ECE454/544: Fault-Tolerant Computing & Reliability Engineering

Lecture #14–

Dynamic Fault Trees

Instructor: Dr. Liudong Xing

Fall 2022

Administrative Issues

- Homework#6 assigned
  - Due by **Nov. 7, Monday**
- Project final report
  - Due by **Nov. 30, Wednesday**
  - Please check out the Report Guidelines for requirements

Review of Lecture #13

- Component sensitivity analysis measures the sensitivity of the system unreliability to the component failure parameters
  - Improvement Oriented: helps identify which components contribute most to the system reliability and thus they will be good candidates for efforts leading to improving system reliability, e.g.: Birnbaum’s measure, improvement potential
  - Maintenance Oriented: helps identify the component that has the largest probability of being the cause of system failure → set up a repairperson’s checklist, e.g.: criticality importance factor, diagnostic importance factor, Fussel-Vesley measure

Topics

- Dynamic fault trees

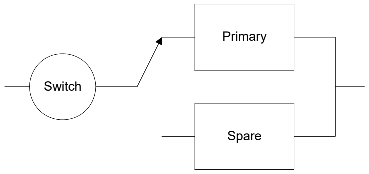
Reference:

J. B. Dugan and S. A. Doyle. “New Results in Fault-Tree Analysis” *Tutorial notes presented at Annual Reliability and Maintainability Symposium*, January 1997

J. B. Dugan, S. J. Bavuso, and M. A. Boyd, "Dynamic fault-tree models for fault-tolerant computer systems," IEEE Transactions on Reliability, vol.41, no.3, pp.363,377, Sep 1992

Dynamic Fault Trees

- Traditional (static) fault trees cannot model **sequence dependent** failures, in which the *order* that events occur is important.
- Sequence dependencies do exist in practical systems



  - Failure criteria depends on the *order* in which the failure occur.
- Special purpose gates were defined for modeling several kinds of dependencies (by Dugan et al.)

Dynamic Gates

- Functional dependency gate
- Cold spare gate
- Warm spare gate
- Hot spare gate
- Priority-AND gate

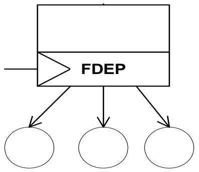
- Examples
  - Hypothetical Example Computer System (HECS)
  - Fault-Tolerant Parallel processor (FTPP)

Functional Dependence Gate

- **Functional dependency**: the occurrence of some event (trigger event) causes other dependent components to become inaccessible or unusable
- **FDEP gate**:
  - separate occurrence of any of dependent basic events has no effect on the trigger event!

The FDEP has no logical output. Thus it is connected to the fault tree with a dashed line.

Trigger event whose occurrence forces other events to occur

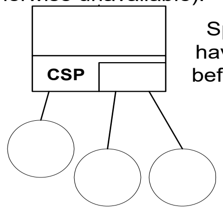


Dependent events that are forced to occur when the trigger event occurs.

Cold Spare Gate (CSP)

- **Cold spares**: spare components that are un-powered and thus do not fail before being used
- **CSP gate:**
  - One primary input and 1 or more alternate inputs
    - Every input is a basic event
    - The primary input is initially powered on
    - The alternate inputs specify components used as cold spares
  - One output becoming true after all input events occur

Output of gate occurs when the primary and all spares have failed (or are otherwise unavailable).



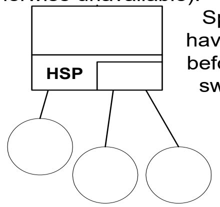
Spare components have *zero* failure rate before being switched into active use.

Primary component

Spare components. Spares are used in defined order.

Hot Spare Gate (HSP)

Output of gate occurs when the primary and all spares have failed (or are otherwise unavailable).



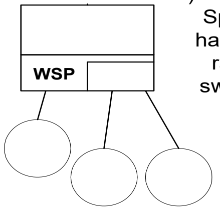
Spare components have *same* failure rate before and after being switched into active use.

Primary component

Spare components. Spares are used in defined order.

Warm Spare Gate (WSP)

Output of gate occurs when the primary and all spares have failed (or are otherwise unavailable).

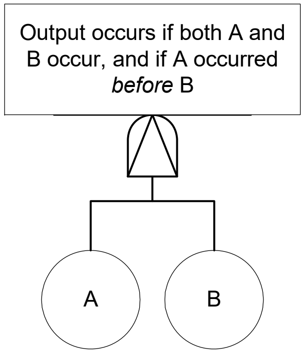


Spare components have *reduced* failure rate before being switched into active use.

Primary component

Spare components. Spares are used in defined order.

Priority-AND Gate (PAND)



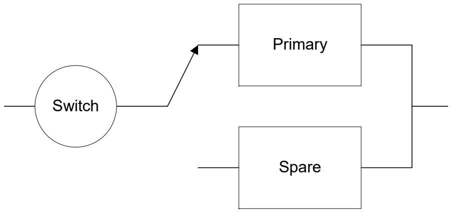
Output occurs if both A and B occur, and if A occurred *before* B

- Logically equivalent to an AND gate, with an added condition that events must occur in a specific order

- To represent more than two events that must occur in a specific order to activate the output, the PAND gate can be cascaded.

Hands-On Problem

- Find the DFT model for the two-component standby sparing system. Assume the **cold sparing method** is used.

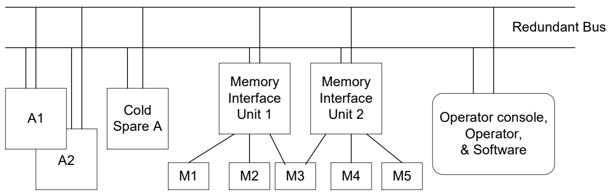


Dynamic Gates

✓ Functional dependency gate
✓ Cold spare gate
✓ Warm spare gate
✓ Hot spare gate
✓ Priority-AND gate

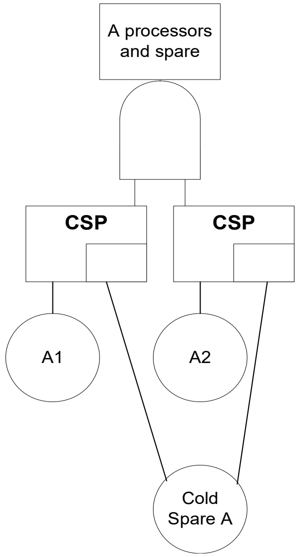
- Examples
  - **Hypothetical Example Computer System (HECS)**
  - Fault-Tolerant Parallel Processor (FTPP)

HECS: Hypothetical Example Computer System



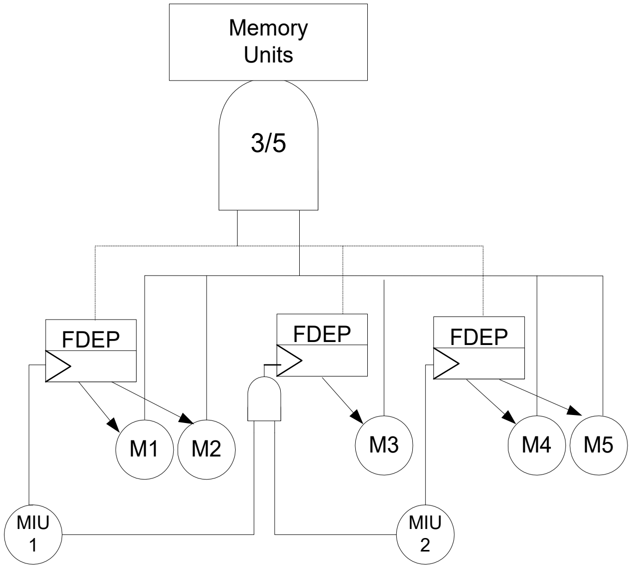
- Processors A1 and A2 share the cold spare A
- 3 out of the 5 memory units are needed; if MIU fails, memory is not accessible
- At least one bus is required
- HECS requires at least 1 of the three processors, at least 3 of the memory units, at least one of the redundant buses, and the operator, console and software to be operating correctly

Modeling the Processor Subsystem

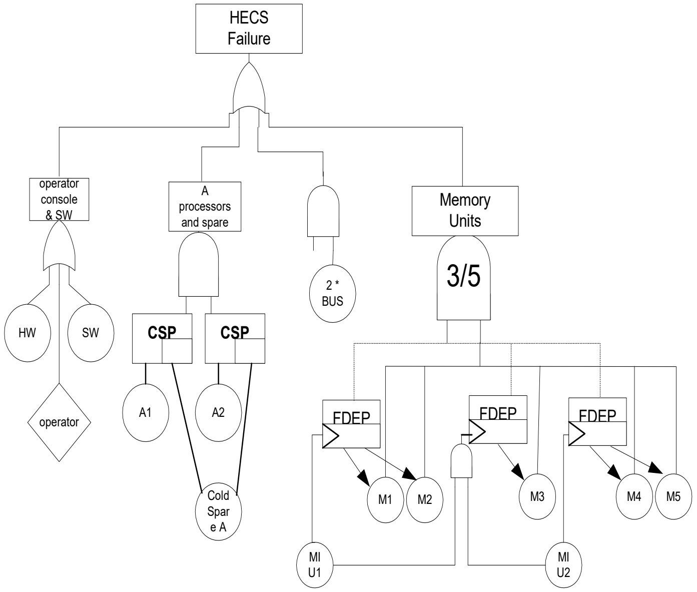


Note: the cold spare is shared between the two processors. First processor to fail is replaced with the spare; the spare is then unavailable if the other fails

Modeling the Memory Subsystem



Dynamic Fault Tree Model for HECS

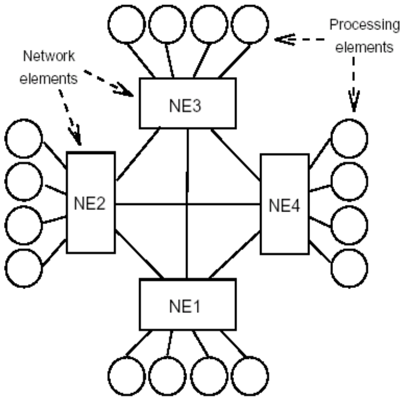


Dynamic Gates

✓ Functional dependency gate
✓ Cold spare gate
✓ Warm spare gate
✓ Hot spare gate
✓ Priority-AND gate

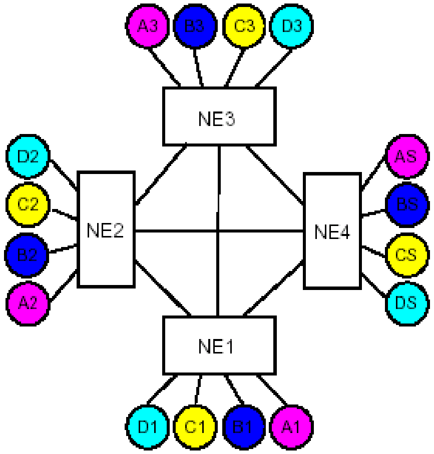
- Examples
  - √ Hypothetical Example Computer System (HECS)
  - **Fault-Tolerant Parallel Processor (FTPP)**

Fault Tolerant Parallel Processor (FTPP, Lecture #1 Revisit)



- 16 processing elements (PE), with 4 connected to each of 4 network elements (NE)
- 16 PE form 4 triads, each with a spare
- NEs are fully connected
- Consider three configurations of the FTTP

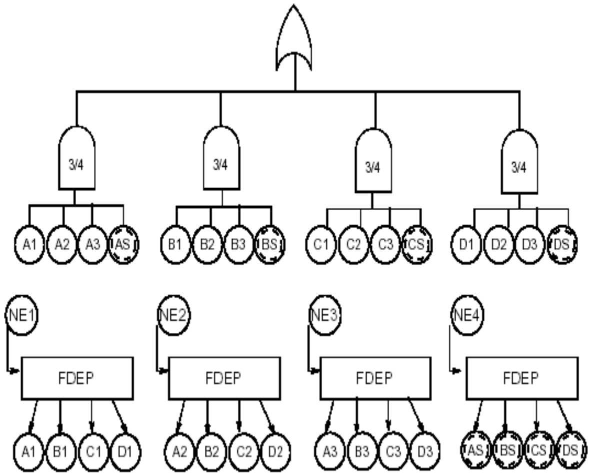
FTPP Configuration #1—
1 Spare per Triad



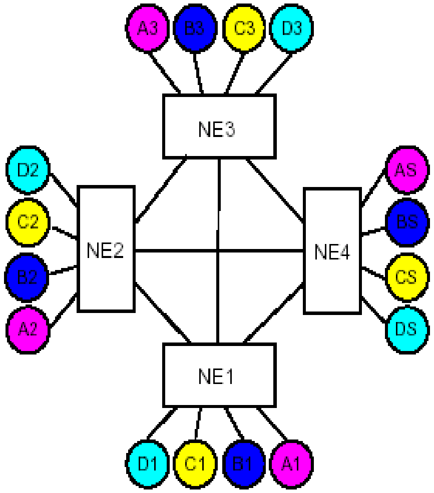
- Divides active elements of a triad among NE1, NE2, NE3; PEs in the same relative position on the first three NEs form a triad
- The PE in the same relative position on NE4 serves as a **hot spare** for the triad
  - One spare for each triad
  - All spares attached to the same network element NE4

DFT for FTPP Configuration #1

- All 4 triads must be operational to make the system operational
- And a triad fails when only one PE remains

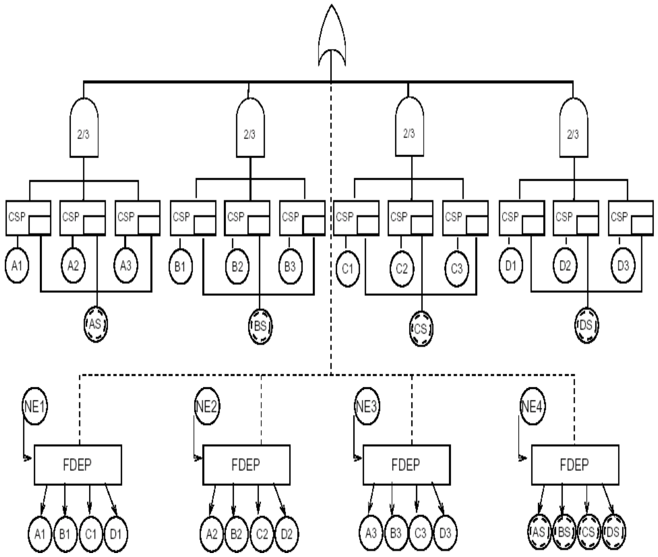


FTPP Configuration #2—
#1 but Cold Spares



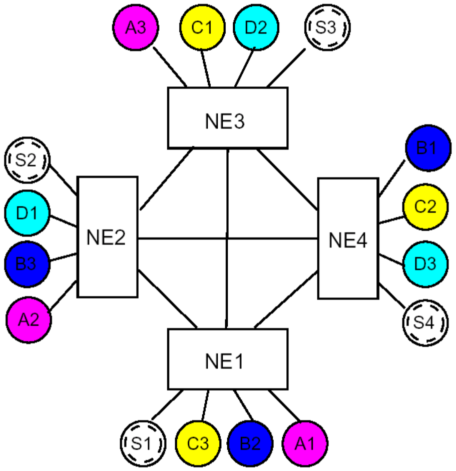
- One **COLD spare** for each triad
- All spares attached to the same network element NE4
- Used to investigate the effect on reliability of keeping spares unpowered until needed

DFT for Configuration #2



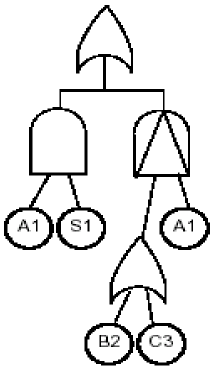
- The cold spare for each triad is connected to all three cold spare gates since it can substitute any of the elements

FTPP Configuration #3 – One Spare Per NE



- **Hot spares** distributed across the NEs
- The spare element on each NE can substitute for any failed PE connected to the same NE

Failure Conditions for FTPP #3



- The **first member of the A triad (A1) fails** if
  - both A1 and its spare (S1) fail
  - OR if either of the other processors on the same NE fail before A1 does, thus using the spare first. In this case there will be no spare available when A1 fails.
- Failure/success criteria of FTPP #3
  - All 4 triads must be operational to make the system operational
  - And a triad fails when only one PE remains

DFT for FTPP Configuration #3

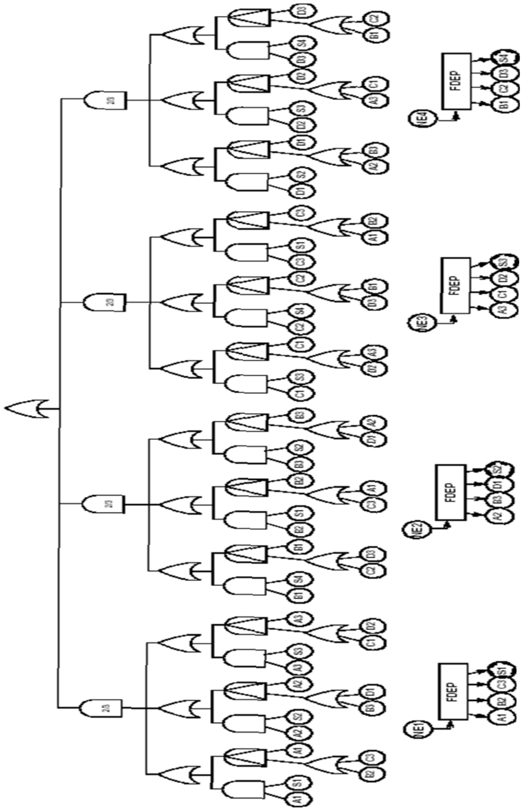
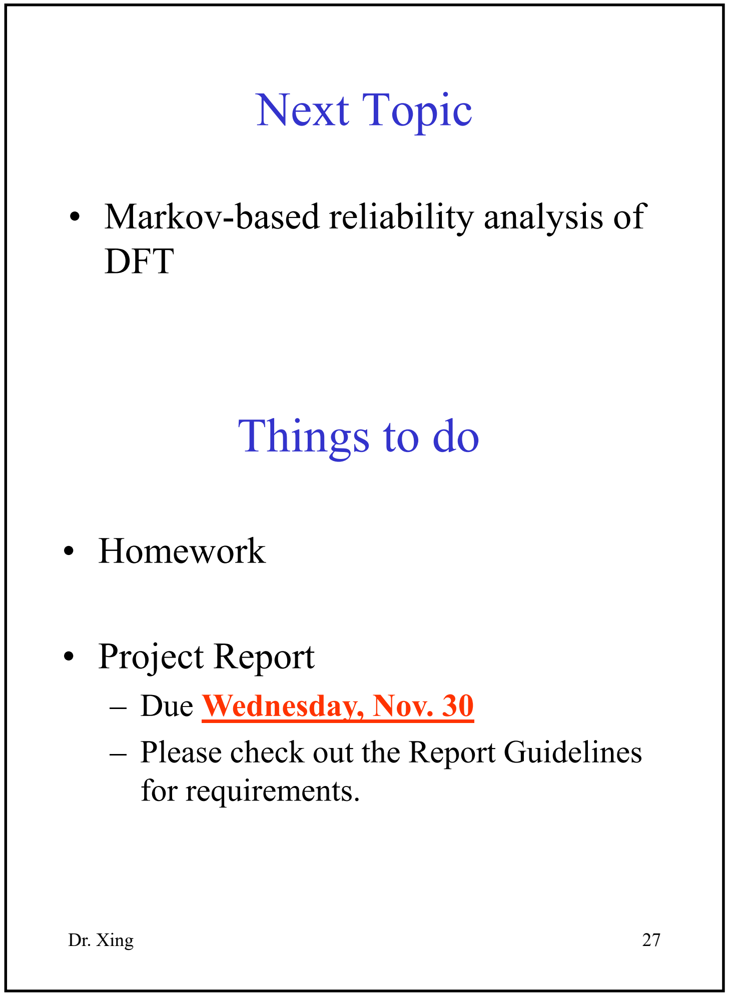


Figure 30 (Dugan97)

Summary of Lecture #14

- Special dynamic gates capture sequential dependencies arising in modeling fault tolerant systems
  - FDEP for modeling situations where one component’s correct operation is dependent upon the correct operation of some other component
  - CSP for modeling cold spares which are unpowered before being used
  - WSP for modeling warm spares which fail at a reduced rate before being used
  - HSP for modeling hot spares which fail at active failure rate before being switched into active use
  - PAND for modeling ordered ANDing events
  - Two examples: HECS and FTPP
  - **Quantitative analysis of dynamic fault trees using Markov models will be the next topic!**



Next Topic

- Markov-based reliability analysis of DFT

Things to do

- Homework
- Project Report
  - Due **Wednesday, Nov. 30**
  - Please check out the Report Guidelines for requirements.