

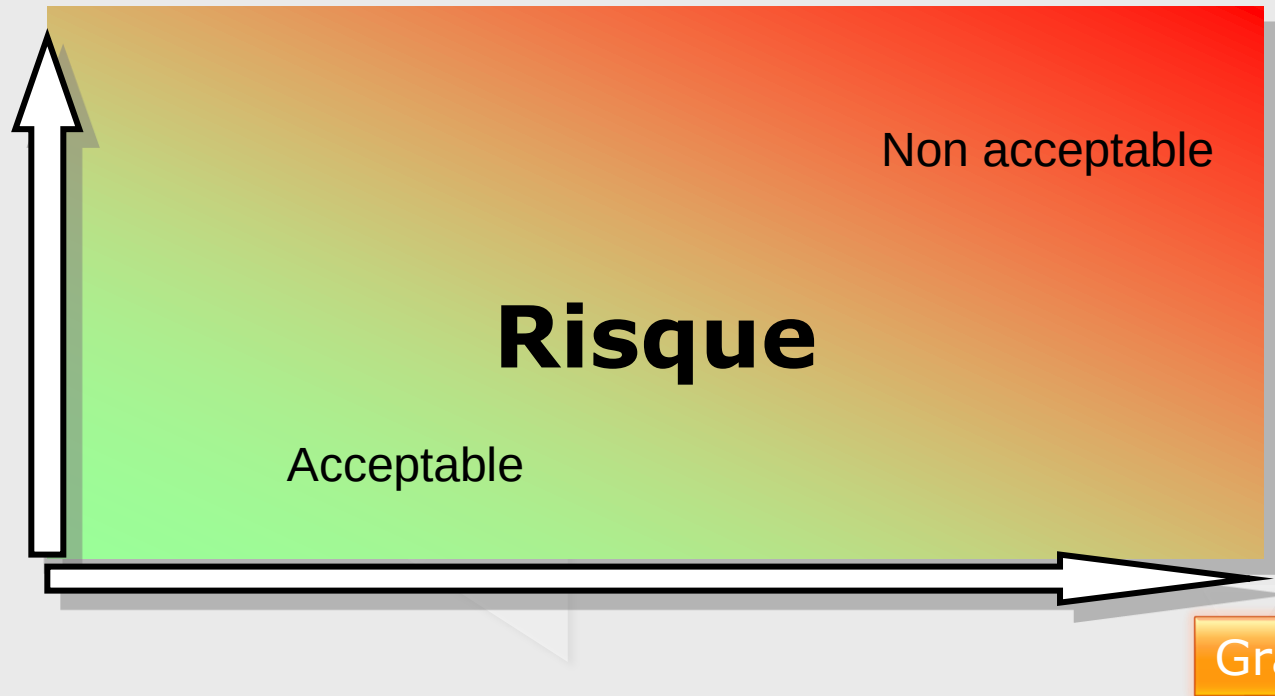
► Contexte automobile et aéronautique



AUTOMOTIVE	AERONAUTICS
Not controllable environment	Managed environment ATC/ ATM
Basic skills required (driving license)	Skilled and trained operators
Not obligatory V2V interaction	Collision avoidance system/ process
Increased and not predictable complexity	Not complex operating situation
Low speeds <300km	Low & High speeds
« Fail safe » failure	« Fail operational » during flight
Obligatory maintenance process mainly on national level	Strict international maintenance protocol
The operation is performed by individuals	Mainly airline companies as operators
Absent or limited state of art	Recorded in detail state of art
Most of safety activities are not imposed by law	The safety process is verified and conformed with national laws

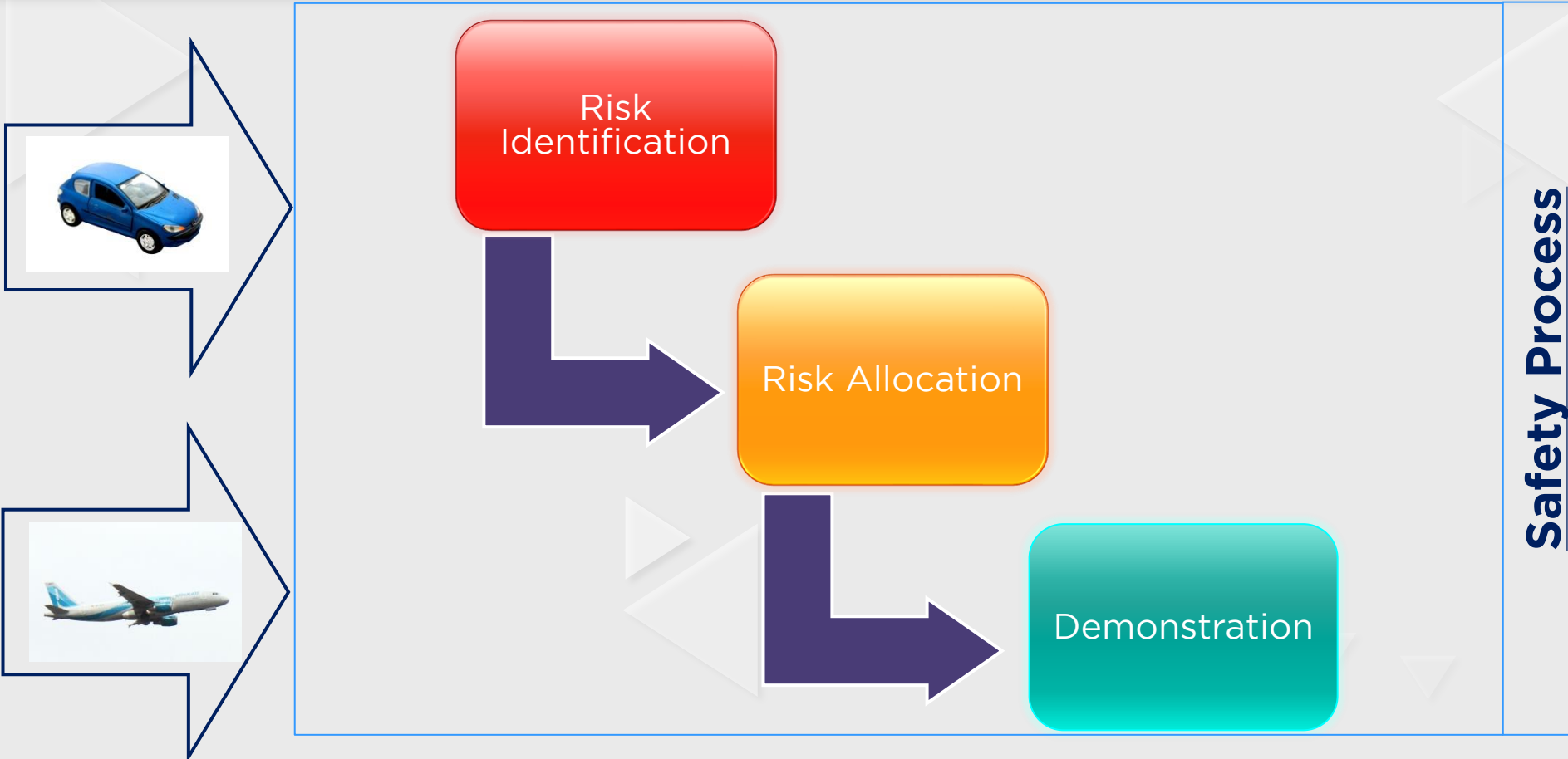
► Qu'est ce que le risque ?

Probabilité



Gravité

▶ Principe démarche sécurité



▶ De quelle sécurité parle t'on ?

Sécurité Active



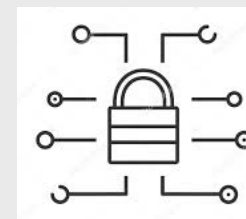
Sécurité Passive



Sécurité Fonctionnelle



Cybersécurité



SOTIF



► De quelle sécurité parle t'on ?

Sécurité Fonctionnelle



Cybersécurité



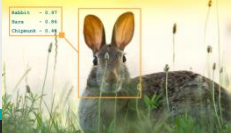
SOTIF



 **Panne Aléatoire**

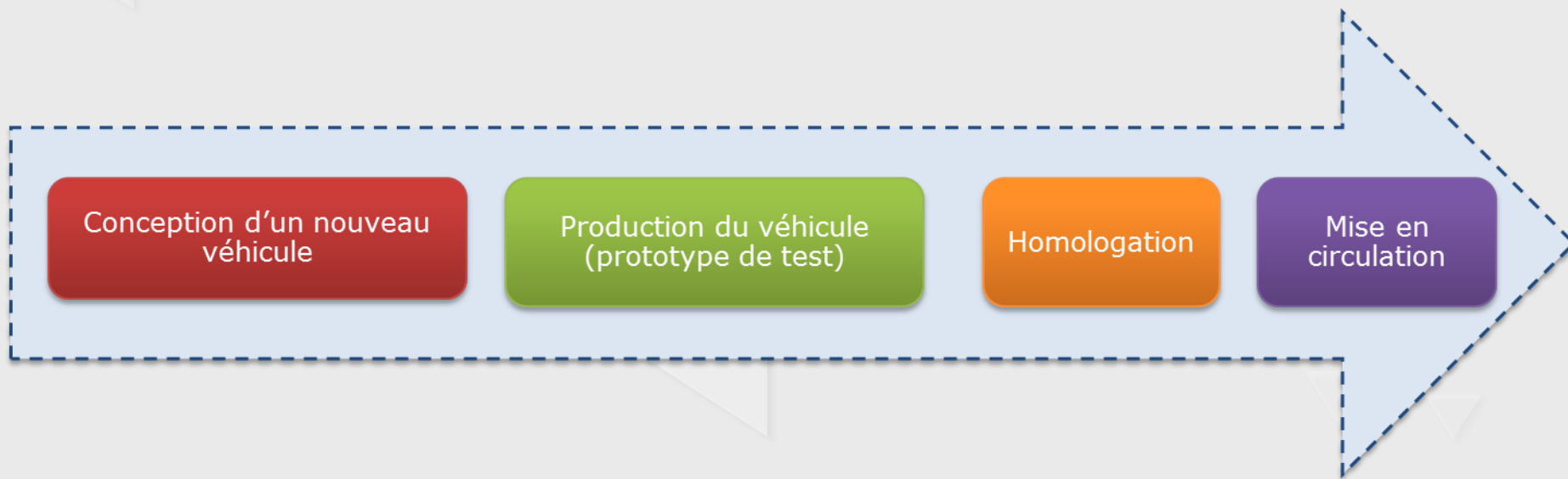
 **Facteur Humain**

 **Panne Systématique**

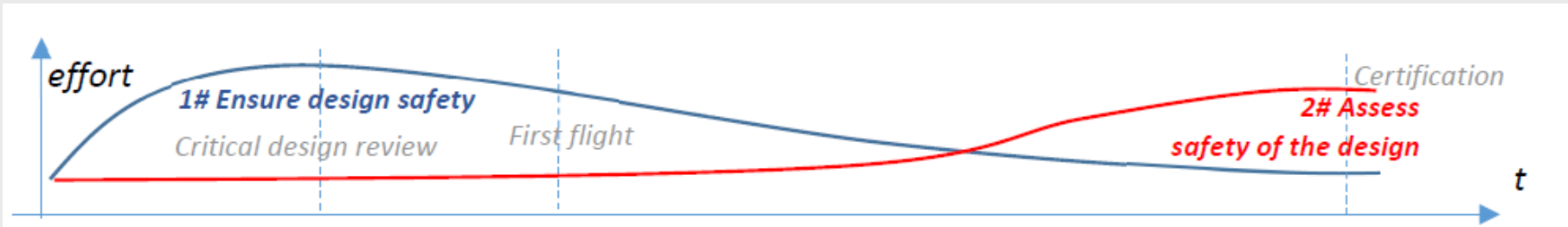
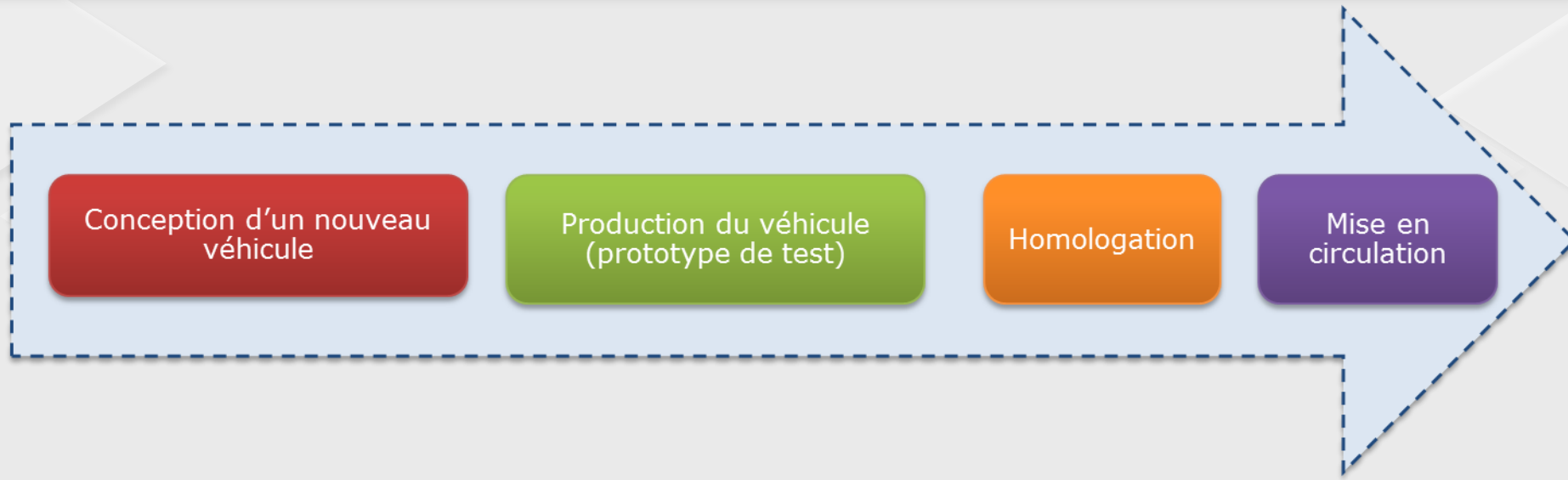
 **Limitation Technologies**

HOMOLOGATION, CERTIFICATION & RÈGLEMENTATION

- ❖ L'homologation, la certification et la réglementation démarre dès les premières étapes de conception, jusqu'à la mise en circulation et l'exploitation.

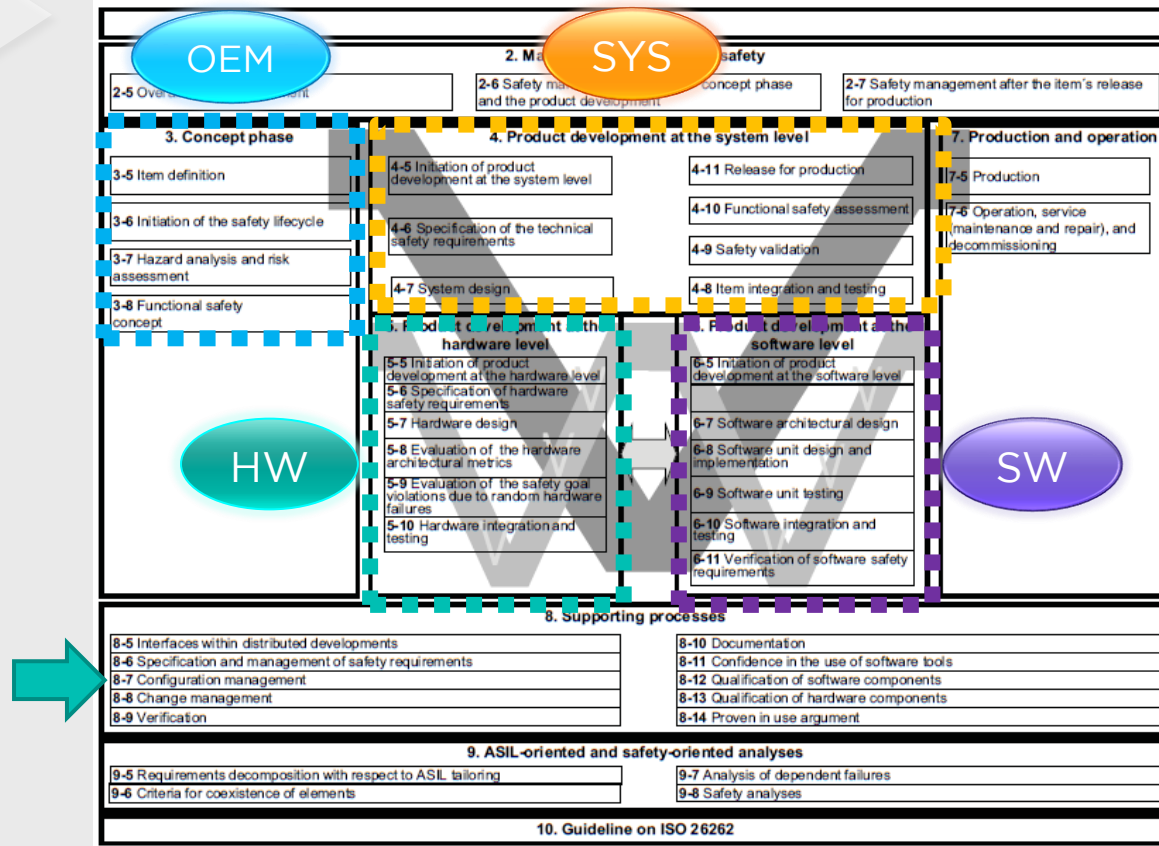


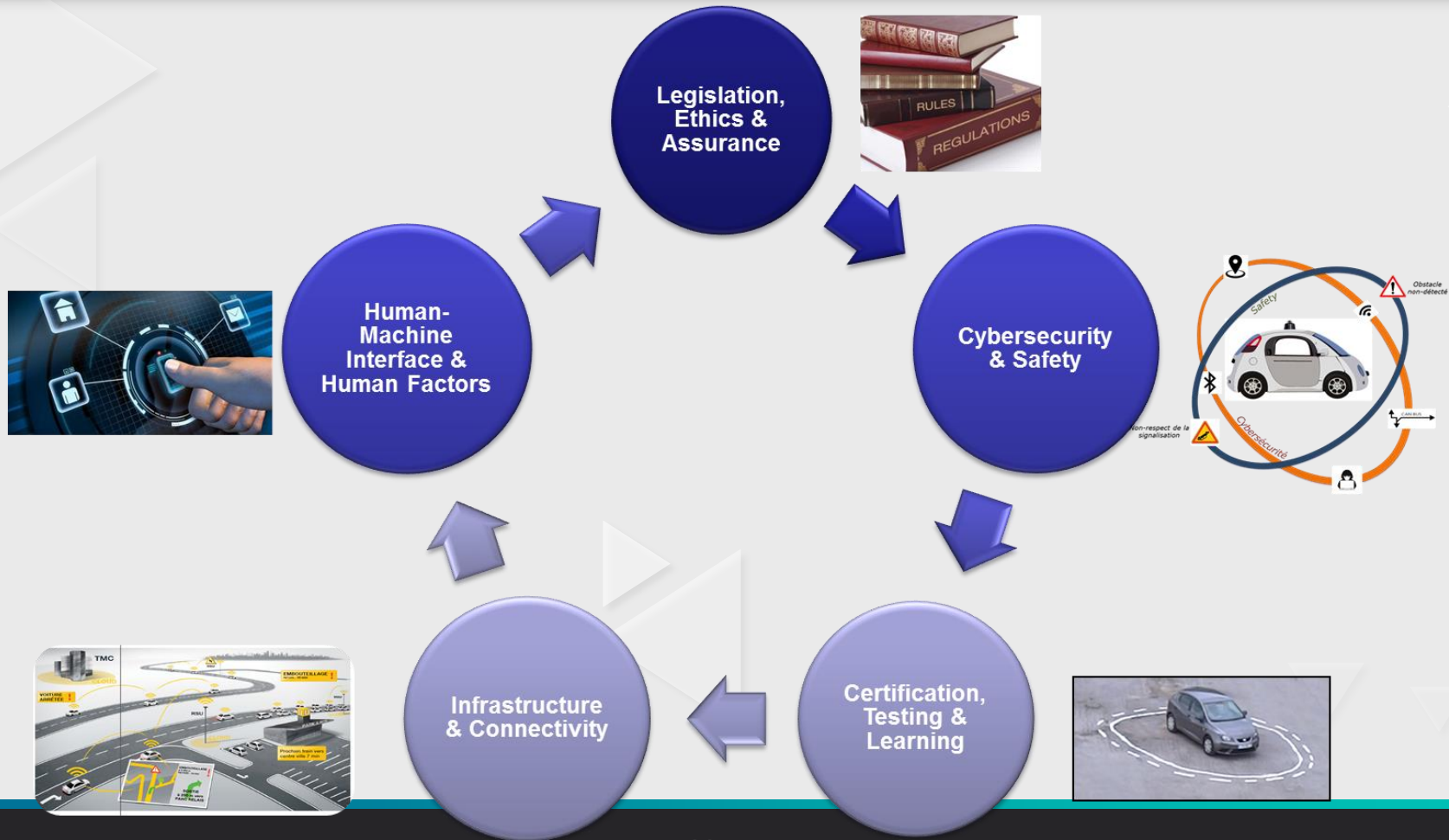
► La « fonction sécurité »



► La « fonction sécurité »

Obj.	Fail	Failure of Safety function (TLF)	Failure effects and criticality
#1	#1-1	Failure to define / verify all requirements needed for A/C safety <i>(missing or poorly defined requirement, or incomplete verification)</i>	Worst case: aircraft is not safe at Certification or EIS <i>(partial safeguard: design teams also analyze the design)</i>
#1	#1-2	Definition of too restrictive requirements regarding A/C safety	A/C is unnecessarily too expensive or its development is delayed <i>(economic impact only)</i>
#2	#2-1	Failure to assess and document the design safety <i>(assuming the design itself is safe)</i>	A/C Certification / EIS is delayed due to rejection by authorities <i>(economic impact only)</i>
#3	#3-1	Failure to support properly the modeling description required by other teams <i>(no answers or inappropriate answers to questions or requests)</i>	Design is driven towards poor choices, or design team has to perform Safety function work on its own to reach correct answers.





<https://www.youtube.com/watch?v=xsQvq4WIUYU>

CONTACTS



Frédéric Deschamps

Frederic.deschamps@lgm.fr

+33750617955

