STPA short example
X-47B Autonomous Aircraft

Disclaimer

These exercises are not meant to represent a complete analysis, and they are not meant to exhaustively demonstrate STPA.

The exercises are only meant to introduce a few core concepts.

X-47B autonomous aircraft

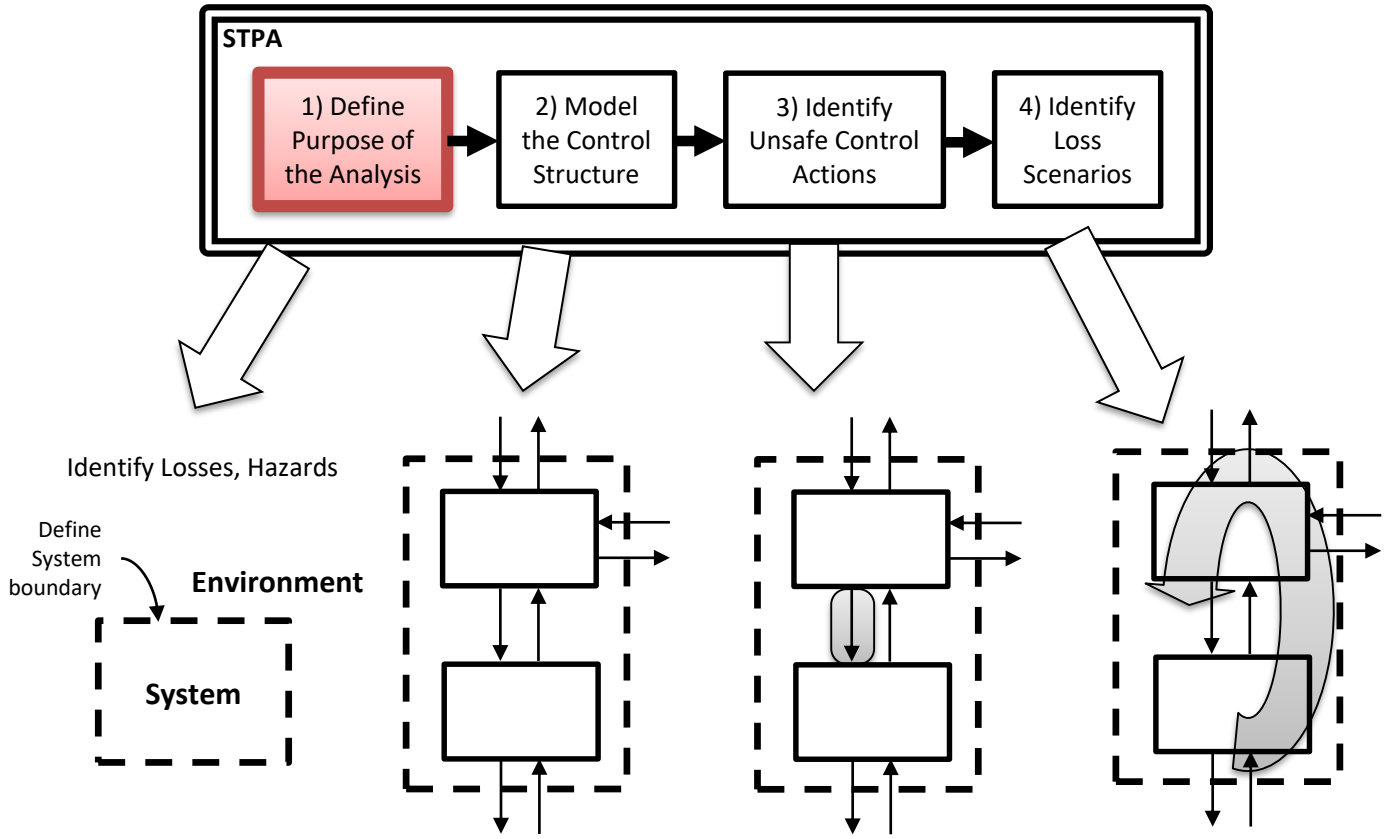
- Design intent: program fully autonomous behavior
- Example: Crosswind limits

Aircraft

- Aircraft uses calculated winds at altitude to estimate if surface crosswind limits would be exceeded on touchdown
- Automatically waveoff if needed
- Aircraft does not receive or use surface wind info from tower

Flight testers

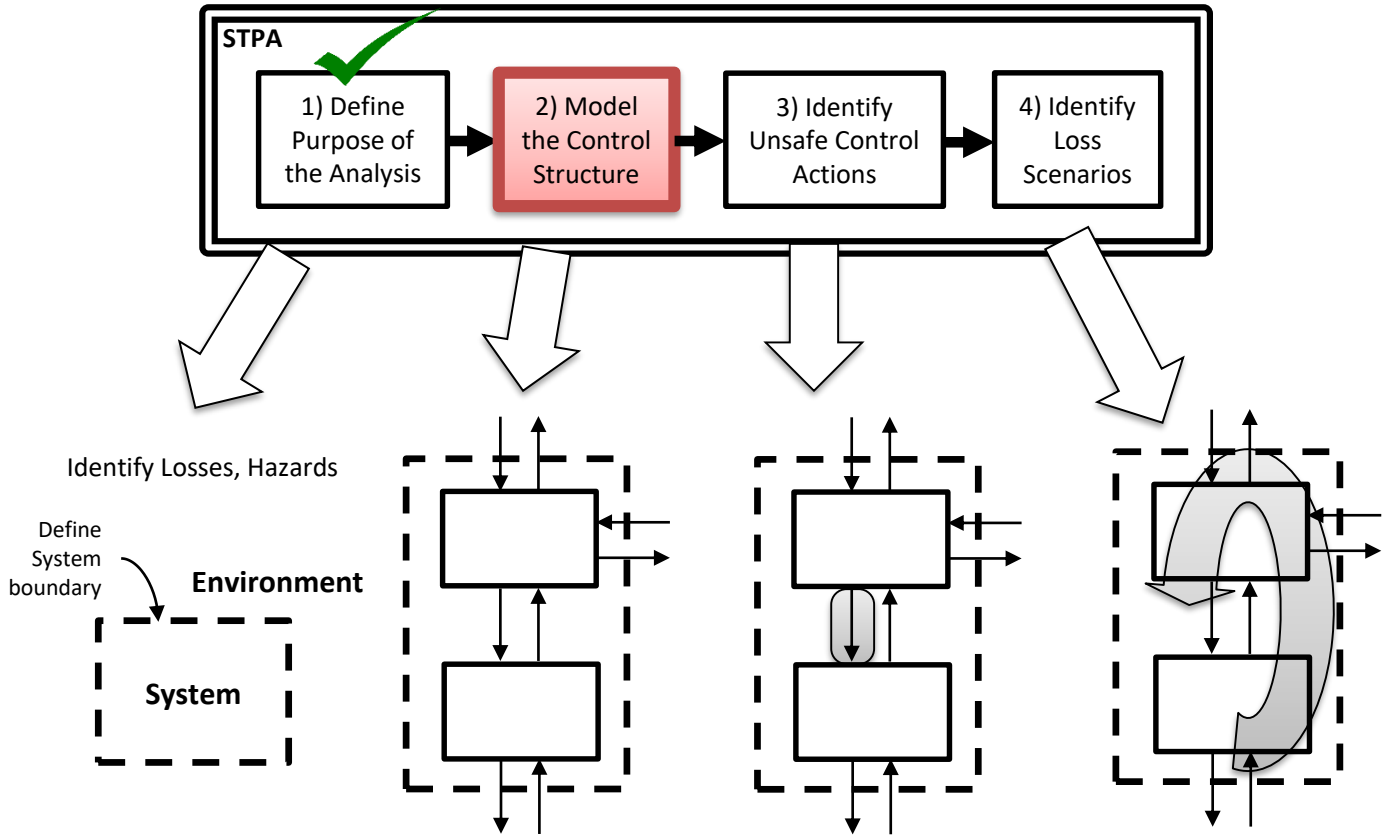
- It would be normal for a pilot to see stronger winds and unfavorable crosswind at altitude, even at 1000ft, but then see a drastic reduction on landing (which is where crosswind limits apply)
- Flight testers can receive surface wind info from tower and assess the potential for crosswind exceedance on landing
- Flight testers can override automation and force landing if needed



(Leveson and Thomas, 2018)

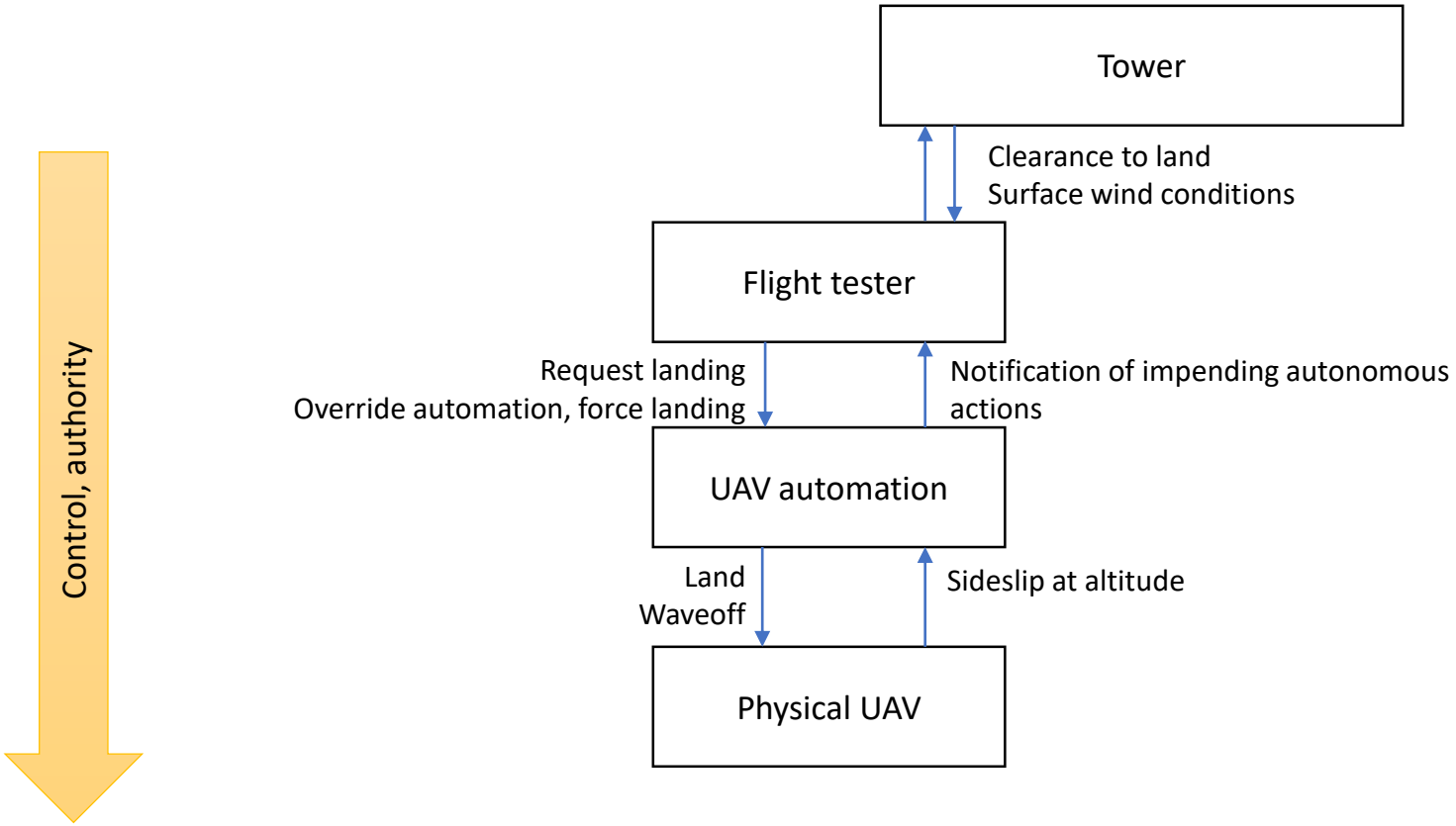
Losses

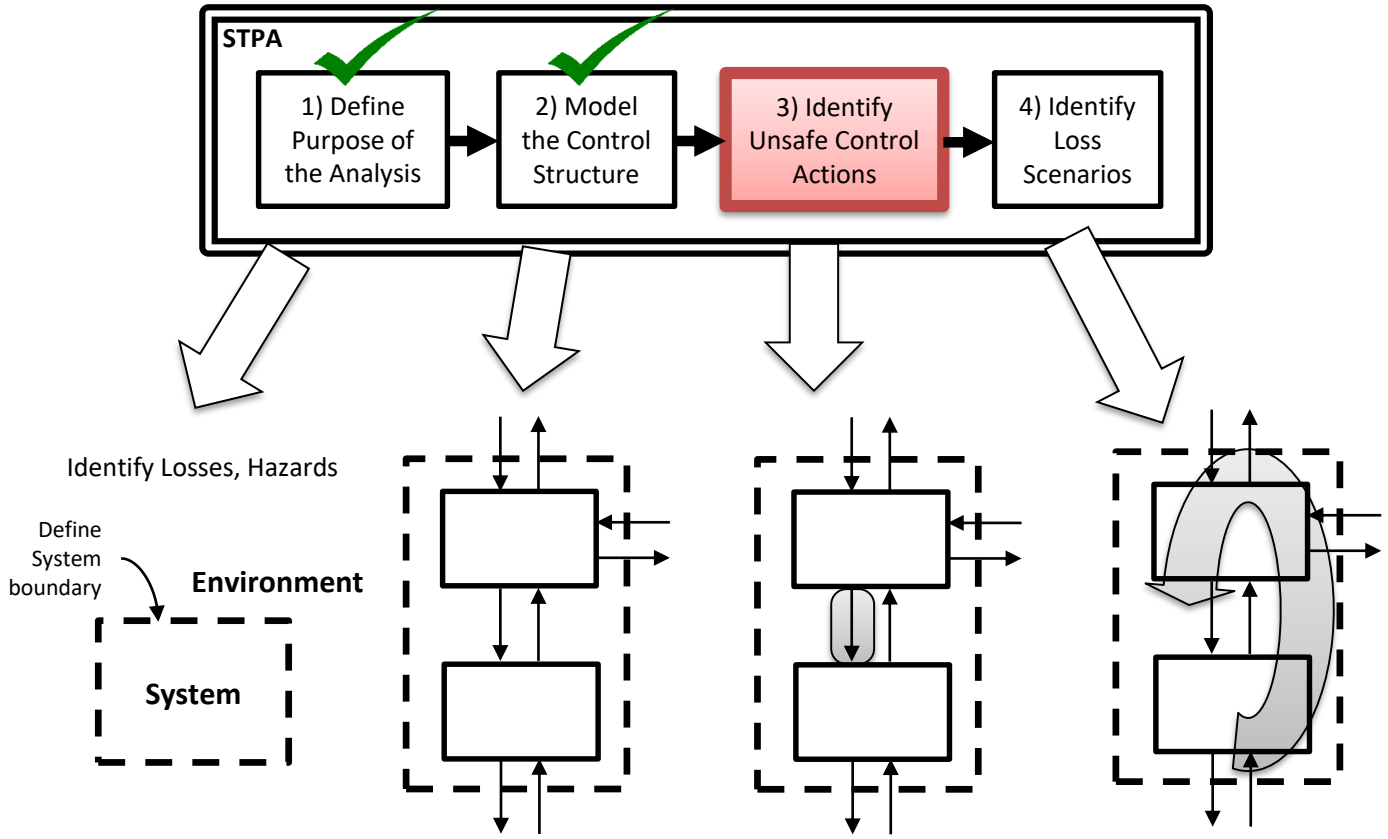
- L1: Loss of life (?)
- L2: Loss of aircraft (e.g. crash)
- L3: Loss of flight testing performed (mission loss)



(Leveson and Thomas, 2018)

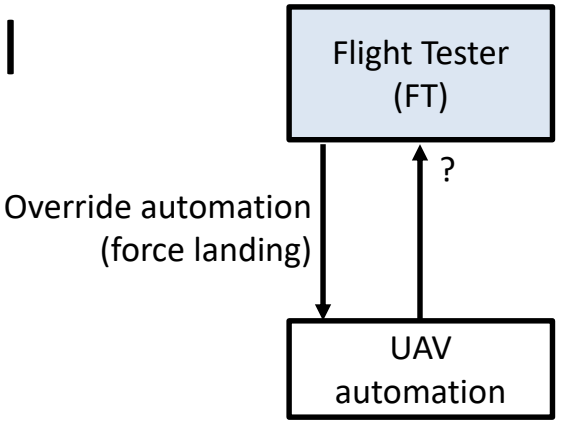
Control Structure



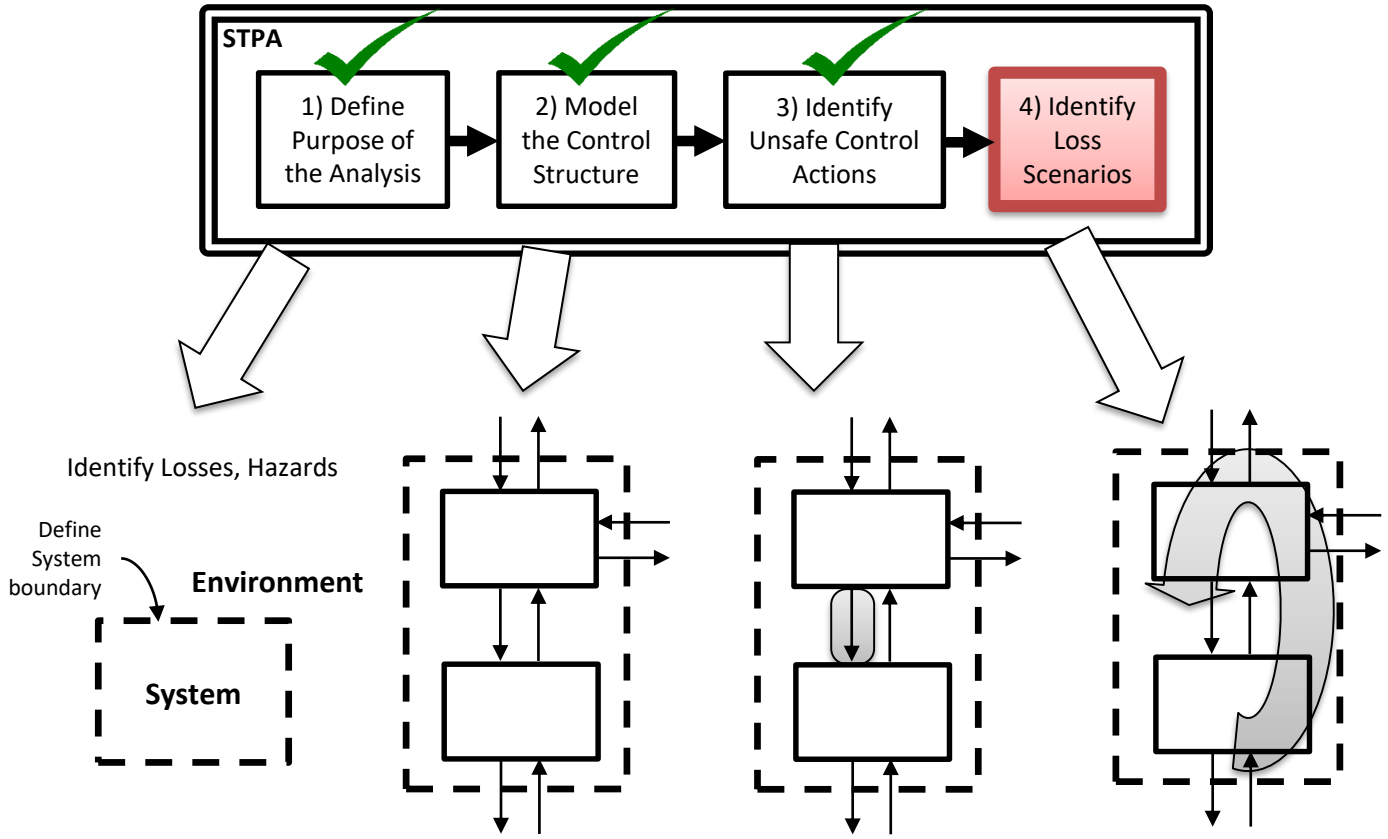


(Leveson and Thomas, 2018)

Unsafe Control Actions

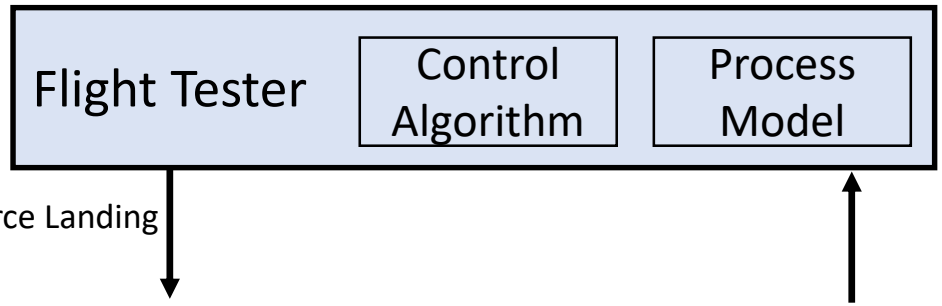


	Not providing causes hazard	Providing causes hazard	Too early, too late, out of order	Stopped Too Soon / Applied too long
Override automation: Force Landing)	**FT does not provide Force Landing Cmd when** _____	**FT provides Force Landing Cmd when** _____	**FT provides Force Landing Cmd too late after** _____ **FT provides Force Landing Cmd too early before** _____	**FT continues providing Force Landing Cmd too late after** _____ **FT stops providing Force Landing Cmd too soon before** _____



(Leveson and Thomas, 2018)

Controller Analysis (Let's do this together!)



Controller output

UCA-1: FT does not provide Force Landing Cmd (i.e. override waveoff) when fuel is low and surface winds are acceptable [L1,L2,L3]

Controller process model

PM-1: FT believes _____ [UCA-1]

Controller input

F-1: FT receives _____ [PM-1]

Consider:

Feedback missing from design

Feedback not sent

Feedback incorrect

Feedback delayed

Etc.

Discuss actual operation of the aircraft