Modellering av avhengigheter i samfunnskritisk infrastruktur

Utfordringer og tilnærminger

Nils Kalstad Svendsen
nilss@hig.no

Norsk Informasjonssikkerhets Laboratorium (NISlab)

15. januar 2009

Oversikt

Brann OsloS 28.11.2007

- 800 persontog og godstog helt eller delvis innstilt
- 80000 passasjerer berørt
- 25000 internettbrukere mistet tilgangen i mer enn 10 timer
- Vitale systemer hos bl.a. politiet gikk ned

Steigen 25.01.2007

- Fem dagers strømbrudd, soneinndeling med 2 timer strøm pr. dag
- Prioriteringsliste
  - Liv og helse
  - Dyrehelse
  - Sikring av materielle verdier

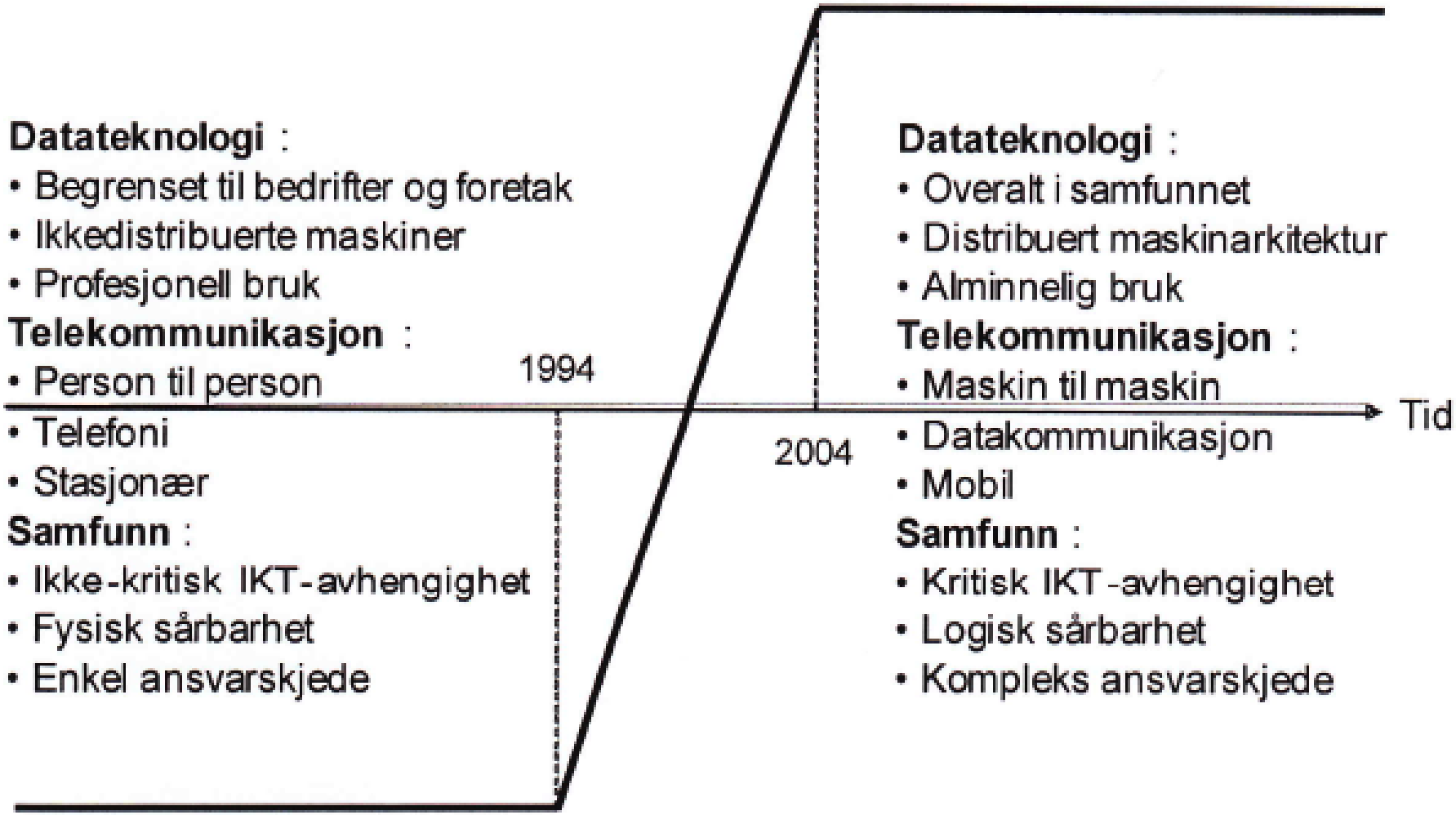
Andre hendelser

- Strømbrudd i nord-østlige deler av USA og Kanada (08.2003)
  - Et kullkraftverk gikk ned
  - Økt belastning på reservelinjer
  - Manglende linjerydding og feilkjede
  - 50 millioner berørte mennesker, tap på 6 milliarder dollar
- Strømbrudd i vestlige Europa (11.2006)
  - E-on skulle slå av en 380000 volt linje over Ems
  - 10 millioner mennesker berørt av strømbruddet i Tyskland, Frankrike, Belgia, Italia, Spania, Østerrike, Nederland og Kroatia
- Påstått Russisk tjenestenekt angrep på Estland (11.2007)
- Påstått Russisk tjenestenekt angrep på Georgia (08.2008)

Et sårbart samfunn

- Offentlige utredninger
  - NOU 1986:12 Datateknikk og samfunnets sårbarhet
  - NOU 2000:24 Et sårbart samfunn
  - NOU 2006:6 Når sikkerheten er viktigst
- FFI: Beskyttelse av samfunnet (BAS)
  - Tidlig fase (1990-tallet): Definerte 14 samfunnsfunksjoner
  - Nav: Kraftforsyning og telekommunikasjon

Et sårbart samfunn



Jan A. Audestad *E-bomber og e-granater: Om IKT og sårbarhet*

Definisjon av samfunnskritisk infrastruktur

Definition (Infrastruktur)

En infrastruktur er et nettverk av uavhengige, i hovedsak privat eide, menneskeskapte systemer og prosesser som fungerer i sammen for å produsere og distribuere en kontinuerlig flyt av essensielle varer og tjenester

Definition (Kritisk infrastruktur (CI))

Kritisk infrastruktur er definert som den mengden av tjenester hvis opphør over tid vil ha store konsekvenser på befolkningen, f.eks. sette liv og helse på spill og skape store økonomiske konsekvenser

Beskyttelse av samfunnskritisk infrastruktur (CIP) er beskyttelse av CI.

Hovedutfordringer ved CIP

- Infrastrukturene er ofte i privat eie
- Eierne er gjerne utenlandske
- Infrastrukturen respekterer ikke nødvendigvis landegrensene
- Mange perspektiver
  - Teknisk
  - Forretningsmessig
  - Juridisk
  - Forsvarsmessig
  - Regulatoriske føringer
  - Nasjonale og internasjonale sikkerhetshensyn
- Krever samarbeid

En proaktiv tilnærming til CIP

Definition (Proaktiv)

Å skape eller kontrollere en situasjon ved å forårsake at noe skjer, framfor å reagere etter at det har skjedd.

En proaktiv tilnærming er hensiktsmessig for

- Langsiktig planlegging
- Operator trening
- Beslutningsstøtte

Mulige tilnærminger til proaktiv scenario beskrivelse i CI

- Eksperimentering: Ikke mulig
- Trening på fullskala modeller: Kostbart og lite fleksibelt
- Simulering: Et mulig alternativ

Utfordringer for simulering av CIP

- Dimensjonsspenn
  - Deler og enheter
  - Undersystemer og systemer
  - Infrastrukturer og sammenkoplede infrastrukturer
- Data
  - Tilgjengelighet for validering og initiering av modeller
  - Databaseadministrasjon (distribuert, flere eiere)
  - Kvaliteten på de tilgjengelige data
  - Tidssynkronisering av tilgjengelige data
  - Sikkerhetsaspekter ved en detaljert database koplet sammen med et simuleringsverktøy

Utfordringer for simulering av CIP

- Validering
  - Tilgjengelighet av data
  - Størrelsen på tilstands- og hendelsesrommet
  - Hva er sannsynlige antalgelser og abstraksjoner
- Metrikker
  - Relevant og uavhengig av infrastruktur
  - Signifikans av måleresultater
- Den menneskelige faktoren
  - Vanlig årsak til feil
  - Rasjonelle beslutninger basert på feilaktig informasjon

Detaljerte modeller eksisterer for individuelle infrastrukturer

Teknikker for simulering av CI

	CI egenskaper	*Kompl*	*Feiling*
Forsyning og etterspørsel	Høy nivå	Lav	Ingen
Innputt-utputt	Sektor interaksjon	Lav	Prop
System dynamikk	Flyt og sykler	Høy	Diverse
Agent baserte	Oppførsel	Voksende	Diverse
Statistikk	Strukturell	Lav	Oppe/nede
Fysikk	Detaljert	Høy	Diverse

Flernivå modell

En kombinasjon av modeller på flere nivåer

- Multigrafmodell for fysiske avhengigheter
  - Noder representerer produsenter og forbrukere
  - Avhengigheter representerer av kanter som bærer avhengighetstyper
  - Fysiske egenskaper tilegnes avhengighetstypene
- Romlig modell for geografiske avhengigheter
  - Fanger opp nærhet mellom infrastrukturer
  - Ikke-trivielle avhengigheter
  - Kvantifisering av nærhet
- Avviksdetektering i kontinuerlige prosesser
  - Kopling mellom fysiske prosesser og informasjonslaget
  - Utforskning av angrepsvektorer og beskyttelsesstrategier

Flernivå modell

- En vedkjennelse av at en modell ikke kan fange opp alle aspekter
- En tilnærming ovenfra og nedover
  - Global analyse med mulitgrafmodellen
  - Romlig modell for analyse av intressante områder
  - Detaljert studie av prosesser med dedikerte modeller
- Trenger ikke implementere komplette modeller for å studere systemet
- Hver modell har rom for forbedringer
- Presisjon kommer med en kostnad i form av kompleksitet
  - Grafmodell: Fysiske aspekter og prioriterings skjema
  - Romligmodell: Effektive og robuste 3D skjema for buffring
  - Avviksdeteksjon: Avanserte multivariabel analyse

Resultater

- Implementert multigrafmodell
  - Beskriver elementær funksjonalitet i flere typer infrastruktur
  - Implementert eksempel med strømforsyning, telekommunikasjon og gassrørledning
  - Simulering av feil i nettverkene og studie av feilpropagasjon
  - Kvantifisering av avhengighet mellom forskjellige infrastrukturer
- Teoretisk utredning av romlige modeller
  - Deteksjon av nærhet
  - Tid fra hendelse til feil
- Utforskning av angrepsvektorer i kontrollsystemer
  - Bruk av multivariabel analyse til å detektere/skjule kontrollangrep mot fysisk infrastruktur

Pågående arbeid

- Angrepsvektorer i SCDA/DCS
  - Modellering av kontroll systemer i
    - LNG anlegg
    - Strømgenerering
  - Utvikling av modeller basert kontrollteori
  - Anvendelse av multivariable statistiske metoder
- Visualisering av avhengigheter mellom kritiske infrastrukturer
  - Bruk av spillmotorer for visualisering
  - Detaljert modellering
  - Begrenset geografisk område

Videre arbeid

- Validering
  - Danne arenaer/fora for validering av modeller
  - Anonymisering av infrastruktur data
- Insentiver ovenfor infrastruktur eiere
  - Juridisk regulering av samarbeid og utveksling av data (nasjonalt og internasjonalt)
  - Kan infrastruktureiere oppnå økonomisk fortjeneste og forbedre sikkerheten ved å dele informasjon
- Forbedring av modellen(e)
  - Interaksjon
  - Visualisering
  - Ytelse