Systems Engineering Requires a Paradigm Shift
A peep into history
SYSTEMS ENGINEERING IS NOT NEW!

Aristotle – Metaphysica 330 BC
PONT DU GARD IN FRANCE (19 BC)
First attempt to teach systems engineering as we know it today came in 1950 at MIT by Mr. Gilman, Director of Systems Engineering at Bell.

“today's systems may embed themselves in history” - Ludwig von Bertalanffy
SAGE - Semi Automatic Ground Environment air-defense system was defined and managed by MIT (1951 –1980)
The earlier Northrop XB-35 of the 1940s had mechanical controls. The B-2 of today has fly-by-wire controls a combination of mechanical electronics and software.
FAILURES HAVE HAPPENED

Systems Engineering has failed us for some time now
AS THE SYSTEMS HAVE BECOME COMPLICATED ACCIDENTS HAVE INCREASED

The first error in 1962

NASA Mariner 1 - 1962

1991
US aviation authority: Boeing 787 bug could cause 'loss of control'

More trouble for Dreamliner as Federal Aviation Administration warns glitch in control unit causes generators to shut down if left powered on for 248 days.

The Boeing 787 has four generator-control units that, if powered on at the same time, could fail simultaneously, causing a complete electrical shutdown. Photograph: Elaine Thompson/AP

SUMMARY: We are adopting a new airworthiness directive (AD) for all The Boeing Company Model 787 airplanes. This AD requires a repetitive maintenance task for electrical power deactivation on Model 787 airplanes. This AD was prompted by the determination that a Model 787 airplane that has been powered continuously for 248 days can lose all alternating current (AC) electrical power due to the generator control units (GCUs) simultaneously going into failsafe mode. This condition is caused by a software counter internal to the GCUs that will overflow after 248 days of continuous power. We are issuing this AD to prevent loss of all AC electrical power, which could result in loss of control of the airplane.
Glitch found in engine software requires immediate checks after issue-plagued fleet is grounded.

The Airbus A400M has been plagued by technical faults and now software glitches that reportedly caused a crash. Photograph: Julio Munoz/EPA

Airbus has issued a critical alert calling for immediate checks on all its A400M aircraft after a report identified a software bug as having caused a fatal crash in Spain earlier this month.

In a statement Airbus said it was "devastated to confirm" the loss of four crew members, adding that another two are in hospital in a serious condition.

Four crew dead!!
The Pentagon's New List Of F-35 Bugs Is Predictably Awful

MICHAEL NUNEZ  4 FEBRUARY 2016 11:00
"There's no brakes... hold on and pray": Last words of man before he and his family died in Toyota Lexus crash

THERE HAVE BEEN FAILURES IN OTHER FIELDS TOO
WE REQUIRE SOMETHING Different
“The world as we have created it is a process of our thinking. It cannot be changed without changing our thinking.”

-Albert Einstein
EFFORT DISTRIBUTION IN SYSTEM DEVELOPMENT
SYSTEM DEVELOPMENT
V MODEL – WE SPEND TIME ON THE RIGHT SIDE

model today
AN INTERESTING METRIC ON THE PROCESS TODAY

Cost of Fixing
Type Errors Found
Effort Spent/Where errors found
WE REQUIRE A PARADIGM SHIFT!
MATHEMATIZE THE LEFT AND AUTOMATE THE RIGHT – IS THE MANTRA

∀x (Fx → Gx)

Automate right

Mathematize left
- Model based representation
- Property based requirements
- Formal proof of correctness of behavior
- Validated control system in the presence of noise, modeling inaccuracy, data ambiguity, faults
▪ Model based testing
▪ Generate random test cases
▪ Generate test cases using Orthogonal arrays
▪ Generate test cases using formal methods
▪ Generate test cases from Mutants
▪ Always measure coverage
Requirements

Make use of Simulink Blocks

Models

Use autocode

C/Ada

Requirement based tests

Structural Autotests

There is a big confusion here on how to write requirements!!

Remember: Models ARE NOT requirements!!

There is a little bit of test case automation here.

THIS IS WHAT WE DO TODAY
THIS IS WHAT WE NEED TO DO NOW

Properties

Use Simulink blocks or any other models

Models

Definitely use autocode

C/Ada

Property Based Autotests

Structural Autotests

Bring in Property Based Requirements

Bring in Property Based Testing

Continue with your automated testing
Thank you

Any questions?
You can find me at
▶ yvjeppu@gmail.com

Our system is only as good as the test cases we have designed to prove it correct