



id: SI_001

model: mistralai/mistral-large-2512

seeds:

04_risiko: sårbarhet

03_relasjon: samarbeid

05_handling: aksepter

01_perspektiv: bruker

02_tidhorisont: kortsiktig

Instans SI_001

Seeds: bruker (frontlinjen som menneske, ikke ressurs) | kortsiktig (minutter/timer, ikke dager) | samarbeid (ikke hierarki) | sårbarhet (åpenhet om usikkerhet) | aksepter (feil som læringsgrunnlag)

Unikt perspektiv: “Sårbar koordinering”

Tradisjonelle kontrollplattformer bygger på perfekte data og toppstyrt kontroll. SI_001 snur dette: **Plattformen må designes for å håndtere kaos, ikke unngå det.** Brannens retning er aldri 100% predikerbar – derfor må systemet akseptere usikkerhet og eksponere sårbarhet i sanntid. Eksempel: Når en drone melder om vindskifte, skal ikke kommandosenteret vente på bekreftelse, men umiddelbart dele rådata med alle instanser – inkludert usikkerhetsmarginer. Dette krever en kultur der feilrapportering belønnes, ikke straffes.

Hvem må med? (Ikke bare de vanlige)

- Frontlinje-brukere** (røykdykkere, lokale skogvoktere, frivillige): De skal designe varslingsgrensesnitt, ikke bare bruke dem. Eksempel: En røykdykker i Australia (Black Summer 2019) rapporterte at varslingsystemet ignorerte lokale vindmønstre – dette ville vært unngått med brukerstyrt utvikling.
- Sårbare grupper:** Eldre, funksjonshemmede, urfolk (f.eks. samiske reinbeitedistrikter). De må ha egne kortsiktige varslingskanaler (SMS, lokalkjente lydsignaler) fordi de faller utenfor standard varslings.
- Internasjonale “failure labs”:** Samarbeid med brannkorps som har mislykkes (f.eks. Californias 2018 Camp Fire, hvor kommunikasjonsbrudd kostet 85 liv). Disse har akseptert sårbarhet og kan bidra med “worst-case”-scenarier.



FoU-prosjekt: 3 arbeidspakker (AP) med seed-integrering

AP1: “Usikkerhetsmotor” (6 mnd)

- Utvikle en algoritme som kontinuerlig kvantifiserer usikkerhet i prediksjoner (f.eks. “60% sannsynlig at brannen snur nordover, men $\pm 20\%$ ”). Data deles automatisk med alle instanser via en “sårbarhetsfeed”.
- **Test:** Simulere branner der 30% av dataene er feil – hvordan reagerer systemet? (Ikke “hvordan unngår vi feil?”)

AP2: “Frontlinje-laboratorium” (12 mnd)

- Lokale brannkorps og frivillige får midlertidig kontroll over deler av plattformen (f.eks. å overstyre varslingsgrenser). Målet er å akseptere at hierarkiet brytes når situasjonen krever det.
- **Test:** “Kaosøvelser” der kommandosenteret mister kontroll i 2 timer – hvordan tilpasser brukerne seg?

AP3: “Sikkerhetsparadokset” (9 mnd)

- Sikkerhet handler ikke om å eliminere risiko, men om å dele den. Eksempel: Når en røykdykker melder om utmattelse, skal systemet umiddelbart omdirigere oppgaver til andre – ikke vente på godkjenning.
- **Test:** “Etisk hacking” der teamet prøver å skjule feil – klarer systemet å avsløre dem via brukerrapportering?

Dissens: Mot “full kontroll”-myten

De fleste plattformer søker fullstendig oversikt. SI_001 sier: **Det er umulig, og farlig å late som.** I stedet for å jage perfekte prediksjoner, bør 30% av FoU-budsjettet gå til å trene brukerne i å håndtere usikkerhet (f.eks. “hvordan ta beslutninger med 50% usikre data”).

Neste steg

1. **Kartlegg “failure cases”:** Kontakt brannkorps i Portugal (2017), Sverige (2018) og Australia (2019) for å hente ut hva som gikk galt – ikke bare “beste praksis”.
2. **Pilot med sårbare grupper:** Start et 3-måneders samarbeid med en samisk reinbeitedistrikt for å utvikle ikke-digitale varslingsmetoder (f.eks. radiokanaler med lokalkjente koder).
3. **Bygg en “usikkerhetsprototype”:** Lag en enkel versjon av plattformen der alle data vises med usikkerhetsmarginer – test den i en kontrollert brannøvelse innen 6 måneder.



SI_001s kjerne: En kontrollplattform er ikke et verktøy for å styre brannen – det er et samarbeidsrom for å overleve den.