OC2020 A-126 - Åpen

Rapport

Smartere transport – Møre og Romsdal: L4.1 Cyber security for et autonomt sjøverts persontransportsystem

Forfatter
Egil Wille

SINTEF Ocean AS

2021-06-02

SINTEF

SINTEF Ocean AS
Postadresse:
Postboks 4762 Torgarden
7465 Trondheim
Sentralbord: 46415000

Foretaksregister:
NO 937 357 370 MVA

Rapport

Smartere transport – Møre og Romsdal: L4.1 Cyber security for et autonomt sjøverts persontransportsystem

RAPPORTNR	PROSJEKTNR	VERSJON	DATO
OC2020 A-126	302004527-8	2.0	2021-06-02

EMNEORD:
Cybersikkerhet, autonomi, cyberrisiko, risikohåndtering, persontransport, maritim

FORFATTER
Egil Wille

OPPDRAGSGIVER(E)
Møre og Romsdal fylkeskommune

OPPDRAGSGIVERS REF.	ANTALL SIDER OG VEDLEGG:
Marte Berild Hjelle	22 + vedlegg

GRADERING	GRADERING DENNE SIDE	ISBN
Åpen	Åpen	978-82-7174-402-1

SAMMENDRAG
Denne rapporten er utarbeidet på oppdrag for Møre og Romsdal fylkeskommune som del av prosjektet Smartere Transport – Møre og Romsdal, hvor hovedformål er å gjennomføre en mulighetsstudie for et helt nytt og banebrytende konsept for persontransport basert på autonome, sjøverts transportløsninger.

Ved høy grad av automasjon ombord er det avgjørende at kritiske digitale systemer i autonome passasjerferjer fungerer etter hensikten og er robuste mot uønskede hendelser. Autonomisystemenes natur gjør dem utsatt for cybertrusler, og god cybersikkerhet er dermed en forutsetning for autonom operasjon.

Basert på litteraturstudier og intervju med relevante aktører presenterer rapporten viktige utfordringer og problemstillinger knyttet til cybersikkerhet i autonome passasjerferjer. Rapporten introduserer også et sett med generelle anbefalinger for hvordan cybersikkerhet bør ivaretas, blant annet med hjelp fra relevante og etablerte rammeverk for risikohåndtering. Dette som grunnlag for videre arbeid ved en eventuell realisering av prosjektets brukercase.

MANAGEMENT SYSTEM CERTIFICATION
DNV·GL
ISO 9001 = ISO 14001
OHSAS 18001

UTARBEIDET AV	KONTROLLERT AV	GODKJENT AV
Egil Wille	Dag Atle Nesheim	Trond Johnsen
Egil Wille	Dag Atle Nesheim (Jun 2, 2021 15:07 GMT+2)	Trond Johnsen (Jun 2, 2021 15:10 GMT+2)

Historikk

VERSJON	DATO	VERSJONSBESKRIVELSE
0.1	2020-11-03	Første utkast, for intern gjennomgang
0.2	2020-11-04	Rapport til intern kvalitetskontroll med anbefalinger om forbedring
1.0	2020-11-19	Ferdigstilt versjon oversendt til oppdragsgiver for kommentarer
2.0	2021-06-02	Endelig versjon oversendt oppdragsgiver

Innholdsfortegnelse

Definisjoner og forkortelser **4**

1 Sammendrag **5**

2 Introduksjon **5**

3 Omfang **7**

4 Metode **8**

5 Relevante standarder og retningslinjer **9**

5.1 ISM-koden og generelle retningslinjer fra IMO 9

5.2 Utvalgte standarder, retningslinjer og rammeverk 9

5.3 Oppsummering av funn 11

6 Risikovurdering og -håndtering **13**

6.1 Risikoer i autonome systemer 14

7 Konklusjoner og anbefalinger **19**

8 Videre utviklingsbehov **20**

9 Referanser **22**

BILAG/VEDLEGG

[Skriv inn ønsket bilag/vedlegg]

Definisjoner og forkortelser

AIS	Automatic Identification System, system for deling av skipsinformasjon og navigasjonsdata. Data sendes mellom involverte enheter via digital VHF.
GNSS	Global Navigation Satellite System, samlebetegnelse for satellittbaserte posisjoneringssystemer som GPS, GLONASS og Galileo.
IACS	Industrial Automation and Control Systems, samlebetegnelse for industrielle automasjons- og kontrollsystemer.
IACS	International Association of Classification Societies, medlemsorganisasjon for klasseselskaper.
IDS	Intrusion Detection System, programvare eller enhet som overvåker nettverk eller systemer for å detektere uvanlig/mistenkelig aktivitet.
IMO	The International Maritime Organization, Den internasjonale sjøfartsorganisasjonen. Ansvarlig for regulering av den internasjonale skipsfarten.
Inntrengingstest	Simulering av cyberangrep under kontrollerte forhold, med hensikt å avdekke sårbarheter i et system. Også kalt penetrasjonstest eller pentest.
IPS	Intrusion Prevention System, system som aktivt stopper/forhindrer inntrenging/angrep når mistenkelig aktivitet detekteres.
ISM-koden	International Safety Management Code, et overordnet regelverk for sikker drift av skip. ISM-koden er vedtatt av IMO.
IT	Informasjonsteknologi, komponenter og programvare som lagrer, prosesserer og utveksler informasjon.
Jamming	Å forstyrre/blokkere f.eks. radiosignaler med støysignal. Kan i noen tilfeller skje utilsiktet, men gjøres vanligvis med overlegg for å gjøre et verktøy (f.eks. GPS) utilgjengelig.
Lidar	Teknologi for objektdeteksjon og avstandsmåling. Basert på refleksjon fra objekter på samme måte som radar, men benytter lys/laser istedenfor radiobølger.
OT	Operasjonsteknologi/operativ teknologi, komponenter og programvare som styrer fysiske prosesser ved hjelp av f.eks. ventiler, pumper, motorer etc.
RCC	Remote Control Center, bemannet kontrollsenter som overvåker og støtter (ubemannede) fartøy via trådløs tilkobling.
SLA	Service Level Agreement, tjenestenivåavtale.
SLAM	Simultaneous Localization And Mapping, metode for å navigere basert på sensordata fra f.eks. Lidar. Et slags kart lages og oppdateres basert på sensordata, samtidig som sensoren(e)s plassering i kartet beregnes. Brukes f.eks. av robotstøvsugere.
Spoofing	Generering av falske signaler, for å "lure" et verktøy (f.eks. GPS) til å oppgi uriktig informasjon.
VHF	Very High Frequency, et radiofrekvensområde som brukes i diverse kommunikasjonssystemer, blant annet AIS.

1 Sammendrag

Cybersikkerhet er noe alle virksomheter med digitale systemer må forholde seg til. Jo mer kritiske de digitale systemene er, jo viktigere blir det å beskytte dem. Autonome/ubemannede passasjerferjer inneholder flere kritiske digitale systemer, f.eks. navigasjonssystemer og fremdriftssystemer, som til sammen skal ivareta passasjerenes sikkerhet og en trygg seilas. Det er dermed høyst nødvendig å sørge for at disse systemene er godt beskyttet mot cybertrusler.

Både cybertrusler og digital teknologi er i kontinuerlig og rask utvikling, noe som gjør at risikobildet er i stadig endring. Det er derfor vanskelig å definere krav/barrierer som vil være "riktige" over tid. Barrierer som gir god beskyttelse i dag er ikke nødvendigvis tilstrekkelige i morgen, fordi det stadig dukker opp nye angrepsmetoder og -verktøy. For utstyr/systemer som ikke inneholder eller påvirkes av programvare, er det relativt lett å stille konkrete krav, f.eks. at materialvalg og dimensjonering må samsvare med veldefinerte standarder for en gitt anvendelse. For digitale systemer endres omgivelsene (herunder cybertrusler) såpass hurtig at det er nødvendig med en mer "fleksibel" formulering av kravene, og det er derfor mer vanlig å fokusere på hva systemene må være i stand til (altså hvilke *funksjonelle krav* som bør ivaretas), enn hvordan de må være bygd opp og hva de må inneholde (dvs. *preskriptive krav*).

Ettersom cybertrusler er i stadig utvikling og endring, er det nødvendig å jobbe kontinuerlig med cybersikkerhet. For å påse at systemene er tilstrekkelig beskyttet må man derfor jevnlig utføre cyberrisikovurderinger, og basert på disse vedlikeholde (og forbedre) cybersikkerheten. Slikt sett kommer man aldri "i mål" med cybersikkerhet, og for å unngå at trusselaktører får et "forsprang" må man ha oversikt over sitt eget risikobilde og sørge for at nødvendige sikkerhetstiltak er på plass til enhver tid.

En ubemannet eller lavt bemannet passasjerferge har begrenset med mulighet til å få hjelp fra mannskap ombord når vanskelige situasjoner oppstår, og det blir derfor spesielt viktig at autonomisystemet er pålitelig og robust mot cybertrusler. Autonomisystemet vil, i tillegg til systemer ombord, også inkludere ett eller flere RCC (remote control center), slik at kommunikasjonen mellom fartøy og RCC må være godt sikret mot både cybertrusler og andre problemer. Enkelte teknologier som brukes mye i maritim virksomhet i dag (f.eks. GPS og AIS) er veldig sårbare for jamming og spoofing, og autonomisystemer bør derfor være i stand til å opprettholde normal drift selv om slike verktøy settes ut av spill.

For å gjøre cybersikkerhetsarbeid på en systematisk og effektiv måte trengs gode systemer for vurdering og håndtering av cyberrisiko. Denne rapporten gir en oversikt over relevante problemstillinger og utfordringer knyttet til cybertrusler for autonome passasjerferjer, samt generelle anbefalinger for hvordan cybersikkerhet bør etableres og vedlikeholdes med utgangspunkt i relevante rammeverk. Diskusjonen og anbefalingene er basert på dokumentstudier og intervjuer med relevante aktører.

2 Introduksjon

Denne rapporten er en leveranse fra delprosjekt "A4.1 – Cyber security" under hovedprosjektet "Mulighetsstudie for utvikling av et fremtidsrettet system for sjøverts persontransport i byområder med sømløs kobling til andre transportformer og som øker andelen kollektivreisende", eid av Møre og Romsdal Fylkeskommune og gjennomført av SINTEF Ocean og SINTEF Ålesund.

Rapporten tar for seg relevante problemstillinger knyttet til cybersikkerhet ved utvikling, etablering og drift av et autonomt sjøverts persontransportsystem som skissert i brukercasene i A1.2, og presenterer generelle anbefalinger for håndtering av disse problemstillingene.

Cybersikkerhet er et stort fagfelt som berører mange forskjellige teknologier, bransjer og virksomheter. Koordineringsgruppen for IKT-risikobildet, bestående av Politiets sikkerhetstjeneste, Etterretningstjenesten og Nasjonal sikkerhetsmyndighet, har definert cybersikkerhet som "Cybersikkerhet omfatter tiltak for beskyttelse mot reelle og potensielle trusler som kanaliseres via IKT-infrastruktur"[1]. Med trusler menes

ifølge ISO/IEC 27005 "en potensiell årsak til en hendelse, som kan resultere i skade på system og organisasjon."[2] I cybersikkerhetssammenheng er det kanskje mest vanlig å forbinde trusler med villede handlinger fra ondsinnede aktører, men i noen tilfeller kan uønskede hendelser ha mer tilfeldige årsaker. Denne rapporten vil primært fokusere på problemstillinger knyttet til villede handlinger, men også enkelte "tilfeldige" trusler blir belyst.

For en gitt teknologi, bransje eller virksomhet gjelder det å identifisere relevante problemstillinger/trusler og jobbe med disse. Relevante standarder og anbefalinger kan langt på vei bidra til å identifisere de vanligste truslene og anbefale tiltak/barrierer mot disse, men trusselbildet er såpass komplekst og dynamisk at man må jobbe kontinuerlig med cybersikkerhet for å beskytte seg mot nye trusler/angrepsmetoder som dukker opp. Det er ikke realistisk å være fullstendig beskyttet mot alle tenkelige trusler og angrep, og aktører må derfor ofte prioritere noen sikkerhetstiltak fremfor andre. Disse prioriteringene vil primært påvirkes av risiko, men kan også påvirkes av økonomi, politiske omstendigheter, geografi, operasjonsprofil, etc.

Cybersikkerhet anses i dag for å være spesielt viktig i de fleste virksomheter, fordi cyberkriminalitet har blitt mye mer lønnsomt, og dermed utbredt, i takt med den voldsomme digitaliseringen som foregår både i næringslivet og privat. Digitalisering og bruk av ny teknologi bidrar til effektivisering og økt tilgjengelighet, men medaljens bakside er at cyberkriminelle får et mye større "volum" å angripe. Denne økte angrepsflaten har bidratt til at cyberkriminalitet har blitt en svært omfattende virksomhet med potensielt store økonomiske og sikkerhetsrelaterte konsekvenser, hvilket igjen har økt viktigheten av cybersikkerhet.

I konteksten "autonom passasjertransport på sjø" er det ikke bare snakk om IT-systemer, men også OT-systemer (Operativ Teknologi). Et autonomt fartøy inneholder systemer som påvirker fysiske tilstander og prosesser, og har dermed et betydelig (fysisk) skadepotensiale dersom disse systemene svikter eller blir utsatt for uønsket forstyrrelse eller manipulasjon. En hacker som tar seg inn i kontrollnettverket til et autonomt fartøy eller dets kontrollsenter, vil ikke bare kunne stjele og manipulere informasjon. Vedkommende vil potensielt også kunne skape driftsstans og/eller manipulere fartøyets maskineri på en destruktiv måte. Dette betyr at cyberangrep mot et slikt fartøy kan ha vesentlig alvorligere konsekvenser sammenlignet med et "rent IT-angrep", fordi de kompromitterte systemene (og deres omgivelser) i ytterste konsekvens kan volde skade på mennesker, miljø og materielle verdier.

Moderne bemannede fartøy med avanserte OT-systemer har alltid operatører i beredskap, som umiddelbart kan gripe inn i situasjoner som OT-systemene har problemer med å håndtere på egen hånd (herunder som konsekvens av cyberangrep). Denne menneskelige "nødløsningen" gjør at man kan skyve mye av ansvaret over på operatørene, slik at OT-systemene primært håndterer "normalsituasjonen", mens operatørene hjelper til/tar over i uventede og uønskede situasjoner. Ubemannede eller delvis ubemannede fartøy kan ikke benytte seg av den samme "nødløsningen", og må derfor være i stand til å håndtere vanskelige situasjoner uten lokal hjelp fra mennesker. Basert på disse krevende omstendighetene kan vi peke på to hovedforskjeller mellom bemannede og ubemannede fartøy:

- **Ubemannede eller periodisk ubemannede fartøy må ha vesentlig mer robuste og selvstendige systemer**: Aksepten for feil og /eller svikt i automasjons-/autonomisystemene vil være meget lav, slik at kravene som stilles til slike systemer (inkludert cybersikkerhetskrav) vil være mye strengere enn for bemannede fartøy. Generelle krav til autonome fartøy beskrives nærmere i L4.3, mens denne rapporten fokuserer på cybersikkerhet.
- **Ubemannede eller periodisk ubemannede vil være avhengig av administrasjon og støtte fra ett eller flere kontrollsenter (RCC), og må ha en robust/pålitelig tilkobling til dette/disse:** Selv om systemene skulle oppnå formidabel robusthet og selvstendighet, er det ikke realistisk at de vil operere fullstendig på egen hånd i overskuelig fremtid. Frem til systemene er godt utprøvd vil det uansett være viktig å ha mennesker i beredskap, og det vil inntil videre være behov for en viss grad av tilsyn fra et ansvarlig menneske. RCC vil være en kritisk komponent i det "totale" systemet (som består av flåte/fartøy og RCC), og det er derfor avgjørende at kommunikasjonen mellom fartøy og RCC er sikker og robust.

Rapporten tar for seg en gjennomgang av utvalgte cybersikkerhet-standarder og rammeverk, og presenterer eksempler på sannsynlige/tenkelige cybertrusler og anbefalinger for håndtering av disse. Følgende prosjekter, arenaer og industriinitiativ har, via intervju og/eller dokumentstudier, hatt innflytelse på aktivitet A4.1:

- CySiMS SE (IPN-prosjekt, støttet av NFR)
- RAPP-Sundbåten (Maritime Robotics).
- Zeabuz (NTNU spin-off).
- Yara Birkeland.

3 Omfang

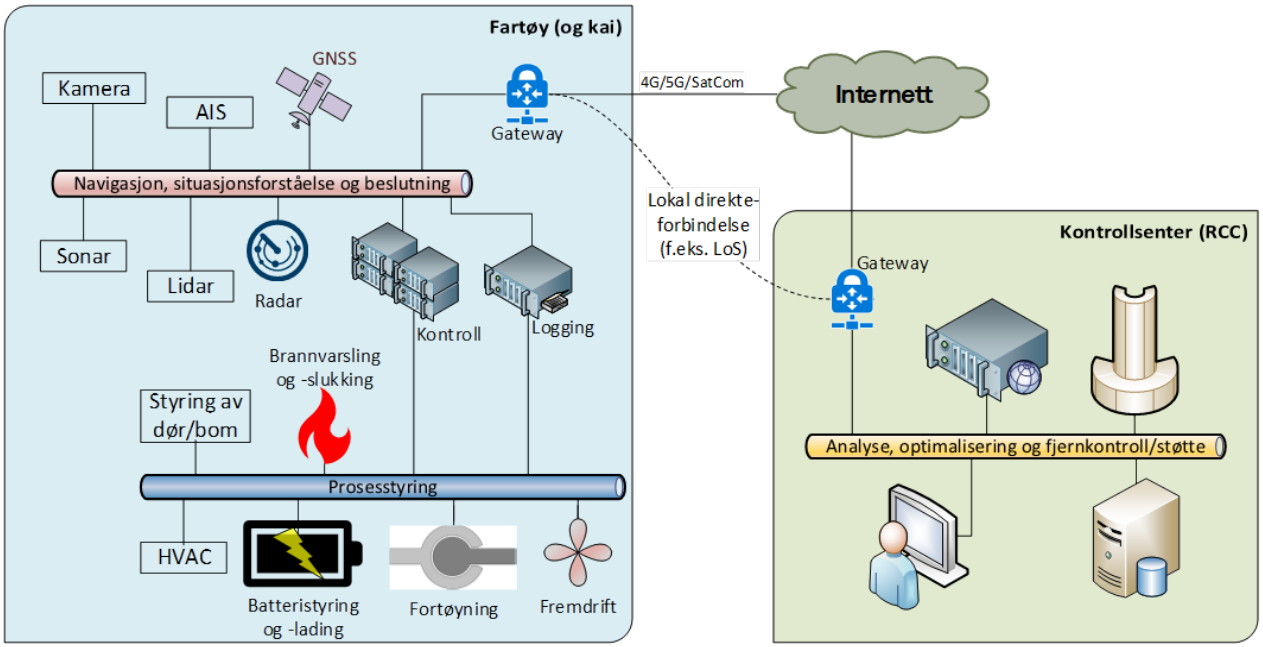
Ettersom prosjektet omhandler autonome passasjerferjer, er det naturlig å ha fokus på teknologien som muliggjør autonomi. Som beskrevet i *Smartere transport leveranse L4.3 – Sikkerhetskrav til et autonomt, sjøverts persontransportsystem* og av NFAS[3] er et autonomt skip et fartøy som kan operere mer eller mindre selvstyrt gjennom ulike grader av automasjon. Mer informasjon om autonomi og autonomigrader finnes i *Smartere transport leveranse A1.1 – Ståstedsanalyse*.

Med tanke på sikkerhet tar leveranse L4.3 for seg relevante regelverk og gir en oversikt over generelle krav som autonome/ubemannede fartøy må oppfylle basert på fysiske og operasjonsmessige parametere som lengde, antall passasjerer, effekt, hastighet, operasjonsområde, lengde på overfart etc. Når det gjelder cybersikkerhet spesifikt, som er hovedfokus for denne rapporten (og dermed et supplement til L4.3), finnes det per i dag ingen lover eller forskrifter som spesifiserer konkrete (dvs. preskriptive) krav for hverken fartøy eller det autonome skipssystemet. En særlig viktig grunn til dette er at preskriptive krav gir en veldig spesifikk beskrivelse av hvordan ulike og detaljerte krav skal etterleves (f.eks. konkrete krav som stilles ved dimensjonering av et skipsskrog som skal tåle påkjenningene som forventes ved ferdsel i en gitt type miljø). For cybersikkerhet ville preskriptive krav relativt raskt bli utdaterte, og dermed lite hensiktsmessige, ettersom cybertrusler – og muligheten til å beskytte seg mot dem er i stadig endring. Derfor er krav vedr. cybersikkerhet basert på en mer funksjonell beskrivelse, som gir mer frihet til systemansvarlig med tanke på risikoanalyse og hvordan konkrete løsninger bør bygges opp (og vedlikeholdes) for å håndtere den dynamiske problematikken rundt cybersikkerhet. Således kreves det at aktører håndterer risiko (herunder cyberrisiko) på en god måte, og viktigheten av gode og veldokumenterte risikovurderinger fremheves.

Med utgangspunkt i etablerte standarder og retningslinjer ser derfor rapporten nærmere på *hvordan* cyberrisiko bør håndteres for å oppnå tilstrekkelig cybersikkerhet. Videre forutsetter det å etablere spesifikke cybersikkerhetskrav at det foreligger et konkret system som kravene skal gjelde for, ettersom cyberrisiko påvirkes av både systemets design og omstendighetene rundt. Siden et konkret system ikke foreligger er det mer formålstjenlig og fremheve generelle anbefalinger fremfor spesifikke krav.

Automasjonssystemene som muliggjør autonom ferdsel er i kategorien operasjonsteknologi (OT), og rapporten vil derfor spesielt vektlegge cybersikkerhet i OT-systemer. I tillegg til automasjonssystemene ombord er tilkoblingen til RCC, samt teknologien og menneskene i RCC, en essensiell del av den autonome persontransportløsningen.

Figur 1 viser en grov skisse av en tenkt autonomiløsning bestående av fartøy og RCC. Rapporten vil primært ta for seg fartøysystemene, RCC og kommunikasjonskanalene mellom RCC og fartøy.



Figur 1 - Forenklet skisse av tenkt autonomiløsning. Viser ikke detaljert topologi, men et utvalg av mulige delsystemer og koblinger mellom disse (Kilde: SINTEF Ålesund).

Oppgavens omfang begrenser seg til trusler og problemstillinger som vurderes som plausible/sannsynlige på leveransetidspunktet og i relativt nær fremtid. Grunnet høy utviklingstakt både innen digital teknologi generelt og blant cyberkriminelle spesielt, er det alltid en fare for at det dukker opp nye trusler og sårbarheter som kan påvirke fagfeltet cybersikkerhet.

4 Metode

Leveransen er hovedsakelig basert på litteraturstudier og intervju med relevante aktører, samt intern ekspertise og erfaring fra andre relevante prosjekter. Intervju med følgende aktører har blitt gjennomført ifm. denne aktiviteten: Zeabuz, Kystverket, Sjøfartsdirektoratet, DNV GL, Kongsberg Maritime og Maritime Robotics.

En samling av relevante cybersikkerhets-standarder har blitt utpekt basert på en innledende gjennomgang av diverse relevante standarder samt tilbakemeldinger fra relevante aktører i intervju. Utvalget av standarder er ikke uttømmende, men gir en oversikt over de mest kjente og anerkjente i bransjen.

Risikovurdering er en essensiell aktivitet innen cybersikkerhetsarbeid og tillegges derfor en del oppmerksomhet i denne leveransen. Ettersom det ikke foreligger noe konkret system å gjøre risikovurdering av, fokuserer rapporten på generell metodikk samt å belyse viktige/relevante problemstillinger knyttet til cybersikkerhet i autonome persontransportsystemer.

Generelle anbefalinger og videre utviklingsbehov er summert opp i slutten av rapporten.

5 Relevante standarder og retningslinjer

Som nevnt finnes det per i dag ingen spesifikke tekniske krav for cybersikkerhet innen maritim virksomhet. Med det sagt stiller den internasjonale sjøfartsorganisasjonen IMO noen grunnleggende krav til håndtering av cyberrisiko gjennom den etablerte ISM-koden (International Safety Management Code).

5.1 ISM-koden og generelle retningslinjer fra IMO

ISM-koden[4] er et regelverk vedtatt gjennom den internasjonale sjøfartsorganisasjonen IMO, og definerer overordnede rammer for sikker drift av fartøy. Et sentralt krav i ISM-koden er at selskaper skal ha og anvende, et sikkerhetsstyringssystem.

ISM-koden, i kombinasjon med *Resolution MSC.428(98)*[5], krever at sikkerhetsstyringssystemene også skal omfatte cybersikkerhet etter 1. januar 2021. Dette betyr at cyberrisiko må håndteres på lik linje med andre risikoer om bord på fartøy. ISM-koden og MSC-428(98) stiller som diskutert i kap 3 ikke konkrete krav til cybersikkerhet, men belyser simpelthen bare problemstillingen og sier at cyberrisiko må håndteres.

Generelle retningslinjer for hvordan cyberrisiko bør håndteres i henhold til ISM-koden finnes i *MSC-FAL.1-Circ.3 - Guidelines on maritime cyber risk management*[6]. Dette er et sirkulær fra IMO som belyser viktige hovedtemaer og gir generelle anbefalinger for hvordan en systematisk håndtering av cyberrisiko bør gjøres. Retningslinjene er ikke særlig detaljerte eller tekniske, men refererer til mer omfattende retningslinjer og standarder for håndtering av cyberrisiko.

For autonome løsninger er det også relevant å se på IMOs retningslinjer for behandling av nyskapende design og likeverdige løsninger (MSC.1/Circ. 1455[7]) og Sjøfartsdirektoratet sitt *Rundskriv – Serie V – Føringer i forbindelse med bygging eller installering av automatisert funksjonalitet, med hensikt å kunne utføre ubemannet eller delvis ubemannet drift*[8]. Disse sier lite om cybersikkerhet, men er relevante fordi de beskriver hvordan prosessen for utvikling og anvendelse av ny teknologi bør være og hvilke krav som gjelder.

5.2 Utvalgte standarder, retningslinjer og rammeverk

Det finnes en rekke utfyllende standarder, retningslinjer og rammeverk innen cybersikkerhet, og flere av disse er relevante og anerkjente innen maritime virksomheter. De kan variere i format, detaljnivå og systemfokus (f.eks. er noen først og fremst egnet for IT-systemer, mens andre er mer tilpasset OT), men de mest populære og kjente standardene har stort sett det samme grunnleggende innholdet.

Tabell 1 summerer opp noen utvalgte standarder/retningslinjer/rammeverk som kan være relevante/nyttige i cybersikkerhetsarbeid knyttet til et autonomt sjøverts persontransportsystem. Utvalget er ikke uttømmende, men gir en oversikt over standarder/retningslinjer/rammeverk som basert på intervju med aktører, er godt kjent og vel ansett.

Tabell 1 - Oversikt over utvalgte relevante standarder og retningslinjer

Standard/referanse	Beskrivelse/kommentar
BIMCO et al., The Guidelines on Cyber Security Onboard Ships[9]	Retningslinjer for cybersikkerhet om bord på skip, forfattet av en gruppe internasjonale shippingorganisasjoner. Formålet med retningslinjene er å hjelpe aktører med å utvikle sin egen metodikk for håndtering av cybertrusler på skip. Metodikken er basert på prinsippene *Identify*, *Protect*, *Detect*, *Respond* og *Recover*, og det refereres blant annet til National Institute of Standards and Technology sitt Cybersecurity Framework (NIST CSF)[10], som er basert på de samme prinsippene. Retningslinjene påpeker at risikohåndteringen vil være både fartøy- og selskapsspesifikk, og gir en risikobasert fremgangsmåte for å identifisere og håndtere cybertrusler. Det legges vekt på viktigheten av å ha en god forståelse for egne systemer og omstendighetene de opererer i, f.eks. roller og avhengigheter i verdikjeden, trusler, sårbarheter og angrepsmetoder. Grunnleggende viktige temaer er godt dekket, og oppgitt fremgangsmåte kan være nyttig for å etablere og vedlikeholde et godt sikkerhetsstyringssystem i henhold til ISM-koden. Retningslinjene er i all hovedsak funksjonsbaserte og fokuserer primært på *hva* som må gjøres, ikke *hvordan*.
IEC 62443-serien[11]	En serie av standarder, tekniske rapporter (TR) og tekniske spesifikasjoner (TS) med særlig fokus på å inkludere IACS (Industrial Automation and Control Systems, også kjent som OT-systemer) i cybersikkerhetsarbeidet. Serien gir veiledning om hvordan *Cyber Security Management System* (CSMS) for IACS skal utvikles og vedlikeholdes, og spesifiserer i tillegg krav for både CSMS og systemer/komponenter. IEC 62443 har risikodrevet tilnærming og vektlegger blant annet sikkerhetsrisikovurdering for systemdesign. Risikovurderingen av et gitt (del-)system bidrar til å angi et fornuftig sikkerhetsnivå, som igjen angir hvilke av de oppgitte kravene som bør gjelde. Høyere sikkerhetsnivå betyr strengere krav. Serien kan benyttes mot diverse systemer og sektorer og har fått bred anvendelse (f.eks transportsektor, energisektor og maritim sektor). De store klasseselskapene har godt kjennskap til denne serien og flere av dem har basert sine cybersikkerhetskrav på blant annet IEC 62443. IEC 62443-serien er organisert i fire deler: • Generelt (62443-1) • Policy og prosedyrer (62443-2) • System (62443-3) • Komponent (62443-4) IEC 62443-serien er særlig relevant for autonome systemer, som er en form for OT-systemer.
ISO/IEC 27000-serien[12]	Kjent og utbredt standardserie for å ivareta IT-sikkerhet. Standardene i serien adresserer styringen av IT-systemer for å påse sikker håndtering (lagring, utveksling og manipulering) av informasjon ved hjelp av *Information Security Management Systems* (ISMS).

	Serien fokuserer først og fremst på IT-systemer, og ikke tilstrekkelig for å håndtere cybersikkerhet for autonome persontransportsystemer. Den vil likevel være høyst relevant, ettersom et autonomt persontransportsystem vil inneholde og/eller integreres med IT-utstyr.
NIST CSF	Et cybersikkerhetsrammeverk (*Cyber Security Framework*, CSF) utgitt av *National Institute of Standards and Technology* (NIST), som gir veiledning for hvordan små og store bedrifter kan håndtere cybertrusler på en systematisk måte. Fremgangsmåten som beskrives er i stor grad risikodrevet. Rammeverket er basert på eksisterende standarder og retningslinjer, og tar utgangspunkt i prinsippene *Identify*, *Protect*, *Detect*, *Respond* og *Recover*. Opprinnelig var rammeverket laget for aktører som leverer og opererer kritisk infrastruktur, men går for å være relevant for "de fleste". NIST CSF refererer til blant annet ISO 27000 og IEC 62443 Relevant og nyttig for både OT- og IT-systemer.
NSMs Grunnprinsipper for IKT-sikkerhet[13]	Et sett med prinsipper og tiltak som anbefales av Nasjonal Sikkerhetsmyndighet (NSM) for å beskytte informasjonssystemer. Prinsippene og tiltakene er et utvalg basert på hva NSM mener er mest relevant for norske virksomheter, og er basert på hovedprinsippene *Identifisere og kartlegge*, *Beskytte og opprettholde*, *Oppdage* og *Håndtere og gjenopprette*. Risikodrevet sikkerhetsarbeid står sentralt. Grunnprinsippene refererer til blant annet ISO/IEC 27000-serien og NIST CSF. Grunnprinsippene fokuserer mest på teknologiske og organisatoriske tiltak, og omtaler i liten grad tiltak for fysisk sikkerhet og det menneskelige perspektiv. Grunnprinsippene er først og fremst relevante for IT-systemer og er kun delvis egnet for beskyttelse av OT-systemer.
Krav og anbefalinger fra klasseselskaper	Klasseselskaper er uavhengige kontrollorganer som blant annet inspiserer og godkjenner skip og offshoreinstallasjoner, for å ivareta og bedre sikkerhet i maritim virksomhet. Flere av klasseselskapene har egne notasjoner/sertifiseringer innen cybersikkerhet, hvor det er mulig å dokumentere at et system innfrir gitte krav til cybersikkerhet. Eksempelvis har DNV GL en notasjon som kalles *Cyber Secure*, hvis krav i stor grad er basert på IEC 62443. De fleste klasseselskapene har også publisert relevante anbefalinger/retningslinjer for cybersikkerhet og for autonome fartøy.

5.3 Oppsummering av funn

De fleste standardene/rammeverkene i tabellen over tar utgangspunkt i hovedfunksjonene *identify*, *protect*, *detect*, *respond* og *recover* i en eller annen form. NSMs Grunnprinsipper for IKT-sikkerhet har norske versjoner av disse begrepene i sine kategorier "*Identifisere og kartlegge*", "*Beskytte og opprettholde*", "*Oppdage*" og "*Håndtere og gjenopprette*". Disse funksjonene må ivaretas for å sikre at en organisasjon evner å ikke bare unngå, men også håndtere uønskede hendelser på en god måte. Det er selvsagt ønskelig at så mange trusler som mulig skal stoppes *før* de skaper problemer, men det er vel så viktig å ha god beredskap slik at problemer som likevel oppstår kan detekteres og håndteres så tidlig og effektivt som mulig, og helst før de eskalerer.

Et annet viktig fellestrekk for standardene/rammeverkene er at de vektlegger viktigheten av kontinuerlig sikkerhetsarbeid. At cybersikkerhetsarbeid ikke tar slutt er en naturlig konsekvens av at digital teknologi er i rask utvikling og at cyberkriminelle jobber iherdig hver eneste dag for å finne nye sårbarheter og angrepsmetoder. Trussel- og sårbarhetsbildet er i stadig endring, og "alle" kan bli utsatt for angrep og

angrepsforsøk. For å være godt beskyttet er man dermed pent nødt til å følge med på endringer i risikobildet og tilpasse seg disse.

Rammeverkene er ikke ment å erstatte organisasjoners styringsprosesser, men heller supplere og bidra til at viktige temaer belyses og håndteres. Det beste risikohåndteringssystemet er det som en bedrift er i stand til å følge og vedlikeholde, og det bør derfor være kjent og håndterlig. Et system som bedriften selv har utformet (med inspirasjon fra gode rammeverk) vil trolig fungere bedre enn et som oppfattes som nytt og ukjent.

For autonome systemer er det et mål at mennesker skal utgjøre en mindre del av totalbildet, og til en viss grad erstattes av avansert kontrollsystemteknologi. For å oppnå dette kreves mye mer pålitelige systemer enn det som finnes på vanlige bemannede fartøy i dag. Systemene skal ikke bare håndtere "vanlig drift" på en god måte, de må også være i stand til å ta gode og riktige avgjørelser i uforutsette og uønskede situasjoner. At de er operative og tilgjengelige til enhver tid er naturlig nok også avgjørende. Det vil derfor være nødvendig å stille svært strenge krav (inkludert cybersikkerhetskrav) til komponenter og systemer som utgjør den tekniske løsningen.

Det har liten hensikt å definere spesifikke/detaljerte cybersikkerhetskrav før en konkret teknisk løsning er skissert, ettersom nødvendige/fornuftige tiltak/barrierer avhenger av (blant annet) systemets design. Viktigheten av å beskytte forskjellige komponenter og systemer bestemmes blant annet av hvor kritiske de er for den totale løsningen og hvor utsatte de er for trusler. For å definere fornuftige/riktige krav er det viktig å ha god og detaljert kjennskap til systemene som skal beskyttes, deres sårbarheter og trusselbildet de skal operere i.

Standardene/rammeverkene som nevnes i Tabell 1 (og evt. andre standarder/rammeverk) kan være nyttige på veien mot en konkret kravspesifikasjon, men formulering/utvikling av krav bør altså skje parallelt med utvikling av teknisk løsning. Ettersom et autonomt sjøverts persontransportsystem vil inneholde en god del operativ teknologi (OT), er det naturlig å se på standarder som er spesielt egnet for OT, slik som IEC 62443 eller NIST CSF. Disse, og spesielt IEC 62443, ble utpekt som særlig relevante for autonome systemer i flere av intervjuene. IEC 62443 trekkes også frem som en relevant/viktig standard innen autonomi av flere klasseselskaper. Som eksempel refererer både DNV GL og ABS til IEC 62443 i sine retningslinjer for autonomi[14,15]. Standarden omtales også i *Recommendation on Cyber Resilience*[16] fra bransjeorganisasjonen IACS (International Association of Classification Societies).

Selv om teknologiske sikkerhetstiltak vil få mye oppmerksomhet ifm. autonome systemer, er det viktig å ikke ta for lett på "ikke-tekniske" tiltak og barrierer. Innenfor cybersikkerhet er det tre viktige forhold man må jobbe med:

- Menneskelige,
- Teknologiske, og
- Organisatoriske (MTO).

Disse blir ofte omtalt som "pillarene" innen cybersikkerhet, og det er viktig å vedlikeholde alle tre. I tillegg til riktige og effektive tekniske barrierer må man altså sørge for at de involverte menneskene har riktig kompetanse og at organisasjonen har gode systemer, prosedyrer og ikke minst kultur for å ivareta cybersikkerhet. Eksempelvis hjelper det lite at et fartøy har alle tenkelige cybersikkerhetsbarrierer, dersom en servicetekniker bruker en bærbar lagringsenhet uten å påse at den er "ren", eller glemmer å endre standardpassordet på en kritisk komponent. Slike sårbarheter lar seg ikke alltid håndtere med tekniske barrierer alene, det blir dermed nødvendig med organisatoriske og menneskelige barrierer i tillegg.

Dersom en autonom persontransportløsning leveres av flere forskjellige leverandører (og kanskje underleverandører), kan det være utfordrende å påse at alle parter ivaretar tilstrekkelig cybersikkerhet. Flere aktører betyr flere potensielle angrepspunkt, og det er derfor meget viktig at alle parter blir tydelig informert om hvilke krav som stilles til leveransene og prosessene rundt, samt at de forstår og forplikter seg til å innfri disse kravene.

6 Risikovurdering og -håndtering

Det kanskje viktigste fellestrekket for standardene/rammeverkene som ble beskrevet i forrige kapittel er at de alle beskriver en risikodrevet tilnærming, hvor risikovurdering er en sentral aktivitet som danner et slags utgangspunkt for sikkerhetsarbeidet. Selv om noen cybertrusler og angrepsmetoder er vanligere enn andre, er det som regel betydelige forskjeller i risikobilde fra system til system.

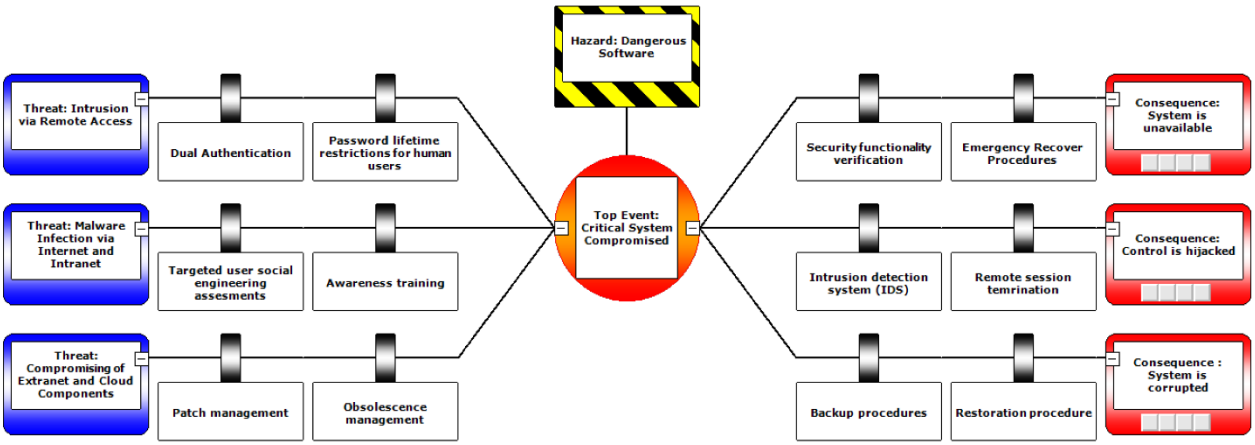
Risikobildet for et gitt system påvirkes av diverse faktorer, blant annet type virksomhet, systemdesign, politiske omstendigheter og geografi. Cyberrisikobildet er i tillegg veldig dynamisk fordi teknologien er i stadig utvikling samtidig som cyberkriminelle jobber intenst med å finne og utnytte sårbarheter. Leverandører og utviklere kan ikke bare fokusere på å forbedre funksjonalitet og effektivitet i systemene sine, de må også vedlikeholde systemenes cybersikkerhet etter hvert som nye trusler og sårbarheter dukker opp. Med et så komplekst og dynamisk risikobilde er det ikke realistisk å definere barrierer som passer for "alle", og den anbefalte praksisen er derfor å gjøre seg kjent med sine egne risikoer (gjennom risikovurderinger) for så å basere cybersikkerhetsarbeidet på disse.

Det finnes forskjellige metoder for å identifisere og vurdere risiko. Virksomheter kan bruke ulike rammeverk (f.eks. ISO/IEC 62443-3-2, ISO/IEC 27005, NIST SP 800-30[17]) til å utvikle/forbedre sin metode. Viktigere enn valg av rammeverk er at metoden er håndterlig og passer for virksomheten, slik at risikovurderingen fungerer etter hensikten og muliggjør identifisering, diskusjon og håndtering av risikoer.

Prosessen med kontinuerlig vurdering og håndtering av risiko er omfattende, og grundige beskrivelser av denne regnes ikke som en del av denne leveransens omfang. Mer info om risikovurdering og -håndtering finnes i de nevnte rammeverkene, mens påfølgende avsnitt summerer opp viktige hovedpoenger.

For å kunne håndtere identifiserte risikoer på en systematisk måte er det nødvendig å sortere/kategorisere dem på en måte som gjør det mulig å prioritere videre oppfølging. En vanlig fremgangsmåte er å gjøre en slags kvantisering av risikoen forbundet med en tenkt uønsket hendelse, basert på en formening om *sannsynligheten* for at en uønsket hendelse inntreffer og *konsekvensen* dersom den skulle inntreffe. Kombinasjonen av sannsynlighet og konsekvens avgjør en uønsket hendelses risiko, som igjen er med på å bestemme hvordan risikoen skal håndteres. Innen cybersikkerhet kan det være ekstra utfordrende å si noe om sannsynligheten for en uønsket hendelse, ettersom det finnes lite statistikk om uønskede hendelser som forårsakes av ondsinnede angripere, sammenlignet med uønskede hendelser som utløses av tilfeldige årsaker. En måte å håndtere dette på er å estimere sannsynlighet basert på angriperens mulighetsvindu, ressurser og motivasjon, som beskrevet i *CySiMS SE – D2.1 Expanded risk and CBA methodology*[18].

I tillegg til å "kvantisere" risikoen tilknyttet de forskjellige uønskede hendelsene, er det nødvendig å forstå "mekanismene" til de uønskede hendelsene, altså hvilke trusler/årsaker som er involvert, hvordan de kan utløse en uønsket hendelse og hva konsekvensen(e) av den uønskede hendelsen vil/kan være. En populær metode for å modellere uønskede hendelser er å lage et såkalt sløyfediagram (bow tie), som gir en grafisk fremstilling av mulige hendelsesforløp fra årsak (venstre side av sløyfen) til uønsket hendelse (knuten) til utfall (høyre side av sløyfen). Et sløyfediagram trenger ikke bare vise hvordan en uønsket hendelse forløper seg, det kan også vise konkrete barrierer som stopper/motvirker hendelsesforløpet. Barrierer kan være både på årsakssiden (for å redusere sannsynlighet) og på utfallsiden (for å redusere konsekvens). Sløyfediagram kan være et nyttig hjelpemiddel for å estimere risiko, samtidig som det kan bidra til å avdekke hvor barrierer bør innføres hvis risikoen er for høy. Figur 2 viser et eksempel på sløyfediagram for cyberrisikovurdering, hentet fra DNVGL-RP-0496[19].



Figur 2 - Eksempel på sløyfediagram for cyberrisikovurdering, fra DNVGL-RP-0496

Når relevante risikoer er identifisert og vurdert, må organisasjonen avgjøre hvordan de skal håndteres. Dette bestemmes ut ifra blant annet alvorlighetsgrad, risikotoleranse og kostnad. Det er i hovedsak fire forskjellige måter å håndtere risiko på[20]:

- **Unngå**: Å unngå aktiviteter eller situasjoner for å "fjerne" risikoen de medfører. Man kan f.eks. velge å unngå en risiko hvis kostnadene forbundet med risikoreduksjon er for store. Å unngå risiko innebærer ofte å velge en alternativ løsning hvor risikoen ikke inngår, eller å rett og slett ikke utføre aktiviteten eller prosjektet.
- **Redusere**: Risiko kan reduseres ved å innføre barrierer. Barrierene reduserer risiko ved å forebygge, oppdage eller reagere på uønskede hendelser. Noen barrierer kan påvirke flere risikoer, noe som i de fleste tilfeller er ønskelig/positivt. Men det finnes også tilfeller hvor en barriere som reduserer risiko ett sted, kan øke risiko et annet sted, så det er viktig å være bevisst på alle avhengigheter mellom risikoer og barrierer.
- **Overføre/dele**: Risiko kan overføres til/deles med andre parter gjennom formelle avtaler. Forsikring er en populær måte å overføre risiko på, det samme gjelder tjenesteutsetting.
- **Akseptere**: I enkelte tilfeller kan organisasjonen velge å ikke gjøre noe for å påvirke risikoen. Det kan f.eks. skyldes at det ikke finnes andre alternativer (enn å akseptere risikoen), eller at alternativene er for kostbare i forhold til forventet effekt

Å avgjøre hvordan de forskjellige risikoene skal håndteres innebærer å veie forskjellige hensyn opp mot hverandre, og beslutningene påvirkes primært av risikonivå (hvor "alvorlig" er hver enkelt risiko?) og kostnad (hva er estimert kostnad for å innføre/ikke innføre et konkret tiltak?). CyCiMS CBA presenterer en metodikk for å gjøre en kost-nytte-analyse (CBA) for sikkerhetstiltak, som kan gi et bedre beslutningsgrunnlag for valg av tiltak.

Etter implementering av valgte barrierer ventes den totale risikoen å være redusert, og organisasjonen har god oversikt over risikobildet. Over tid vil risikobildet imidlertid endre seg (først og fremst på grunn av endringer i trusselbildet), og det er derfor nødvendig å gjøre risikovurdering regelmessig. En vanlig anbefaling er at risikovurdering bør gjøres hvert år eller ved betydelige systemendringer. Eksempelvis sier kraftberedskapsforskriften[21] at risikovurderinger skal minimum gjennomgås årlig og oppdateres ved behov.

6.1 Risikoer i autonome systemer

Bemannede og ubemannede/autonome fartøy vil ha mange av de samme cyberrisikoene, men noen risikoer vil være høyere for et ubemannet fartøy. Blant annet løsningens design og fartøyets autonominivå vil ha betydelig innvirkning på hvor høy en gitt risiko er. Eksempelvis vil et fartøy som i all hovedsak er fjernstyrt

(uten nevneverdig situasjonsforståelse og beslutningsevne) få større problemer hvis det mister kontakt med RCC enn et fartøy som kan ta avgjørelser på egen hånd og seile trygt til nærmeste kai.

Autonome/ubemannede passasjerferjer er ny og banebrytende teknologi og kan av den grunn bli et attraktivt mål for hackere som primært er motivert av nysgjerrighet ("er det mulig å bryte seg inn?") og kanskje et håp om å være de første som får det til. Det er ikke nødvendigvis snakk om de mest kompetente og ressurssterke aktørene, men det er sannsynlig at en betydelig gruppe "glade amatører" vil bruke en del tid på å utforske systemet og dets sårbarheter, og kollektivt utgjøre en betydelig trussel.

Tabell 2 inneholder eksempler på uønskede hendelser som kan være særlig relevante å diskutere ifm. risikovurdering for en ubemannet passasjerferje. Eksemplene er ikke uttømmende, og utvalget er basert på intervju og litteraturstudier og tar for seg problemstillinger som fremstår som særlig relevante/interessante for autonome systemer.

Tabell 2 - Oversikt over angrep/hendelser/trusler som kan være relevante temaer å diskutere ifm. risikovurdering for et autonomt sjøverts persontransportsystem.

Uønsket hendelse	Beskrivelse/kommentarer
Jamming av GNSS-signal (f.eks. GPS)	Signalene som mottas fra GNSS-satellitter er så svake at de lett kan forstyrres eller "overdøves" av innretninger som sender ut støysignaler med samme frekvens, slik at GNSS-mottakeren mister evnen til å fastslå posisjonen sin. Dette kalles jamming, og kan gjøres av "hvem som helst" med enkelt/billig utstyr. Slik jamming er ulovlig i Norge, men utstyr for jamming er relativt lett å få tak i og kan kjøpes for noen hundrelapper. De brukes blant annet av kriminelle for å unngå at andre kan se hvor de befinner seg. <u>Mulige tiltak:</u> Unngå for stor avhengighet til GNSS. Anvend andre teknologier for posisjonsreferanse (hydroakustikk, lidar SLAM, radar etc.) som supplement/alternativ til GNSS.
Spoofing av GNSS-signal	Spoofing betyr å sende ut tolkbare, men uriktige signaler, og på den måten "lure" GNSS-mottakeren til å oppgi en annen posisjon enn den virkelige. Hvis et fartøy utsettes for spoofing og ikke detekterer at signalene er uriktige, kan konsekvensene bli betydelige. Spoofing krever mer avansert utstyr og kompetanse enn jamming, men er relativt enkelt å få til for amatører, med utstyr som ikke behøver å koste noe mer enn et par tusenlapper. <u>Mulige tiltak:</u> Unngå for stor avhengighet til GNSS. Viktig at spoofede signaler detekteres og ignoreres. Anvend andre teknologier for posisjonsreferanse (hydroakustikk, lidar SLAM, radar etc.) som supplement/alternativ til GNSS.
Spoofing av AIS-signal	AIS er en teknologi som gjøre det mulig for fartøy å dele posisjonen sin med andre fartøy via radiosignaler (VHF). Systemet har ingen autentisering eller kryptering, så det er relativt enkelt å spoofe disse signalene. En angriper kan f.eks. sende falske AIS-signaler som "påstår" at det befinner seg en rekke fartøy i farvannet rundt en autonom passasjerferje. <u>Mulige tiltak:</u> Unngå for stor avhengighet til AIS. Viktig at spoofede signaler detekteres og ignoreres. Anvend andre teknologier (radar, Lidar, kamera etc.) for situasjonsforståelse som supplement/erstatning.
Tap av kommunikasjon mellom fartøy og RCC	Kommunikasjonen mellom fartøy og RCC kan falle bort av forskjellige årsaker, og det er ikke realistisk å forvente at en tilkobling skal ha 100% oppetid. Det er derfor viktig å ha en eller flere reserveløsninger, slik at kommunikasjonen kan opprettholdes selv om en av tilkoblingene svikter. De redundante tilkoblingene må være forskjellige og uavhengige, for å unngå at de blir rammet av samme problem. Systemet bør også være forberedt på at kommunikasjonen kan falle bort fullstendig på tross av redundante linjer. <u>Mulige tiltak:</u> Sørg for å ha redundante løsninger med færrest mulig likheter/avhengigheter. Minst to ulike teknologier, f.eks. satellittkommunikasjon og 5G. Lokal kommunikasjon (uavhengig av "ekstern" infrastruktur) som en av de redundante løsningene.

Begrenset ytelse i 4G- eller 5G-nett	"Åpne nett" (f.eks. 4G/5G) kan få kapasitetsproblemer dersom en stor gruppe forbrukere genererer mye datatrafikk i et lite område. En stor folkeansamling i nærheten av et autonomt fartøy kan tenkes å generere så mye datatrafikk at det går ut over kvaliteten på fartøyets RCC-tilkobling. <u>Mulige tiltak:</u> Still tydelige krav til leverandør av telekommunikasjon i form av f.eks. en tjenestenivåavtale (SLA). Ha redundante kommunikasjonslinjer til RCC som ikke rammes av samme problem.
Lasersabotasje mot Lidarsensor	Lidarsensorer kan være sårbare for sabotasje fra laserlyskilder. Den enkleste angrepsmetoden er en slags "jamming", hvor laserlys enkelt og greit rettes mot sensoren for å "blende" den (saturation attack). En annen angrepsmetode er en form for spoofing, hvor lasersignaler sendes mot Lidar-sensoren på en måte som lurer den til å "se" ikke-eksisterende objekter. Et slikt spoofing-angrep kan tenkes å fremkalle plutselige manøvrer, eller få et fartøy til å stanse helt, selv om det i realiteten er klar bane. <u>Mulige tiltak:</u> Bruk flere forskjellige teknologier for situasjonsforståelse, slik at fartøyet kan både detektere og håndtere bortfall og sabotasje.
Komponent/enhet "plantet" om bord eller ved kai	Angripere kan av forskjellige årsaker ønske å plante enheter om bord på fartøyet eller ved kai, for å bruke dem til å gjøre rekognosering og/eller utføre angrep. En godt skjult enhet gir angriperen anledning til å "være tilstede" over lengre tid uten å bli oppdaget, slik at vedkommende lettere kan bli kjent med driften og planlegge/utføre angrep. <u>Mulige tiltak:</u> Sørg for at det er fysisk vanskelig å plante/skjule uvedkommende innretninger. Gjennomfør regelmessige inspeksjoner for å avdekke eventuelle uregelmessigheter.
Angriper tar kontroll over PA-anlegg	Selv om et PA-anlegg (Public Address, høyttalersystem for å gi talebeskjeder til passasjerer) ikke har noen viktig funksjon i den tekniske persontransportløsningen, er det et system som kan skape betydelige problemer i "feil hender". Hvis en angriper får til å sende falske meldinger via PA-anlegget kan konsekvensene i verste fall bli like store som ved mer "tekniske" angrep. <u>Mulige tiltak:</u> Sikre PA-anlegg på lik linje med fartøyets øvrige systemer.
Passasjer kobler seg til nettverk om bord eller ved kai	Det er viktig å påse at uvedkommende ikke har anledning til å koble seg til enheter nettverk som er tilknyttet fartøyets OT-systemer. Dersom fartøyet har trådløst gjestenettverk må dette være satt opp slik at det ikke går an å få tilgang til OT-nettverk via gjestenettet. <u>Mulige tiltak:</u> Unngå unødvendig trådløs kommunikasjon i OT-systemer. Sørg for at OT-nettverk om bord ikke er fysisk tilgjengelig for passasjerer. Eventuelle ethernetporter og andre tilgangspunkt bør være godt sikret, ikke bare plassert bak et lokk/deksel.

Bortfall av RCC	Vurder nøye risikoen for at hele RCC kan falle bort. Kan hele RCC rammes av en og samme uønskede hendelse, f.eks. strømbrudd, brann, flom, etc.? Hvordan vil det kunne påvirke fartøy i drift? Mulige tiltak: Designe RCC slik at det er mest mulig robust mot uønskede hendelser som kan skape bortfall (gode systemer for å detektere, unngå og bekjempe brann, nødstrøm, etc.). Ha flere RCC, med færrest mulig felles avhengigheter.
Kompromittert RCC-klient	Hvis en angriper på en eller annen måte får kontroll over en operatørstasjon i RCC, vil vedkommende potensielt kunne gjøre stor skade. Både sannsynligheten for og konsekvensen av et slikt angrep vil avhenge av systemets design og hvilke sikkerhetsbarrierer som er på plass. Mulige tiltak: God deteksjon av uønskede tilkoblinger til RCC-enheter (f.eks. brannmur, IDS/IPS). Sørg for at RCC-enheter ikke brukes til private formål.
Uvedkommende får fysisk tilgang til RCC	Angripere kan bruke forskjellige metoder for å få tilgang til enheter eller nettverk som befinner seg i RCC. De kan for eksempel tenkes å utgi seg for å være servicepersonell (rørlegger, renholder, elektriker, leverandør av frukt, etc.) for å få innpass, for så å tukle med systemkomponenter og/eller plante eget utstyr. Andre metoder for å få uberettiget tilgang kan være bestikkelse av ansatte eller fysisk innbrudd. Mulige tiltak: Ha gode prosedyrer for håndtering av eksternt personell for å hindre at uvedkommende slippes inn. Sørg for at besøkende personell er under oppsyn til enhver tid og at ansatte har tilstrekkelig kompetanse og årvåkenhet til å avdekke mistenkelig oppførsel. Ha god fysisk sikring av RCC.
Servicepersonell "tar med seg" malware inn i systemene	I noen situasjoner kan det være nødvendig at servicepersonell kobler mobile enheter (f.eks. laptop eller USB-pinne) til autonomisystemet for å gjøre oppgradering eller feilsøking. Dersom utstyret som brukes er infisert med en eller annen form for malware, kan dette spre seg til autonomisystemet og skape store problemer. Mulige tiltak: Påse at det finnes både tekniske barrierer/verktøy og gode prosedyrer for å ivareta god cyber-hygiene. Sørg for at alle relevante krav kommuniseres tydelig og følges av alle involverte parter.
4G-nett faller bort, og backup-tilkobling virker ikke	Å ha redundante og uavhengige løsninger er vel og bra, men hjelper lite dersom nødløsningen(e) ikke har tilstrekkelig pålitelighet. Skjulte feil kan gi store problemer fordi de kan forbli uoppdaget frem til krevende situasjoner oppstår. En enkelt feil kan på den måten føre til totalt bortfall av RCC-tilkobling, slik at fartøyet blir overlatt til seg selv. Mulige tiltak: Påse at redundante løsninger monitoreres og testes jevnlig. Unngå at en løsning "alltid" er primærvalget, mens en annen løsning "alltid" er backup. Veksle jevnlig mellom hvilke (redundante) løsninger som brukes, slik at eventuelle problemer oppdages og håndteres istedenfor å forbli skjulte.

Fartøy A blir bedt om å gjøre en konkret manøver, men fartøy B responderer isteden	Dersom den autonome persontransportløsningen består av mer enn ett fartøy, er det ytterst viktig å unngå at fartøyene forveksles, særlig i forbindelse med kritisk manøvrering. <u>Mulige tiltak:</u> Gode prosedyrer og opplæring for å unngå forveksling. Lokasjonsbaserte softwarebegrensninger som kun tillater en gitt manøver i et bestemt område.

I tillegg til problemstillinger som de i tabellen over, har temaet "generell sabotasje" en tendens til å dukke opp i diskusjoner rundt cybersikkerhet. Eksempler på sabotasje kan være hærverk på sensorer, utløsing av brannalarm og annen fysisk "tukling" som har til hensikt å skape problemer for driften av fartøyet. Selv om slik sabotasje ikke alltid er direkte knyttet til cybersikkerhet kan det være verdt å ta med i risikovurderingen, fordi det kan påvirke designvalg og andre ting som kan være relevant for cybersikkerheten.

Fysisk sikring og cybersikkerhet er temaer som i noen tilfeller påvirker hverandre, så de bør ses i sammenheng der det er hensiktsmessig. Både "vanlig risiko" og cyberrisiko kan påvirke designvalg (og omvendt), så sikkerhetsarbeidet bør foregå parallelt med design/utvikling slik at alle relevante hensyn kan vurderes før beslutninger tas.

7 Konklusjoner og anbefalinger

Dagens cyberrisikobilde er komplekst og kan variere mye fra system til system. Fornuftige barrierer for et gitt system er ikke nødvendigvis "riktige" for et annet system. Videre er risikobildet i stadig utvikling, slik at barrierer som gir god beskyttelse i dag er ikke nødvendigvis tilstrekkelige i morgen. All virksomhet innebærer en viss risiko, og selv om store midler går til å minimere risiko finnes det ingen garanti for at uønskede hendelser ikke inntreffer og forvolder skade. Derfor er beredskap og hendelseshåndtering også en viktig del av cybersikkerhetsarbeidet.

For å ivareta god beskyttelse må organisasjoner jobbe kontinuerlig med cybersikkerhetsarbeid, basert på regelmessig risikovurdering og generell utvikling i relevante bransjer. Å ta lærdom fra egne og andres erfaringer er også viktig. Det finnes diverse rammeverk for å etablere og anvende gode systemer for sikkerhetshåndtering, og for autonome systemer har IEC 62443 og NIST CSF blitt utpekt som spesielt relevante fordi de er tilpasset OT-systemer og tar for seg konkrete barrierer/tiltak som bør være på plass.

Autonome/ubemannede fartøy skiller seg fra tradisjonelle bemannede fartøy ved at de er mye mer avhengige av at de tekniske systemene fungerer godt, ettersom menneskelig hjelp ikke kan ytes på samme måte som på et bemannet fartøy. Dette krever at hvert enkelt delsystem er robust og pålitelig, men også at det finnes redundante og uavhengige reserveløsninger slik at kritiske funksjoner kan opprettholdes selv om enkeltkomponenter eller enkeltsystemer skulle svikte.

Selv om fartøy kan operere noenlunde selvstendig uten mannskap om bord, vil de være avhengige av menneskelige operatører som administrerer den overordnede driften, tar avgjørelser på høyt nivå, og yter støtte når det er nødvendig. Disse funksjonene er såpass viktige at stabil og pålitelig kommunikasjon mellom fartøy og RCC vil være avgjørende.

Ettersom tilkoblingen mellom fartøy og RCC er såpass kritisk, vil det være nødvendig med en eller flere reserveløsninger for denne kommunikasjonen. De redundante tilkoblingene må være uavhengige og basert på forskjellige teknologier, slik at ikke alle tilkoblingene kan settes ut av spill av samme uønskede hendelse. Hver enkelt tilkobling må alene kunne levere god nok båndbredde og latenstid til at fartøyet kan operere normalt.

Teknologier som GNSS og AIS brukes i stor utstrekning på bemannede fartøy i dag, men er så sårbare at de ikke alene bør utgjøre en viktig del av et autonomt persontransportsystem. Grunnet mangel på autentisering og kryptering kan GNSS- og AIS-signaler relativt lett spoofes, så et autonomt system som bruker slik teknologi må være i stand til å detektere når det mottar uriktig informasjon.

Ettersom autonome transportsystemer er ny og banebrytende teknologi, er det betydelig fare for at de vil få uønsket oppmerksomhet fra hackere som "for moro skyld" prøver å bryte seg inn. Spesielt nysgjerrige amatører kan tenkes å prøve seg, for å "se om det går an" og for å få anerkjennelse dersom de lykkes og blir "førstemann".

Nedenfor er en liste over noen overordnede anbefalinger for cybersikkerhet i et autonomt sjøverts persontransportsystem (rekkefølgen er tilfeldig/ikke prioritert):

- **Bruk redundante løsninger/funksjoner hyppig**: Redundante løsninger (f.eks. flere forbindelser mellom fartøy og RCC og flere teknologier for å bestemme fartøyets posisjon) har til hensikt å sørge for at kritiske funksjoner kan ivaretas på tross av tenkelige feilscenarier. Denne filosofien avhenger av at reserveløsningene faktisk fungerer når de må ta over. Det er derfor viktig at alle teknologiene/løsningene brukes jevnlig, slik at eventuelle problemer oppdages så tidlig som mulig. Hvis en løsning "aldri" er i bruk er det større fare for at den kan være rammet av skjulte problemer.
- **Gjør kontinuerlig og risikodrevet cybersikkerhetsarbeid**: Det er viktig å kjenne risikobildet til enhver tid, og siden risikobildet er i stadig endring må man gjøre regelmessige risikovurderinger. Sikkerhetstiltak oppdateres fortløpende på bakgrunn av kartlagt risiko.
- **Vær bevisst på at status i virkeligheten kan avvike fra status "på papiret"**: Autonome passasjerferjer er såpass komplekse (og konfigurerbare) systemer at det vil være meget krevende å ha full kontroll over alle detaljer til enhver tid. Selv små avvik fra spesifikasjonen kan medføre betydelig sårbarhet (f.eks. at en enhet er satt opp med standardpassord istedenfor et sterkt og unikt passord). Arbeidet med risikovurdering bør derfor inkludere praktiske aktiviteter for å sjekke virkelig status (og ikke bare forventet status). For å få god oversikt over både autonomisystemets og organisasjonens evne til å unngå og håndtere uønskede hendelser, anbefales både øvelser og inntrengingstester. (Se f.eks. NSMs Grunnprinsipper for IKT-sikkerhet for mer info om inntrengingstester). Slike aktiviteter kan i seg selv medføre betydelig risiko, og må derfor risiko vurderes og planlegges nøye før de gjennomføres.
- **Se til andre industrier**: Det foregår mye forskning og utvikling innen autonom transport, og enkelte aktører har allerede høstet store mengder verdifull erfaring. Spesielt bilindustrien har sett stor utvikling det siste tiåret, og mange av utfordringene og erfaringene derfra vil være relevante og verdifulle for autonom passasjerferjevirksomhet.

8 Videre utviklingsbehov

Det er ikke mulig å peke på spesifikke utfordringer uten å vite mer om detaljene i et konkret forslag til autonomiløsning, så videre utviklingsbehov får i denne sammenheng bli et sett med generelle aktiviteter som sannsynligvis må gjennomføres. Flere av aktivitetene vil/bør foregå samtidig, så rekkefølgen på punktene er ikke kronologisk.

- **Spesifiser en konkret løsning**: Ettersom cybersikkerhetsarbeidet i stor grad vil være basert på en konkret løsning, er det naturlig å produsere ett eller flere spesifiserte utkast til løsning på et tidlig tidspunkt. Det vil være mange hensyn (innen både cybersikkerhet og andre fagområder) som vil påvirke hvordan den endelige løsningen blir, så løsningen vil utvikle seg gradvis etter hvert som relaterte beslutninger tas.
- **Etabler et godt system for håndtering av cyberrisiko og bruk dette**: Å oppnå og vedlikeholde god cybersikkerhet krever systematisk og kontinuerlig arbeid, som igjen krever gode verktøy/rammeverk. Bruk gjerne IEC 62443 og/eller NIST CSF som inspirasjon eller utgangspunkt.
- **Finn/utvikle robuste og uavhengige reserveløsninger for kritiske funksjoner**: Å ha god redundans i kritiske funksjoner er vanlig designfilosofi også i bemannede systemer, men blir enda

viktigere for systemer som skal operere uten kontinuerlig oppsyn fra menneskelig operatør. Spesielt systemer for navigasjon, situasjonsforståelse og kommunikasjon med RCC må være svært robuste og pålitelige. På dette feltet har nok mye skjedd allerede. Relevante utstyrs- og systemleverandører må involveres, disse antas å vite mest om status for tekniske utfordringer.

- **Samarbeid med relevante myndigheter**: Som nevnt i L4.3 har Sjøfartsdirektoratet beskrevet en godkjennelsesprosess for autonome og ubemannede fartøy i sitt *Rundskriv – Serie V – Krav til dokumentasjon i forbindelse med bygging av autonome, ubemannede og/eller fjernstyrte fartøy*, hvor det blant annet legges vekt på viktigheten av grundige risikovurderinger. Dette gjelder også cyberrisikovurderinger, så det vil være naturlig å følge opp cyberrisiko på samme måte som annen risiko i godkjennelsesprosessen.

9 Referanser

[1] Koordineringsgruppen for IKT-risikobildet, (2010), Bakgrunnsnotat Cybersikkerhet. https://www.regjeringen.no/contentassets/252f869fdfac46648e41e6ca5fb0600a/cybersikkerhet_svar-med-merknader_nsm-pst-etterretningstjenesten.pdf

[2] ISO/IEC, (2018), Information technology — Security techniques — Information security risk management (ISO/IEC 27005). https://www.iso.org/standard/75281.html

[3] Rødseth, Ø.J. og Nordahl, H., (2017), Definitions for Autonomous Merchant Ships, NFAS – Norwegian Forum for Autonomous Ships. http://nfas.autonomous-ship.org/resources.html

[4] International Maritime Organization (IMO), International Safety Management Code. https://www.imo.org/en/OurWork/HumanElement/Pages/ISMCode.aspx

[5] International Maritime Organization (IMO), Resolution MSC.428(98) – Maritime Cyber Risk Management in Safety Management Systems. https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/ResolutionMSC.428(98).pdf

[6] International Maritime Organization (IMO), MSC-FAL.1/Circ.3 Guidelines on maritime cyber risk management. https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/MSC-FAL.1-Circ.3-GuidelinesOnMaritimeCyberRiskManagement(Secretariat).pdf

[7] International Maritime Organization (IMO), MSC.1/Circ.1455 – Guidelines for the approval of alternatives and equivalents as provided for in various IMO instruments.

[8] Sjøfartsdirektoratet, Rundskriv – Serie V - Føringer i forbindelse med bygging eller installering av automatisert funksjonalitet, med hensikt å kunne utføre ubemannet eller delvis ubemannet drift. https://www.sdir.no/sjofart/regelverk/rundskriv/foringer-i-forbindelse-med-bygging-eller-installering-av-automatisert-funksjonalitet-med-hensikt-a-kunne-utfore-ubemannet-eller-delvis-ubemannet-drift2/

[9] BIMCO et. al., The Guidelines on Cyber Security onboard Ships – Version 3. https://www.bimco.org/about-us-and-our-members/publications/the-guidelines-on-cyber-security-onboard-ships

[10] National Institute of Standards and Technology (NIST), (2018), Framework for Improving Critical Infrastructure Cybersecurity. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

[11] ISA/IEC 62443, https://www.isa.org/intech-plus/2019/may/new-isa-iec-62443-standard-specifies-security-capa

[12] ISO/IEC 27000, https://www.standard.no/fagomrader/ikt/it-sikkerhet/

[13] Nasjonal Sikkerhetsmyndighet (NSM), Grunnprinsipper for IKT-sikkerhet versjon 2.0. https://nsm.no/regelverk-og-hjelp/rad-og-anbefalinger/grunnprinsipper-for-ikt-sikkerhet-2-0/introduksjon-1/

[14] DNV GL, Class Guideline for autonomous and remotely operated ships (DNVGL-CG-0264).

[15] Bureau Veritas, Guidelines for autonomous shipping (Guidance note NI 641 DT R000 E).

[16] International Association of Classification Societies (IACS), Recommendation on Cyber Resilience. http://www.iacs.org.uk/news/iacs-launches-single-standalone-recommendation-on-cyber-resilience/

[17] National Institute of Standards and Technology (NIST), SP 800-30 - Guide for Conducting Risk Assessments. https://www.nist.gov/privacy-framework/nist-sp-800-30

[18] Meland, P.H. og Bernsmed, K., D2.1 Expanded risk and CBA methodology. http://nfas.autonomous-ship.org/resources/cysims-se-d21.pdf

[19] DNV GL, Recommended practice – Cyber security resilience management for ships and mobile offshore units in operation (DNVGL-RP-0496)

[20] Digitaliseringsdirektoratet, https://internkontroll-infosikkerhet.difi.no/godt-vite/risikohandtering/hva-er-risikohandtering

[21] Forskrift om sikkerhet og beredskap i kraftforsyningen (kraftberedskapsforskriften). https://lovdata.no/dokument/SF/forskrift/2012-12-07-1157