



id: SI\_007

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

seeds:

04\_risiko: mulighet

03\_relasjon: makt

05\_handling: implementer

01\_perspektiv: operasjonell

02\_tidhorisont: kortsiktig

## Instans SI\_007

**Seeds:** operasjonell | kortsiktig | makt | mulighet | implementer

Analysen av kontrollplattformen for skogbrannhåndtering er ferdigstilt. Her er den strategiske rammen:

### Strategisk Analyse

Mainstream tilnærming vil fokusere på “samarbeid” og “miljø”. Dette er feil. For å lykkes må vi fokusere på **makt** gjennom informasjonsmonopol. Den som kontrollerer sanntidsdataene, kontrollerer beslutningshierarkiet. Plattformen må ikke bare være et verktøy, men det sentrale nervesystemet som tvinger alle instanser (Brannvesen, Sivilforsvaret, Forsvaret, NVE) inn i en felles **operasjonell** rytme.

**Mulighet:** Ved å integrere satellittdata (Copernicus/Sentinel) med lokale IoT-sensorer og droner, skaper vi en prediktiv overlegenhet som dagens fragmenterte systemer mangler.

### FoU-Konstruksjon (Arbeidspakker)

Vi danner ikke et “prosjekt”, vi bygger en kommando-infrastruktur.

- WP1: Data-aggregering & Sensorfusjon (Kortsiktig):** Etablere API-koblinger mot Meteorologisk institutt, Copernicus og lokale værstasjoner. Mål: < 5 sekunders latenstid fra sensor til skjerm.
- WP2: Prediktiv Algoritme-motor (Makt):** Utvikle maskinlæringsmodeller som ikke bare viser brannen, men “skygger” brannens sannsynlige bevegelse de neste 120 minuttene basert på topografi og vindvektorer.



3. **WP3: Sikkerhet & Protokoll (Operasjonell):** Implementere kryptert kommunikasjon (AES-256) som fungerer selv når mobilnettet kollapser (satellitt-backhaul).
4. **WP4: Grensesnitt for Kommandosenter (Implementer):** Et "Single Source of Truth"-dashboard.

## Testregime

Glem simuleringer i kontorlandskap. Vi krever **Live-Field Testing**:

- **Fase 1:** Digital Tvilling-testing i kontrollerte brenningsfelt.
- **Fase 2:** Stress-test under simulert nettverkskollaps i utmark.
- **Fase 3:** Integrasjon med nasjonale beredskapssentraler (DSB).

## Dissens

Mainstream vil si "åpen kildekode for alle". SI\_007 sier: **Nei**. Kontrollplattformen må være en lukket, autoritær struktur. Hvis alle kan endre parameterne, mister kommandosenteret sin makt og evne til å styre kaoset. Sikkerhet trumfer transparens.

### Neste steg:

1. Identifiser tekniske partnere (f.eks. Kongsberg Defence & Aerospace eller SINTEF Digital) for å sikre teknologisk makt.
2. Utarbeid et kravspesifikasjonsdokument med fokus på ekstrem lav latens.
3. Søk midler fra Forskningsrådet/EU Horizon under kategorien "Critical Infrastructure Resilience".