Risikostyring og digitalisering i transportsektoren

Sizarta Sarshar

Avd. Risiko, Sikkerhet og sikring

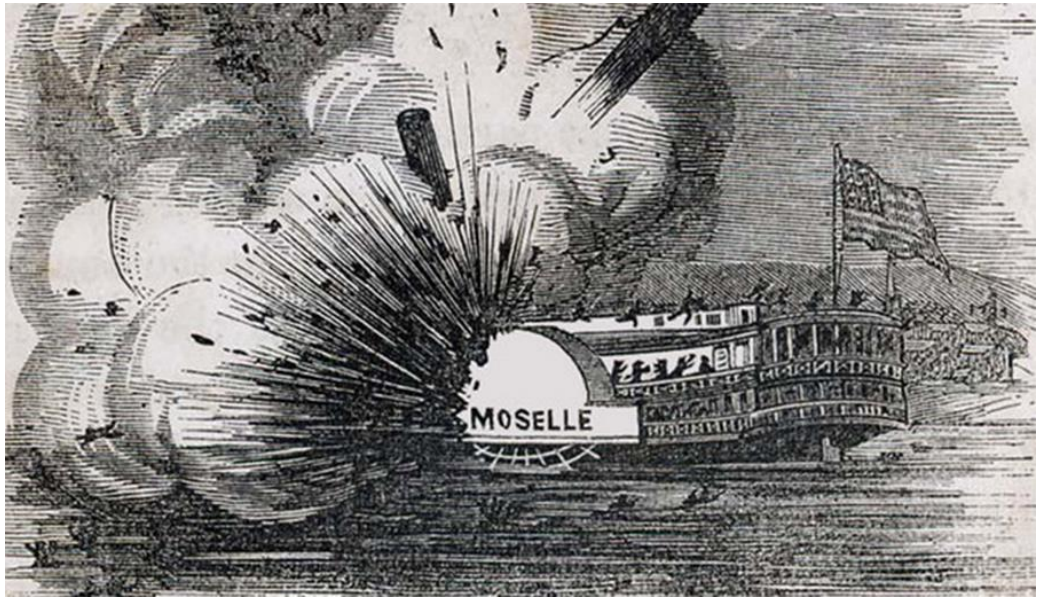
Sektor for Digitale Systemer

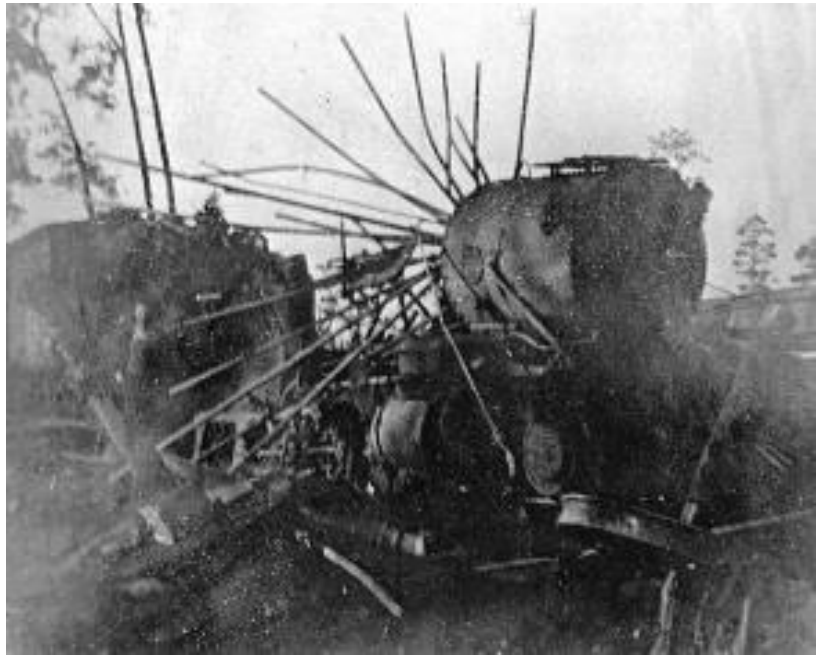
Institutt for energiteknikk

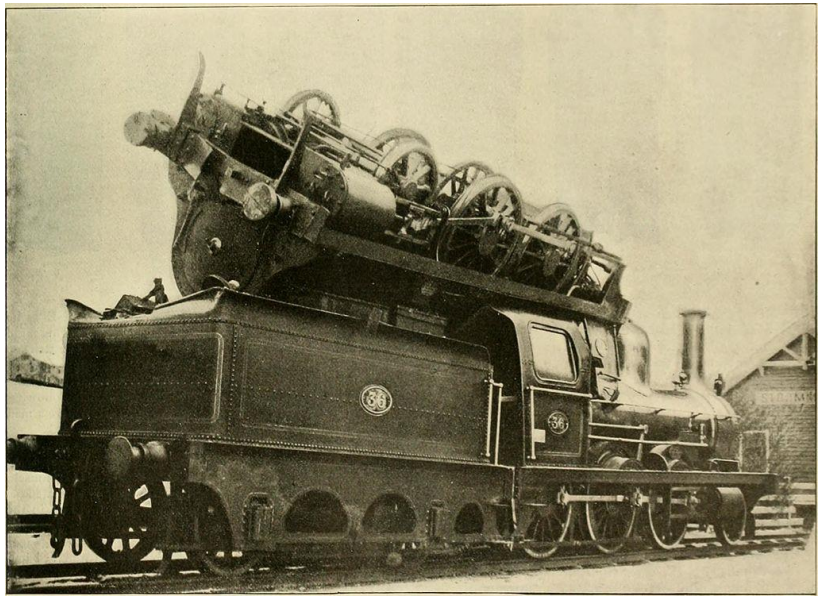
Temaer

- Rask utvikling og operasjonalisering av ny teknologi er alltid utfordrende
- Den pågående utviklingen av digitale løsninger medfører spesielle utfordringer
- Overser kravene som stilles til risikostyring viktige forhold?
- Hva kan vi gjøre for å møte disse utfordringene?

Et lite historisk tilbakeblikk







Hva var (er!) problemet?

- Undervurderer det faktum at nye teknologiske muligheter gir *nye måter å feile på*…
- Risikoargumenter blir lett oppfattet som «bakstreverske»
- Det tar tid før regelverk tar igjen utviklingen

- For en risikoanalytiker er det krevende både å henge med, og få nødvendig oppmerksomhet

Les: «High pressure steam engines and computer software», Nancy Leveson, 1992

Risikostyring og digitale systemer - Har vi egentlig noen utfordring her?

- Vi har jo flere tiårs erfaring med avanserte og digitale kritiske systemer!
  - Luftfart
  - Jernbane
  - Romfart
  - Prosessindustri
  - Kjernekraft

Har vi ikke allerede den kompetansen vi trenger for å håndtere risiko for digitale ITS-løsninger?

Intelligente transportsystemer innebærer…

- Betydelig digitalisering av kjøretøy og infrastruktur
- Nye tjenester for optimalisering av transport – Implementert på digitale plattformer
- Nye forretningsmodeller – Hvor digitale løsninger er selve ryggraden
- For at dette skal kunne realiseres må vi ha en sammenkobling av enheter, funksjoner og tjenester på et nivå av kompleksitet vi ikke har sett tidligere

Dette medfører betydelig risikoeksponering – For både mennesker, kritiske samfunnsfunksjoner og økonomiske interesser

Krav til kritiske digitale systemer vs utviklingen av ITS-løsninger

Typiske krav

- High cohesion – low coupling
- Begrenset funksjonalitet
- Verifiserbarhet
- Standardiserte utviklingsmiljøer
- Utviklingsprosesser med sterke krav til sporbarhet og etterprøvbarhet
- Bruk av velkjente løsninger
- mm.

Nye digitale systemer

- «Alt er koblet til alt»
- Systemene gjør mange forskjellige ting
- Skytjenester
- Systemer lærer selv og tilpasser seg
- Utviklingsprosessene er raske
- Nye teknologiske løsninger tas i bruk fortløpende
- mm.

Altså egenskaper man normalt *ikke* ønsker når kritiske systemer skal utvikles…

Noen spesifikke utfordringer

- Høy kompleksitet kan gjøre det *umulig* å verifisere at et system er sikkert nok
- Overgangen fra «kjekt å ha» til kritisk kan være glidende
  - GPS er OK som hjelpemiddel, men som basis for navigasjon av førerløse biler…?
- Kunstig intelligens gir mange muligheter, men det er svært utfordrende å dokumentere tilstrekkelig sikkerhet
- Må håndtere mange typer *dependability* samtidig:
  - Safety, reliability, security, mm.

Lov om utprøving av selvkjørende kjøretøy

Krav til safety

- Generelle og overordnede

Krav til håndtering av personopplysninger

- Eget kapittel, med 5 paragrafer

Det er altså langt mer spesifikke krav til håndtering av personopplysninger, enn til å forhindre at noen kan omkomme som følge av en programmeringsfeil…

Hva bør vi gjøre?

- Være bevisste på at nye teknologiske løsninger også medfører nye måter å feile på
  - Ekstremt viktig at vi har fokus på nye farer og uønskede hendelser tidlig nok!
  - Vår nåværende kunnskap og erfaring er *ikke* dekkende for de systemene som kommer

- Det må stilles krav til reell risikostyring helt fra start
  - Må kunne *dokumentere* akseptabel risiko før noe tas i bruk
  - Baseres på kjente prinsipper

- Systemene må designes og utvikles slik at de både er mulige å analysere, og slik at de er robuste – dvs. oppfører seg forutsigbart i tilfelle feil og uønskede hendelser
  - Standardisering, *på mange nivåer*

- Det må være fokus på helhetlig risikostyring – dvs. kontroll med så vel safety og reliability som security

Takk for oppmerksomheten

Sizarta Sarshar

sizarta.sarshar@ife.no