

© Gert Jervan, TTÜ/ATI

1918 TALLINNA TEHNIKAÜLIKOOL
TALLINN UNIVERSITY OF TECHNOLOGY

Department of computer Engineering
ati.ttu.ee

IAF0030

Arvutitehnika erikursus I

Süsteemide usaldusväärsus ja veakindlus
Dependability and fault tolerance

Loeng 5
Liiasus (Riistvara ja tarkvara)

gert.jervan@pld.ttu.ee

Tallinn University of Technology
Department of Computer Engineering
Estonia


© Gert Jervan, TTÜ/ATI

IAF0030 - Arvutitehnika erikursus I

Lecture Outline

- ✓ Introduction
- ✓ Hardware Redundancy
- ✓ Software Redundancy
- ✓ Information Redundancy
- ✓ Time Redundancy

Some materials from:
Kewal Saluja
Hongyu Sun
Zaipeng Xie
Meng-Lai Yin
Rajesh Gupta
Elena Dubrova



1918 TALLINNA TEHNIKAÜLIKOOL
TALLINN UNIVERSITY OF TECHNOLOGY

2

© Gert Jervan, TTÜ/ATI

IAF0030 - Arvutitehnika erikursus I

Fault Tolerance

- ✓ A **fault-tolerant system** is one that can **continue** to correctly perform its specified tasks in the presence of hardware failures and/or software errors.
- ✓ Fault tolerance is the attribute that enables a system to achieve fault-tolerant operation.
- ✓ Fault tolerance is not a new field:
 - 1949, the EDVAC computer duplicated the ALU and compare the results
 - 1955, the UNIVAC computer incorporated parity check for data transfers
 - 1952, John von Neumann, lectures on the use of replicated logic modules to improve system reliability,
 - etc.

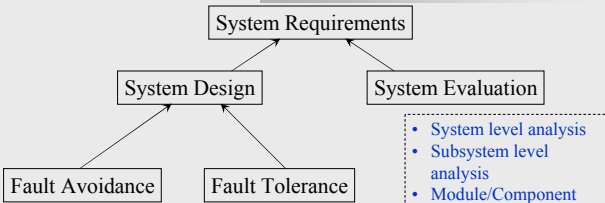
1918 TALLINNA TEHNIKAÜLIKOOL
TALLINN UNIVERSITY OF TECHNOLOGY

3

© Gert Jervan, TTÜ/ATI

IAF0030 - Arvutitehnika erikursus I

System Design & Evaluation Top-Level View



```

    graph TD
      SR[System Requirements] --> SD[System Design]
      SR --> SE[System Evaluation]
      SD --> FA[Fault Avoidance]
      SD --> FT[Fault Tolerance]
      SE --> SLA[System level analysis]
      SE --> SSubLA[Subsystem level analysis]
      SE --> MCLLA[Module/Component level analysis]
    
```

Possible techniques

- Parts selection
- Design reviews
- Quality control
- Design Methodology
- Documentation

Possible techniques

- Redundancy (Hardware, Software, Information, Time)
- Fault detection
- Fault masking
- Fault containment
- Reconfiguration

Possible Techniques

- FMEA
- FTA
- RBD
- Markov
- Petri net

1918 TALLINNA TEHNIKAÜLIKOOL
TALLINN UNIVERSITY OF TECHNOLOGY

4

© Gert Jervan, TTÜ/ATI

1918 TALLINNA TEHNIKAÜLIKOOL
TALLINN UNIVERSITY OF TECHNOLOGY

Department of computer Engineering
ati.ttu.ee

Hardware Redundancy

© Gert Jervan, TTÜ/ATI

IAF0030 - Arvutitehnika erikursus I

Hardware Redundancy

- ✓ 3 basic forms: passive, active, and hybrid
 - Passive: Mask faults rather than detect faults without requiring any system or operator action
 - Active: Fault has to be detected before it can be tolerated. Actions: location, containment, recovery (for component removal)

1918 TALLINNA TEHNIKAÜLIKOOL
TALLINN UNIVERSITY OF TECHNOLOGY

6

© Gert Jervan, TTÜ/ATI IAF0030 - Arvutitehnika erikursus I

Passive Hardware Redundancy

- ✓ Use fault masking to hide the occurrence of faults and prevent the faults from resulting in errors
- ✓ Mask faults rather than detect faults
- ✓ Achieve fault tolerance without requiring any system or operator action
- ✓ Voting mechanisms, majority voting
- ✓ Do not need fault detection or reconfiguration
- ✓ Many drawbacks

TALLINNA TEHNIKAÜLIKOOL
TALLINN UNIVERSITY OF TECHNOLOGY

© Gert Jervan, TTÜ/ATI IAF0030 - Arvutitehnika erikursus I

Passive Hardware Redundancy

- ✓ N-Modular Redundancy (generalization of TMR or Triple Modular Redundancy)
- ✓ TMR: Triplicate the hardware and perform a majority vote to determine the output of the system
 - If one of the modules becomes faulty, the 2 remaining fault-free modules mask the results of the faulty module when the majority vote is performed

TALLINNA TEHNIKAÜLIKOOL
TALLINN UNIVERSITY OF TECHNOLOGY

© Gert Jervan, TTÜ/ATI IAF0030 - Arvutitehnika erikursus I

TMR Technique

Tolerates N/2 faults

TALLINNA TEHNIKAÜLIKOOL
TALLINN UNIVERSITY OF TECHNOLOGY

© Gert Jervan, TTÜ/ATI IAF0030 - Arvutitehnika erikursus I

TMR/Voter Structures

TALLINNA TEHNIKAÜLIKOOL
TALLINN UNIVERSITY OF TECHNOLOGY

© Gert Jervan, TTÜ/ATI IAF0030 - Arvutitehnika erikursus I

Fault-Tolerance Capability

- Assuming perfect voter, how many module faults can the TMR technique tolerate?
- What if 2 modules fail the same way?
- Does TMR technique provide fault detection capability?
- How about imperfect voter?
- Performance impacts from the voter in the TMR technique

TALLINNA TEHNIKAÜLIKOOL
TALLINN UNIVERSITY OF TECHNOLOGY

© Gert Jervan, TTÜ/ATI IAF0030 - Arvutitehnika erikursus I

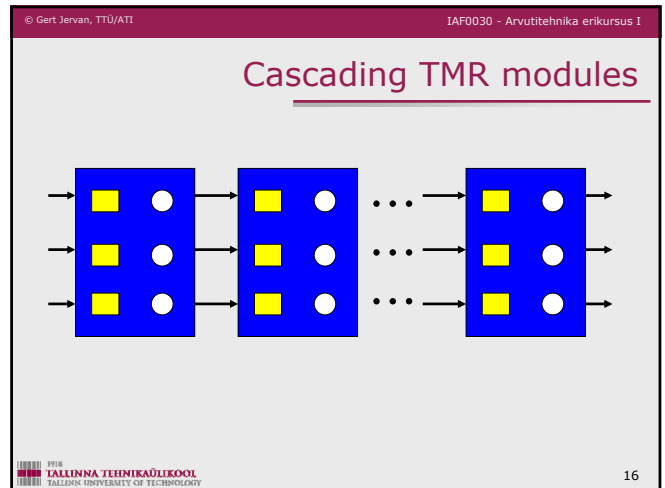
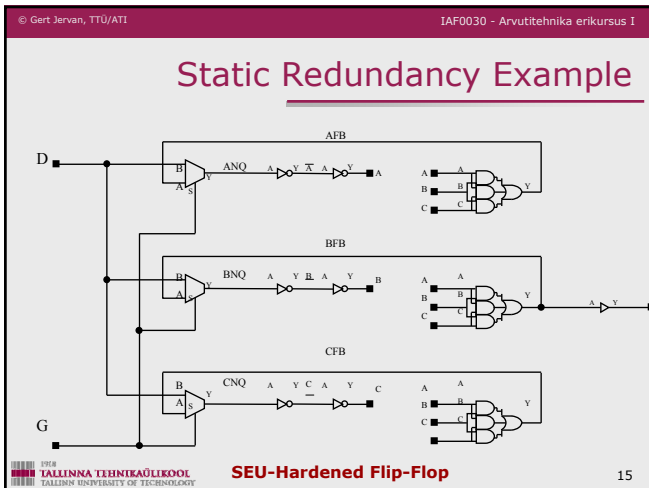
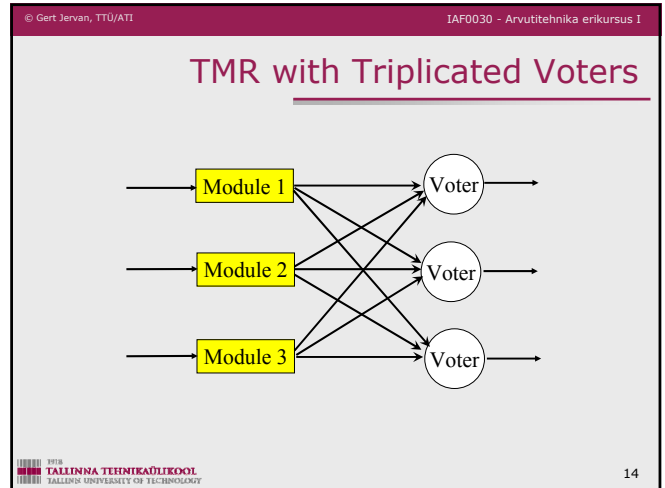
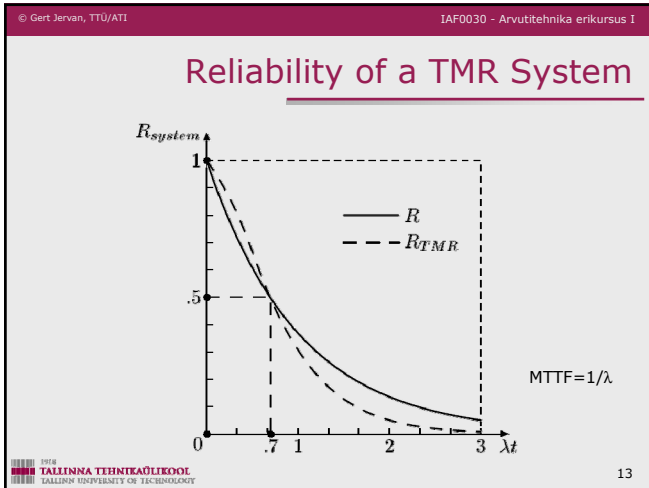
Reliability of a TMR System

$$R_{TMR} = R_1R_2R_3 + (1 - R_1)R_2R_3 + R_1(1 - R_2)R_3 + R_1R_2(1 - R_3)$$

$$R_1 = R_2 = R_3 = R$$

$$R_{TMR} = 3R^2 - 2R^3$$

TALLINNA TEHNIKAÜLIKOOL
TALLINN UNIVERSITY OF TECHNOLOGY



- © Gert Jervan, TTÜ/ATI IAF0030 - Arvutitehnika erikursus I
- ### Passive hardware redundancy
- ✓ Types of voting
 - Majority
 - in many practical situations it is meaningless
 - Average
 - can have poor performance if a sensor always provide very low value
 - Mid value
 - a good choice - can be very costly to implement in HW
- 17

© Gert Jervan, TTÜ/ATI IAF0030 - Arvutitehnika erikursus I

Passive Hardware Redundancy

- ✓ Comparison between hw and sw voter schemes

	HW	SW
cost	high	low
flexibility	inflex	flex
synch.	tightly	loosely
perform.	high (fast)	low (slow)
types of voting	majority (others costly)	diff (no extra cost)

18

© Gert Jervan, TTÜ/ATI IAF0030 - Arvutitehnika erikursus I

Example Systems Using TMR Technique

- ✓ JPL STAR (Self-Testing And Repairing computer)

The diagram illustrates the JPL STAR computer architecture. At the center is a 'test and repair processor'. Surrounding it are several functional blocks: 'PROCESSORS' (Control, Logic, Memory programs), 'MEMORIES' (Read-only, Read-write, Memory out to I/O, Memory out to I/O), 'Input/output', 'Interrupt', 'Status and switch lines', 'Power source', 'Control bus', and 'Power bus'. There are also connections to 'spacecraft subsystems'.

TALLINNA TEHNIKAÜLIKOOL
TALLINN UNIVERSITY OF TECHNOLOGY

19

© Gert Jervan, TTÜ/ATI IAF0030 - Arvutitehnika erikursus I

Example Systems Using TMR Technique

- ✓ FAA WAAS (Wide Area Augmentation System)

The diagram shows the FAA WAAS system. It features several 'WAAS Satellites' in orbit and 'WAAS Reference Stations' on the ground. The ground stations are connected to the satellites, which then broadcast 'Correction Messages' to aircraft. The system is shown over a map of North America.

TALLINNA TEHNIKAÜLIKOOL
TALLINN UNIVERSITY OF TECHNOLOGY

20

© Gert Jervan, TTÜ/ATI IAF0030 - Arvutitehnika erikursus I

WAAS Block Diagram

The block diagram shows the WAAS system architecture. On the left, 'Wide-area Reference Station (WRS), 1 of 25' contains three 'WRE' blocks. These are connected via a 'WAN' to a 'Wide-area Master Station (WMS), 1 of 2'. The WMS contains 'Corr-1', 'Corr-2', 'Safety Monitor', 'C o m p', and 'O & M' blocks. The WMS is connected via another 'WAN' to 'Ground Earth Station (GES)'. The GES consists of 'GUS' blocks and 'Separate GES' blocks.

TALLINNA TEHNIKAÜLIKOOL
TALLINN UNIVERSITY OF TECHNOLOGY

21

© Gert Jervan, TTÜ/ATI IAF0030 - Arvutitehnika erikursus I

Active Hardware Redundancy

- ✓ Achieve fault tolerance by **detecting** the existence of faults and performing some action to **remove** the faulty parts
- ✓ Require the system be **reconfigured** to tolerate faults
- ✓ 3 steps: fault detection, fault location, and fault recovery

TALLINNA TEHNIKAÜLIKOOL
TALLINN UNIVERSITY OF TECHNOLOGY

22

© Gert Jervan, TTÜ/ATI IAF0030 - Arvutitehnika erikursus I

Active Hardware Redundancy

The flowchart illustrates the Active Hardware Redundancy process. It starts with 'Normal Operation' (green box). A 'Fault occurs' (yellow box) leads to 'Error occurs' (orange box), which then leads to 'System failure' (red box). From 'System failure', the process goes to 'Fault detection and location', then 'Reconfiguration and recovery', and finally back to 'Normal Operation'. There is also a path from 'Fault occurs' to 'Degraded Operation' (grey box), which then leads to 'Fault detection and location'.

TALLINNA TEHNIKAÜLIKOOL
TALLINN UNIVERSITY OF TECHNOLOGY

23

© Gert Jervan, TTÜ/ATI IAF0030 - Arvutitehnika erikursus I

Dynamic Redundancy

- ✓ Uses Extra Components
- ✓ Only 1 Copy Operates At A Times
 - Fault Detection
 - Fault Recovery
- ✓ Spares Are On "Standby"
 - Hot Spares
 - Cold Spares

TALLINNA TEHNIKAÜLIKOOL
TALLINN UNIVERSITY OF TECHNOLOGY

24

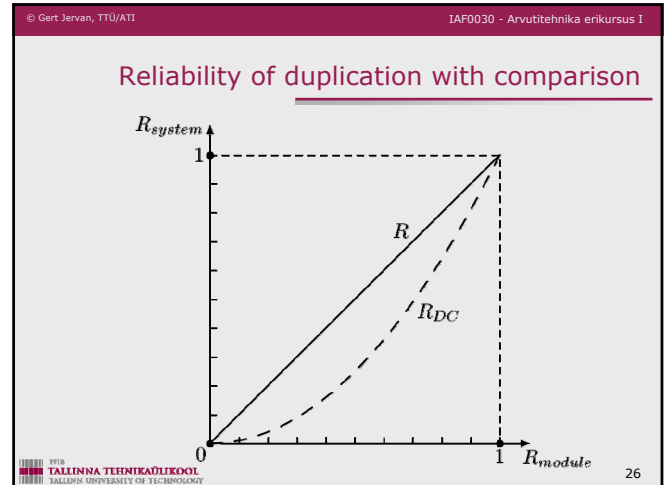
© Gert Jervan, TTÜ/ATI IAF0030 - Arvutitehnika erikursus I

Duplication with Comparison

- ✓ Both modules perform the same computations in parallel and compare the results
- ✓ An error message is generated if the two results disagree
- ✓ Only fault detection, no fault tolerance
- ✓ Can be used as a fundamental fault detection technique in active redundancy approach, for example, the pair-and-a-spare technique

TALLINNA TEHNIEKÜLIKOOLOO
TALLINN UNIVERSITY OF TECHNOLOGY

25



© Gert Jervan, TTÜ/ATI IAF0030 - Arvutitehnika erikursus I

Duplication with Comparison

- ✓ Problems:
 - if there is a fault on input line, both modules will receive the same erroneous signal and produce the erroneous result
 - comparator may not be able to perform an exact comparison
 - synchronisation
 - no exact matching
 - - comparator is a single point of failure

TALLINNA TEHNIEKÜLIKOOLOO
TALLINN UNIVERSITY OF TECHNOLOGY

27

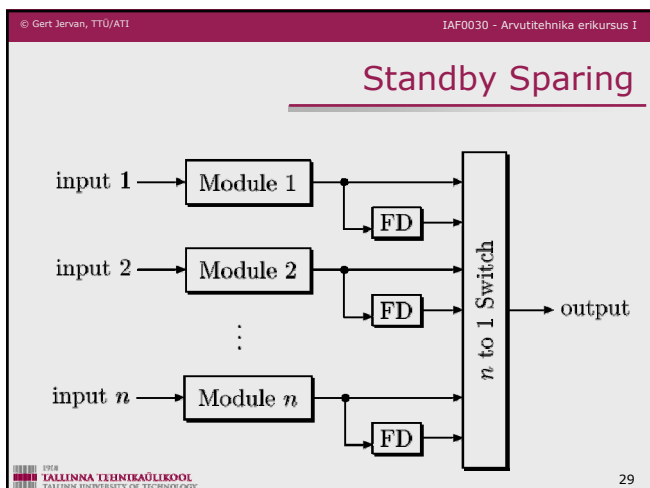
© Gert Jervan, TTÜ/ATI IAF0030 - Arvutitehnika erikursus I

Implementation of comparator

- ✓ In hardware, a bit-by-bit comparison can be done using two-input exclusive-or gates
- ✓ In software, a comparison can be implemented with a COMPARE instruction
 - commonly found in instruction sets of almost all microprocessors

TALLINNA TEHNIEKÜLIKOOLOO
TALLINN UNIVERSITY OF TECHNOLOGY

28



© Gert Jervan, TTÜ/ATI IAF0030 - Arvutitehnika erikursus I

Spares

- ✓ Hot spares
 - all modules are powered up
 - spares can be switched into use immediately after the primary module becomes failed
- ✓ Cold spares
 - the primary modules are powered up
 - the spares are powered down, which are powered up and switched into use when the primary modules fail
- ✓ Warm spares

TALLINNA TEHNIEKÜLIKOOLOO
TALLINN UNIVERSITY OF TECHNOLOGY

30

Standby Sparing (standby replacement)

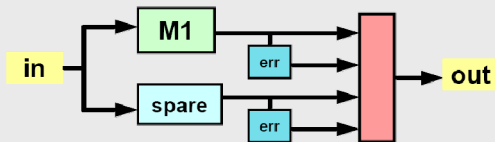
- ✓ Active hardware redundancy
- ✓ One module is operational and one or more modules serve as standbys (or spares)
- ✓ Various fault detection or error detection schemes are used to determine whether a module has become faulty
- ✓ Fault location is used to determine exactly which module, if any, is faulty.

Standby Sparing (standby replacement)

- ✓ If a fault is detected and located, then the faulty module is removed from operation and replaced with a spare
- ✓ The reconfiguration can be viewed as a switch.
- ✓ Can bring a system back to full operation after the occurrence of a fault.
- ✓ Require momentary disruption in performance when reconfiguration is performed.

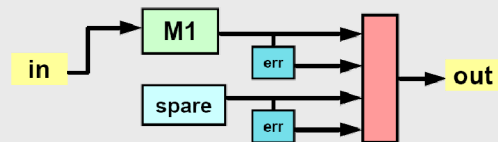
Hot Standby Sparing

- ✓ In hot standby sparing spares operate in synchrony with on-line module and are prepared to take over any time



Cold Standby Sparing

- ✓ In cold standby sparing spares are unpowered until needed to replace a faulty module



Hot & Cold Standby Sparing

- ✓ Hot standby sparing can minimize the performance disruption. The spares operate in synchrony with the on line modules and are prepared to take over at any time.
- ✓ In cold standby sparing, the spares are unpowered until needed to replace a faulty module. Hence extra time is required to bring the module back to operation. The advantage is that spares do not consume power until needed. Satellite application is a good example for cold standby sparing.

Pair-and-a-spare Technique

- ✓ Combine the features in standby sparing and duplication with comparison
- ✓ 2 modules are operated in parallel at all times and their results are compared to provide the error protection capability
- ✓ The error signal from the comparison is used to initiate the reconfiguration process (switch) that removes faulty modules and replaces them with spares

© Gert Jervan, TTÜ/ATI IAF0030 - Arvutitehnika erikursus I

Pair-and-a-spare scheme

<http://www.stratus.com/>

37

© Gert Jervan, TTÜ/ATI IAF0030 - Arvutitehnika erikursus I

Example Systems

- ✓ Apollo telescope mount pointing computer
- ✓ Saturn 5 LVDC memory section
- ✓ Compaq Himalaya architecture

38

© Gert Jervan, TTÜ/ATI IAF0030 - Arvutitehnika erikursus I

Types of Redundancy

NASA Office of Logic Design - klabs.org

- ✓ Classified on how the redundant elements are introduced into the circuit
- ✓ Choice of redundancy type is application specific
- ✓ Active or Static Redundancy
 - External components are not required to perform the function of detection, decision and switching when an element or path in the structure fails.
- ✓ Standby or Dynamic Redundancy
 - External elements are required to detect, make a decision and switch to another element or path as a replacement for a failed element or path.

39

© Gert Jervan, TTÜ/ATI IAF0030 - Arvutitehnika erikursus I

Redundancy Techniques

40

© Gert Jervan, TTÜ/ATI IAF0030 - Arvutitehnika erikursus I

Simple Parallel Redundancy

Active - Type 1

In its simplest form, redundancy consists of a simple parallel combination of elements. If any element fails open, identical paths exist through parallel redundant elements.

41

© Gert Jervan, TTÜ/ATI IAF0030 - Arvutitehnika erikursus I

Duplex Parallel Redundancy

Active - Type 2

This technique is applied to redundant logic sections, such as A1 and A2 operating in parallel. It is primarily used in computer applications where A1 and A2 can be used in duplex or active redundant modes or as a separate element. An error detector at the output of each logic section detects noncoincident outputs and starts a diagnostic routine to determine and disable the faulty element.

42

© Gert Jervan, TTÜ/ATI IAF0030 - Arvutitehnika erikursus I

Bimodal Parallel Redundancy

(a) Bimodal Parallel/
Series Redundancy

(b) Bimodal Series/
Parallel Redundancy

Active - Type 3

A series connection of parallel redundant elements provides protection against shorts and opens. Direct short across the network due to a single element shorting is prevented by a redundant element in series. An open across the network is prevented by the parallel element. Network (a) is useful when the primary element failure mode is open. Network (b) is useful when the primary element failure mode is short.

43

© Gert Jervan, TTÜ/ATI IAF0030 - Arvutitehnika erikursus I

Simple Majority Voting

Active - Type 4

Decision can be built into the basic parallel redundant model by inputting signals from parallel elements into a voter to compare each signal with remaining signals. Valid decisions are made only if the number of useful elements exceeds the failed elements.

44

© Gert Jervan, TTÜ/ATI IAF0030 - Arvutitehnika erikursus I

Adaptive Majority Voting

Active - Type 5

This technique exemplifies the majority logic configuration discussed previously with a comparator and switching network to switch out or inhibit failed redundant elements.

45

© Gert Jervan, TTÜ/ATI IAF0030 - Arvutitehnika erikursus I

Gate Connector Voting

Active - Type 6

Similar to majority voting. Redundant elements are generally binary circuits. Outputs of the binary elements are fed to switch-like gates which perform the voting function. The gates contain no components whose failure would cause the redundant circuit to fail. Any failures in the gate connector act as though the binary element were at fault.

46

© Gert Jervan, TTÜ/ATI IAF0030 - Arvutitehnika erikursus I

Non-Operating Redundancy

Standby - Type 7

A particular redundant element of a parallel configuration can be switched into an active circuit by connecting outputs of each element to switch poles. Two switching configurations are possible.

- 1) The element may be isolated by the switch until switching is completed and power applied to the element in the switching operation.
- 2) All redundant elements are continuously connected to the circuit and a single redundant element activated by switching power to it.

47

© Gert Jervan, TTÜ/ATI IAF0030 - Arvutitehnika erikursus I

Operating Redundancy

Standby - Type 8

In this application, all redundant units operate simultaneously. A sensor on each unit detects failures. When a unit fails, a switch at the output transfers to the next unit and remains there until failure.

48

© Gert Jervan, TTÜ/ATI IAF0030 - Arvutitehnika erikursus I

Hybrid Hardware Redundancy

✓ Hybrid:

- combine the attractive features of both the passive and active approaches
 - fault masking
 - fault detection
 - fault location
 - recovery

TALLINNA TEHNIEAÜLIKOOL
TALLINN UNIVERSITY OF TECHNOLOGY

49

© Gert Jervan, TTÜ/ATI IAF0030 - Arvutitehnika erikursus I

Self-Purging Redundancy

Can mask $n-2$ module faults

TALLINNA TEHNIEAÜLIKOOL
TALLINN UNIVERSITY OF TECHNOLOGY

50

© Gert Jervan, TTÜ/ATI IAF0030 - Arvutitehnika erikursus I

Self Purging Redundancy

✓ Initially start with NMR

✓ Purge one unit at a time till arrive at TMR

- can tolerate more faults initially compared to NMR with spare
- cost of the switch - higher?

TALLINNA TEHNIEAÜLIKOOL
TALLINN UNIVERSITY OF TECHNOLOGY

51

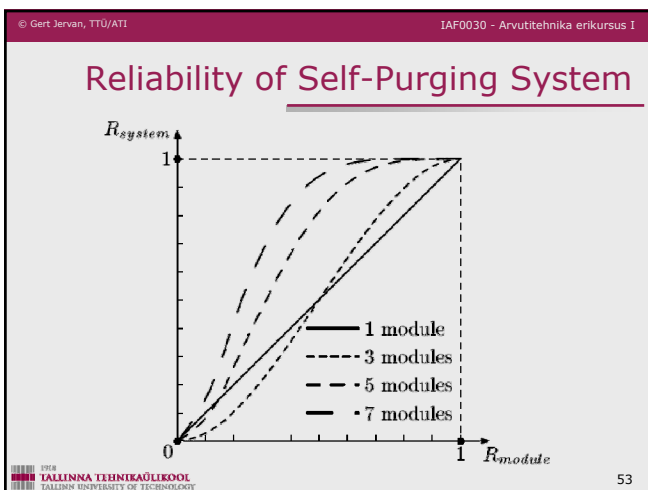
© Gert Jervan, TTÜ/ATI IAF0030 - Arvutitehnika erikursus I

Basic Structure of a Switch

✓ If output of a module disagrees with the output of the system, its contribution to the voter is forced to be 0 (threshold voter)

TALLINNA TEHNIEAÜLIKOOL
TALLINN UNIVERSITY OF TECHNOLOGY

52



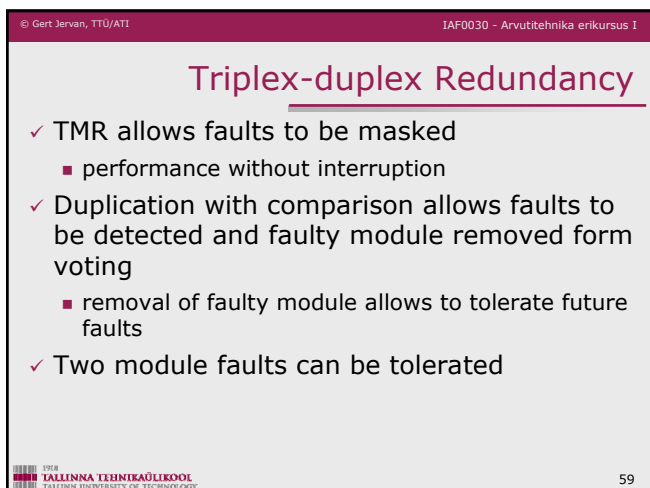
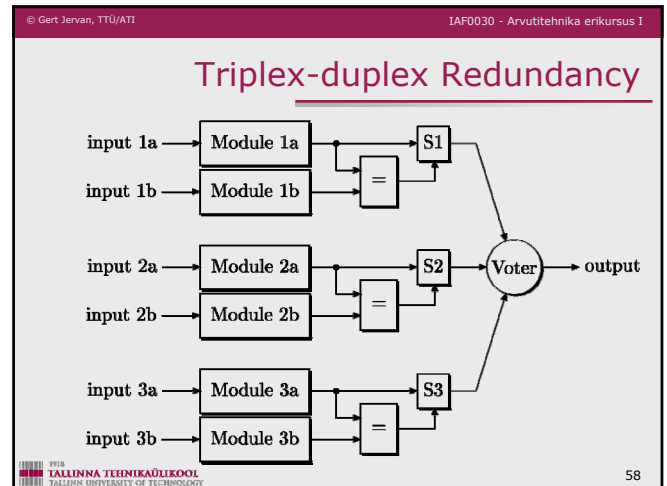
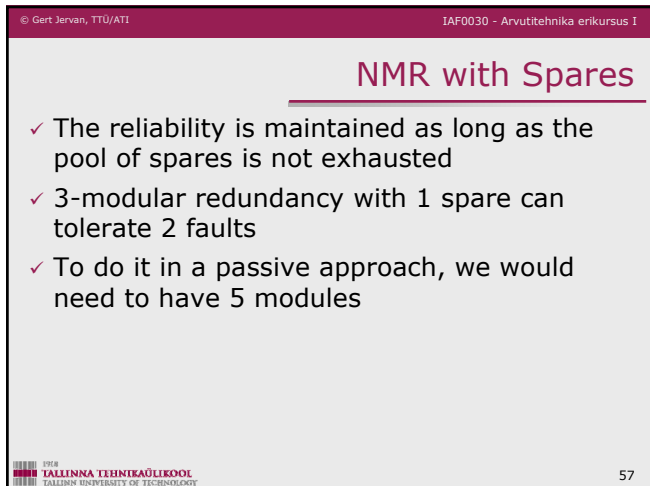
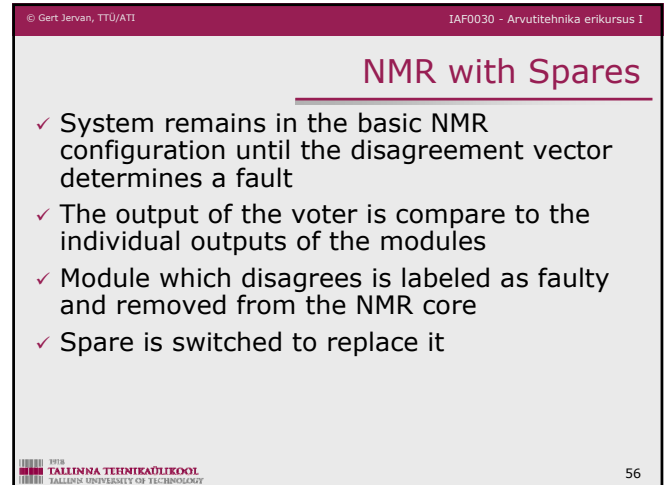
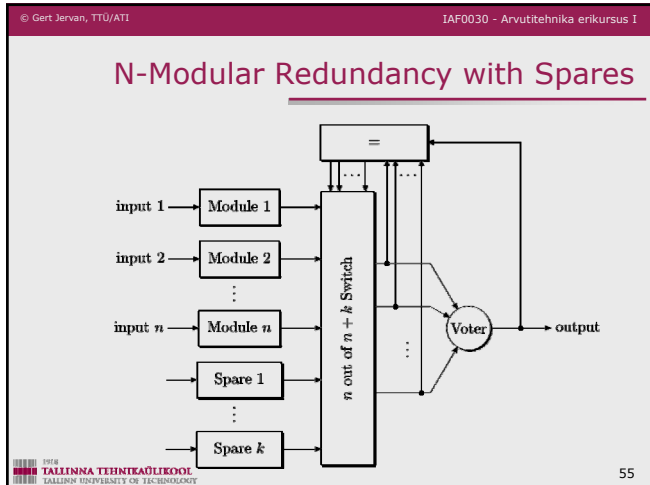
© Gert Jervan, TTÜ/ATI IAF0030 - Arvutitehnika erikursus I

N-Modular Redundancy with Spares

- Most hybrid redundancy are based on the concept of N-modular redundancy (NMR) with spares
- The idea is to provide N modules arranged in a voting configuration
- Spares are provided to replace failed modules
- The advantage of NMR with spares is that a voting configuration can be restored after a fault has occurred

TALLINNA TEHNIEAÜLIKOOL
TALLINN UNIVERSITY OF TECHNOLOGY

54



© Gert Jervan, TTÜ/ATI IAF0030 - Arvutitehnika erikursus I

Introduction

- ✓ Less understood and less mature than in hardware
- ✓ Software does not degrade over time
- ✓ Design faults
- ✓ Environment

1918 TALLINNA TEHNIKAÜLIKOOL
TALLINN UNIVERSITY OF TECHNOLOGY 61

© Gert Jervan, TTÜ/ATI IAF0030 - Arvutitehnika erikursus I

Introduction

- ✓ Many current techniques for software fault tolerance attempt to leverage the experience of hardware redundancy schemes
 - software N-version programming closely resembles hardware N-modular redundancy
 - recovery blocks use the concept of retrying the same operation in expectation that the problem is resolved after the second try.

1918 TALLINNA TEHNIKAÜLIKOOL
TALLINN UNIVERSITY OF TECHNOLOGY 62

© Gert Jervan, TTÜ/ATI IAF0030 - Arvutitehnika erikursus I

Problems

- ✓ Traditional hardware fault tolerance techniques were developed to fight
 - permanent components faults primarily
 - transient faults caused by environmental factors secondarily.
- ✓ They do not offer sufficient protection against design and specification faults, which are dominant in software.

1918 TALLINNA TEHNIKAÜLIKOOL
TALLINN UNIVERSITY OF TECHNOLOGY 63

© Gert Jervan, TTÜ/ATI IAF0030 - Arvutitehnika erikursus I

Concepts for Traditional SFT

- ✓ Software design and implementation errors cannot be detected by simple replication of identical software units, assuming the same inputs are provided to each copy.
- ✓ Some form of diversity must accompany the redundancy
 - Software redundancy → Design diversity
 - Information or data redundancy → Data diversity
 - Temporal redundancy → Temporal diversity
 - Environment diversity
 - Hardware redundancy

1918 TALLINNA TEHNIKAÜLIKOOL
TALLINN UNIVERSITY OF TECHNOLOGY 64

© Gert Jervan, TTÜ/ATI IAF0030 - Arvutitehnika erikursus I

Single- and multi-version

- ✓ Software fault-tolerance techniques can be divided into two groups:
 - single-version
 - multi-version
- ✓ Single version techniques aim to improve fault tolerant capabilities of a single software module
 - fault detection, containment and recovery mechanisms
- ✓ Multi-version techniques employ redundant software modules, developed following design diversity rules

1918 TALLINNA TEHNIKAÜLIKOOL
TALLINN UNIVERSITY OF TECHNOLOGY 65

© Gert Jervan, TTÜ/ATI IAF0030 - Arvutitehnika erikursus I

Redundancy Allocation

- ✓ A number of possibilities have to be examined:
 - at which level the redundancy need to be provided
- ✓ Redundancy can be applied to a procedure, or to a process, or to the whole software system
 - which modules are to be made redundant
- ✓ Usually, the components which have high probability of faults are chosen to be made redundant.
- ✓ The increase in complexity caused by redundancy can be quite severe and may diminish the dependability improvement

1918 TALLINNA TEHNIKAÜLIKOOL
TALLINN UNIVERSITY OF TECHNOLOGY 66

© Gert Jervan, TTÜ/ATI IAF0030 - Arvutitehnika erikursus I

Single-Version (Dynamic) Techniques

- ✓ Dynamic redundancy kicks in only when an error is detected.
- ✓ Four phases
 - 1. **Error detection:**
fault tolerance techniques effective only when an error is detected
 - 2. **Damage assessment and containment:**
to what extent the "damage" has spread because of the delay between a fault and its manifestation/detection?
 - 3. **Error recovery:**
techniques to reach from a corrupted to a safe state
 - 4. **Fault treatment and continued service:**
error correction.

1918 TALLINNA TEHNIEKÜLIKOOI
TALLINN UNIVERSITY OF TECHNOLOGY

67

© Gert Jervan, TTÜ/ATI IAF0030 - Arvutitehnika erikursus I

1 - Error Detection

- ✓ The goal is to determine that a fault has occurred within a system.
- ✓ Various types of acceptance tests are used to detect faults
 - the result of a program is subjected to a test
 - if the result passes the test, the program continues its execution
 - a failed test indicates a fault

1918 TALLINNA TEHNIEKÜLIKOOI
TALLINN UNIVERSITY OF TECHNOLOGY

68

© Gert Jervan, TTÜ/ATI IAF0030 - Arvutitehnika erikursus I

Acceptance Test

- ✓ Acceptance test is most effective if it can be calculated in a simple way and if it is based on criteria that can be derived independently of the program application.
- ✓ The existing techniques include
 - timing checks
 - coding checks
 - reversal checks
 - reasonableness checks
 - structural checks
 - replication checks
 - dynamic reasonableness checks

1918 TALLINNA TEHNIEKÜLIKOOI
TALLINN UNIVERSITY OF TECHNOLOGY

69

© Gert Jervan, TTÜ/ATI IAF0030 - Arvutitehnika erikursus I

Timing Checks

- ✓ Timing checks are applicable to system whose specification include timing constrains
- ✓ Based on these constrains, checks are developed to indicate a deviation from the required behavior.
 - Watchdog timer is an example of a timing check
 - Watchdog timers are used to monitor the performance of a system and detect lost or locked out modules.

1918 TALLINNA TEHNIEKÜLIKOOI
TALLINN UNIVERSITY OF TECHNOLOGY

70

© Gert Jervan, TTÜ/ATI IAF0030 - Arvutitehnika erikursus I

Coding Checks

- ✓ Coding checks are applicable to system whose data can be encoded using information redundancy techniques
- ✓ Usually used in cases when the information is merely transported from one module to another without changing it content.
 - Arithmetic codes can be used to detect errors in arithmetic operations

1918 TALLINNA TEHNIEKÜLIKOOI
TALLINN UNIVERSITY OF TECHNOLOGY

71

© Gert Jervan, TTÜ/ATI IAF0030 - Arvutitehnika erikursus I

Reversal Checks

- ✓ In some system, it is possible to reverse the output values and to compute the corresponding input values.
- ✓ A reversal checks compares the actual inputs of the system with the computed ones.
 - a disagreement indicates a fault.

1918 TALLINNA TEHNIEKÜLIKOOI
TALLINN UNIVERSITY OF TECHNOLOGY

72

© Gert Jervan, TTÜ/ATI IAF0030 - Arvutitehnika erikursus I

Reasonableness Checks

- ✓ Reasonableness checks use semantic properties of data to detect fault.
 - a range of data can be examined for overflow or underflow to indicate a deviation from system's requirements
- ✓ Maximum withdrawal sum in bank's teller machine
- ✓ Address generated by a computer should lie inside the range of available memory

TALLINNA TEHNIKAÜLIKOOL
TALLINN UNIVERSITY OF TECHNOLOGY

73

© Gert Jervan, TTÜ/ATI IAF0030 - Arvutitehnika erikursus I

Structural Checks

- ✓ Structural checks are based on known properties of data structures
 - a number or elements in a list can be counted, or links and pointer can be verified
- ✓ Structural checks can be made more efficient by adding redundant data to a data structure,
 - attaching counts on the number of items in a list, or adding extra pointers

TALLINNA TEHNIKAÜLIKOOL
TALLINN UNIVERSITY OF TECHNOLOGY

74

© Gert Jervan, TTÜ/ATI IAF0030 - Arvutitehnika erikursus I

2 - Damage Assessment & Containment

- ✓ Necessary due to the delay between fault and error
- ✓ Goal of containment is to minimize damage caused by a faulty component
 - "firewalling"
- ✓ Assessment closely related to containment techniques used
- ✓ Techniques for fault containment:
 - modularization
 - partitioning
 - system closure
 - atomic actions

TALLINNA TEHNIKAÜLIKOOL
TALLINN UNIVERSITY OF TECHNOLOGY

75

© Gert Jervan, TTÜ/ATI IAF0030 - Arvutitehnika erikursus I

Modularization

- ✓ Software system is divided into modules with few or no common dependencies between them
- ✓ Modularization attempts to prevent the propagation of faults
 - by limiting the amount of communication between modules to carefully monitored messages
 - by eliminating shared resources

TALLINNA TEHNIKAÜLIKOOL
TALLINN UNIVERSITY OF TECHNOLOGY

76

© Gert Jervan, TTÜ/ATI IAF0030 - Arvutitehnika erikursus I

Partitioning

- ✓ Modular hierarchy of a software architecture is partitioned in horizontal or vertical dimensions
- ✓ Horizontal partitioning separates the major software functions into independent branches
 - The execution of the functions and the communication between them is done using control modules
- ✓ Vertical partitioning distributes the control and processing function in a top-down hierarchy.
 - High-level modules normally focus on control functions, while low-level modules perform processing

TALLINNA TEHNIKAÜLIKOOL
TALLINN UNIVERSITY OF TECHNOLOGY

77

© Gert Jervan, TTÜ/ATI IAF0030 - Arvutitehnika erikursus I

System Closure

- ✓ System closure technique is based on a principle that no action is permissible unless explicitly authorized
- ✓ In an environment with many restrictions and strict control all the interactions between the elements of the system are visible
 - prison
- ✓ It is easier to locate and disable any fault.

TALLINNA TEHNIKAÜLIKOOL
TALLINN UNIVERSITY OF TECHNOLOGY

78

© Gert Jervan, TTÜ/ATI IAF0030 - Arvutitehnika erikursus I

Atomic Action

- ✓ An atomic action among a group of components in an activity in which the components interact exclusively with each other.
 - no interaction with the rest of the system
- ✓ Two possible outcomes of an atomic action:
 - it terminates normally
 - it is aborted upon a fault detection
- ✓ Fault containment area is defined and fault recovery is limited to atomic action components

TALLINNA TEHNIKAÜLIKOOL
TALLINN UNIVERSITY OF TECHNOLOGY

79

© Gert Jervan, TTÜ/ATI IAF0030 - Arvutitehnika erikursus I

3 Fault Recovery

- ✓ Once a fault is detected and contained, a system attempts to recover from the faulty state and regain operational status
 - If fault detection and containment mechanisms are implemented properly, the effects of the faults are contained within a particular set of modules at the moment of fault detection.
- ✓ The knowledge of fault containment region is essential for the design of effective fault recovery mechanism

TALLINNA TEHNIKAÜLIKOOL
TALLINN UNIVERSITY OF TECHNOLOGY

80

© Gert Jervan, TTÜ/ATI IAF0030 - Arvutitehnika erikursus I

Exception Handling

- ✓ Exception handling is the interruption of normal operation to handle abnormal responses
- ✓ Possible events triggering the exceptions:
 - Interface exceptions
 - signaled by a module when it detects an invalid service request
 - Local exceptions
 - signaled by a module when its fault detection mechanism detects a fault
 - Failure exceptions
 - signaled by a module when it has detected that its fault recovery mechanism is unable to recover successfully

TALLINNA TEHNIKAÜLIKOOL
TALLINN UNIVERSITY OF TECHNOLOGY

81

© Gert Jervan, TTÜ/ATI IAF0030 - Arvutitehnika erikursus I

Recovery

- ✓ Forward or Backward
- ✓ Forward: continues from an erroneous state by making selective corrections to the system state
 - includes making safe the controlled environment which may be hazardous or damaged because of failure
 - system specific and depends upon accurate predictions
 - e.g., redundant pointers in data structures, self-correcting codes

TALLINNA TEHNIKAÜLIKOOL
TALLINN UNIVERSITY OF TECHNOLOGY

82

© Gert Jervan, TTÜ/ATI IAF0030 - Arvutitehnika erikursus I

Recovery

- ✓ Backward: relies on restoring the system to a previous safe state and executing an alternative section of the program
 - safe functionality but different algorithm
 - the point to which a process is restored is called a **recovery point** and the act of establishing it is called **checkpointing**.
 - BER can be used to recover from unanticipated faults including design errors.
 - State restoration is not always possible in (real-time) embedded systems.

TALLINNA TEHNIKAÜLIKOOL
TALLINN UNIVERSITY OF TECHNOLOGY

83

© Gert Jervan, TTÜ/ATI IAF0030 - Arvutitehnika erikursus I

Backward Recovery

- ✓ Attempts to return the system to a correct or error-free state.
- ✓ For transient faults
- ✓ Example: recovery blocks (RcB)

TALLINNA TEHNIKAÜLIKOOL
TALLINN UNIVERSITY OF TECHNOLOGY

© Gert Jervan, TTÜ/ATI IAF0030 - Arvutitehnika erikursus I

Static Checkpoints

- ✓ A static checkpoint takes a single snapshot of the system state at the beginning of the program execution and stores it in the memory.
 - If a fault is detected, the system returns to this state and starts the execution from the beginning.
 - Fault detection checks are placed at the output of the module

1918 TALLINNA TEHNIKAÜLIKOOL TALLINN UNIVERSITY OF TECHNOLOGY 85

© Gert Jervan, TTÜ/ATI IAF0030 - Arvutitehnika erikursus I

Dynamic Checkpoints

- ✓ Dynamic checkpoints are created dynamically at various points during the execution
 - If a fault is detected, the system returns to the last checkpoint and continues the execution.
 - Fault detection checks need to be embedded in the code and executed before the checkpoints are created

1918 TALLINNA TEHNIKAÜLIKOOL TALLINN UNIVERSITY OF TECHNOLOGY 86

© Gert Jervan, TTÜ/ATI IAF0030 - Arvutitehnika erikursus I

Static vs. Dynamic

- ✓ In static approach, the expected time to complete the execution grows exponentially with the execution requirements.
 - static checkpointing is effective only if the processing requirement is relatively small.
- ✓ In dynamic approach, it is possible to achieve linear increase in execution time as the processing requirements grow

1918 TALLINNA TEHNIKAÜLIKOOL TALLINN UNIVERSITY OF TECHNOLOGY 87

© Gert Jervan, TTÜ/ATI IAF0030 - Arvutitehnika erikursus I

Strategies for dynamic checkpointing

- ✓ Equidistant
 - places checkpoints at deterministic fixed time intervals
 - the time between checkpoints is chosen depending on the expected fault rate
- ✓ Modular
 - places checkpoints at the end of the sub-modules in a module, after the fault detection checks for the submodule are completed
 - the execution time depends on the distribution of the sub-modules and expected fault rate
- ✓ • Random

1918 TALLINNA TEHNIKAÜLIKOOL TALLINN UNIVERSITY OF TECHNOLOGY 88

© Gert Jervan, TTÜ/ATI IAF0030 - Arvutitehnika erikursus I

Advantages

- ✓ Conceptually simple
- ✓ Independent of the damage caused by a fault
- ✓ Applicable to unanticipated faults
- ✓ General enough to be used at multiple levels in a system

1918 TALLINNA TEHNIKAÜLIKOOL TALLINN UNIVERSITY OF TECHNOLOGY 89

© Gert Jervan, TTÜ/ATI IAF0030 - Arvutitehnika erikursus I

Problems

- ✓ Non-recoverable actions exist in some systems
 - these actions cannot be compensated by simply reloading the state and restarting the system
 - firing a missile
 - soldering a pair of wires
- ✓ The recovery from such actions can be done
 - by compensating for their consequences
 - undoing a solder
 - by delaying their output until after additional confirmation checks are completed
 - do a friend-or-foe confirmation before firing

1918 TALLINNA TEHNIKAÜLIKOOL TALLINN UNIVERSITY OF TECHNOLOGY 90

© Gert Jervan, TTÜ/ATI IAF0030 - Arvutitehnika erikursus I

Forward Recovery

- ✓ Attempts to find a new state from which the system can continue operation.
- ✓ Utilize error compensation based on redundancy to select or derive the correct answer or an acceptable answer.
- ✓ Example: N-version programming (NVP), N-copy programming (NCP), and the distributed recovery block (DRB)

91

© Gert Jervan, TTÜ/ATI IAF0030 - Arvutitehnika erikursus I

Forward Recovery

- ✓ Efficient for predictable errors

92

© Gert Jervan, TTÜ/ATI IAF0030 - Arvutitehnika erikursus I

4 - Fault Treatment and Continued Service

- ✓ Even with recovery, the error may recur. Need to eradicate the fault from the system
- ✓ Automatic treatment of faults is very application specific
- ✓ Make some assumptions. For instance:
 - all faults are transient
- ✓ Fault treatment in two stages
 - Fault location
 - System repair
- ✓ Fault location
 - use error detection techniques to trace a fault to a component (hardware or software)
 - System repair
 - sometimes it has to be done while the system is in operation.

93

© Gert Jervan, TTÜ/ATI IAF0030 - Arvutitehnika erikursus I

Multi-Version Techniques

- ✓ Multi-version techniques use two or more versions the same software module, which satisfy design diversity requirements.
 - different teams, different coding languages or different algorithms can be used to maximize the probability that all the versions do not have common faults

94

© Gert Jervan, TTÜ/ATI IAF0030 - Arvutitehnika erikursus I

Design Diversity

- ✓ Higher cost

95

© Gert Jervan, TTÜ/ATI IAF0030 - Arvutitehnika erikursus I

SFT Techniques Using Design Diversity

Techniques	Abbr.	Error Processing
Recovery Blocks	RcB	Error detection by AT and backward recovery
N-Version Programming	NVP	Vote
N Self-Checking Programming	NSCP	Error detection by AT and forward recovery

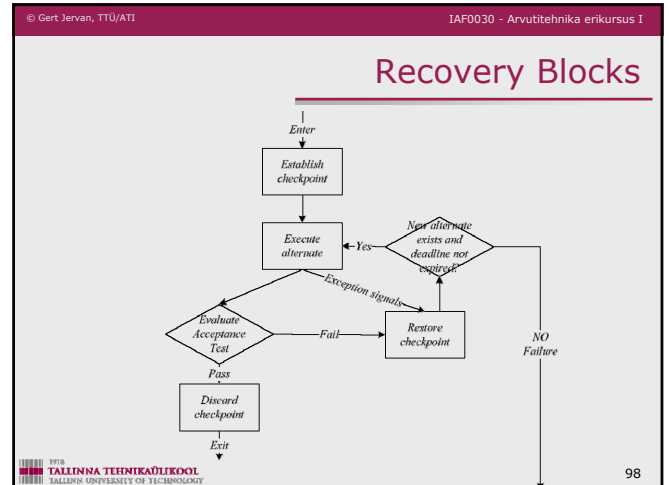
AT – Acceptance Test 96

© Gert Jervan, TTÜ/ATI IAF0030 - Arvutitehnika erikursus I

Recovery Blocks

- ✓ Combines checkpoint and restart approach with standby sparing redundancy scheme
- ✓ n different implementations of the same program
 - Only one of the versions is active
 - If an error is detected by the acceptance test, a retry signal is sent to the switch
 - The system is rolled back to the state stored in the checkpoint memory and the execution is switched to another module

97



© Gert Jervan, TTÜ/ATI IAF0030 - Arvutitehnika erikursus I

Recovery Blocks

Method	Recovery block
Error Processing Technique	Error detection by AT and backward recovery
Criteria of Accepting Result	Absolute, with respect to specification
Execution Scheme	Sequential
Consistency of Input Data	Implicit, from backward recovery principle

99

- © Gert Jervan, TTÜ/ATI IAF0030 - Arvutitehnika erikursus I
- ## Recovery Blocks
- ✓ A language level support for backward error recovery
 - blocks in the normal programming language sense, but
 - at the entrance to the block is an automatic recovery point and
 - at the exit an acceptance test to test that the system is in an acceptable state
 - if the acceptance test fails, the program is restored to the recovery point at the beginning of the block and an alternative module is executed
 - repeat this process with alternative modules
 - if all fail, recovery must take place at a higher level
 - ✓ In terms of four phases of software fault tolerance
 - Error detection <-> acceptance test
 - Damage assessment <-> not needed due to BER
 - Fault treatment <-> stand-by spare code
- 100

- © Gert Jervan, TTÜ/ATI IAF0030 - Arvutitehnika erikursus I
- ## Recovery Blocks
- ✓ Similarly to cold and hot standby sparing, different version can be executed either serially, or concurrently
 - Serial execution may require the use of checkpoints to reload the state before the next version is executed
 - The cost in time of trying multiple versions serially may be too expensive, especially for a real-time system.
 - A concurrent system requires n redundant hardware modules, a communications network to connect them and the use of input and state consistency algorithms.
- 101

© Gert Jervan, TTÜ/ATI IAF0030 - Arvutitehnika erikursus I

Syntax of Recovery Blocks

```

ensure <acceptance test>
by
  <primary module>
else by
  <alternative module>
else by
  <alternative module>
...
else by
  <alternative module>
else error
        
```

- ✓ Recovery blocks can be nested
- ✓ If all alternatives in a nested recovery block fail the acceptance test, the outer level recovery point will be restored
 - (and an alternative module to that block will be executed).

102

© Gert Jervan, TTÜ/ATI IAF0030 - Arvutitehnika erikursus I

N-Version Programming

- ✓ Resembles N-modular hardware redundancy
- ✓ N different software implementations of a module are executed concurrently.
- ✓ The selection algorithm (voter) decides which of the answers is correct
 - a voter is application independent
 - this is an advantage over recovery block fault detection mechanism, requiring application dependent acceptance tests

103

© Gert Jervan, TTÜ/ATI IAF0030 - Arvutitehnika erikursus I

NVP

```

    graph TD
      Enter --> DistributeInputs[Distribute Inputs]
      DistributeInputs --> Version1[Version 1]
      DistributeInputs --> VersionN1[Version N-1]
      DistributeInputs --> VersionN[Version N]
      Version1 --> VersionN1
      VersionN1 --> DM{DM}
      VersionN --> DM
      DM --> Exit[Exit]
      DM --> ExceptionFailure[Exception Failure]
    
```

104

© Gert Jervan, TTÜ/ATI IAF0030 - Arvutitehnika erikursus I

N-version Programming

Method	N-version programming
Error Processing Technique	Vote
Criteria of Accepting Result	Relative, on variant results
Execution Scheme	Parallel
Consistency of Input Data	Explicit by dedicated mechanisms

105

© Gert Jervan, TTÜ/ATI IAF0030 - Arvutitehnika erikursus I

N-Version Programming

- ✓ Consists of independent generation of N (>2) functionally equivalent programs from same initial specifications
 - Design Diversity, Different Programming Language, Methods..
- ✓ Programs execute concurrently, results are arrived at by consensus (majority voting).
- ✓ Questions
 - How are results compared? How is voting conducted?
- ✓ NVP depends upon
 - good initial specification, independence of effort, abundance of effort.
- ✓ NVP can be taken further
 - compiling, processing, ...

106

© Gert Jervan, TTÜ/ATI IAF0030 - Arvutitehnika erikursus I

NVP

- ✓ Controlled by a **driver** process
 - invokes each of the versions
 - waiting for the versions to complete
 - comparing and acting on the results
- ✓ Problem: assumes programs run to completion!
 - So the versions must actually interact (with the driver program)
 - **Comparison Points:** points in the versions when programs must communicate their votes to the driver process
 - Defines granularity of the fault tolerance
 - How the versions communicate and synchronize depend upon the programming language used, its model of concurrency

107

© Gert Jervan, TTÜ/ATI IAF0030 - Arvutitehnika erikursus I

Vote Comparison in NVP

- ✓ Efficiency of vote comparison is critical
- ✓ Complicated by comparison procedure
 - Not all results are single numeric values
 - The "consistent comparison problem"
 - When using "thresholds" for comparison the errors can stack up, resulting different execution paths in *all* versions.

Two sequential thresholding lead to different execution paths in all three versions.

The problem will reappear even when using inexact comparison (just have to be near a threshold value).

And what happens when there are multiple solutions?

108

© Gert Jervan, TTÜ/ATI IAF0030 - Arvutitehnika erikursus I

NVP versus RB

- ✓ NVP is static where as RB is dynamic redundancy
- ✓ Both have design overheads
 - alternative algorithms
 - NVP requires a driver
 - RB requires an acceptance test
- ✓ Runtime overheads
 - NV requires more resources
 - RB requires establishing recovery points
- ✓ Both susceptible to errors in requirements
- ✓ Error detection
 - vote comparison (NVP) versus acceptance test (RB)
- ✓ Atomicity requirement
 - NV vote before it outputs to the environment, RB must output only following the passing of the acceptance test.

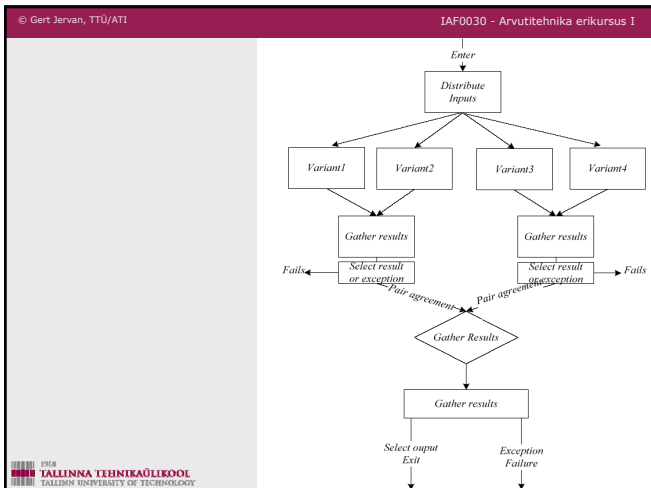
109

© Gert Jervan, TTÜ/ATI IAF0030 - Arvutitehnika erikursus I

N Self-Checking Programming

- ✓ N self-checking programming combines recovery block concept with N version programming
- ✓ The checking is performed either by using acceptance tests, or by using comparison.
- ✓ Examples of applications of N self-checking programming:
 - Lucent ESS-5 phone switch
 - Airbus A-340 airplane

110



© Gert Jervan, TTÜ/ATI IAF0030 - Arvutitehnika erikursus I

NSCP

Method	N self-checking programming
Error Processing Technique	Error detection and result switching Then, Detection by comparison or by AT(s)
Criteria of Accepting Result	Relative, on variant results or Absolute with respect to specification
Execution Scheme	Parallel
Consistency of Input Data	Explicit, by dedicated mechanisms

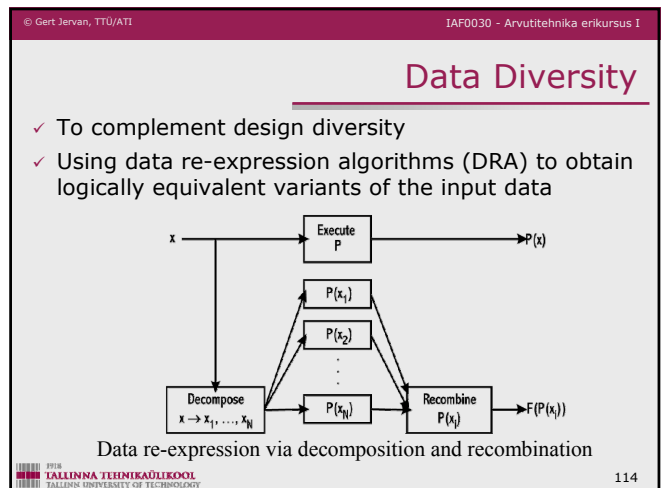
112

© Gert Jervan, TTÜ/ATI IAF0030 - Arvutitehnika erikursus I

Comparison

- ✓ N self-checking programming using acceptance tests
 - The use of separate acceptance test for each version is the main difference of this technique from recovery blocks
- ✓ N self-checking programming using comparison
 - resembles triplex-duplex hardware redundancy
 - An advantage over N self-checking programming using acceptance tests is that the application independent decision algorithm is used for fault detection

113



© Gert Jervan, TTÜ/ATI IAF0030 - Arvutitehnika erikursus I

SFT Techniques Using Data Diversity

SFT Techniques	Abbr.	Error Processing
Retry Blocks	RtB	Acceptance test and Backward recovery
N-Copy Programming	NCP	Run the same process concurrently or sequentially

TALLINNA TEHNIEKÜLIKOOI
TALLINN UNIVERSITY OF TECHNOLOGY

115

© Gert Jervan, TTÜ/ATI IAF0030 - Arvutitehnika erikursus I

Retry Blocks

```

    graph TD
      Enter --> Init[Initialize checkpoint]
      Init --> DRA{New DRA exists  
AND (Deadline not expired)}
      DRA -- Yes --> Exec[Execute Algorithm]
      DRA -- No --> Backup[Invoke backup]
      Exec --> Restore[Restore checkpoint]
      Restore --> EvalAT{Evaluate AT}
      EvalAT -- Pass --> Discard[Discard checkpoint]
      EvalAT -- Fail --> Restore
      Discard --> Exit[Exit]
      Backup --> EvalATBackup{Evaluate AT for backup}
      EvalATBackup --> Exception[Exception Failure]
  
```

TALLINNA TEHNIEKÜLIKOOI
TALLINN UNIVERSITY OF TECHNOLOGY

116

© Gert Jervan, TTÜ/ATI IAF0030 - Arvutitehnika erikursus I

Retry Blocks

Method	Retry blocks
Error Processing Technique	Error detection by AT and backward recovery by DRA
Criteria of Accepting Result	Absolute, with respect to specification
Execution Scheme	Sequential
Consistency of Input Data	Implicit, from backward retry principle

TALLINNA TEHNIEKÜLIKOOI
TALLINN UNIVERSITY OF TECHNOLOGY

117

© Gert Jervan, TTÜ/ATI IAF0030 - Arvutitehnika erikursus I

NCP

```

    graph TD
      Enter --> Distribute[Distribute Inputs]
      Distribute --> V1[Version1]
      Distribute --> V2[Version2]
      Distribute --> Vm[Versionm]
      V1 --> C1[Copy1]
      V2 --> C2[Copy2]
      Vm --> Cn[Copyn]
      C1 --> Gather[Gather results]
      C2 --> Gather
      Cn --> Gather
      Gather --> DM{DM}
      DM -- Select output --> Exit[Exit]
      DM -- Exception Failure --> Exception[Exception Failure]
  
```

TALLINNA TEHNIEKÜLIKOOI
TALLINN UNIVERSITY OF TECHNOLOGY

118

© Gert Jervan, TTÜ/ATI IAF0030 - Arvutitehnika erikursus I

N-copy Programming

Method	N-copy programming
Error Processing Technique	Decision mechanism (DM) and forward recovery
Criteria of Accepting Result	Relative, on variant results
Execution Scheme	Parallel
Consistency of Input Data	Explicit by dedicated mechanisms

TALLINNA TEHNIEKÜLIKOOI
TALLINN UNIVERSITY OF TECHNOLOGY

119

© Gert Jervan, TTÜ/ATI IAF0030 - Arvutitehnika erikursus I

Design Diversity

- ✓ The most critical issue in multi-version software fault tolerance techniques is assuring independence between the different versions of software through design diversity
- ✓ Software systems are vulnerable to common design faults if they are developed by the same design team, by applying the same design rules and using the same software tools

TALLINNA TEHNIEKÜLIKOOI
TALLINN UNIVERSITY OF TECHNOLOGY

120

Design Diversity

- ✓ Decision to be made when developing a multiversion software system include
 - which modules are to be made redundant
 - usually less reliable modules are chosen
 - the level of redundancy
 - procedure, process, whole system
 - the required number of redundant versions
 - the required diversity
 - diverse specification, algorithm, code, programming language, testing technique
 - rules of isolation between the development teams

Questions?