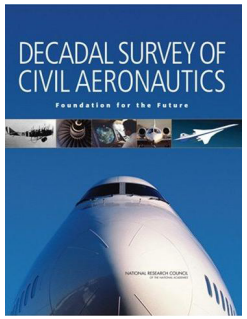
Advanced Software V&V for Civil Aviation and Autonomy

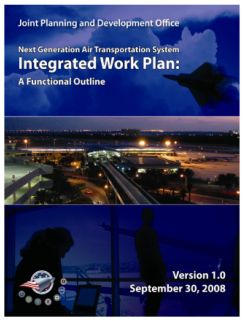
Dr. Guillaume Brat

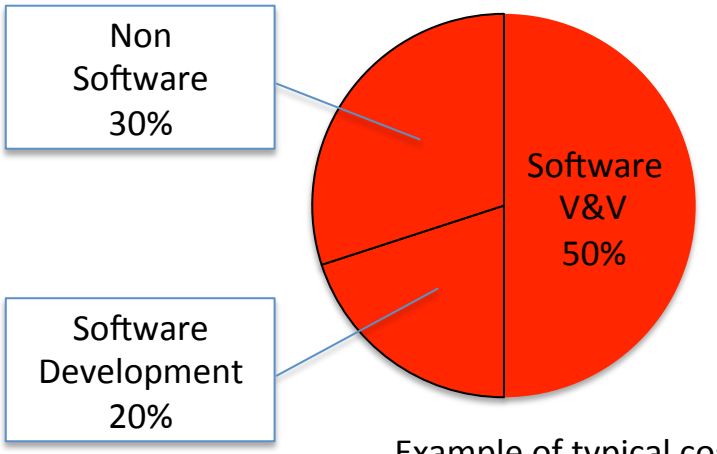
NASA Ames Research Center

Motivation for V&V research



The Decadal Survey for Civil Aeronautics and the NextGen Integrated WorkPlan both call for more research on the validation and verification of complex systems

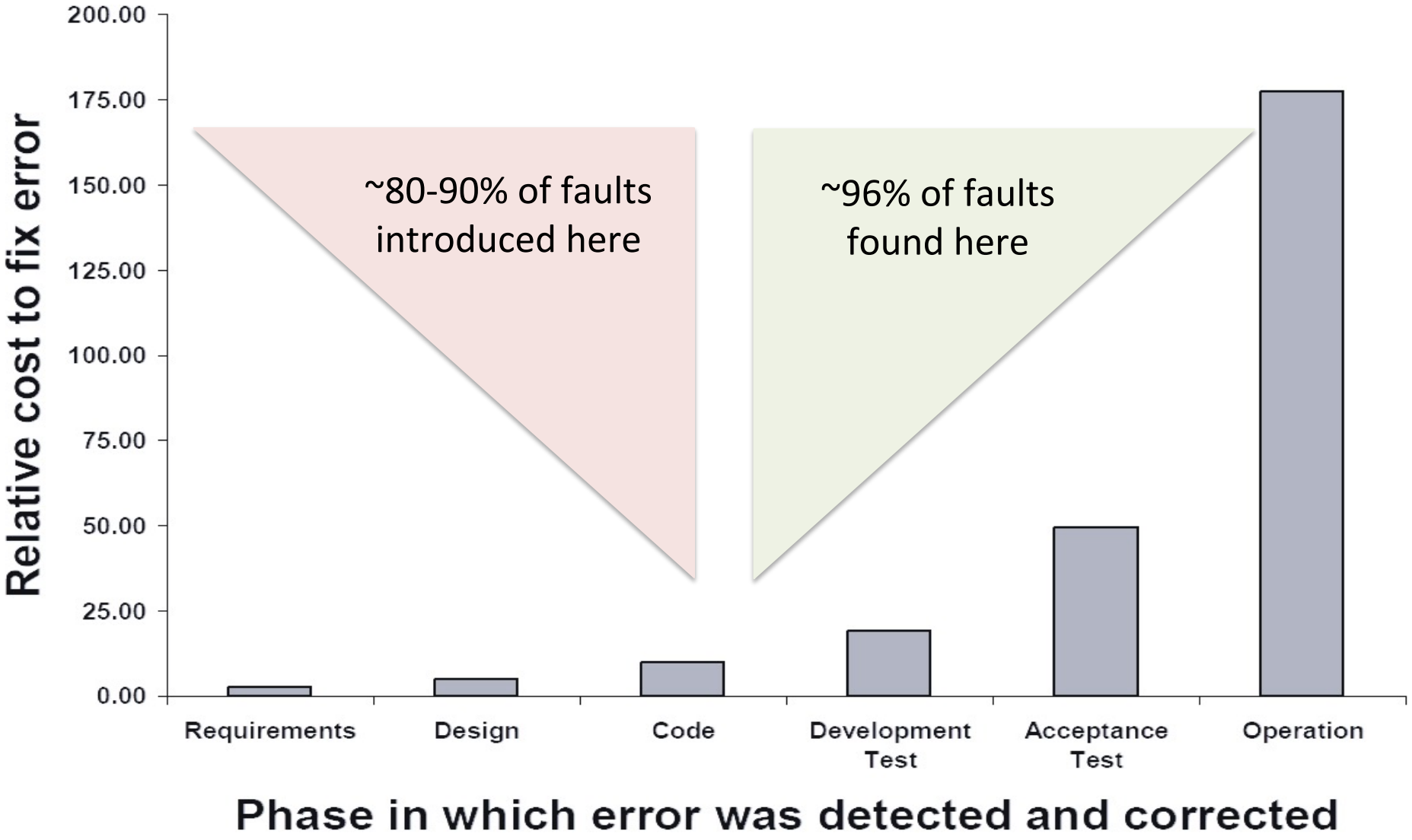




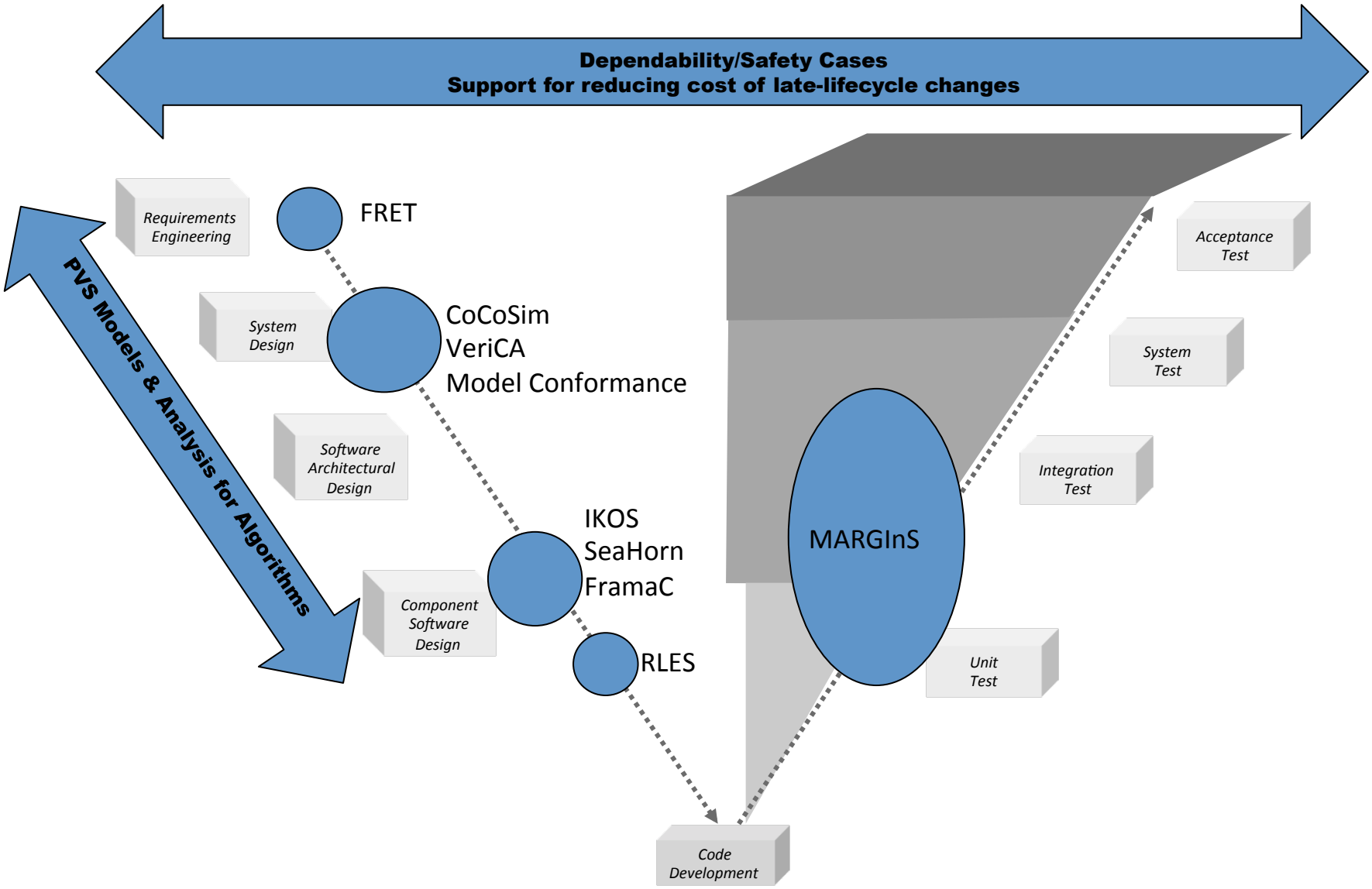
Example of typical cost in Aviation

- Software costs are very high
- V&V cost is 40-50% of the SW cost
- Driven by certification requirements

Reasons for the high cost of S/W



Areas addressed by NASA tools



Current V&V Tools and Capabilities

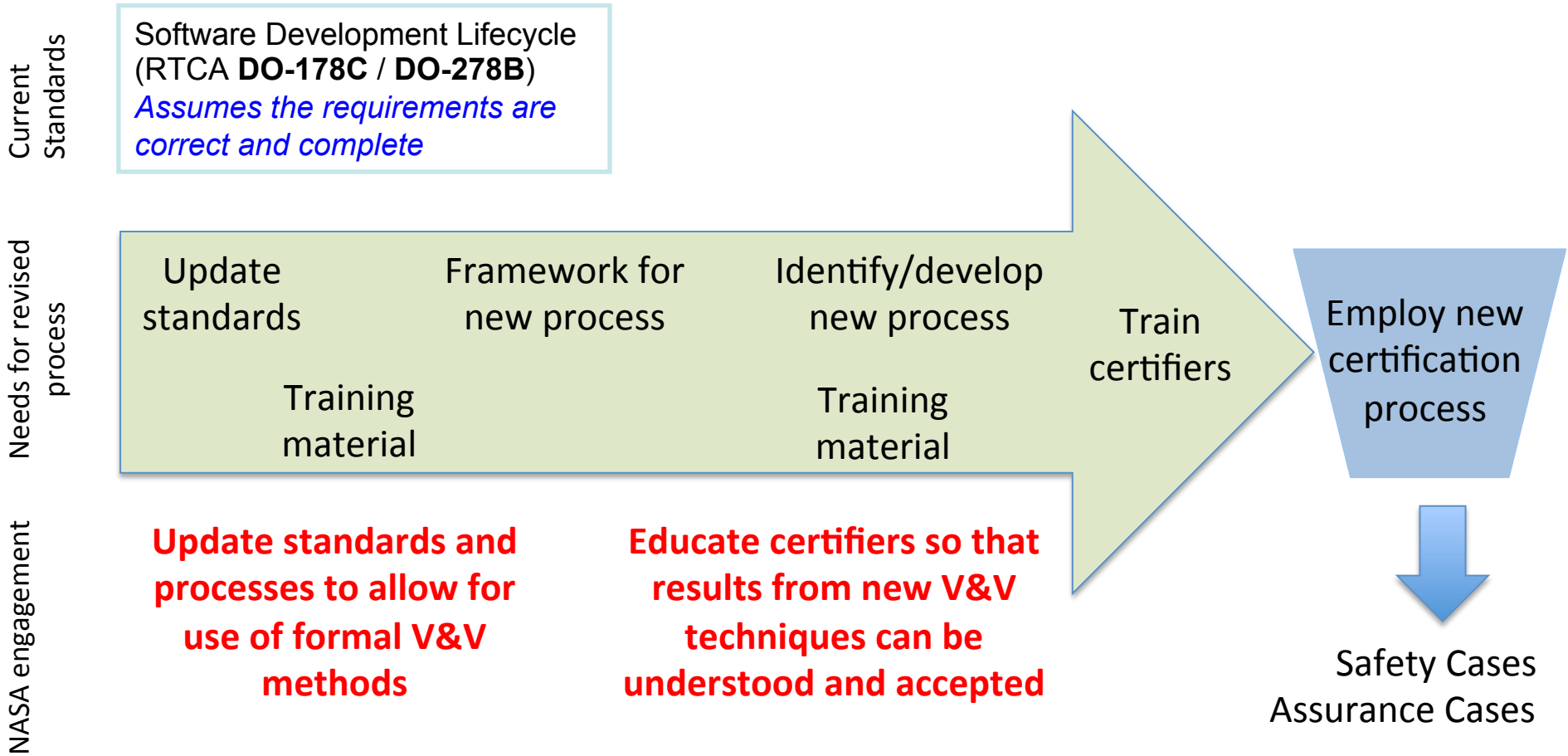
Requires theorem prover expertise	Combination of formal method with control theory experts	Accessible to moderate/ expert programmer	Requires proficiency in statistics	EXPERTISE
PVS	Simulink, C, Stateflow	C limited C++	blackbox	TARGET
Algorithmic proofs using theorem proving	Model checking for checking/ guaranteeing safety requirements	Static code analysis for run-time errors and safety requirements	Statistical-based testing to learn unsafe boundaries of operation	CAPABILITY

Requirements — Design — Code — Testing — Operation

Future V&V Tools and Capabilities

	Requirements	Design	Code	Testing	Operation
EXPERTISE	Accessible to engineers	Accessible to engineers	Accessible to programmer	Requires proficiency in statistics	
TARGET	English-like	SCADE MatLab	Full C++ Floating-point analysis	blackbox	
CAPABILITY	Requirement capture and analysis	Checking/ guaranteeing safety requirements on design models	Static code analysis for run-time errors	Statistical-based testing to learn unsafe boundaries of operation	

FAA/Regulator Needs



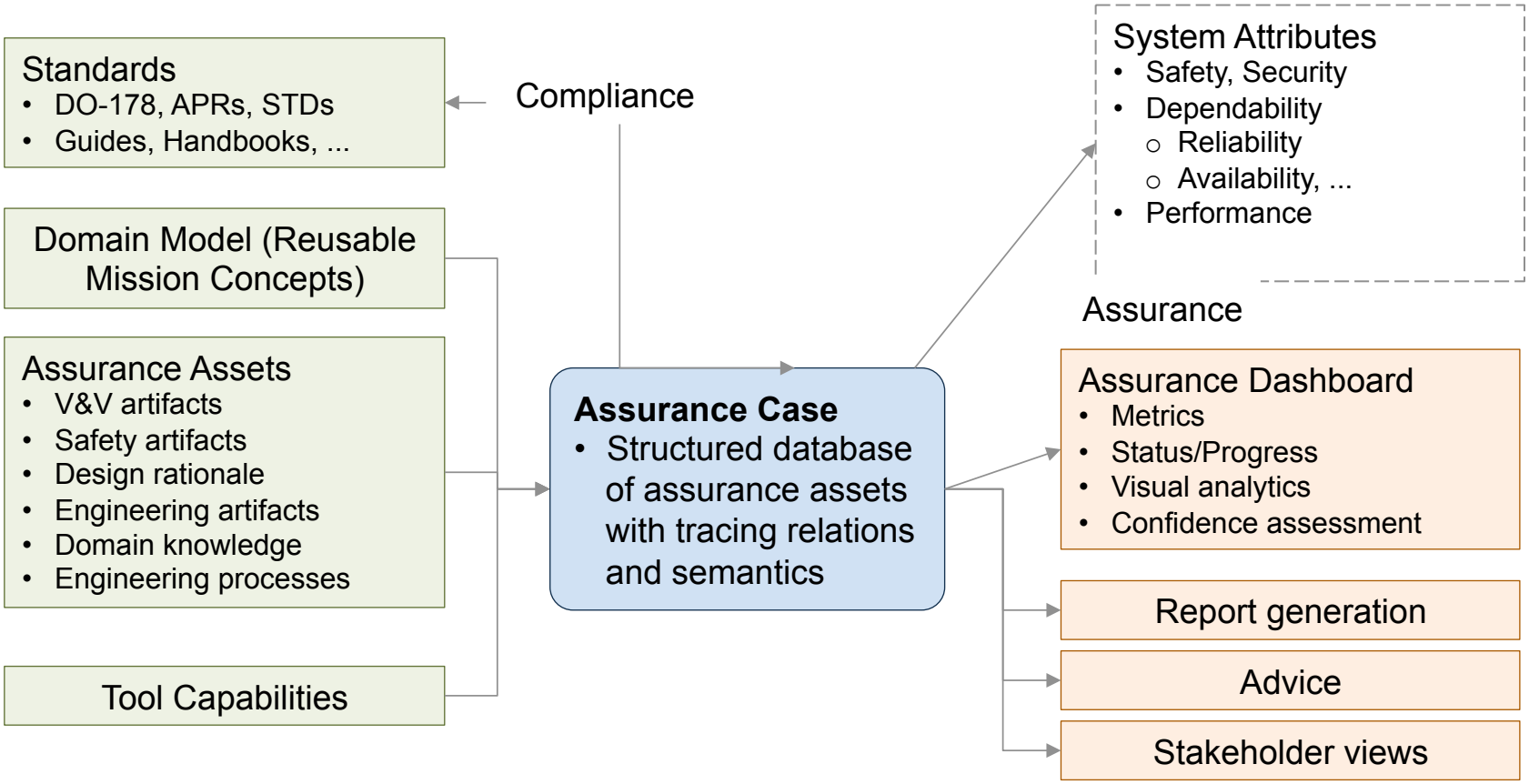
Assurance Cases

- An *assurance case* is
  - A set of assurance claims connected to a body of **evidence** through a structured argument, to provide a comprehensive, defensible and valid justification that **a system meets its assurance requirements** for a given application in a defined operating environment

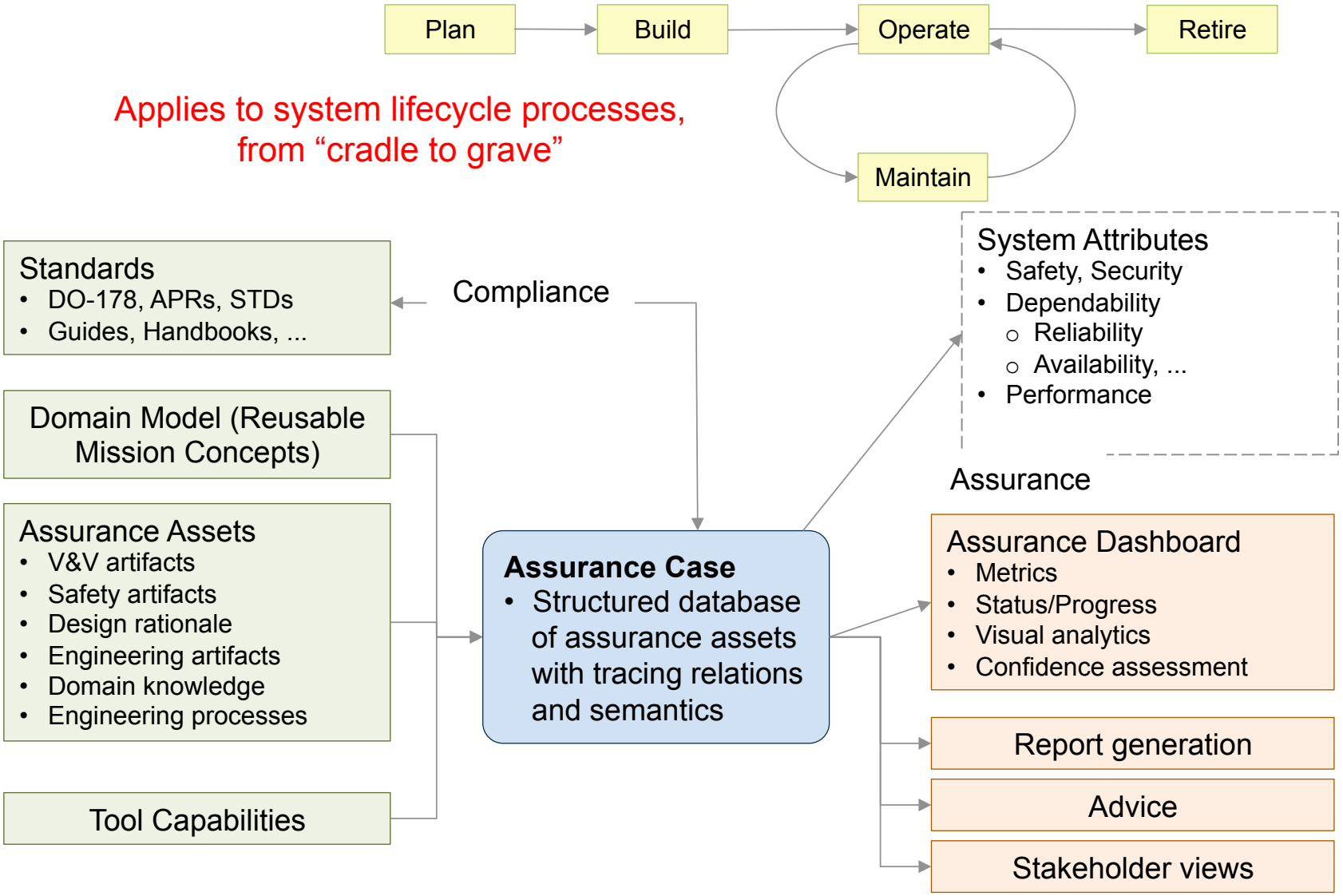
Assurance Case
- Structured database of assurance assets with tracing relations and semantics

  - A means for integrating safety and mission assurance (S&MA) information.

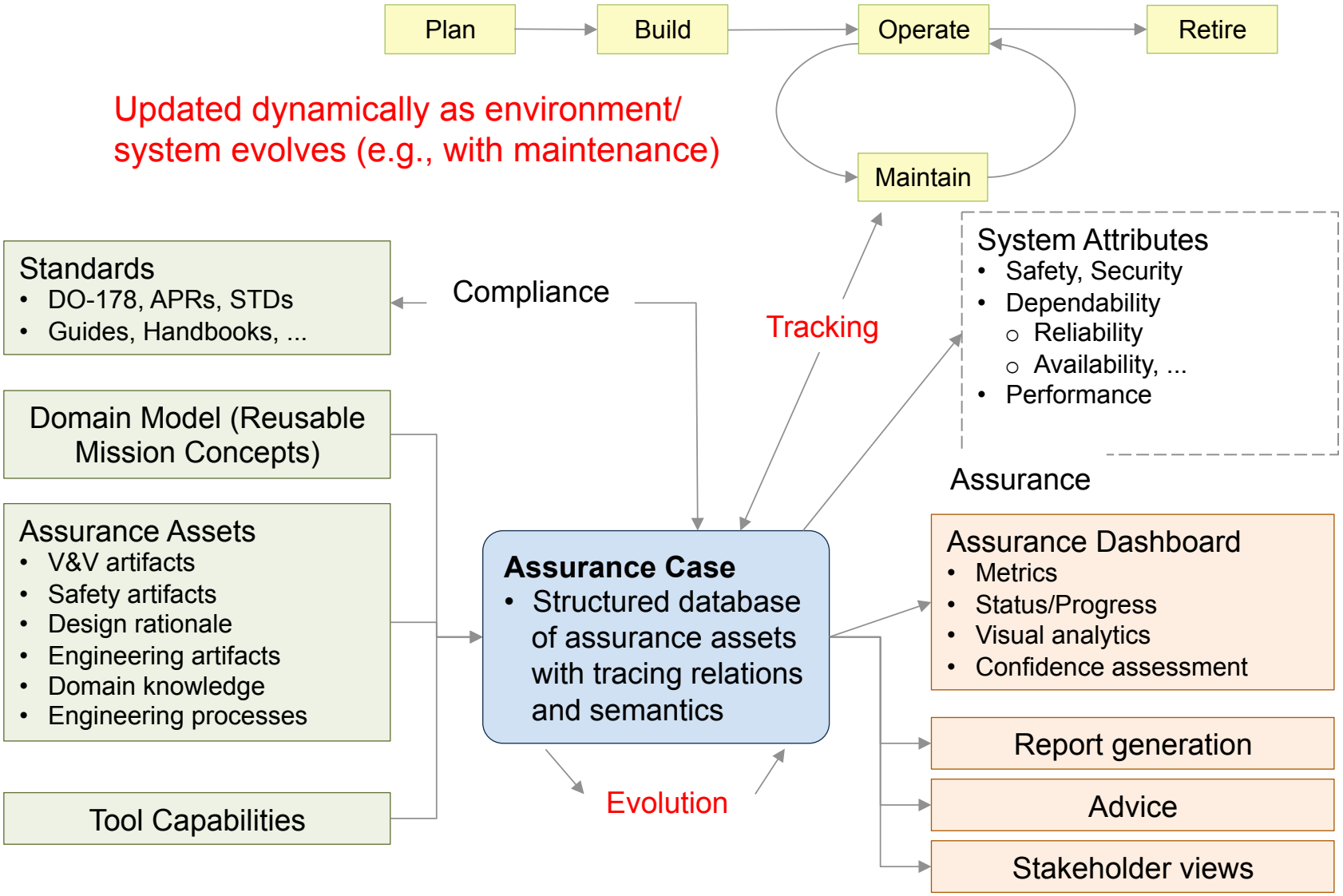
Assurance Cases



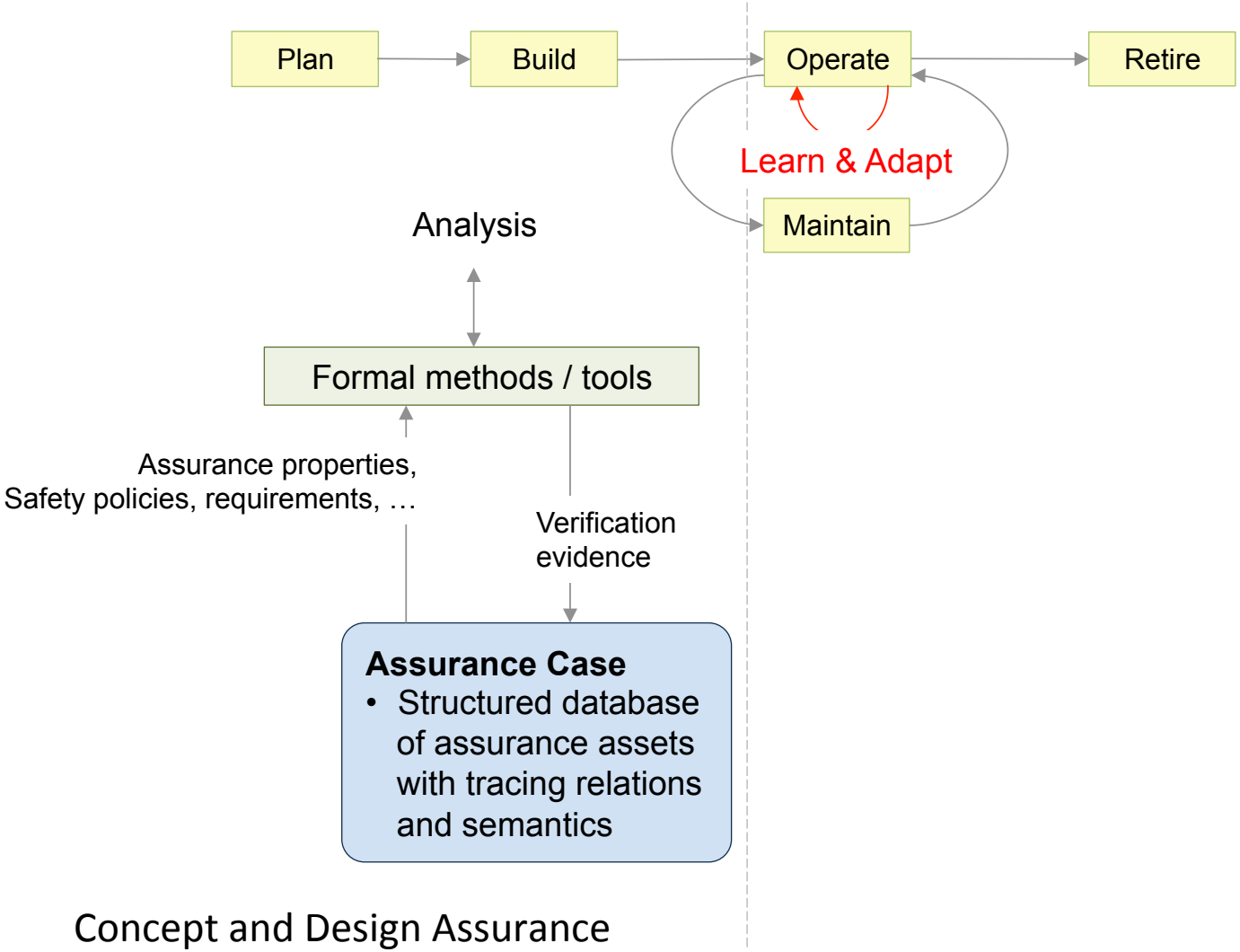
Assurance Cases and Lifecycle



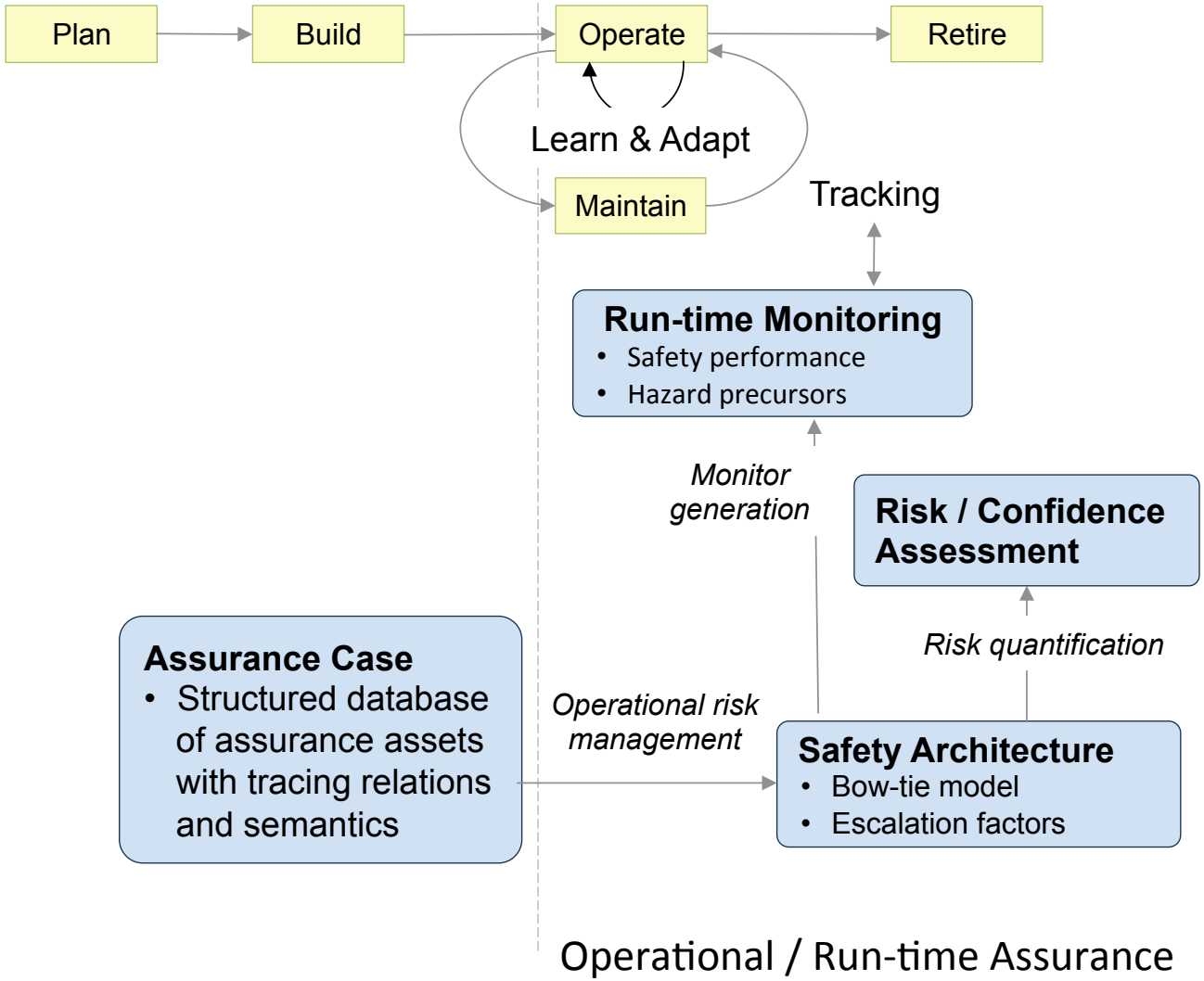
Assurance Cases and Lifecycle



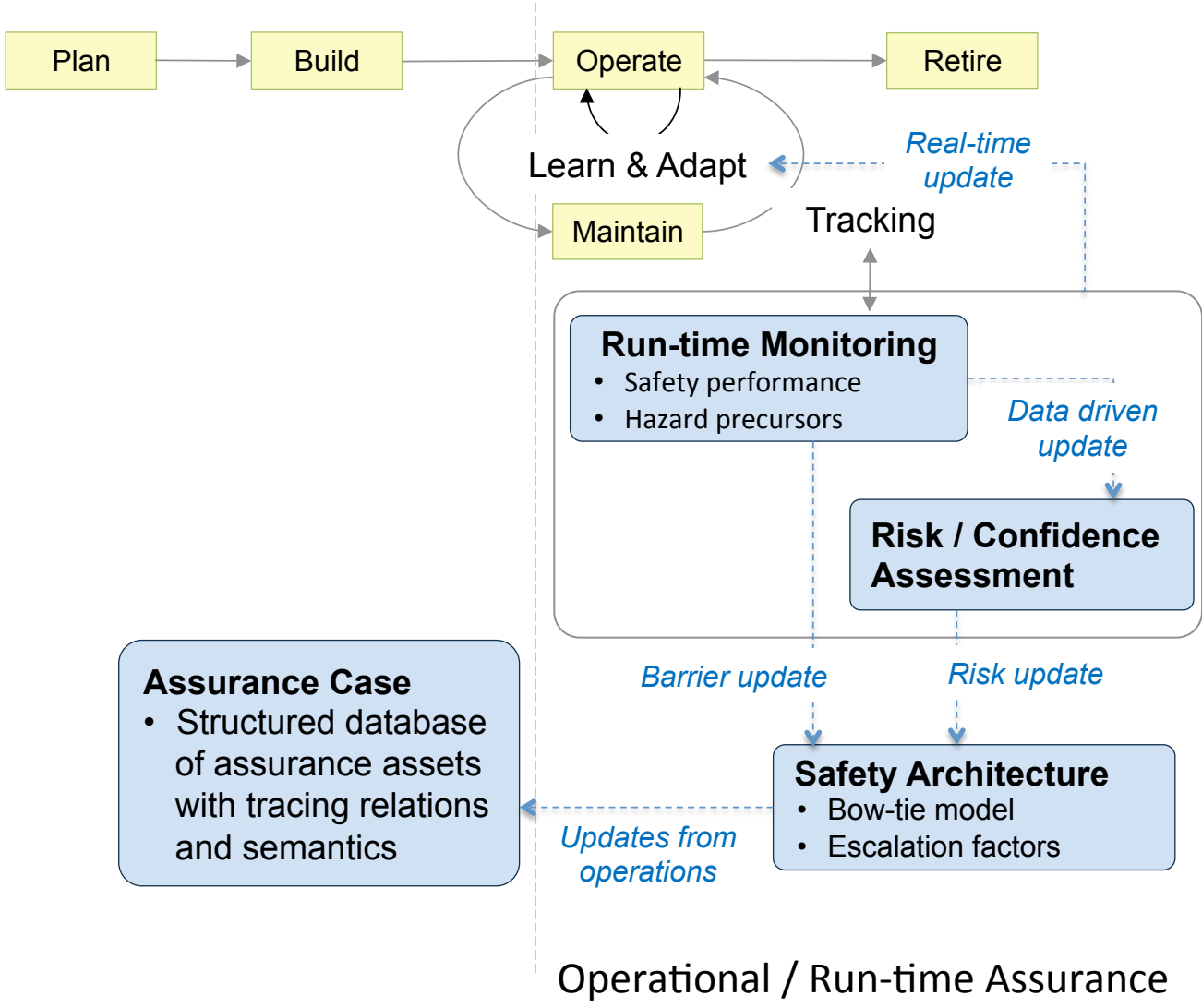
Assurance Cases and Autonomy



Assurance Cases and Autonomy

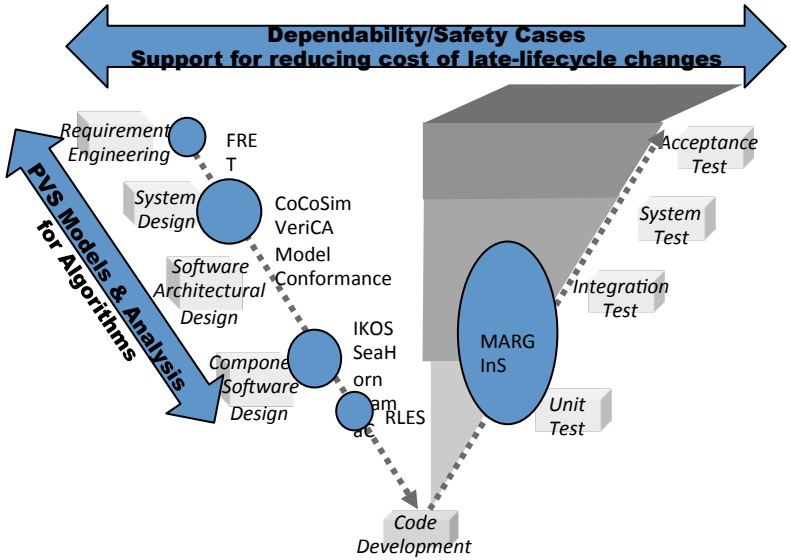


Assurance Cases and Autonomy



Conclusions

- **Goal**: Address the impact of V&V of overall cost of S/W for aviation
- **Solution**: Bring V&V earlier in the lifecycle by using formal methods
- **Status**: Prototype tools for all phases
  - Requirement tool is in its infancy



- **Innovation**: gather V&V evidences in assurance cases that extend throughout the lifecycle
- **Future**: Address V&V of autonomy through the use of assurance cases at runtime