Throwing Cinderblocks at Safety Engineering

Chuck Wolber
Associate Technical Fellow
The Boeing Company

Preliminaries

Preliminaries

- Thanks!
- How should we sell safety to the OSS community?

- Safety is a diverse form of scrutiny.
- Safety drives thoughtful design.
- Safety drives testing.

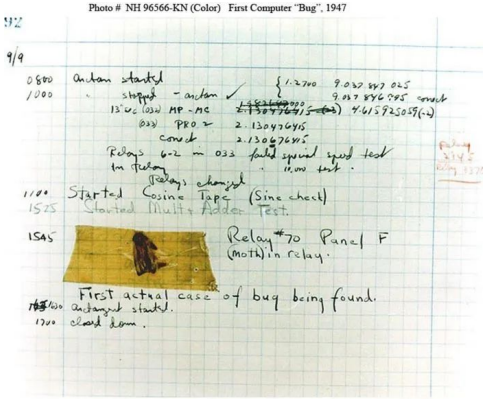
Recap: Old vs. New

Bugs

Everything is a bug…

A bug is a violation of expectations.
A **security** bug is a violation of expected **privilege**.
A **safety** bug is a violation of expected **margin of safety**.

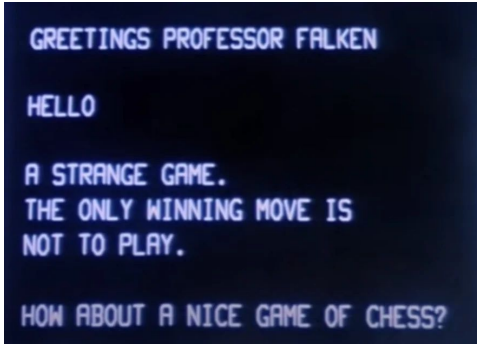
Context is everything… therefore design must be clearly specified and testable.



Source: Naval Surface Warfare Center, Dahlgren, Virginia

Cinder Blocks

A **safe**   system is not necessarily **secure.**
A **secure** system is not necessarily **safe.**

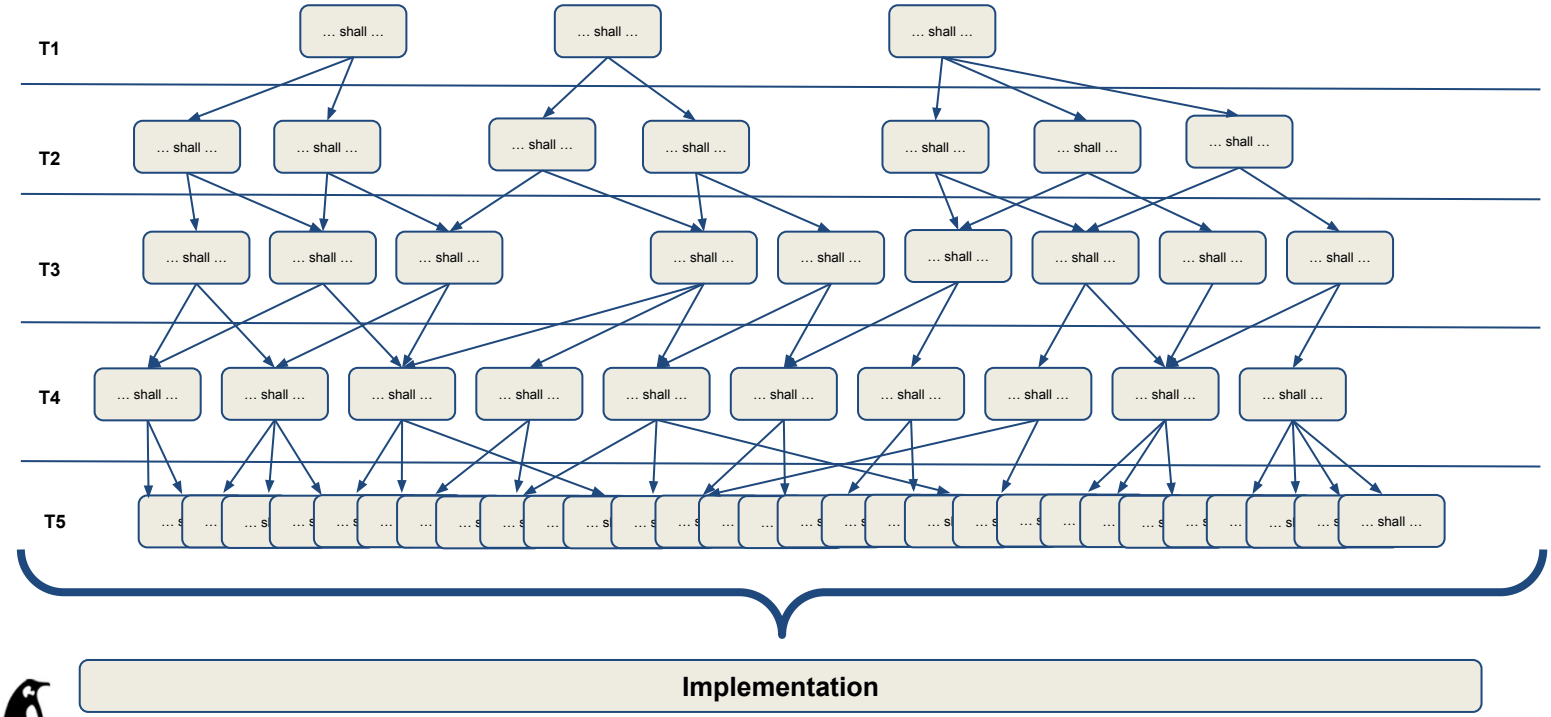


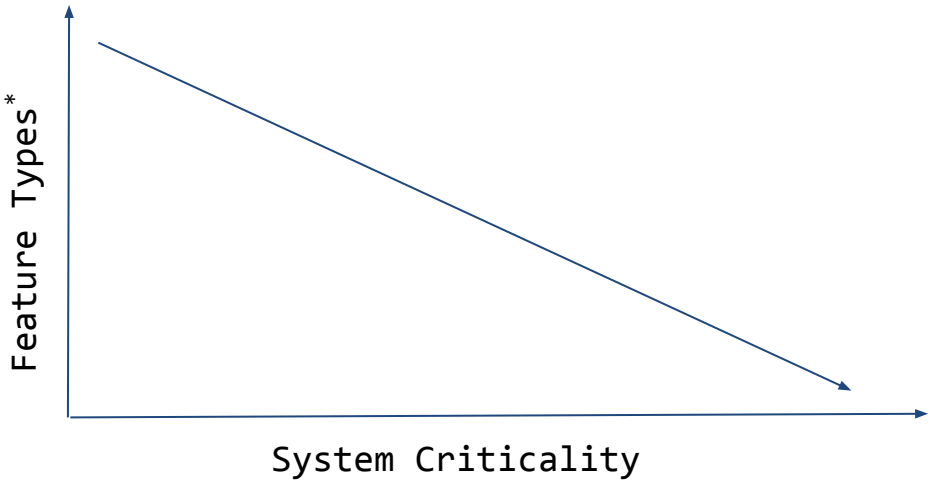
Source: War Games (1983)

Safety engineering concerns itself with what **shall** happen. (Provable)

Security engineering concerns itself with what **shall not** happen. (Unprovable)

(Testable) Design Expression





*Feature Type != Feature Quantity

Hardware Separation?

- Gold standard? Very debatable…
- Aerospace is *VERY* low volume.
- Power and cooling is *VERY* limited.
- Must be reliable and easy to fix.

Ideas?

- Time and space partitioning?
- Interconnectivity?
- Other ideas?