Use of Combined System and Software Reliability Models for Satellite Ground Systems Dependability Predictions

Presented to

GSAW 04

Presented by

Myron Hecht

Aerospace Corporation

El Segundo, CA

March, 2004

Outline

- Background
- Benefits
- How it's done
- Example Application
- Results
- Conclusions

Background

- Integration testing comes when the cost and schedule constraints are the most stringent
- Benefits of additional testing are unclear; resource requirements, costs and schedule impact are very clear
- Optimization strategy: minimize testing time subject to the constraint of the lowest acceptable level of reliability
- *Key Question addressed by this work: how can a program manager determine when that threshold of acceptability will be reached?*

Benefits

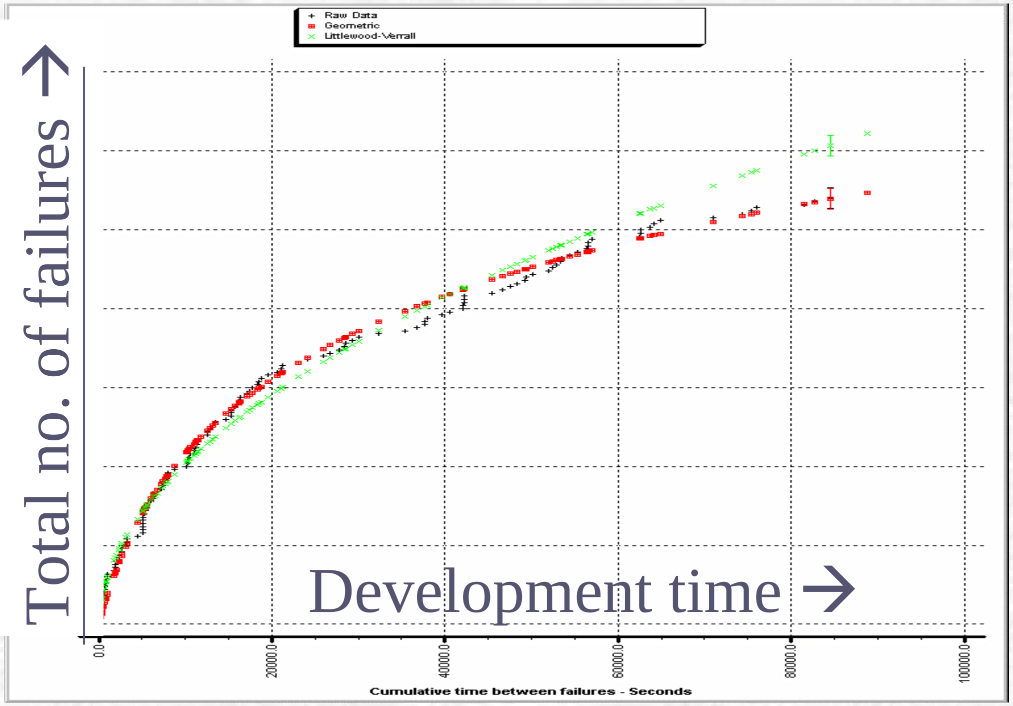
- Provides a program manager with a way of relating benefits of software and integration testing to a predicted level of quality
  - How much time do I need to get to an MTBF (hardware and software) of 168 hours?
  - If I only have time for another 6 weeks of testing, what is the expected MTBF likely to be?

THE AEROSPACE CORPORATION

How It's done

- Use software reliability growth (often called reliability prediction) models to project reliability for individual runtime components
- Integrate these component level models into traditional system reliability models
- Iterate the system model predictions over the projected span of the development activity

Software Reliability Growth Models



In general: models predict future numbers of failures in an interval or the failure rate based on past defect discovery rates and the amount of operating time.

Geometric and Littlewood Verrall Models

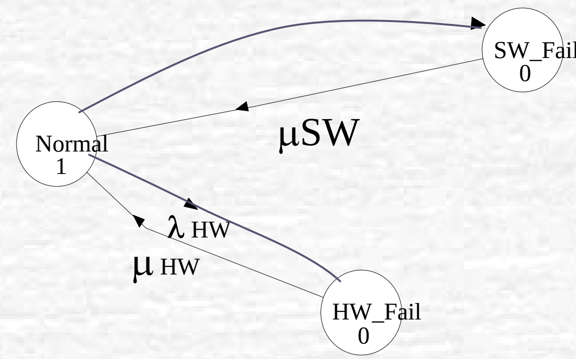
Source: W. Farr, "Software reliability modeling survey," (Chapter 3), in M. Lyu, ed. Handbook of Software Reliability Engineering, McGraw Hill, 1996

THE AEROSPACE CORPORATION

System Reliability Models

- Reliability Block Diagram models

  - Effectively, considering software as simply another component
  - Do not handle reconfiguration, recovery, and common mode failures in redundant systems
    - Imperfect recovery
    - Non-instantaneous recovery



- Markov models
  - State-based
  - Do address reconfiguration and recovery
  - Require assumption of constant failure rate but this can be addressed by multiple iterations

THE AEROSPACE CORPORATION

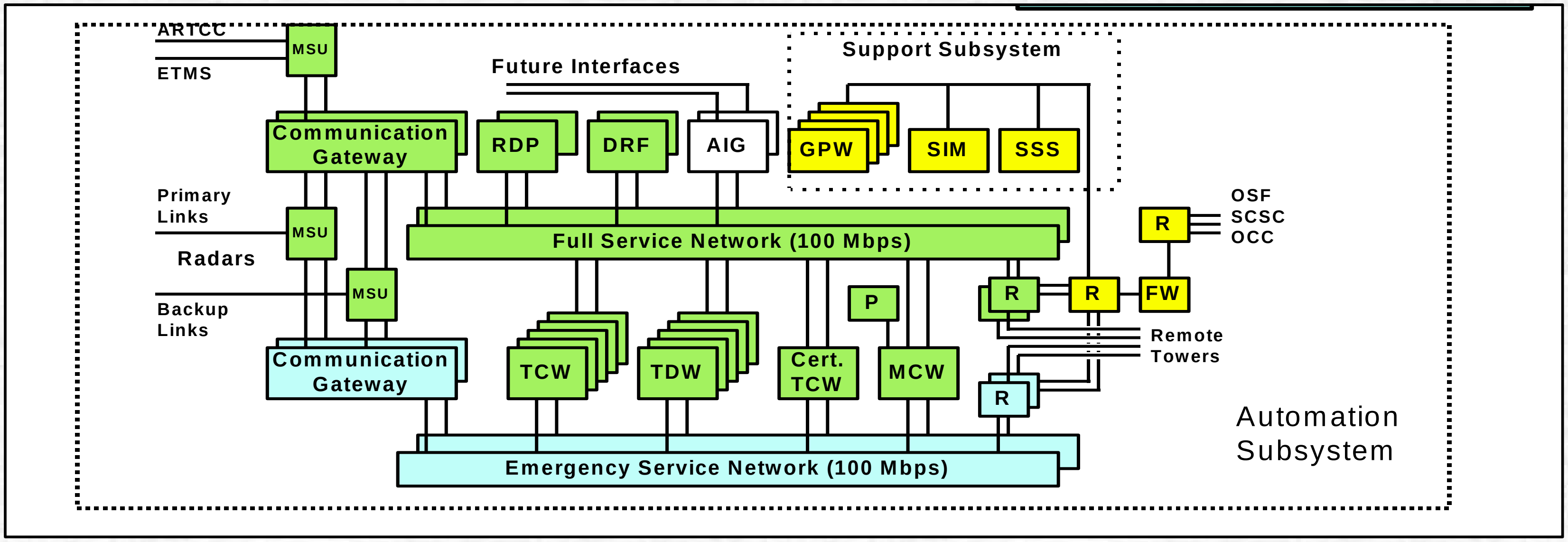
Example System: STARS
(Standard Terminal Automation Replacement System)

- FAA system upgrade to terminal air traffic control
- Operational profile similar to satellite ground system
  - Constant operation
  - Multiple consoles and graphical situation displays
  - Processing of real-time sensor data
  - High availability requirement
- Further information:

  http://www2.faa.gov/ats/atb/Sectors/Automation/STARS/index.htm

THE AEROSPACE CORPORATION

System architecture:

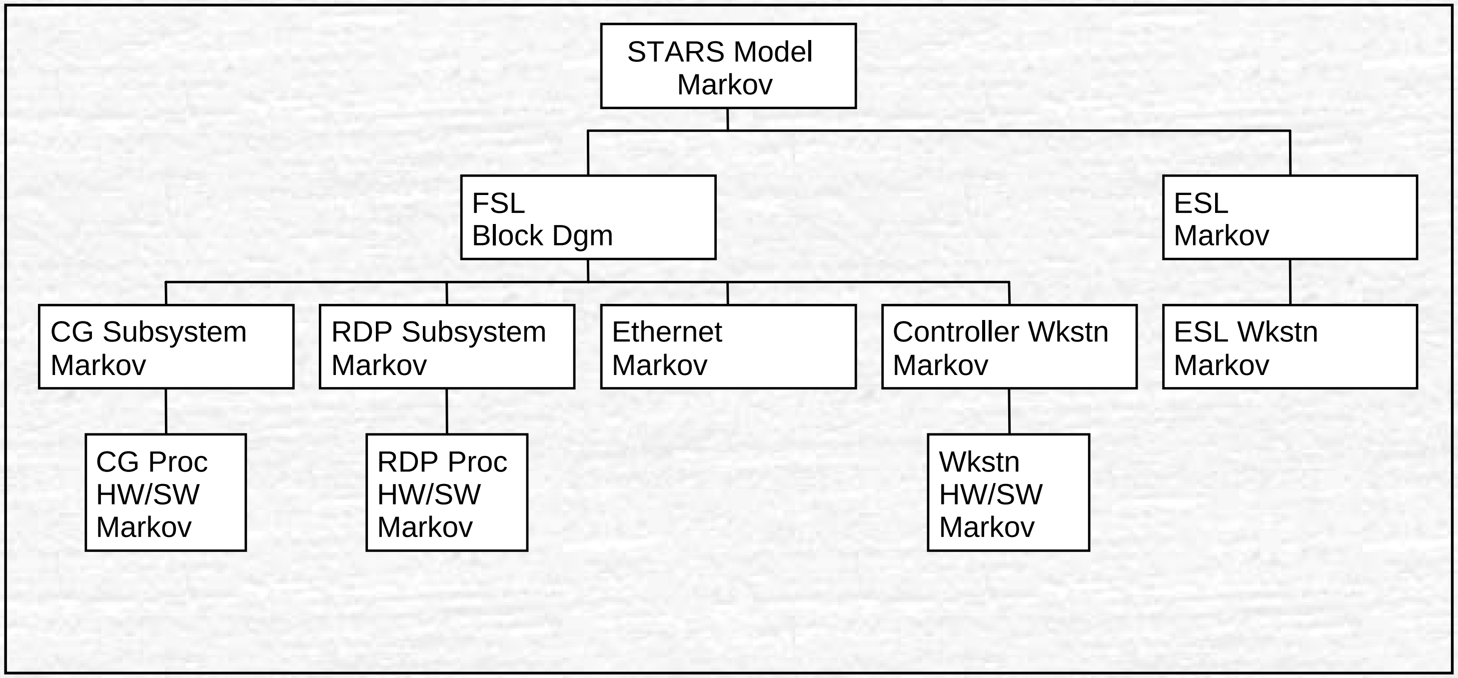


Source: STARS System Segment Specification, CDRL A031
Federal Aviation Administration ATB 230, September, 1997

- Two diverse networks (Full service and emergency)
- Full service network has separate radar data processing
- Each network dual redundant
- Complex software for data processing and display

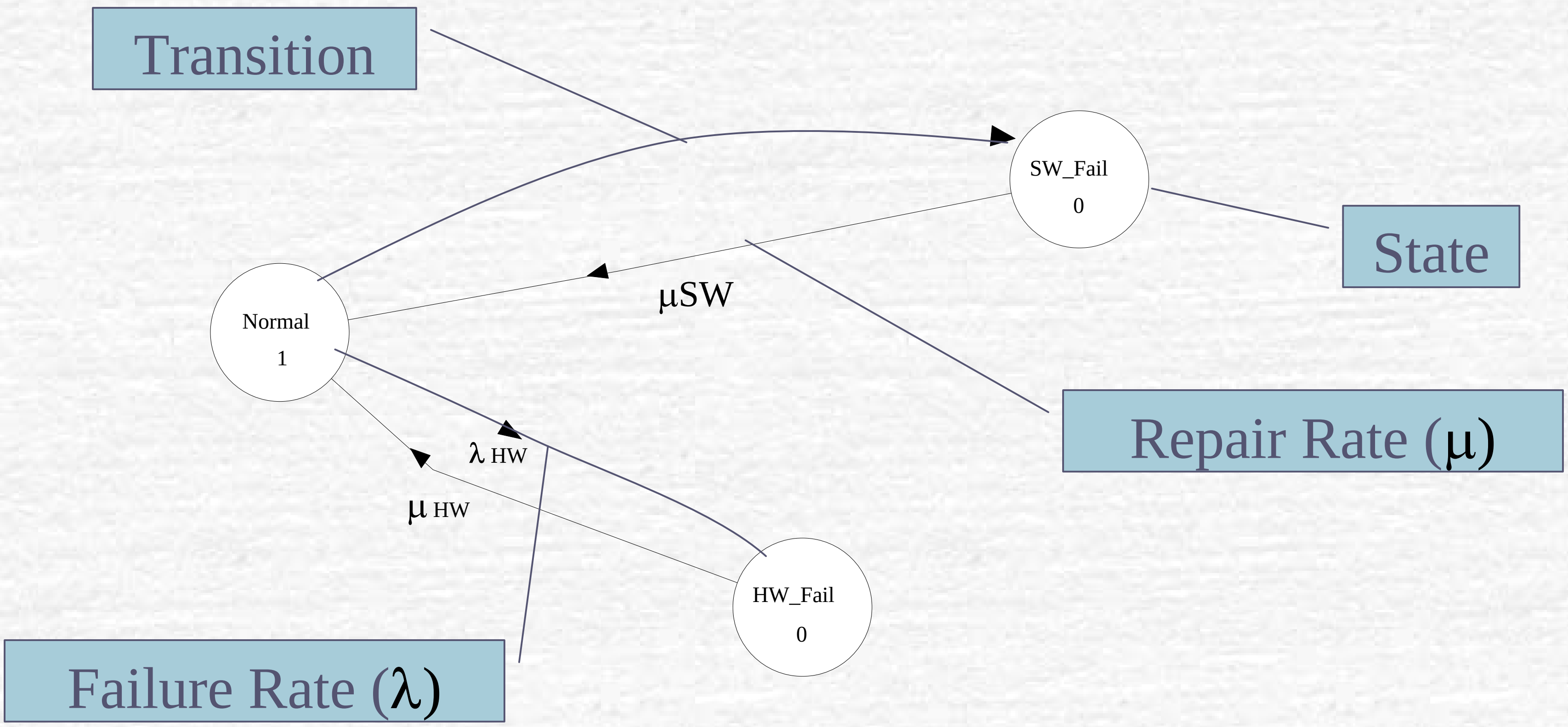
THE AEROSPACE CORPORATION

Simplified Model Hierarchy

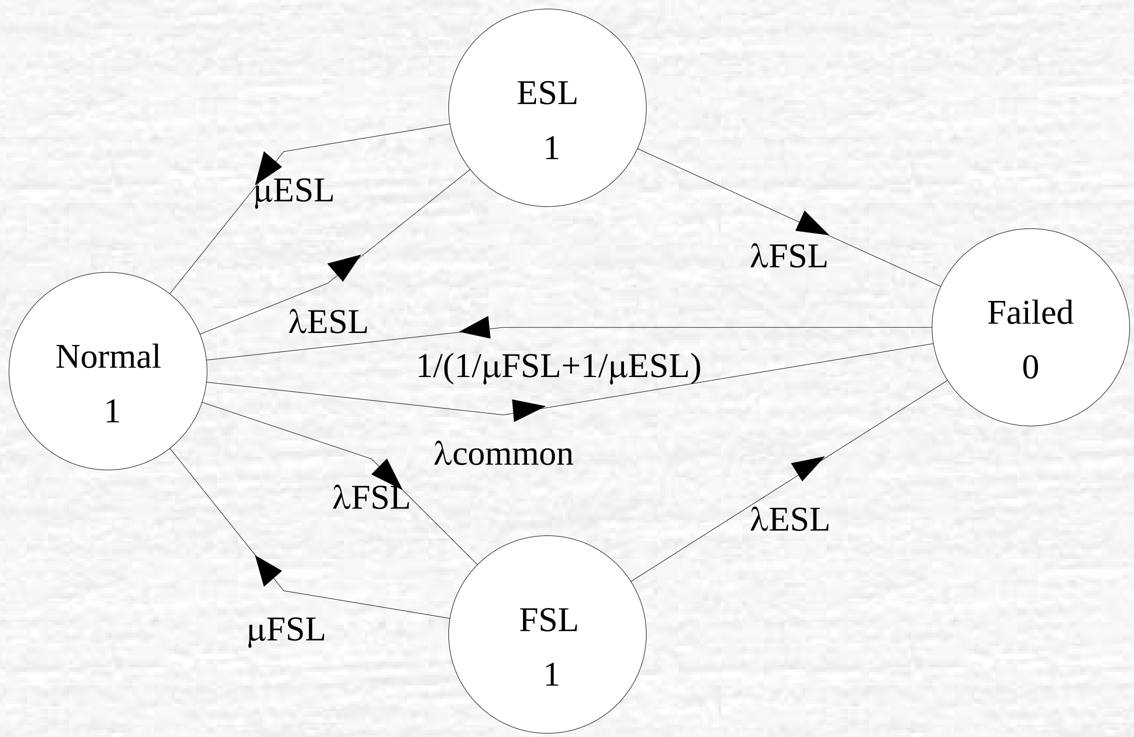


THE AEROSPACE CORPORATION

Markov Diagram Notation

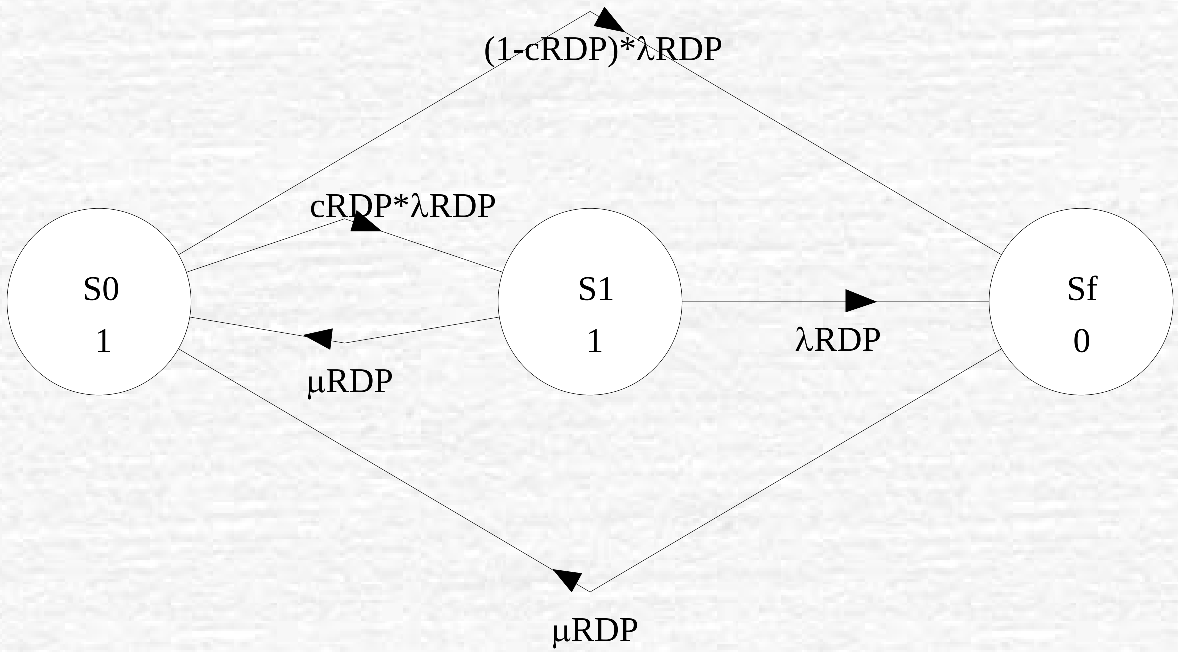


Top Level System Diagram



THE AEROSPACE CORPORATION

Radar Data Processing Subsystem Model



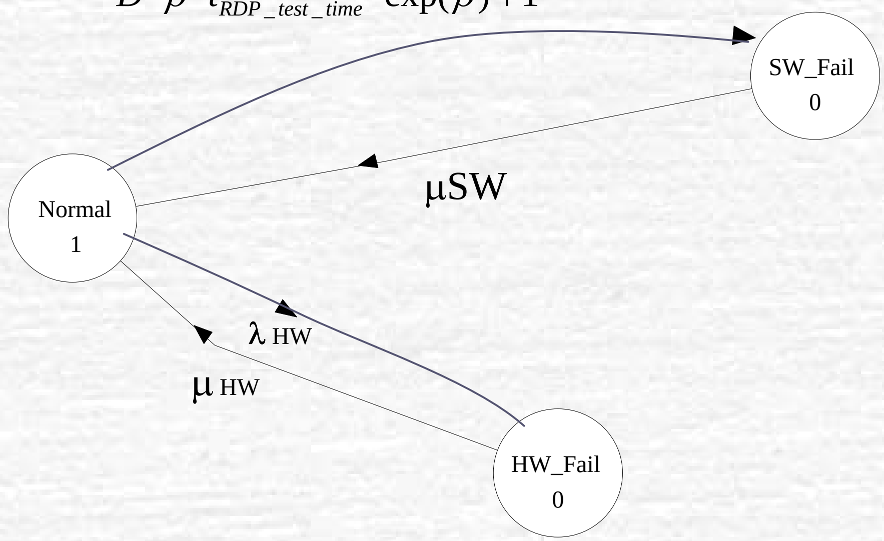
RDP Hardware/Software Top Level Model

Geometric Distribution for application SW failure rate

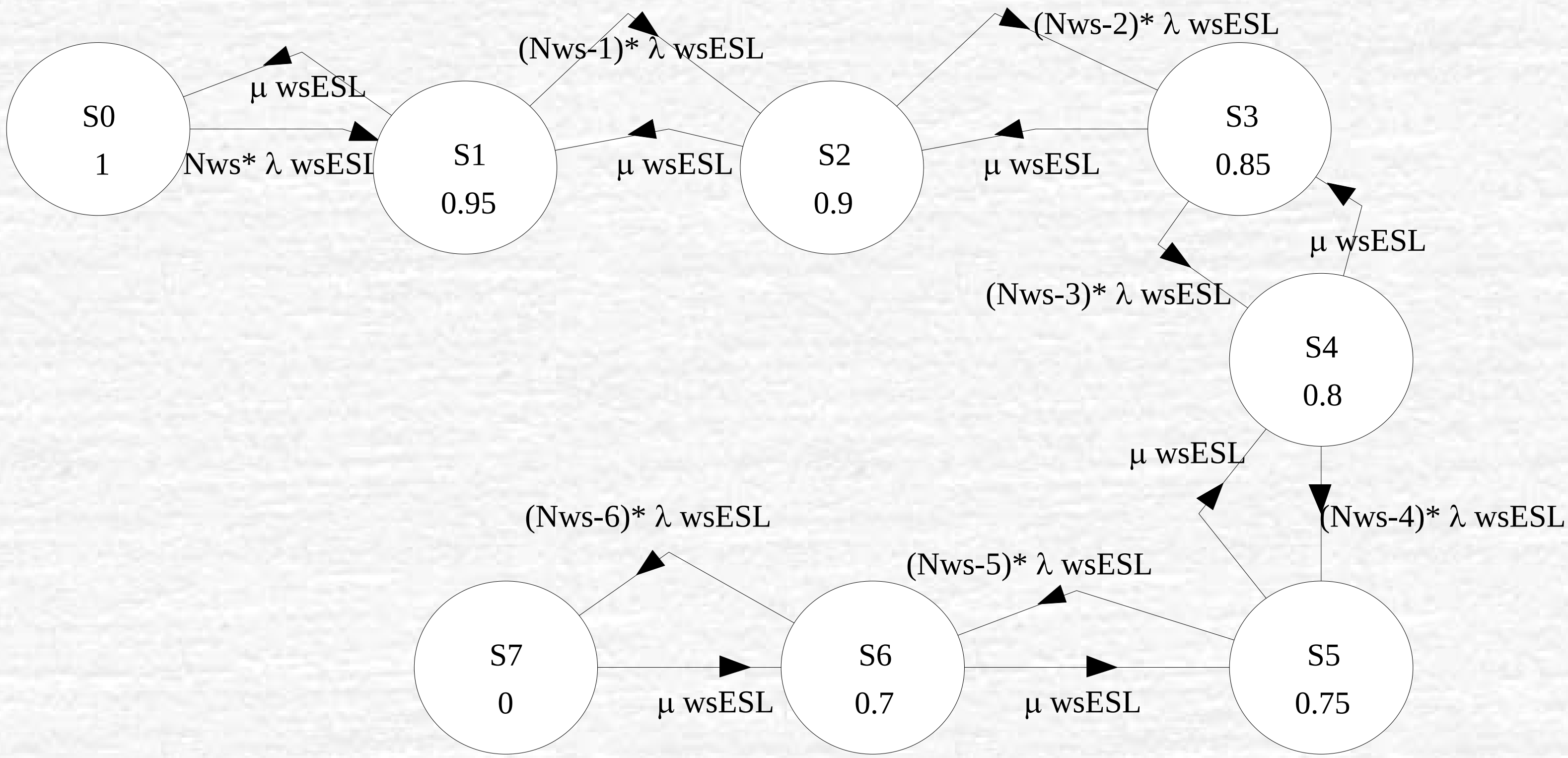
Decreasing failure rate term (as a function of test time) for application

$$\lambda_{OS} + \frac{D \cdot \exp(\beta)}{D \cdot \beta \cdot t_{RDP\_test\_time} \cdot \exp(\beta) + 1}$$

Constant failure rate term for OS

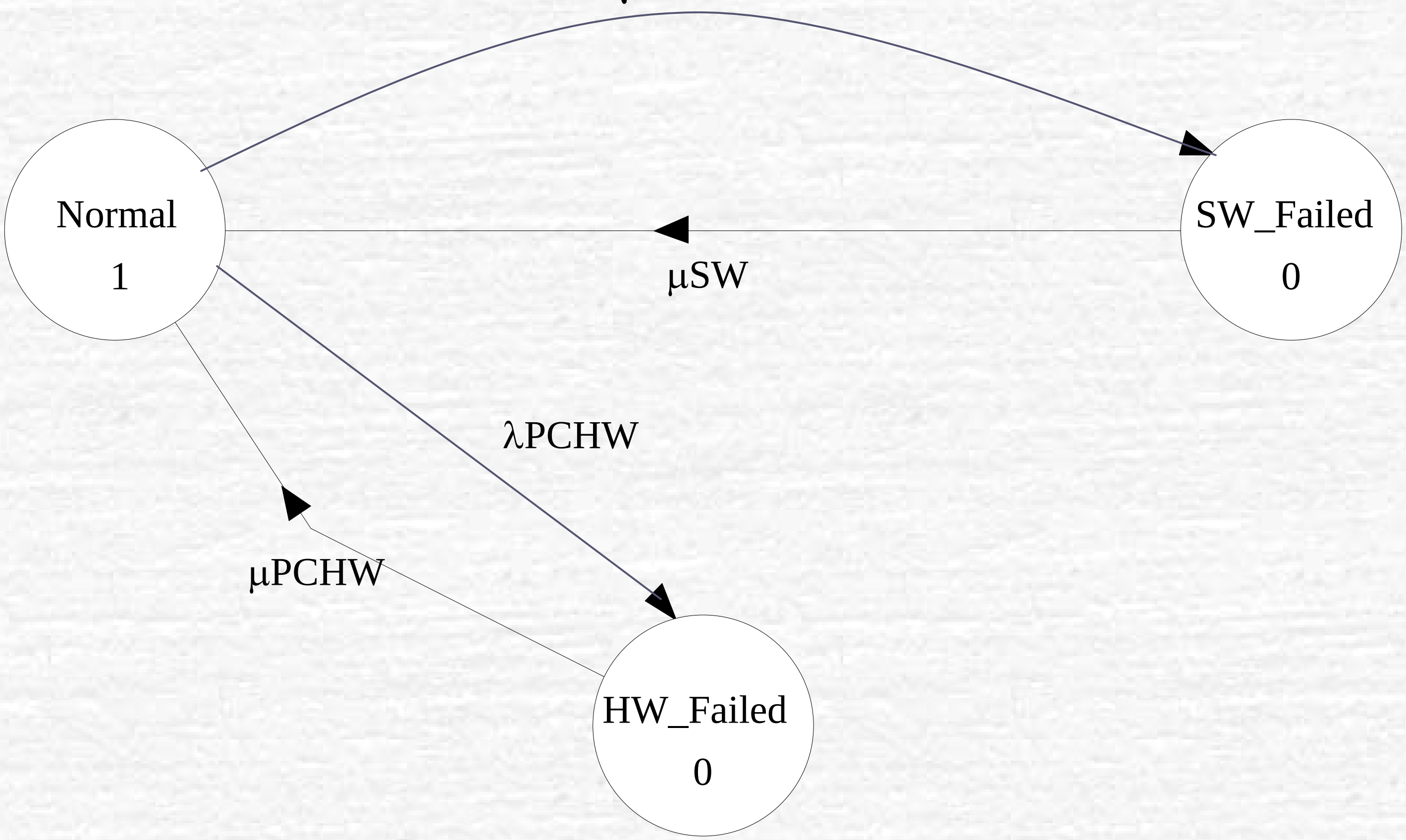


Workstation Network model



Individual Workstation Model

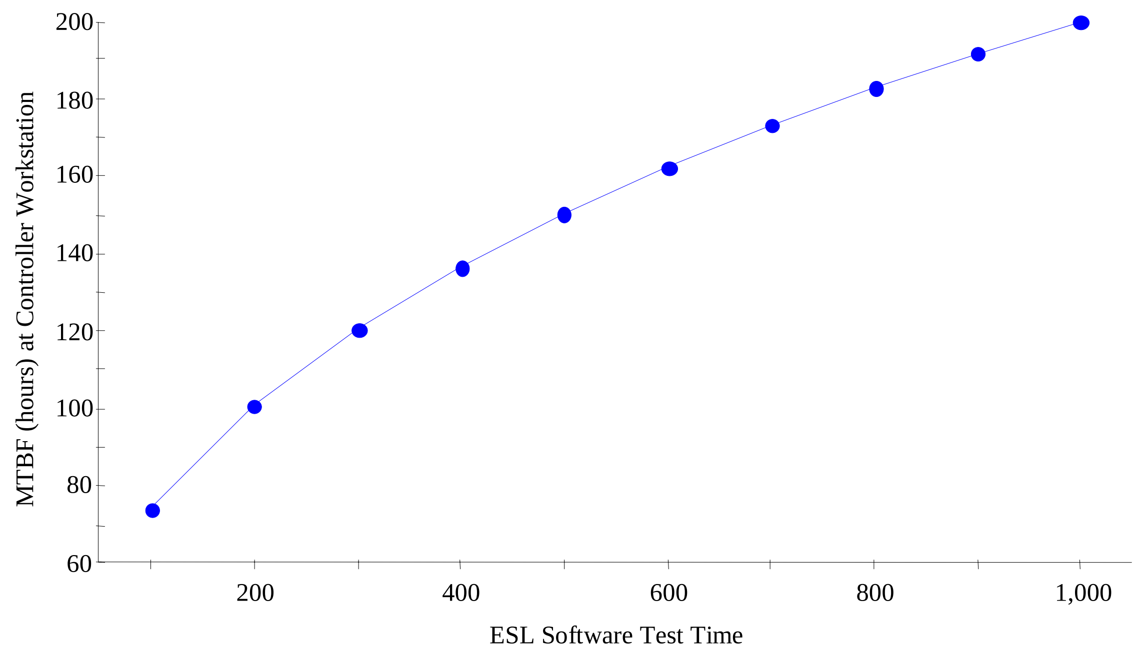
$$\lambda_{OS} + \frac{\alpha - 1}{\sqrt{\beta_o^2 + 2\beta_1 t_{test}(\alpha - 1)}}$$ (Littlewood-Verall)



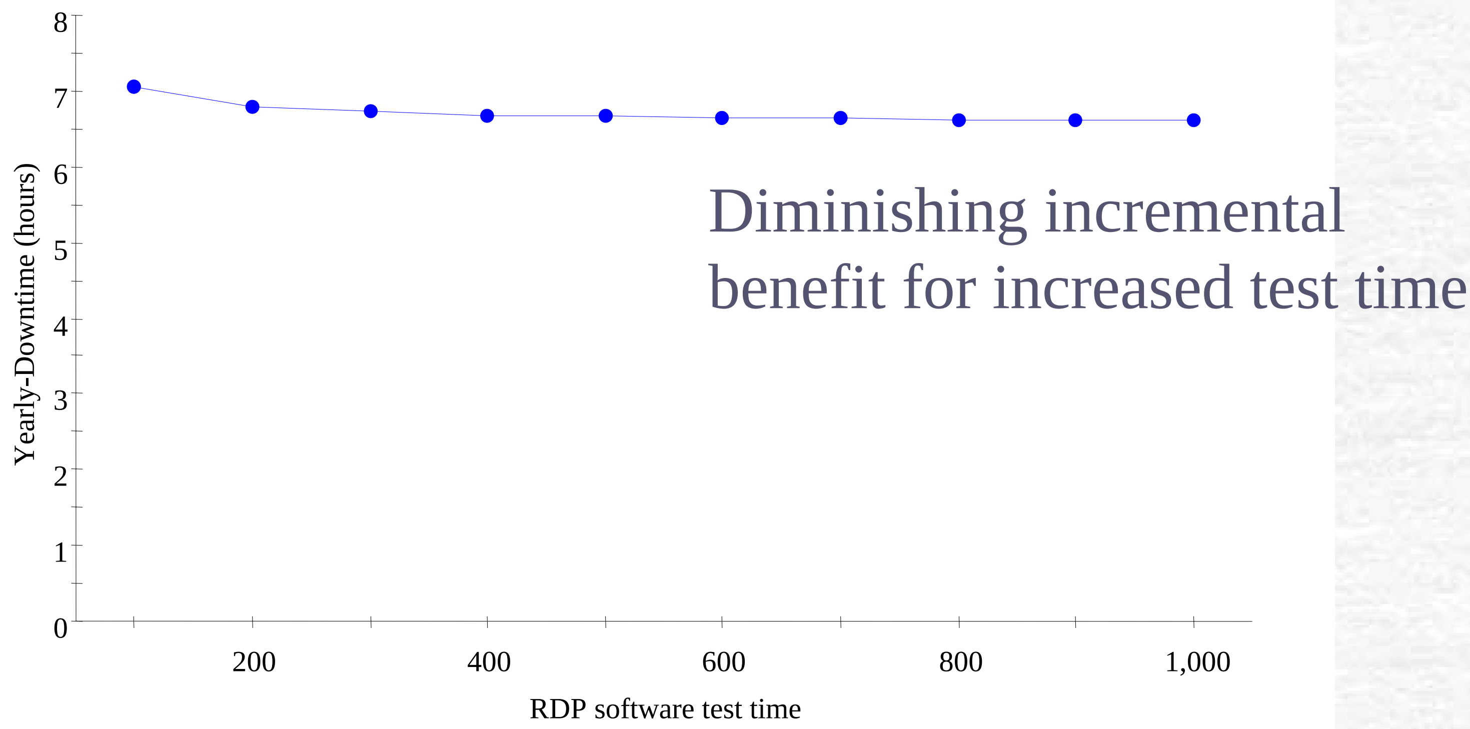
THE AEROSPACE CORPORATION

Workstation Reliability as a Function of Software Test Time

Diminishing incremental benefit for increased test time



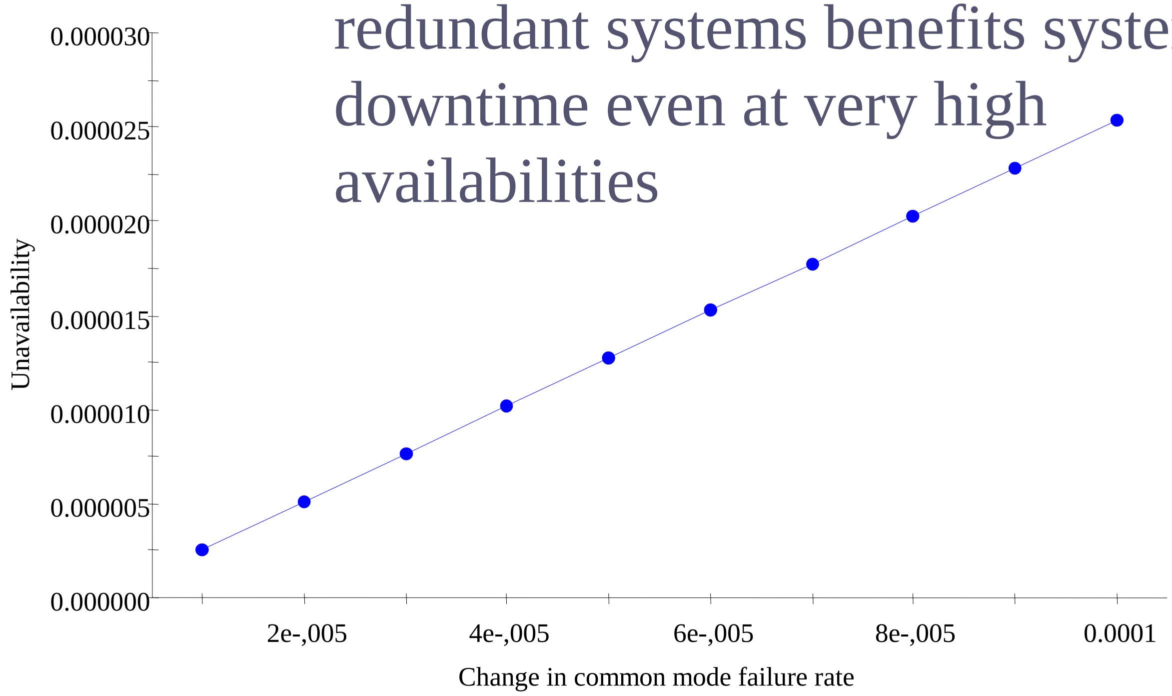
Impact of Software Testing on Downtime of a Single RDP Processor



THE AEROSPACE CORPORATION

Impact of Common Mode Failure Rate

Testing focused on finding common mode failures in redundant systems benefits system downtime even at very high availabilities



THE AEROSPACE CORPORATION

Conclusions

- Satellite Ground Systems are software intensive and have high reliability requirements
- Unavailable and unreliable systems cause space vehicle failures or degraded missions
- Approach described in this presentation is a way of reducing that risk

Additional information

- M. Hecht, “Use of Combined System and Software Reliability Models for Reliability Growth Predictions” *Eighth ISSAT International Conference on Reliability and Quality in Design,* August 7-9, 2002, Anaheim, CA
- http://www.issatconferences.org/order.html

THE AEROSPACE CORPORATION