26th annual INCOSE international symposium
Edinburgh, UK
July 18 - 21, 2016

From Agile Systems Engineering to Agile Safety Engineering

James Lawson

Contents

- Why Agile safety engineering?
- Agile safety engineering techniques,
- Case study.

Experience

- Eurofighter
- F-35 Lightning II
- A400M Brakes
- 787 Electrical Brakes
- Learjet 85 EPS
- MTU EPMU
- Bell 525 SPDS/ TRUs
- Pilatus PC-24 ISGS
- Pilatus PC-24 SPDS
- PCM for 777X Flight Controls
- PCM for C919 CCN
- Zee Aero ‘flying car’

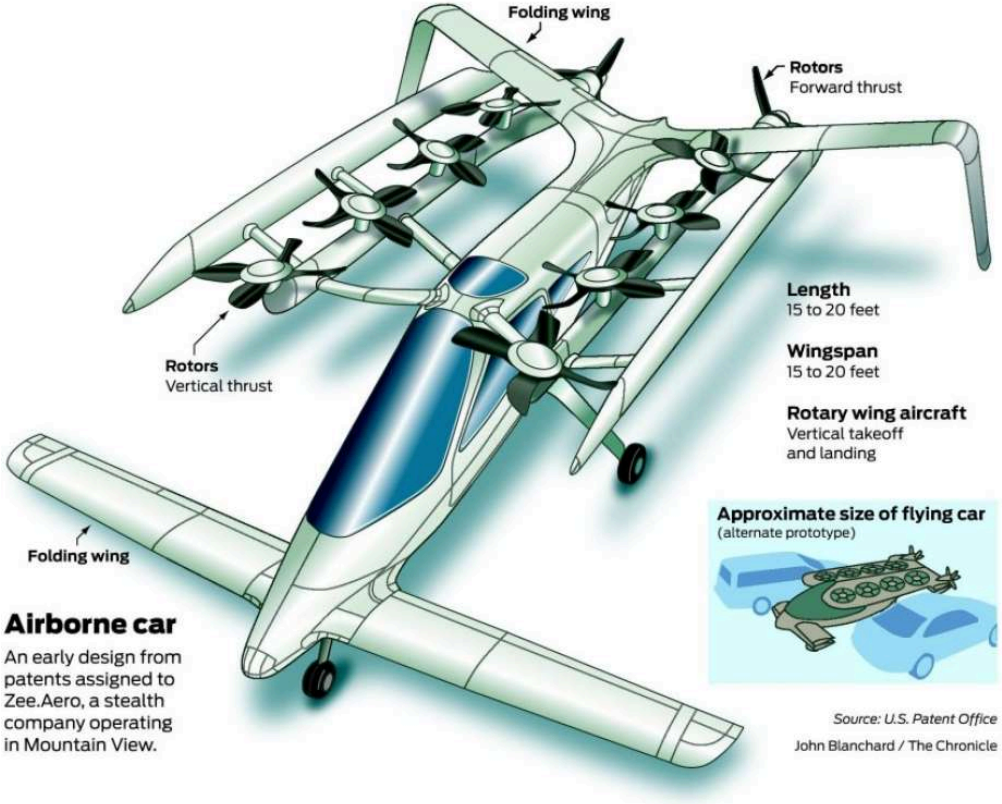
Why Agile Safety Engineering?

26th annual INCOSE international symposium
Edinburgh, UK
July 18 - 21, 2016

- Automation, complexity and integration (more ways things can fail):
  - Road vehicles,
  - Aircraft and;
  - Flying cars.
- Need for a ‘lightweight’ approach to safety engineering which becomes more rigorous as design matures.
  - Changes are cost prohibitive if made too late in the design life cycle,
  - The rigidity of safety requirements is in contrast to other requirements which can often be relaxed.

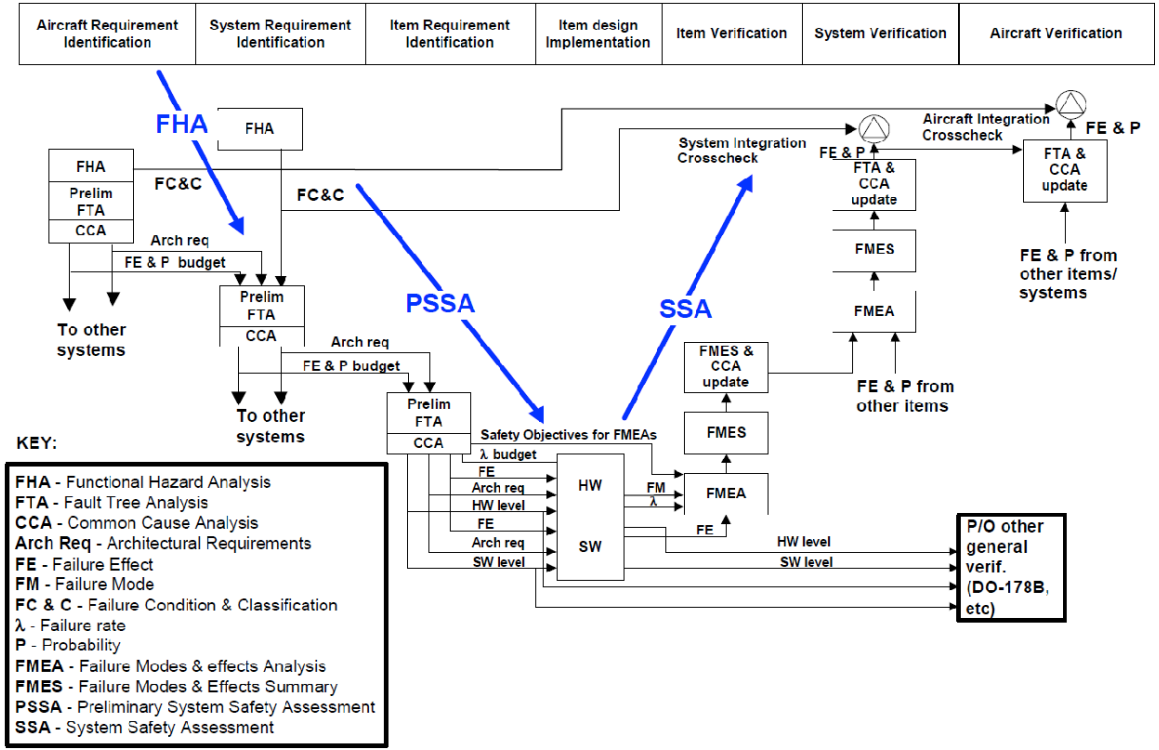
People really are putting autopilots in cars:

People really are building flying cars:



The V-model:

- Multiple levels of FTA, CCA, FMEA and FMES,
- Integration of different levels is challenging,
- Inability to react to unanticipated change,
- Aircraft can be over-designed or under-designed (reliability impact in addition to cost impact).



Agile safety engineering techniques:

26th annual INCOSE international symposium
Edinburgh, UK
July 18 - 21, 2016

- Hybrid piece part/ functional Failure Modes and Effects Analysis (FMEA),
  - A functional FMEA if sufficient to show compliance to probability budgets,
  - A piece part FMEA if functional FMEA is insufficient,
  - Failure Mode Distributions (FMDs) if necessary.
- A framework with interchangeable models as opposed to a V-model,
  - Supports rapid reassessment as information becomes available.
- The removal of conservatism as needed in a step-by-step iterative fashion,
  - Steps are halted when compliance to probability budgets is achieved.
- Integration of the different interchangeable models.
  - Fabric joining interchangeable models does not need to be reestablished,
  - Rapid reassessment as product evolves,
  - Rapid reassessment as product is deployed to a new environment.

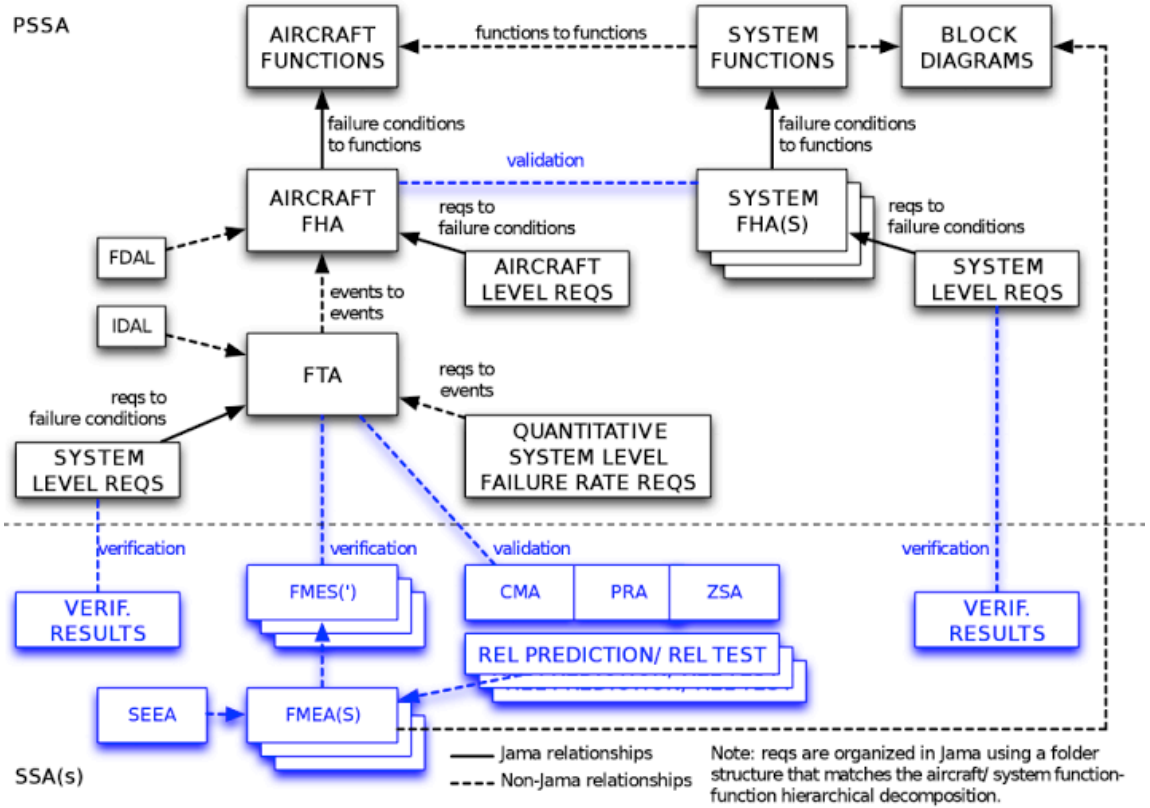
Case study ‘flying car’:

26th annual INCOSE international symposium
Edinburgh, UK
July 18 - 21, 2016

- No certification basis precedent,
  - Chicken and egg questions ‘how much automation?
  - Unsettled certification basis. What is it?
- Overlapping iterations with a need to converge on a certifiable product,
  - What are the known deficiencies?
  - Are changes resulting in a more certifiable product?
  - Many unmanned and manned prototypes with several parallel paths.
- Automation, complexity and integration and a need to respond to changing requirements.
  - Unsettled mission profile,
  - Electronic flight control system,
  - Auto land/ takeoff and hover stabilisation.

Framework:

- System FHAs validate Aircraft FHA,
- Fewer FTAs,
- Careful selection and abstraction of effects shifts effort away from FTAs,
- Hybrid FMEAs reduce effort,
- FMES is glue between FTAs and FMEAs and is automatically generated.



Results ‘flying car’:

26th annual INCOSE international symposium
Edinburgh, UK
July 18 - 21, 2016

- Quick evaluation of many prototypes in parallel,
  - Effort completed within weeks by a small team,
  - Where information is missing conservatism is applied.
- Different mission profiles evaluated,
- Agile safety engineering framework is an integral part of effort,
  - Incorporation of independent over voltage/ over current protection,
  - High and low voltage power distribution architecture,
  - Incorporation of monitoring only as required to show compliance to probability budgets,
  - Most significant contributors to overall probability budgets identified and removed via a cut set analysis.
- Issue papers written where certification basis questions exist.
  - Complex COTs hardware common mode analysis,
  - Design Assurance Levels (DALs).