og andre nettverk. SDN controllere kan også være implementert som VNFer og styrt av tjenesteorkestratorer og NFV MANO.

I Figur 3.3 beholdes forbindelsen mellom BSS/OSS og enkelte tradisjonelle nettelementer siden det i praksis vil kunne finnes nettelementer det ikke er hensiktsmessig å integrere med tjenesteorkestrator.

Det finnes to viktige initiativ i telekommunikasjonsbransjen som jobber med å utvikle hvert sitt NFV MANO:

- ONAP [18] er et initiativ tilsluttet Linux Foundation som ledes av store internasjonale teleselskaper som AT&T og China Telecom og utstyrsleverandører som for eksempel Huawei. ONAP inneholder NFV MANO, men ser også ut til å inneholde en del funksjonalitet innen tjenesteorkestrering.

- Open Source MANO (OSM) [19] er et initiativ under ETSI hvor teleselskapet Telefonica er toneangivende. OSM har over hundre medlemsorganisasjoner, blant disse finner vi Telenor. OSM ser ut til å være begrenset til å implementere ETSI MANO.

OSM og ONAP trekkes her fram fordi de store teleselskapene putter mye innsats i disse systemene, og de kan ende opp som industristandarder som tilstøtende systemer som tjenesteorkestrator og VNFer må forholde seg til. I tillegg til ONAP og OSM finnes det kommersielle alternativer som enten er helt isolerte systemer eller løsninger som bygger på funksjonalitet fra OSM eller ONAP.

Det er et mål å få både tjenesteorkestratorer og NFV MANO-løsninger til å styre nettet på egen hånd ved hjelp av såkalte *closed feedback loops*. I den videre teksten bruker vi begrepet MANO som fellesbetegnelse for både tjenesteorkestrator og NFV MANO. Closed feedback loop innebærer at MANO mottar måledata fra nettverket, analyserer disse og bruker definerte regler eller kunstig intelligens til å ta avgjørelser om nødvendige endringer i nettet. MANO sender deretter managementmeldinger på egen hånd til det underliggende nettverket. Et eksempel på en slik closed feedback loop er at NFV MANO mottar måledata som viser at trafikkpåtrykket på en VNF er for høyt, og selv starter flere VNFer av samme type som sammen klarer å håndtere trafikken.

Det kreves en del arbeid før en VNF kan integreres i NFV-miljøet hos en operatør. En VNF må ha et managementgrensesnitt tilpasset NFV MANO i henhold til spesifikasjonene fra ETSI. I tillegg må hele konfigurasjonen til VNFen representeres i en modell som integreres i MANO. Enkeltstående nettelementer modelleres i de fleste tilfeller med YANG. Per i dag kreves det lang tid, gjerne ett helt år, å få til integrering av nye VNFer hos en operatør [5].

Det er viktig å påpeke at innføringen av MANO neppe vil erstatte BSS/OSS. En del detaljer om hvordan tjenester er realisert, vil være håndtert av MANO, og en del BSS/OSS-systemer vil dermed kunne forenkles noe.

3.3 Management på tvers av nettverk med ulikt eierskap

Dette kapittelet fokuserer på integrasjon mellom nettverk med ulikt eierskap og hvordan management kan foregå mellom nettverkene. Ofte er disse nettene eid og driftet av ulike operatører som selv ønsker å ha management av sitt eget nettverk. Tradisjonelt har det ikke vært noen integrasjon av managementløsninger når to operatører har koblet sammen nettverkene sine for å gi en sammenhengende tjeneste. I kapittel 3.3.1 beskrives det hvordan dette tradisjonelt har foregått. I kapittel 3.3.2–3.3.4 presenteres tre aktuelle initiativer som er relevante for å integrere managementløsninger mellom ulike operatører. Det diskuteres hvilke muligheter disse initiativene gir for management av tjenester som leveres over mer enn ett nettverk.

3.3.1 Tradisjonell integrasjon

I dette avsnittet oppsummeres det utfordringer vi erfarer[2] operatører tradisjonelt har hatt med management av forbindelser som går på tvers av nettverk med ulikt eierskap.

Før forbindelser kan etableres på tvers av operatører, må det først etableres fysiske sammenkoblinger av operatørenes kommunikasjonsnettverk – dette må gjøres uavhengig av integrasjon av managementsystemer.

Når to operatører som er sammenkoblet skal etablere tjenester gjennom sine nett har det tradisjonelt kun vært en integrasjon av selve nettverkene, men ikke av BSS/OSS-systemene. Mangel på slik integrasjon betyr at driftsrelaterte oppgaver utføres med manuelle prosesser. Her følger noen eksempler på oppgaver som ofte er automatisert gjennom OSS/BSS-systemene i eget nett, men som involverer manuelle prosesser når forbindelser skal etableres mellom to operatører.

- *Etablering av tjenester*
  Operatøren som ønsker at en tjeneste skal etableres må sende en forespørsel om hva som skal settes opp, spesifisert med relevante tekniske parametere. Parameterne er avhengig av hva slags tjeneste som etableres, men kan for eksempel være IP-adresser, VLAN-nummer, båndbredde og tjenestekvalitetsparametere. Tjenesten er etablert når begge operatører har lagt inn alle parameterne i sine BSS/OSS-systemer. Tradisjonelt har parameterne blitt utvekslet manuelt mellom operatørene, noe som har ført til at det tar tid (dager/uker) å få etablert nye tjenester gjennom flere operatørers nett.

- *Endringer av allerede etablert tjeneste*
  Dersom en parameter, for eksempel overføringskapasitet, skal endres, må dette også forespørres og legges inn manuelt i begge operatørers BSS/OSS-systemer. Leveringstid for endringer kan i likhet med etablering av logiske forbindelser være lang på grunn av de manuelle prosessene som kreves.

- *Overvåking av levert tjeneste*
  Operatørene kan tilby hverandre webgrensesnitt eller periodiske rapporter om ytelsen til

[2] Inkludert førsteforfatters erfaringer fra tidligere stilling i Telenor Global Services

tjenesten gjennom sitt nett. Dette kan være rapporter over antall tapte pakker eller trafikkmengde som har blitt transportert. Disse rapportene må leses av mennesker og måledataene vil ikke bli tilgjengelig i eget netts BSS/OSS-systemer slik tilsvarende parametere fra eget nett er.

- *Håndtering av feil på tjenesten*
  Tjenesten vil i utgangspunktet bli gjenopprettet uavhengig av om feil skjer i eget nett eller i ekstern leverandørs nett, da begge operatører oppdager og retter feil i egne nett. Utfordringer med feil på tjenester som leveres ved bruk av eksterne operatører kan være relatert til informasjonsutveksling. Eksempel på problemstillinger som kan oppstå er usikkerhet omkring hvorvidt en ekstern leverandør har oppdaget en feil i nettverket sitt, eller usikkerhet omkring hvor lang tid det kan forventes å ta å rette en feil.

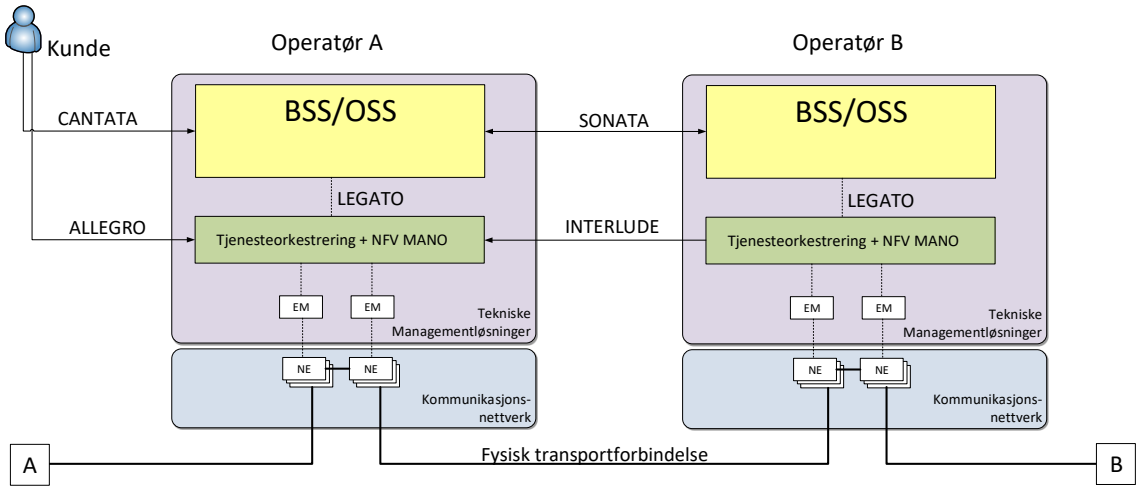
3.3.2 MEF LSO

Telebransjen jobber, gjennom initiativet Lifecycle Service Orchestration (LSO) [20], med å redusere tiden det tar å etablere logiske forbindelser gjennom flere operatørers nett. LSO definerer grensesnitt mellom kunder og operatører og mellom operatører for etablering og drift av kommunikasjonstjenester. LSO administreres av organisasjonen MEF (MEF sto tidligere for Metro Ethernet Forum). Fokuset til MEF har først og fremst vært på å levere leide Ethernet-linjer, men har de senere årene blitt utvidet til flere tjenester, som optisk transport og IP-forbindelser. Vi tror teleoperatørene vil satse på LSO fordi de trenger dette for å møte kundenes forventning til leveringstider på tjenestene, samtidig som automatisering er nødvendig for å redusere kostnader.

LSO bruker andre begreper enn BSS/OSS og Tjenesteorkestrering (MANO), men det er likevel mulig å se hvordan LSO passer sammen med rammeverket fra Figur 3.3. En slik modell er vist i Figur 3.4. LSO-grensesnittene CANTATA og SONATA brukes til å utføre operasjoner som omhandler *kommersielle og administrative* forhold, henholdsvis mellom en operatør og en kunde og mellom to operatører. Informasjon som utveksles her kan være adressene til endepunktene A og B, forhandling av pris på tjenesten og maksimal overføringskapasitet på tjenesten. En kunde har et forhold til Operatør A og bestiller tjeneste av denne gjennom grensesnittet CANTATA. Operatør A kan ikke levere tjenesten på egen hånd og bruker her LSO-grensesnittet SONATA til å bestille forbindelse via Operatør B.

LSO-grensesnittene ALLEGRO og INTERLUDE brukes til å utføre operasjoner som omhandler tekniske forhold henholdsvis mellom en operatør og en kunde og mellom to operatører. Når en tjeneste er avtalt levert kan en kunde bruke grensesnittet ALLEGRO til å utføre justeringer på tjenesten innenfor avtalen og til å kontrollere og overvåke tjenesten som er levert. Tilsvarende funksjonalitet mellom Operatør A og Operatør B går over INTERLUDE-grensesnittet.

I tillegg til de nevnte eksterne grensesnittene, spesifiserer LSO også grensesnitt internt hos en operatør. I Figur 3.4 vises grensesnittet LEGATO mellom BSS/OSS og MANO, i tillegg definerer LSO grensesnitt for management av Element Managere og nettelementer.



Figur 3.4 MEF LSO referansearkitektur.

Grensesnittene i LSO er ikke ferdig spesifisert, men standardiseringsarbeidet ser ut til å ha god fremgang. SONATA-grensesnittet for bestilling av Ethernet-forbindelser mellom operatører er spesifisert og operatørene AT&T og Colt har tatt i bruk SONATA, slik at når AT&Ts kunder bestiller forbindelser som termineres hos Colt, vil disse forbindelsene kunne etableres automatisk [21].

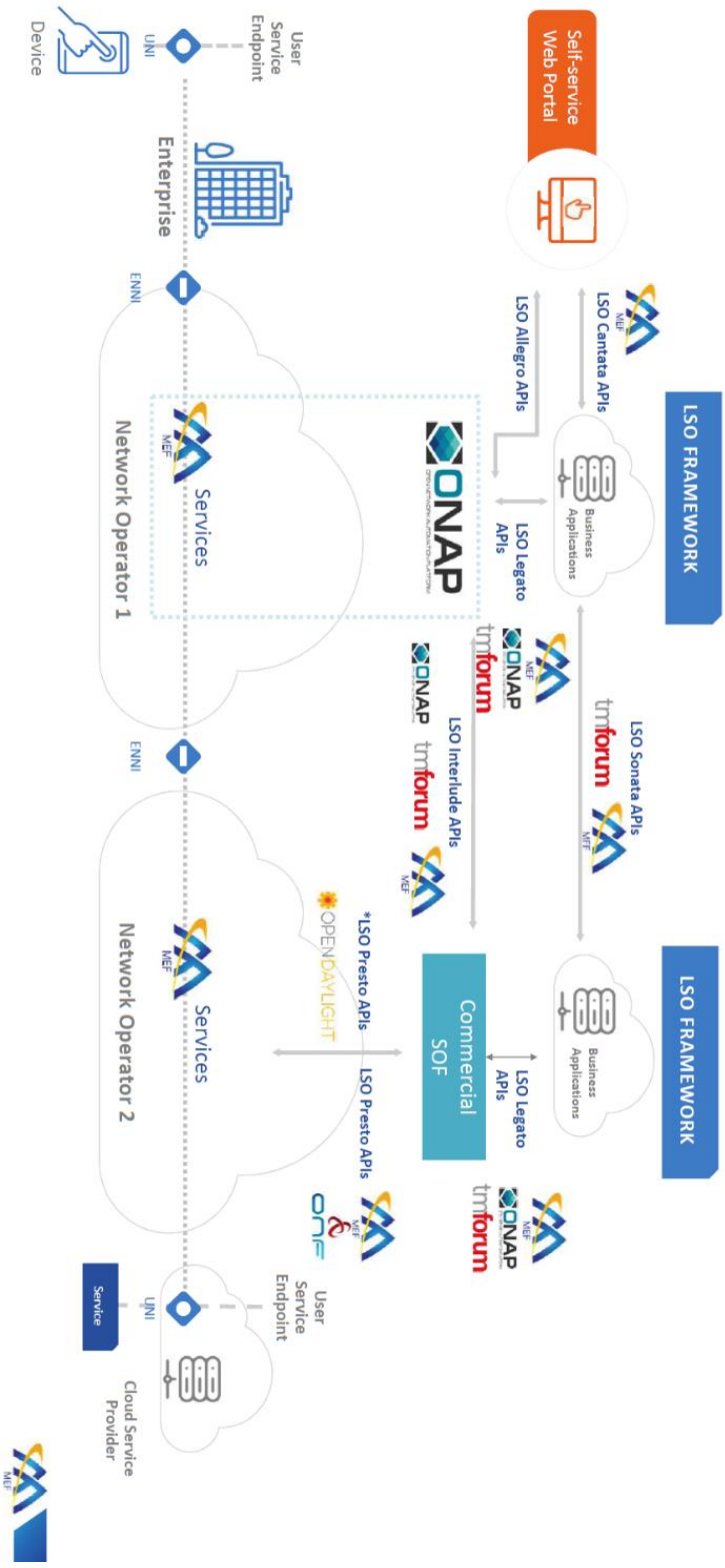
LSO baserer seg på eksisterende standarder der dette finnes. For eksempel gjenbruker LEGATO og SONATA spesifikasjoner fra TMForums Open APIs. APIene er offentlig tilgjengelige på GitHub[3]. MEF samarbeider med ONAP-prosjektet om flere av de nevnte APIene. En oversikt over MEF LSO-arkitekturen og partnere som er involvert i utvikling av standardene, er vist i Figur 3.5.

3.3.3 Interoperabilitet for NFV

I tillegg til å etablere forbindelser mellom ulike operatører, kan det også være interessant å ha mulighet til å flytte VNFer mellom nett. At en operatør kan kjøre sine VNFer hos en annen operatør er et av use-casene ETSI har definert for NFV, dette use-caset heter *Network Functions Virtualisation Infrastructure as a Service* (NFVIaaS) [22]. Et mulig slikt tilfelle ville være om en kunde som har skreddersydde tjenester i 5G-nettet i et land, flyttet seg til et annet land og ved hjelp av NFVIaaS kan få samme tjeneste levert der – uten økt forsinkelse.

Det arbeides med en ETSI-standard for NFVIaaS [23], men det ser ut som det er langt fram til at NFVIaaS eventuelt skal bli tilgjengelig kommersielt.

[3] https://github.com/MEF-GIT/

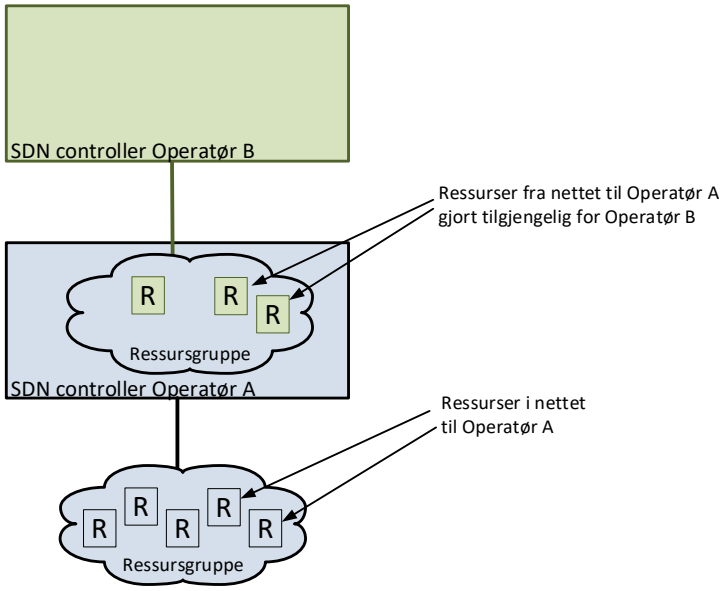


Figur 3.5 Oversikt over grensesnitt og samarbeidspartnere i MEF LSO, fra [24].

3.3.4 Integrasjon mellom SDN controllere

SDN-arkitekturen, slik den er definert av Open Networking Foundation i [25], legger opp til et hierarki der en SDN controller kan eksponere nettverksressurser til en annen SDN controller. Ressursene som eksponeres, kan være et utvalg av ressursene i det underliggende nettet. Et eksempel på dette kan være at én enkelt bølgelengde i en fiber avgis som ressurs til den andre SDN controlleren, mens resten beholdes til eget bruk. En illustrasjon på dette er vist i Figur 3.6. Her har SDN controller i Operatør A eksponert noen ressurser, R, fra sin tildelte ressursgruppe nederst, videre oppover til SDN controller hos operatør B.

Denne arkitekturen gjør det mulig for en operatør å bruke og drive management av ressurser i en annen operatørs nettverk på samme måte som i sitt eget nett. Det ser imidlertid ut til å være et stykke fram til at denne arkitekturen vil kunne bli tilgjengelig for bruk mellom operatører.



Figur 3.6 Interoperabilitet mellom SDN controllere, tilpasset fra Figure 1 *i [25].*

3.4 Vurdering av standarder og rammeverk for management

I sivil sektor foregår det for tiden en omfattende utvikling innen management av kommunikasjonsinfrastrukturer. Utviklingen er drevet av nye teknologier som NFV og SDN, mens det spesielt er innføringen av 5G, samt krav til kostnadseffektivisering, som driver opp farten.

En sentral komponent i fremtidig management er MANO. MANO vil ha høy grad av standardisering gjennom grensesnitt fra ETSI og MEF LSO. Bruk av disse grensesnittene vil muliggjøre automatisering av management.

For at nettelementer – det være seg fysiske eller virtuelle – skal kunne integreres med MANO, må de ha grensesnitt som gjør at hele oppførselen til nettelementene kan modelleres. Det ser ut som det er YANG som er modelleringsspråket som vil bli brukt på nettelementer.

BSS/OSS vil bestå og vil fortsatt være et uoversiktlig landskap. Det er ikke helhetlige krav til hva løsningene skal gjøre og hvordan de skal virke sammen. Innen BSS/OSS virker det som om det fortsatt vil være nødvendig å gjøre integrasjonsarbeid for å få til samvirke mellom komponenter.

Tradisjonelt har det vært manuelle trinn involvert i prosesser relatert til management av forbindelser som leveres på tvers av leverandører. MEF LSO er et lovende rammeverk for integrasjon av BSS/OSS mellom ulike operatørers nettverk.

4 Teknologikomponenter

I kapittel 3 ble ulike typer managementsystemer gjennomgått. Dersom ambisjonsnivået for management er forholdsvis høyt, slik vi forutsetter i denne rapporten, vil det være mange systemer som til sammen utgjør BSS/OSS-løsningen i et kommunikasjonsnettverk og disse systemene trenger å utveksle relativt mye informasjon seg imellom. Dette kapittelet inneholder en overordnet gjennomgang av teknologikomponenter som er relevante for å få til en effektiv informasjonsutveksling internt i BSS/OSS-løsningene samt mellom BSS/OSS og Nettelementene (NE). Disse temaene danner bakgrunnen for løsningene som presenteres i kapittel 5.

Kapittel 4.1 inneholder en diskusjon omkring valg av arkitektur for utveksling av meldinger mellom ulike BSS/OSS-systemer og NE. Kapittel 4.2 inneholder en diskusjon om hvordan ulike systemer kan kommunisere mot meldingsutvekslingsarkitekturen. I kapittel 4.3 diskuteres det hvordan tillitshåndtering kan gjøres, mens i kapittel 4.4 diskuteres problemer med og løsninger for utveksling av informasjon mellom ulike graderingsnivåer.

4.1 Meldingsutvekslingsarkitektur

Som diskutert i kapittel 3.1, vil det være forholdsvis mange systemer involvert i management av en kommunikasjonsinfrastruktur. Der hvor mange komponenter skal kommunisere etter et mønster som vil forandres over tid er det ønskelig å kunne benytte en kommunikasjonsinfrastruktur med disse egenskapene:

- Alle skal kunne sende meldinger til alle andre.
- Én melding skal kunne sendes til mange mottakere.
- Meldinger skal leveres mottaker asynkront gjennom en *push-operasjon*.
- Meldinger skal kunne gis indirekte adresser, f.eks. i form av en emneknagg.
- Meldinger som ikke kan leveres straks skal kunne mellomlagres i en kort periode.

Det er altså ønskelig med en asynkron logisk sentralisert meldingsutvekslingsinfrastruktur for managementtrafikk. I denne rapporten bruker vi begrepet «buss» til å beskrive en slik infrastruktur. Slike busser inngår gjerne som sentral kommunikasjonsvei i store distribuerte systemer. Bussen tillater at komponenter kan abonnere på informasjon som blir sendt fra andre prosesser som benytter den samme bussen.

Merk at det finnes ulike typer busser. For noen år siden var Enterprise service bus (ESB) [26] en populær arkitektur og i [9] anbefales det å benytte en ESB. I de senere år ser det ut til at industrien har gått bort i fra ESB og bruker nå ofte løsninger som er mindre omfattende, slik som *microservices architecture* som IBM beskriver i [27]. MANO-verktøyene ONAP og OSM, som ble introdusert i kapittel 3.2, bruker begge en type bussløsning til kommunikasjon mellom de

ulike komponentene verktøyene er bygget opp av. ONAP bruker en såkalt *microservices bus* [28], mens OSM bruker programvaren Apache Kafka [29]. Denne rapporten anbefaler ikke spesifikke produkter ut over at det anbefales at det velges en buss som innehar de fem egenskapene nevnt i punktlista ovenfor.

Bruk av en buss vil for eksempel muliggjøre at varsler fra én enkelt sensor kan mottas av både et konsoll for nettverksovervåking, en prosess som samler trafikkstatistikk fra mange sensorer, og en prosess som kartlegger cyberangrep. Prosessen som kartlegger cyberangrep kan igjen sende sine bidrag gjennom bussen til en prosess som presenterer et *Recognized Cyber Picture (RCyP)*. Slik kan bussen være en bærer av informasjon ikke bare fra primærkilder, men mellom alle ledd i verdikjeden.

Prinsippet med asynkron overføring av informasjon (push-operasjon) er viktig i systemer som håndterer hendelser, dvs. endringer i systemets tilstand som ikke direkte skyldes brukerbetjening. Buss-komponenter med synkron informasjonsoverføring er ikke nyttig for bruk i management.

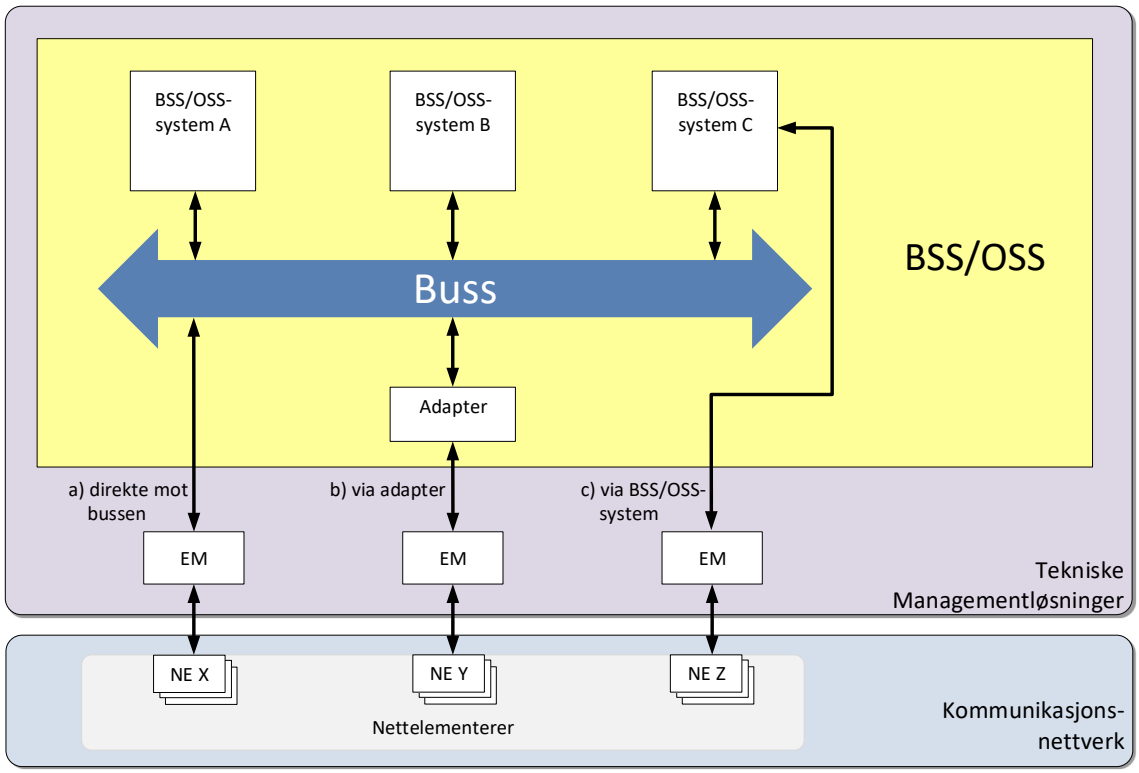
En buss er i prinsippet en enkel konstruksjon som ikke krever mye ressurser. I praksis ser vi at industriprodukter av denne typen inkluderer funksjonalitet for transaksjonssemantikk, lastfordeling, krasjhåndtering, tillitshåndtering, med mer. Disse funksjonene er ikke en del av den prinsipielle bussen og bidrar til en omfattende programvareinstallasjon.

4.2 Adaptere mot kommunikasjonsinfrastruktur

Teknologikomponentene som inngår i et system for management vil i noen grad benytte ulik representasjon for den informasjonen som utveksles. Det vil derfor være en stor fordel å benytte standardiserte formater og protokoller. Som nevnt i kapittel 3.1 er OpenAPI-standardene fra TMForum de mest aktuelle å benytte.

Noen BSS/OSS-systemer vil støtte OpenAPI-standardene, og for disse vil det være forholdsvis enkelt å koble de til bussen. Det vil sannsynligvis også finnes BSS/OSS-systemer som ikke kan benytte standardiserte grensesnitt, og det eksisterer derfor et konverteringsbehov når disse systemene skal utveksle informasjon gjennom bussen.

Figur 4.1 viser tre alternativer for integrering av Nettelementer (NE) mot bussen. I figuren er alle NE koblet til en Element Manger (EM), mens i noen tilfeller vil det ikke finnes en EM og nettelementene vil kommunisere direkte med BSS/OSS-systemene. Alternativ a) er en direkte integrering mot bussen. I alternativ b) er det etablert en adapter mellom EM. I alternativ c) går kommunikasjonen mellom EM og ett enkelt BSS/OSS-system. Alternativ c) er ikke ønskelig da dette gjør det vanskelig å etablere kommunikasjon mellom EM og andre BSS/OSS-systemer enn C.



Figur 4.1 Integrasjon mellom nettelementer og BSS/OSS med en felles buss.

Det kan tenkes at det også vil være behov for å etablere adaptere mellom enkelte BSS/OSS-systemer og bussen. Dette er ikke vist i Figur 4.1. Adapteren tilpasser EMers eller BSS/OSS-systemers kommunikasjon til bussens grensesnittregler. Et adapter kan ha ulike tilnærminger til denne oppgaven som:

- Tilpasning til en felles syntaks, for eksempel JSON [30].
- Skape tunneler, hvor informasjonen pakkes inn i et annet objekt som sendes gjennom kommunikasjonsnettverket og blir pakket ut ved mottakeren. En slik konstruksjon kan brukes der det er viktig å beholde komponentenes egen innholdsrepresentasjon helt fram til mottakeren.

Den store fordelen med å bruke adaptere for å konvertere til og fra en felles syntaks, er at ellers inkompatible komponenter kan bidra til verdikjeden. Ulempen med å bruke adaptere er at det krever mye ad-hoc programmering som er vanskelig å kvalitetssikre og forvalte. Man må unngå å bygge opp en mengde kritiske komponenter som ingen har oversikt over eller ansvar for.

4.3 Løsning for tillitsstyring

I utgangspunktet gis alle BSS/OSS-systemer som er koblet til en buss ubegrenset adgang til å kommunisere med andre systemer som er koblet til bussen. Dette innebærer å innhente informasjon og påvirke nettelementer og vil gi høyeste mulige fleksibilitet i systemet. Det er imidlertid flere grunner til at dette ikke vil være gunstig:

- Feilbetjening og programvarefeil kan få store konsekvenser.
- Teknologimiljøer kan ønske å ha eksklusiv adgang til å styre «sine» komponenter.
- Koalisjonspartnere kan ha behov for separat systemstyring.
- Et vellykket cyberangrep på bussen vil ha ubegrensede konsekvenser.

Systemdesignet krever en avveining mellom den fleksibiliteten uhindret adgang vil skape, og den nødvendige beskyttelsen som er en forutsetning for et stabilt system. Tillitsstyring kan håndheve denne avveiningen gjennom et delsystem som registrerer systemer og deres tillatelser/privilegier, kombinert med tjenester for autentisering av aktørene (binde aktørens identitet til handlinger) og handlingskontroll (misvisende kalt tilgangskontroll/access control), hvor en handling skal gjennomføres eller avvises basert på aktørens tillatelser. Loggføring av gjennomførte handlinger sikrer at det kan føres kontroll med hvilket system som har utført hvilke handlinger.

I et såkalt løst koplet system, hvor enkeltkomponentene kommuniserer gjennom et åpent medium som også andre kan benytte, vil det være nødvendig med autentiseringmekanismer mange steder. En komponent som tilbyr tjenester som kan redusere systemets integritet, må beskyttes med autentisering og handlingskontroll, også når den betjener andre komponenter. Selve kommunikasjonsmediet krever også lignende beskyttelse, særlig når det tar form av et buss-system som beskrevet i kapittel 4.1.

Tillatelser i et buss-system kan regulere ulike type handlinger:

1. Tillatelse til å kople seg til bussen for å sende og motta informasjon.
2. Tillatelse til å publisere eller abonnere på bestemte meldinger/meldingstyper.
3. Tillatelse til å motta bestemte meldinger/meldingstyper.

Disse alternativene representerer en suksessivt økende granularitet, men også økende kostnader knyttet til administrasjon og kontroll av tillatelser. Disse tillatelsene og tilhørende kontroller er vanskelig å håndtere i et system som spenner over flere myndighetsdomener, dvs. områder som ønsker å administrere aktørtillatelser for sitt eget område av nettverket. For å unngå å registrere aktører i mange sideordnede domener for dette formålet, må det opereres med et føderert system for tillitshåndtering.

Handlingskontroll på tvers av myndighetsdomener, dvs. utstedt i ett domene og kontrollert i et annet, krever en såkalt kryssdomenetillit, som representeres av egne tillatelser. Slike mekanismer er teknisk beskrevet og vel forstått, men finnes i liten grad i kommersielle systemer [31].

Som nevnt opererer Forsvarets nettverk med ulike graderingsnivåer, og sammenkoplingen mellom ulike graderingsnivåer er gjenstand for sterk regulering og krav til godkjenning. Det er ikke realistisk å anta at samme buss kan besørge kommunikasjon mellom ulike sikkerhetsnivåer, fordi separasjonen mellom disse ikke vil være tilstrekkelig ivaretatt. Det blir derfor nødvendig å operere med flere busser i et system for management; både av hensyn til separasjon, og trolig også fordi et føderert system for tillitsstyring ikke vil være mulig å realisere.

4.4 Informasjonsutveksling mellom ulike graderingsnivå

En utfordring med å ha flere graderingsnivåer er at det er komplisert å etablere systemer for informasjonsflyt mellom graderingsnivåene. En oversikt over løsninger og muligheter finnes i [32]. Det legges i denne rapporten til grunn at det er mulig å etablere en løsning som lar informasjon flyte fra lavere gradering til høyere gradering gjennom en såkalt *diode*. Gjennom å bruke en buss til meldingsutveksling, kan dioden abonnere på de meldingene som ønskes mottatt av BSS/OSS på høyeste graderingsnivå. Alternativt kan det abonneres på alle meldinger på bussen slik at all informasjon blir tilgjengelig på høyere graderingsnivå.

Det finnes systemer for sikker informasjonsutveksling fra systemer på et høyere graderingsnivå til et lavere graderingsnivå, men disse bygger på en rekke forutsetninger og antakelser som ikke alltid vil være til stede. Det legges derfor til grunn at informasjon ikke kan flyte automatisk fra høyere graderingsnivå til et lavere graderingsnivå.

Busser knyttet til ulike sikkerhetsnivåer vil kunne koples sammen med allerede godkjente mekanismer for dette, da kan det sendes data fra lavt til høyt sikkerhetsnivå, men ikke omvendt.

5 Helhetlig managementløsning for Forsvaret

I dette kapittelet foreslås en helhetlig løsning for management av kommunikasjonsnettverk for Forsvaret basert på foregående kapitler.

I en tidligere utgitt rapport [8] er det utarbeidet en taksonomi som er ment å beskrive de ulike aspektene av management som er viktigst for de ulike kommunikasjonsnettene Forsvaret benytter seg av. Taksonomien baserer seg på sivilt utviklede rammeverk (ISOs *FCAPS* og *ITIL*) og NATOs *C3 Classification Taxonomy*. Taksonomien inneholder følgende aspekter for management:

- *Monitorering og rapportering* er managementløsninger som løpende mottar informasjon om status for nettverket. Disse systemene er tiltenkt driftspersonell og gir informasjon de trenger for å kunne sørge for at nettverket fungerer som det skal. Monitorering og rapportering omfatter begreper som ytelsesovervåking, overvåking av feil og alarmer, samt informasjon om trender, for eksempel trafikkbelastning, som brukes til langsiktig planlegging av nettverksutbygging. Ulike brukere med ulike oppgaver vil her bruke ulike «views», det vil si de får ulik fremstilling av informasjonen. Tradisjonelt har OSS-systemer for monitorering og rapportering benyttet polling over SNMP-protokollen [33]. Nye teknologier som *streaming telemetry* [34, 35] benytter i stedet asynkrone meldinger over en bussarkitektur som beskrevet i kapittel 4.

- *Konfigurasjonsstyring* er managementløsninger som inneholder konfigurasjonen til nettelementene eller nettverkstjenestene i en konfigurasjonsdatabase. Med en løsning for konfigurasjonsstyring skal man kunne konfigurere en tjeneste fra ett sted, ikke gjennom flere EMer. Et viktig prinsipp for konfigurasjonsstyring er å bestemme om den riktige konfigurasjonen for nettelementene ligger i nettelementene eller i management-systemet. Clemm, i «Network Management Fundamentals» [2], skriver at førstnevnte er vanlig i større bedrifter (enterprises) mens sistnevnte er brukt hos større nettverksoperatører. For NFV og SDN er det managementsystemene som har «fasiten» i form av riktig konfigurasjon. Med et forholdsvis høyt ambisjonsnivå vil det være riktig å strekke seg mot at det er managementsystemet som har den riktige konfigurasjonen og ved avvik må konfigurasjon i nettelementene overskrives.

- *Situasjonsbilde* er en fremstilling av relevant informasjon for ulike grupper som har behov for informasjon om tilstand i nettverket. En slik gruppe er brukerne av nettverkets tjenester som ønsker å vite hvilke tjenester som er tilgjengelige mot hvilke brukere. Slike systemer er nyttige for Forsvarets operative enheter. En type situasjonsbilde er Recognized Cyber Picture (RCyP).

- *Prioriteringsmekanismer* er mekanismer som gir mulighet for, dynamisk og på kort sikt, å tilpasse hvordan ulike typer trafikk og trafikk fra ulike brukere prioriteres i nettverket.

Behovet for slike mekanismer kommer fra forventede endringer i operasjonsmønstre og trusler mot kommunikasjonsinfrastrukturen.

- *Konsekvensanalyse*[4] består av systemer som gir oversikt over hvilke konsekvenser ulike hendelser har på nettet. Dette er løsninger for planlegging på kort og lang sikt. På kort sikt dreier konsekvensanalyse seg om å forstå hvordan feilhendelser og planlagte endringer på nettelementer vil påvirke tjenestene som går i nettet. Management innebærer da å ha kontroll på hvordan endringer gjennomføres slik at disse ikke får negative konsekvenser for tjenestene. På lang sikt bidrar konsekvensanalyse til forståelse for hvordan kommunikasjonsinfrastrukturen bør utvikles.

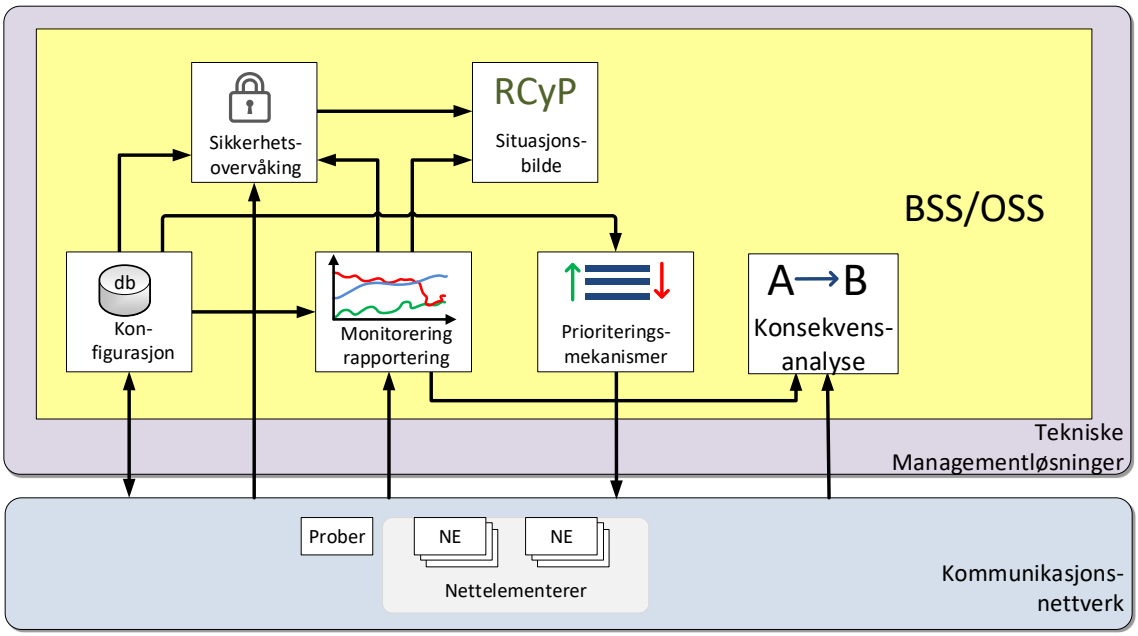
- *Sikkerhetsstyring* har som mål å kontrollere tilgangen til ressursene i nettverket for å sikre de mot villede og utilsiktede handlinger. Sikkerhetsstyring er et aspekt som inngår i alle de andre aspektene av management. Som et eksempel må konfigurasjon bidra til å gjøre nettverket sikkert mot inntrengingsforsøk, mens monitorering og rapportering bør gi et bilde av sikkerhetsstatus i nettet. I dag finnes det som regel egne systemer for *sikkerhetsovervåking* (Security Information and Event Management – SIEM) og vi viderefører dette begrepet i den videre diskusjonen.

Med utgangspunkt i disse hovedaspektene skisseres det i resten av kapittelet hvor managementsystemer som understøtter disse aspektene bør implementeres og hvordan managementsystemene er relatert til hverandre. De ulike aspektene over vil ikke nødvendigvis kunne kobles mot programvareløsninger i et én-til-én-forhold. Enkelte programvareløsninger kan omfatte mer enn ett aspekt, og enkelte aspekter kan kreve flere programvareløsninger.

Figur 5.1 viser BSS/OSS-systemer som representerer de ulike aspektene innen management og deres koblinger mot kommunikasjonsinfrastrukturen. Figuren viser også mulige relasjoner mellom de ulike BSS/OSS-systemene. For eksempel antas det at situasjonsbilde er avhengig av informasjon fra sikkerhetsovervåking og monitorering og rapportering. Det antas her en forholdsvis høy grad av integrasjon mellom de ulike systemene. For eksempel er det her antatt at system for konfigurasjonsstyring vil sende informasjon om hva som skal monitoreres og rapporteres. Alternativt kan slik informasjon legges inn manuelt direkte i system for monitorering og rapportering. Med en viss grad av integrering mellom de ulike systemene i BSS/OSS, vil det likevel bli et substansielt antall grensesnitt mellom systemer.

Det kan være en fordel å benytte en arkitektur som gir en smidig integrering mellom systemene, for eksempel med en meldingsutvekslingsarkitektur som beskrevet i kapittel 4.1 og her kalt buss. Det må også vurderes om det er hensiktsmessig å etablere adaptere mot kommunikasjonsinfrastrukturen slik at disse også er koblet direkte til bussen, som diskutert i kapittel 4.2. I resten av dette kapittelet baseres diskusjonen på integrering via en slik bussarkitektur.

[4] I denne rapporten brukes uttrykket konsekvensanalyse der begrepet påvirkningsstyring ble brukt i [8].



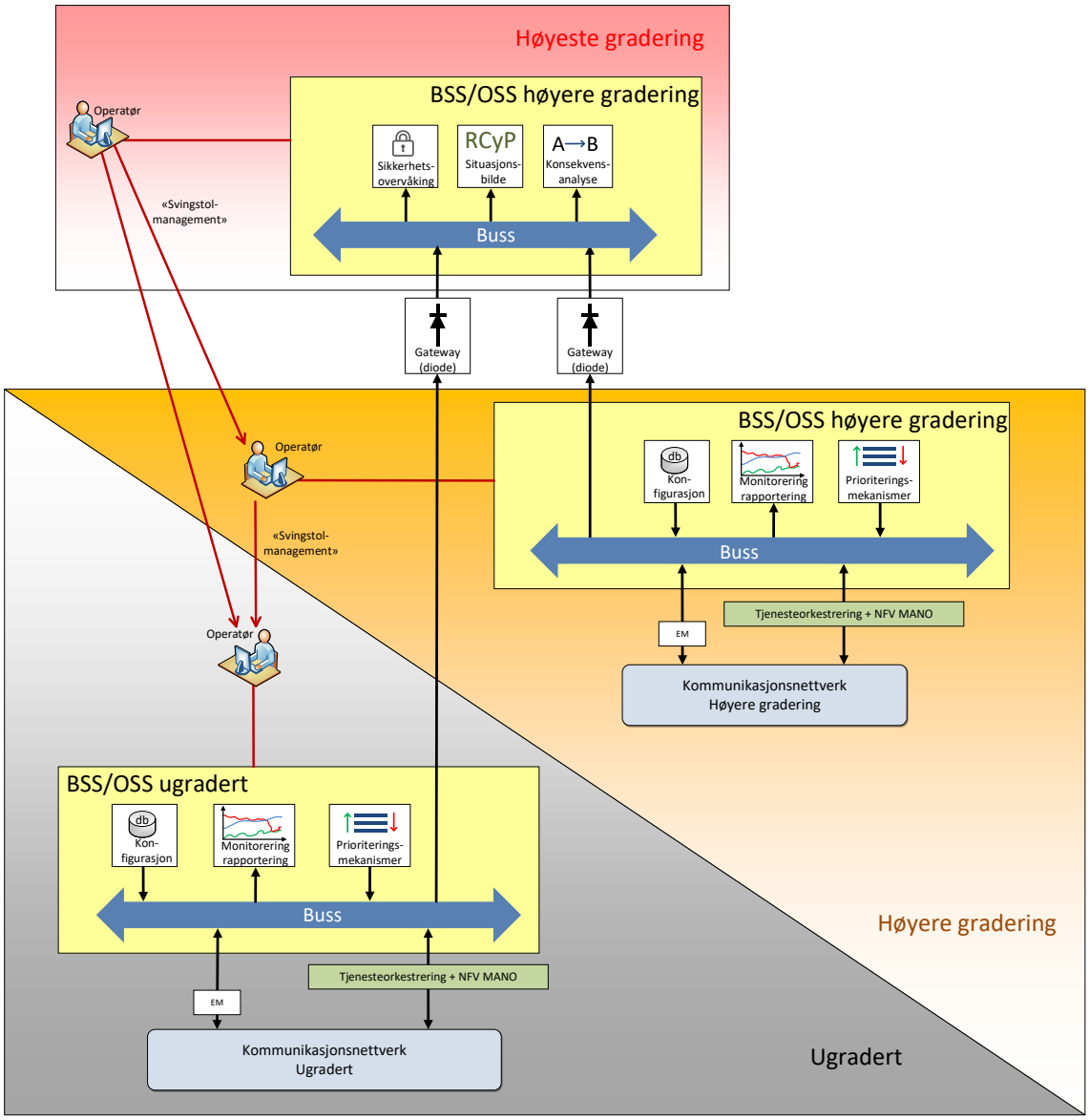
Figur 5.1 Aspekter innen management og eksempel på relasjon mellom disse.

5.1 Ulike graderingsnivåer i stasjonære nettverk

En av utfordringene med kommunikasjonsnettverk i Forsvaret er at de befinner seg på ulike graderingsnivåer. Figur 5.2 viser et tilfelle der det finnes kommunikasjonsnettverk på to ulike graderingsnivåer, et ugradert nettverk og et nettverk med høyere gradering. Hvert av disse nettverkene har et eget BSS/OSS slik som skissert i kapittel 3.2. Det er etablert en buss for intern kommunikasjon mellom de ulike managementsystemene innen hvert av de to graderingsnivåene slik som diskutert i kapittel 4.

Som diskutert i kapittel 4.4, antar vi at det er mulig å bruke en diodeløsning til å overføre informasjon fra lavere graderingsnivå til høyere graderingsnivå, men ikke motsatt vei. Som indikert i Figur 5.2 er eneste måte å overføre informasjon fra systemer på høyere graderingsnivå til systemer på lavere graderingsnivå å manuelt legge inn informasjon via det som uformelt her kalles «svingstolmanagement».

En konsekvens av at det finnes ulike graderingsnivåer er at BSS/OSS-systemer, som behandler informasjon om tilstand i hele nettet, må befinne seg på det høyeste graderingsnivået. I Figur 5.2 gjelder dette analysekomponentene for sikkerhetsovervåking, situasjonsbilde og konsekvensanalyse. Disse systemene må motta informasjon relatert til management fra lavere graderingsnivå via diodeløsninger. Disse systemene vil normalt ikke ha behov for å sende informasjon til nettelementer, og disse systemene vil derfor være mulig å realisere i et miljø med flere graderingsnivåer under antakelsen om en-veis informasjonsflyt, gitt at de befinner seg på høyeste graderingsnivå.



Figur 5.2 Helhetlig løsning for managementløsninger for stasjonær kommunikasjonsinfrastruktur.

Systemer for konfigurasjonsstyring og prioriteringsmekanismer har behov for å konfigurere elementer i nettet. Samtidig bør disse managementsystemene ha informasjon fra nettelementene for å kunne bestemme henholdsvis riktig konfigurasjon og prioritet. På grunn av denne toveis-kommunikasjonen må systemer for konfigurasjonsstyring og prioriteringsmekanismer befinne seg på samme graderingsnivå som nettelementene de utfører management av. Konsekvensen av dette blir at det må etableres slike managementløsninger for hvert graderingsnivå i kommunikasjonsinfrastrukturen.

Systemer for monitorering og rapportering er først og fremst løsninger som benyttes til å drifte nettverket og som benyttes av driftspersonell som står for den løpende driften av nettverket. Disse systemene kan i utgangspunktet befinne seg på høyeste graderingsnivå og få full oversikt over nettverket. Likevel kan det være hensiktsmessig å beholde denne funksjonaliteten på det laveste graderingsnivået. Det må gjøres en avveining av hvor viktig det er å holde informasjon fra begge graderingsnivåene samlet i ett system. Hvis nettverkene er uavhengige, er det ikke nødvendigvis behov for å samle all informasjon på høyeste nivå. I forbindelse med automatisering med *closed feedback loops* er det nødvendig at informasjon holder seg på det laveste nivået for at system for konfigurasjonsstyring skal kunne styre den ugraderte infrastrukturen på bakgrunn av informasjon fra system for monitorering og rapportering.

I eksempelet fra Figur 5.2, er det kun to graderingsnivåer. Forsvaret har vesentlig flere nettverk med ulike graderingsnivåer. Det kreves omfattende arbeid å etablere og vedlikeholde et slikt oppsett med egne BSS/OSS for hvert nivå. Det er en viktig avveining hvor høye ambisjonene skal være innen de ulike nettverkene Forsvaret opererer.

5.2 Integrasjon mellom ulike stasjonære nettverk

Som diskutert i kapittel 2.4, vil Forsvaret i fremtiden benytte kommersielle operatørers kommunikasjonsnettverk til å levere tjenester. På samme måte som ved benyttelse av eget kommunikasjonsnettverk vil det stilles krav til management av disse delene av den sammensatte infrastrukturen. Uten integrasjon av managementløsningene mellom Forsvaret og de kommersielle operatørene kan man ikke automatisk ha kontroll på den delen av en tjeneste som er produsert i kommersiell operatørs nettverk. I første omgang ser det ut som disse aspektene av management vil kunne forbedres gjennom å integrere Forsvarets og operatørenes managementløsninger som beskrevet nedenfor.

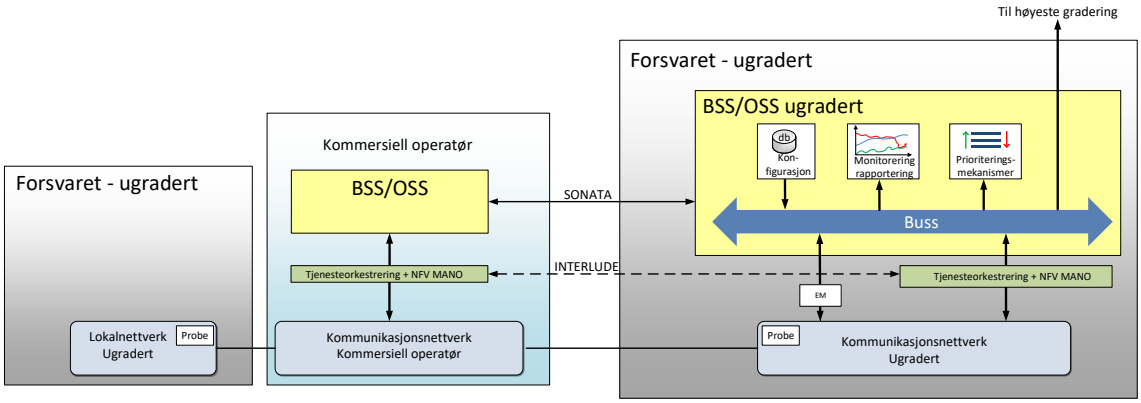
- Integrert funksjonalitet for monitorering og rapportering samt situasjonsbilde vil gjøre det mulig å lokalisere problemer hurtig så man kan agere deretter.

- Innen konfigurasjonsstyring vil det bli mulig å gjøre endringer raskt, for eksempel å øke kapasitet på en eksisterende forbindelse eller å få etablert kapasitet til nye lokasjoner. Hvis nettverket er koblet sammen med flere kommersielle operatører, kan man flytte tjeneste fra en kommersiell operatør som har problemer i sitt nettverk over til en annen operatør som ikke har problemer.

- Innen prioriteringsmekanismer vil det bli mulig å endre prioriteringsregler for trafikk ikke bare i eget nett, men også i eksterne nettverk. Dette vil gi mulighet for bedre å tilpasse konfigurasjonen til endringer i trafikkmønstre.

Når det gjelder konsekvensanalyse og sikkerhetsstyring, virker dette å være noe mer komplisert å realisere da det kreves detaljert innsikt i kommersiell operatørs nettverk.

Som nevnt i kapittel 3.3, forventer vi at MEFs rammeverk LSO vil kunne benyttes til å etablere, overvåke og kontrollere forbindelser gjennom flere operatørers nett. Vi mener det er ønskelig at norske nettverksoperatører utvikler støtte for LSO og tilbyr dette til Forsvaret. Videre er det viktig at Forsvaret følger opp og implementerer støtte for LSO i sine systemer. Integrasjon kan da foregå som vist i Figur 5.3.



Figur 5.3 Integrasjon mellom Forsvarets stasjonære ugraderte nett og nettverk fra kommersiell operatør som muliggjør automatisk etablering av nettverksforbindelser.

I første omgang er det LSOs SONATA-grensesnitt som blir tilgjengelig, og dette grensesnittet vil støtte konfigurasjonsstyring og muligens også prioriteringsmekanismer. På sikt kan det være ønskelig å benytte LSOs INTERLUDE-grensesnitt mellom MANO hos Forsvaret og MANO hos kommersielle operatører for å realisere monitorering og rapportering inn mot Forsvarets MANO.

Bildet kan endre seg litt, avhengig av i hvor stor grad tjenester settes ut til strategiske samarbeidspartnere. En aktuell løsning kan være at Forsvaret setter ut NFV til eksterne leverandører. Som nevnt i kapittel 3.3, finnes det per i dag ikke grensesnitt eller APIer som lar Forsvaret styre oppførsel til VNFer hos andre leverandører. Drift av slike funksjoner må dermed, slik det ser ut nå, gjøres av de eksterne leverandørene.

Et mulig spesialtilfelle av integrasjonen i Figur 5.3 er at hele den ugraderte infrastrukturen til Forsvaret er satt ut til en ekstern leverandør. I dette tilfellet har ikke Forsvaret et ugradert nettverk, men har likevel behov for BSS/OSS på ugradert nivå.

5.3 Integrasjon av deployerbare og mobile nettverk

For å levere kommunikasjonstjenester til militære operasjoner benytter Forsvaret både deployerbare og mobile nettverk. Som tidligere nevnt gir disse typene nettverk enkelte utfordringer for management sammenlignet med stasjonære nettverk. Deployerbare nettverk og mobile nettverk diskuteres i henholdsvis kapittel 5.3.1 og 5.3.2.

5.3.1 Deployerbare nettverk

Deployerbare kommunikasjonsnettverk ligner på stasjonære kommunikasjonsnettverk i den tiden de er aktive. Det antas at det for de deployerbare nettverkene er ønskelig med sammenkobling med stasjonær BSS/OSS for stasjonær del av infrastrukturen. Det synes å være to alternative måter å knytte sammen management av deployerbare nettverk med management av stasjonær kommunikasjonsinfrastruktur.

Det første alternativet innebærer at det ikke etableres egne BSS/OSS i deployerbare nettverk, men at nettelementene i deployerbare nettverk kobler seg opp mot BSS/OSS i stasjonær infrastruktur. Dette alternativet kaller vi en sentralisert løsning. For at dette skal fungere tilfredsstillende er det en forutsetning at BSS/OSS-systemene håndterer at nettelementene tidvis er koblet ut av nettet uten at dette gir alarmer og feilmeldinger i systemene.

Det andre alternativet vil være at det etableres egne BSS/OSS-systemer for de deployerbare nettverkene. Dette blir en desentralisert løsning for BSS/OSS. Med en helt desentralisert løsning vil det ikke være mulig med helhetlig management av infrastrukturen som omfatter både stasjonære og deployerbare nettverk med mindre man tar i bruk løsninger som MEF LSO mellom de ulike BSS/OSS-systemene.

Uavhengig av alternativ, trengs det Element Manager (EM)-systemer i de deployerbare nettverkene som muliggjør at personell i felt kan konfigurere de taktiske nodene for å få de koblet opp mot stasjonær infrastruktur. EM-systemene kan ha forholdsvis enkle grensesnitt som gir mulighet til å velge mellom ulike bærere for tilkobling mot stasjonær infrastruktur. At konfigurasjon endres ute i nettet gjør det noe mer komplisert med sentral lagring av konfigurasjonen. Det burde likevel være mulig å ha en mal for hva som er en gyldig konfigurasjon av nettelementer i deployerbare nettverk og sikre at denne overholdes.

Når det gjelder monitorering og rapportering, må det tas høyde for at nettelementer vil dukke opp og forsvinne igjen. Uten slike hensyn, vil det genereres alarmer da hendelser oppfattes av systemene som feilhendelser. Dette bør være overkommelig å håndtere siden det vil være forhåndsplanlagt når dette skjer, men det kan kreve tilpasning av managementsystemene.

I internasjonale operasjoner vil Forsvaret typisk etablere forbindelser med andre nasjoners nett. I tråd med kravene til Federated Mission Networking (FMN) [36], etableres det et ugradert felles kommunikasjonsnettverk mellom deltakerlandene som baserer seg på konseptet Protected Core Networking (PCN) [37]. PCN er, slik det er spesifisert per i dag [38], beregnet på stasjonære og deployerbare nettverk. Det vil fremover arbeides med en felles løsning for management kalt *Network Management and Cyber Defense* (NMCD). NMCD vil blant annet bidra til et felles situasjonsbilde (RCyP) for PCN-nettverket.

5.3.2 Mobile nettverk

Komponenter i virkelig mobile nettverk som Forsvaret opererer, vil antakelig bare i begrenset grad kunne bruke de samme managementløsningene som for stasjonær infrastruktur i sivil

sektor. I mobile nettverk vil nettelementer være tidvis tilkoblet og tidvis frakoblet uten at disse endringene er planlagt. Det kan være vanskelig å håndtere informasjon fra mobile nettelementer som kommer og går i slike sentraliserte systemer. Blir det for mye «støy» i systemer for monitorering og rapportering og situasjonsbilde (RCyP) blir det vanskelig for driftspersonell å holde oversikt. En mulig konsekvens er at overvåking av nettelementer i mobil infrastruktur blir skrudd av.

Når det gjelder arbeid med FMN i mobilt domene, er dette arbeidet i oppstartfasen. Det vil trolig være behov for andre managementløsninger enn de som utvikles i NMCD for deployerbare nettverk.

De mobile nettene er gjerne ad-hoc nettverk. Det finnes et IETF Internet draft som gir en oversikt over utfordringer og noen muligheter for management i ad-hoc-nettverk [39]. Oppsummert kan vi si at mobil infrastruktur er det vanskeligste området å få management til å fungere godt i, og det finnes lite standarder og rammeverk som vil passe for disse nettverkene.

6 Vurderinger og anbefalinger

På bakgrunn av arbeidet med denne rapporten kan vi gi følgende anbefalinger til Forsvaret[5] for moderne løsninger for management av kommunikasjonsinfrastrukturen.

Vi anbefaler først å vurdere nøye hvilket ambisjonsnivå man skal ha for management i Forsvarets nett. Denne rapporten har basert seg på enkle antakelser om at det er riktig å legge seg på et forholdsvis høyt ambisjonsnivå. Vi anbefaler at Forsvaret gjør en grundig vurdering av operative effekter for ulike ambisjonsnivå for å kunne ta et valg. Videre anbefaler vi at Forsvaret etablerer et målbilde for management ut i fra valgt ambisjonsnivå.

Det anbefales videre å se på behov for integrasjon mellom de ulike managementløsningene som trengs for å oppfylle det valgte ambisjonsnivået. I denne rapporten har vi anbefalt en helhetlig mangementløsning bygget på en asynkron buss.

En del av teknologiene og grensesnittene som diskuteres i denne rapporten er ikke tilgjengelige i kommersielle produkter i dag, men det er stort fokus og mye arbeid på standarder og rammeverk i kommersiell sektor. Vi anbefaler at Forsvaret følger nøye med på utviklingen av MANO og spesielt rammeverkene OSM og ONAP.

For stasjonær og deployerbar infrastruktur anbefales det å følge med på utviklingen av rammeverk for management på tvers av operatører. Ved å benytte slike rammeverk kan Forsvaret i fremtiden få effektivt management av deployerbare nettverk. Det mest lovende av disse rammeverkene er MEF LSO som ser ut til å ha sterk støtte i industrien.

For mobil infrastruktur finnes det ikke noen anbefalte rammeverk eller løsninger å bygge på. Det må vurderes fra tilfelle til tilfelle hva slags funksjonalitet som kan integreres med managementløsningene i den stasjonære infrastrukturen.

Ved materiellanskaffelser anbefales det allerede fra i dag å vurdere nøye hvordan nettelementene kan passe inn i et tenkt målbilde for management. En viktig faktor er at nettelementene lar seg konfigurere fra et sentralt konfigurasjonssystem.

[5] Her sikter vi også til personell i andre etater som har oppgaver knyttet til å utvikle, fremskaffe og velge løsninger for Forsvarets kommunikasjonsinfrastruktur.

Forkortelser

API	Application Programming Interface
BSS	Business Support System
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
EM	Element Manager
ESB	Enterprise Services Bus
ETSI	European Telecommunications Standards Institute
FKI	Forsvarets kommunikasjonsinfrastruktur
FMN	Federated Mission Networking
INI	Forsvarets informasjonsinfrastruktur
IP	Internet Protocol
JSON	JavaScript Object Notation
LSO	Lifecycle Service Orchestration
MANO	Management and Orchestration
NE	Nettelement (Network Element)
NFV	Network Functions Virtualisation
NFVI	Network Functions Virtualisation Infrastructure
NFVIaaS	Network Functions Virtualisation Infrastructure as a Service
NMCD	Network Management and Cyber Defense
NMS	Network Management System
ONAP	Open Network Automation Platform
OSM	Open Source MANO
OSS	Operations Support System
PCN	Protected Core Networking
RCyP	Recognized Cyber Picture
SDN	Software Defined Networking
SIEM	Security Information and Event Management
SNMP	Simple Network Management Protocol
VNF	Virtual Network Function

Referanser

[1] Forsvarsdepartementet, «Kampkraft og bærekraft. Langtidsplan for forsvarssektoren,» *Proposisjon til Stortinget (forslag til stortingsvedtak). Prop. 151 S (2015–2016),* 17 juni 2016.

[2] A. Clemm, Network Management Fundamentals. A guide to understand how network technology really works, Cisco Press, 2007.

[3] S. N. Kvalvik, H. Berg, E. Elman, E. Graarud, O. K. Halvorsen, T. Hanson, B. Lien og K. Waage, «Hvordan skape økonomisk handlingsrom i den nye langtidsplanen?,» FFI-rapport 19/01934, - potensial for forbedring og effektivisering 2021–2024.

[4] Forsvarsdepartementet, «Vilje til beredskap – evne til forsvar. Langtidsplan for forsvarssektoren,» *Proposisjon til Stortinget (forslag til stortingsvedtak), Prop. 62 S (2019 – 2020),* april 2020.

[5] A. Mykkeltveit, «SDN NFV World Congress, Den Haag, oktober 2018,» FFI-reisenotat 18/02322, 2018.

[6] A. Mykkeltveit og P. Kristiansen, «Testing av Protected Core Networking (PCN) på NATOs interoperabilitetsøvelse CWIX 2019,» FFI-rapport 20/01319, 2020.

[7] A. Mykkeltveit, «3rd Open Source MANO hackfest Fornebu 25.-29. juni 2018,» FFI-reisenotat 18/01646, 2018.

[8] P. Kristiansen og O. I. Bentstuen, «Management av Forsvarets kommunikasjonsinfrastruktur. Innspill til videre utvikling,» FFI-rapport 17/01692. BEGRENSET, 2017.

[9] Analysis Mason, «Drift og overvåking av Forsvarets IKT infrastruktur. Rapport for Forsvarsmateriell,» 2018.

[10] «Trender som påvirker Forsvarets kommunikasjonsinfrastruktur,» FFI-fakta, 2019. [Internett]. Available: https://www.ffi.no/publikasjoner/arkiv/trender-som-pavirker-forsvarets-kommunikasjonsinfrastruktur.

[11] Forsvarsmateriell, «Nye kommunikasjonsnoder innført i Forsvaret,» , 16. November 2017. [Internett]. Available: https://forsvaret.no/forsvarsmateriell/presserom/nye-kommunikasjonsnoder-innf%C3%B8rt-i-forsvaret.

[12] ITU-T, «Principles for a telecommunications management network,» ITU-T Recommendation M.3010 (02/2000), 2000.

[13] TMForum, «Open APIs: Turning business strategy into reality,» White Paper, 2016.

[14] TMForum, «Open APIs,» [Internett]. Available: https://www.tmforum.org/open-apis/.

[15] ETSI, «Network Functions Virtualisation (NFV); Management and Orchestration,» ETSI GS NFV-MAN 001 V1.1.1 (2014-12), 2014.

[16] M. Bjorklund, The YANG 1.1 Data Modeling Language, IETF RFC 7950, 2016.

[17] OASIS, Topology and Orchestration Specification for Cloud Applications Version 1.0, OASIS Standard, 2013.

[18] Linux Foundation, «ONAP - Open network automation platform,» [Internett]. Available: https://www.onap.org.

[19] ETSI, «Open Source MANO (OSM),» [Internett]. Available: https://osm.etsi.org/.

[20] MEF, «Lifecycle Service Orchestration (LSO) : Reference Architecture,» Service Operations Specification MEF 55, 2016.

[21] SDX Central, «AT&T, Colt Use MEF's LSO Sonata APIs to Automate Network Ordering,» 24 juni 2019. [Internett]. Available: https://www.sdxcentral.com/articles/news/att-colt-use-mefs-lso-sonata-apis-to-automate-network-ordering/2019/06/.

[22] ETSI, «Network Functions Virtualisation (NFV); Use Cases,» ETSI GR NFV 001 V1.2.1 (2017-05), 2017.

[23] ETSI, «Network Functions Virtualisation (NFV) Release 3; Management and Orchestration; Multiple Administrative Domain Aspect Interfaces Specification,» ETSI GS NFV-IFA 030 V3.3.1 (2019-09), 2019.

[24] P. Menezes, «MEF's Automation Strategy for Digital Transformation,» Materiale fra presentasjon under TM Forums konferanse Digital Transformation North America 2019, september 2019. [Internett]. Available: https://dtaw.tmforum.org/wp-content/uploads/2019/09/Pascal-Menezes-MEF.pdf.

[25] Open Networking Foundation, «SDN Architecture,» Issue 1.1, ONF TR-521, 2016.

[26] K. Lund, T. H. Bloebaum og F. T. Johnsen, «Enterprise Service Bus – definisjon og bruksområder,» FFI-rapport 2013/00441, 203.

[27] K. Clark, T. Curcio og N. Glowacki, «Agile integration architecture - Using lightweight integration runtimes to implement a container-based and microservices-aligned integration architecture,» IBM, 2018. [Internett]. Available: https://www.ibm.com/downloads/cas/J7E0VLDY.

[28] H. Zhao, «ONAP Microservices Bus Tutorial,» The Linux Foundation, 2018. [Internett]. Available: https://www.slideshare.net/HuabingZhao/microservice-bus-tutorial.

[29] Apache, «Kafka - A distributed streaming platform,» [Internett]. Available: https://kafka.apache.org/.

[30] T. Bray, The JavaScript Object Notation (JSON) Data Interchange Format, IETF RFC 8259, 2017.

[31] A. Fongen, «Federated Identity Management in a tactical multi-domain network,» *Int. Journal on Advances in Systems and Measurements*, vol. 4, nr. 3&4, 2011.

[32] N. A. Nordbotten, F. Mancini, B. H. Farsund, R. Haakseth, A. M. Hegland og F. Lillevold, «Information sharing across security domains,» FFI-rapport 2015/00456, 2015.

[33] D. Harrington, R. Presuhn og B. Wijnen, An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks, IETF RFC 3411, 2002.

[34] Cisco, «Streaming Telemetry,» [Internett]. Available: https://developer.cisco.com/docs/ios-xe/#!streaming-telemetry-quick-start-guide/streaming-telemetry.

[35] Ciena, Blue Planet, «What is streaming telemetry?,» [Internett]. Available: https://www.blueplanet.com/blog/What-is-streaming-telemetry.html.

[36] Federated Mission Networking, FMN Spiral Specification Roadmap, https://tide.act.nato.int/fmnroadmap/index.php?title=Editing_Guidelines#Roadmap_Perspectives.

[37] G. Hallingstad og S. Oudkerk, «Protected core networking: an architectural approach to secure and flexible communications,» *IEEE Communications Magazine*, vol. 46 (11), p. 35–41, 2008.

[38] NATO Standardization Office (NSO), AComP-5637 Protected Core Networking (PCN) Edition A Version 1, Ratification Draft 1.

[39] J. Nguyen, R. Cole, U. Herberg og J. Dean, «Network Management of Mobile Ad hoc Networks (MANET): Architecture, Use Cases, and Applicability,» IETF Internet-draft (expired), 2013. [Internett]. Available: https://tools.ietf.org/html/draft-nguyen-manet-management-00.

About FFI

The Norwegian Defence Research Establishment (FFI) was founded 11th of April 1946. It is organised as an administrative agency subordinate to the Ministry of Defence.

FFI's MISSION

FFI is the prime institution responsible for defence related research in Norway. Its principal mission is to carry out research and development to meet the requirements of the Armed Forces. FFI has the role of chief adviser to the political and military leadership. In particular, the institute shall focus on aspects of the development in science and technology that can influence our security policy or defence planning.

FFI's VISION

FFI turns knowledge and ideas into an efficient defence.

FFI's CHARACTERISTICS

Creative, daring, broad-minded and responsible.

Om FFI

Forsvarets forskningsinstitutt ble etablert 11. april 1946. Instituttet er organisert som et forvaltningsorgan med særskilte fullmakter underlagt Forsvarsdepartementet.

FFIs FORMÅL

Forsvarets forskningsinstitutt er Forsvarets sentrale forskningsinstitusjon og har som formål å drive forskning og utvikling for Forsvarets behov. Videre er FFI rådgiver overfor Forsvarets strategiske ledelse. Spesielt skal instituttet følge opp trekk ved vitenskapelig og militærteknisk utvikling som kan påvirke forutsetningene for sikkerhetspolitikken eller forsvarsplanleggingen.

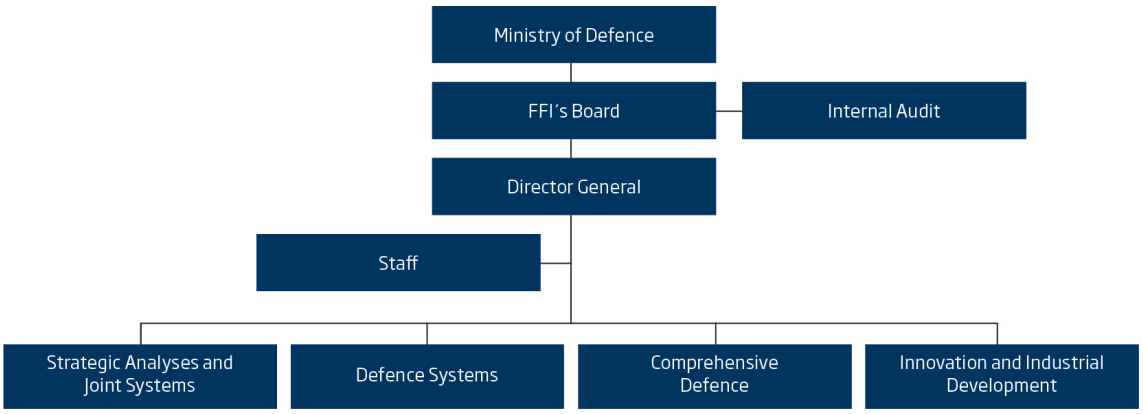
FFIs VISJON

FFI gjør kunnskap og ideer til et effektivt forsvar.

FFIs VERDIER

Skapende, drivende, vidsynt og ansvarlig.

FFI's organisation



Forsvarets forskningsinstitutt
Postboks 25
2027 Kjeller

Besøksadresse:
Instituttveien 20
2007 Kjeller

Telefon: 63 80 70 00
Telefaks: 63 80 71 15
Epost: ffi@ffi.no

Norwegian Defence Research Establishment (FFI)
P.O. Box 25
NO-2027 Kjeller

Office address:
Instituttveien 20
N-2007 Kjeller

Telephone: +47 63 80 70 00
Telefax: +47 63 80 71 15
Email: ffi@ffi.no

FFI Forsvarets forskningsinstitutt
Norwegian Defence Research Establishment