

FoU-utfordringer innen IT-sikkerhet

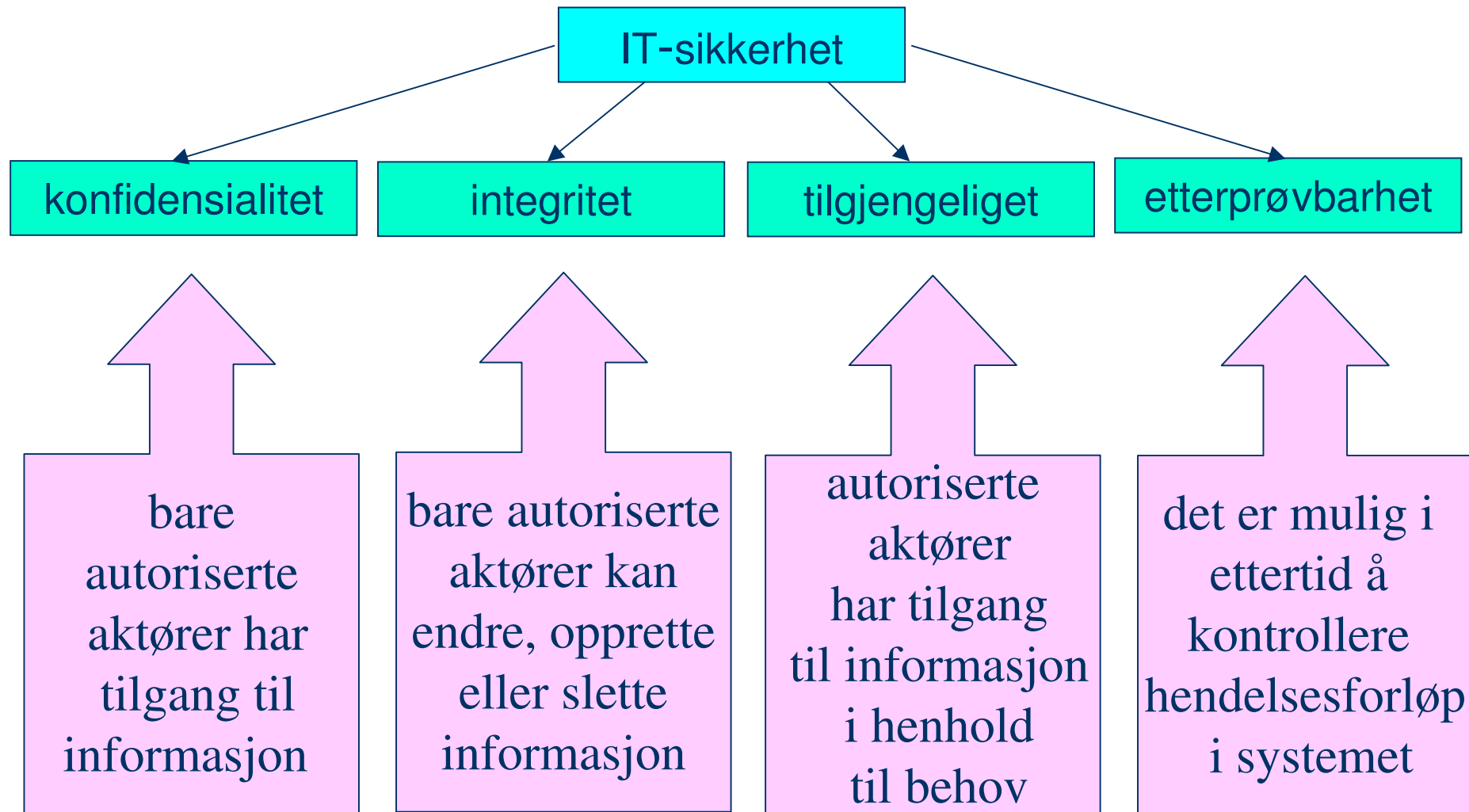
Ketil Stølen
SINTEF
6. mars 2003

Innhold

- **IT-sikkerhet** – hva er det?
- **IT-sikkerhet** er ikke kun teknologi
- **IT-sikkerhet** forutsetter risikoanalyse
- **IT-sikkerhet** – en del av systemutviklingen
- **IT-sikkerhet** må understøttes av verktøy

- **IT-sikkerhet** – tema for SINTEF-forskning
- **IT-sikkerhet** prioriteres av NFR og EU

IT-sikkerhet – hva er det?



IT-sikkerhet er ikke kun teknologi

- Sikkerhet krever ikke bare teknisk forståelse.
- Sikkerhetsproblemer er ofte av ikke-teknisk art.
- Mange sikkerhetsproblemer har et internt opphav
- Organiseringen av informasjonssikringen og medarbeidernes kunnskap og holdninger er minst like viktig som teknologien.
- En forsvarlig sikkerhetsevaluering forutsetter en uniform beskrivelse av systemet som helhet:
 - hvordan det brukes
 - virksomheten rundt
 - teknologien

IT-sikkerhet forutsetter risikoanalyse

- Risikoanalyse er et middel til å identifisere sikkerhetsbehov og sikkerhetsløsninger som svarer til disse behovene.
- Rent teknisk er nødvendig sikkerhetsteknologi tilgjengelig.
- Men hva skal man med sikkerhet hvis ingen kan bruke systemene?
- Identifiser først sikkerhetsbehov.
- Velg løsning deretter.

IT-sikkerhet – en del av systemutviklingen

- Sikkerhet adresseres tradisjonelt først etter at systemet er “ferdig”.
- Kravanalyse og risikoanalyse er to sider av samme sak og bør integreres.
- Kravanalysen fokuserer på ønsket oppførsel
 - **Involverer:** Brukere, utviklere, tekniske eksperter, ledere
 - **Virkemiddel:** Spesifikasjon av bruksscenarier
 - **Resultat:** Kravspesifikasjon
- Risikoanalysen fokuserer på uønsket oppførsel
 - **Involverer:** Brukere, utviklere, tekniske eksperter, ledere
 - **Virkemiddel:** Spesifikasjon av trusselscenarier
 - **Resultat:** Risikoakseptanskriterier

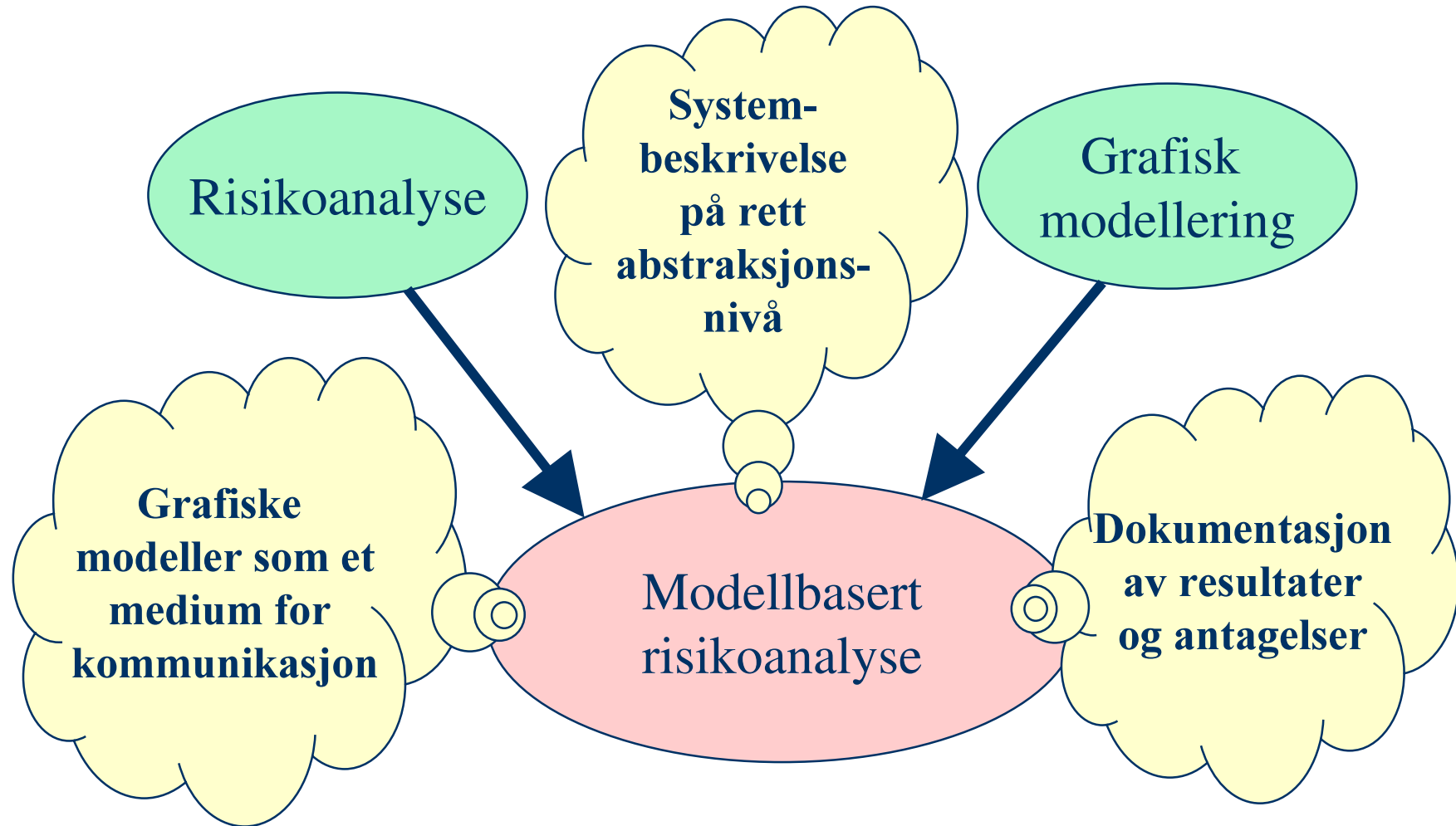
IT-sikkerhet må understøttes av verktøy

- Vi trenger verktøy som understøtter
 - sikkerhetsarkitektur og funksjonalitet
 - monitorering
 - sårbarhetsanalyse
- Men det er ikke nok!
- Vi trenger også verktøy som understøtter
 - sikkerhetsdokumentasjon
 - sikkerhetstesting
 - vedlikehold av sikkerhetsløsninger
 - gjenbruk av sikkerhetserfaringer
 - modelldrevet sikkerhetsarkitektur

IT-sikkerhet – tema for SINTEF-forskning

- **CORAS (2001-2003)** – Budsjett: 40 MNOK
 - Full tittel: *A platform for risk analysis of security critical systems*
 - EU-prosjekt med elleve partnere fra fire europeiske land
 - Norske partnere: IFE, NR, NST, Telenor, SINTEF
 - Har utviklet en vertøystøttet metodikk for modellbasert risikoanalyse rettet mot IT-sikkerhet
 - Anvendt innen e-handel og telemedisin
- <http://www.nr.no/coras>

IT-sikkerhet - Modellbasert risikoanalyse



IT-sikkerhet – tema for SINTEF-forskning

■ iTrust (2002-2005) – Budsjett: 4 MNOK

- Full tittel: *Arbeidsgruppe på tillitsledelse i åpne dynamiske systemer*
 - EU-prosjekt med mer enn 20 europeiske partnere
 - Norske partnere: IRI, SINTEF
 - Forum for flerfaglig undersøkelse av tillit som et middel og forutsetning for etablering av en global IT-infrastruktur
- <http://www.itrust.uoc.gr/>

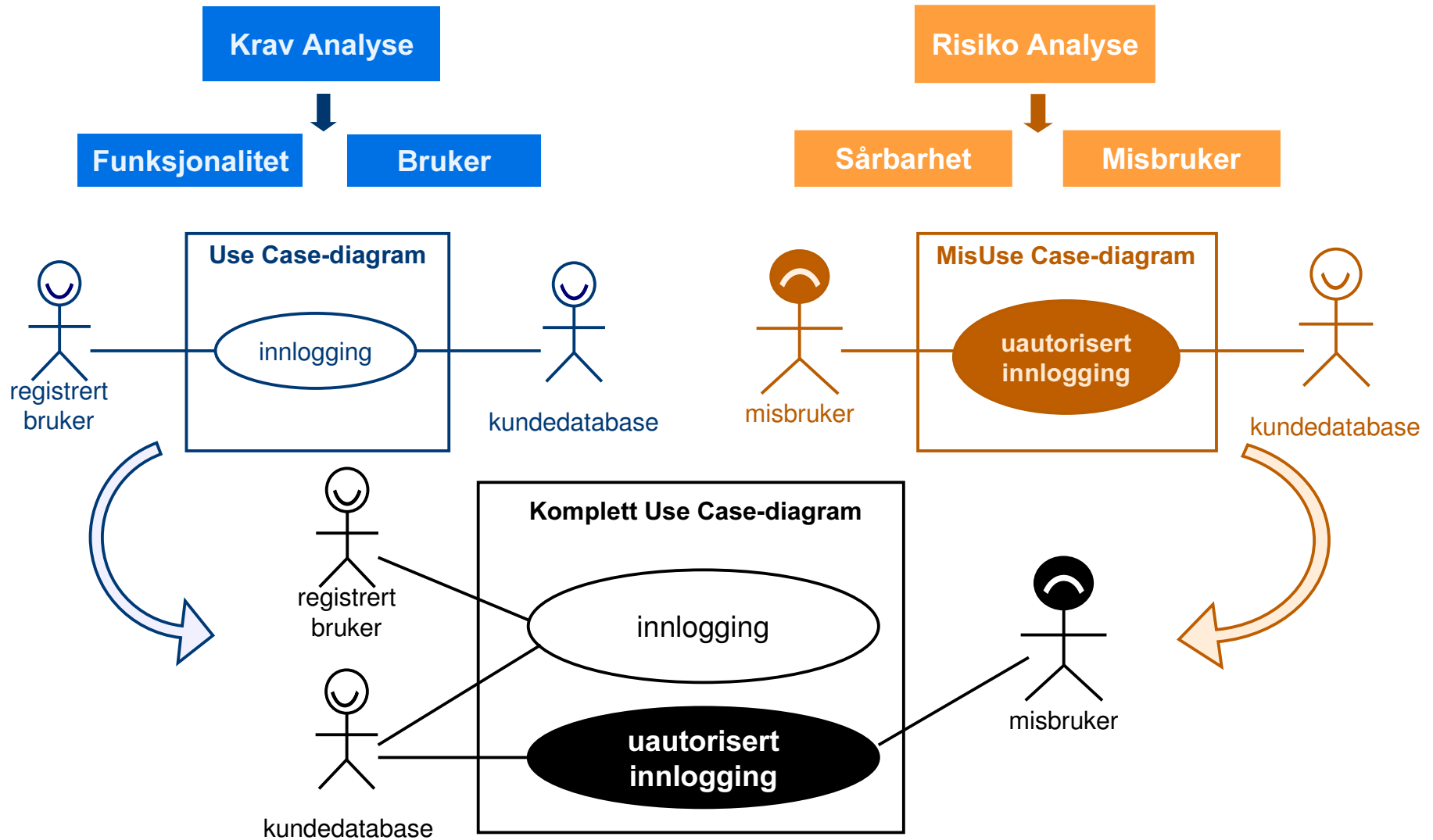
IT-sikkerhet – tema for SINTEF-forskning

- **SARDAS (2003-2006)** – Budsjett: 8 MNOK
 - Full tittel: *Sikring av tilgjengelighet ved robust design, evaluering og spesifisering*
 - Støttes av Forskningsrådets program: *Grunnleggende IKT Forskning*
 - Partnere: Ericsson, NTNU, UIO, SINTEF
- <http://www.ifi.uio.no/~ketils/sardas/sardas.htm>

IT-sikkerhet – tema for SINTEF-forskning

- **SECURIS (2003-2006)** – Budsjett: 12 MNOK
 - Full tittel: *Modelldrevet utvikling og analyse av sikre IT-systemer*
 - NFR prosjekt - Kompetanseprosjekt med brukermedvirkning
 - Partnere: FLO/IKT, NetCom, SIS, SINTEF
 - Konsortiet vil bli utvidet med to bedriftspartnere
- <http://www.informatics.sintef.no/projects/securis/>

IT-sikkerhet – integrert analyse



IT sikkerhet prioriteres av NFR og EU

■ NFR

- Program for “IKT sikkerhet og sårbarhet”
- 59 MNOK 2003-2007

■ EUs sjette rammeprogram (6FP)

- Strategisk målsetning for 2003/04-programmet:
 - **Towards a global dependability and security framework**
- Første søknadsfrist: 24. april

■ SINTEF er aktivt med på mer enn 120 6FP-initiativer

- Samarbeider gjerne med norske bedrifter og institusjoner
- **Ta kontakt!**