DEPS - A FORMAL MODELING LANGUAGE FOR SYSTEM ARCHITECTURE SYNTHESIS

Laurent Zimmer & Pierre-Alain Yvars
Dassault Aviation SupMéca–Quartz

AGENDA

- SYSTEMS & MODEL-BASED SYSTEM ENGINEERING
- DEPS PROJECT
- CASE STUDY
- CONCLUSION
- FUTURE WORK

SYSTEMS
&
MODEL-BASED
SYSTEM ENGINEERING

SYSTEMS

SYSTEMS ARE EVERYWHERE, OF ANY KIND AND IN EVERYTHING

They are technical, embedded, real-time, software-intensive, cyber-physical, systems-of-systems

SYSTEMS ARE MORE AND MORE COMPLEX.

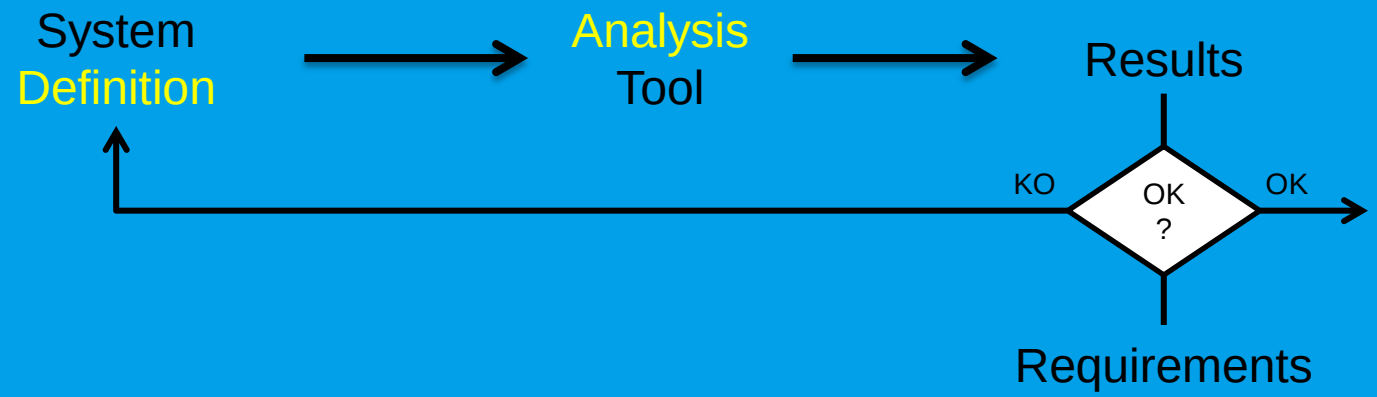
Mastering them requires a dedicated computer assisted engineering e.g.

- Model Driven Engineering (MDE)
- Model-Based System Engineering (MBSE)
- Model-Based System Analysis (MBSA)
- Model-Based System Safety Assessment (MBSSA) ...

MBSE

STATE-OF-THE-ART OF MBSE:

- Modeling languages to share a common system definition (UML, SysML, AADL...)
- Analysis software tools to simulate, check, verify …



MBSE

CURRENT LIMIT OF MBSE

MBSE does not address design problems like:

- System Sizing
- Configuration Setting
- Resource Allocation
- Architectural Synthesis

MBSE

CURRENT LIMIT OF MBSE

MBSE does not address design problems like:

- System Sizing → some design parameters are not fixed
- Configuration Setting → some components are not selected
- Resource Allocation → some resources are not allocated
- Architectural Synthesis → a mix of everything

MBSE

CURRENT LIMIT OF MBSE

MBSE does not address design problems like:

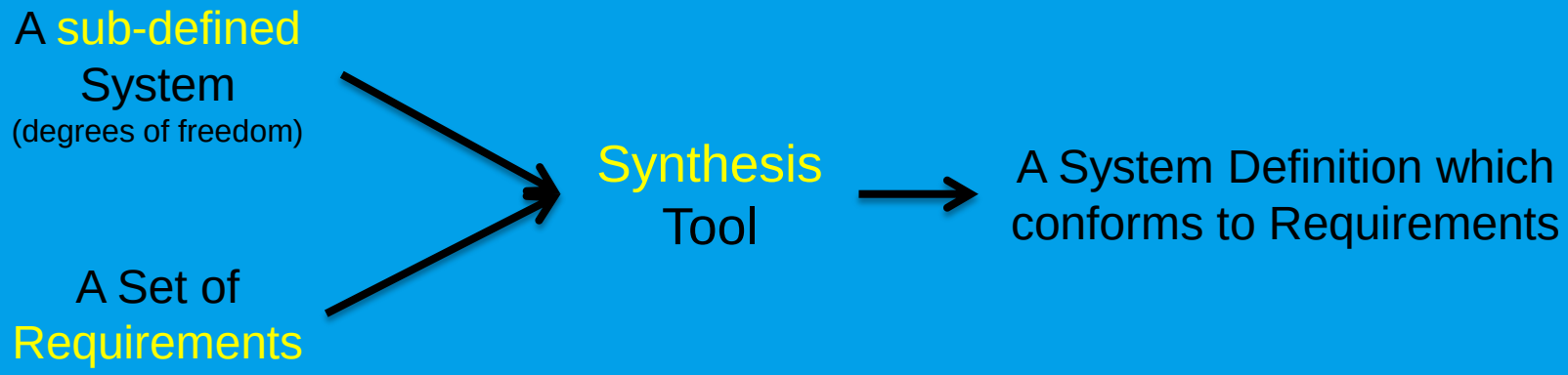
- System Sizing → some design parameters are not fixed
- Configuration Setting → some components are not selected
- Resource Allocation → some resources are not allocated
- Architectural Synthesis → a mix of everything

- A system to be designed is sub-defined
- Solving a design problem is completing a sub-defined model

MBSE

MBSE HAS TO BE REVISED TO ADDRESS DESIGN PROBLEMS

A Design Problem is a matter of synthesis. We need MBSS instead of MBSA

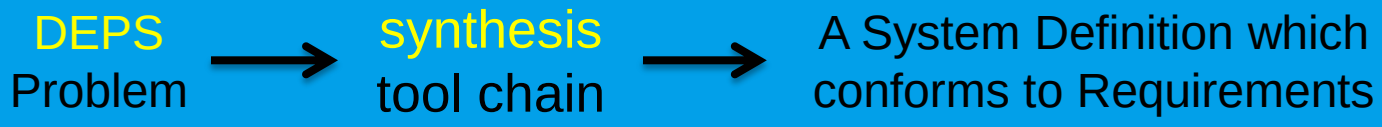


DEPS PROJECT

DEPS PROJECT

GOAL

Specifying DEPS (Design Problem specification) a formal modeling language to set system design problems and developing the related synthesis tool chain to solve them



DEPS PROJECT

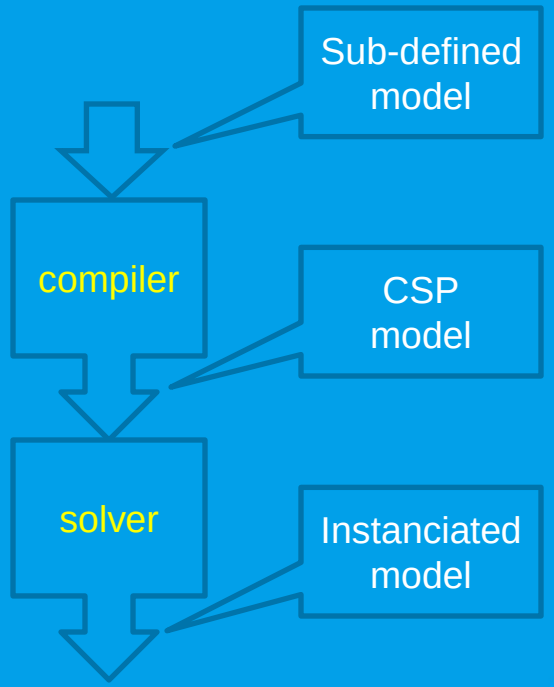
SYNTHESIS TOOL CHAIN:

DEPS COMPILER

- Ahead-of-time with static type checking
- generation of sub-defined model instances with constraints

DEPS SOLVER

- Purpose-built
- Mixed (integer/real) solving capabilities



DEPS LANGUAGE

DECLARATIVE MODEL-BASED LANGUAGE COMBINING:

OBJECT-ORIENTED KNOWLEDGE REPRESENTATION

- Class-instance model, inheritance, composition, aggregation

+

EXPRESSION OF PROPERTIES

- Algebraic equations or inequalities, global constraints

+

ONTOLOGY FOR ENGINEERS

- Quantities, dimensions, units

DEPS LANGUAGE

```
Model Partition ()
Constants
Variables
  icpu: CpuIndex ;
Elements
Properties
End
```

```
Quantity CpuIndex
 Kind : Integer ;
 Min  : 1 ;
 Max : 4 ;
 Unit : u ;
End
```

```
Model segregation (P1, P2)
Constants
Variables
Elements
 P1 : Partition ;
 P2 : Partition ;
Properties
  P1.icpu <> P2.icpu;
End
```

DEPS LANGUAGE

```
Model GasModel (MolarMass)
 Constants
   MolarMass: MolarMass;
 Variables
  Mass: mass;
 Elements
 Properties
End
```

```
Model Tank(p, t, Gas)
 Constants
  R : Real = 8.314 ;
  p : Pressure ;
  t :  Temperature ;
 Variables
  V : Volume ;
 Elements
 Gas : GasModel ;
 Properties
  p*V= (Gas.Mass/Gas.MolarMass)*R*t;
End
```

DEPS LANGUAGE

```
Model Component ()
 Constants
 Variables
  I: intensity ;
 Elements
   P1, P2: Port() ;
 Properties
   P1.I :=  I; P2.I := -I;
End
```

```
Model Resistor(R) extends Component
 Constants
  R : Resistor;
 Variables
 Elements
 Properties
  P1.V-P2.V = R*I;
End
```

CASE STUDY

CASE STUDY

DEPLOYMENT OF AIRCRAFT SYSTEMS ON AN IMA TYPE AVIONICS PLATFORM

The aim is to size the processing capacity of the platform and to generate a correct by construction multi-system deployment.

Deployment constraints issued from a preliminary Safety Analysis have to be expressed in terms of:

- Duplication, triplication … of processing channels, of applications
- Material segregation of resources used by duplicated paths or applications (no common resource!)

CASE STUDY

DEPS MODELING

System

- Aircraft functions:

  processing channels, paths, applications, partitions

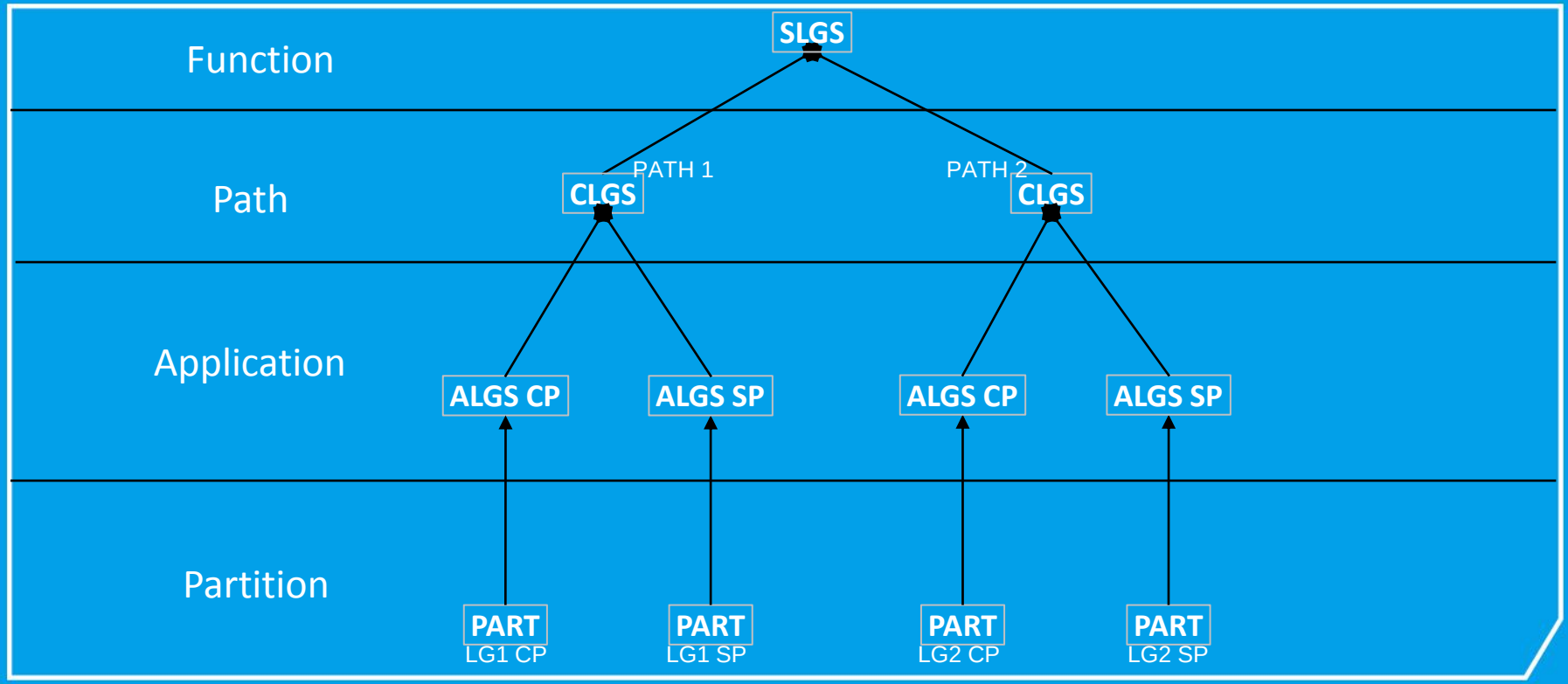
Platform

- Computation modules

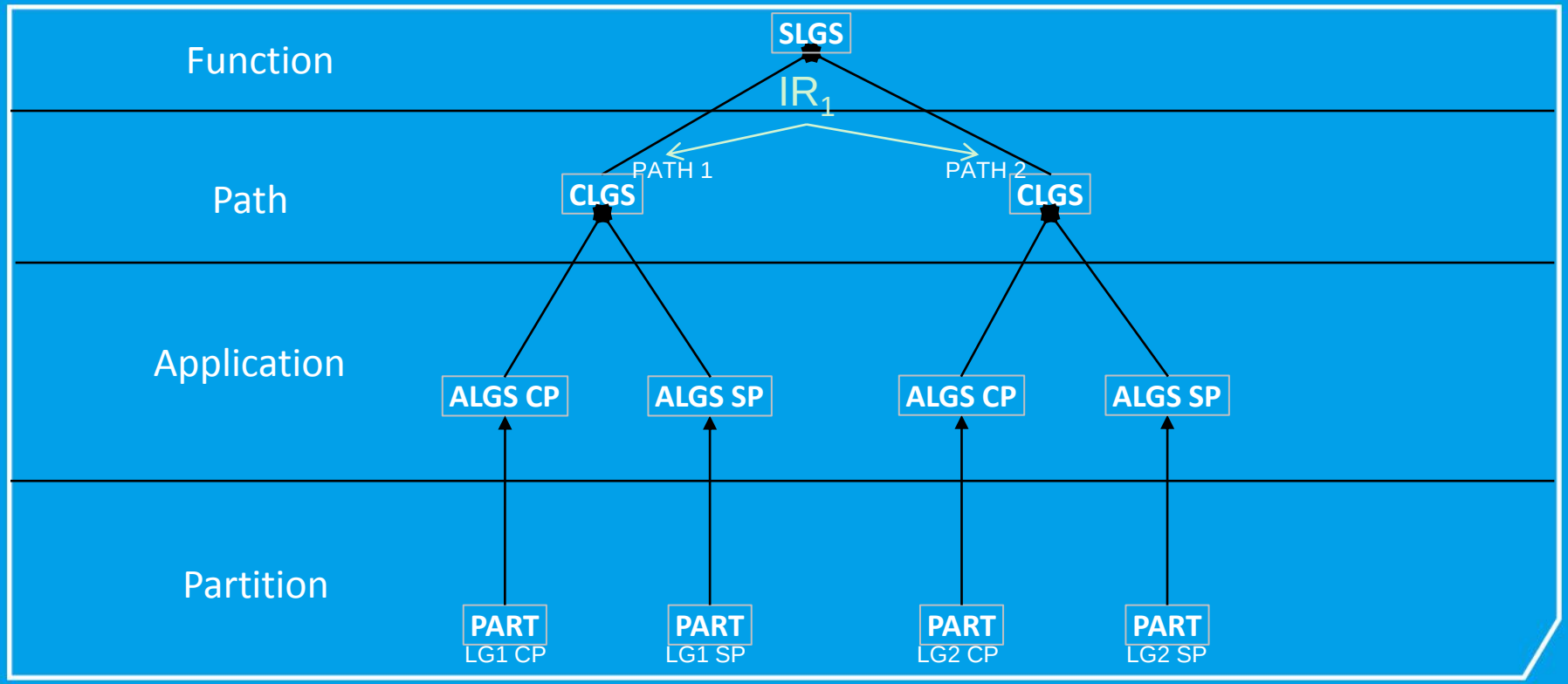
Requirements and constraints

- Safety requirements
- Capacity constraints

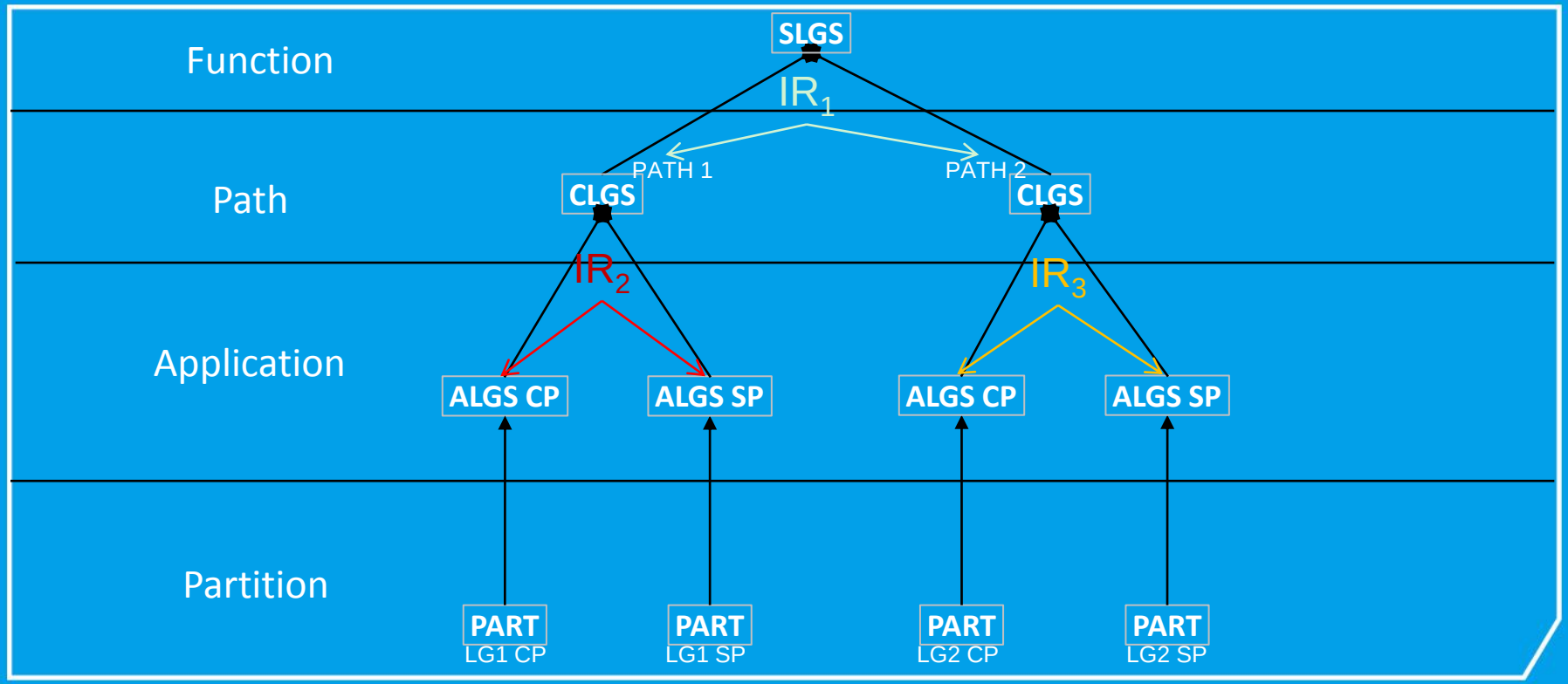
PROBLEM SPECIFICATION



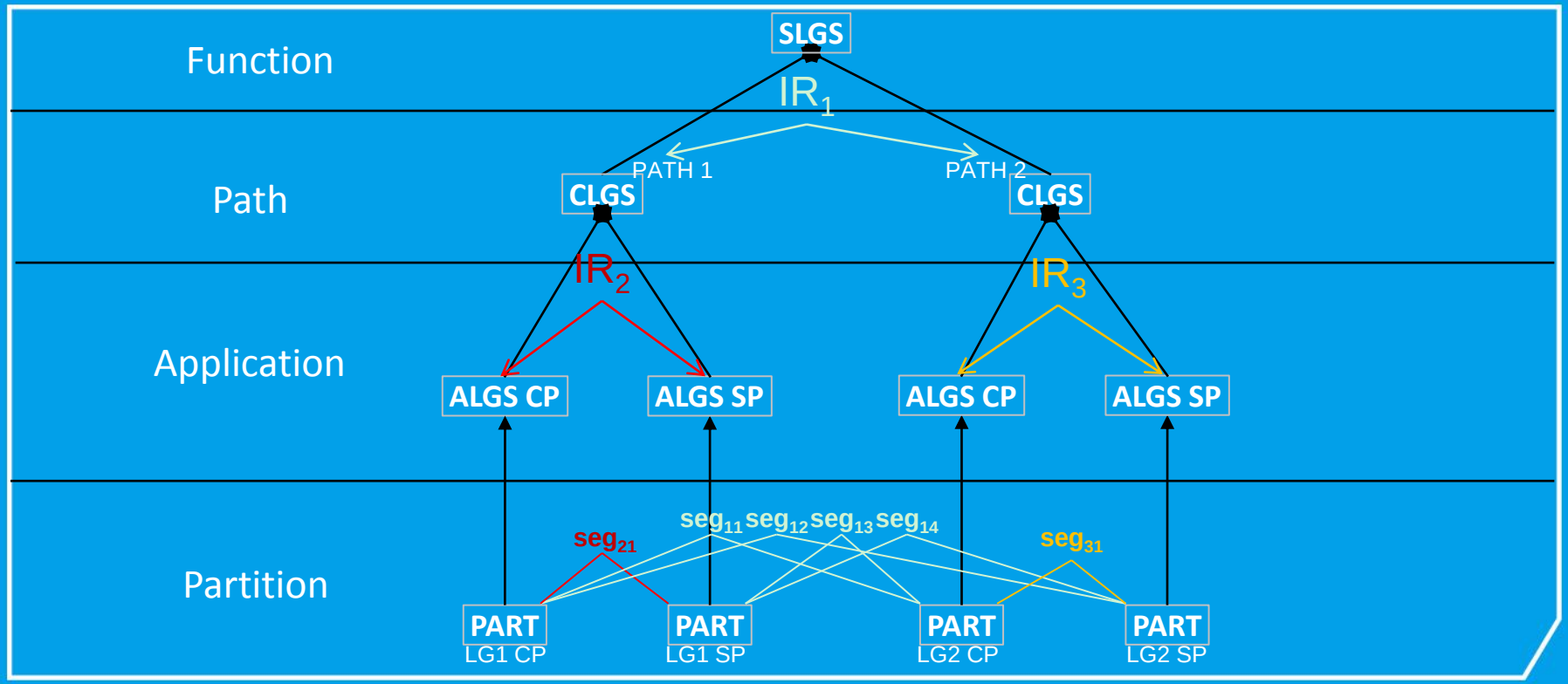
PROBLEM SPECIFICATION



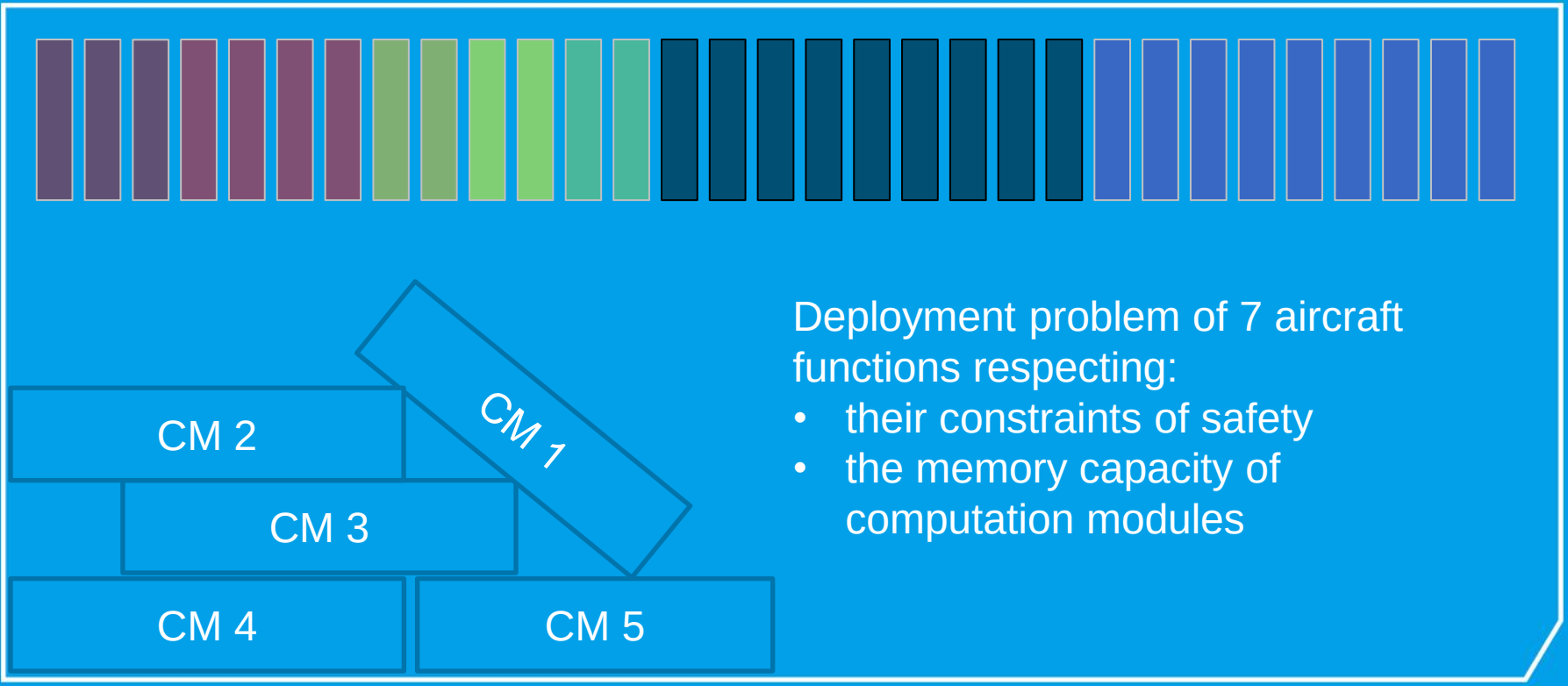
PROBLEM SPECIFICATION



PROBLEM SPECIFICATION



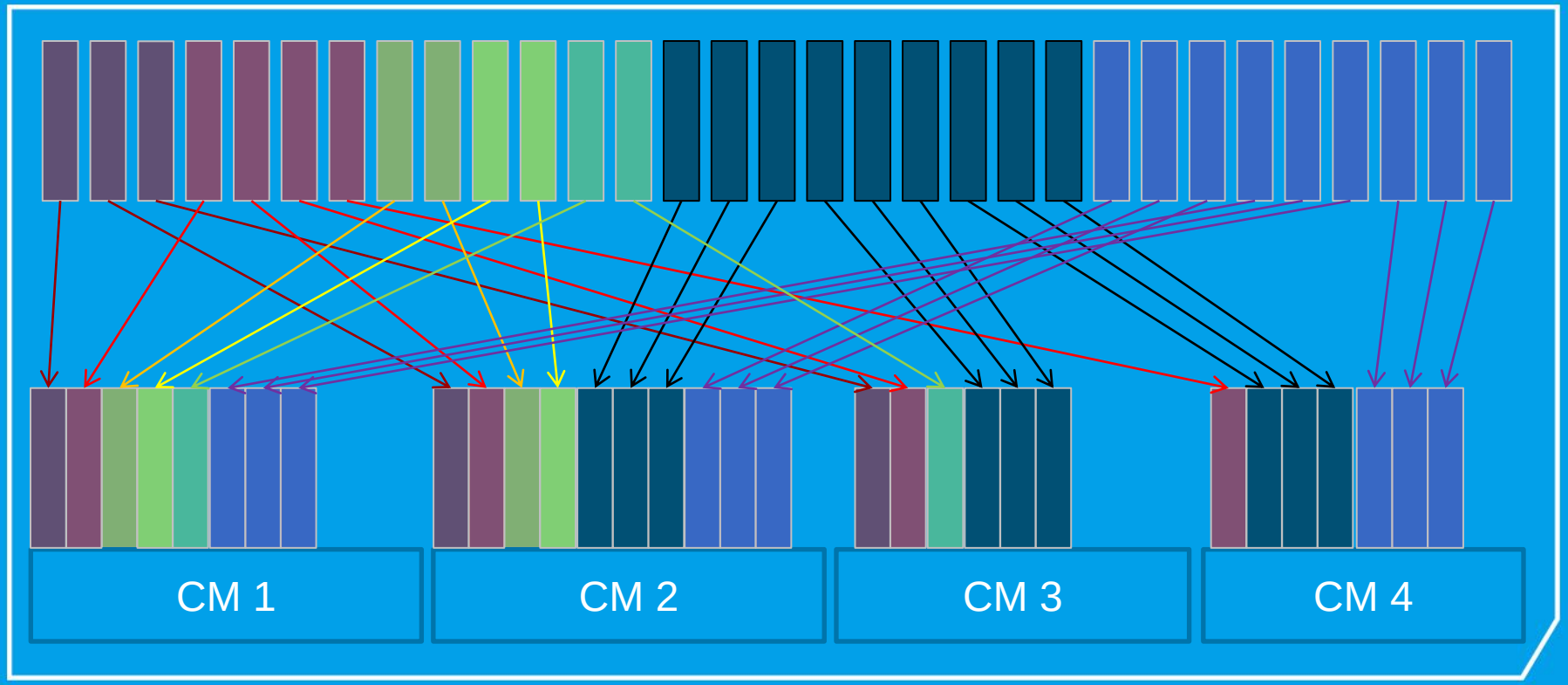
PROBLEM SOLVING



Deployment problem of 7 aircraft functions respecting:

- their constraints of safety
- the memory capacity of computation modules

PROBLEM SOLVING



CONCLUSION

CONCLUSION

DEPS

A high level modeling language:

- to represent a (sub-defined) system, its elements and its architecture
- to express requirements as properties between some elements

A problem solving tool chain:

- to complete sub-defined models

CASE STUDY

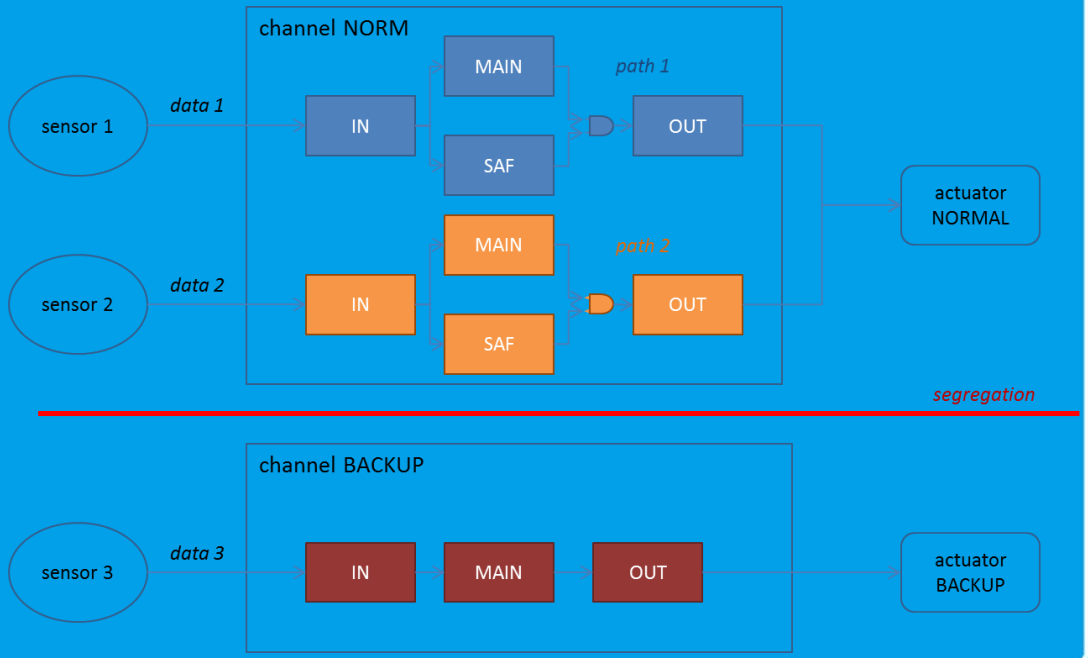
- a seamless synthesis process implemented in the tool chain
- a deployment problem set in an elegant and concise way and solved efficiently

FUTURE WORK

FUTURE WORK

MODELING THE WHOLE PROCESSING CHANNEL:

- sensors
- communication network
- effectors
- electrical supply



FUTURE WORK

TAKING ADDITIONAL REQUIREMENTS AND CONSTRAINTS INTO ACCOUNT AT ONCE:

- Safety
- Security
- QoS
- Resource Capacity
- Physical constraints
- Costs
- …

FUTURE WORK

EVALUATION OF THE NEXT VERSION OF DEPS IN ORDER TO:

- Check the suitability of the language for designing complex system architectures
- Have an influence* on the capability of future versions to address at the best the design of embedded systems

* The DEPS Link association (www.depslink.com) supports the development and The promotion of the DEPS language

THANK YOU FOR YOUR ATTENTION

QUESTIONS ?

Laurent ZIMMER
Dassault Aviation
laurent.zimmer@dassault-aviation.com

Pierre-Alain YVARS
SupMéca – Quartz
pierre-alain.yvars@supmeca.fr