



id: SI\_003

model: anthropic/claude-opus-4.6

seeds:

04\_risiko: sårbarhet

03\_relasjon: makt

05\_handling: implementer

01\_perspektiv: strategisk

02\_tidhorisont: langsiktig

## Instans SI\_003

**Seeds:** strategisk | langsiktig | makt | sårbarhet | implementer

### Strategisk maktanalyse: Hvem eier brannen — og hvem eier dataen?

Dette er ikke et teknologiprojekt. Det er et **maktprosjekt**. Den som kontrollerer sanntidsdata om brannspredning, kontrollerer beslutningene — evakuering, ressursallokering, skyldfordeling. Sårbarheten ligger ikke i brannen, men i **hvem som får tilgang til plattformen og når**.

### Unik posisjonering

Eksisterende systemer (EFFIS, FIRMS/NASA, Canada's CWFIS) er **observasjonsverktøy**, ikke kommandoplattformer. Ditt prosjekt skiller seg ved å integrere **prediktiv styring + koordinert svarmstyring av ressurser + beslutningsautoritet i sanntid**. Det unike er den lukkede kontrollsløyfen: sensor → prediksjon → ordre → verifikasjon.

**Dissens-poeng:** De fleste FoU-prosjekter undervurderer det politiske. DSB, kommuner og Forsvaret har overlappende mandater ved skogbrann. Plattformen må implementere en maktstruktur — hvem overruler hvem? Dette må designes inn, ikke løses etterpå.



## Konsortium (maktbalansert)

Rolle	Aktør	Hvorfor
Prosjekteier/koordinator	SINTEF Digital / FFI	Strategisk tyngde, NATO-kobling
Domeneekspert	DSB + Nibio	Brannmodellering, skogdata
Sanntidssensor	Andøya Space / Kongsberg	Satellitt + droner, langsiktig industribygging
AI/prediksjon	UiO/IFI eller NTNU IDI	Maskinlæring brannspredning
Sårbarhet/sikkerhet	mnemonic / NSM	Cybersikkerhet kommandoplattform
Sluttbruker	110-sentralen, Sivilforsvaret	Reell operativ testing

## Finansiering

- **Forskningsrådet:** IKTPLUSS eller BRANNSIKKERHET (8-15 MNOK, 3-4 år)
- **EU Horizon Europe:** Cluster 3 “Civil Security for Society” — DRS-calls (4-6 MEUR)
- **EØS/Nordisk:** NordForsk klimatilpasning
- **NATO SPS** hvis dual-use vinkles mot Forsvaret

## Arbeidspakker (implementeringsfokus)

**AP1 — Sårbarhetskartlegging** (M1-12): Trusselmodell for plattformen selv. Hvem angriper et brannkontrollsystem? Insider-trussel, GPS-spoofing av droner, falske sensordata.

**AP2 — Prediksjonsmotor** (M1-24): Ensemble-modell: topografi + vind + fuktighet + vegetasjon. Trenes på historiske data (Nibio/Met), valideres mot faktiske branner.

**AP3 — Svermkoordinering** (M6-30): Protokoll for instans-synkronisering. Latenskrav <2 sek. Graceful degradation ved kommunikasjonstap — **den farligste sårbarheten**.

**AP4 — Kommandostruktur-design** (M6-24): Juridisk og operativt: hvem har beslutningsmakt på plattformen? Implementer rollebasert tilgang med eskaleringsprotokoller.

**AP5 — Feltest** (M24-36): Live-øvelse med 110-sentral. Kontrollert brenning (Nibio Hoxmark) med dronesverm + prediksjonsvalidering.



---

## Neste steg

1. **Innen 2 uker:** Booking av møte med FFI (avd. Totalforsvar) og DSB for å avklare maktfordelingsspørsmålet — dette avgjør hele arkitekturen
2. **Innen 6 uker:** Skriv 2-siders konseptnotat rettet mot Forskningsrådets IKTPLUSS med eksplisitt dual-use argument, og send til SINTEF Digital for partnersonderinger
3. **Parallelt:** Kontakt DG HOME i EU-kommisjonen for å time søknaden mot neste Horizon Europe DRS-utlysning (frist typisk mars 2026)