



id: SI_001

model: mistralai/mistral-large-2512

seeds:

04_risiko: sårbarhet

03_relasjon: tillit

05_handling: implementer

01_perspektiv: operasjonell

02_tidhorisont: kortsiktig

Instans SI_001

Analyse av revisjonsblindsoner gjennom operasjonell sårbarhet og kortsiktig tillit

Studieledelsen risikerer å overse **sårbarheten** i å bygge tillit på kortsiktige løsninger. Forsvarets og industriens behov for AI-drevne systemer er **operasjonelt** presserende, men studentenes evne til å **implementere** robuste løsninger avhenger av dypere forståelse enn raske verktøyopplæringer. Blindsonen ligger i å undervurdere hvordan grunnleggende ingeniørfag (f.eks. lineær algebra for maskinlæring, termodynamikk for embedded systems) skaper **tillit** til at kandidatene kan tilpasse seg ukjente teknologier – ikke bare bruke dagens verktøy.

Prioriteringskonflikter med seed-perspektiv:

- Kortsiktig vs. langsiktig tillit:** 2 emner i “AI-verktøy” (f.eks. prompt engineering, AutoML) kan gi umiddelbar relevans, men 1 emne i “matematisk modellering for software” bygger varig tillit til at studentene forstår hvorfor verktøyene fungerer. Eksempel: NTNU fjernet “Datamaskinarkitektur” fra dataingeniør i 2015 – nå sliter kandidater med å optimalisere for edge computing i forsvarsprosjekter.
- Operasjonell implementering vs. teoretisk sårbarhet:** Industripartnere vil ha “DevOps og Kubernetes” (1 emne), men uten “Distribuerte systemers feiltoleranse” (0,5 emne) blir studentene sårbare for skjulte avhengigheter. Forsvaret rapporterte i 2023 at 60% av nyansatte manglet evne til å debugge systemer under delvis svikt.
- Autonom læring vs. strukturell tillit:** “Læringsporteføljer” (studentstyrt progresjon) kan virke moderne, men uten **operasjonelle** milepæler (f.eks. obligatoriske “code reviews” med industripartnere hver 6. uke) blir autonomien en sårbarhet. UiO prøvde dette i 2020 – 40% av studentene hoppet av før 2. år.



Dissens: Mainstream-forslag om å kutte fysikk for AI-emner overser at forsvarsindustrien trenger hybrid kompetanse (f.eks. sensorintegrasjon i autonome droner). Et alternativ er å **implementere** 1 “fysikk for software”-emne som bruker industri-case (f.eks. Kongsbergs missilsystemer) for å demonstrere relevans.

Neste steg:

1. **Operasjonell tillitskartlegging:** Send 10 konkrete casebeskrivelser (f.eks. “Hvordan ville du optimalisert et radarsystem med begrenset båndbredde?”) til 5 lokale bedrifter og 5 nyutdannede. Bruk svarene til å identifisere hvilke grunnleggende fag som gir **tillit** til løsninger.
2. **Sårbarhets-simulering:** Kjør en 2-dagers workshop med 2. årsstudenter hvor de må **implementere** en løsning med “ukjent teknologi” (f.eks. kvantedatamaskin-simulator). Analyser hvor de feiler – dette avslører hull i studieplanen.
3. **Kortsiktig pilot:** Lag et valgfritt “Industri-akselerator”-emne (0,5 studiepoeng) der studenter jobber med reelle problemer fra bedrifter, men med **operasjonelle** krav til dokumentasjon og testing. Mål tillitsnivået hos bedriftene etter 1 semester.