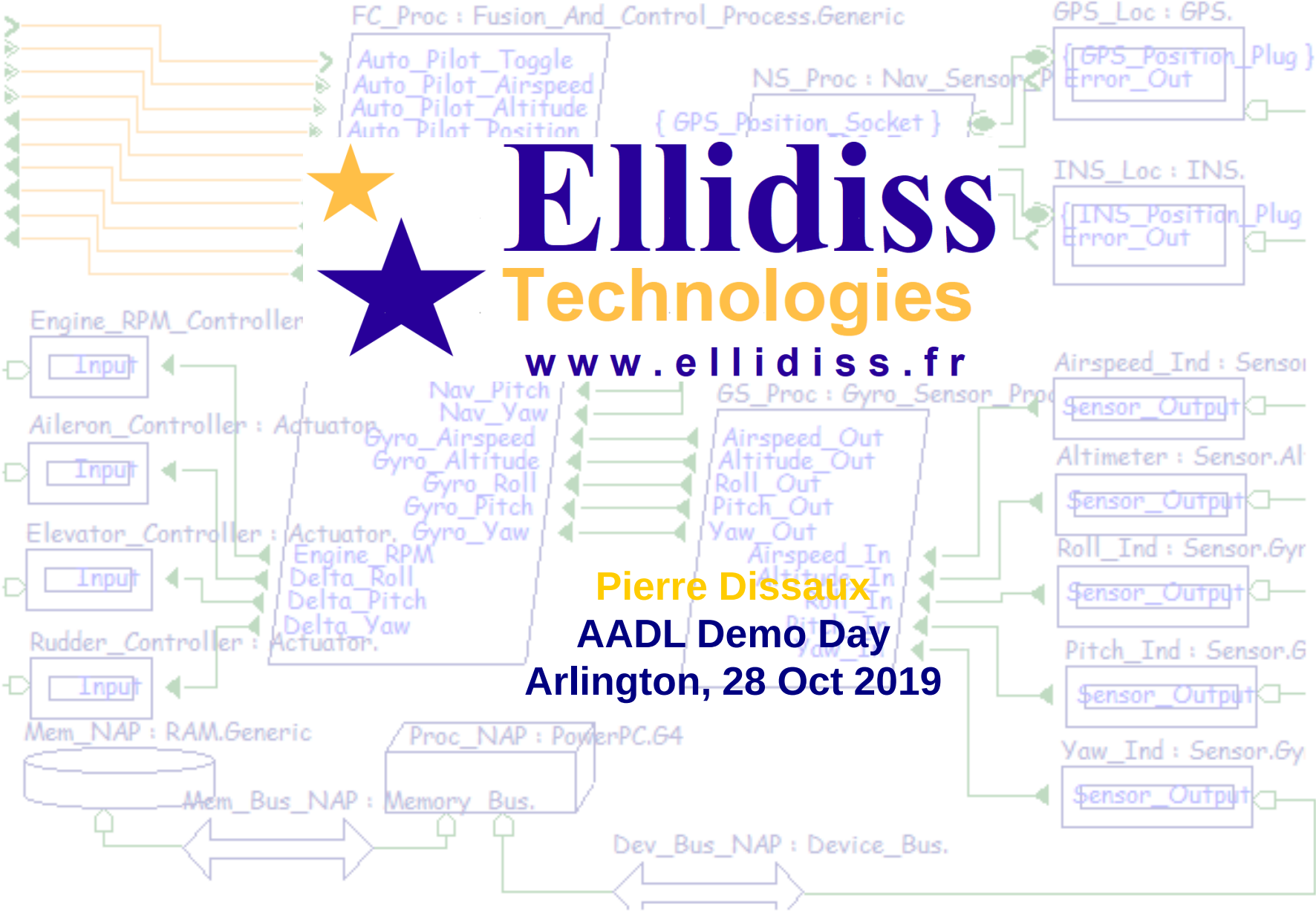


Ellidiss Technologies

www.ellidiss.fr

Pierre Dissaux

AADL Demo Day

Arlington, 28 Oct 2019

Ellidiss Technologies
www.ellidiss.fr

Critical Software Design tools (HOOD)

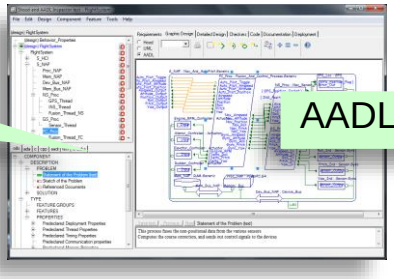
Eurofighter Typhoon

Tiger

Airbus A350

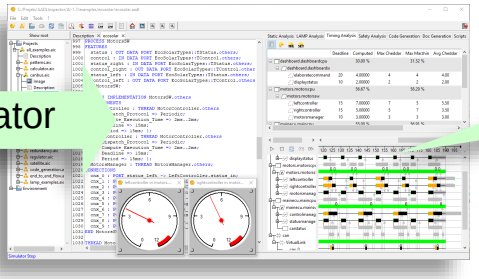
Real-Time, Safety and Security modeling and analysis tools (AADL)

software design



Stood for AADL

AADL generator



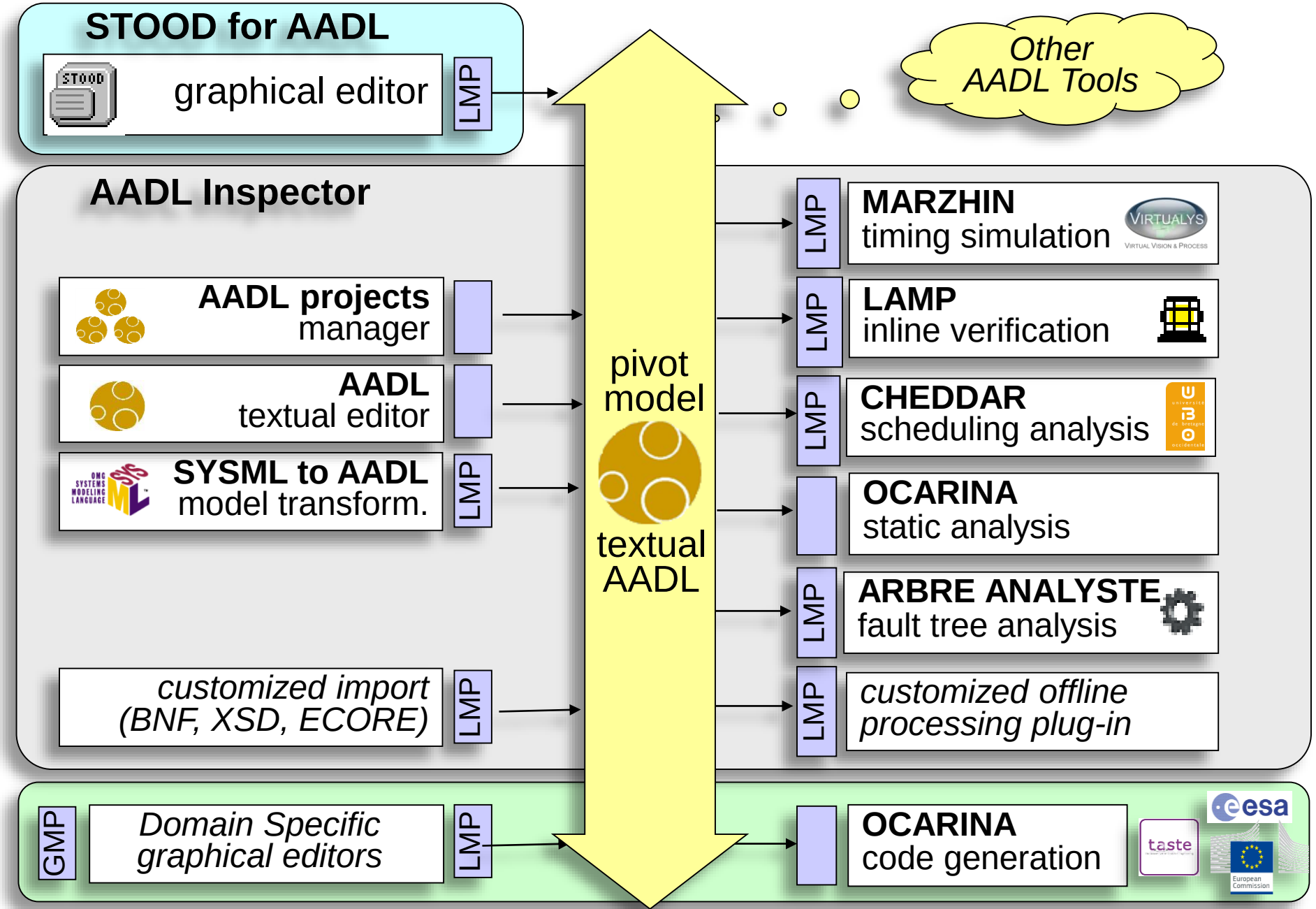
AADL Inspector

early verification

Modeling tools and model processing technologies (GMP, LMP)

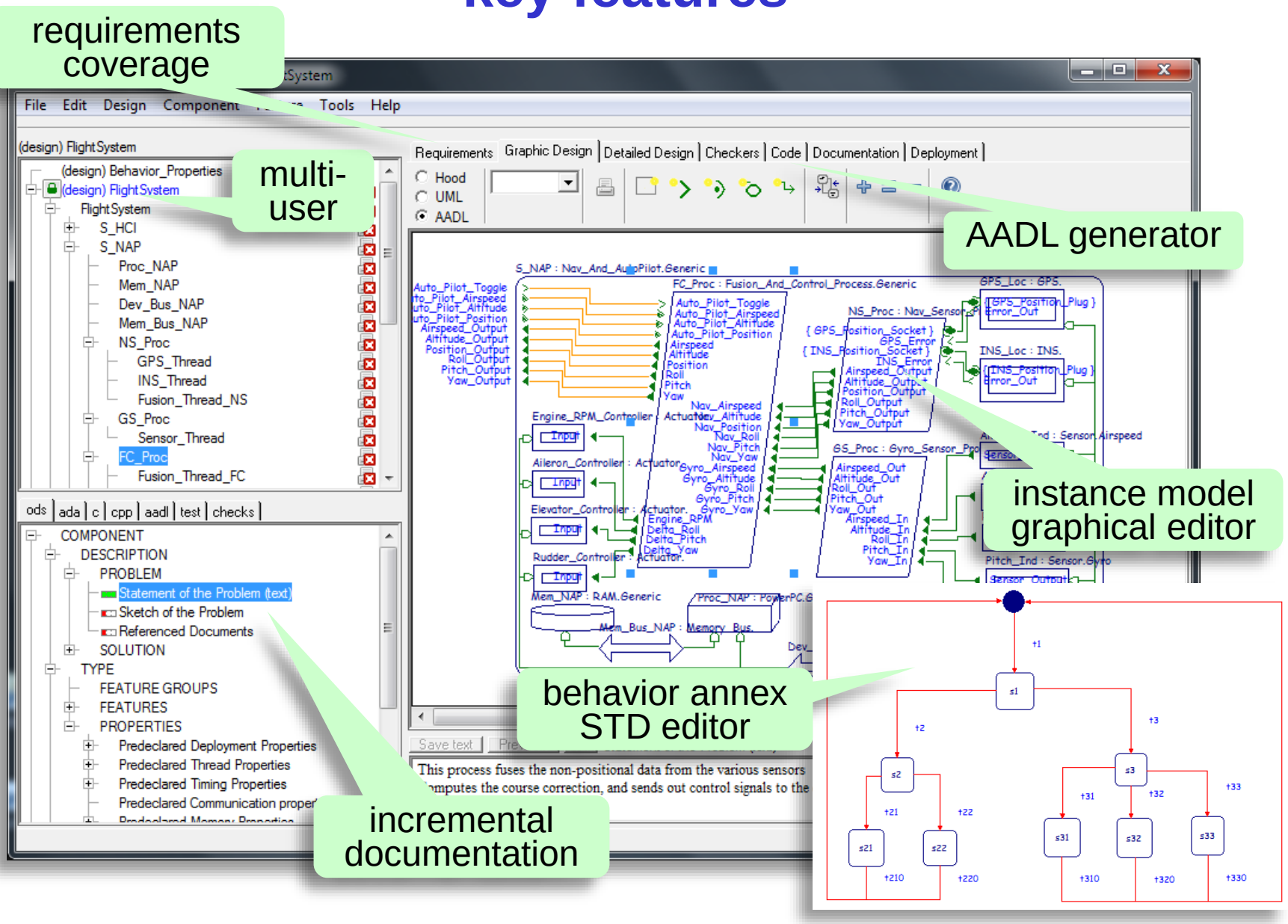
Ellidiss Technologies
www.ellidiss.fr

AADL centric tool-chains



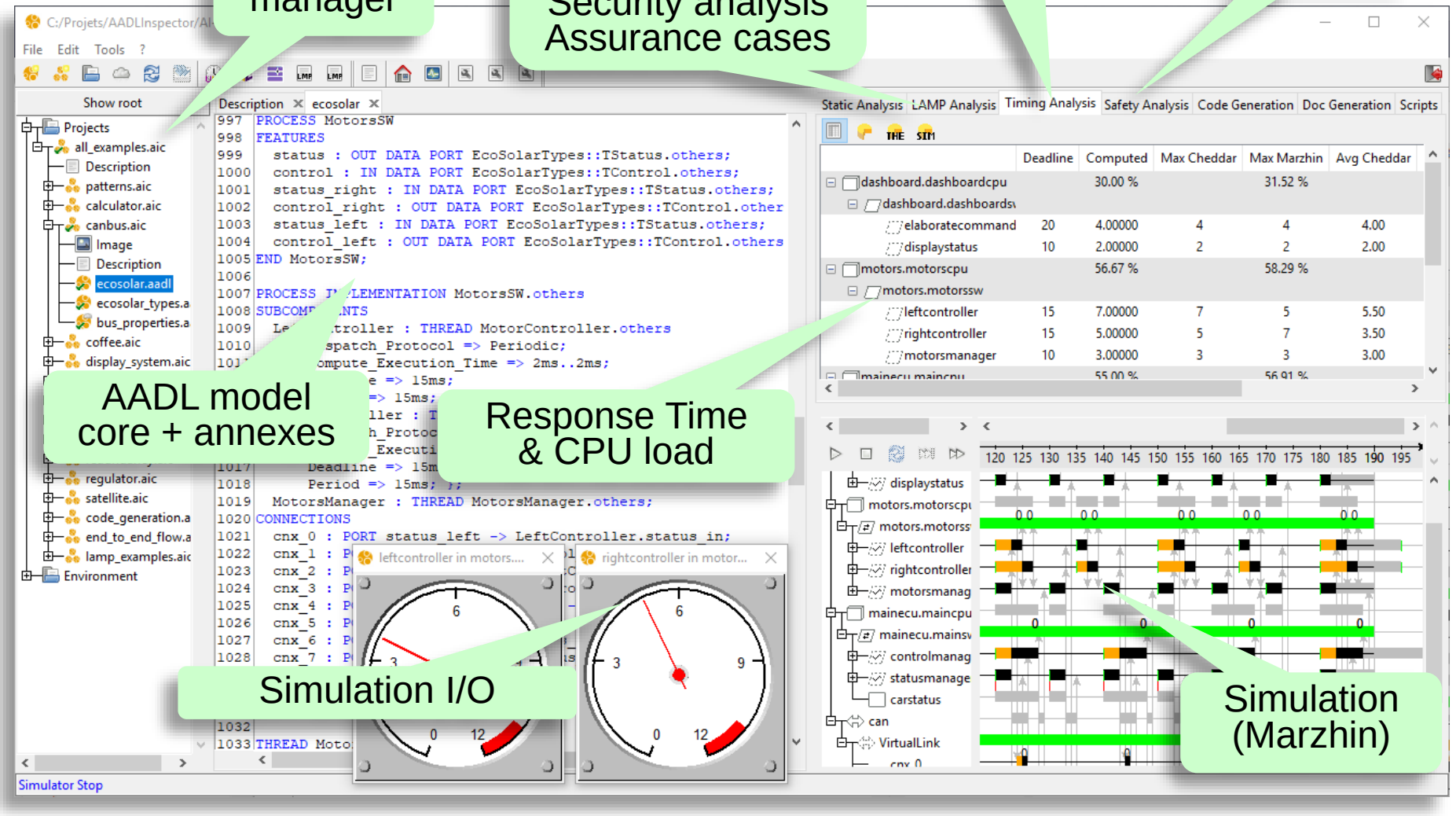
Ellidiss Technologies
www.ellidiss.fr

Stood for AADL key features



Ellidiss Technologies
www.ellidiss.fr

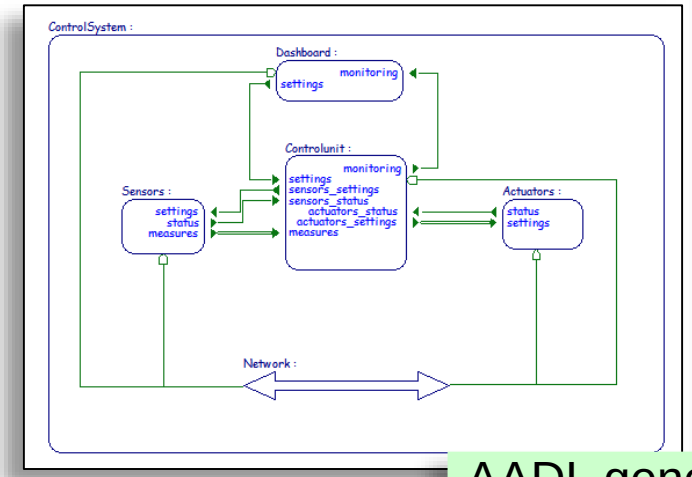
AADL Inspector key features

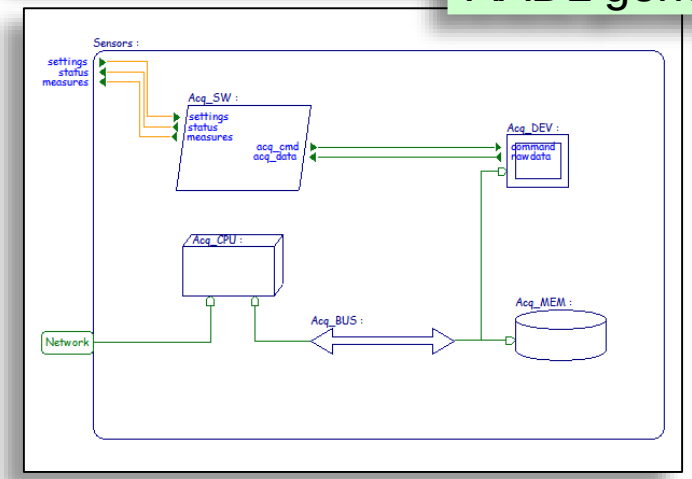


Ellidiss Technologies
www.ellidiss.fr

Example 1/4

AADL modeling with Stood






```
SYSTEM IMPLEMENTATION ControlSystem.others
SUBCOMPONENTS
 Sensors:      SYSTEM Sensors.others;
 Controlunit:  SYSTEM Controlunit.others;
 Actuators:    SYSTEM Actuators.others;
 Dashboard:    SYSTEM Dashboard.others;
 Network:      BUS Network;
CONNECTIONS
 cnx1:  PORT Dashboard.settings -> …
 cnx2:  PORT Controlunit.monitoring -> …
 cnx3:  PORT Controlunit.sensors_settings -> …
 cnx4:  PORT Sensors.status -> …
 cnx5:  PORT Sensors.measures -> …
 cnx6:  PORT Controlunit.actuators_settings -> …
 cnx7:  PORT Actuators.status -> …
 cnx8:  BUS ACCESS Network -> Dashboard.Nwk;
 cnx9:  BUS ACCESS Network -> Sensors.Nwk;
 cnx10: BUS ACCESS Network -> Actuators.Nwk;
 cnx11: BUS ACCESS Network -> Controlunit.Nwk;
FLOWS
 f1: END TO END FLOW
  Sensors.f1 -> cnx5 -> Controlunit.f1 -> cnx6 -> Actuato
PROPE TIES
  Connection_Binding => (reference(Network))
  es to cnx1,cnx2,cnx3,cnx4,cnx5,cnx6,cnx7
 Timing => Immediate
  applies to cnx5,cnx6;
ANNEX EMV2 {**
 use behavior errorlibrary::failstop;
 composite error behavior
 states
  [ Dashboard.FailStop or
    Sensors.FailStop or
    ControlUnit.FailStop or
    Actuators.FailStop or
    Network.FailStop ]-> FailStop;
 end composite;
**};
END ControlSystem.others;
```

```
PACKAGE ControlSystemTypes
PUBLIC

  DATA T_measures
  PROPERTIES
    LAMP::Security_Level => 5;
  END T_measures;

  DATA T_monitoring
  PROPERTIES
    LAMP::Security_Level => 2;
  END T_monitoring;

-- …

END ControlSystemTypes;
```

Real Time

Safety

AADL generator

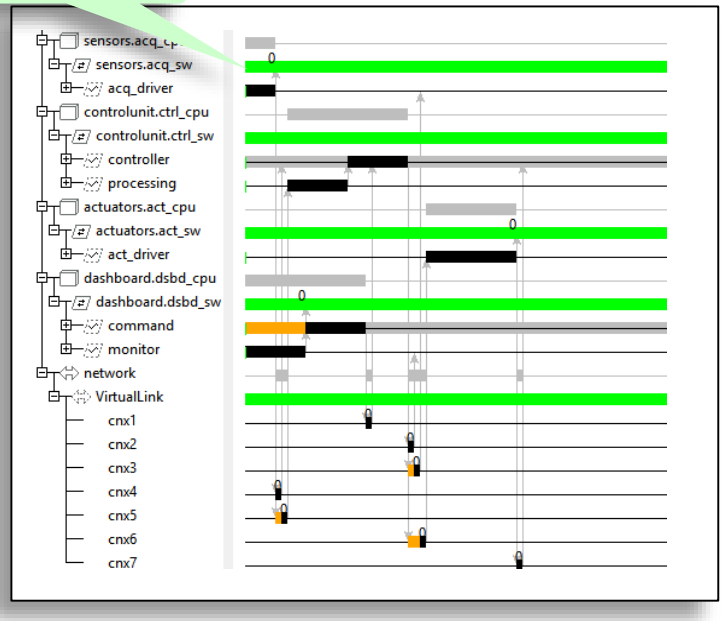
Security

Ellidiss Technologies
www.ellidiss.fr

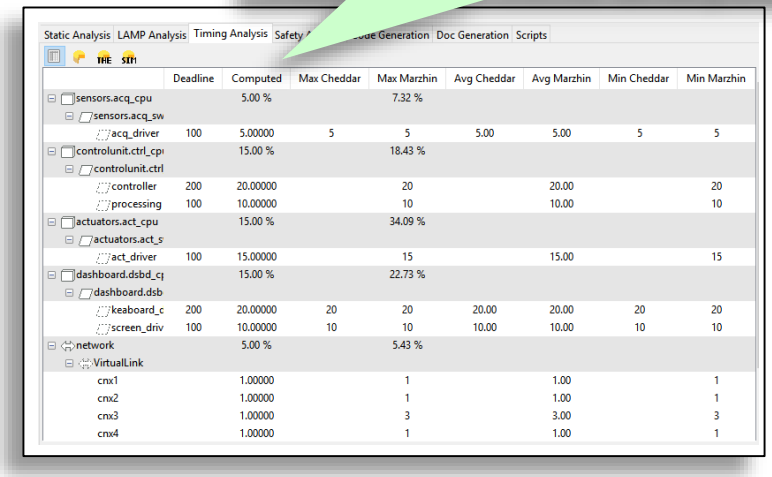
Example 2/4

Real-Time analysis with Marzhin and Cheddar

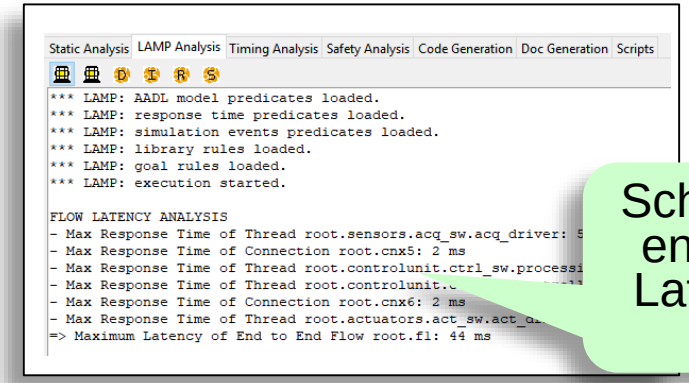
Simulation



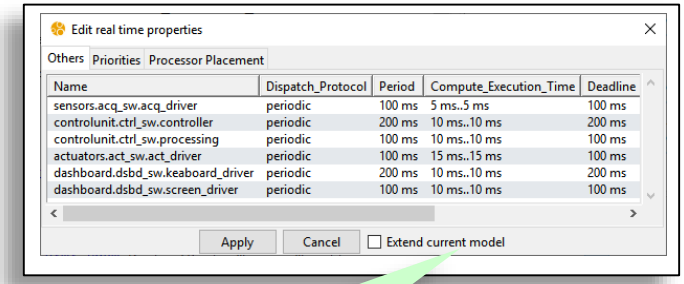
Response Time analysis



Scheduling Aware end to end Flow Latency Analysis with LAMP



Real-Time properties update



Ellidiss Technologies
www.ellidiss.fr

Example 3/4

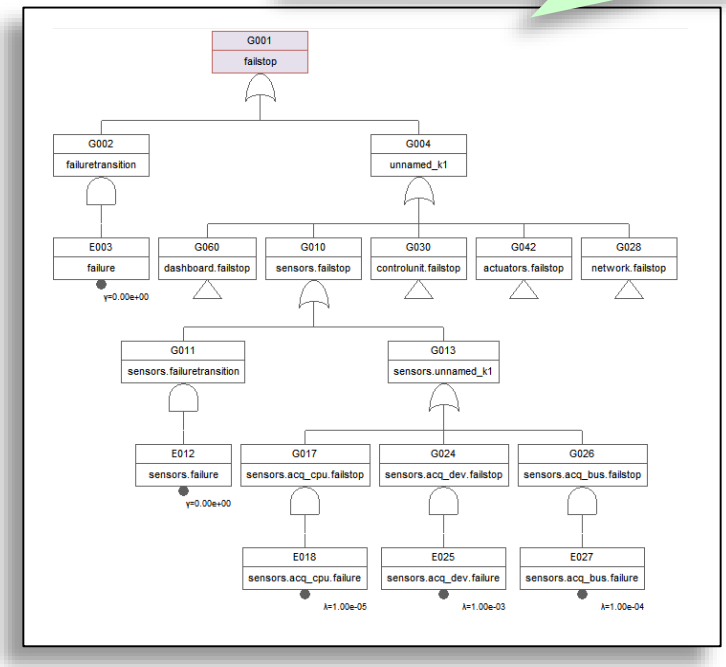
Open PSA generator

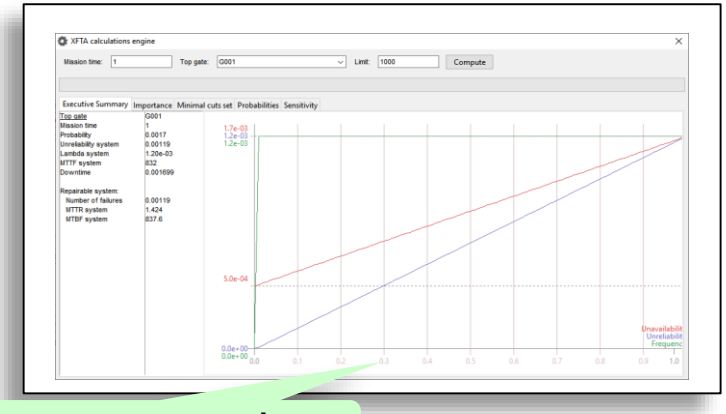
Static Analysis | LAMP Analysis | Timing Analysis | Safety Analysis | Code Generation | Doc Ge

```
<?xml version="1.0" encoding="UTF-8"?>
<open-psa author="Arbre Analyste" version="1.12">
  <label>from AADL model</label>
  <attributes>
    <attribute name="company" value="Ellidiss"/>
    <attribute name="author" value="AADL Inspector 1.7"/>
    <attribute name="creation-date" value="0"/>
    <attribute name="modification-date" value="0"/>
    <attribute name="version" value="1"/>
    <attribute name="performances" value="Q,F,T"/>
    <attribute name="page-id" value="1"/>
    <attribute name="page-1-name" value="A - failstop"/>
    <attribute name="page-1-description" value=""/>
    <attribute name="page-1-group" value="0"/>
    <attribute name="compute-id" value="1"/>
    <attribute name="compute-1-name" value="A - failstop"/>
    <attribute name="compute-1-gate" value="failstop"/>
    <attribute name="compute-1-time" value="1"/>
```

Safety analysis with Arbre Analyste (*)

Fault Tree Analysis





MTBF computation

(*) https://www.arbre-analyste.fr/en.html#

Ellidiss Technologies
www.ellidiss.fr

Example 4/4

Security analysis with LAMP

Security policy

- *Sec_R1*: All components involved in a same end to end Flow must be at the same security level.
- *Sec_R2*: The security level of a component is the higher security level value associated with its Data ports.
- *Sec_R3*: When two components are connected via a shared Bus, they must comply with the No-Read-Up and No-Write-Down rules.

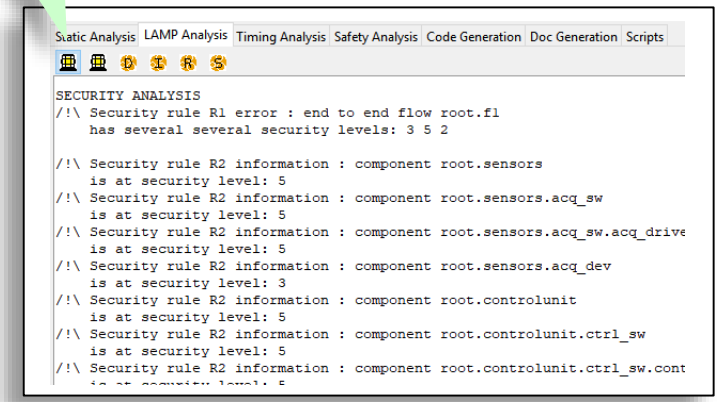
Security model

```
PROPERTY SET LAMP IS
-- …
Security_Level : AADLINTEGER APPLIES TO
  (Data, Data Access, Port, Parameter);
-- …
END LAMP;
```

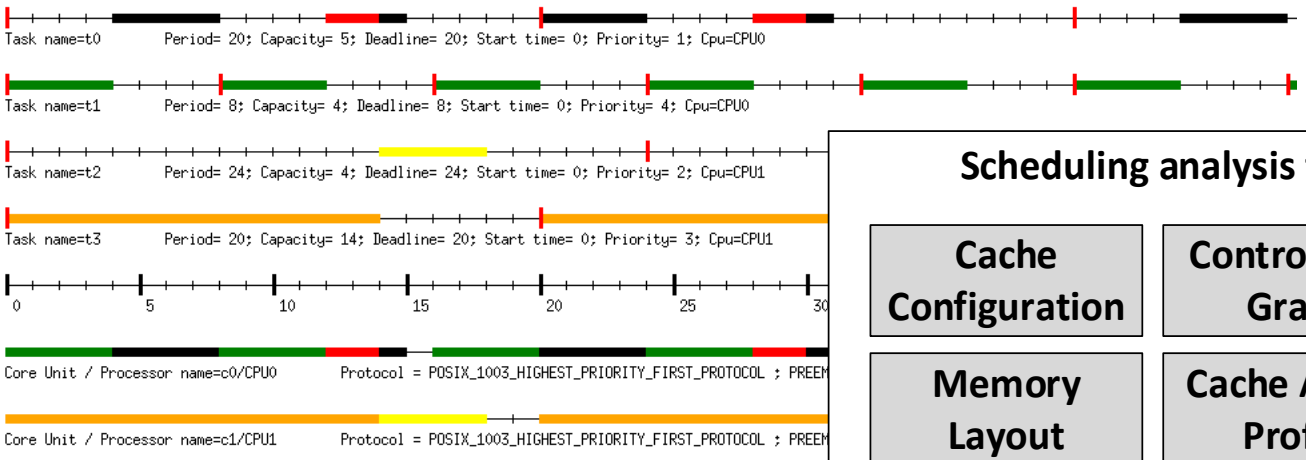
Security rules implementation (LAMP)

```
PACKAGE ControlSystemAnalysis
PUBLIC

ANNEX LAMP {**
/* rule Sec_R1 */
checkFlowSecurity :-
 getRoot(R), getClassifier(R,P,T,I),
 getAncestorRec(P,T,I,Q,U,J),
 isFlowImplementation('END TO END',Q,U,J,E),
 concat('root.',E,F),
 getEndToEndFlow('root',E,M),
 getFlowSecurityLevels(M,[],L,0,N), N > 1,
 printMessageSec_R1(F,L).
checkFlowSecurity :- nl.

/* rule Sec_R2 */
checkMaxSecurityLevel :-
 getMaxSecurityLevel(X,L),
 printMessageSec_R2(X,L).
checkMaxSecurityLevel :- nl.

/* rule Sec_R3 */
checkNoWriteDown :-
 isAADLBusBinding(_,C,_),
 isAADLConnection(_,P,T,I,_,_,_,C,_,_,_,_),
 getConnectionEnds(P,T,I,C,Xs,Xd),
 getMaxSecurityLevel(Xs,Ls),
 getMaxSecurityLevel(Xd,Ld),
 Ls > Ld,
 printMessageSec_R3(C,Ls,Ld).
checkNoWriteDown :- nl.

-- …
END ControlSystemAnalysis;
```

Security assessment (LAMP)



Cache-Aware Scheduling Analysis



Scheduling analysis for systems with cache

Cache Configuration	Control Flow Graph	Worst-Case Execution Time
Memory Layout	Cache Access Profile	Scheduling Policy

Scheduling simulation with cache:

- L1 uniprocessor instruction caches
- Sustainable CPRD model (Cache Preemption Related Delay)
- And known feasibility interval (prooved): [0, LCM(Pi)]

Cache-Aware Priority Assignment Algorithm:

- Audsley oriented algorithm

F. Singhoff
S. Rubini
L. Lemarchand
H. Nam Tran

Ellidiss Technologies
www.ellidiss.fr

Our offer

Products

- **Stood** for AADL: instance model graphical editor for AADL
- **AADL Inspector**: analysis and simulation
- LMP Dev-kit: model processing development framework

Technology

- LMP: model processing toolbox (prolog)
- **LAMP**: model processing language for AADL
- GMP: DSL graphical editor framework
- Research collaboration with University of Brest/Lab-STICC (Cheddar)

Services

- Tools sales, support and long-term maintenance
- HOOD & AADL consulting
- Graphical front ends development
- Model processing tools (rules checkers, generators)
- Model transformations
- Tool-chains integration
- R&D partnerships