Elektronisk personellkontroll-system for Marinen

Truls Fismen[1], Andreas Reiming[1] og Kirsi Helkala[1][0000-0003-3698-4585]

[1] Forsvarets Høgskole, Cyberingeniørskolen, Lillehammer, Norge
truls.fismen@gmail.com, andreas.reiming@gmail.com,
khelkala@mil.no

Abstrakt. Marinens fartøy opererer med ulike beredskapsnivåer i sjøen. Ved høyeste beredskap, såkalt «klart skip», eller ved brann og/eller havari er det tidskritisk at fartøyspersonellet mønstrer på sine predefinerte plasser og at fartøysledelsen raskt kan gjøre opp personellstatus. I noen tilfeller opplever fartøysbesetningene problemer med å oppnå personellkontroll på en effektiv måte. I dag er dette en prosess som tar lang tid ved at man manuelt må kontrollere personell på utestasjoner, for så å rapportere dette inn til operasjonsrom ved hjelp av telesamband. Denne artikkelen presenteres utviklingsprosjektet av et elektronisk system for personellkontroll, som er utviklet for å tilfredsstille Marinens brukerkrav og tekniske krav, og nasjonale juridiske krav for systemer som behandler personopplysninger. Funnene er basert på Skjold-klasse korvett, men kan generaliseres til samtlige av Marinens seilende plattformer.

Nøkkelord: Personellkontroll, personvern, informasjonssikkerhet.

1 Introduksjon

Marinen opplever problemer med å oppnå personellkontroll om bord på sine fartøysklasser på en effektiv måte. I dag er dette en prosess som tar lang tid ved at man manuelt må finne status på personell. Motivasjonen for prosjektet kommer fra viktigheten av å kunne opprette personellkontroll på kortest mulig tid om bord på Marinens fartøy under tidskritiske og uoversiktlige forhold. Et konkret eksempel på en situasjon hvor et slikt system kunne ha hatt verdi er Helge Ingstad-ulykken i 2018. Her opplevde skipssjefen at det tok lang tid å oppnå kontroll på personellet under en svært stressende og uoversiktlig situasjon. Tidligere skipssjef Preben Ottesen på KNM Helge Ingstad uttalte til VG i etterkant av hendelsen at det i fredstid er førsteprioritet å få kontroll på mannskapet under ulykker. Dette tar vanligvis noen få minutter, men under havariet opplevde han at dette tok mye lenger tid enn vanlig [23]. Påvirkende årsak var blant annet strømbrudd og utfall av fartøyets sambandssystemer og dermed manglende evne til å rapportere status, i tillegg til at flere besetningsmedlemmer var innesperret på lugarer og følgelig ikke hadde mulighet til å melde fra.

Denne artikkelen er forkortelse av en utviklingsoppgave som ble gjort som en bacheloroppgave ved Cyberingeniørskolen [15]. Opprinnelig oppgave har ikke blitt offentlig publisert fordi den inneholder begrenset informasjon. Informasjon som er gradert eller unntatt offentlighet er utelatt og ikke å bli diskutert i denne artikkelen.

Artikkelen presenterer besvarelsen til oppgavens problemstilling: «Hvilke krav stilles til et elektronisk system som skal gi informasjon om personellstatus i form av personelltilstand og posisjon, og hvordan kan et slikt system utvikles og implementeres på korvetter i Skjold-klassen?»

2 Bakgrunn

Selv om prototyputvikling er en teknisk prosess, må de tekniske løsningene for et elektronisk system som behandler om personopplysninger tilfredsstille juridiske krav. I resterende del av kapitlet gjennomgås de juridiske aspekter og lover som er sentrale for valgene gjort under utviklingsprosessen. I tillegg må informasjonssikkerhet ivaretas når systemer blir utviklet [10, 17].

2.1 Personvernforordringen

Personvernforordningen er en forordning for å regulere behandling av personvernopplysninger i EØS. Dette er i norsk lov gjennomført gjennom personopplysningsloven av 2018. I forordningen blir begrepet «behandling» definert til blant annet å omfatte innsamling, registrering, lagring og bruk av personopplysninger. Begrepet «personopplysninger» omfatter opplysninger om en identifisert eller identifiserbar fysisk person, jf. art. 4 nr. 1. Et sentralt aspekt ved forordningen og personvernopplysningsloven er at organisasjoner, eksempelvis Forsvaret, må inneha et legitimt behandlingsgrunnlag for å kunne behandle personvernopplysninger, jf. art. 6 nr. 1.[21]

Behandlingsgrunnlagene for å behandle personvernopplysningen finner man i art. 6 nr. 1 bokstav a) til f) i personopplysningsloven [21]. Et sentralt poeng er at det kan finnes flere behandlingsgrunnlag som kan passe til et enkelt formål, men man kan kun ha et behandlingsgrunnlag per formål. Under er en liste over de ulike behandlingsgrunnlagene med en beskrivelse hentet fra art. 6 nr. 1 a) til f) i personopplysningsloven.

a) Den registrerte har samtykket til behandling av sine personopplysninger for ett eller flere spesifikke formål.
b) Behandlingen er nødvendig for å oppfylle en avtale som den registrerte er part i, eller for å gjennomføre tiltak på den registrertes anmodning før en avtaleinngåelse.
c) Behandlingen er nødvendig for å oppfylle en rettslig forpliktelse som påhviler den behandlingsansvarlige.
d) Behandlingen er nødvendig for å verne den registrertes eller en annen fysisk persons vitale interesser.
e) Behandlingen er nødvendig for å utføre en oppgave i allmennhetens interesse eller utøve offentlig myndighet som den behandlingsansvarlige er pålagt.
f) Behandlingen er nødvendig for formål knyttet til de berettigede interessene som forfølges av den behandlingsansvarlige eller en tredjepart, med mindre den registrertes interesser eller grunnleggende rettigheter og friheter går foran og krever vern av personopplysninger, særlig dersom den registrerte er et barn.

Det er verdt å nevne at ved bruk av art.6 nr.1 bokstav c) eller e) som behandlingsgrunnlag, må det også finne hjemmel i norsk lov [21], f.eks. sikkerhetsloven [20].

2.2 Grunnleggende personvernprinsipper

Datatilsynet har formulert en følgende personvernsprinsipper for å ivareta lovlig, rettferdig og transparent behandling av personvernsopplysninger [9]. Disse er basert på artikkel 5, 6 og 9 i personvernforordningen.

Formålsbegrensning: Formålet med behandlingen av personvernsopplysningene må være identifisert og beskrevet presist. Dette må gjøres på en entydig måte slik at alle interesserte har lik forståelse for hva disse opplysningene skal brukes til. Dette betyr også at dataene ikke kan brukes til andre formål enn de som er beskrevet med mindre det hentes inn nytt samtykke.

Dataminimering: Prinsippet om dataminimering innebærer å begrense innsamlet data til det minimum som er nødvendig for formålet. Dette betyr at identitetsopplysninger som ikke er relevant for formålet ikke skal innsamles. Det kan også være relevant å begrense hvor mange og hvilke personer det samles inn opplysninger om.

Riktighet: Personopplysninger som behandles skal være korrekte og nøyaktige. Hvis det er nødvendig, skal de oppdateres. Dette innebærer at den med behandlingsansvar har ansvar for å slette og endre uriktige personopplysninger, også i backuper.

Lagringsbegrensning: Prinsippet om lagringsbegrensing betyr at informasjon bare skal lagres så lenge som nødvendig og deretter slettes eller anonymiseres automatisk.

Integritet og konfidensialitet: Dette prinsippet innebærer at integriteten og konfidensialiteten bevares. Dette betyr at det skal være iverksatt tiltak for at utenforstående ikke får tilgang til å lese eller endre informasjonen som er lagret.

Ansvarlighet: Ansvarlighet betyr at den ansvarlige må opptrå i samsvar med gjeldene regler for behandling av personopplysninger. Det er ikke nok å ha ansvaret, man må også vise at man tar det alvorlig. Dette innebærer å etablere tekniske og organisatoriske tiltak for å sørge for at opplysningene blir ivaretatt på en ansvarlig måte.

2.3 Skjold-klasse

Fig. 1. Skjold-klassen korvett [6]/Henriette Dæhli/Forsvaret.

Denne artikkelen er basert på Marinens Skjold-klasse fartøy, illustrert på fig. 1. Fartøyene er en blanding mellom luftputebåt og katamaran, noe som muliggjør at man kan løfte fartøyet med vifter under skrogkonstruksjonen. Dette minsker fartøyets motstand i vannet og muliggjør høy hastighet. De er bygget med en «stealth teknologi» som gjør

at de er vanskelig å oppdage på radar og det blir benyttet et lett kompositttmateriell for å oppnå lav vekt. Skjold-klassen er noen av verdens raskeste militære fartøyer og kan i hovedsak bekjempe overflatetrusler, men innehar noe anti-luftkapasitet. Selv om artikkelen fokuserer om Skjold-klassen, kan ideen generaliseres til andre fartøy. Selv implementasjonen må likevel testes, fordi material av fartøy kan påvirke signaler.

3 Metode

Prosjektet har vært et utviklingsprosjekt og benyttet en iterativ og smidig metodikk med fire faser. I kravinnhentingsfasen ble det utarbeidet hvilke krav som stilles til et elektronisk system for personellkontroll. Det ble kartlagt bruker- og tekniske krav til systemet via samtaler med teknisk personell om bord. Intervjugodkjenning ble gitt av Norsk senter for forskningsdata og Forsvarets forskningsnemd. Videre utledet vi juridiske krav som stilles til et slikt system under veiledning av jurist i Cyberforsvaret. Kravene blir presentert i kap. 4.

Informasjonsinnhentingsfasen handlet om sambandsmidlene som eksisterer på korvetter i Skjold-klassen (gradert) og muligheten for å utvikle et eget system. Kompetansehevingen ble i denne fasen gjennomført ved litteraturstudie. Inspirasjon for å utvikle en personellkontroll system ble hentet fra åpne kilder på internett som forklarte hvordan lignende systemer lages [16, 27, 29, 31]. I tillegg, har flere tekniske sider blir benyttet for eksempel [4, 5, 12, 18, 25, 26, 28].

I utvikling og implementasjonsfasen ble det utviklet en prototype av et elektronisk system for personellkontroll til bruk på Skjold-klassen ved hjelp av smidig systemutviklingsmetodikk. Fordelen ved å benytte denne metoden mot den mer tradisjonelle systemutviklingsmetoden er i hovedsak at man kan ta høyde for oppdukkende krav og behov som stilles til systemet [29]. Ulempen med denne metoden kan være at man styrer mot kundenes subjektive krav, og at disse ikke nødvendigvis realiserer målene som stilles til et system. Prototypen blir presentert i kap. 5.

Til slutt ble prototypen til systemet testet og evaluert. Testene fokuserte på hvordan systemet oppfyller kravene som er utledet fra de tidligere fasene. Testresultatene er presentert i kapittel 6, mens evaluering av prototypen er presentert i kap. 7. Her diskuter vi systemet oppimot de ulike kravene som ble utledet i fase én. I tillegg til dette diskuterer vi hvilke sikkerhetstrusler som vil være relevante for et slikt system. Opprinnelig var intensjonen å utføre tester om bord på fartøyet, men dette var ikke mulig på grunn av Covid-19 situasjonen. Testene ble derfor gjennomført på en bygning.

4 Resultat I: Krav

Kapitlet presenterer resultatene i følgende rekkefølge: Først tar vi for oss de ulike kravene utledet til det elektroniske systemet for personellkontroll både bruker-, tekniske- og juridiske krav. Etter dette presenteres utviklet elektronisk system for personellkontroll. Argumentasjon for valgene som har blitt tatt kommer etter denne. Til slutt legges det frem resultater fra testene som ble gjennomført.

4.1 Kravspesifisering

Basert på samtaler med teknisk personell og egne erfaringer ble det utledet bruker krav og tekniske krav. Kravene er selvforklarende og blir ikke diskutert i detalj her.

1. Systemet skal kunne gi posisjon og status på personellet.
2. Posisjon bør være nøyaktig ned til hvilket rom personen befinner seg, i hvert fall til en sone.
3. Det skal være enkelt å benytte systemet, og det skal ikke komme i veien.
4. Batteritid, i tilfell strøm faller ut, for alle leddene i systemet må være så god at mannskapet ikke må tenke på dette.
5. Systemet må ikke kunne oppdages av andre fartøy.
6. Systemet skal ikke interferere med andre systemer om bord på fartøyet.

4.2 Personvern

Formålsbegrensning setter krav om at formålet med innhentingen av personopplysningene må være strengt definert og informasjonen vi lagrer så lite som det er behov for. Det er også kritisk at dataensom blir innhentet ikke skal benyttes til andre formål enn det som er beskrevet. Formålet med det elektroniske systemet er å sørge for personellkontroll ved stressende og kritiske situasjoner som de ulike beredskapstilstandene ved eksempelvis «klart skip», «brann» og «havari».

1. Systemet må ha en funksjon som gir mulighet for å skru det av og på.
2. Dataen som systemet innsamler skal kun benyttes til å opprette personellkontroll ved situasjoner hvor dette er viktig for liv og helse om bord, også under trening.
3. Alle på fartøyet skal bli informert når systemet aktiveres.
4. Posisjon og statusdata skal ikke lagres av systemet.
5. Mengden personopplysninger må minimeres slik at man kun henter inn informasjon som er kritisk for at systemet skal levere tilstrekkelig funksjonalitet.

Årsaken for første kravet er at systemet kun skal benyttes i situasjoner hvor det er kritisk å opprette personellkontroll, og det derfor ikke vil være nødvendig at det er på til alle tider. For å følge dette prinsippet bør systemet inneha denne funksjonen.

Det andre kravet stilles fordi det understøtter prinsippet om at man kun benytter dataen til formålet. Det kan tenkes at uten et krav som dette vil løsningen kunne misbrukes. Eksempelvis at systemet blir benyttet for å overvåke personellet, og vurdere effektiviteten i arbeidet deres [30]. Dette må man unngå ved å sette strenge krav til formålet og når systemet skal kunne tas i bruk. I dette tilfellet er ikke systemet ment for å fungere som en effektivitets måler og man må av den grunn minimere sjansen for at det kan misbrukes slik.

Det tredje kravet kan praksisers enten at det sies ifra på forhånd i hvilke situasjoner systemet tenkes å nyttes, eller eksempelvis at man melder at det tas i bruk over høyttaler også kjent som PA-anlegg. Dette er igjen på bakgrunn av at personellet om bord på fartøyet skal være klar over når de blir overvåket.

Lagringsbegrensning setter krav om at informasjonen på systemet kun lagres så lenge det er nødvendig og at det deretter slettes eller anonymiseres [9]. Likevel kan man argumentere for at det ville det kunne være nyttig å lagre data en kort periode, f.eks. benytte den i etterforskning ved ulykker eller lignende. Dette kunne blitt gjort ved å skrive ned en periode man lagrer dataen i en samtykkeerklæring.

Det femte kravet baseres på dataminimering prinsippet som sier at datainnsamlingen og personopplysninger må begrenses til kun det som er nødvendig for formålet [9]. Det er verdt å nevne at dette prinsippet understøtter krav tre, men også blir understøttet av prinsippet om formålsbegrensning.

4.3 Behandlingsgrunnlag

Bruken av systemet vil medføre behandling av personopplysninger. Av denne grunn må det bli vurdert om Forsvaret har såkalt behandlingsgrunnlag etter art. 6 nr. 1 i Personvernforordningen (se kap. 2.1). I art. 6 nr. 1 a) til f) er det syv alternativer man kan benytte for å argumentere for behandlingsgrunnlag, og man kan kun benytte seg av én av disse. Vi har vurdert grunnlag a) og d) som sentrale for dette systemet.

Det kan argumenteres for at grunnlag a) kan benyttes da denne omhandler at en virksomhet kan behandle personopplysninger om de har innhentet samtykke fra de det gjelder. Det er sentralt at samtykke er frivillig og at vedkommende er godt informert, samt at formålet er godt spesifisert [8]. Dette vil kunne være mulig å få til ved å lage et skriv om hvilke personopplysninger som skal innhentes, formålet for innhentingen av informasjonen og hva det skal brukes til. Likevel kan det være problematisk at personell ikke egentlig får en reel mulighet til å gi samtykke, f.eks. hvis samtykke må gis for å kunne jobbe på fartøyet, blir det vanskelig å bedømme hvorvidt samtykket er frivillig.

Grunnlag d) kan benyttes som behandlingsgrunnlag. Dette behandlingsgrunnlaget går ut på at det må være nødvendig for å «verne den registrertes eller en annen fysisk persons vitale interesser» [8]. Denne er veldig aktuell å benytte for det elektroniske systemet på bakgrunn av at formålet med systemet er knyttet til liv og død, altså i hovedsak fare for helsen. Dette behandlingsgrunnlaget blir av Datatilsynet beskrevet som svært snevert [8]. Likevel mener vi at liv og helse på Marinens fartøy, spesielt i kritiske situasjoner som klart skip, havari og brann havner innenfor denne tolkningen, og dermed er grunnlag d) det beste behandlingsgrunnlaget for det elektroniske personellkontroll systemet.

5 Resultat II: Elektronisk system for personellkontroll

Basert på kravene vist i kap. 4 har vi laget en prototype på et innendørs posisjoneringssystem med funksjoner for personellkontroll. Det overordnede målet til systemet er å kunne gi informasjon om hvilket rom eller sone personellet på fartøyet befinner seg i, og en mulighet til å enkelt kunne melde ifra om egen tilstand.

Overordnet er systemet bygd opp slik at hver person utrustes med en liten BLE-beacon (Bluetooth Low Energy Identifier) [26] som bæres på kropp, for eksempel rundt halsen. Fartøyet blir utrustet med en sender og mottaker i hvert rom eller i en definert

sone. Denne sender og mottakeren består av maskinvare og programvare som skanner etter BLE-beacons, henter ut informasjon og sender denne informasjonen videre til en sentralisert hub via rutere utstasjonert i fartøyet. Informasjonen den sender videre er informasjon om RSSI-verdien (Received Signal Strength Indicator) [22] og BLE-beaconets UUID (universally unique identifier) [26], samt rommets ID. Denne sentraliserte huben prosesserer dataen og fremviser posisjonen til de ulike personene og tilstand på en skjerm som brukeren kan nyttiggjøre seg av. En overordnet oversikt over systemet er vist på fig. 2.

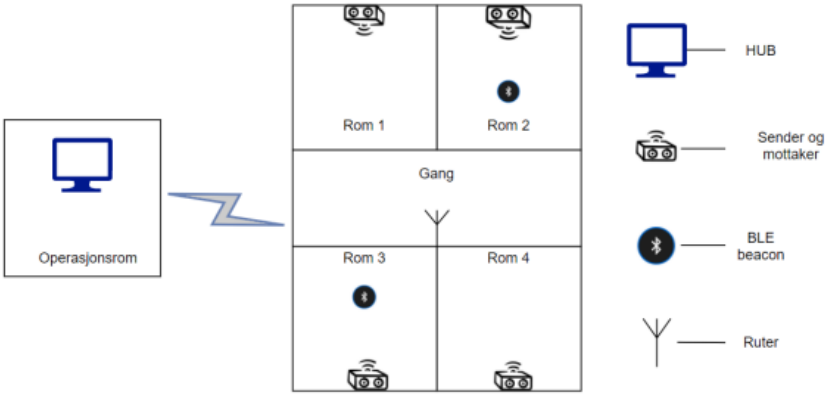

Fig. 2. Overordnet oversikt over systemet.

Prototypen består av fem sensorsystem er med tilhørende XBee-moduler (se fig. 3) og en hub med en XBee-modul koblet til en Arduino UNO (se fig. 4), som igjen er tilkoblet en Raspberry Pi. Størrelsen på sensorsystemene er omtrent 10 cm x 15 cm. Størrelsen på BLE-beacon (se fig. 5) er omtrent 3cm x 3 cm.

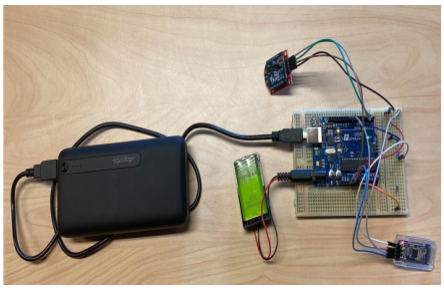

Fig. 3. Sensorsystemet.

Fig. 4. Hub.

Fig. 5. BLE.

5.1 Sensorsystemet

Maskinvaren som blir benyttet i sensorsystemet er HM-10 moduler [2], Arduino UNO [5, 14] og BLE-beacons [1]. I tillegg består sensorsystemet av en strømforsyning

som er tiltenkt å koble i fartøyets strømnett, og en batteripakke med et 9 volt batteri som kan overta med en gang strømmen om bord faller ut.

HM-10 benyttes for å skanne etter BLE-beacons. For å hente ut dataen fra HM-10 må man laste inn en programkode på Arduino UNO [4]. Denne koden henter først informasjonen fra HM-10 modulen ved å sende kommandoen «AT+DISI?» som returnerer alle Bluetooth-enheter og gir informasjon om disse på et ibeacon format [3]. Videre sorterer koden ut UUID og RSSI verdien til oppdagede BLE-beacons. I tillegg legger koden til IDen til rommet HM-10 modulen befinner seg. Dette for å kunne knytte rom oppimot RSSI-verdi i huben. Denne rom-IDen er et tall på to bytes som er unikt for hvert rom og legges inn når arduinoene programmeres. Informasjonen koden sorterer ut lagres i en variabel slik at den kan hentes ut for å videresendes til huben.

Nettverksstrukturen til sensorsystemet er et stjernenettverk, fordi de forskjellige BLE-beacons kommuniserer med HM-10 modulen uten å kommunisere med hverandre [16, 18]. HM-10 modulen vil være koordinatoren i nettet mens BLE-beacons vil være ulike noder i nettverket som kommuniserer med koordinatoren.

5.2 Transmisjon

Maskinvaren som blir benyttet i transmisjonsdelen er XBee-moduler [11, 13]. Disse brukes for å sende informasjonene fra sensorsystemet videre til den sentraliserte huben. Disse er koblet til de samme Arduino UNO som benyttes i sensorsystemet. Til prototypen er det anskaffet XBee PRO S2C-moduler og adaptere. Disse adapterene benyttes for å sørge for enkel og stabil kommunikasjon mellom modulene og Arduino UNO.

XBee-modulene konfigureres via det tilhørende programmet XCTU. Det lastes inn en fastvare på modulene for at de kan operere i et maske-nettverk og videre det konfigureres innstillinger for å tillate kommunikasjon mellom modulene og arduinoene.

En av modulene blir konfigurert til koordinator i nettet, mens resten blir konfigurert til rutere. Programvaren for å sende dataen fra sensorsystemet som benyttes i transmisjonsdelen er sammenflettet med programkoden på Arduino UNO som benyttes for å hente ut informasjonen fra sensorsystemet. Her benytter vi et eget bibliotek på programmeringsmiljøet til arduinoen, Arduino Integrated Development Environment (IDE) [24] for å lage en kode som fyller datapakker med informasjonen som hentes ut i sensorsystemet og videresender dette til huben.

XBee modulene som blir benyttet i denne prototypen er konfigurert til å operere i et maske-nettverk. Den ene XBee modulen i nettverket som er konfigurert til å være koordinator vil motta alt av datapakker som enten sendes fra et sensorsystem innen rekkevidde eller som er videresendt av ulike sensorsystemer eller egne rutere.

XBee-modulene koblet til sensorsystemet vil være konfigurert til å fungere som rutere. Dette vil si at de sender ut dataen de får fra det tilkoblede sensorsystemet, i tillegg til å videresende data de mottar fra andre XBee-moduler tilknyttet andre sensorsystemer. Det er også mulig å konfigurere XBee-moduler til ruter uten tilknytning til et sensorsystem. Denne vil kun videresende datapakker den mottar og er tiltenkt å fungere som reelle hvis man har dårlig forbindelse i noen områder.

5.3 Hub

For at en bruker av prototypen skal kunne nyttiggjøre seg av informasjonen som hentes har vi laget en hub som kan presentere dataen som innhentes fra forskjellige områder i fartøyet. Det er definert tre operasjoner som må bli utført i huben. Først må dataen koordinator XBee-modulen mottar hentes ut via en tilkoblet Arduino UNO. Deretter må denne sensordataen analyseres av et program for å finne posisjon og tilstand til personellet. Etter dette må informasjonen fremvises, slik at det den kan benyttes for å forbedre personellkontroll.

En XBee-modul som er konfigurert til koordinator benyttes for å motta all informasjon som sendes i nettverket. Denne XBee-modulen er koblet til en Arduino UNO. Arduinoen har et program som leser dataen mottatt fra XBee-modulen og sender den ut på USB-porten som serielldata.

Serielldataen mottas av Raspberry Pien [25] og analyseres ved hjelp av Python-kode. Raspberry Pien er koblet til en tilhørende 8 tommers skjerm. Til prototypen er det anskaffet én Raspberry Pi [28] og en tilhørende 8 tommer skjerm.

På Raspberry Pien settes det opp kommunikasjon til arduinoen for å motta meldinger via UART-protokollen. Meldingene sjekkes for om de er på riktig format ved en regulærtuttrykksjekk. Hvis formatet er riktig, sorteres meldingen basert på rom-ID (to første bytes) og UUID (neste 20 bytes). Finnes det en oppføring for denne UUIDen og rom-IDen oppdateres RSSI verdien, ellers legges det til en ny verdi. Samtidig lagres det tidspunktet verdien ble lagt til. Neste gang det kommer inn en melding som gjelder samme UUID vil programmet sjekke om det har verdier som er eldre enn ett minutt og slette disse. Dette er for å unngå gamle utdaterte verdier i systemet. Til slutt sorterer programmet hvilket rom som har best signalstyrke til beaconet basert på RSSI og skriver ut hvilket rom beaconet befinner seg.

5.4 Argumentasjoner for metoder, protokoll og maskinvare brukt i prototypen

Det ble valgt å benytte signalmåling basert på signalstyrke over metoder basert på tid. En av de grunnene var at det finnes mye kommersiell hyllevare man kan benytte for å finne informasjon om signalstyrke. En annen grunn var at metoder basert på tid krever mer avanserte komponenter, noe som kan føre til at systemet blir dyrere og større. Dette vil kunne gå imot kravet om at systemet ikke skal være i veien for personellet. Ulempen med signalmåling basert signalstyrke er at systemet kan bli noe mer unøyaktig.

Det ble valgt å benytte nærhet posisjoneringskalkulering over trilaterasjon og triangulering. Den mest definerende grunnen er at BLE-beacon som benyttes i systemet ikke trenger å ha forbindelse med flere sensorsystemer samtidig, og det er nyttig i et fartøysmiljø. En annen grunn er at den ikke trenger alt for komplisert programvare. Ulempen med denne metoden er at den gir noe mer unøyaktig posisjon enn de andre metodene.

Prototypen til systemet er bygget opp av stjerne -og maskenettverktopologi. Stjernetopologi er valgt til sensorsystemet fordi dette muliggjør at man kan hente ut informasjon om noder i nettverket fra en koordinator. I tillegg er det mye kommersiell maskinvare som støtter denne topologien og lite konfigurasjon som kreves for å realisere denne

topologien. Masketopologi er valgt til sensorsystemet fordi dette lager et redundant nettverk. Informasjonen fra sensorsystemene vil kunne sendes over maskenettverket. Rekkevidden til systemet vil også øke på bakgrunn av at man kan sende informasjon via noder til destinasjonen. I likhet med stjernetopologi finnes det mye kommersiell maskinvare som støtter denne topologien.

Protokollene som er benyttet i prototypen er BLE [19] og Zigbee [12]. BLE benyttes til sensorsystemet og Zigbee til transmisjon fra sensorsystemene til huben. Overordnet er det ingen av disse protokollene som interferer med andre systemer på Skjold-klassen, noe som er et viktig argument for at de er valgt til systemet.

BLE er valgt til sensorsystemet fordi den støtter stjernetopologi og det finnes mye kommersiell maskinvaresom benytter seg av denne protokollen. I tillegg er UUID-formatet man identifiserer noder med veldig verdifullt for å kunne identifisere personell, og for å utvikle programvare. Videre er protokollen utviklet for lavt energiforbruk, dette gjør at maskinvare protokollen benyttes på vil ha god batteritid. Rekkevidden er på 15 m innendørs, noe som er godt nok for at den skal kunne nyttes i sensorsystemet.

Zigbee er valgt til transmisjonsdelen fordi, for det første, protokollen støtter masketopologi og teoretisk opp til 64000 noder i et nettverk [12] og den har en teoretisk rekkevidde på 30 m innendørs ved 2400 MHz versjonen. Et annet element er at det finnes mye kommersiell maskinvare man kan benytte. Det er verdt å nevne at ved 2400 MHz kan den interferere med Wi-Fi. Likevel skrus gjerne trådløse nettverk av under seilas, noe som kan være et argument for at denne frekvensen er gunstig å benytte.

Maskinvaren (BLE-beacons, HM-10 moduler, Arduino UNO, XBee-moduler og Raspberry Pi) er overordnet valgt fordi de støtter posisjoneringsmetoden, nettverkstopologi og protokoller. Fordel for BLE-beacon er liten i størrelse med god batteritid, og har en knapp som vi kunne programmere med ønsket funksjon. I tillegg opererer den på en frekvens som ikke interfererer med allerede eksisterende sambandsmidler. Fordel for HM-10 modulen er at den er kompatibel med BLE-beacon og har tilkoblingsmuligheter til Arduino UNO mikrokontrolleren.

XBee-modulen ble valgt fordi det er en Zigbee-modul med god rekkevidde og har gode muligheter for maskenettverk. I tillegg kan den tilkobles til Arduino UNO mikrokontrolleren og en benytter frekvenser som ikke vil påvirke de allerede eksisterende sambandsløsningene om bord, med unntak av Wi-Fi. Arduino UNO og Raspberry Pi ble valgt fordi de innehar nok datakraft for å kjøre trengte programmene.

6 Resultat III: Testing av prototypen

For å kunne vurdere prototypen ble det gjennomført tester for å evaluere systemets rettidighet og nøyaktigheten til nærhetsprogramvaren. Indirekte ble systemets rekkevidde også testet. Måling av tid ble gjort med stoppeklokke og måling av avstand med målebånd.

6.1 Test av registreringstid ved bytte av posisjon

Målet med denne testen var å finne ut hvor lang tid det tar for systemet å oppdatere ny posisjon på en BLE-beacon når den bytter rom. For å prøve å unngå feilmålinger satt vi ut to sensorsystem med god avstand på omtrent 8 meter. Startpunktet for testet er området man går ut fra sonene til det ene sensorsystemet og inn i sonen til det andre sensorsystemet. Det er her man starter stoppeklokken og måler tid fram til det oppdateres at BLE-beacon har blitt flyttet fra rom 1 til rom 2 eller motsatt. Det ble gjennomført 10 tester og resultatene er fremlagt i tab. 1. Resultatet gir gjennomsnitt 12,22 sekunder med standardavvik 4,58 sekunder.

Tab. 1. Resultater av rombytting.

Forsøk	1	2	3	4	5	6
Tid	11,14	9,79	22,63	4,67	15,91	9,45
Forsøk	7	8	9	10	$\bar{x}$	**sd**
Tid	14,02	9,02	13,83	11,73	**12,22**	**4,58**

6.2 Test av registreringstid ved innmelding av status

Ved denne testen er formålet å finne ut hvor lang tid det tar for prototypen å oppdatere innmeldingen av personellstatus fra BLE-beacon. I et forsøk på å få mest mulig nøyaktige målinger benyttet vi kun et sensorsystem og en BLE-beacon. Deretter målte vi tiden fra man trykker inn knappen på BLE-beacon til det ble fremvist på huben. Det ble gjennomført 10 tester og resultatene er fremlagt i tab. 2. Resultatet gir gjennomsnitt 11,52 sekunder med standardavvik 3,50 sekunder.

Tab. 2. Resultater av status innmelding.

Forsøk	1	2	3	4	5	6
Tid	10,23	13,34	15,63	7,19	8,76	15,76
Forsøk	7	8	9	10	$\bar{x}$	**sd**
Tid	13,43	7,23	7,67	15,92	**11,52**	**3,50**

6.3 Test av nøyaktighet til prototypen

Ved denne testen var formålet å finne ut hvor nøyaktig prototypen kan levere posisjonsdata. Testmiljøet er rom på en kaserne med størrelse på omtrent 3 meter i bredden og 6 meter i lengden. Måten testen ble gjennomført var ved at en testperson tok en BLE-beacon rundt halsen og gikk en runde i testmiljøet (se fig. 2). Personen begynte i gangen, deretter gikk personen til rom 1, rom 2, rom 3 og rom 4. Det ble også gjennomført målinger ved å legge en BLE-beacon nærmest mulig veggen mot et annet sensorsystem for å se om man får feil posisjonsdata. I tillegg til dette gjennomførte vi testen med åpne og lukkede dører.

Det overordnede resultatet fra testene er at prototypen leverer riktig posisjonsdata når man er tydelig innenfor rommet til et sensorsystem, men kan være noe unøyaktig i grensepartiet mellom flere sensorsystemer. Resultatene fra testen gjennomført med

åpne dører er fremlagt på fig. 6. Områdene markert i oransje er de hvor det kan oppstå feilposisjonering, disse går omtrent en meter inn i rommet og noe utenfor.

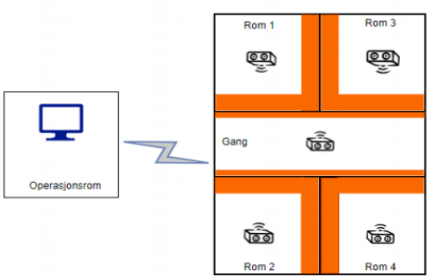

Fig. 6. Nøyaktighet ved åpne dører.

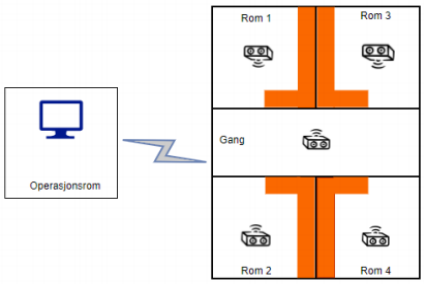

Fig. 7. Nøyaktighet ved lukkede dører.

Resultatene fra testen gjennomført med lukkede dører er fremlagt på fig. 7. Områdene markert i oransje er de hvor det kan oppstå feilposisjonering, disse går omtrent en meter inn i rommet, men her vil de avgrenses mer enn med åpne dører.

7 Diskusjon

For å vurdere prototypen skal vi ta utgangspunkt i hvordan det utfyller de ulike kravene definert for et elektronisk system for personellkontroll.

7.1 Bruker og tekniske krav

Det første bruker kravet var at systemet skulle kunne gi posisjon og status på personellet. Den utviklede prototypen vil oppfylle dette kravet ved at den gir informasjon om rom eller sone personellet befinner seg i fartøyet. I tillegg til at man kan melde inn egen status ved å trykke på en knapp på BLE-beacon. Når dette sees opp mot hvilken posisjon personell skal ha ifølge rullen til skipet, kan det bestemmes om skipet er klart eller om det kreves å sette i gang personsøk for å lokalisere vedkommende. I denne artikkelen har vi ikke testet BLE-beacon sin nyttighet i «man over bord» situasjoner.

Det andre brukerkravet var at system et burde gi posisjon som er nøyaktig nok til å levere informasjon om hvilket rom personellet befinner seg. Den utviklede prototypen oppfyller delvis dette kravet. Ut fra resultatene om nøyaktighet til prototypen ser man at prototypen kan levere unøyaktig rom data i grensepartiene mellom sensorsystemer. Av denne grunn kan man argumentere for at systemet vil fungere bedre til å levere data om sone, og ikke rom. Testene er riktignok simulert på rom med lettvegger. Av den grunn kan man argumentere for at det er vanskelig å si hvordan posisjoneringen vil være på en korvett med mulig andre vegger. Likevel ved tykkere vegger og materiale av stål vil sannsynligvis posisjoneringen bli mer nøyaktig på grunn av at strålingens diffraksjon påvirkes av materialer med høyere tetthet. Av den grunn kan det argumenteres for at nærhetsteknikken som brukes nå egner seg best på fartøy med tykke vegger,

som for eksempel stålskottene på en fregatt. Ved lettvegger som eksisterer på korvett bør man mulig kunne benytte en trianguleringsalgoritme som gir bedre nøyaktighet.

Det tredje brukerkravet var at systemet skulle være lett for mannskapet å benytte, samt at det ikke skulle komme i veien. Det kan argumenteres for at prototypen oppfyller dette kravet i stor grad. Mannskapet må gå rundt med en liten BLE-beacon i et halsbånd, eller ha den liggende i uniformen. Sensorsystemene blir satt ut på strategiske steder som ikke skal føre til noen hindring og hvor det er tillat å ha sensorer. Huben plasseres i nærheten av operasjonsrommet hvor den ikke bør komme i veien for noen og er, med tanke på gradering tillat å installere, kun være et ekstra hjelpemiddel for personellkontrollansvarlig. Kravet til batteritid, tenker vi å vare tilfredsstillende i denne prototypen.

Det femte kravet er tekniske kravet som omhandlet at systemet ikke skal kunne oppdages av andre fartøy. Dette oppfyller systemet ved å benytte protokoller med lav rekkevidde. Maksrekkevidden til Zigbee ved 2400MHz, som er frekvensen vi har brukt, er på 400 meter. Dette vil være betydelig kortere enn avstanden man visuelt kan se fartøyet. Dette er allikevel ikke testet av oss med avanserte EK-sensorer, noe som bør gjøres før systemet tas i bruk.

Det siste kravet er tekniske kravet som omhandler at systemet ikke skal interferere med andre systemer om bord på fartøyet. Dette kravet oppfyller systemet ved at man har kartlagt de ulike interne sambandsmidlene om bord på fartøyet. Deretter ble det valgt protokoller som ikke interfererer med noen av de kartlagte systemene, hverken ved lik frekvens eller protokoll. Dette vil sørge for at de andre systemene om bord ikke vil bli påvirket av personellkontrollsystemet.

7.2 Juridiske krav

Det første juridiske kravet var at systemet skulle ha en funksjon som gir mulighet for å skru systemet av og på. På mange måter kan man argumentere for at prototypen til systemet oppfyller dette kravet. For å skru av huben og sensorsystemene kan man koble ut strømtilførselen. Altså har prototypen en funksjon for å skru systemet av og på, likevel vil dette være tungvint. Av den grunn kan det argumenteres for at det vil være hensiktsmessig å utvikle en mer sentralisert metode på et ferdigstilt system der man har mulighet til å skru av og på sensorene fra huben.

Det andre juridiske kravet som ble definert for systemet omhandlet at informasjonen som innhentes av systemet kun skal nyttes til å opprette personellkontroll ved situasjoner hvor dette er viktig for liv og helse, og ved trening på slike situasjoner. På skjermen til huben og det tilhørende tastaturet kan man starte og stoppe programmet som nyttiggjør seg av dataen som sendes fra de ulike sensorsystemene. Av den grunn kan man argumentere for at prototypen legger til rette for dette kravet.

Det tredje juridiske kravet omhandler at personellet på fartøyet skal bli informert når systemet aktiveres. Dette er noe som ikke direkte kan knyttes opp til systemet, men bruken av det. Ved dette kravet må det meldes over PA-anlegg at systemet startes og opplyses om at personellets posisjon overvåkes, for eksempel i begynnelse av en seilas.

Det fjerde juridiske kravet omhandler at posisjon og statusdata ikke skal lagres av systemet. Dette oppfyller systemet ved at det er utformet til å ikke lagre dataen den mottar, kun fremvise det når nødvendig.

Det femte juridiske kravet omhandler at mengden personopplysninger må begrenses til kun det som er kritisk for funksjonen til systemet. Prototypen benytter kun navn eller stilling, posisjon og tilstand. Av denne grunn kan man argumentere for at prototypen oppfyller dette kravet. I tillegg sendes hverken navn eller stilling til personen over radio, kun UUID til BLE-beaconet de bærer. Denne UUIDen blir kun knyttet til navn i huben, og bare den som har tilgang til systemet kan koble UUID og person sammen.

7.3 Sikkerhetstrusler aktuelle for prototypen

Ethvert elektronisk system som angir posisjon og status på personell er utsatt for både passive og sikkerhetstrusler. En relevant passiv sikkerhetstrussel er at et trådløst system som sender data over eteren kan bli oppdaget av en fiendtlig aktør i det elektromagnetiske spekteret [7]. Dette kan føre til at posisjonen til fartøyet blir avslørt på bakgrunn av strålingen som emitteres. Ved å benytte Bluetooth og Zigbee-protokollen i prototypen kan man argumentere for at denne sikkerhetstrusselen ikke er relevant. Dette er i hovedsak på grunn av at rekkevidden på disse protokollene er veldig kort, og man vil mest sannsynlig bli oppdaget visuelt lenge før man blir oppdaget i det elektromagnetiske spekteret. Det er også verdt å nevne at sikkerheten til personell har førsteprioritet i fredstid, noe som gjør at et system som eventuelt har en høyere signatur i det elektromagnetiske spekteret, kan nyttes i fredstid.

En annen relevant passiv sikkerhetstrussel er at en fiendtlig aktør kan hente ut informasjon fra et slikt system, og dermed svekkes konfidensialiteten til systemet [10]. Likevel er det flere aspekter som gjør at dette er krevende ved den utviklede prototypen. For det første må man være innenfor kort avstand av fartøyet for å kunne av lytte signalene. Skulle man mot formodning være innenfor avstand til å avlytte systemet er det flere andre sikkerhetstiltak man må gjennom. Begge protokollene støtter AES-128 kryptering, noe som gjør det noe mer krevende å hente ut informasjon, men ikke umulig. I tillegg til å bryte krypteringen må man ha en programvare som kan nyttiggjøre seg av de ulike RSSI verdiene og UUIDen. Av denne grunn kan det argumenteres for at sannsynligheten for at konfidensialiteten til prototypen blir brutt er lav.

Et annet aspekt som er sentralt å diskutere er hvilke nytteverdier en eventuell fiendtlig aktør vil ha av informasjon knyttet til prototypen. Dersom en fiendtlig aktør kommer så nært innpå fartøyet vil det være andre ting som er av større interesse. Videre er det mulig å slå av eller la være å benytte systemet til kai der dette er en reell trussel. Det mest kritiske vil i hovedsak kunne være om en fiendtlig aktør finner tilstanden til fartøyet og personopplysninger. Når det kommer til personopplysninger, vil man knytte UUID til navn eller stilling i huben. Dette vil ikke sendes over nettverket og av den grunn kan man si at det vil være enda mer krevende å hente ut denne informasjonen. Når det kommer til muligheten for å kunne hente ut informasjon fra andre systemer kan dette unngås ved å sørge for at personellkontrollsystemet er fullstendig frakoblet og fysisk separert fra andre systemer om bord.

En aktiv sikkerhetstrussel et trådløst system som sender data over trådløse medier kan bli utsatt for er jamming, eller andre metoder en fiendtlig aktør kan benytte seg av for å sette systemet ut av spill [17, 32]. Tilgjengeligheten til systemet vil bli svekket hvis systemet slutter å fungere, enten grunnet fiendtlig påvirkning eller av andre

grunner [10]. Kommunikasjonen i prototypen mellom BLE-beacons og HM-10 modulene vil bli lite påvirket av jamming. Årsaken til dette er at Bluetooth protokollen benytter seg av frekvenshopping spredt spektrum. I tillegg til dette benytter Bluetooth Adaptiv Frekvens Hopping, en teknikk som bytter frekvens hvis det er mye støy på den. Dette er i hovedsak for å unngå å benytte frekvenser som har mye trafikk, men gir også redundans mot jamming. Selv om Zigbee-protokollen på XBee-modulene har ikke samme robusthet mot jamming, er ikke jamming den største trusselen til prototypen. Elektronisk personellkontrollsystem blir nemlig beskyttet av korvetten selv. Fartøyet i praksis blir en Faraday-bur, som beskytter kommunikasjonssystemer inn i fartøyet fra utvendig påvirkning.

En annen aktiv sikkerhetstrussel er at et trådløst system som sender data over trådløse medier kan bli manipulert av en fiendtlig aktør og dermed påvirke integritet av systemet. Selv om dette er en relevant sikkerhetstrussel, vil den trolig være lite relevant for prototypen. Dette er på grunn av at det vil være vanskelig for en fiendtlig aktør å infiltrere systemet da de må være svært nære for å være innenfor dekningen til systemet.

8 Konklusjon

Helge Ingstad-ulykken i 2018 viste at Marinen opplever problemer med å oppnå personellkontroll om bord på sine fartøysklasser på en effektiv måte. I denne artikkelen viser vi en prototype for en elektronisk personellkontroll systemet, som tilfredsstiller tekniske krav i Skjold-klassen, og Marinens generelle bruker krav. I tillegg, er systemet laget for å tilfredsstille juridiske kravene for systemer som handler personopplysninger. Selv om artikkelen fokuserer Skjold -klassen, vil funnene ha føringsverdi til andre fartøystyper i Marinen.

Referanser

1. Amazon: Blue Charm Beacons, https://www.amazon.com/Blue-Charm-Beacons-BluetoothBC011MultiBecon/dp/B085XN9B7N/ref=sr_1_3?dchild=1&keywords= Bluetooth+Beacon&qid=161953875&sr=8-3, aksessert 10. apr. 2021.
2. Amazon: DSD TECH HM-10 Bluetooth, https://www.amazon.com/DSD-TECH-Bluetooth-iBeacon-Arduino/dp/B06WGZB2N4, aksessert 10. apr 2021.
3. Apple inc.: iBeacon, https://developer.apple.com/ibeacon/, aksessert 29. apr 2021.
4. Arduino: Language reference, https://www.arduino.cc/reference/en/, aksessert 1. Apr. 2021.
5. Arduino: UNO, https://www.arduino.cc/en/Main/arduinoBoardUno, aksessert 30. apr. 2021.
6. Arstad, S: Forsvarets forum. https://forsvaretsforum.no/nyhetsvarsel-sjoforsvaret/kristian-9-laget-knm-glimt-av-pepperkake/175101, aksessert 25. mai 2021.
7. CRFS: Naval Emission Control, https://www.crfs.com/applicationstory/naval-emcon-emissions-control/, aksessert 29. jan. 2021.
8. Datatilsynet: Behandlingsgrunnlag, https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/behandlingsgrunnlag/veileder-om-behandlingsgrunnlag/, aksessert 17. mar. 2021.
9. Datatilsynet: Grunnleggende personvernsprinsipper. https://www.datatilsynet.no/rettigheter-og-plikter/personvernprinsippene/grunnleggende-personvernprinsipper/, aksessert 17. mar. 2021.

10. Datatilsynet: Informasjonssikerhet og internkontroll, https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/informasjonssikkerhet-internkontroll/etablere-internkontroll/iverksette-styringssystem-for-informasjonssikkerhet/, aksessert 16. mar. 2021.
11. DIGI: Documentation XBee-PRO S2C DigiMesh® 2.4, https://www.digi.com/ resources/documentation/digidocs/pdfs/90001506.pdf, aksessert 15. apr. 2021.
12. DIGI: xbee, https://www.digi.com/xbee, aksessert 15. apr. 2021.
13. DIGI-Key: XBee S2C, https://www.digikey.com/en/product-highlight/d/digi-intl/xbee-s2c-802-15-4-rf-modules, aksessert 10 apr. 2021.
14. ELFA DISTRELEC: Mikrokontrollerkort, Uno, Arduino. https://www.elfadistrelec.no/ aksessert, 31. apr. 2021.
15. Fismen, T., Reiming, A.: Personlig samband/tracker-løsning på fartøy. Bacheloroppgave, Forsvarets Høgskole, Cyberingeniørskolen, Lillehammer, Norge (2021).
16. Frenzel, L.E.: Principles of electronic communication systems. 4th edn. McGraw-Hill Education, (2016).
17. Jaatun, M.G.: Sikkerhet uten en tråd, https://infosec.sintef.no/informasjonssikkerhet/2018/10/sikkerhet-uten-en-trad/, aksessert 15. apr. 2021.
18. Jinan Huamao Technology: Bluetooth, http://www.jnhuamao.cn/bluetooth.asp, aksessert 1. jan. 2021.
19. Jin Huamao Technology: Bluetooth 4.0 BLE module. http://www.jnhuamao.cn/bluetooth40_en.zip, aksessert 1. mar. 2021.
20. LOVDATA: Lov om nasjonal sikkerhet. https://lovdata.no/dokument/NL/lov/2018-06-01-24, aksessert 17. mar. 2021.
21. LOVDATA: Personopplysningsloven. https://lovdata.no/dokument/NL/lov/2018-06-15-38, aksessert 17. mar. 2021.
22. Malajner, M., Planinsic, P., Cucej, Z., Benkic, K.: Using RSSI value for distance estimation in wireless sensor networks based on ZigBee. In: 15th International Conference on Systems, Signals and Image Processing, pp. 303-306, IEEE, Bratislava, Slovak Republic (2008).
23. Matre, J.: Skipssjefen på KNM «Helge Ingstad»: Slik opplevde han det dramatiske havariet. https://www.vg.no/nyheter/innenriks/i/vmBGO4/skipssjefen-paa-knm-helge-ingstad-slik-opplevde-han-det-dramatiske-havariet, aksessert 8. feb. 2021.
24. Rapp,A.: xbee-arduino, https://github.com/andrewrapp/xbee-arduino, aksessert 7. apr. 2021.
25. Raspberry Pi Foundation: Raspberry Pi 4 model b, https://www.raspberrypi.org/products/raspberry-pi-4-model-b/, aksessert 17. mar. 2021.
26. ReelyActive: Bluetooth Low Energy (BLE) Identifier Reference, https://reelyactive.github.io/ble-identifier-reference.html, aksessert 25. mar. 2021.
27. Reinsnes, L.A., Anders Imenes A., Utvikling av støtteverktøy for nettverksbasert ESM. Bacheloroppgave, Forsvarets Høgskole, Cyberingeniørskolen, Lillehammer, Norge (2019).
28. RS: Raspberry Pi Display Kit, https://no.rsonline.com/web, aksessert 10. apr. 2021.
29. Sørensen, A., Egeland, E.S.: Agile Systemutviklingsmetoder. Masteroppgave, Universitetet i Agder, Kristiansand, Norge (2007).
30. Virgillito, D.: Tracking technologies and ther impact on privacy, https://resources.infosecinstitute.com/certification/3-tracking-technologies-and-their-impact-on-privacy/, aksessert 21. jan. 2021.
31. Vo, T.: Indoor position tracking based on arduino, XBee and ethernet shield, https:// github.com/thovo/Arduino-Indoor-Position-Tracking/blob/master/reports/Report.pdf, aksessert 21. jan. 2021.
32. Wilkins.S.: Wireless lan security threats. https://www.pluralsight.com/blog/it-ops/wireless-lan-security-threats, aksessert 22. mar. 2021.