

Jeg tar utgangspunkt i de ikke-funksjonelle kravene fra løsningsforslaget til øving 1. Og mine egne krav fra øving 1.

Måleravlesning er sårbar i den forstand at kommunikasjonen mellom nettselskapet og måler foregår over nettet. Dersom det ikke brukes en kryptert kommunikasjonskanal kan utenforstående personer lytte på kanalen og plukke opp meldinger sendt fra måler til nettselskap. Dette bryter med det ikke-funksjonelle kravet **personvern**. Dersom kommunikasjonen ikke er sikret på noen måte (f.eks gjennom passordbeskyttelse og kryptering) kan både privatpersonene som har strømmåleren hjemme kunne manipulere dataen sendt til strømselskapet for å sette strømforbruk mindre enn det er faktisk er, eller utenforstående kan sette den høyere/nekte at forbruk sendes. Dette bryter med det ikke-funksjonelle kravet **integrity**. Jeg ser ikke helt hvorfor utenforstående kan ha nytte av dette annet enn for gøy eller blackmail (nekter strømmåleren å sende data til penger er betalt f.eks), men motivet til privatpersonene er jo selvsagt lavere strømmregning.

Måledatabasen og kundedatabasen hos nettselskapet har fra øving 1 et krav om **pålitelighet**. Dette kan fort brytes dersom det ikke finnes backup av databasen(e). Data kan plutselig mistet dersom det f.eks er et lynnedslag slik at strømmen til databasene(e) kuttes. I tillegg har vi samme argumentasjon som for måleravlesning når det kommer til bryting av **personvern**. Dersom det ikke brukes en kryptert kanal eller passordbeskyttede databaser, kan utenforstående få tilgang til sensitiv informasjon om kunder. Denne informasjonen kan være spennende for personer som vil selge den videre. Informasjonen kan også brukes til å finne ut av passord/pin-koder kundene bruker på andre tjenester. (Fødselsdato, etternavn osv).

Som nevnt i LF til øving 1 er **nettstasjonen** sårbar i unormale frekvensområder. Dette kan utnyttes av ondsinnede personer som kan utføre jamming (sende støy i nærheten av nettstasjonen). Dette vil bryte det ikke-funksjonelle kravet **safety** og at den skal være **fail-safe**. Nettstasjonen kan da oppføre seg unormalt og f.eks sende ut elektrisitet som kan føre til brann i område/støt til personer i nærheten. Dette kan også føre til unøyaktige målinger, som bryter med et ikke-funksjonelt krav om **ytelse**.

Kravet om **safety** i **Aksesspunktene i kommunikasjonsnett** kan brytes ved at disse er tilgjengelige for allmennheten. Dersom de er tilgjengelig for alle, ser jeg for meg at de er mer utsatt for miljøskader, f.eks lynnedslag, jordskjelv og regn. Dette igjen bryter med kravet om **pålitelighet**, da disse miljøfaktorene kan skade aksesspunktene og hindre kommunikasjon. Videre kan krav om **personvern** brytes, ved at det brukes en usikker kommunikasjonskanal. Da kan utenforstående lytte til kommunikasjonen som går igjennom punktene, hindre «videresending» av data mellom punktene og/eller manipulere dataen. Dette kan igjen være interessant for å selge informasjon, blackmail og lavere strømmregning.

Ved **leveranse av strøm** kan kravet om **pålitelighet** brytes ved at en kabel ryker. Dette kan skje hvis den er gammel, noen ødelegger den med vilje, eller generelle miljøskader (lynnedslag, storm, etc). Hvis denne ødelagte kabelen ligger langt unna f.eks «reperasjonspersonale» (eks hyttefelt langt opp i fjellet), vil det ta lang tid å reparere den, som bryter med kravet om **høy maintainability**.