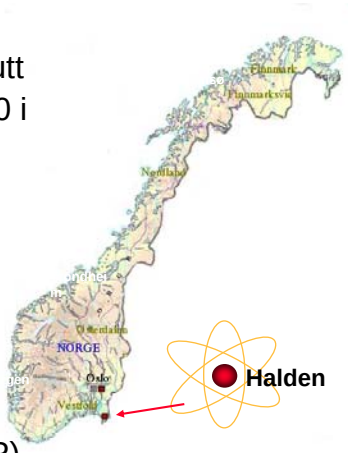
Vurdere sikkerhet ved hjelp av HAMBO simulatoren?

ICT Risk and Dependability (RID)
contact: Bjørn Axel Gran
bjorn.axel.gran@hrp.no

Institutt for energiteknikk

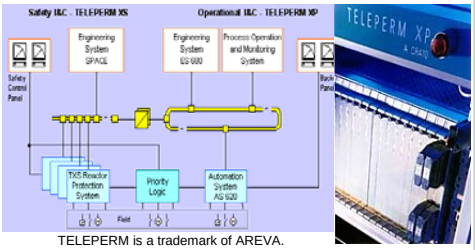
- Etablert 1948
- Norges nest største forskningsinstitutt
- Nærmere 600 ansatte, derav ca. 260 i Halden
- Omsetning ca. NOK 600 millioner
- 5 sektorer
  - Energi, Miljøteknologi og Fysikk
  - Nukleærteknologi
  - Petroleumsteknologi
  - Nukleær Sikkerhet og Pålitelighet
  - Sikkerhet MTO
- Vertskap for Halden Prosjektet (HRP)



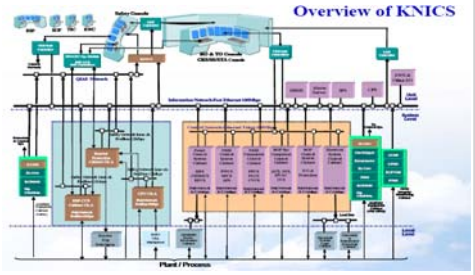
Status: Sikkerhet av Digitale Systemer

Trenden er:

- eksisterende, eldete analoge systemer erstattes med digitale instrumentering og kontroll systemer (I&C).
- design av fremtidige nukleære anlegg (generasjon III+ og IV) vil anvende digitale I&C systemer pga fordelene ovenfor eksisterende analoge systemer.
- fremskritt innen IKT blir brukt for å oppnå økt sikkerhet og bedre økonomi i planlegging, operasjon og vedlikehold.

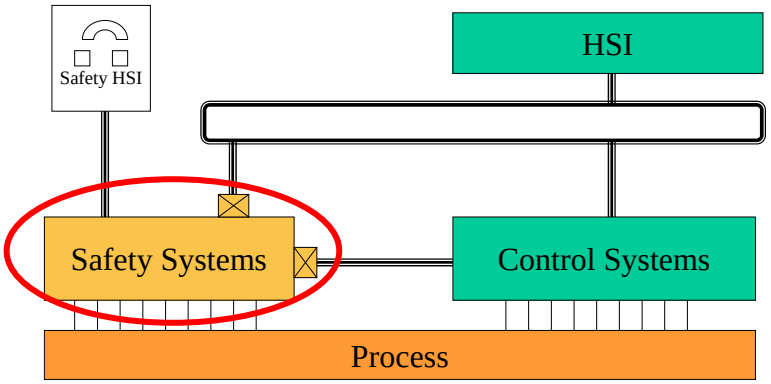


TELEPERM is a trademark of AREVA.



Mål og fokus

- Målet for forskningen på sikkerhet av programmerbare systemer er å bidra til suksessfull introduksjon av digitale I&C systemer. Fokus er på sikkerhetsrelevante systemer:



Oversikt

- Dette krever forskning relatert til områder som:
  - Integrasjon av systemutviklings- og risikoanalyse prosessene
  - Modernisering av I&C systemer
  - Analyse av avanserte I&C systemer
  - Analyse av feilpropagering og felles feil (CCF)
- Hovedspørsmålet er:
  - Hvordan argumentere at systemer er sikkert nok?

Eksempel: California 14. Sept. 2004

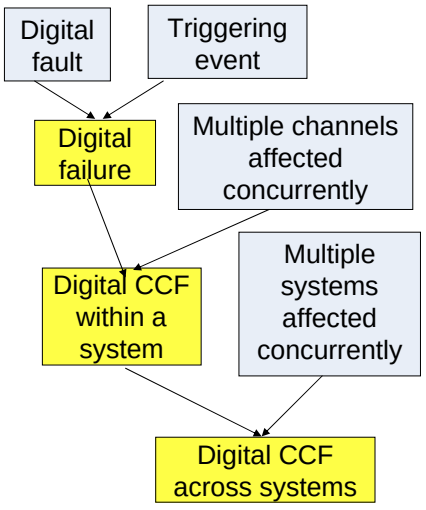
- Systemet Harris VCCS hadde vært i drift siden 90-tallet
- 14.april 2004 mistet ATC kontakten med 400 fly
- De kunne observere på radar at noen var på kollisjonskurs, men kunne ikke gjøre noe.
- Systemet krevde manuell resetting (sw watchdog) hver 30. dag
- Dette hadde ikke skjedd, og etter 50 dager kom en time-out i en ikke kritisk del,
- Som fikk hele systemet til å stenge ned.
- Og, reserve systemet feilet når det skulle brukes
- Redningen: TCAS (uavhengig system i flyene): hindret minst 4 kollisjoner

HRP 2009-11 Ch 10.3: Assessment of Error Propagation and Common Cause Factors

- Objectives:
  - ...
  - To evaluate approaches and applications of the HAMBO simulator for assessment of error propagation and common cause failures.
  - .....
- HAMBO
  - one out of 3 nuclear simulators in HAMMLAB
  - a full-scope simulator of the Swedish boiling water reactor Forsmark 3 plant.
  - a simulator with extended operational domain

Background

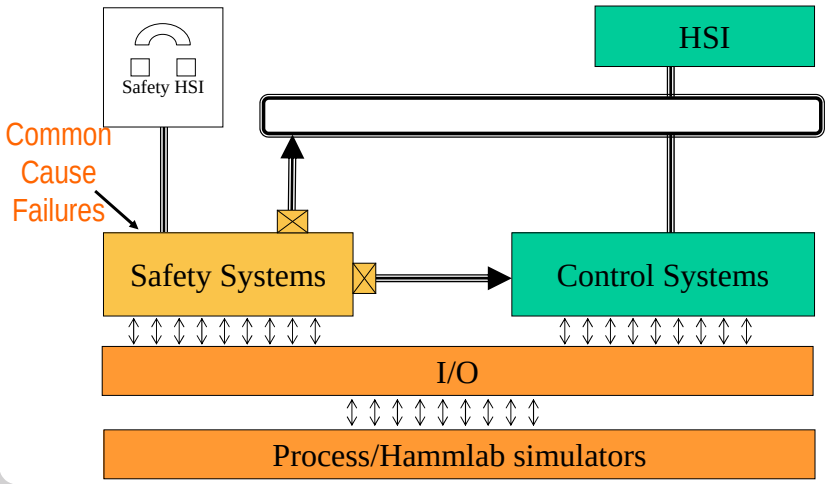
- Systems become more integrated
- The complexity of systems increases
- Thus, there is an increased need for methods that assess
  - that various applications are adequately isolated
  - that failures do not propagate between applications
  - applications for the potential existence of common cause failures and their effects



What?

- Scope:
  - to design CCF experiments using the HAMBO simulator
  - focus on the practical concerns and research needs as identified by the participants representing the HRP community.
- Focus:
  - Although related, “development for avoiding common cause factors” is not the primary focus
  - The focus is on how to assess systems and applications for the potential existence of common cause failures and their effects.

HAMBO simulator for new purposes: CCF assessment

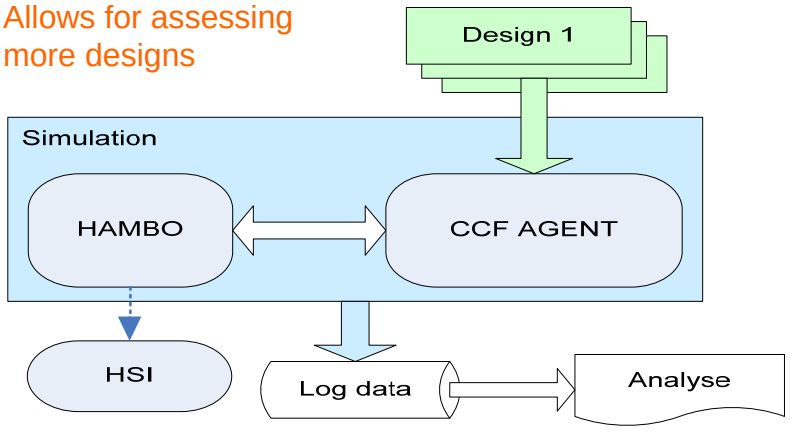


Experimental idea

- To simulate the functionality of the application to be assessed:
  1. Identify the system to be simulated
  2. Provide an description of the architecture
  3. Transform the architecture and apply as input to a CCF agent
  4. Modify HAMBO to provide the relevant signals
  5. Define the test conditions in the CCF agent
  6. Run the simulation: HAMBO and CCF agent
  7. Log data for further analysis

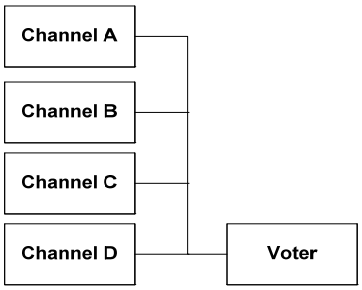
Experiment /framework

- Allows for assessing more designs

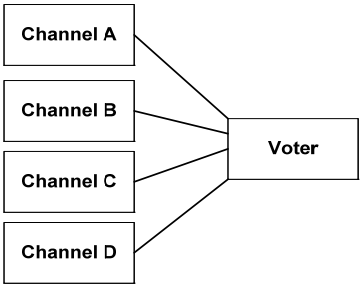


Example

- 2 designs: bus signalling and point-to-point signalling

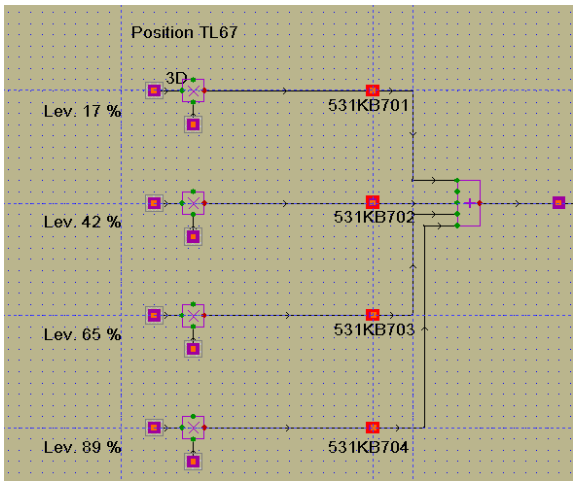


Bus signaling



Point-to-point signalling

1. Identify the system to be simulated



System: Adder

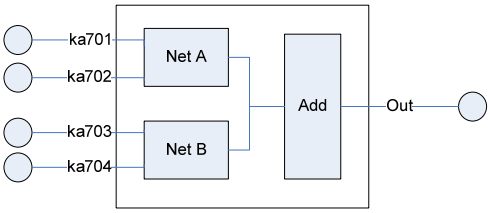
Screen-dump from Hambo

Input signal

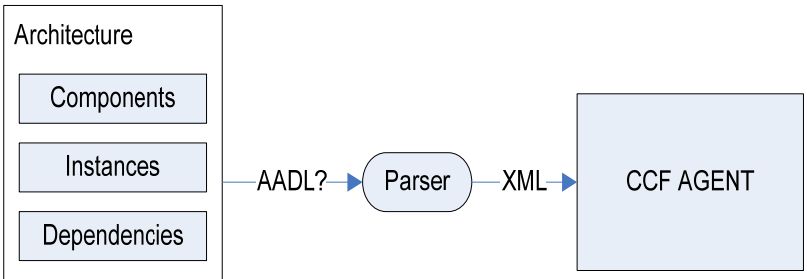
Output signal point

2. Provide an description of the architecture

- Devices
  - ka701: device sensor.flux;
  - ka702: device sensor.flux;
  - NetA: system function.network;
- Connections
  - DataConnection1: data port ka701.sensor_data -> NetA.sensor_data_1;
  - DataConnection2: data port ka702.sensor_data -> NetA.sensor_data_2;
- Dependencies
  - States: Error Free (EF), Undetected Corruption (UC), Failed (FA)
  - NetA.EF when NetA.EF and ((ka701.EF or ka702.EF) and not (ka701.UC or ka702.UC))
  - NetA.UC when NetA.UC or ka701.UC or ka702.UC
  - NetA.FA when NetA.FA or (ka701.FA and ka702.FA)



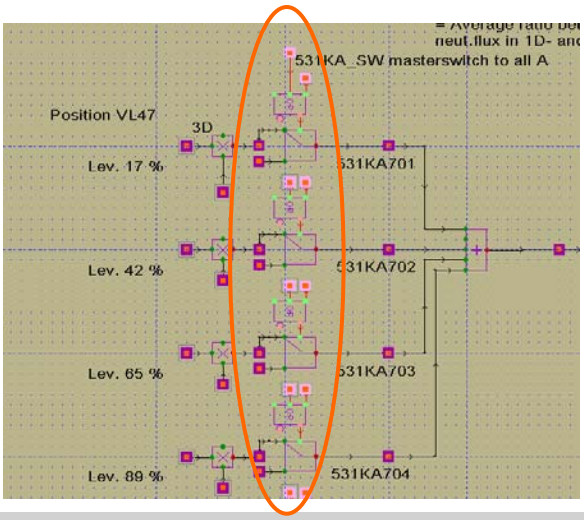
3. Transform the architecture and apply as input to the CCF agent



Transformation could be done by:

- AADL: Architecture Analysis & Design Language
- SDL: Specification and Description Language
- ...

4. Modify HAMBO to provide the relevant signals



System: Adder

Screen-dump from Hambo

Input signal

Output signal point

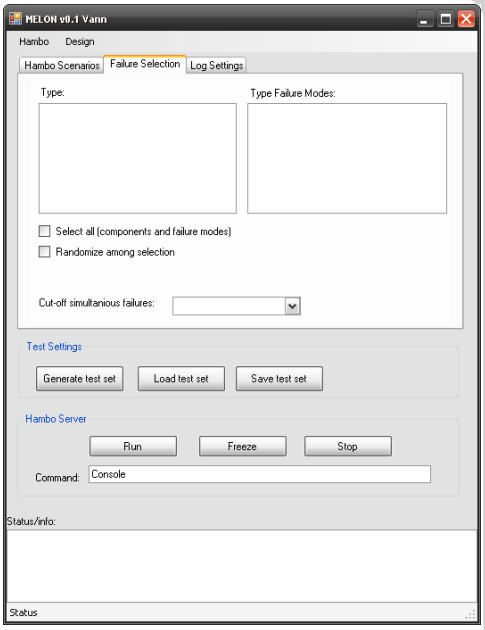
Modified input signal

5. Define the test conditions in the CCF Agent

- What to simulate:
  - Failure modes
  - Which scenarios
- Log
  - Effect (e.g. on presented data for operator) during the presence of failure modes
  - Alarms, mitigations etc.

6. Run the simulation

7. Log data



Halden Workshop Meeting

- **on "*Common cause failures –Research Needs*"**
  - *Date: 4th (9:00) – 5th (16:00) February, 2009*
  - *Place: hosted by ISTec, Garching, Germany*
  - Invitation posted at HPG and available under
    - **www.ife.no/events/commoncause/**
  - Deadline extended
- The group work and discussions are expected to provide answers to the following questions:
  - why is common cause failures a concern?
  - what are the main concerns in assessment of common cause failures?
  - how to use the HAMBO simulator for such assessments?

Konklusjon / Spørsmål

- Vi starter opp en ny eksperimentell fremgangsmåte for å vurdere sikkerhet.
- 2 åpne spørsmål:
  - er fremgangsmåten anvendbar?
  - gir den resultater som kan anvendes i sikkerhets analyser?
- Samme oppsett er også planlagt brukt for vurdering av "advanced control" (Ph.D. studie A. Hauge)
- Spørsmål?
  - avd. leder RID: Bjørn Axel Gran
  - CCF HAMBO prosjektleder: Sizarta Sarshar