It's a Bird… It's a Plane… It's a Satellite?!!

5 things flight software engineers should consider when designing inexpensive LEO spacecraft.

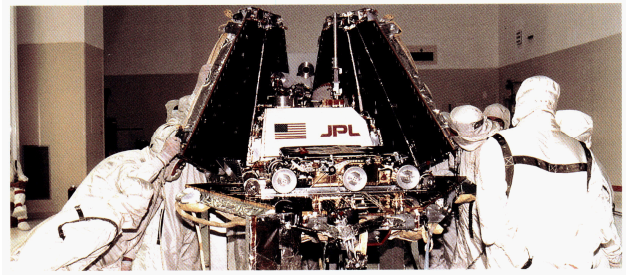
info@stolperconsult.com
www.stolperconsult.com

Steven A. Stolper

Who am I?

More than 20 years as an embedded software developer, consultant, and technical leader

- **Jet Propulsion Laboratory**
  - Mars Pathfinder
  - Galileo Orbiter
  - Others…

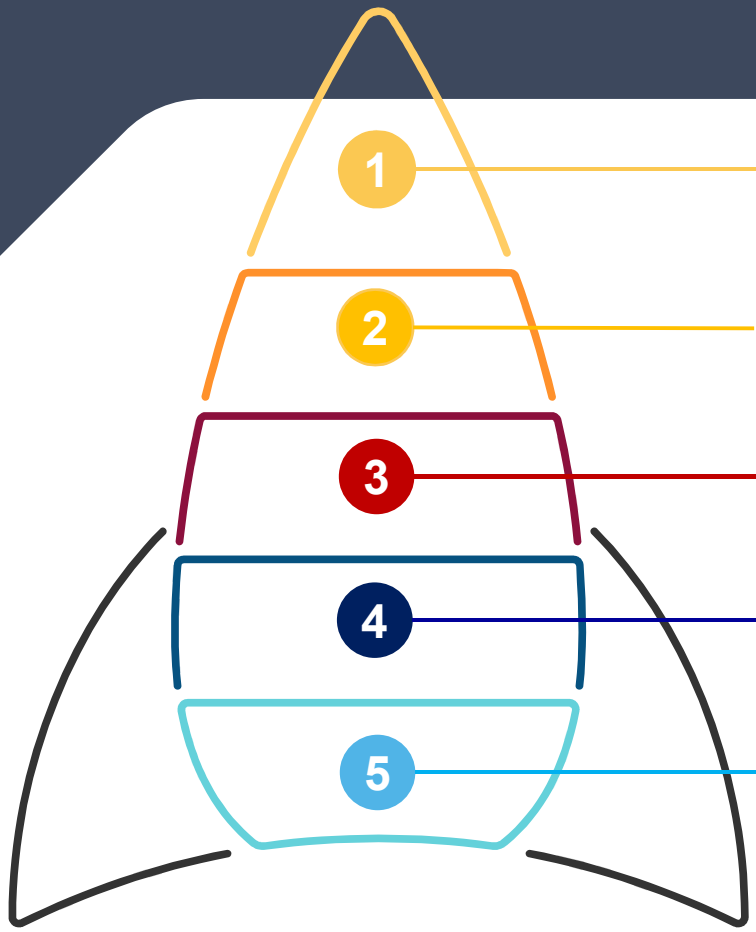


- **Silicon Valley**
  - Skybox Imaging/Google
  - Silicon Spice/Broadcom
  - Brocade Communications
  - Eyefluence/Google

- **Software/Programmatic Consultant**
  - Commercial and academic spacecraft flight teams
  - Mobile and embedded devices

Steven A. Stolper

Contents



Steven A. Stolper

The Premise

The assumptions underlying this discussion

2 Different Approach

Approaches often differ from those used by "traditional" spacecraft-building organizations.

COTS + Streamlined Development 3

They select commercial off-the-shelf components, streamline the flight software development processes, and operate their spacecraft differently from more traditional organizations.

1 Cost as a Driver

"New Space" companies want to revolutionize space travel by lowering the cost.

Different Assumptions 4

You may recognize the subsystems, but your assumptions about reliability, radiation tolerance, and cost are all wrong.

Steven A. Stolper

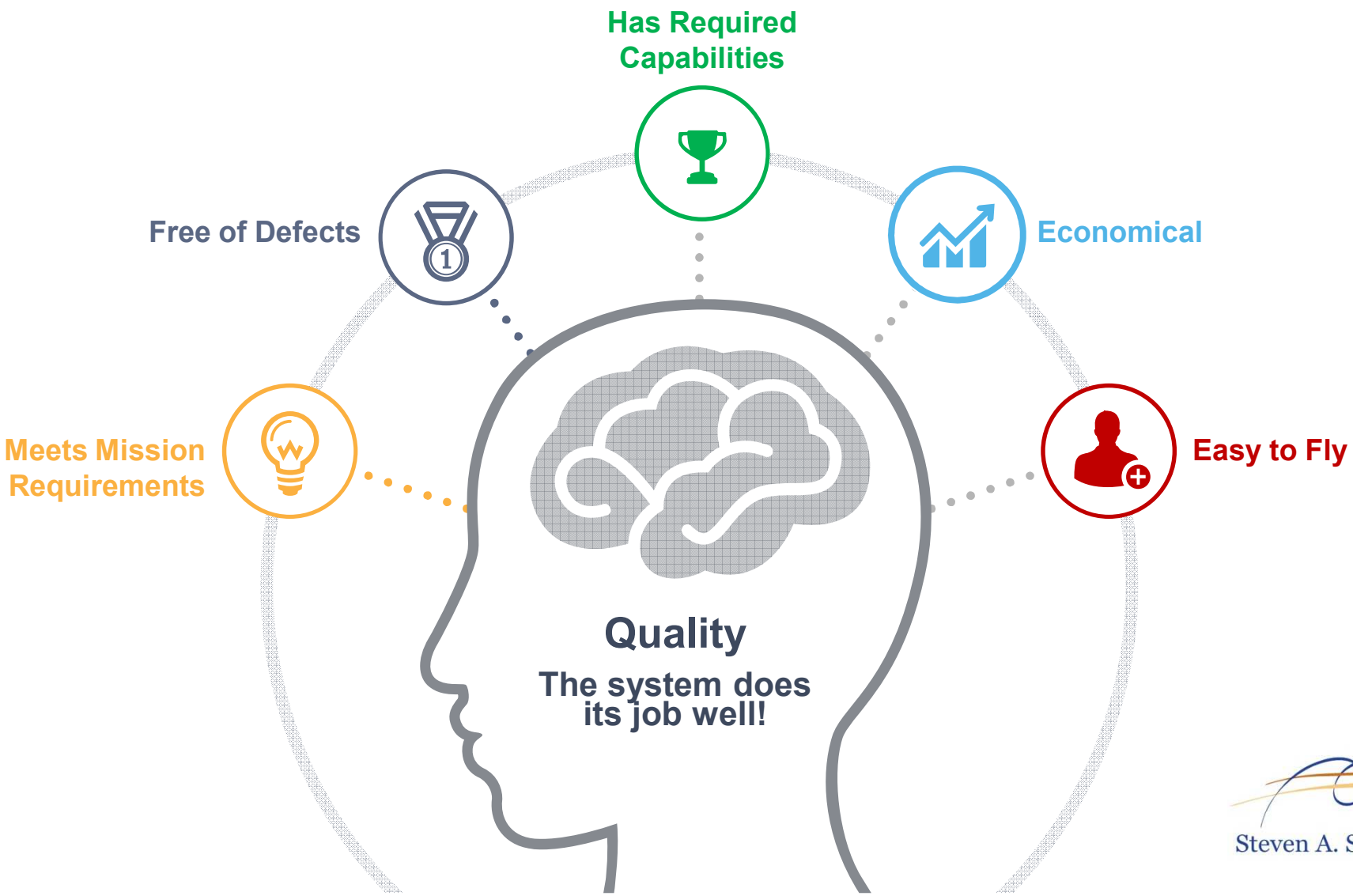
Designing for Quality

Better, Faster, Cheaper… Pick any two!

This is a Myth!!!

What is Quality?

Building low cost spacecraft with high quality

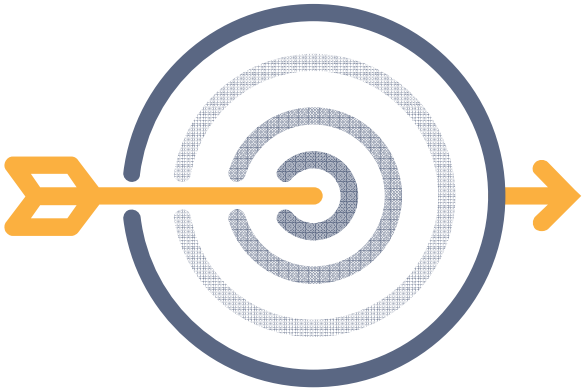


Steven A. Stolper

What is Quality? (Cont)

Build the “right” spacecraft for your mission

- Honda Civic vs. Cadillac
- McDonalds Hamburger vs. Filet Mignon
- Design the “right” spacecraft for your mission/company
- The Iron Triangle
- Don’t cut corners, cut features.
- **Cheating is a valid engineering solution!**



Steven A. Stolper

LEO Operations & Flight Software

Visualize how operators will fly your spacecraft

Polar Orbit / LEO

Design and Operations

- Tracking passes short. (2-12 min @ ~600 km)
- Passes Every ~90 minutes
- Coverage: You can't afford many ground stations
- You want many spacecraft

- S/C design and operations need to be geared toward this. (Telemetry design, Command dictionary)

- Examples:
  - Assess, receive, transmit
  - Automated commanding
  - No "fat fingering" or “cowboy ops”

Steven A. Stolper

Security Considerations

It's embarrassing when teenagers hack into your S/C.

Security Issues

Think about security at design time

Don't Get Locked Out

Design the system so you can never be locked-out of a healthy S/C. The security state should be deterministic.

Bandwidth Consumption

How does encryption effect the effective bandwidth?
How does it effect data return on a noisy link?

Communications Problems

Separate security problems from communications problems.
Have accountability/visibility through the system (Fishbone).
How does encryption fit in?

Key Material

How do you protect your key material/certificates?
In the MOC?
In the GSE?
When contractor building S/C and/or launching in a foreign country?

Safe Mode & Anomalies

Consider how security posture changes in Safe Mode or during Command Loss Response.

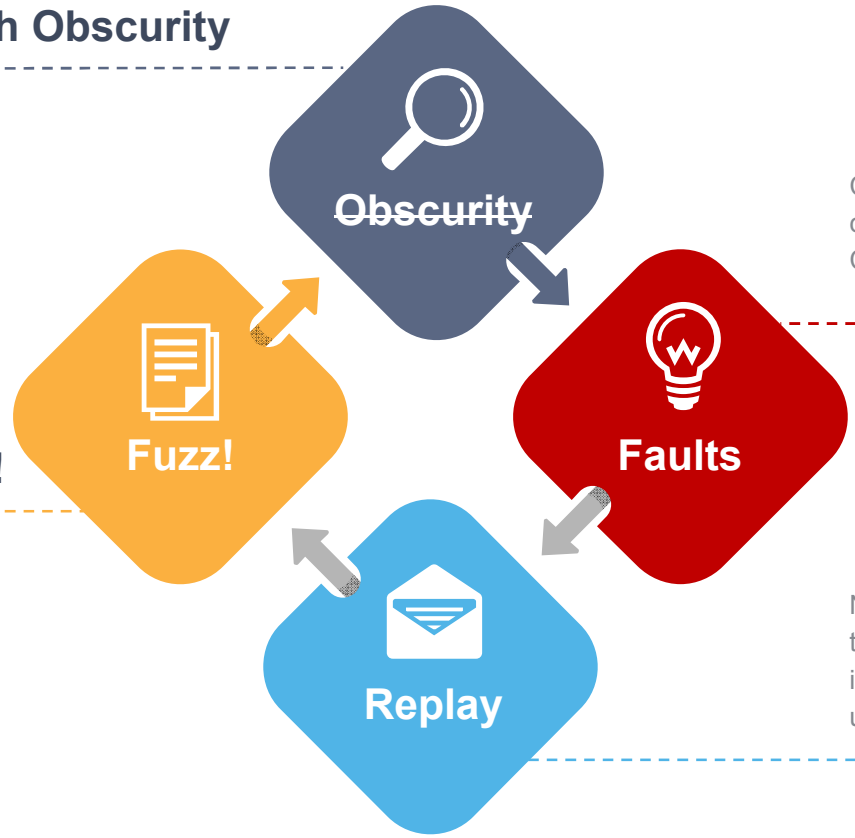
Steven A. Stolper

Some Security Guidelines

A Little Forethought Goes a Long Way

No Security Through Obscurity

Security is binary. Your system is or it isn't. Even if the security scheme is public, the system should be safe as long as the key material remains secret.



Consider how security posture changes when Safe Mode or Command Loss Response.

Anticipate Anomalies

Fuzz Your Software!

Test! Test! Test! Send random gibberish commands to the flight software during nightly/continuous testing.

Never allow commands or telemetry recorded during testing, integration, or previous passes be used against you.

Protect against Replay Attack

Steven A. Stolper

Visibility

Look deep into nature, and then you will understand everything better.
- Albert Einstein

Visibility Issues

Many flight software engineers overlook visibility

Short Passes

Pass variability (2 -12 min), Can miss entire orbits depending on ground track and number of stations. (Memory, prioritization)

Limited Downlink

Limited downlink bandwidth due to S/C attitude, power, health, time-sharing with payload

Off-track Data

The volume of off-track data may exceed the ability to downlink on the next pass.

Changing Rates

Spacecraft health and link reliability can limit ability to downlink telemetry. How do you optimize for different rates?

Many Spacecraft

Arbitrating between multiple S/C over ground stations simultaneously
Common mode failure = Many sick spacecraft

Categorize Your Data

A wonderful serenity has taken possession of my entire soul.

1 Real-Time

Current state of the spacecraft, timely data, instantaneous performance

2 Recorded

Off-track data used to reconstruct S/C behavior over the course of the orbit. Trending data. Anomalies that occur off-track.

Events 4

Yell and scream when anomaly occurs!
Include as much relevant data as possible.
Positive confirmation of nominal events.
Explicit messages to reconstruct intent during off-track periods.

High Rate Data 3

First-fault data. Can run continuously and can "trap" problems by freezing capture when problems occur. Some problems too fast for telemetry.

Steven A. Stolper

Safe Mode & Autonomous Recovery

Better Safe than Sorry

Give Yourself a Safe Mode

Try to use as little equipment as possible (COTS)

Power Safe

Much of your orbit will be in eclipse. Plan for it and prevent "bouncing" when exiting occultation.

Payload Safe

Your payload is your mission.

Do you need to actively control temperature?

Thermally Safe

Can you talk to the S/C at any attitude?

Communications Safe

Steven A. Stolper

Special Considerations

Build the “right” spacecraft for your mission

- With COTS hardware, SEUs are a part of doing business.

- Consider failing operationally
  - Your S/C is an earning asset.
  - Your S/C spends most of its time off-track
  - If you have a “cheap fleet,” each S/C still needs to look after itself – common mode failure

Questions?

Steven Stolper

info@stolperconsult.com

www.stolperconsult.com

Steven A. Stolper