



id: SI_005

model: anthropic/claude-opus-4.6

seeds:

04_risiko: sårbarhet

03_relasjon: tillit

05_handling: implementer

01_perspektiv: strategisk

02_tidhorisont: kortsiktig

Instans SI_005

Seeds: strategisk | kortsiktig | tillit | sårbarhet | implementer

Perspektiv: Implementeringssårbarhet som strategisk kjerne

De fleste FoU-prosjekter innen krisehåndtering feiler ikke på forskning — de feiler på **implementering**. Min analyse starter derfra.

Hva gjør dette sårbart?

Kontrollplattformen din har én kritisk svakhet: **tillitskjeden**. Kommandosentralen er verdiløs hvis feltinstansene (droner, sensorer, brannmannskaper) ikke stoler på dataene — eller omvendt. Tillit bygges ikke i arkitektur, men i **kortsiktige, repeterbare tester** der feil eksponeres tidlig.



Hvem må med — og hvorfor akkurat disse?

Partner	Rolle	Strategisk begrunnelse
DSB	Sluttbruker/kravstiller	Uten DSB har du ingen implementeringsvei
NIBIO	Brannprediksjonsmodeller (terreng, vegetasjon)	Norsk kontekst, FARSITE-kompetanse
FFI	Sanntidssensorikk, C2-systemer	Allerede FoU på kommando/kontroll
Sopra Steria/Kongsberg	Systemintegrator	Plattformkompetanse, TRL-løfting
RISE (Sverige) / CEREN (Frankrike)	Internasjonal testfasiliteter	Storskala branntesting Norge mangler
Universitetet i Agder / NTNU	ML-prediksjonsmodeller, IoT	Akademisk forankring

Finansiering

- **Kortsiktig (0-12 mnd):** Forskningsrådets IPN (Innovasjonsprosjekt i næringslivet), budsjett 15-25 MNOK, 3 år. Tematisk åpning: «Samfunnssikkerhet og beredskap».
- **EU:** Horizon Europe Cluster 3 (Civil Security), spesifikt HORIZON-CL3-2025-DRS — krev internasjonal partner.
- **NATO DIANA** for dual-use sensorikk.

Arbeidspakker — designet for sårbarhetshåndtering

AP1: Tillitsarkitektur (M1-M8) — Definer dataflyt, autentisering, fallback ved nettverkstap. Hvem ser hva, når? Zero-trust-modell.

AP2: Prediksjonsmotor (M1-M18) — Koble FARSITE/Prometheus med live sensordata (vind, fuktighet, IR-satellitt via Copernicus EMS). Kortsiktig prediksjon (0-6 timer) prioriteres over langsiktig — det er der beslutninger tas.

AP3: Koordineringsprotokoll (M6-M24) — Svermintelligens for droner/sensorer. MQTT-basert meldingslag. Test: Kan en instans miste forbindelse i 20 min uten at systemet degraderer?

AP4: Felttest og validering (M12-M30) — Kontrollerte branner (CEREN, Frankrike). Norsk pilottest med Sivilforsvaret. **Her avdekkes sårbarhetene** — dette er prosjektets egentlige kjerne.

AP5: Implementeringspakke (M24-M36) — Operasjonalisering mot DSB/110-sentraler. Uten denne er alt akademisk øvelse.



Hva er genuint unikt?

Dissens-poeng: De fleste prosjekter selger «AI-prediksjonsplattform». Det unike her er **sanntids tillitssikret koordinering under kaos** — der data er usikker, nettverk faller ut, og mennesker må stole på maskiner under livsfare. Det er et **menneske-maskin-tillit-problem**, ikke primært et datavitenskap-problem.

Neste steg

1. **Denne uken:** Book møte med DSB Beredskapsavdelingen og FFI avd. Beskyttelse — uten disse to er prosjektet uten implementeringsvei
2. **Innen 30 dager:** Skriv 2-siders konseptnotat med sårbarhetsfokus, send til Forskningsrådets programrådgiver for IPN Samfunnssikkerhet for tidlig tilbakemelding
3. **Innen 60 dager:** Gjennomfør tabletop-øvelse med potensielle partnere — simuler et brannscenario der systemet feiler, og observer hvor tilliten bryter sammen