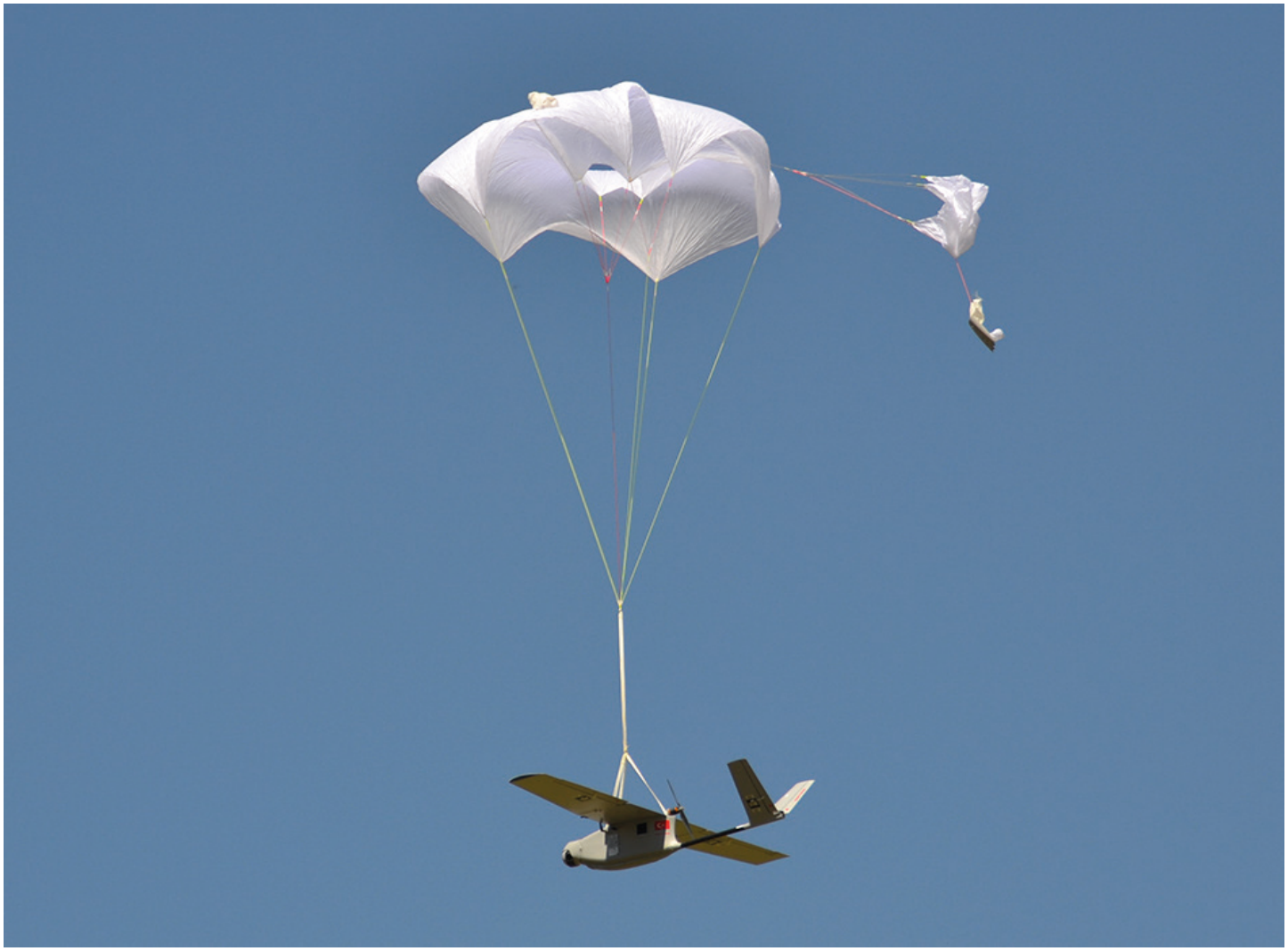
Felsäkerhet för obemannade farkoster: Metodintroduktion

ERIK BRANZÉN OCH KARIN KRAFT



FOI-R--5358--SE
ISSN 1650-1942 Januari 2023

Erik Branzén och Karin Kraft

Felsäkerhet för obemannade farkoster: Metodintroduktion

Titel	Felsäkerhet för obemannade farkoster: Metodintroduktion
Title	Fail-safety for unmanned vehicles: Introduction to Methods
Rapportnummer	FOI-R--5358--SE
Månad	Januari
Utgivningsår	2023
Antal sidor	39
ISSN	1650-1942
Uppdragsgivare	Försvarsmakten
Forskningsområde	Övrigt
FoT-område	Temaområde
Projektnummer	E716571
Godkänd av	Christian Jönsson
Ansvarig avdelning	Cyberförsvar och Ledningsteknik
Exportkontroll	Innehållet är granskat och omfattar ingen information som är underställd exportkontrollagstiftningen.

Sammanfattning

Denna rapport behandlar området obemannade farkoster med autonoma delfunktioner och metoder för ökad felsäkerhet med fokus på områdena feldetektion, feldiagnostik och felhantering. En farkosts möjlighet att utföra sitt uppdrag är begränsat av dess förmåga att förhindra, undvika, tolerera och återhämta sig från fel. Dessa fyra egenskaper kan ses som lager av åtgärder och då en förmåga brister bör nästa ta över. Felsäkerheten höjs om fler lager av åtgärder adderas för att hantera ett fel. Närvaro av fel utgör risker och deras konsekvenser måste vägas mot varandra vid design och hantering av farkosten. Rapporten innehåller de generella metoderna som utgör områdena feldetektion, diagnostik och hantering och ger, med ett nyanserat felbegrepp, en översiktsbild på lämpliga frågeställningar och arbetssätt som kan öka en farkosts felsäkerhet. En slutsats från rapporten är att mycket av forskningen kring felsäkerhet inte har varit domänöverskridande vilket har lett till olika taxonomier och ramverk för riskbedömning och felhantering. Rapporten utgör tillsammans med rapporten "*Felsäkerhet för obemannade farkoster: Domänöversikt*" en kunskapsbas och utgångspunkt för vidare forskning.

Nyckelord: UAV, AUV, UGV, USV, feltolerans, felhantering, feldiagnostik, autonoma farkoster

Summary

This report investigates unmanned vehicles with autonomous functionality and methods for increased fail safety with a focus on fault detection, diagnostics and handling. A vehicle's ability to perform during a mission is limited by its fault prevention, avoidance, tolerance and recovery capabilities. These four abilities can be seen as layers of measures and if one layer fails another should take over. The vehicles' level of fail-safety is increased if more layers of measures are added to combat a specific fault. The list of faults constitute risks whose consequences have to be handled in the design and use of the vehicle. An analysis of those risks can inform method choice in the form of technical solutions. An important conclusion from the report is that much of the research on fail safety has been domain specific, leading to divergent taxonomies as well as different frameworks for risk analysis and mitigation. Together with the report "*Fail-safety for unmanned vehicles: Domains*", this document provides a knowledgebase and a starting point for further research.

Keywords: UAV, AUV, UGV, USV, fault tolerance, fault handling, fault diagnosis, autonomous vehicles

Innehåll

1 Inledning

Denna rapport ger tillsammans med rapporten ”*Felsäkerhet för obemannade farkoster: Domänöversikt*” [1] en översiktsbild över forsknings- och teknikområdet felsäkerhet för obemannade farkoster. Syftet är att etablera en kunskapsbas och motivera för vidare forskning i syfte att öka kompetensen inom området hos totalförsvarsmyndigheterna, däribland Försvarsmakten, Försvarets materielverk (FMV) och Totalförsvarets forskningsinstitut (FOI).

Mer specifikt försöker rapporten beskriva hur en riskanalys för ett tekniskt system kan mynna ut i metodval för feldetektion, feldiagnostik och felhantering. Rapportens ytterligare syften är att nyansera begreppet fel genom att rita upp en karta över dess användning i olika kontexter samt att ge förslag till fortsatt forskningarbete inom området på FOI.

Läsaren rekommenderas att även läsa rapporten [1] för att få en komplett bild av bakgrunden och det dimensionerande problemet som motiverar forskningsområdet. FOI har forskat om obemannade farkoster under en längre tid och för en översikt över de senaste årens forskning hänvisas läsaren till [2–7].

1.1 Problemformulering

En farkosts motståndskraft mot fel är ett resultat både av designen och handhavandet. Tekniska system som ökar motståndskraften kan stödja handhavandet genom att skapa observerbarhet för felaktiga tillstånd, och även i viss mån automatisera felhanteringen. Systemen baseras på en mängd tekniker, exempelvis klassiska statistiska metoder och maskininlärning, och rapporten presenterar metoder för att välja verktyg givet ett visst fall.

Med den ökande komplexiteten som följer av utvecklingen av större och mer uthålliga obemannade farkoster ökar ofta behovet av felsäkerhet. Behovet reflekterar den ökade mängden av systeminteraktioner i cyberfysiska system där hårdvara och mjukvara samspelar. Genom att integrera kartläggning av systemhälsa i mjukvara istället för att låta den tillhandahållas av människor kan farkostens autonomigrad förstärkas [8]. Det kan öka farkostens tillförlitlighet, skapa minskad risk för skada på omgivning och personer och även minskad risk för farkosten själv, samt reducera kostnader för underhåll och reparation. Detta uppnås genom att allvarliga fel undviks med hjälp av prediktionsmodeller eller genom att isolering av en riskkälla underlättar underhållsarbetet och leder till högre tillgänglighet för farkosten [9, 10]. I en felprediktion är syftet att förutspå systemets framtida hälsa. Denna prediktion kan vara viktig i det autonoma beslutsfattandet, exempelvis genom att en optimeringsalgoritm minimerar risktagande [11]. I semiautonoma farkoster kan informationen och riskbedömningen istället vidarekopplas till mänskliga aktörer som i sin tur kan ta kontroll över systemet eller ge nya instruktioner [12, 13].

Varje adderad metod för felsäkerhet i en obemannad farkost bidrar till en ökad komplexitet i delsystemen. Den ökade komplexiteten kan i sin tur generera nya riskkällor. Det är viktigt att väga den ökade felsäkerheten mot resursanvändning, enkelhet och användarvänlighet i form av reparerbarhet, samt kostnader associerade med handhavandet av farkosten. I Branzén och Kraft [1] beskrivs vanliga riskkällor för obemannade farkoster och för att fatta beslut om implementation av tekniska lösningar behöver en heltäckande riskanalys genomföras. De tekniska lösningarna tar ofta formen av feldetektion, feldiagnostik och felhantering vilket är det som denna rapport fokuserar

på.

Syftet med att integrera hälsounderhållande funktioner är att göra farkosten robust och felsäker, vilket innebär att den ska fungera enligt kravställningen i oförutsedda situationer som uppstår i miljön där den är aktiv respektive hantera fel innan de påverkar farkostens funktion.

Fel kan undvikas, förhindras, tolereras, eller återhämtas från och en högre felsäkerhet innebär att farkosten har flera lager av felhanteringsåtgärder.

1.2 Rapportstruktur

Rapportens struktur utgår från det arbete som kan bedrivas för att först kartlägga fel och risker och sedan identifiera de lösningar, tekniska som icketekniska, som minimerar och åtgärdar felet eller risken. Först presenteras en begreppsöversikt där olika typer av fel särskiljs samt illustreras. Efterföljande kapitel illustrerar några arbetssätt för att öka ett systems felsäkerhet med metoder tagna från olika forsknings- och teknikdomäner. Teknikdelområdena feldetektion, feldiagnostik och felhantering beskrivs sedan och rapporten avslutas med en diskussion om metodval för olika typer av fel samt ett förslag på forskningsinriktning.

1.3 Avgränsningar

Rapporten fördjupar sig inte i enskilda systems behov av felsäkerhet utan beskriver problem för en generell farkost. Behov för olika domäner, samt diskussion kring olika farkosttypers riskkällor presenteras i domänrapporten [1].

Rapporten behandlar endast ytligt sådana fel som är direkt orsakade av den mänskliga faktorn. Rapporten fokuserar på de tekniska lösningar som är ämnade att ge farkoster förmågan att bedöma sin hälsa, som funktion av de fel som potentiellt inträffat. Fel som är direkt orsakade av en antagonist berörs inte heller. Extern påverkan, i form av exempelvis väderförhållanden och underlag, skiljs här från antagonism, där en tydlig avsikt från en medveten motståndare orsakar felet. Extern påverkan kan leda till interna fel och en tydlig skiljelinje kan därför inte dras mellan dessa.

I rapporten presenteras även en beskrivning av arbetet kring riskanalys och riskbedömning av fel, men området beskrivs endast kortfattat. Syftet med riskanalysen är att placera en farkost i en uppdragskontext där påverkan av fel vägs mot andra faktorer. Den tekniska implementationen av feldetektion, -diagnostik och -hantering behöver en riskanalys som ingångsvärde. Eftersom fokus i denna rapport ligger på fel handlar den främst om metoder för felhantering, vilket är en del av den generellare riskhanteringen.

Handhavande och underhållsarbete beskrivs inte i detalj i rapporten. Tekniska system som stöd för underhåll är dock en viktig del av forskningsområdet diagnostik och beskrivs översiktligt i kapitel 4.

2 Begreppsöversikt

Detta avsnitt innehåller definitioner av nyckelbegrepp som används i rapporten, samt en diskussion kring behovet av att nyansera dessa begrepp.

2.1 Fel och risk

Ordet *fel* kan ha olika betydelser beroende på sammanhang. Det kan användas som substantiv, adjektiv och adverb och exempel på dessa användningar i vardagsspråk är ”styrsystemet innehåller ett fel”, ”styrsystemet skickade fel signaler” och ”styrenheten räknade fel”. Alla dessa exempel är vanliga och korrekta användningar av begreppet i dagligt tal, men de varierande användningarna gör att definitionen av *fel* och *felhantering* har olika innebörd för olika personer och olika forskningsområden. Till detta kommer effekten av att flera ord i engelskan, som ”fault”, ”malfunction” och ”failure”, översätts till ”fel” på svenska. Vid användning i forskningssammanhang behöver det fel som studeras i det specifika fallet och metoden definieras. Detta kan göras ur olika perspektiv beroende på vad som undersöks och några definitioner för fel i tekniska system beskrivs nedan.

En möjlig definition av de engelska begreppen i Isermann m.fl. [14] utgår från den påverkan som felet har på systemet:

- **Malfunction, fel, bristande förmåga**: Ett temporärt avbrott i systemets funktionalitet. Det är en avvikelse från normalt beteende som ännu inte har kritisk påverkan.
- **Fault, fel, förlust av förmåga**: En otillåten förlust av en systemegenskap med påverkan på systemet.
- **Failure, haveri**: Ett permanent kritiskt avbrott i systemets förmåga att utföra en efterfrågad funktion under förutbestämda manövreringsvillkor. Kritisk påverkan.

Fel kan även definieras i ett tidsperspektiv. Al-Assad m.fl. [15] beskriver en sådan indelning enligt följande:

- **Permanent fel:** Ett fel som består under hela systemets livslängd om ingen åtgärd görs.
- **Intermittent fel:** Ett fel vars effekter inte är närvarande hela tiden utan uppstår i vissa situationer.
- **Transient fel:** Ett fel som består under mycket kort tid och ofta uppstår slumpmässigt från miljöfaktorer.

En uppdelning av fel kan göras utifrån hur de påverkar systemet, samt var i systemet de uppstår. Gao m.fl. [16] och Sobhani-Tehrani m.fl. [17] ger följande exempel på en sådan uppdelning:

- **Sensorfel**:
  - bias: avvikelse från korrekt värde,
  - drift: ökande avvikelse från korrekt värde,

  - förlorad noggrannhet: varierande avvikelse,
  - frysning: sensorn visar samma värde,
  - kalibreringsfel: konstant avvikelse.
- **Ställdonsfel**:
  - fastlåsning: ställdonet fastnar i ett fixerat läge,
  - flytande: ställdonet bidrar ej till styrning,
  - max/min: ställdonet ger maximal eller minimal styrning oavsett kommando,
  - förlorad effekt: ställdonet tappar i kapacitet.
- **Processfel**.

Processfel inkluderar fel som uppstår i andra moduler i systemet eller i stödsystem, som exempelvis energiförsörjningen. Sensorfel karakteriseras av att de ligger i inmatningsdelen där signaler skickas in till systemet, medan fel på ställdon sker i produktionsdelen. För en mer utförlig redogörelse av felförlopp och hur de påverkar hela det tekniska systemet, se kapitel 4.1.

Fel som inträffar hos en obemannad farkost med autonoma funktioner ha en rad olika orsaker som till exempel sensorfel, yttre påverkan, mekaniska fel på ställdon eller systematiska fel. Fel kan yttra sig på olika sätt, exempelvis genom avvikande rörelse eller att uppmätta signaler och sensordata skiljer sig från ett känt eller förutbestämt normaltillstånd. Olika fel kan resultera i samma symptom. Både felaktig sensordata och effektförlust i motorn kan få farkosten att röra sig på ett avvikande sätt.

Ett annat begrepp som förekommer i litteraturen kopplad till detektion, diagnostik och hantering av fel är **risk**. En risk är en konsekvens av en händelse (internt fel, extern påverkan m.m.) associerad med en sannolikhet. En **riskanalys** innebär att konsekvenser av olika händelser värderas mot deras sannolikheter. Det finns många typer av riskmodeller. Handboken för systemsäkerhet (HSystSäk) [18] ger en utförlig modell för alla möjliggörande faktorer som leder till olyckor och denna beskrivs kortfattat i avsnitt 4.1.

2.2 Feldetektion och feldiagnostik

Begreppet diagnostik används i olika vetenskapliga domäner och är väletablerat i medicinska sammanhang. I denna rapport används diagnostik kopplat till säkerhet och hälsa för tekniska system.

Nyberg m.fl. [19] presenterar två huvudsakliga användningar av begreppet feldiagnostik för tekniska system. Den ena användningen inkluderar feldetektion, där diagnostik innebär att detektera, identifiera samt isolera eller lokalisera felet eller felen. Den andra användningen avser endast identifiering och isolering eller lokalisering av felet eller felen. Denna rapport använder sig av den senare definitionen där feldetektion särskiljs från feldiagnostik.

Diagnostik kan göras oavsett om ett system är operativt eller inte. Nyberg m.fl. [19] använder begreppen **offline** och **online**. Diagnostik online görs medan systemet är i drift. Realtidsdata används för att hitta momentana fel. Om ett akut fel uppstår kan diagnostiken förhoppningsvis upptäcka det, och det finns möjlighet att åtgärda det med en felhanteringsmetod.

Diagnostik som sker offline görs antingen innan eller efter det att systemet i fråga är operativt, det vill säga före eller efter ett uppdrag. Diagnostik som utförs före ett uppdrag kan ha till syfte att säkerställa systemets hälsa innan uppdraget börjar, exempelvis

genom tester i en kontrollerad miljö. Insamlad data från en körning kan analyseras i efterhand för att till exempel undersöka systemets hälsa eller för att leta efter orsaken till ett tidigare haveri.

Det går även att skilja på aktiv och passiv detektion och diagnostik. Vissa fel uppstår endast i särskilda situationer, vilket kräver att systemet aktivt måste påverkas för att denna typ av fel ska kunna upptäckas. Vid passiv detektion och diagnostik upptäcks fel endast genom att övervaka systemet utan att påverka det.

Detektionen och diagnostiken av fel kan i sig vara felaktiga. Detta kallas inferensfel och delas in i två grupper: falskt positiva detektioner (Typ I) och missade detektioner (Typ II). Vid en missad detektion tror systemet felaktigt att en händelse inte har inträffat när den i själva verket har det. Vid en falsk positiv detektion tror systemet felaktigt att en händelse har inträffat, trots att den inte har det.

2.3 Felhantering

Det saknas en standardiserad beskrivning av metoder för felhantering. Nedan introduceras en rad begrepp med syfte att generellt förklara hur felhantering kan utföras. Vissa metoder kan passa in under flera rubriker.

Felhantering kan göras proaktivt eller reaktivt. Syftet med **proaktiv** felhantering är att förhindra eller undvika fel. Proaktiv felhantering kan vara **preventiv**, exempelvis genom underhåll av systemet, eller **prediktiv** genom att försöka förutspå fel i förväg, till exempel genom analys av driftdata.

Syftet med **reaktiv** felhantering är att tolerera eller att återhämta sig från ett fel, genom att läka, bromsa, tolerera eller negligera felet som uppstått. Denna typ av felhantering sker i realtid, som ett resultat av att ett fel har uppstått.

Al-Assad m.fl. [15] delar in felhantering enligt följande punkter:

- **Felundvikande**: En åtgärd som syftar till att förhindra att felet inträffar.
- **Felnegligering**: Bortse från felet. Exempelvis kan riskanalysen visa på minimala konsekvener för felet eller låg sannolikhet för att felet utvecklas till något allvarligt. Då kan beslut tas att inte hantera felet.
- **Felläkning**: En åtgärd som syftar till att reparera felet så att dess påverkan på systemet upphör.
- **Felmaskering/bromsning**: En åtgärd som bromsar felet, genom att förhindra felets påverkan från att bli större eller genom att lindra konsekvenserna.
- **Omkonfigurering**: En åtgärd där systemet ändrar sitt fundamentala beteende för att kompensera för felet eller minska felets påverkan.

En **riskhantering** är det sista steget i en riskanalys och har till syfte att mildra konsekvensen eller sannolikheten för händelsen. Begreppet är starkt kopplat till **felhantering** men vissa skillnader finns. Detta resonemang utvecklas i kapitel 5.

3 Framtagning av felsäkert system

Detta kapitel beskriver översiktligt hur felsäkerheten för ett system kan stärkas samt hur felsäkerhet kan integreras i ett system från grunddesignen, genom att göra systemet både mer robust mot extern påverkan och feltolerant mot interna fel. Denna rapport fokuserar på obemannade farkoster, men metoderna i detta kapitel är generella och kan appliceras på tekniska automatiserade system i allmänhet. Kapitlet beskriver hur funktioner för feldetektion, -diagnostik och -hantering kan integreras i ett system och vilka steg arbetet består av från grundläggande beskrivning av systemet till utformningen av felhanteringen. Exempelvis är det viktigt att det finns en detaljerad och korrekt beskrivning av systemet så att fel kan kartläggas och en riskanalys kan värdera felen. Riskanalysen ligger till grund för val av metoder för detektion, diagnostik och hantering. Val av arbetsprocess för att generera den önskade felsäkerhetsnivån utgår bland annat från systemkrav och begränsningar i resurser, tid, och kunskap med mera.

3.1 Felsäkerhetsnivå

Denna rapport utgår från att ett system är utformat för att utföra en eller flera specifika uppgifter. Systemet har funktioner som är kopplade till uppgiften och tillsammans utgör dessa funktioner förmågan. För att förstå vilka faktorer som kan äventyra systemets förmåga kartläggs yttre och inre riskkällor. Dessa utgörs till exempel av både yttre störningar som exempelvis kraftig vind eller interna fel på sensorer eller aktuatorer enligt exemplen i kapitel 2. Med ökande komplexitet av uppgift behövs ofta fler och mer avancerade funktioner och nivån av felsäkerhet kan anpassas i utvecklingen och användningen av systemet. En tolerabel risknivå finns ofta definierad för olika typer av olyckor och den kan ofta översättas till felsäkerhetsnivåer för de fel som kan leda till olycka [18].

Samverkan mellan funktioner i systemet blir viktigare ju svårare och större uppgiften är. I komplexa miljöer och uppdrag är risken större för beslutsfel antingen av en operatör eller av ett internt beslutssystem. Detta skulle enligt tidigare definition utgöra ett processfel och dessa kan vara svåra att modellera för ett komplext system i en komplex miljö.

ISO-standarden för riskhantering [20] beskriver faktorer som definierar en organisations handlingsutrymme och begränsningar i olika situationer. Dessa faktorerer kan i viss mån överföras på området för denna rapport, obemannade farkoster, och även på system med autonoma funktioner i en bredare mening. Några nyckelfaktorer som utgör ett system och dess förmåga utifrån standarden är därmed:

- **Mål och beslut som fattas**. Hur är mål definierade och kvantifierade samt vilka beslut kan systemet själv fatta? Vid hög grad av autonomi fattas beslut om delmål och taktikval av systemet utan mänsklig delaktighet.
- **Förväntade resultat och utfall av förmågans applicering**. Hur är systemets förmåga utformad och vilket är det förväntade resultatet? Förmågan är utformad efter ett förväntat resultat men för ett system med autonoma funktioner är det svårt att deterministiskt kartlägga alla utfall av systemets användning.
- **Förklaringsmodeller**. Hur kan systemet beskrivas i termer av modeller, kvalitativt och kvantitativt? Ett system med autonoma funktioner kan ha inbyggda algoritmer som återkopplar insamlad data och justerar modeller i realtid.

- **Tidsomfång, rumsliga begränsningar**. När och var används systemet? Även ett system med autonoma funktioner är anpassat för att användas i specifika miljöer och fungerar inte nödvändigtvis i en godtycklig fysisk omgivning.

- **Verktyg för utvärdering av systemet och dess förmåga**. Vilken information finns tillgänglig för förståelse för systemets funktion och förmåga? För att kunna förstå hur systemet verkar behövs god kunskap om vad som är mätbart samt hur både externa och interna informationskedjor ser ut. I ett system med autonoma funktioner kan det finnas utvärderingsmetoder implementerade i systemet.

- **Resurser som används samt ansvarsbärande och dokumentation av förlopp**. Vilken information och vilka resurser används av systemet, hur ser beslutskedjor ut och var ligger ansvaret? Hur är dessa processer dokumenterade? Vilka möjligheter finns att återskapa tidigare förlopp under systemets användning? Ett system med autonoma funktioner kan dokumentera sitt förlopp och kommunicera till relevanta mottagare (människor eller andra system). I och med att systemet i viss mån fattar egna beslut bör ansvarsfrågan vara dokumenterad, tydlig och transparent.

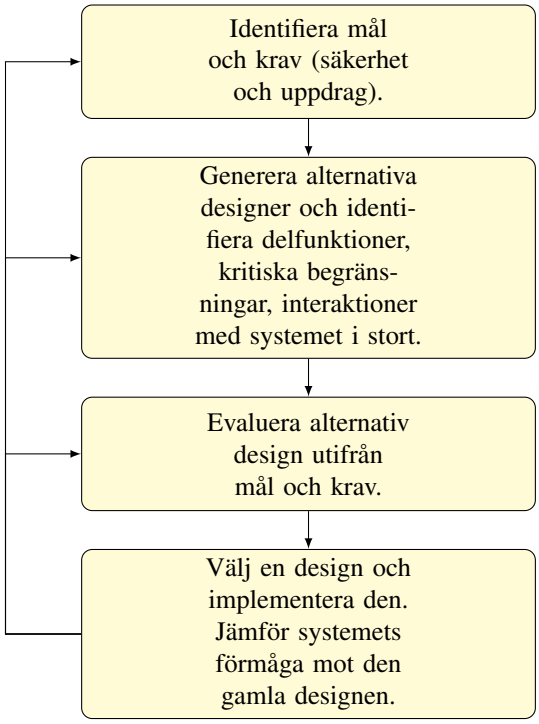
- **Relation till andra system och förmågor**. Vilka andra system, människor och organisationer samverkar systemet med? Vilka informationsutbyten görs? All samverkan mellan ett system med autonoma funktioner och andra system och människor bidrar till en ytterligare komplexitet.

I HSystSäk [18] analyseras olycksrisken utifrån att systemet och dess användning bryts ned i tre faktorer som tillsammans kan generera en **vådahändelse** som vid **exponering** kan leda till olycka eller förlust av förmågekritisk funktion: **utlösare, riskkällor** och **bidragande orsaker**. Alternativa samt kompletterande modeller för felförlopp och -propagering presenteras i avsnitt 4.1.

3.2 Arbetsprocessen

I arbetet med att ta fram ett felsäkert och robust system används både god teoretisk kunskap om systemets fundamentala begränsningar, uppgiftens omfång och erfarenhet av systemet. Erfarenhet skapas genom användning av systemet och det är viktigt att den dokumenteras och återkopplas i nästa cykel av arbetet. Då kan systemet i fråga bli mer felsäkert med tiden. Det är även möjligt att nya fel uppstår som ett resultat av att systemet designas om eller används på ett nytt sätt. Leveson och HSystSäk [18, 21] lyfter vikten av det iterativa arbetet med betoning på både riskanalys, ny användning och designtillägg och processen presenteras i figur 3.1. Om en riskanalys inte görs i anknytning till att systemet förändras och grundläggande antaganden om systemet eventuellt inte längre är giltiga, kommer specifikationen som systemet bygger på att bli ogiltig. Det kan leda till oförutsedda fel. HSystSäk lyfter att riskhantering främst görs genom eliminering av riskkällor och genom konstruktion med designtillägg. Det finns många standarder och designregler som hjälper här, däribland MIL-STD-882E som är en internationell standard för systemsäkerhet.

Att integrera säkerhetskritiska funktioner i system redan från designstadiet är önskvärt, men inte möjligt i system som redan är implementerade och i bruk. Säkerhetsnivån kan höjas genom en utökning av systemet men detta skapar nya potentiella problem. Om hårdvaran är svår att omkonfigurera kan möjligheten för att integrera nya komponenter vara mindre. Det kan även vara svårt att integrera nya kretsar om originalhårdvaran är kompakt utformad. Om systemet är föråldrat och innehåller dåligt underhållen mjukvara och hårdvara, samt om kunskap kring systemet saknas försvåras arbetet med att modellera systemet och kartlägga fel. I en situation liknande



Figur 3.1: Figuren visar ett förslag på ett iterativt arbete för att kontinuerligt implementera nya designer utifrån säkerhets- och förmågekrav [21]. För att bevara den långsiktiga felsäkerheten behöver arbetet itereras vid ny design och förändrad användning av systemet.

denna ökas säkerhetsnivån framförallt via handhavandet, genom utbildning och skydd av personal som kan tänkas exponeras. [18]

Mohan m.fl. [22] beskrivs problematiken kring felsäkerhet specifikt för tunga autonoma lastbilar när ett system genomgår flera generationer av uppgraderingar och förändringar. En riskanalys som gjordes för systemets första versioner kan visa sig vara ogiltig och en ny riskanalys behöver då genomföras. De felsäkra funktionerna (detektion, diagnostik och hantering) behöver adderas till systemet och kommer i viss mån att konkurrera om systemets resurser avseende energi och beräkningskapacitet.

En arbetsprocess för framtagning av ett modellbaserat diagnostiksystem presenteras av Nyberg m.fl. [19]. Processbeskrivningen utökas här för att inkludera felhantering. Beskrivningen kan ses som en del i det iterativa arbetet, men är också relevant där ett befintligt system ska utökas med förmågan att hantera fel. Processen sammanfattas i följande steg:

1. Kartlägg de fel som behöver diagnosticeras. Utgå från ett behov av felhantering som uppkommit efter en riskanalys. Kartlägg under vilka krav diagnostiken har ställts.

2. Bygg upp kunskap kring systemet och de fel som ska diagnostiseras.

3. Etablera vad som är normal drift för systemet. Vilka tillstånd utgör det önskade operationella tillståndet och hur påvisas detta i drift?

4. Etablera förståelse för felens påverkan på systemet. Modellera dessa fel samt hur de kan påvisas. Relatera felen till systemets normalläge.

5. Designa kvantitativa eller kvalitativa test (mätstorheter) för systemets komponenter och delsystem. Var noga med att fel går att isolera från varandra.

6. Designa hypotestest för felen som utgår från mätstorheterna. Undersök testernas känslighet för typ I och typ II-fel. (se begreppsdefinition kap 2.2)

7. Utforma felhanteringsstrategier. Arbeta proaktivt i högsta möjliga grad men integrera reaktiva metoder för fel med potentiellt allvarliga konsekvenser. Gör en avvägning mellan alternativ efter att ha jämfört prestanda, resursintensitet och komplexitet.

8. Skapa en modell av diagnossystemet och felhantering för simulering. Svagheter kan då lokaliseras innan implementering i ett verkligt system.

9. Implementera diagnossystemet och felhanteringen. Testa systemet i händelse av individuella samt multipla fel. Skapa underlag för nästa arbetscykel.

Efter det sista steget kan det iterativa arbetet som beskrevs tidigare ta vid. Val av metod för detektion, diagnostik och hantering utgår från riskanalysen och systemets begränsningar. Exempel på sådana begränsningar är tillgång till data från givare, effektverkan i ställdon och frihetsgrader i rörelse.

3.3 Riskanalys

Syftet med att göra en riskanalys är att i förebyggande syfte identifiera potentiella risker och oönskade händelser, samt att uppskatta sannolikheten att de inträffar och allvarlighetsgraden av deras konsekvenser. Riskanalysen kan därefter användas som grund för att ta fram åtgärder för att undanröja och minimera sannolikheterna och konsekvenserna av olika risker.

En riskanalys kan bidra med förståelse för hur ett system fungerar och vilka krav som finns på systemet i miljön som det ska verka i. Riskanalysen kan utgå ifrån ett specifikt uppdrag eller från en kravställning på vad ett system ska kunna hantera.

Nedan listas några vanliga termer inom riskanalys tillsammans med en kort förklaring av dem.

- **Riskkälla (hazard)**: Ett tillstånd som kan döda, skada eller orsaka sjukdom hos människor, skada system, utrustning eller egendom, skada miljön. En riskkälla är en förutsättning för en skada eller olycka.

- **Olycka (accident)**: En oplanerad händelse som resulterar i död, skada eller förstörd eller skadad egendom eller utrustning.

- **Incident**: En händelse som inte är en olycka men som påverkar eller skulle kunna påverka uppdragets säkerhet.

- **Orsak**: De mekanismer som utlöser riskkällan som i sin tur kan resultera i en olycka eller en incident.

- **Kontroll**: En åtgärd vars syfte är att minska eller eliminera riskkällans orsaker eller effekter.

- **Systemtillstånd**: De tillstånd där ett system kan existera.

- **Effekt**: De verkliga eller förutsedda skadliga resultat som kan förväntas om riskkällan inträffar i ett definierat systemtillstånd.

- **Allvarlighet**: Konsekvenserna och påverkan av riskkällans effekt uttryckt i förlust eller skada.
- **Risk**: Kombinationen av allvarlighet och sannolikhet för att riskkällans effekt ska inträffa. Det förväntade värdet på förlust som en riskkälla har orsakat.
- **Mildrande åtgärder**: Åtgärder som vidtas för att mildra risken, antingen genom att minska allvarligheten hos effekten eller sänka sannolikheten för att den ska inträffa.

En riskanalys kan göras, dels vid utveckling och kravställning på ett system, dels vid enskilda uppdrag med ett existerande system. I det senare fallet kan riskanalysen användas för att väga olika angreppssätt mot varandra.

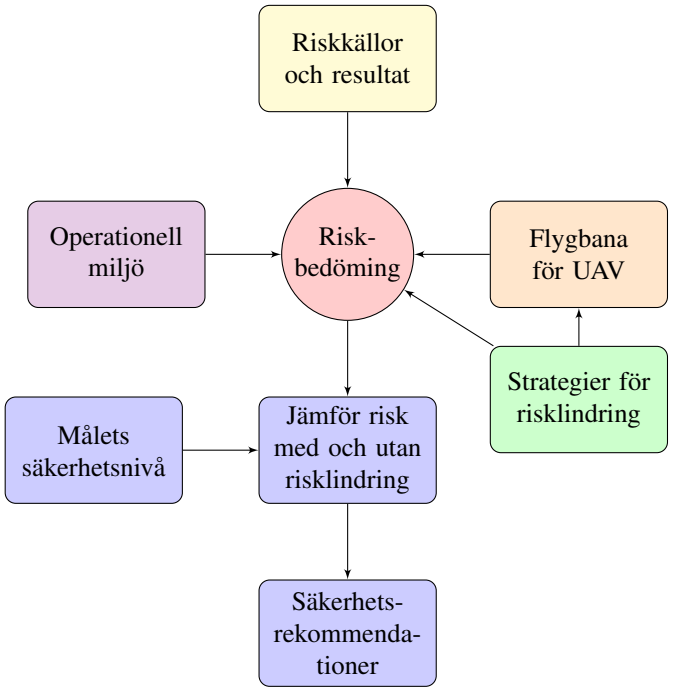
ISO-standarden [20] innehåller regelverk för hur en riskanalys för ett obemannat system ska utföras samt hur en proaktiv riskbedömning för en kravställning på ett system kan se ut. Arbetet med riskhantering kan delas in följande steg:

1. **Identifiering av riskkällor:** Alla riskkällor och incidenter som kan leda till att uppdraget påverkas och farkosten eller omgivningen skadas identifieras i det här steget.
2. **Riskbedömning:** En bedömning av risken med de riskkällor som har identifierats i det tidigare steget sker genom bedömning av skador vid en olycka och sannolikheten för att den inträffar.
3. **Riskvärdering:** Väga risken mot en tolerabel risknivå för att avgöra behovet av riskhantering och risklindring.
4. **Risklindring:** Resultatet av riskbedömningen och de nivåer för acceptans som finns visar vilken risklindring som måste införas.
5. **Dokumentation:** Processen och dess utförande och resultat ska dokumenteras för att kunna utvärdera resultaten.

Figur 3.2 visar en schematisk bild över de olika delarna i en riskanalys. De olika delarna kan var för sig göras mer detaljerade genom till exempel riskuppskattning, beskrivning av miljön och omständigheterna kring uppdraget. För mer detaljer se [23]. Det första steget i en riskanalys är att identifiera olika riskkällor. I rapporten ”*Felsäkerhet för obemannade farkoster: bakgrund*” [1] ges exempel på vanliga riskkällor för obemannade farkoster i de olika domänerna (luft, mark, sjö). Händelser och olyckor kan klassificeras utifrån sina konsekvenser och allvarlighetsgraden hos dem. Vilken säkerhetsmarginal som bedöms lämplig för olika konsekvenser avgör vilka åtgärder som är lämpliga att sätta in för att undvika olika typer av händelser.

Tabell 3.1 presenterar en allmänn skala i fem steg för att klassificera en olycka med en UAV och vilken säkerhetsmariginal som bedöms behövas med hänsyn till olyckans konsekvenser [23].

I tabell 3.2 ges en indelning av sannolikhetsnivåer för olyckor, hämtad från Barr m.fl. [23]. Den andra kolumnen presenterar en kvalitativ beskrivning av den tillåtna sannolikheten att olyckan inträffar. Den tredje kolumnen är tom, men för ett specifikt system med tillgänglig data för riskuppskattning kan en kvantitativ nivå bestämmas. Beroende på en kombination av hur allvarliga olyckorna är och vilken sannolikhetsklass de tillhör samt vilken risk beslutsfattaren är beredd att ta, kan ett beslut fattas om vilka insatser som ska göras och vad systemet ska klara av.



Figur 3.2: Figuren visar en process på en övergripande nivå för riskbedömning vid ett uppdrag med en UAV hämtad från [23]. Processen kan användas för andra system med anpassning av de delar som är specifika för just det systemet.

Tabell 3.1: Kategorisering av allvarlighet hos riskkällor [23].

Kategori	Skador	Säkerhetsmarginal
5: Katastrofal	Flera dödsfall	
4: Farlig	Enstaka dödsfall och/eller flera allvarliga skador	Stor minskning
3: Allvarlig	Icke-allvarliga skador	Betydande minskning
2: Lindrig	Inga	Liten minskning
1: Ingen säkerhetseffekt	Inga	Ingen effekt

Tabell 3.2: Sannolikhetsklasser för att en olycka ska inträffa [23]. För att fylla den sista kolumnen krävs statistiskt underlag och sannolikhetsberäkningar.

Sannolikhetsklass	Tillåten sannolikhet kvalitativ	Kvantitativ
A: Inget sannolikhetskrav	Inget krav på frekvens	
B: Sannolik	Inträffar flera gånger under farkostens livstid	
C: Otrolig	Inträffar troligtvis en gång under livstiden	
D: Extremt otrolig	Osannolik, men inträffar möjligtvis en gång under livstiden	
E: Extremt osannolik	Kan antas att den inte inträffar	

Det finns olika metoder för klassning och detta är i grunden en beslutsfattandeprocess som kan modelleras på olika sätt. För ytterligare sådan kategoriseringar och riskmatriser hänvisas till kapitel 4 i HSystSäk [18].

4 Feldetektion och feldiagnostik

Målet med feldetektion och feldiagnostik är att upptäcka och identifiera fel i ett system, innan de hinner få allvarliga konsekvenser. Möjligheterna till att detektera och diagnostisera fel avgörs av deras observerbarhet, det vill säga förmågan att kunna härleda felen utifrån de tillstånd hos systemet som det finns möjlighet att observera och få värden på. Feldetektion handlar om själva upptäckandet av fel, bristande funktionalitet eller händelseförlopp utanför normalläget. När det kommer till autonoma och obemannade farkoster kan exempelvis störningar i farkostens beteende detekteras som avvikande och identifieras som ett tecken på att ett fel har uppstått. För att kunna avgöra vad som är en lämplig åtgärd när ett fel har inträffat och detekterats är det viktigt att förstå felets påverkan på farkosten, om felet kan bli allvarligare samt var i farkosten felet har sitt ursprung eller om det är orsakat av yttre omständigheter. Syftet med feldiagnostik är att avgöra felets ursprung eller orsak, lokalisera felet i farkosten samt analysera felets påverkan. Denna information kan därefter användas som underlag när ett beslut om eventuell åtgärd ska fattas.

Metoder för detektion och diagnostik kan delas in i **datadrivna** och **modellbaserade**. Ett typexempel på datadriven feldetektion är när en maskininlärningsalgoritm tränas att känna igen olika förlopps normaltillstånd för att kunna identifiera när normaltillståndet inte är uppfyllt. En efterföljande diagnostik kan därefter karakterisera händelsen utifrån en felmodell som i sin tur kan vara analytisk eller framtagen med hjälp av data [19]. Modellbaserad detektion använder sig istället av en analytiskt framtagen modell av systemet som kontinuerligt jämförs med systemets faktiska tillstånd för att identifiera avvikelser.

När feldetektion och feldiagnostik integreras i en farkost kan observerbarhet och potentiella konsekvenser för de möjliga felen vägas mot resursanvändning (kostnad för system, beräkningskomplexitet, energianvändning m.m.). I vissa fall kan det vara lätt att detektera att något är fel men svårt att dra slutsatser om felets orsak och dess följder. I en sådan avvägning ställs en automatiserad funktion för diagnostik mot att en mänsklig operatör får gripa in. Det gäller inte bara beslut om trolig orsak och allvarlighetsnivå utan även åtgärd. Det finns exempel från transport- och fordonsindustrin där koncept tagits fram för beslutsstöd via operatörscentrum, så kallade kontrolltorn, där människor kan ta över kontrollen när det obemannade systemet inte kan hantera situationen. Ett exempel på en sådan situation är när diagnostiken genererar flera felhypoteser med liknande sannolikheter. Ett fundamentalt problem med sådana beslutsöverlämmnanden är att en människa förväntas ta över en situation när denne är som minst förberedd och systemet är som mest svårhanterligt [13, 24].

en väl genomförd riskanalys bör ligga till grund för metodvalet för felhantering. Vissa fel har liten påverkan på farkosten och behöver inte detekteras och diagnostiseras i realtid. Andra fel resulterar i haveri om de inte detekteras och diagnostiseras i realtid. Frågorna som bör ställas inför metodvalet samt några tankemodeller presenteras i kapitel 6. I detta kapitel beskrivs även olika metoder, deras styrkor och svagheter samt olika typer av felförlopp.

Feldetektionen kan i sig visa sig inte stämma. Detta kan yttra sig på två olika sätt: falsk positiv detektion eller missad detektion (se kapitel 2.2).

4.1 Felförlopp och felpropagering

Vid utformningen av diagnostiken i ett system där lokaliseringen av felkällan är av betydelse behövs en förståelse och modeller av systemet för att kunna spåra möjliga förlopp som har resulterat i det aktuella felet. Därigenom är det möjligt att lokalisera var felet har uppstått genom att följa processen i motsatt riktning. Ett exempel på detta tillvägagångssätt är felträdsanalys.

Om det inte är viktigt att lokalisera felkällan är en vanligt förekommande lösning att detektera fel enligt den så kallade enlagersprincipen. Här bortser man från att systemet består av flera lager av processer och delsystem där ett fel i ett lågt lager kan propagera uppåt. Exempel på sådana enlagerslösningar finns inom fordonsindustrin där diagnostiken i fordonet ibland kopplar ett detekterat fel (låg oljenivå) direkt till en åtgärd (stanna fordonet). Ett fel uppstår, detekteras och en åtgärd utförs, men orsaken till att felet har uppstått är inte viktigt i sammanhanget.

Representation av felförlopp är svårt, men viktigt som underlag för en riskanalys samt vid feldiagnostik där fellokalisering, även benämnt felisolering, är önskad. Alla fel har i grunden orsaker även om de ibland förenklat kan anses vara slumpmässiga. Väldigt ofta är felförlopp komplexa och en bakåtiteration i händelsekedjan kan vara svår och missvisande. Detta argument presenterar Leveson [21] med tillägg att sådana bakåtiterationer ofta leder till felaktiga slutsatser. För enkla system kan det vara en bra metod, men när systemen i fråga är stora och inkorporerar många icketekniska aspekter fungerar det sämre. För tekniska system med en begränsad mängd delsystem kan felförlopp ofta kartläggas med relativt hög tillförlitlighet och det möjliggör inte bara bättre haveriutredningar men även online-diagnostik [25, 26]. Flera fel kan dock ha överlappande effekter på ett system och då krävs flera oberoende teststorheter för att isolera felen.

Ett felförlopp består dels av att fel propagerar, dels av att fel förvärras. Ett fel som uppstår i ett delsystem kan propagera till en annat genom interaktioner eller beroenden. Zibaei m.fl. [25] presenterar en metod för att koppla detekterade händelser till ett detekterat fel med syftet att lokalisera felkällan, och kombinerar en förloppsmodell på farkostnivå med detektionsmetoder på delsystemsnivå. Regler för kausalitet används för att filtrera bort potentiella händelser och generera förslag på möjliga felförlopp.

4.2 Metoder

Metoder för detektion och diagnostik kan delas upp i två huvudgrupper, datadrivna och modellbaserade, och en introduktion ges i följande avsnitt.

4.2.1 Datadrivna metoder

En datadriven metod baseras på insamlad data från systemet, exempelvis data från en farkost under tidigare uppdrag. Datan kan innehålla felaktiga tillstånd eller data från normal drift. Feldata kan ta formen av statistik för hur ofta fel inträffar eller data som relaterar händelser som definieras som felaktiga till driftdata. Normaldata kan användas för att definiera normalt beteende hos en komponent, ställdon eller delsystem. Ett fel eller anomali är när normalt beteende inte observeras. Klassiska datadrivna metoder bygger på fourieranalys eller statistiska signalbehandlingsverktyg, men maskininlärning används i ökande grad för detta ändamål. Maskininlärning har inom diagnostiken bl.a. fyllt en roll av att skapa felmodeller i större och mer komplexa system där ”osynliga” relationer mellan fel och händelser kan finnas. Maskininlärning kan med andra ord stödja klassiskt modellbyggande, men i viss mån även ersätta det genom att förfina modeller med aktuell eller historisk driftdata respektive modellering från grunden. Exempel på detta finns i Kumar m.fl. [27] där en dold Markov-modell

(Hidden-Markov model) används för att skapa en degraderingsmodell för komponenter. Masalimov [28] använder maskininlärning för att bygga diagnostiska modeller för CNC-maskiner [1] i en fabrik med hjälp av insamlad driftdata från fabrikens maskiner.

Datadrivna metoder kan tillämpas både i detektions- och diagnostikfasen. Så kallad outlier-detektion används ibland i feldetektionen för att hitta avvikelser som i sin tur kan härstamma från fel, speciella händelser eller intrång [29]. Avvikande data detekteras och sedan appliceras metoder för att klassificera den som fel, händelser eller intrång. Maskininlärning kan även användas för att direkt associera data med vissa fel och degraderingstillstånd. I exemplet från [28] används både rå driftdata från maskiner (elektriska strömmar, vridmoment, rotationshastigheter m.m.) och metadata kopplat till maskinerna, när de varit i drift och vilken typ de är av, för att träna algoritmer till att kartlägga fel. Genom att känna till en maskins tillstånd (degraderad drift, helt trasig) vid vissa tidpunkter och den samtida råa driftdatan kan algoritmen tränas med maskininlärning och sedan appliceras för att göra detektion och klassificering i en gemensam lösning. Här är det viktigt att vara medveten om problem med metoderna och vilka feltillstånd som finns representerade i datan som används för metoderna.

Maskininlärning har visat sig vara ett kraftfullt verktyg för att hitta avvikande beteende och skapa sambandsmodeller. Resultaten från maskininlärning med neuronnät är dock ofta svårbegripliga och lider i stor utsträckning av bristande förklarbarhet [30]. Detta kan äventyra tilliten hos metoden vilket är en viktig nackdel i militära tillämpningar.

4.2.2 Modellbaserade metoder

Det saknas en skarp gräns mellan modellbaserad och datadriven diagnostik. En enkel skillnad är att datadrivna metoder inte skapar en modell av systemet utan drar slutsatser direkt från data, medan modellbaserade metoder använder sig av en modell. Modellbaserad diagnostik kännetecknas av en kontinuerlig jämförelse mellan systemets faktiska tillstånd i form av signaler från sensorer och inre processer med en modell av systemet. Modellen kan vara kvalitativ eller kvantitativ, och vara framtagen analytiskt eller datadrivet. Det är även möjligt att uppdatera modellen utifrån realtidsdata. En deskriptiv modell beskriver relationer mellan förlopp och processer, ofta i termer av logik och påståenden om funktioner och beteenden, och är ofta kvalitativ. En analytisk modell är kvantitativ och beskriver ett förlopp i matematiska termer, exempelvis differentialekvationer [31]. För tekniska system är modellen ofta deskriptiv, analytisk eller en kombination av båda.

En modell kan ha många roller. Friedenthal m.fl. [32] identifierar tre huvudsakliga roller för en modell:

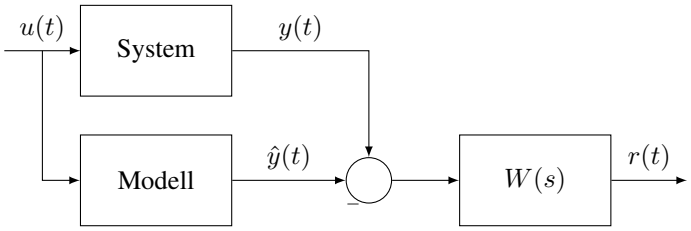
- **Representation**: Modellen ska representera en delmängd av ett objekt eller en process med hög precision.
- **Förenkling**: Modellen ska anta en enklare form än det verkliga objektet eller förloppet.
- **Abstraktion**: Modellen ska vara en abstrakt representation av något. Det innebär att vissa saker bortses ifrån i den förenklade representationen.

Representationskomponenten är den kanske viktigaste rollen en modell har. Modellen är ofta abstraherad i form av matematiska funktioner som representerar de olika förlopp som ska övervakas.

[1] Computer Numerical Control

För att modellbaserade detektions- och diagnostiksystem ska fungera långsiktigt är det viktigt att ta hänsyn till att de modellerade delsystemen långsamt förändras över tid, så kallad drift. För att illustrera detta delar Nyberg m.fl. [19] upp ett system i aktuator, process och sensor och påpekar att drift i någon av dessa delar kommer att göra modeller felaktiga över tid. Exempel på sådan drift kan vara fysisk degradering av komponenter i sensorer och aktuatorer som inte nödvändigtvis degraderar systemets prestanda, men likväl skapar ett ökande modellfel med tiden. En process kan även driva om den har kapacitet för inlärning och således förändras med tiden.

Den modellbaserade detektionen eller diagnostiken kräver en tillförsel av modeller, ofta analytiska. Förloppet som ska modelleras kan vara stokastiskt eller deterministiskt. Byggandet av kvantitativa modeller kan delas in i parametriska och parameterlösa metoder. En parametrisk metod utgår från en struktur och försöker matcha insamlad data till strukturen. En vanlig situation är att en serie insignaler och utsignaler från en process erhålls varpå en redan bestämd processtruktur parametersätts för att bäst matcha signalerna. Ett exempel på en sådan situation är då en fysisk verklighet inspirerar en processtruktur men parametrar är okända. En parameterlös metod kräver ingen förutfattad struktur och modellen genereras endast från jämförelsen mellan insignal och utsignal. Processen ses som en svart låda. I en sådan metod kan den struktur väljas (linjär, icke-linjär, vågform, diskret o.s.v.) som ger bäst matchning mellan insignal och utsignal. Parameterlösa metoder är ofta svårare att implementera än parametriska metoder men ger överlag mer noggranna modeller [33].



Figur 4.1: Utsignal från sensorer jämförs med en modell. Det ger en så kallad residual. Residualen filtreras för att minimera effekten av brus och andra kända störningen. Den resulterande signalen jämförs med ett tröskelvärde för att avgöra om ett fel har inträffat eller inte [19].

4.2.3 Aktiva metoder

Vissa fel uppstår bara i särskilda miljöer eller situationer. En aktiv metod för feldetektion och diagnostik består av att simulera insignaler, interagera med den berörda komponenten eller i en säker miljö använda systemet för att excitera ett visst fel [19]. Avsikten är att isolera orsaken till felet eller att förstå felförloppet genom att generera felet. Det tar ofta formen av tester som bedrivs i kontrollerade miljöer där effekterna av felet kan kontrolleras. Tester är bra lämpade för intermittenta fel och har till syftet att hitta fel innan systemet är operativt. För komplexa tekniska system bör testprotokoll även integreras på komponentnivå [34]. Då kan intermittenta fel detekteras nära felkällan och konsekvenser kan undvikas tidigt i drift. Även testning av delsystemens funktionalitet är viktigt. Sineglazov m.fl. [35] beskriver vikten av att testa navigeringssystem för UAV:er och metoder för detta. Testning är en proaktiv åtgärd men kan även integreras reaktivt i diagnostiken för att möjliggöra ett system att förstå orsaken till ett fel och dess påverkan på systemet. Aktiv testning av ett system med degraderad funktionalitet kan generera ytterligare fel och bör göras med försiktighet.

4.2.4 Passiva metoder

En passiv metod för detektion och diagnostik påverkar inte systemets drift. Diagnostiken lyssnar på systemet från mätdata och inre processer och drar slutsatser om eventuella fel [19]. I passiv detektion och diagnostik kan intermittenta fel vara svåra att detektera eftersom det inte finns någon garanti för att den specifika situation som utlöser felet inträffar. Hur ett fel yttrar sig kan även bero på den operationella miljön och utan möjlighet att påverka miljön genom aktiv testning kan vissa fel vara svåra att detektera. En passiv detektion och diagnostik görs i realtid eller baserat på historik.

5 Risk- och felhantering

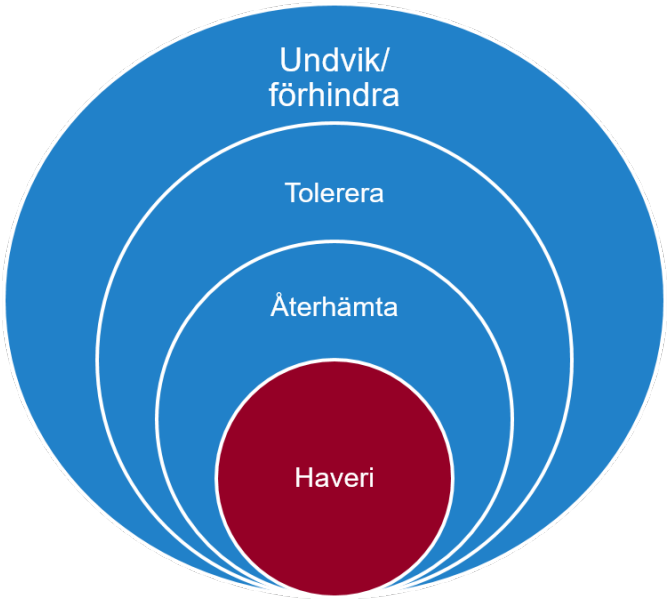
Enligt Nationalencyklopedin [36] är den allmänna betydelsen av **risk** möjligheten att något skadligt eller negativt ska inträffa. För tekniska system kan risken för en olycka kvantifieras som sannolikheten att en händelse inträffar kombinerat med olyckans konsekvens [18]. Utifrån denna definition kan risken minskas antingen genom att minska sannolikheten att en händelse inträffar eller att minska konsekvenserna av olyckan (eller både och). För tekniska system hanteras risker både proaktivt genom design eller förberedelser och reaktivt genom handhavande vid drift av systemet. Detta gäller även obemannade system som helt eller delvis saknar eller endast begränsat sköts av en operatör, vilket gör att de delar av riskhanteringen som annars sker under drift flyttas till det tekniska systemet.

För att kunna agera autonomt bör ett system ha inbyggda metoder för att identifiera och hantera uppkomna situationer som annars hade skötts av en operatör på egen hand. Detta resulterar i att den direkta påverkan från den så kallade mänskliga faktorn minskas, men den finns fortfarande indirekt kvar i designen och implementationen av systemet, som en missad eller felaktigt implementerad hantering av en specifik situation. Därför behövs en riskanalys för att belysa situationer där autonom riskhantering behövs eftersom felhanteringssystem ersätter delar av checklistan som en operatör följer i realtid för att avstyra allvarliga konsekvenser.

En risklindrande åtgärd kan ta många former. I tekniska system är det vanligt att funktioner för feldetektion, -diagnostik och -hantering implementeras. I komplexa tekniska system finns olika lager av riskhanterande åtgärder och bakom många historiska haverier ser Leveson [21] brister inom bl.a. säkerhetsrutiner och utbildning i systemanvändning för operatörer.

En händelse eller ett förlopp som utgör en risk kan vara resultatet av ett internt fel, en felaktig användning av systemet eller en yttre påverkan. Felhantering kan således ses som en undergrupp till riskhantering. Att implementera feldetektion, feldiagnostik och felhantering är en risklindrande åtgärd, men en risklindrande åtgärd behöver inte alltid ha till syfte att detektera, diagnostisera och hantera fel. Många risker är svåra att kvantifiera och ett system som identifierar och lindrar alla risker i realtid är sällan möjligt, och ett naivare system som endast berör fel är därför vanligare. Eftersom fokus i denna rapport ligger på *fel* handlar detta kapitel främst om metoder för felhantering, vilket kan ses som en del av en generellare riskhantering.

Syftet med felhantering är att säkerställa systemets fortsatta förmåga att utföra sin uppgift, givet ett aktivt eller potentiellt fel. Metoder för felhantering kan klassificeras utifrån olika aspekter, exempelvis tid (när utförs hanteringen i relation till felet?), vilka typer av fel som hanteras (allvarligt, icke allvarligt?) och vilka verktyg som används. Felhantering kan ske i olika lager och detta illustreras i figur 5.1 som ett lökdiagram. Ett potentiellt fel i en kritisk delfunktion utgör en riskkälla och bör i högsta mån hanteras proaktivt. Om detta inte är möjligt bör felet kunna tolereras genom exempelvis redundans. Om detta inte heller är möjligt bör farkosten kunna återhämta sig på något sätt, till exempel genom en omkonfigurering, nödlandning och reparation. Om detta inte lyckas kan det resultera i en förlust av kritiska förmågor vilket innebär att uppdraget inte blir utfört och att farkosten eventuellt får allvarliga skador.



Figur 5.1: Lökdiagram för felsäkerhet hos system. Ett fel som penetrerar alla lager av felhantering kommer att leda till haveri det vill säga en permanent förlust av en kritisk funktion. Ju fler metoder varje lager består av desto högre grad av felsäkerhet erhålls men möjligheten att åtgärda felet är beroende på observerbarheten hos det.

5.1 Metoder

Metoder för felhantering kan översiktligt delas upp utifrån en tidsaspekt som antingen **proaktiva** eller **reaktiva**. Proaktiva metoder kan vara **prediktiva** eller **preventiva**, och har gemensamt som syfte att förhindra eller undvika att ett fel uppstår eller förvärras. Reaktiva metoder sker i realtid med syftet att tolerera eller återhämta sig från ett fel som har inträffat. Här kan det vara viktigt att skilja på åtgärden ”*att implementera en metod*” och själva metoden i sig. Att designa algoritmer för omkonfiguration i händelse av fel i en farkost är en proaktiv åtgärd, medan omkonfigurationen i sig kan ses som en reaktiv insats. Om inte åtgärden som genererade metoden och metoden själv skiljs åt kan alla metoder ses som proaktiva.

En vanlig metod för att hantera fel är redundans, en feltolerant åtgärd som erbjuder en motståndskraft mot det felaktiga tillståndet där felet uppstår. Feltolerans kan generellt klassificeras som reaktivt eftersom den ofta tar formen av ett metodbyte, ändrat beteende eller fysisk omkonfigurering, men är integrerat i systemet för att minimera påverkan av felet, det vill säga gör inget försök att undvika felet.

5.1.1 Preventiva metoder

Fel kan betraktas som utlösande faktorer eller bidragande orsaker till vådahändelser. En preventiv åtgärd för felhantering syftar därför till att förhindra fel från att inträffa. Åtgärder av den här typen är kraftfulla för att öka säkerheten i ett system. Som beskrevs i 4.1 kan multipla fel öka sannolikheten för en vådahändelse mer än vad varje fel gör för sig och det är därför viktigt att åtgärda dem preventivt innan systemet i fråga blir operativt. Preventiva metoder består huvudsakligen av att undvika fel genom själva utformandet av systemet, där en felträdsanalys har hjälpt i en riskbedömmning. Något som skiljer preventiva metoder från prediktiva är avsaknaden av en modell för händelsekedjor och felförlopp som stödjer feldiagnostik i realtid. Exempelvis kan skrovet på en isbrytare förstärkas preventivt utan information om exakt hur stor risken är för att skrovet går sönder i en given situation. Ett annat exempel

är preventivt underhåll där statistik kan användas som grund för hur ofta underhåll bör göras, men där systemets faktiska tillstånd vid en viss given tidpunkt inte används i schemaläggningen. Om något går sönder innan det inplanerade underhållet kan en reaktiv åtgärd behöva sättas in.

5.1.2 Prediktiva metoder

En prediktiv metod skiljer sig från en preventiv metod i och med att en riskanalys och prediktion av systemhälsa vägs in i åtgärden i realtid. En prediktiv metod kan vara felundvikande, felbromsande eller felnegligerande. Det som kännetecknar en prediktiv metod är att god analytisk förmåga kopplat till konsekvenser och felpropagering för beslut vägs in i åtgärden med aktuell och nyinsamlad data. Detta kräver tillgång till modeller av händelsekedjor och hur felen utvecklas i systemet. Ett exempel är prediktivt underhåll där en prediktionsmodell för komponenters livslängd används för att minimera risken för fel samt för att maximera driftstiden. Det används bland annat inom transportindustrin.

5.1.3 Reaktiva metoder

Reaktiva felhanteringsmetoder sker ofta i realtid efter att ett fel har uppstått och har som syfte att läka, bromsa, tolerera eller negligera felet som har inträffat. Bakgrunden är ofta en degraderad funktionalitet, eller en direkt observerad riskkälla eller händelse som inom kort kan leda till en degraderad funktionalitet. Ett exempel på det senare är låg oljenivå i en motor, vilket kan leda till ett haveri om det inte åtgärdas. I det exemplet kan orsaken vara ett fel eller att någon glömt fylla på med olja. En annan reaktiv metod för felhantering är omkonfiguration av systemet för att minska konsekvenserna av, eller åtgärda orsaken till, ett haveri eller mindre allvarligt fel. Det kan till exempel innebära att koppla bort en elmotor som drar stora mängder ström men inte generar kraft eller att ändra flygsätt på grund av tappad styrförmåga. Den reaktiva åtgärden bör stå i relation till felets konsekvenser, och kan därför kombineras med metoder för att analysera konsekvensen av olika fel. Vissa fel behöver inte alltid hanteras då deras konsekvenser kan vara försumbara för systemet och uppgiften.

5.1.4 Fysisk och analytisk redundans

En vanlig metod för att etablera feltolerans är redundans [14], där idén är att hantera fel genom att ha flera verktyg för samma uppgift. Dessa kan antingen avlösa varandra (dynamisk redundans) eller jobba parallellt och rösta om vad som är det korrekta resultatet (statisk redundans).

Att använda flera fysiska komponenter som kan lösa samma uppgift kallas för fysisk redundans. Om förlusten av en viss egenskap hos ett system är allvarlig kan flera komponenter, som med fördel är toleranta mot olika felkällor, användas för att uppnå den egenskapen samt ersätta eller komplettera varandra om en komponent går sönder.

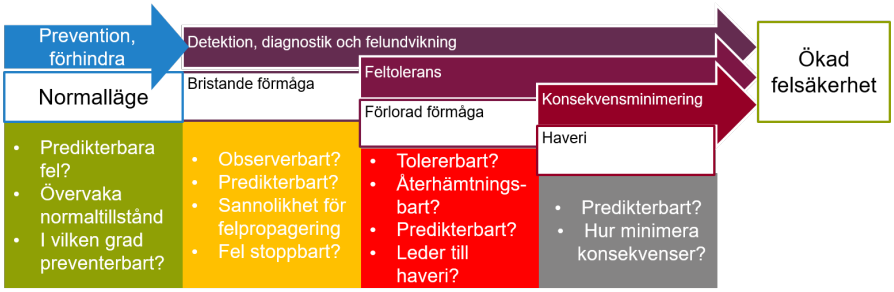
Analytisk redundans tar istället formen av oberoende algoritmer och matematiska modeller som uppskattar en storhet baserat på olika mätdata. Ett exempel är sensorfusionering i PNT-system[1] där mätningar från flera olika sensorer vägs ihop och farkosten förses med en tillståndsuppskattning tillsammans med osäkerhetsbedömning. Systemet bör fungera i händelse av sensorbortfall. Nyttan av att flytta redundansen från hårdvara, som är en gammal och välbeprövad lösning, till mjukvara har varit känd länge. Willsky m.fl. [37] lyfter i sin publikation från 1976 detta som ett verktyg för att både minska den fysiska komplexiteten i system och göra dem billigare.

[1] Position, Navigering, Tid

6 Diskussion om metodval och systemutformning

Detta kapitel innehåller förslag på hur riskanalysen och kunskap kring de olika felförloppen kan resultera i metodval och systemarkitektur.

Efter att en farkost eller ett system som ska få ökad felsäkerhet är kartlagt och riskkällor är identifierade kan arbetet fortsätta med framtagning av metoder för felhantering. Kartläggningen av riskkällor och de fel de kan orsaka föreslås inkludera situationer där fel kan uppstå, felförlopp samt allvarlighetsgrad. Riskvärdering, felens natur samt systemets eller farkostens tillgängliga resurser och begränsningar ligger därefter till grund för metodvalen gällande felsäkerhet. Detta kapitel föreslår, utifrån tidigare kapitel, en generell modell och exempel på detta metodval.



Figur 6.1: I varje steg i felförloppet ställs vissa frågor så att rätt metod kan implementeras. Detektion och diagnostik kan implementeras i alla steg och de kan hjälpa till att förhindra att felet förvärras. Feltolerans är viktigt om felet leder till förlust av förmåga och om förlusten leder till haveri bör effekten av olyckan minimeras.

6.1 Metodkombinationer och avvägningar

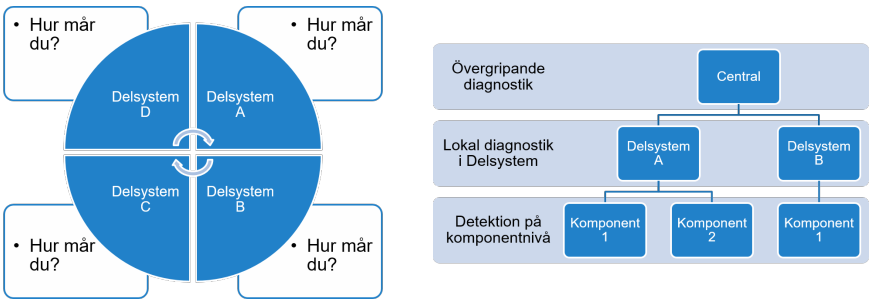
Hantering av enskilda fel i olika delsystem kan ske aktivt eller passivt och ske online eller offline. Dessa egenskaper kan kombineras på olika sätt beroende på den specifika situationen. Valet av kombination är beroende av vilken typ av fel det gäller, samt efter vilka krav som finns på realtidshantering. Passiv detektion och diagnostik kan ske både online, när systemet är i drift, och offline när systemet inte är i drift. Aktiv detektion och diagnostik kan också ske både online och offline, valet beror på felets karaktär. Det är en fördel om allvarliga fel kan detekteras i realtid och metoder online är att rekommendera. Mindre allvarliga fel kan hanteras offline.

Som exempel på två fel är oljeläckage från en motor och trasiga vindrutetorkare. Oljeläckaget är viktigt att detektera, eventuellt diagnosticera, samt hantera om det sker under drift, det vill säga online. De trasiga vindrutetorkarna kan hanteras offline. Ett oljeläckage skulle exempelvis kunna detekteras med hjälp av en givare för oljenivån med en tillhörande beräkningskrets för realtidsjämförelse med ett tröskelvärde som varnar för avvikelser (passivt, online). För att undersöka om något är fel med vindrutetorkarna skulle enkla tester kunna genomföras innan start för att se att allt fungerar som det ska (aktivt, offline). Denna typ av analys för metodval sammanfattas förenklat i figur 6.1, som syftar till att beskriva en tankeprocess för metodval.

Valet av metoder görs även utifrån vad som är resurseffektivast. En implementering av felsäkerhet medför en utökning av ett tekniskt system vilket i sig medför ökad komplexitet. Den kan göras med mjukvara, hårdvara eller både och. Genom att införa felsäkerhet i delsystem kommer en övergripande felsäker arkitektur där fel i delsystem hanteras centralt och där analytiska metoder avlöser hårdvarulösningar att behövas för att automatisera felsäkerheten för hela farkosten. Det är också viktigt att se över hur farkostens olika system kan generera risker och fel. Här kan slutsatsen bli att sänka ambitionsnivån och införa ett mindre komplext delsystem samt att sänka autonominivån. Det är också möjligt att låta en mänsklig operatör ta över farkosten vid fel men detta är ofta svårt och riskfyllt i sig.

6.2 Arkitekturer

När metoder har valts ut för de enskilda felen i farkosten eller systemet behöver en övergripande arkitektur konstrueras där lokala fel i komponenter och delsystem kan kopplas till det övergripande systemet. I detta avsnitt beskrivs kortfattat motiven till en övergripande arkitektur samt några exempelarkitekturer. Felförlopp kan detekteras lokalt och den lokala inferensen om feltyp är en parameter i en global förmågebedömning eller rot-orsaksanalys. Den informationen kan i sin tur utgöra viktiga ingångsvärden i en beslutsalgoritm på högre nivå. I exempelsystemet från [25] som togs upp i avsnitt 4.1 beskrivs hur lokal diagnostik översätts till händelser som jämförs i en algoritm för rot-orsaksanalys på farkostnivå. Det är tydligt hur en central diagnostik som överblickar hela systemet kan gynna farkosten i form av ett beslutsunderlag.



(a) Top pull **(b)** Bottom push

Figur 6.2: Två typer av arkitekturer för diagnostik i ett helt system eller farkost. I ”top pull”-arkitekturen frågar den centrala diagnostiken varje delsystem hur de mår med en viss frekvens medan i en ”bottom push”-arkitektur skickar varje delsystem meddelande när fel inträffar lokalt.

Två vanliga arkitekturer är s.k. ”bottom push” och ”top pull”. I en ”bottom push”-arkitektur (figur 6.2b) ligger den centrala diagnostiken och väntar på rapportering från lokala diagnostikmoduler. När ett fel inträffar lokalt pushas ett meddelande upp i hierarkin och den centrala diagnostiken gör en bedömning av det nya totala tillståndet. Denna arkitektur kan ses som asynkron eftersom varje lokal diagnostik meddelar uppåt när händelsen inträffar och inte med en viss frekvens. I en ”top pull”-arkitektur (figur 6.2a) genomsöker den centrala diagnostiken varje delsystem regelbundet och frågar om diagnostik. Varje delsystem kan göra en diagnostisk bedömning regelbundet men meddelar endast uppåt i hierarkin då centralen frågar om den. En sådan arkitektur är synkron eftersom varje delsystem genomsöks med en konstant eller varierande frekvens. Det finns även hybridarkitekturer mellan ”top pull” och ”bottom push” där allvarliga fel kan skickas upp i hierarkin asynkront samtidigt som delsystemen genomsöks regelbundet. Det kan vara en kraftfull metod för att garantera att allvarliga fel hanteras snabbt.

7 Slutsatser och framtida forskning

I detta arbete har existerande generella metoder för felsäkerhet belysts ur perspektivet obemannade farkoster med tillämpningar som är relevanta för Försvarsmakten. Här diskuteras det som har presenterats i rapporten och slutligen ges förslag på framtida forskningsområden.

7.1 Slutsatser

Automatiserade metoder för feldetektion, feldiagnostik och felhantering är viktigt för att möjliggöra högre automationsgrad hos obemannade farkoster. Betydelsen av dessa funktioner ökar med ökade krav på uthållighet och uppgifter, samt med storlek och komplexitet hos själva farkosten. Ju högre risk för allvarliga konsekvenser vid en olycka desto mer krävs av integrerad felsäkerhet i farkosten. Forskningsområdet är stort och det finns många delar där mer arbete behöver göras.

Denna rapport visar att det finns många metoder för att identifiera och hantera fel i olika delsystem och även för att kompensera för dem, reaktivt som proaktivt. Med dessa metoder kan farkosten operera med högre tillförlitlighet, men många delar i forskningen saknas. Fokus i mycket av forskningen är att implementera metoder för specifika delsystem. Endast ett fåtal metoder har på senare år behandlat feldiagnostik och felhantering för hela farkosten. Den mesta forskningen berör interna fel på ställdon och sensorer, ofta separerat från varandra. För att ett autonomt system ska vara både robust och felsäkert måste en metod kunna hantera fel i alla delsystem, samt även extern påverkan.

Denna rapport har försökt bryta ned begrepp och metoder i sina fundamentala byggstenar. Fel har nyanserats i flera dimensioner: allvarlighetsgrad, tidsomfång samt propagering i systemet, det vill säga om det är ett latent fel eller ett felaktigt tillstånd som degraderar farkostens förmågor. Bedömningen av en riskkälla kan utgå från dessa dimensioner och val av metoder följer därefter. Riskkällan bör värderas mot farkostens uppgift och nyckelegenskaper. Detta diskuteras i domänrapporten [1].

Historiskt har det forskats mycket om felsäkerhet. Däremot är systemfel och interaktionsfel hos obemannade farkoster med maskininlärningsmetoder ett relativt nytt forskningsområde. Utvecklingen av intelligenta system har pågått under mycket lång tid och tillämpningarna av maskininlärning har ökat snabbt under de senaste decennierna. Om tekniken är mogen nog för avancerade tillämpningar i högautomatiserade farkoster återstår att se. Det finns såväl risker som möjligheter vid införande av maskininlärning i feldetektion och -diagnostik.

7.2 Framtida forskning

Den här rapporten ger en inledande översikt till nuvarande kunskapsläge om felsäkra obemannade farkoster med autonoma funktioner. För att kunskapen ska vara tillämpbar av Försvarsmakten och FMV behövs både bredd och djup i forskningsverksamheten. Det framtida arbetet bör leda till en kunskapsuppbyggnad inom teoretiska metoder, algoritmer, tillämpningar, arkitektur- och systemkunskap och riskanalyser. De domänspecifika kunskaperna, det vill säga hur Försvarsmakten samt andra försvarsmakter använder och underhåller tekniska system ur ett felsäkerhetsperspektiv bör även förbättras.

För att bygga upp en kunskap om robusta och feltoleranta farkoster behövs forskning om hur hela farkosten ska hanteras då fel inträffar. Mycket av den existerande forsk-

ningen rör delsystem och endast ett fåtal försök för att felsäkra ett helt system presenteras i rapporten [1]. För att göra det krävs ett systemtänkande och uppbyggande av arkitektur för hur en farkost modelleras och hur beslut ska fattas för hela farkosten och den miljö där den är verksam. Att utföra tester på en verklig farkost innebär en stor möjlighet till insikter om hur metoderna fungerar och vad som behöver utvecklas. Eftersom fel ofta beror på oförutsedda händelser kommer ett verkligt system att bidra till förståelse för problemen och vad som kan hända. Genom att bygga upp modeller och testa funktioner på hela farkosten i en miljö med simulerad yttre påverkan kan felförlopp och metoder implementeras, testas och utvärderas.

Under arbetet har följande områden där framtida forskning bör bedrivas identifierats och svar på följande frågeställningar bör tas fram.

- Vilka metoder behöver vara implementerade i delsystem för att uppnå önskad nivå av felsäkerhet och hur ska de utvärderas och verifieras?
- Arkitekturer och metoder för att en obemannad farkost ska vara felsäker behöver utvecklas och testas. Vilken komplexitet är lämplig i Försvarsmaktens tillämpningar och hur avväger man grad av autonomi och felsäkerhet för att få maximal förmåga i förhållande till resurser?
- Vilka teknikbehov uppstår i kompromissen mellan grad av autonomi och flexibilitet, gentemot tillit och förutsägbarhet?
- Hur kombineras uppdragsstyrning och felsäkerhetssystem i en obemannad farkost?

Med dessa frågeställningar som utgångspunkt föreslås forskning och aktiviteter inom följande områden.

- Matematisk modellering av farkoster, felförlopp och dess påverkan på systemet:
  - Beskrivning av en farkost med en analytisk modell med hjälp av fysikaliska samband och kunskaper om fel som kan inträffa vid användning av farkosten.
  - Användning av driftdata från en farkost för att beskriva ett normaltillstånd och tillåtna systemtillstånd för att sedan kunna identifiera feltillstånd.
  - Utvärdering av dessa modeller och deras respektive för- och nackdelar.
- Framtagning av en simulator för tester av felsäkra metoder för obemannade farkoster. Simulatorn bör modellera hur fel som inträffar påverkar farkosten.
- Tillämpning av befintlig forskning på fysiska farkoster för att testa metoderna i verkliga miljöer i alla domäner med syfte att i förlängningen utveckla och implementera nya förmågor.
- Systemvärdering:
  - Fel inträffar i en viss användning av farkosten och därför behöver realistiska scenarier utarbetas för att simuleringar ska bli så verklighetsnära som möjligt.
  - Arbete med att förstå olika farkoster och tekniska system, samt hur de används av Försvarsmakten. Farkosten och alla aktörer i dess sammanhang behöver ingå i en analys för att utvärdera användning och för att utveckla metoder på rätt nivå.

  - Riskanalysarbete för farkoster med hänsyn till användning, organisation och tekniska faktorer.

- För att utveckla verklighetstrogna modeller (både datadrivna och analytiska) behövs tillgång till driftdata, systembeskrivningar och incidentrapporter eller -beskrivningar. Data behöver tillgängliggöras och samlas in, lagras och förvaltas. En infrastruktur för överföring och lagring av data över tid behöver byggas upp i form av kontaktnät, tekniska lösningar på datatransport samt databaser för lagring.
- Metodikutveckling av riskidentifiering, riskvärdering och risklindring för obemannade farkoster.
- Utvärdering av metoder för feldetektion och -diagnostik där både missade detektioner och falska alarm testas. Det är viktigt att göra detta för ett fysiskt system och där kan både UAV och UGV som redan finns på FOI användas. Både datadrivna, med inslag av maskininlärning, och modellbaserade metoder kan utvärderas och jämföras och respektive fördelar och nackdelar presenteras.
- Utveckling och analys av felsäkerhet i samverkande system och svärmar.
- Undersökning av möjliga metoder för felsäkerhet med ”adaptiv” autonomi. I svåra situationer kan en människa behöva kliva in och ge stöd i form av fjärrstyrning och beslutsfattande. Det kan vara ett sätt att öka felsäkerheten och graden av autonomi i obemannade farkoster i militära tillämpningar.

På kort sikt kommer arbetet att fokuseras på att utvärdera metoder för feltolerant styrning, implementera datadriven och modellbaserad feldetektion och -diagnostik för att etablera analytisk redundans för en befintlig UAV, samt att undersöka arkitekturer för feltolerant kooperativ navigering i en UAV-svärm.

Litteraturförteckning

[1] E. Branzén och K. Kraft. Felsäkerhet för obemannade farkoster: Domänöversikt, 2023. Totalförsvarets forskningsinstitut, FOI-R--5357--SE.

[2] L. Forssell. Sammanställning av tidigare studier på RPAS, 2022. Totalförsvarets forskningsinstitut, FOI Memo 7583.

[3] J. Rantakokko, J. Appelgren, K. Bengtsson, M. Hagström, O. Jansson, K. Kraft, F. Näsström, F. Kullander, J. Nygårds, M. Pettersson, J. Rydell och R. Woltjer. Gemensamma teknikbehov inom obemannade och autonoma system - Slutrapport, 2021. Totalförsvarets forskningsinstitut, FOI-R--5096--SE.

[4] J. Rantakokko, K. Bengtsson, J. Nygårds, F. Näsström och R. Woltjer. Teknikö-versikt autonoma och obemannade system - Del 2: Markstriden, 2020. Totalförsvarets forskningsinstitut, FOI-R--4901--SE.

[5] J. Rantakokko, F. Näsström, R. Woltjer, T. Mårtensson, M. Hagström och A. Foyer. Tekniköversikt autonoma och obemannade system del 4: Luftstriden, 2022. Totalförsvarets forskningsinstitut, FOI-R--5167--SE.

[6] J. Rantakokko, K. Bengtsson, C. Svensson, R. Lennartsson och M. Skarstind. Tekniköversikt autonoma och obemannade system Del 3: Sjöstriden, 2022. Totalförsvarets forskningsinstitut, FOI-R--5088--SE.

[7] J. Rantakokko. Tekniköversikt autonoma och obemannade system - del 1: Historik, 2019. Totalförsvarets forskningsinstitut, FOI-R--4680--SE.

[8] Jiuping Xu och Lei Xu. Chapter six - fault diagnostics. I: Jiuping Xu och Lei Xu, redaktörer, *Integrated System Health Management*, ss 247–317. Academic Press, 2017.

[9] M. Esperon-Miguez, P. John och I. K. Jennions. A Review of Integrated Vehicle Health Management Tools for Legacy Platforms: Challenges and Opportunities. *Progress in Aerospace Sciences*, 56:19–34, 2013.

[10] L. Rylander, M. Eneberg, J. Mårtensson och A. Pernestål. Design of Diagnosis Service System for Self-Driving Vehicles - Learnings from the Driver's Role Today. *2021 Global Reliability and Prognostics and Health Management (PHM-Nanjing)*, 2021.

[11] X. Tao, J. Mårtensson, Warnquist. H och A. Pernestål. Short-term Maintenance Planning of Autonomous Trucks for Minimizing Economic Risk. *Reliability Engineering and System Safety*, 220:108251–108251, 2021.

[12] S. Orf, M. R. Zofka och J. M. Zöllner. From Level Four to Five: Getting rid of the Safety Driver with Diagnostics in Autonomous Driving. *2020 IEEE International Conference on Multisensor Fusion and Integration for Intelligent Systems (MFI)*, ss 19–25, 2020.

[13] X. Zhao, R. Darwish och A. Pernestål. Automated Vehicle Traffic Control Tower: A Solution to Support the Next Level Automation. *International Journal of Transport and Vehicle Engineering*, 14(7):332 – 342, 2020.

[14] Rolf Isermann. *Fault-Diagnosis Systems From Fault Detection to Fault Tolerance*, band 28. Springer, 01 2006.

[15] H. Al-Asaad. A Simplified Overview of Handling Faults in Systems Around us. *2016 IEEE AUTOTESTCON*, 2016.

[16] Z. Gao, C. Cecati och S. X. Ding. A Survey of Fault Diagnosis and Fault-Tolerant Techniques—Part I: Fault Diagnosis With Model-Based and Signal-Based Approaches. *IEEE Transactions on Industrial Electronics*, 62(6):3757–3767, 2015.

[17] E. Sobhani-Tehrani och K. Khorasani. *Fault Diagnosis of Nonlinear Systems Using a Hybrid Approach*. Springer, 2009.

[18] Försvarsmakten. Försvarsmaktens handbok Systemsäkerhet 2011 Del 1 Gemensam. Teknisk rapport, Försvarsmaktens Säkerhetsinspektion och FMV , 2011.

[19] M. Nyberg och E. Frisk. *Model Based Diagnosis of Technical Processes*. Linköpings universitet, 2000.

[20] ISO Central Secretary. Risk management — Guidelines. Standard ISO 31000-1:2018, International Organization for Standardization, Geneve, Schweiz, 2018.

[21] N. Leveson. *System Safety Engineering: Back To The Future*. Massachusetts Institute of Technology, 2008.

[22] N. Mohan, M. Törngren, V. Izosimov, V. Kaznov, P. Roos, J. Svahn, J. Gustavsson och D. Nesic. Challenges in Architecting Fully Automated Driving; with an Emphasis on Heavy Commercial Vehicles. *2016 Workshop on Automotive Systems/Software Architectures (WASA)*, ss 2–9, 2016.

[23] L. Barr, R. Newman, E. Ancel, C. Belcastro, J. Foster, J. Evans och D. Klyde. Preliminary Risk Assessment for Small Unmanned Aircraft Systems. *17th AIAA Aviation Technology, Integration, and Operations Conference*, 2017.

[24] SAE Levels of Driving Automation™ Refined for Clarity and International Audience, 2021. Society of Automotive Engineers. https://www.sae.org/blog/sae-j3016-update. Hämtad: 11-07-2022.

[25] E. Zibaei, S. Banescu och A. Pretschner. Diagnosis of Safety Incidents for Cyber-Physical Systems: A UAV Example. *2018 3rd International Conference on System Reliability and Safety (ICSRS)*, ss 120–129, 2018.

[26] P. Ma, Y. Wang, X. Su och T. Wang. A Novel Fault Localization Method with Fault Propagation Context Analysis. *2013 Third International Conference on Instrumentation, Measurement, Computer, Communication and Control*, ss 1194–1199, 2013.

[27] A. Kumar, F. Tseng, Y. Guo och R. B. Chinnam. Hidden-Markov Model Based Sequential Clustering for Autonomous Diagnostics. *2008 IEEE International Joint Conference on Neural Networks (IEEE World Congress on Computational Intelligence)*, ss 3345–3351, 2008.

[28] K. A. Masalimov. A Machine Learning based Approach to Autogenerate Diagnostic Models for CNC machines. *2020 35th IEEE/ACM International Conference on Automated Software Engineering (ASE)*, ss 1358–1360, 2020.

[29] N. Ghosh, K. Maity, R. Paul och S. Maity. Outlier Detection in Sensor Data Using Machine Learning Techniques for IoT Framework and Wireless Sensor Networks: A Brief Study. *2019 International Conference on Applied Machine Learning (ICAML)*, ss 187–190, 2019.

[30] F. Emmert-Streib, O. Yli-Harja och M. Dehmer. Explainable Artificial Intelligence and Machine Learning: A Reality Rooted Perspective, 2020.

[31] S. Friedenthal. Types of Models - SEBoK, 2021. https://www.sebokwiki.org/wiki/Types_of_Models. hämtad: 2022-03-22.

[32] S. Friedenthal. What is a Model? - SEBoK, 2021. https://www.sebokwiki.org/wiki/What_is_a_Model%3F. hämtad: 2022-03-24.

[33] A. Kumar. Difference between parametric vs. non-parametric models, 2021. https://vitalflux.com/difference-between-parametric-vs-non-parametric-models/. hämtad: 2022-03-22.

[34] S. Freschi och L. A. Shombert. Optimizing the Use of Component-Level BIT in System-level Test and Diagnosis: a Consistent Diagnostic Information Architecture Approach. *1998 IEEE AUTOTESTCON Proceedings. IEEE Systems Readiness Technology Conference. Test Technology for the 21st Century (Cat. No.98CH36179)*, ss 103–110, 1998.

[35] V. M. Sineglazov och S. O. Dolgorukov. Dynamic Testing of UAV Navigation System. *2017 IEEE 4th International Conference Actual Problems of Unmanned Aerial Vehicles Developments (APUAVD)*, ss 211–214, 2017.

[36] Nationalencyklopedin. https://www.ne.se/info/. Hämtad: 2022-09-27.

[37] A. S. Willsky. A Survey of Design Methods for Failure Detection in Dynamic Systems. *Automatica*, 12(6):601–611, 1976.

FOI är en huvudsakligen uppdragsfinansierad myndighet under Försvarsdepartementet. Kärnverksamheten är forskning, metod- och teknikutveckling till nytta för försvar och säkerhet. Organisationen har cirka 1000 anställda varav ungefär 800 är forskare. Detta gör organisationen till Sveriges största forskningsinstitut. FOI ger kunderna tillgång till ledande expertis inom ett stort antal tillämpningsområden såsom säkerhetspolitiska studier och analyser inom försvar och säkerhet, bedömning av olika typer av hot, system för ledning och hantering av kriser, skydd mot och hantering av farliga ämnen, IT-säkerhet och nya sensorers möjligheter.

FOI
Totalförsvarets forskningsinstitut
164 90 Stockholm

Tel: 08-55 50 30 00
Fax: 08-55 50 31 00

www.foi.se