Prof. Philip Koopman

Carnegie Mellon University

Electrical & Computer ENGINEERING

Lifecycle & Configuration Management

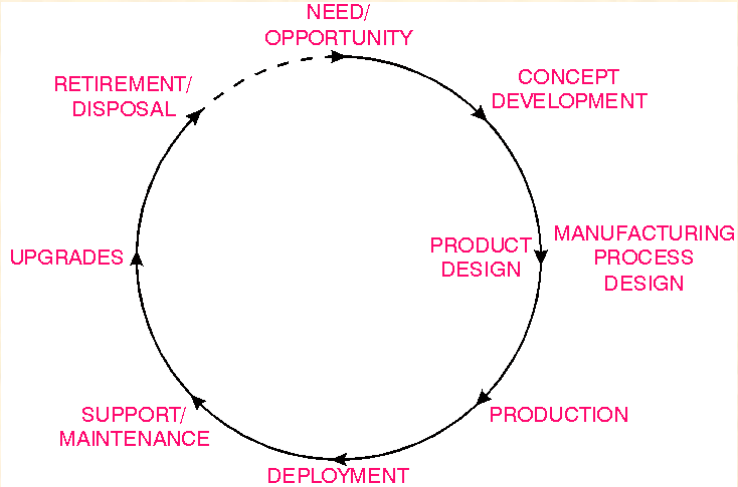
"Good judgment comes from experience,
and experience comes from bad judgment."

– Frederick P. Brooks

Lifecycle Issues

Carnegie Mellon University

- Anti-Patterns:
  - No version control
  - No configuration management
  - Incremental features without baseline



- Lifecycle issues
  - Version control: keeping different versions straight
  - Configuration management: what's in the deployed system
  - Lifecycle: old embedded systems (almost) never die
    - Spare parts for obsolete systems
    - Mid-life upgrades

INSTALLATION ERROR —

Airbus confirms software configuration error caused plane crash

Airbus A400M flight recorder data confirms "quality issue" in setup caused failure.

SEAN GALLAGHER - 6/1/2015, 12:38 PM

A protoype of the Airbus A400M at the 2010 Farnborough Airshow.

https://www.youtube.com/watch?v=TUiX6m6WLdY&ab_channel=Sciences

The Register 6/10/15:

"Torque calibration parameters were wiped"…
"Pilots only get warning above 120 meters off the ground"

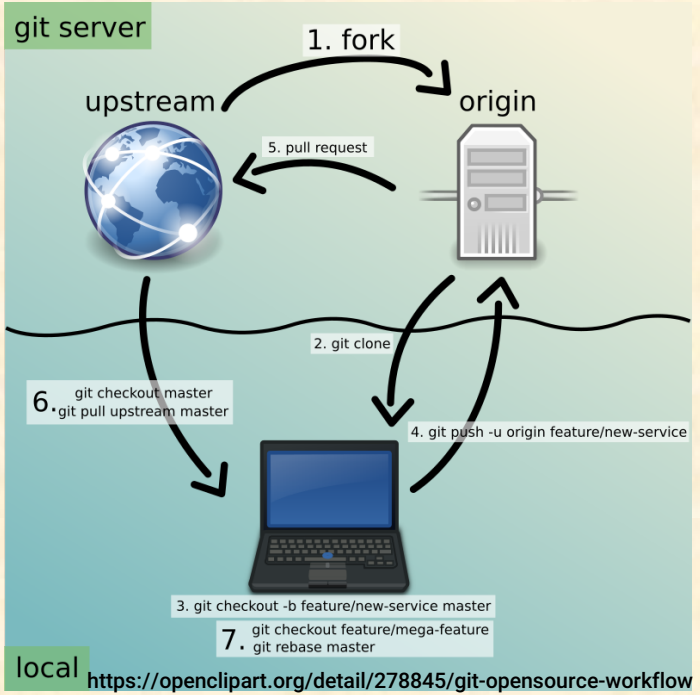
As Ars reported on May 19, Airbus had issued a warning to its military customers about a potential software problem in the engine control software for the A400M. The release of the exact cause of the crash, however, had been delayed because a Spanish magistrate placed the flight data recorders from the aircraft under seal. Airbus has since been able to obtain the flight data, which Lahoud said confirms that the engine control software had been improperly configured during the installation of the engines on the ill-fated aircraft.

http://arstechnica.com/information-technology/2015/06/airbus-confirms-software-configuration-error-caused-plane-crash/

Version Control

Carnegie Mellon University

- Stores & navigates snapshots of versions
  - Ability to roll-back to previous version
  - Synchronizes compatible versions
    - Development vs. release versions
    - “Branch” and “merge” parallel efforts
  - Given a version number, give me the software
- Many popular tools – use one!
  - Watch out for binary file management
  - Multi-site can require special care
- Beyond the obvious…
  - Also version: design documents, requirements, tests, tool chain
  - Need process for who/what/when to update version
  - Needs to tie into disaster recovery (have you tested it?)



https://openclipart.org/detail/278845/git-opensource-workflow

Configuration Management

Carnegie Mellon University

- CM is identifying a particular version
  - Which version has which bug fixes?
  - Which version has which features?
  - Which version should be the next release?
  - Which version is in a failed product?
- Beyond the obvious…
  - Snapshot every build and record its manifest
  - Make sure returned units can self-report version
    - Which library version, which driver version, etc.
    - Need SW version, HW version, config data version (if applicable)
    - Attempts to track this in a central database never work 100%
  - Need to know which SW is compatible with which HW
    - Need to be able to re-create a build, which might require obsolete tools
  - Feature activation: which features have been licensed by user?

Airbus A-380 bolt with part tracking information. (Size: 2 cm x 1 cm)

Gas Pump Startup Printout Example


```
CLAMSHELL PRINTER BOARD
-----------------------

 ** CONFIGURATION **

- Revision :          V0507
- CHKS/CRC :(C2B1)  5517h
- S/N :          yy/ww-ssss
- Pre Heating  :        on
- Paper Temp.  :      high
- Auto Advance :        on
- Watchdog     :        on
- Opto Jam  s/h:     CC/99
- Opto Pass s/h:     28/0A

 ** SERIAL INTERFACE **

- Parameters   :     n,8,1
- Flow Control : Dtr/Dsr
- Baud Rate    :     38400
- Level I/O    :       TTL


 !"#$%&'()*+,-./01234567
89:;<=>?@ABCDEFGHIJKLMNO
PQRSTUVWXYZ[\]^_'abcdefg
hijklmnopqrstuvwxyz{|}~
```

Embedded Systems Live (almost) Forever

Carnegie Mellon University

- 10-50 year lifecycles are common
  - Example: SAGE air defense system
    - Started 1954; deployed 1963
    - Vacuum tubes; 500,000 lines of code
    - In operation until 1983
  - 1AESS telephone switch: 1976 through 2008+
  - Aircraft can operate for 25-30 years
  - Cars routinely operate for 15+ years
- Challenges
  - Disaster recovery (includes vendor bankruptcy)
  - End-of-life for hardware & software
  - Adding new services to existing platform
  - Security problems if not updated

Britain's Doomsday Nuke Subs Still Run Windows XP

The fate of the country's nukes is in the hands of an obsolete operating system.

By Kyle Mizokami Jan 21, 2016

https://www.popularmechanics.com/military/weapons/a19061/britains-doomsday-subs-run-windows-xp/

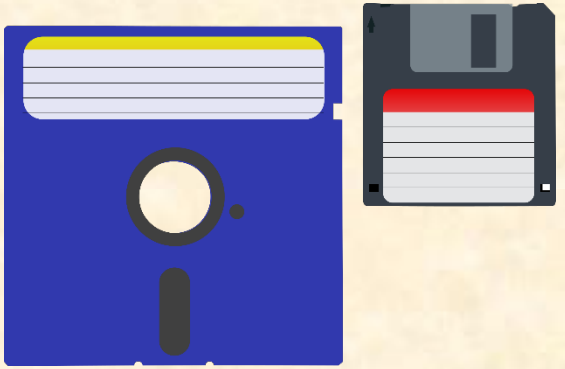
Posted on April 26, 2018 at 12:59 PM

WINDOWS 95 POWERED MEDICAL EQUIPMENT ARE BEING HIT BY HACKERS

https://koddos.net/blog/windows-95-powered-medical-equipment-are-being-hit-by-hackers/

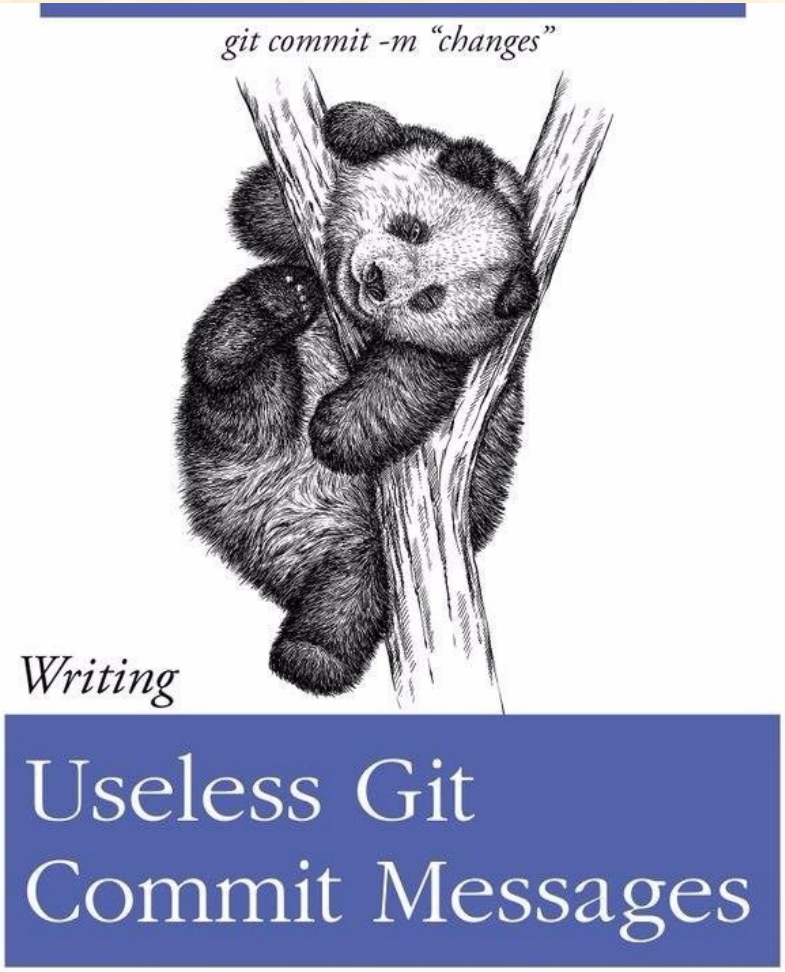
Best Practices for Lifecycle Management

Carnegie Mellon University



- Take CM & Versioning seriously – they are different
  - Use a formal Build Process to release
    - Check that all versions in build are correct; record manifest
  - Plan for 2x the lifecycle you think will happen
    - And have a plan for product end of life

- Lifecycle pitfalls
  - Releasing the wrong version
    - Development version, debug version (e.g., watchdog turned off), etc.
  - Cutting corners on software configuration management
    - What if you can't reconstruct software involved in a field failure?
  - Getting caught without replacement parts
    - Pay attention to end-of-life buys
    - Anticipate obsolete: hardware, media, tools, libraries, …

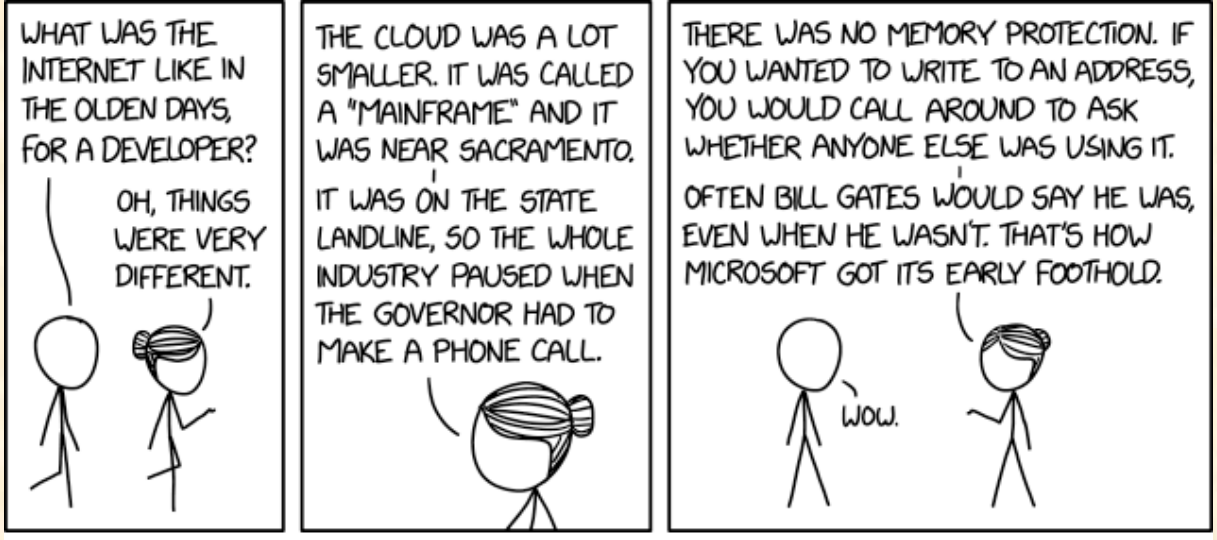


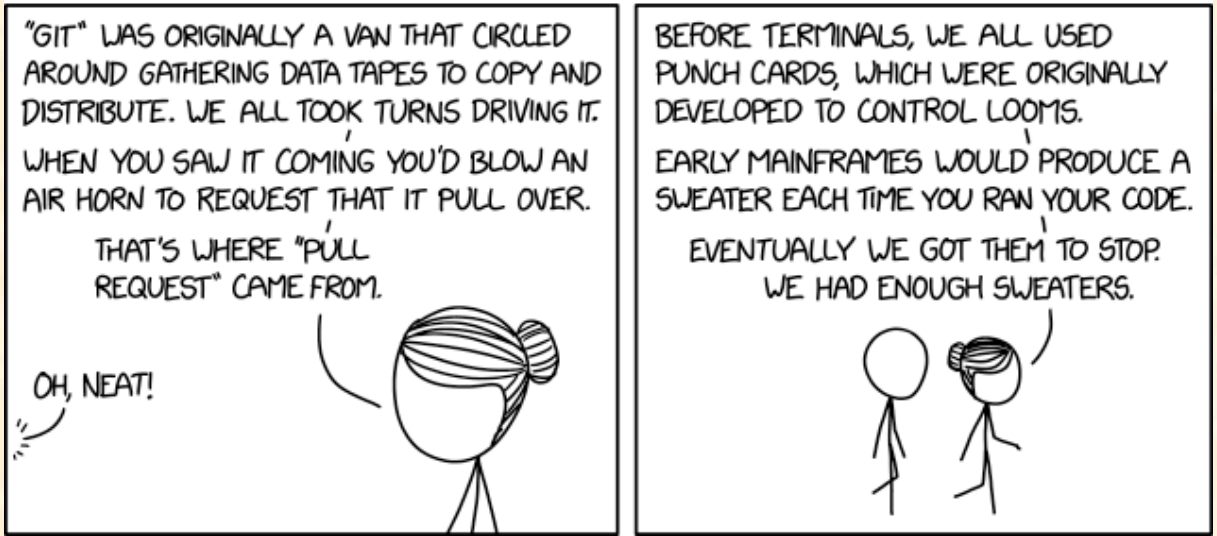
https://goo.gl/pvDMHX CC BY-NC 2.0

COMMENT	DATE
CREATED MAIN LOOP & TIMING CONTROL	14 HOURS AGO
ENABLED CONFIG FILE PARSING	9 HOURS AGO
MISC BUGFIXES	5 HOURS AGO
CODE ADDITIONS/EDITS	4 HOURS AGO
MORE CODE	4 HOURS AGO
HERE HAVE CODE	4 HOURS AGO
AAAAAAAA	3 HOURS AGO
ADKFJSLKDFJSDKLFJ	3 HOURS AGO
MY HANDS ARE TYPING WORDS	2 HOURS AGO
HAAAAAAAAANDS	2 HOURS AGO

AS A PROJECT DRAGS ON, MY GIT COMMIT MESSAGES GET LESS AND LESS INFORMATIVE.

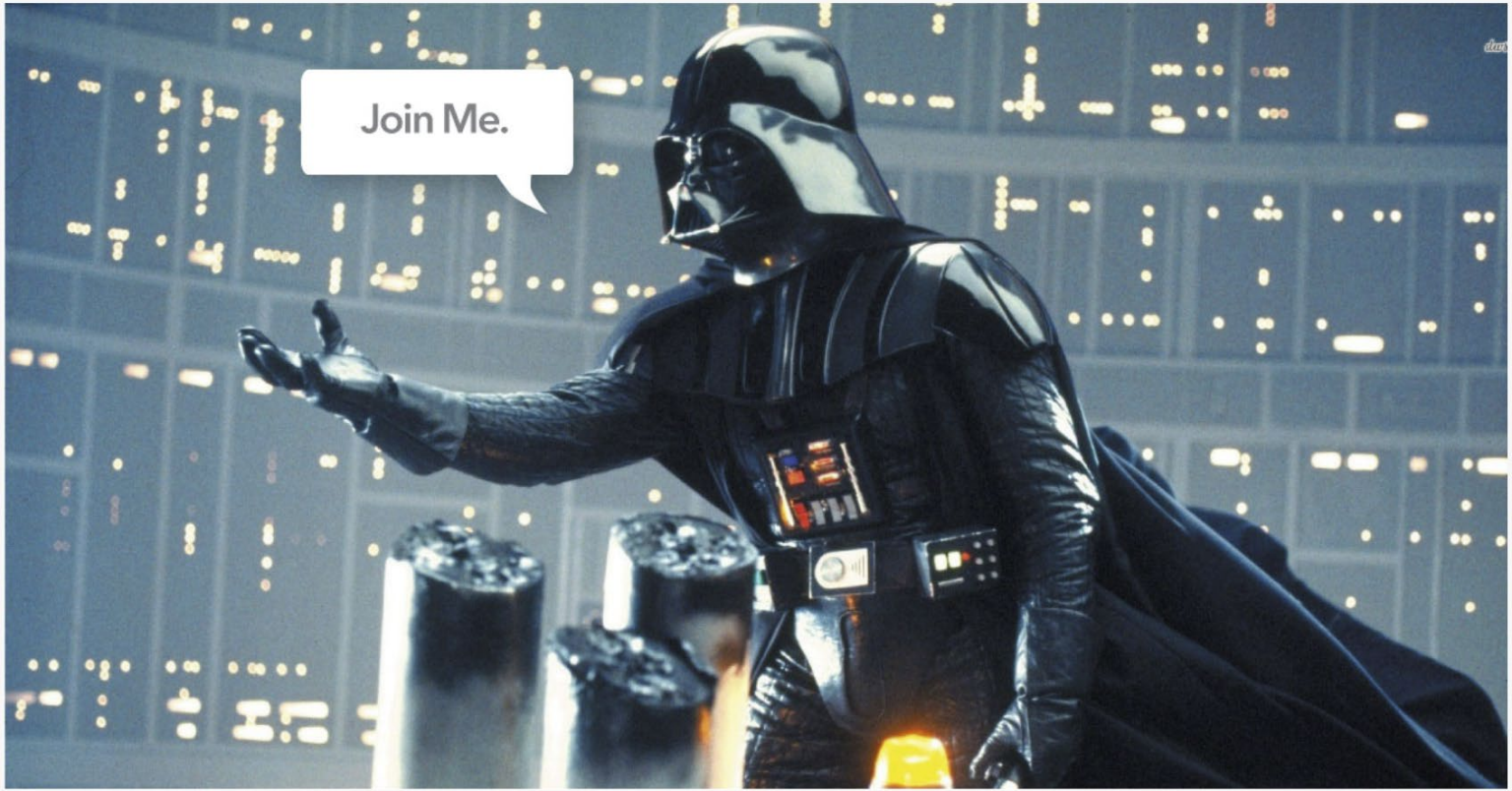
https://xkcd.com/1296/





https://m.xkcd.com/2324/

“Poorly documented legacy code leads to anger. Anger leads to hate. Hate leads to spaghetti code.”



Darth Vader is a trademark of Disney, not SciTools.

https://scitools.com/legacy-code-your-journey-to-the-dark-side/

