AVIC CAPE

Aviation Industry Corporation of China
China Aero-Polytechnology Establishment

Case study of a landing gear system safety analysis by using MBSA

Xiaoxun Li

2014.10.29

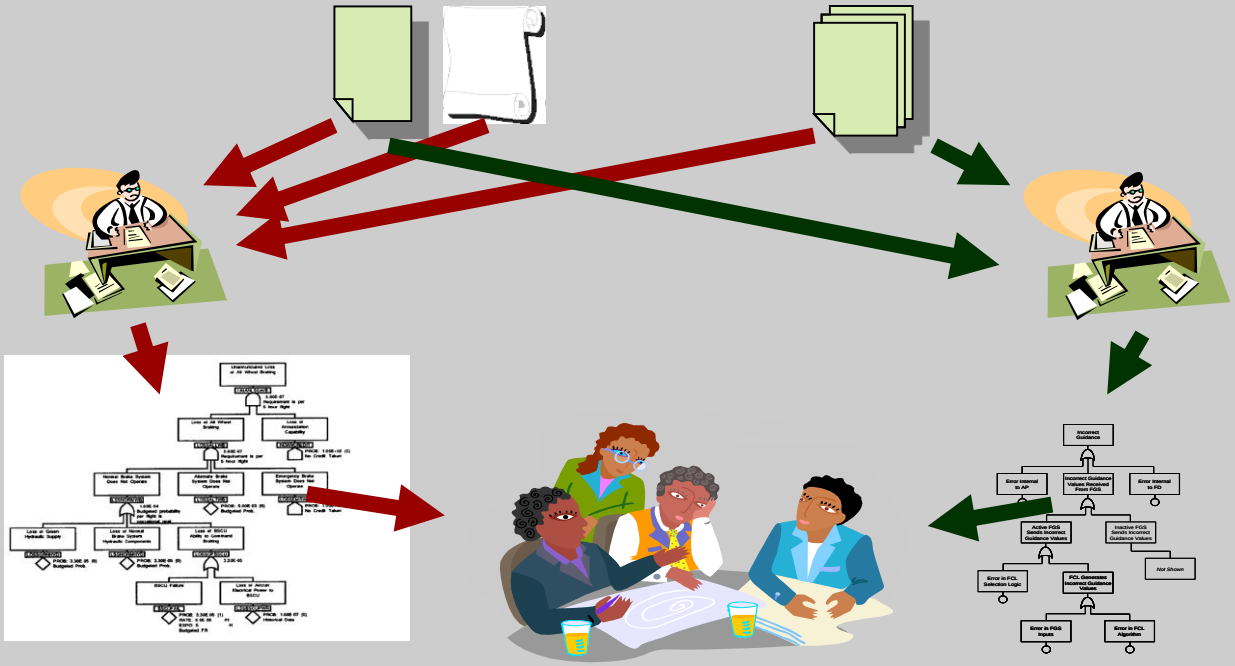
Content

- Background
- Altarica-based safety analysis process
- Case study

CAPE

Background

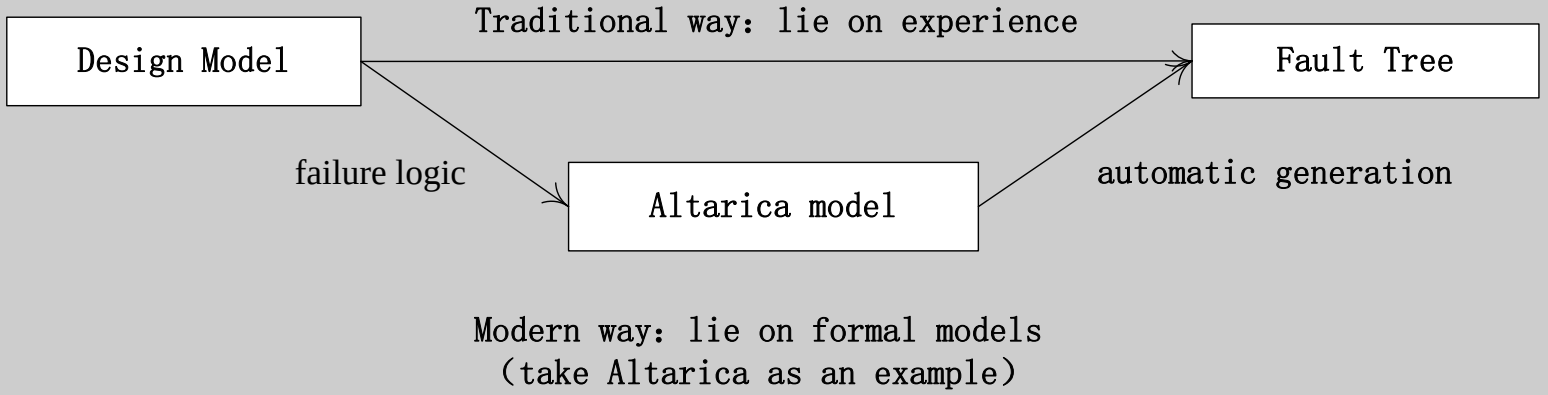
- Traditional fault trees are established by analysts based on experience, which means that the fault trees could hardly reflect the real designs



CAPE

Background

- Formal models are usually built through the real system structures and functions, for example, Altarica could reflect the failure logic information of systems.



CAPE

Model-based safety analysis process

- Within EADS, APSYS(www.apsys.eads.net) is the company responsible for safety analysis. APSYS' software platform, SIMFIA, is based on the same standard Altarica, moreover, it allows the utilization of classical SAFETY technologies and methods based on construction or generation of fault trees as well as the most advanced SAFETY methods MBSA.

Model-based safety analysis process

- Through the application of SIMFIA in the project, we find that:
  - Model the framework needs: function tree, system composition diagram;
  - Define the model in detail needs: function failure condition and its effects, equipment failure modes and data;
  - Establish fault transfer relationship needs: function principle diagram.
- In order to standardize the use of SIMFIA software, the key information needs at least in application of SIMFIA are as follows:
  - Function tree, system composition diagram;
  - Function failure condition and its effects;
  - Equipment failure mode;
  - Function principle diagram.

CAPE

Model-based safety analysis process

- Step1: comprehensive review the function of the system according to the detailed design of the system, build function tree and system composition diagram to define the scope and the minimum unit of the analysis;
- Step2: according to the detailed design of the system, comprehensive review the system function principle and the relationship between these equipment, especially the input and output relationship between these equipment and the outer system;
- Step3: according to the detailed design and functional tree, analysis the failure condition of each function and their effects in different phases, carry out system FHA;

CAPE

Altarica-based safety analysis process

- Step4: according to the detailed system design, system composition diagram and the equipment FMECA results, analysis functional and hardware failure mode of each failure mode and their failure probability;
- Step5: on the basis of failure condition and the principle of the system and the failure mode analysis results, with the discuss result with the engineer about the relationship between all equipments, establish the system model by SIMFIA;
- Step6: FHA results are as the top event, use SIMFIA to generate the fault tree from the system model;
- Step7: based on the fault tree to carry out qualitative and quantitative analysis, and create system safety analysis report.

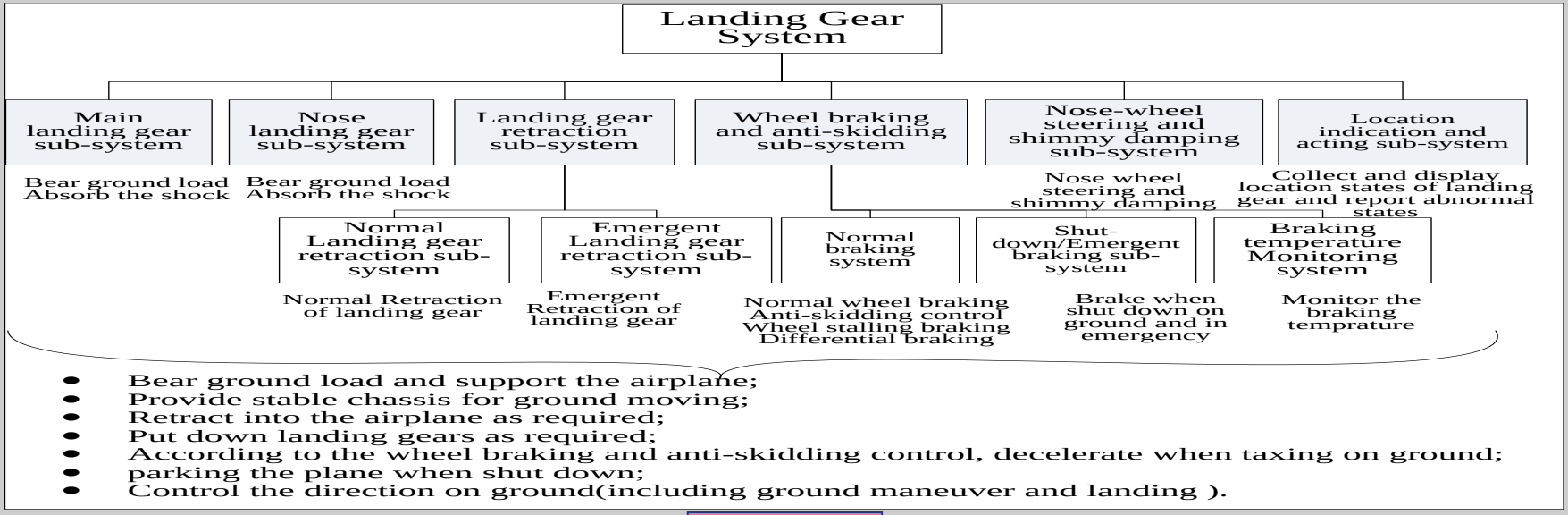
CAPE

Case study

- Landing gear is the only component that supports the entire aircraft, so it is a part of the aircraft that cannot be separated. This article select landing gear system as the study case, but due to the limited space and security requirements, we need to simplify the real landing gear system, only the nose-wheel steering and shimmy damping sub-system will be analyzed here.

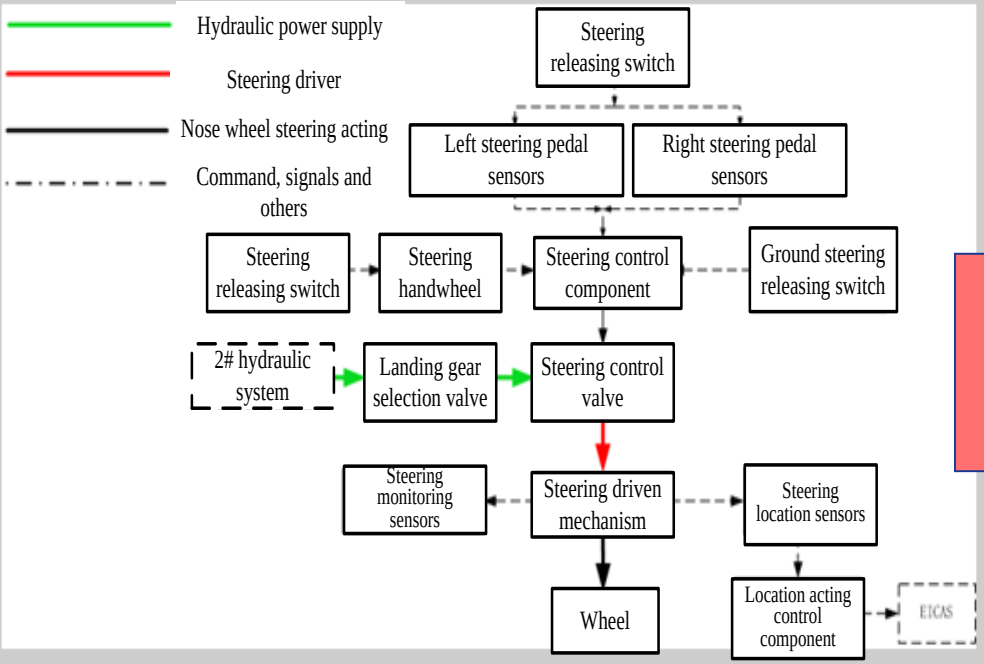
CAPE

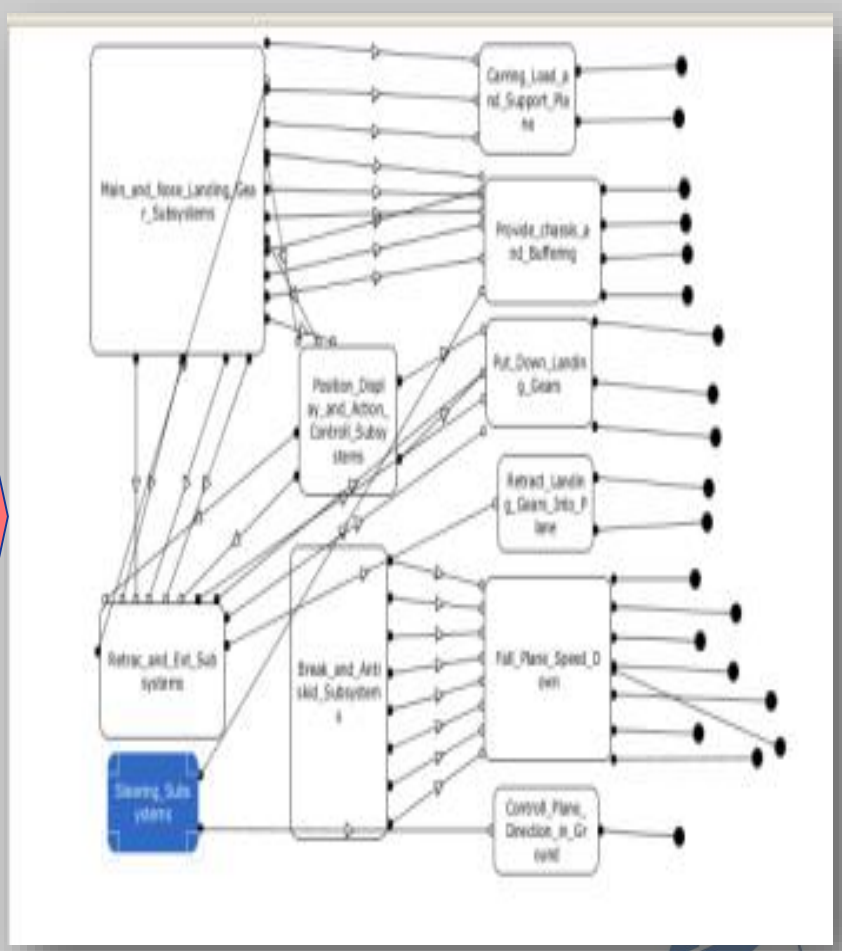
Case study



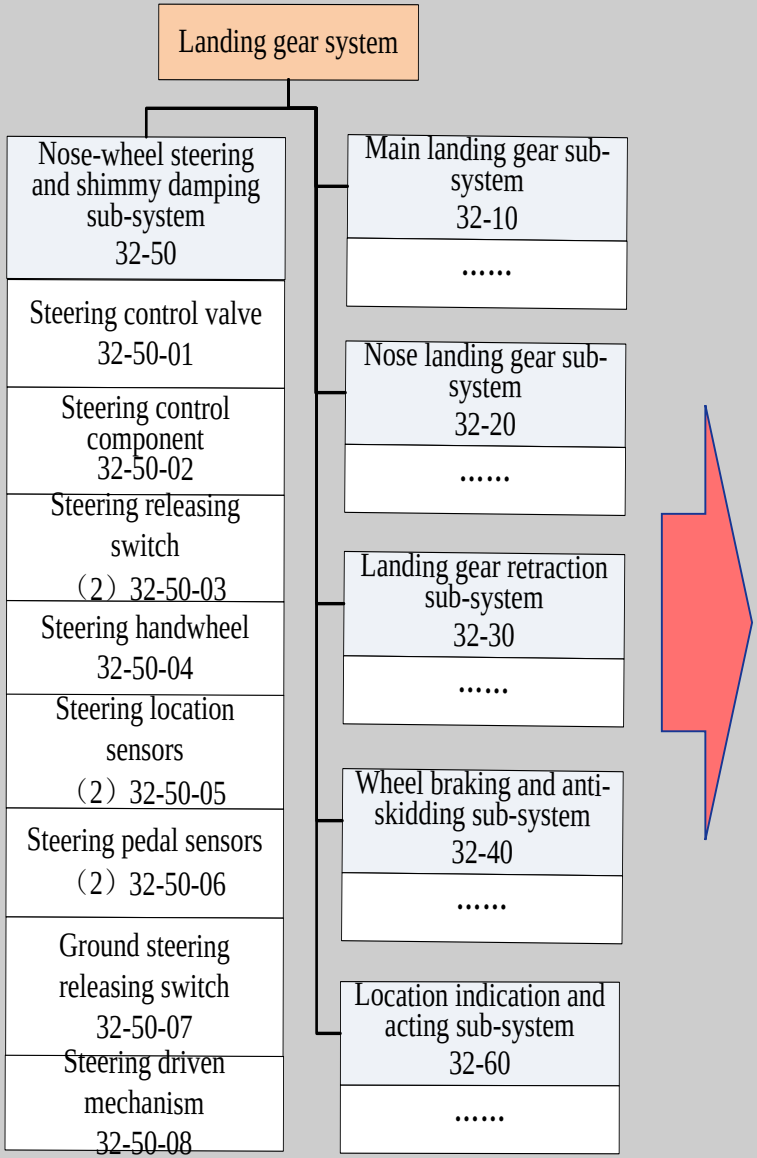
Failure condition	Phase	Effects	Class	Safety equirements
landing gear shimmy damping function fail	G、T、L	● Aircraft: landing gear shock and vibration seriously; ● Crew: hard to control the aircraft, operating burden increase heavily; ● Passenger: may feel discomfort or injury.	III	$<10^{-5}$
differential brake and steering gear fail, loss of ground direction control function	G、T、L	● Aircraft: at low speed can use brake to stop, at high speed can control rudder to control aircraft ground direction; ● Crew: operating burden increase slightly; ● Passenger: discomfort.	IV	$<10^{-3}$
non directive deflection	G、T、L	● Aircraft: may lost control of the aircraft and even lead to completely damaged; ● Crew: may die because of the damage of the plane; ● Passenger: may be due to the damage of the plane and most or all of the death.	I	$<10^{-9}$

Case study


Hydraulic power supply
Steering driver
Nose wheel steering acting
Command, signals and others
Steering releasing switch
Left steering pedal sensors
Right steering pedal sensors
Steering releasing switch
Steering handwheel
Steering control component
Ground steering releasing switch
2# hydraulic system
Landing gear selection valve
Steering control valve
Steering monitoring sensors
Steering driven mechanism
Steering location sensors
Wheel
Location acting control component
EICAS



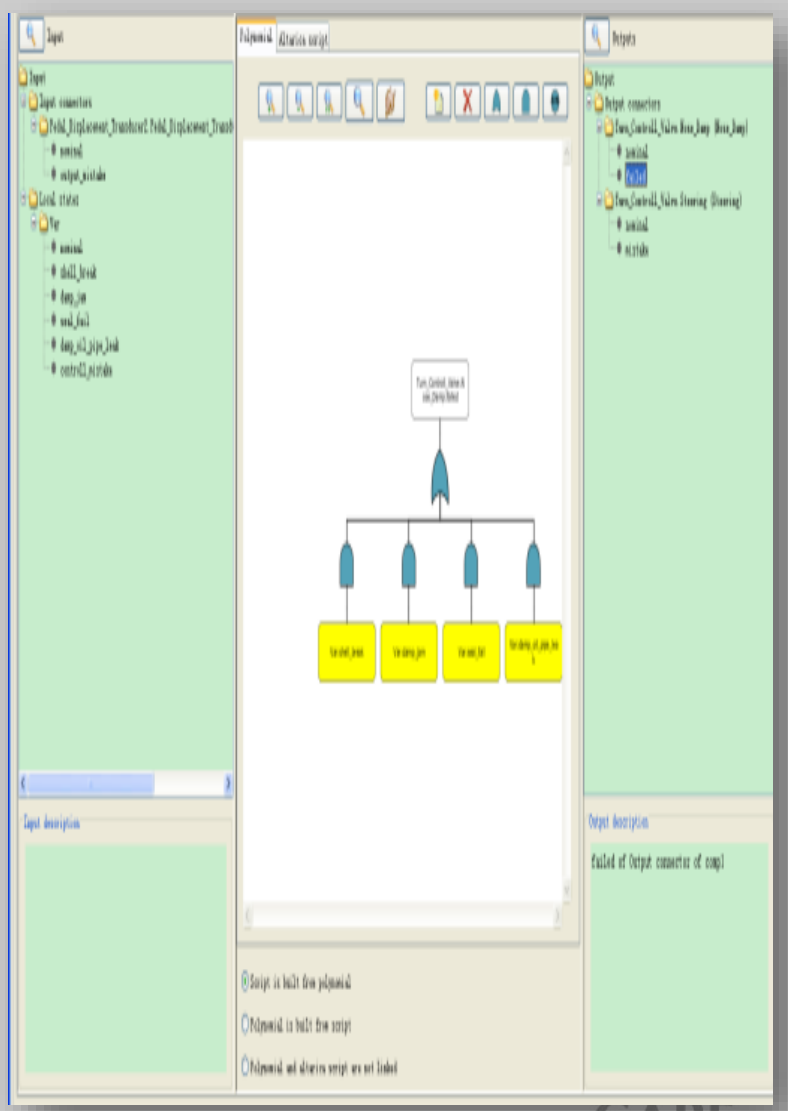
Case study



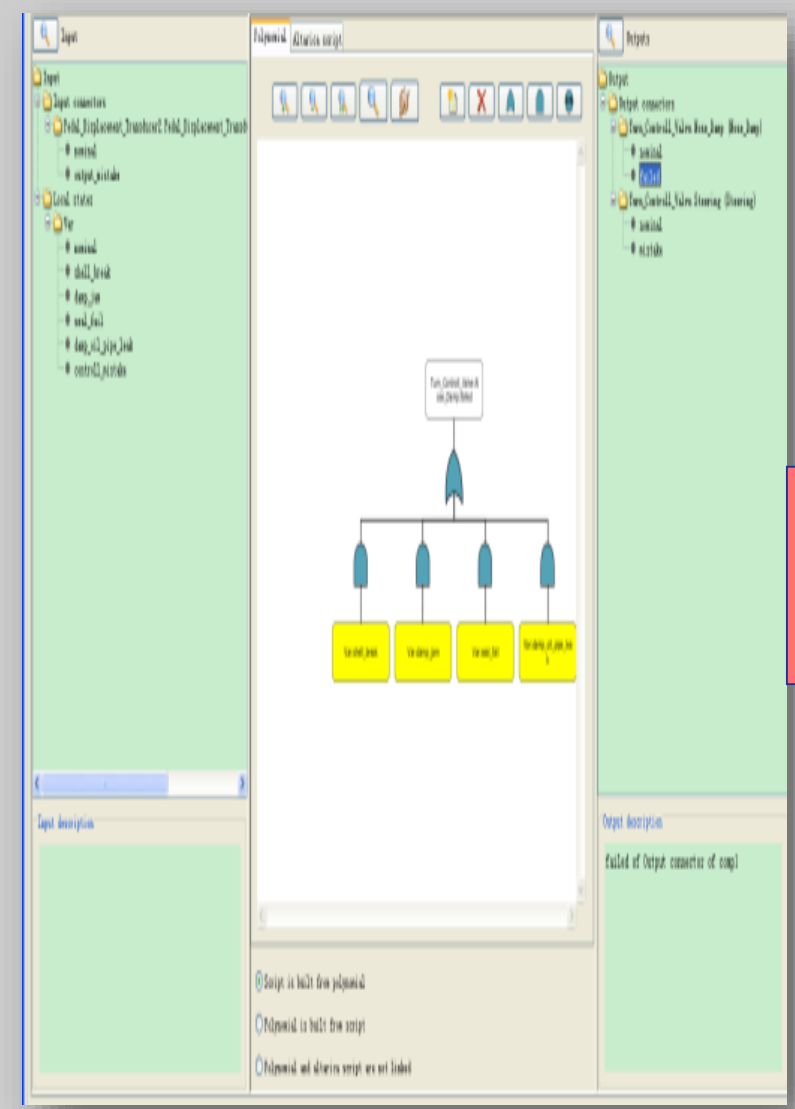
Name	Failure condition	Effects
Steering control valve	The pressure relief valve in the closed position	nose wheel pressure relief function loss, load increase while wheel under lateral impact
	Error control	Non directive deflection
	The damping valve obstruction or oil leakage, anti swing valve seal failure, shell rupture	the nose wheel shimmy function loss
	Steering control component failure, servo valve fault, compensator pressure retaining valve blocked in the closed position, the valve seal failure	loss of active steering function
	Servo valve coil or solenoid valve spring failure	loss of freedom steering function
Steering control component	Steering control circuit or the information path fault	loss of active steering function
	The pedal Steering control circuit failure	loss of the pedal steering function
	Steering control logic fault	steering not accurate, excessive or insufficient, increase the burden on the staff
Steering hand wheel	the line fault	lost hand steering
	Steering control component performance decline	hand steering lack of precision, increase the burden on the staff
Steering feedback sensor	No signal	loss of active steering function
	Error signal	steering not accurate, excessive or insufficient, increase the burden on the staff

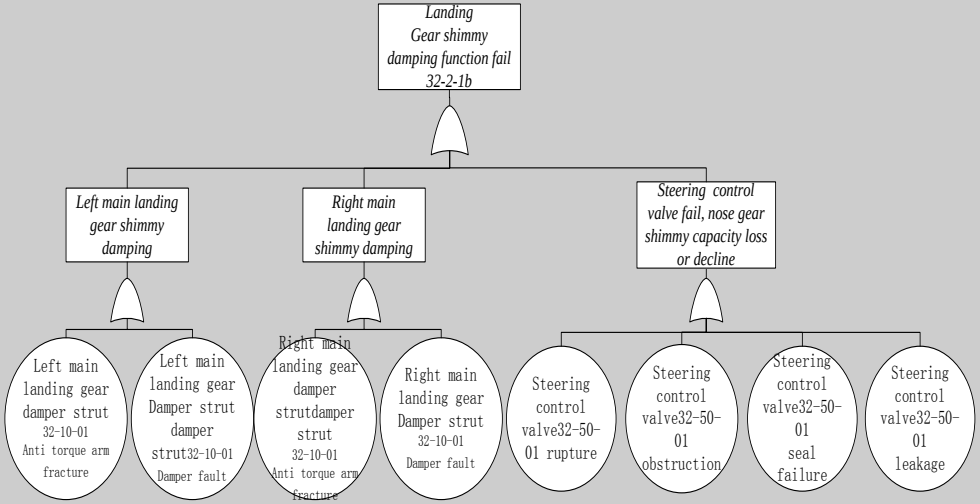
Case study

Name	Failure condition	Effects
Steering control valve	The pressure relief valve in the closed position	nose wheel pressure relief function loss, load increase while wheel under lateral impact
	Error control	Non directive deflection
	The damping valve obstruction or oil leakage, anti swing valve seal failure, shell rupture	the nose wheel shimmy function loss
	Steering control component failure, servo valve fault, compensator pressure retaining valve blocked in the closed position, the valve seal failure	loss of active steering function
	Servo valve coil or solenoid valve spring failure	loss of freedom steering function
Steering control component	Steering control circuit or the information path fault	loss of active steering function
	The pedal Steering control circuit failure	loss of the pedal steering function
	Steering control logic fault	steering not accurate, excessive or insufficient, increase the burden on the staff
Steering hand wheel	the line fault	lost hand steering
	Steering control component performance decline	hand steering lack of precision, increase the burden on the staff
Steering feedback sensor	No signal	loss of active steering function
	Error signal	steering not accurate, excessive or insufficient, increase the burden on the staff



Case study





CAPE

Case study

- The model is not the system function model but the fault model, that is to say, the model is based on the system architecture, and but not to inject fault in the real system or function model that simulates the real system, so there is the likely to presence of deviation between fault models and the real situation;
- The MBSA case gives in this paper needs a lot of detailed design information in the modeling process, so it is difficult to carry it out in the early, and its superiority is very difficult to reflect;
- Preparation of MBSA was based more on historical data and engineering experience to complete and the input can affects the accuracy of the model, for example, the equipment failure modes is the input of MBSA, if we cannot fully find out all the failure modes, the model we built is not accuracy any more.

Thank You !

www.cape.cn