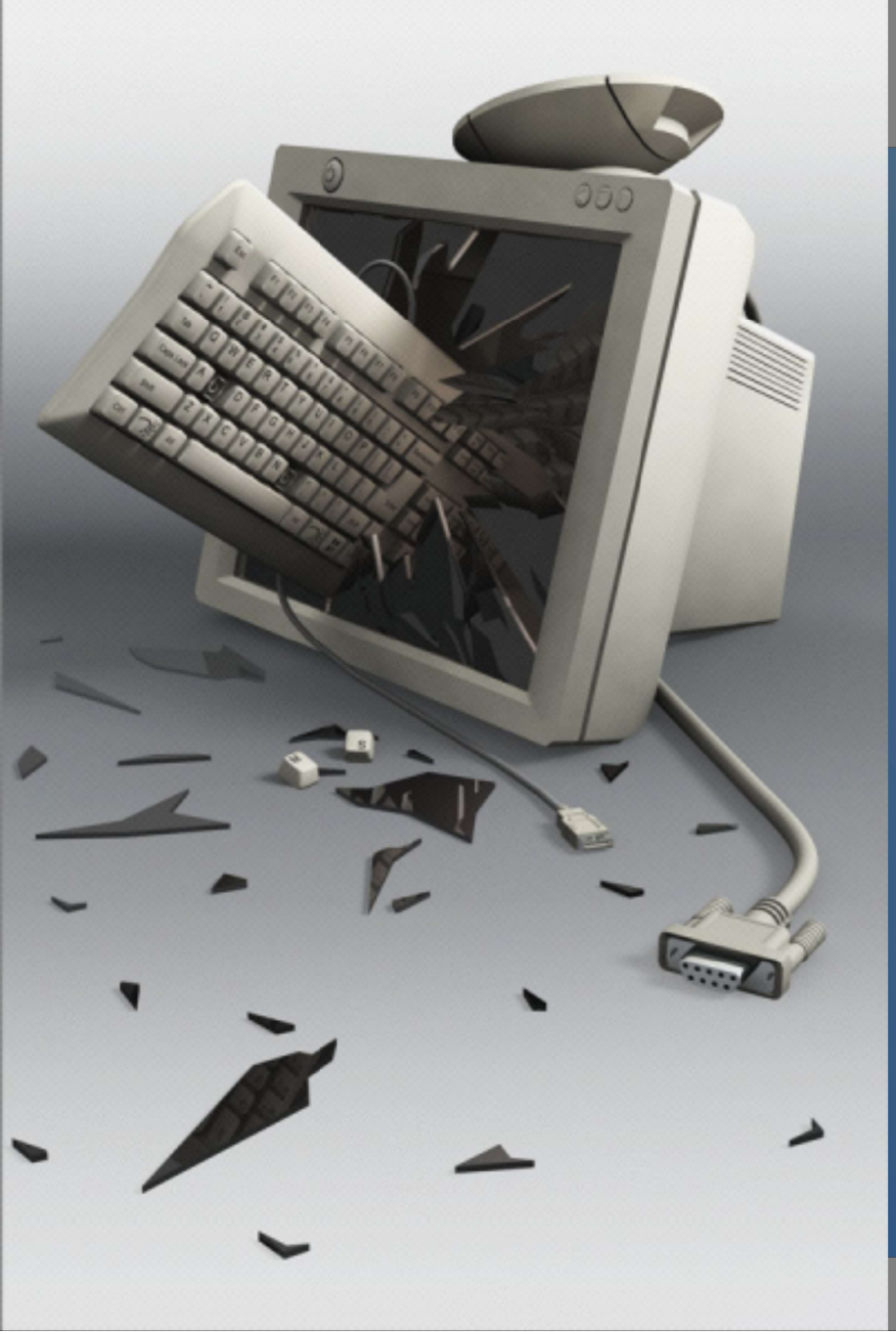


FMEA

What could possibly go

w

r

o

n

g

?

What could possibly go wrong?

- Developers often focus on new features, not full system in use.
  - Ex: Students write project that has no way to add user to user database.
    “Hey, I've got SQL terminal to created *my* user...”
- We need to know..
  - Shows us how the system is likely to fail in the field!
  - Eye-opening!

Example: Submarine

- Arctic exploration via autonomous submarine
  - Imagine assignment 3 (beat box) transformed into a sonar system
  - Sonar emits a ping sound and receives an echo off objects in the water.
  - Allows submarine to map obstacles.
- Mapping As3 Features --> Submarine Features
  - Play sound -->..
  - Accelerometer -->.. (vibrations)
  - Webpage: --> User-interface
  - Two boards networked to do left & right sonar

FMEA

- FMEA:..
- Brainstorm
  - How can components of a system fail
- Rate
  - What will the effects of these failures be?
  - How likely is the failure?
  - Can we detect the failure?
- Compute
  - What is the risk for this possible failure?

FMEA Process

1) Imagine how some component could fail
2) List effects of failure
   - Rate .. (1-10)
3) Think what could cause this failure
   - Rate.. (1-10)
4) State how this failure is currently detected
   - Rate .. (1-10)
5) Compute Risk Priority Number [RPN]:
   multiply above three scores (1-1000)
6) List possible actions to reduce this risk

Ratings

AIAG Compelled Rating			
Rating	Severity of Effect	Likelihood of Occurrence	Ability to Detect
10	Hazardous without Warning	Very high; Failure is almost inevitable	Can not detect
9	Hazardous with Warning	Very high; Failure is almost inevitable	Very remote chances of detection
8	Lose of primary function	High; Repeated failures	Remote chances of detection
7	Reduced primary function performance	High; Repeated failures	Very low chances of detection
6	Lose of secondary function	Moderate; Occasional failures	Low chances of detection
5	Reduced secondary function performance	Moderate; Occasional failures	Moderate chances of detection
4	Minor defect noticed by most customers	Moderate; Occasional failures	Moderate high chances of detection
3	Minor defect noticed by some customers	Low; Relatively low failures	High chances of detection
2	Minor defect noticed by discriminating customers	Low; Relatively low failures	Very high chances of detection
1	No effect unlikely	Remote; Failure is unlikely	Almost certain

http://lh3.ggpht.com/_EhOQGW2GHBg/SxPl_hyZP6I/AAAAAAAAHzs/MOYLGt7YJPk/AIAG-Rating-Severity-Occurance-Detection%5B2%5D.jpg?imgmax=800

Submarine Failure Mode Example

- Complete this failure mode
  - Component: Audio output (‘ping’)
  - Failure mode: Speaker unplugged
  - Failure effect: _____
    Severity #: _____
  - Potential cause: _____
  - Occurrence #: _____
  - How to detect failure: _____
    Detection #: _____
  - RPN (Risk): _____
  - Actions: _____

Ex: Some failures to consider

- Complete an FMEA for the following failure modes
  - Audio output: unplugged
  - Accelerometer: stops registering movement
  - Accelerometer: fried (not responding to software)
  - CPU: system load too high
  - Application: audio buffer underflow
  - Application: ping-queing thread locks-up
  - Application: crash (ex: via null pointer exception)
  - Web server crash

FMEA Example Sheet

FMEA

Component	Failure Mode	Failure Effect	Sev	Potential Causes	Occ	How to detection failure?	Det	Risk	Actions Recommended
Status LED	Burnt out								
Audio Output	Unplugged								
Accelerometer	Stops registering movement								
	Fried								
CPU	System load too high								
App	Audio buffer underflow								
	ping-queueing thread locked								
	Crash								
Web server	Crash								

Reliability

- We always try to design reliable system
- It would be valuable to be able to quantify this

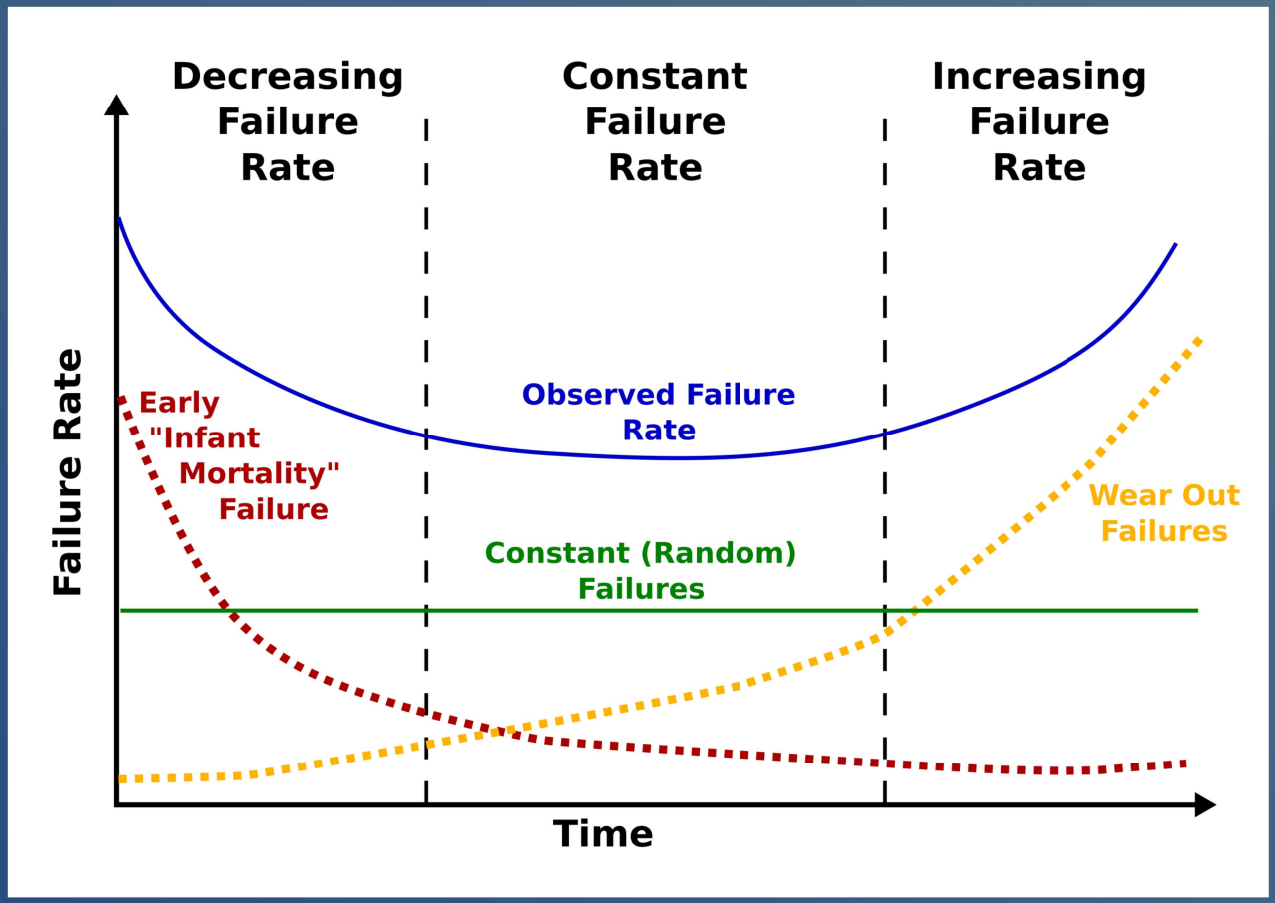
MTBF

- MTBF
  - Mean Time Between Failures
  - For example if we had 3 sets of identical equipment fail after 400, 500 and 800 hours, the MTBF would be 566 hours.
- For use in calculations we assume failure is equally likely at any time/

Failure Rate

- FIT
  - Failures In Time
  - Number of expected failure in 1,000,000,000 hours
  - This measurement is more common in semiconductor industry

Bathtub Curve

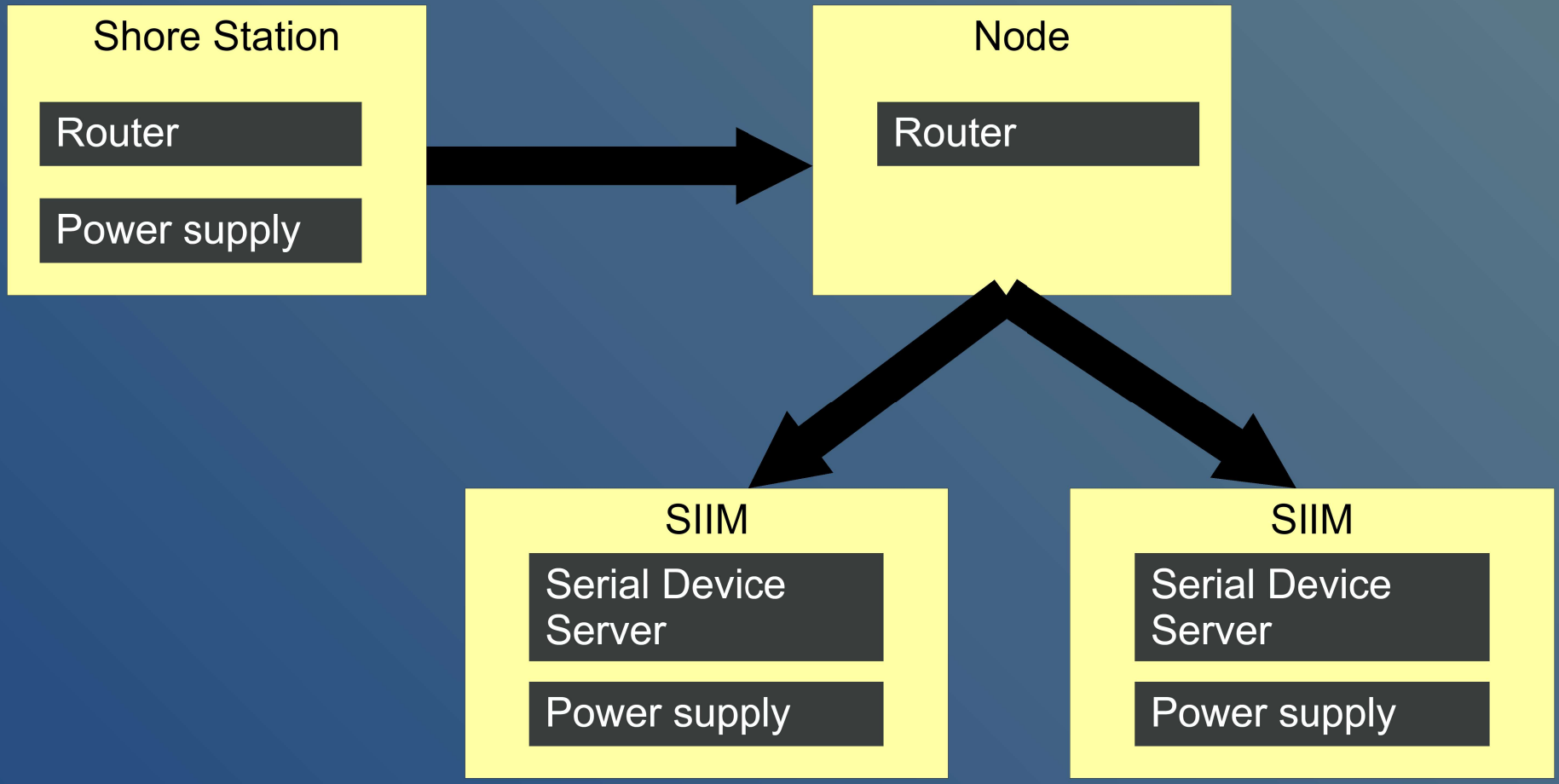


- Image from Wikipedia

MTBF Example

- VENUS (Victoria Experimental Network Under the Sea)
- Not the actual equipment used and over simplified.
- We will use this to do a basic calculation

VENUS Architecture



MTBF Calcutation

- See Spreadsheet and Data Sheets

Summary

- FMEAs help a team improve product quality
  - identify possible failures by assuming the part failed, and then consider its effect.
- Rating each failure's:
  - severity, likelihood, and detectability
- gives quantitative data to prioritize enhancements
- Reliability Calculations:
  - Mean Time Between Failure
  - Failure In Time