Principles, rules, hints and art of computer system design

Lin Zhong
Guiding principles
Acknowledgment of human limitation
Keep It Simple

• *When in doubt, use brute force*
  • time favors brute force

• *When in doubt, leave it out*
  • adding a feature increases development effort disproportionately

• *Avoid excessive generality*
  • If it’s good for everything, it’s good for nothing
Make it available

Open design principle
Let anyone comment on the design;
You need all the help you can get

Principles of Computer System Design by Salzter & Kaashoek
Linus’s Law

• “Given enough eyeballs, all bugs are shallow”
  —Linus Torvalds
How to structure your system
End to end principle

- “functions placed at low levels of a system may be redundant or of little value when compared with the cost of providing them at that low level”

- functions: security, reliability, safety,…

End-to End Arguments in System Design by Saltzer, Reed and Clark, 1984
Separation of mechanism and policy

- Mechanism: access control & allocation of resources
- Policy: who has access and get what resources
Why separation?

- Policy changes faster
- Policy and mechanism require different privilege
- Policy and mechanism may come from different sources.
Separation of concerns
Separate interface from implementation

• Keep interface constant
Rule of Modularity

- Write simple parts connected by clean interfaces
Robustness principle

- Be tolerant of inputs, strict on outputs
The CMOS Inverter: A First Glance

V_{DD}

V_{in}

V_{out}

C_L

V_{out}

V_{in}

1 2 3 4 5

NMOS off
PMOS lin

NMOS sat
PMOS lin

NMOS lin
PMOS sat

NMOS lin
PMOS off

NMOS sat
PMOS sat
The regenerative property of CMOS gates
The regenerative property of CMOS gates

(a) A chain of inverters.

(b) Regenerative gate
The regenerative property of CMOS gates

(a) A chain of inverters.

(b) Regenerative gate

(c) Non-regenerative gate
Decouple modules with indirection

- Indirection supports replaceability
Decouple modules with indirection

• “All problems in computer science can be solved by another level of indirection”
  
  • David Wheeler
  
  • known as *Fundamental theorem of software engineering*

• “except for the problem of too many layers of indirection”
  
  • Kevin Henney’s Corollary

*Principles of Computer System Design* by Salzter & Kaashoek
Rule of Representation

• Fold knowledge into the data so that program logic can be stupid and robust

• “Data is more tractable than program logic. It follows that where you see a choice between complexity in data structures and complexity in code, choose the former. More: in evolving a design, you should actively seek ways to shift complexity from code to data.”
Booting Linux

• The old way (still the way on your PC): the kernel has the knowledge of the hardware

• The new way: the hardware knowledge is in the device tree (DTB). A generic kernel consults it
Checklist

CESSNA 172S EMERGENCY PROCEDURES CHECKLISTS

EMERGENCY FREQUENCY .................. 121.50

Airspeeds
- Engine Failure after takeoff ... 70 KIAS
- Maximum Glide ... 88 KIAS
- Landing without engine power ... Flaps up - 70 KIAS
- Flaps down - 65 KIAS

Engine Failure After Takeoff
- Airspeed ... 70 KIAS (Flaps Up)
- Mixture ... LEAN CUTOFF (PULL OUT)
- Fuel Shutoff Valve ... OFF (PULL OUT)
- Ignition Switch ... OFF
- Cabin Door ... UNLATCHED
- Land ... STRAIGHT AHEAD

Engine Failure During Flight
- Airspeed ... 88 KIAS
- Fuel Shutoff Valve ... ON (IN)
- Auxiliary Fuel Pump ... ON
- Mixture ... RICH
- Ignition Switch ... BOTH

Emergency Landing Without Power
- Airspeed ... 70 KIAS
- Mixture ... LEAN CUTOFF
- Fuel Shutoff Valve ... OFF
- Ignition Switch ... OFF
- Seat Belts ... SECURE
- Doors ... UNLATCHED
- Touchdown ... LIGHTLY TAIL LOW
- Brakes ... APPELY HEAVILY

Telephone Numbers:
- Colorado Flight Center ... 970-245-8444
- Collin Fay ... 970-260-6547
- Bradley Sullivan ... 970-210-5527
- Flight Service ... 800-992-7433
- KJGT ATIS ... 970-245-7851
- KJGT Tower ... 970-257-9175

Emergency Squawk Code ............ 7700

Alternator Failure
- Alternator Master Switch ... OFF
- Alternator Circuit Breaker (ALT FLD) ... RESET (IN)
- Master Switch ... CYCLE OFF, then ON
- Low Voltage Light ... CHECK OFF
- Avionics Master Switch ... CYCLE OFF
- If Low Voltage Light Remains ON, Alternator ... OFF
-Nonessential Electrical Equipment ... OFF
- Land As Soon As Practical

Fire During Start On The Ground
- Starter ... CONTINUE CRANKING
- Engine fails to start, throttle ... FULL OPEN
- Mixture ... LEAN CUTOFF
- Master Switch ... OFF
- Ignition Switch ... OFF
- Fuel Shutoff Valve ... OFF (PULL OUT)
- Auxiliary Fuel Pump ... OFF

Engine Fire In Flight
- Mixture ... LEAN CUTOFF (PULL OUT)
- Fuel Shutoff Valve ... OFF (PULL OUT)
- Auxiliary Fuel Pump ... OFF
- Master Switch ... OFF
- Cabin Heat and Air Vents ... OFF / CLOSED
- Altimeter ... PITCH FOR 100 KIAS (base line climb)
- Forward Landing ... EXECUTE

Electrical Fire During Flight
- Master Switch ... OFF
- Cabin Heat and Air Vents ... OFF / CLOSED
- Fire Extinguisher ... ACTIVATE

Communications Failure
- Frequency ... CHECK
- Volume and Squawk ... CHECK
- Speaker ... SELECT
- Headset Jacks ... RESET
- Hand Mic ... CHECK
- Circuit Breakers ... CHECK
- Other Radios or Cell Phone ... USE IF AVAILABLE
- VOR Frequency ... MONITOR
- Squawk ... 7000
- Tower Light Signals ... OBSERVE / COMPLY

REFER TO THE PILOT'S OPERATING HANDBOOK FOR COMPLETE EMERGENCY CHECKLISTS!

If you have an emergency or are otherwise unable to return when expected, please call us toll-free at 1-866-897-7910 to advise us of your new ETA. You may also reach Collin Fay at (970) 260-6547 or Bradley Sullivan at (970) 210-5527.
THE NEW YORK TIMES BESTSELLER

THE CHECKLIST MANIFESTO

HOW TO GET THINGS RIGHT

PICADOR

ATUL GAWANDE

BESTSELLING AUTHOR OF BETTER AND COMPLICATIONS
About the development process
Rule of Optimization

• Prototype before polishing. Get it working before you optimize it.
Law of diminishing returns

• The more one improves some measure of goodness, the more effort the next improvement will require
Law of diminishing returns

Goodness

Effort
Law of diminishing returns

It matters where you are on the curve?
Design for interaction

• You won’t get it right the first time, so make it easy to change

Principles of Computer System Design by Salzter & Kaashoek
Rule of Extensibility

- Design for the future, because it will be here sooner than you think
Rule of Generation

• Avoid hand-hacking; write programs to write programs when you can