



id: SI\_003

model: google/gemma-4-26b-a4b-it

seeds:

04\_risiko: sårbarhet

03\_relasjon: makt

05\_handling: forhandle

01\_perspektiv: operasjonell

02\_tidhorisont: historisk

## Instans SI\_003

**Seeds:** operasjonell | historisk | makt | sårbarhet | forhandle

Analysen av kontrollplattformen skifter fokus fra “verktøy” til “systemisk kontrollmekanisme”.

**Det unike perspektivet:** Mainstream vil fokusere på sensorer og algoritmer. SI\_003 ser at hovedutfordringen ikke er data, men **maktfordeling** og **informasjonsasymmetri**. I dag er brannbekjempelse fragmentert; hver instans (kommune, statsforvalter, luftambulans) sitter på sin egen “sannhet”. Din plattform må ikke bare være en visualisering, men et digitalt suverenitetsverktøy som tvinger frem en felles situasjonsforståelse.

**Strategisk partnerskap (Forhandling):** Ikke start med IT-leverandører. Start med de som har det operasjonelle ansvaret og de som eier risikoen:

1. **Operasjonelle kjerneaktører:** DSB (Direktoratet for samfunnssikkerhet og beredskap) og Sivilforsvaret.
2. **Teknisk autoritet:** NORSAR eller MET (Meteorologisk institutt) for prediksjonsmodeller.
3. **Industriell makt:** Forsvarssektoren (for sensor-teknologi og kryptert kommunikasjon).

**FoU-struktur (Arbeidspakker):** Vi må unngå “pilot-fellen” hvor systemet dør etter testfasen.

- **WP1: Protokoll-standardisering (Makt/Forhandle):** Hvordan definerer vi “sannhet”? Utvikle en felles datastandard som gjør at en drone fra en privat aktør snakker samme språk som et militært helikopter.



- **WP2: Prediktiv Sårbarhetsanalyse (Sårbarhet):** Implementering av digitale tvillinger av landskapet som ikke bare ser brann, men ser hva brannen treffer (infrastruktur, kraftnett, bebyggelse).
- **WP3: Operasjonell Kommandosentral (Operasjonell):** Høy-redundant UI som tåler informasjons-overload.

**Testmetodikk:** Glem simulerte øvelser i kontorlandskap. Vi krever **“Live-Stress-Testing”**:

- **Fase 1:** Shadow-mode under reelle skogbranner (plattformen kjører i bakgrunnen uten å styre).
- **Fase 2:** Kontrollert “Chaos Engineering” – injisering av falske/feilaktige sensordata for å teste systemets evne til å oppdage manipulasjon (sikkerhet).

**Dissens:** Mainstream vil bygge en sentralisert “Gud-modus”. Dette er en sårbarhet. Hvis kommandosenteret faller, faller alt. Jeg foreslår en **desentralisert kommandostruktur** hvor plattformen fungerer som en distribuert ledger (liknende blockchain) for situasjonsdata, slik at kontrollen kan flyttes til felten hvis sentralen går ned.

**Neste steg:**

1. Identifiser én nasjonal nøkkelperson i DSB for en uformell “validere-konseptet”-samtale.
2. Utarbeid en teknisk kravspesifikasjon som prioriterer interoperabilitet over funksjonalitet.
3. Definer de 3 mest kritiske sårbarhetene i dagens manuelle koordinering.