A Method and Model to Predict Initial Failure Rates

Harry W. Jones, Ph.D., MBA

Overview

- System reliability is often much less than estimated.
  - Failure rates can be ten times higher than anticipated.
- Most forecasts of reliability are bottom-up best case estimates.
  - System failure rates are estimated simply by summing up the component failure rates.
  - Most failures are due to design errors, interface problems, system level effects, misunderstood environment, and human error – not components.
- The fundamental cause of excessively favorable reliability predictions is over-optimism.
  - The cure for over-optimistic estimates is to use historical failure rate data from similar projects.

Over-optimism

- Over-optimism causes too-favorable predictions.
  - Confident engineers assemble estimates bottom-up.
  - They include the known factors.
  - They ignore possible problems, especially mistakes.
- The Nobel laureate, Daniel Kahneman, found that planning estimates are usually over-optimistic.
  - Forecasts are unrealistically close to the best case.
  - They do not reflect experience in similar cases.
- Over-optimism produces two effects:
  - Very favorable estimates
  - Overconfidence that the favorable estimates will be met

Traditional reliability analysis

- Traditional reliability analysis assumes that system failures are due to component failures.
  - Failure rate data is collected in handbooks and reliability block diagrams are used to estimate the overall system failure rate.
  - The system failure rate is assumed to be the sum of the component failure rates.
  - In the mid-1900's, components such as electronic tubes accounted for most failures.
- Now more failures are caused by poor requirements, bad design, manufacturing problems, software, and human error.

Objections to traditional reliability

- Unrealistic assumptions
  - All failures are due to component failures.
  - The failures are independent.
  - Replacing a failed part makes the system good-as-new.
- In reality,
  - Component failures are a small part of all failures.
  - Bad design or manufacturing produces common cause failures.
  - Repairs can be imperfect or cause other failures.

Data on system failure causes

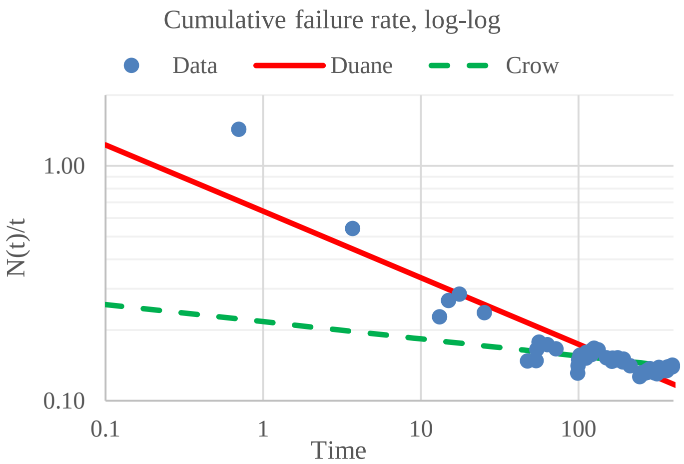
Components (22%)	Failure resulting from a part not performing its intended function.
No defect (20%)	Intermittent failures that cannot be reproduced.
Manufacturing (15%)	Failures resulting from errors in manufacturing.
Induced (12%)	Failures resulting from an externally applied stress such as maintenance.
Design (9%)	Failures resulting from bad design.
Wear out (9%)	Failures resulting from wear out.
Software (9%)	Failure due to a software fault.
System Management (4%)	Failures to interpret system requirements or provide the resources required.

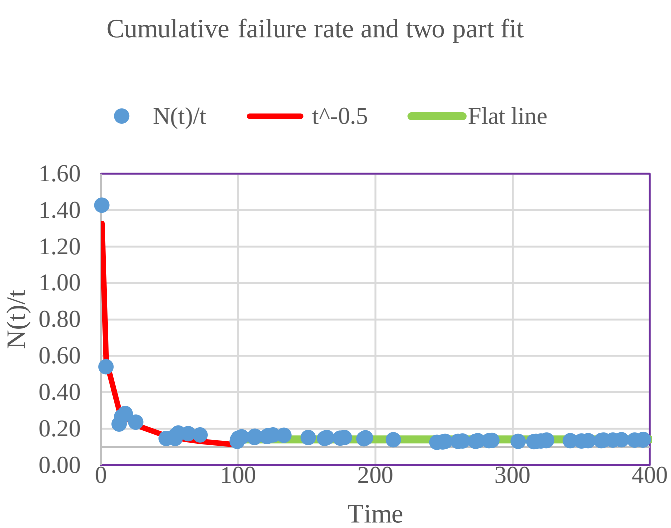
- The table gives failure causes for electronic systems.
  - Only 22% were due to components.
- A study of over 500 systems found that "only 20% of the field problems encountered were hardware reliability problems."
- Another avionics study found failure rates 7 to 20 times higher than predicted.

Curing over-optimism using historical data

- The suggested cure for over-optimism is to base estimates on historical data from similar projects.
  – Failure rates can be 5 to 20 times higher than parts based predictions.
- A rough guess is that the initial system failure rate will be about 10 times the traditional parts-based failure estimate.
- This suggests using two estimates,
  – the bottom-up parts-based estimate, and
  – a system level estimate 10 times larger.

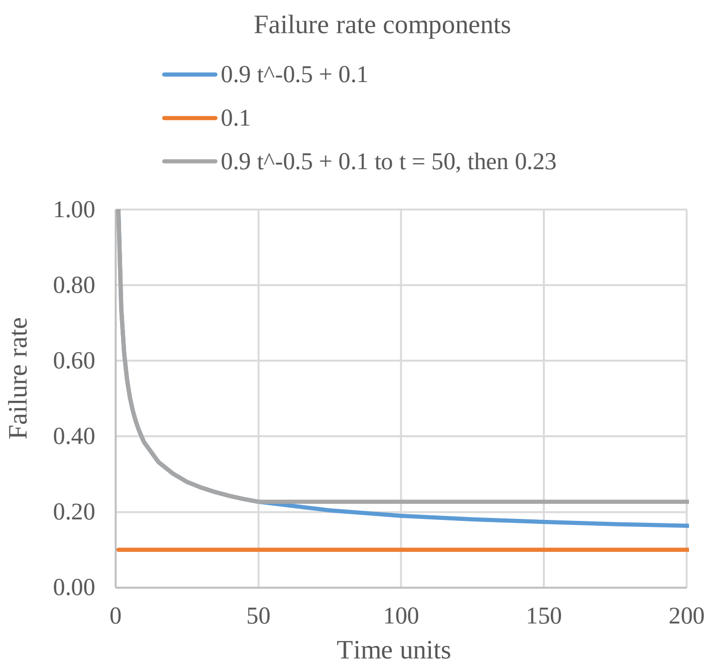
Duane-Crow reliability growth model





- Reliability growth $N(t)/t = k\, t^{-\alpha}$
- Duane used a visual line fit, Crow used model-based computation.
- But failure rate does not really drop to zero.

The abcd model is better



- The abcd model

  Failure rate = $a\ t^{-b} + c$, from $t = 0$ to t_d

  Failure rate = $d + c$, after $t_{d,}$ where $d = a\ t_d^{-b}$

    The failure rate d could be corrected but was not.

- For the Duane-Crow data

  Failure rate = $1.37\ t^{-0.99} + 0.14$ from $t = 0$ to $t_d = 100$

  Failure rate = $0.01 + 0.14 = 0.15$ after $t_d = 100$

Predicting the initial failure rate using the abcd model

- Failure rate = $a\ t^{-b} + c$, from $t = 0$ to t_d
- Failure rate = $d + c$, after t_d
  - Assume that $d = y\ c$
  - $a\ t_d^{\ -b} = d = y\ c$
  - $a = c\ y\ t_d^{\ b}$
- The initial failure rate at $t = 1$ is $c\ y\ t_d^{\ b} + c$
  - The factor $y\ t_d^{\ b}$ can be estimated from data.
  - The larger t_d, the smaller d and y, so the range is reduced.

Initial failure rate prediction for the Duane-Crow data

- The initial failure rate at $t = 1$ is $c\, y\, t_d^{\,b} + c$
  - For the Duane-Crow data set, $b = 0.99$, $c = 0.14$, $t_d = 100$.
  - The initial failure rate at $t = 1$ is $1.37 + 0.14 = 1.51$, approximately equal to the first data point, 1.43.
  - At $t_d = 100$, failure rate $= c + d = 0.01 + 0.14 = 0.15$.
- The reliability growth parameter b is typically 0.2 to 0.8.
- The long term constant failure rate c can be estimated as equal to the total component based failure rate.
- The scale factor that multiplies c is $y\, t_d^{\,b}$, and here is equal to $137/0.14 = 9.8$.
  - Comparisons to data indicate that this is a typical value.

Is10 times the base rate reasonable?

- This assumes the parts-based failure estimate is correlated with the system level failure rate.
  - Both rates increase as parts count and system complexity increase.
  - The parts-based failure rate is a lower bound on the system failure rate.
- But the system level failure causes include design, manufacturing, environment, operational, and management problems.
  - These seem difficult to tie to parts count or to predict.
- Can we do better?
  - Prediction using reliability growth models?
  - Engineering judgment?

The initial failure rate is unpredictable

- Reliability growth models assume that:
  - Infant mortality failures occur due to design and other errors.
  - In early testing, these failures are found and fixed, reducing the failure rate.
- The time of the first failure determines the initial system failure rate.
  - If there are several infant mortality failure modes, the time when the first one occurs is a random event.
- The initial failure rate is very variable, even with this simple model.

Engineering judgment is untrustworthy

- A space shuttle risk analysis found the solid-fuel rocket boosters had a failure rate of about 1 in 40.
  - But NASA made an “engineering judgment” and assumed a failure probability of 1 in 1,000 or 10,000.
- An Air Force review noted that this had no justification and suggested a failure rate of around 1 in 100.
  - NASA’s internal analysis assigned a failure in the solid rocket booster a probability of 1 in 100,000.
- After the Challenger accident, analysis found that the probability of a fatal accident was about 1 in 100.
  - Even after Challenger, the NASA chief engineer thought the actual risk would be 1 in 100,000, “based on engineering judgment.”

Conclusion

- Failure rate estimates based only on adding component failure rates are usually too low.
  - Such over-optimistic estimates can cause insufficient attention to improving reliability.
- Making a rough adjustment, multiplying the parts-based failure rate estimates by 10 based on historical experience, is more likely to be accurate.
  - More realistic failure rate estimates can lead to better reliability specifications, plans, design, and testing, and ultimately to better reliability.