A Model Based Approach for Safety Analysis

Embedding Altarica in Alstom MBSE Process

Elie Soubiran, Fabien Belmonte

ITEA2 – 2009/2012

IMOFIS

ANR – 2008/2011

Journée SysML
13 Novembre 2012

ALSTOM

Agenda

Alstom: Four main activities

92,600 employees in 100 countries

Thermal Power sector
Equipment & services for power generation

Renewable Power sector
Equipment & services for power generation

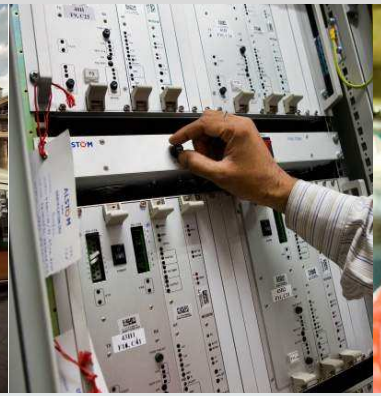
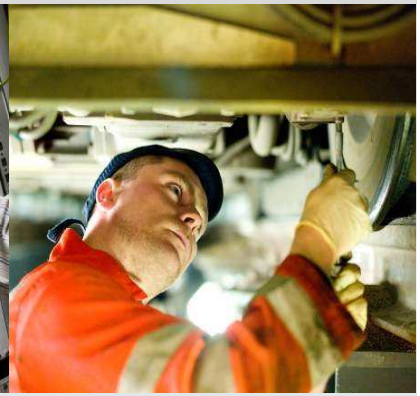
Grid sector
Equipment & services for power transmission

Transport sector
Equipment & services for rail transport

Alstom Transport, the only railway multi-specialist

24,700 employees in more than 60 countries



- The only manufacturer in the world to master all businesses of rail sector
- The most complete range of systems, equipments and services:
  Rolling Stock / Infrastructures / Signalling / Services /
  Turnkey transport systems

- N°1 in high and very high speed
- N°2 in urban transport (tramways, metros
- N°2 in signalling
- N°2 in maintenance

A wide range of products and services

Infrastructure, signalling, services and maintenance





SIGNALLING

Atlas: Revolution in interoperable drive systems

Urbalis: Optimal and efficient monitoring
of complex urban transport systems

SERVICES AND MAINTENANCE

Full Maintenance Management

Spare parts management

Renovation

Traintracer

INFRASTRUCTURE

Track laying

Electrification

Electric power supply

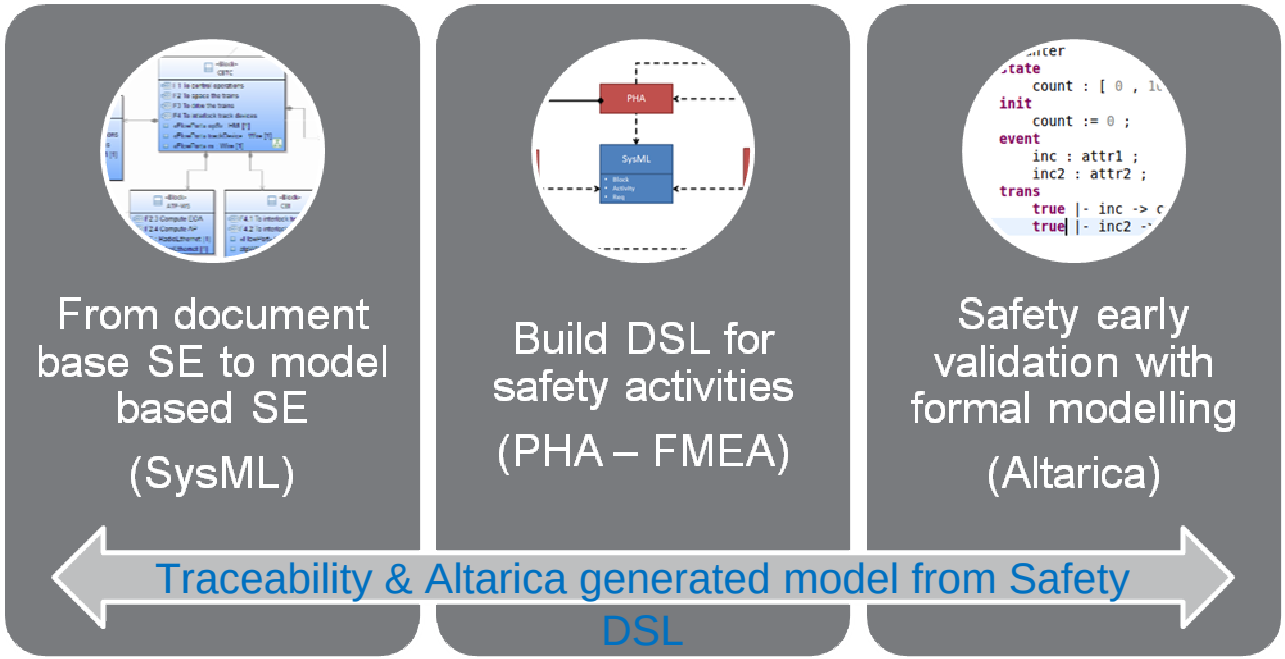
Electromechanical equipment

Our work in a nutshell

Towards Integrated Model Based System and Safety Engineering – Early Validation

Needs & Motivations:

- Development of complex and safety critical system engineering;
- Insure traceability of system design modelling artefacts and safety assets;
- Perform computer aided safety 'early validation': Simulation of hazardous scenarios, accident sequences analysis and generation of fault trees.

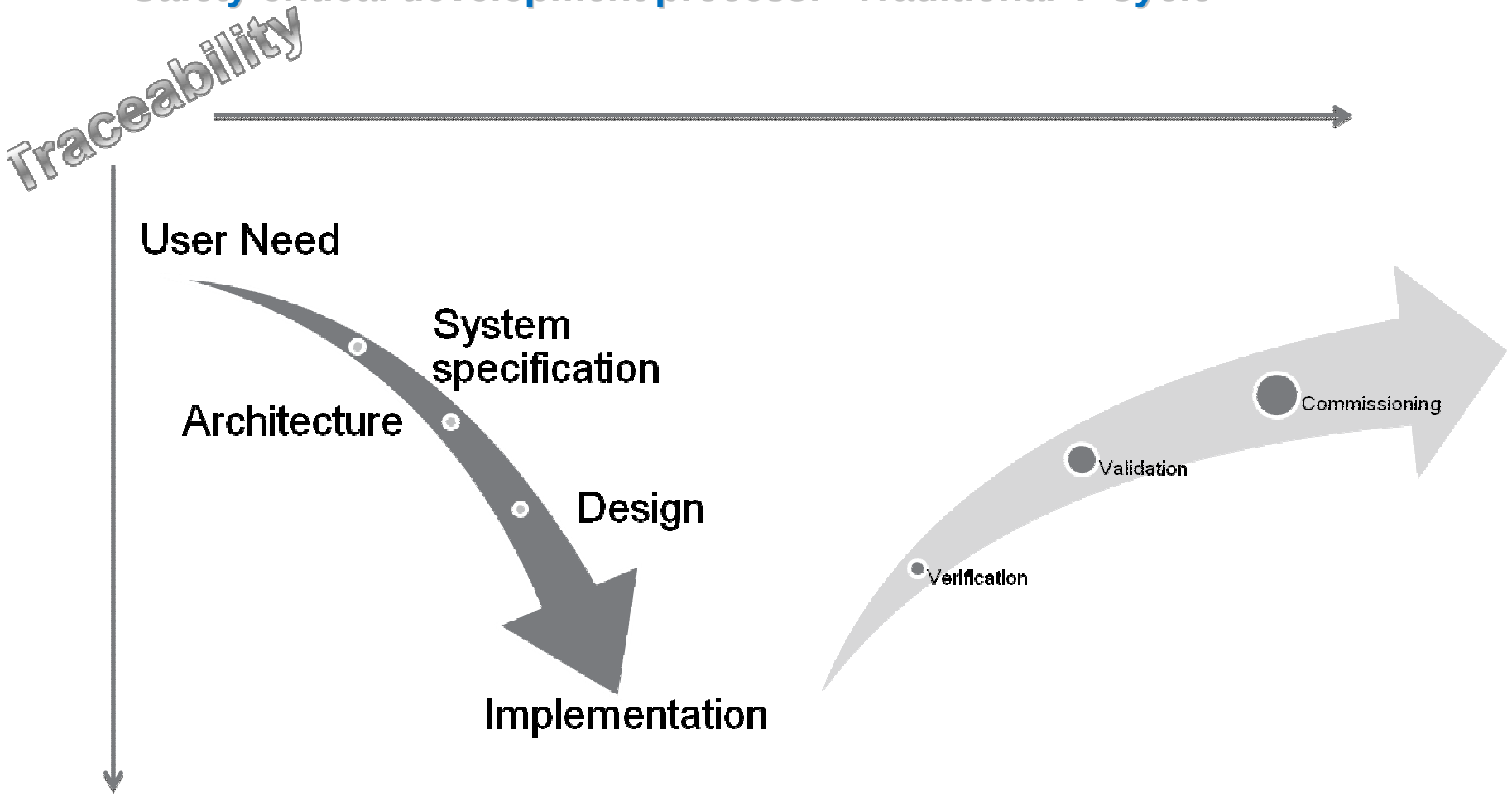


Objectives

- Context of Work
  - SysML model
  - IMOFIS DSL for PHA
  - Eclipse Modelling Framework
- Develop a DSL for FMEAs
  - FMEA modelling
  - Errors propagation though the dataflow
  - Insure traceability with SysML system specification
  - Insure traceability from Hw-Sw to PHA (bottom-up)
- Formalise the FMEA hierarchy (translation from DSLs to Formal model)
  - Generate the accident cases sequences
  - Generate Accident cases Fault Trees
  - Identify critical failures paths
  - Simulate the dysfunctional behaviour of the system

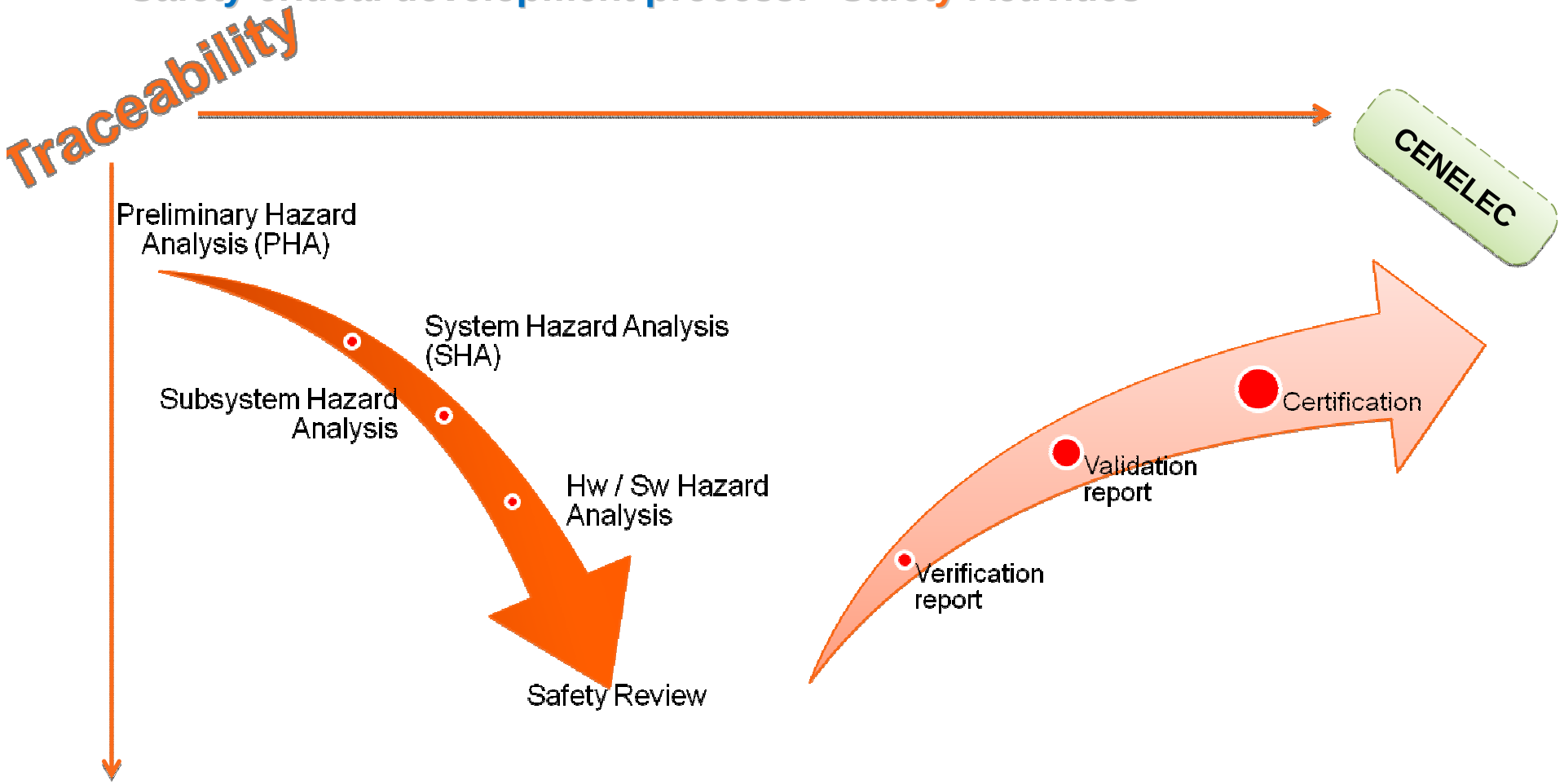
Context: Railway signalling system development

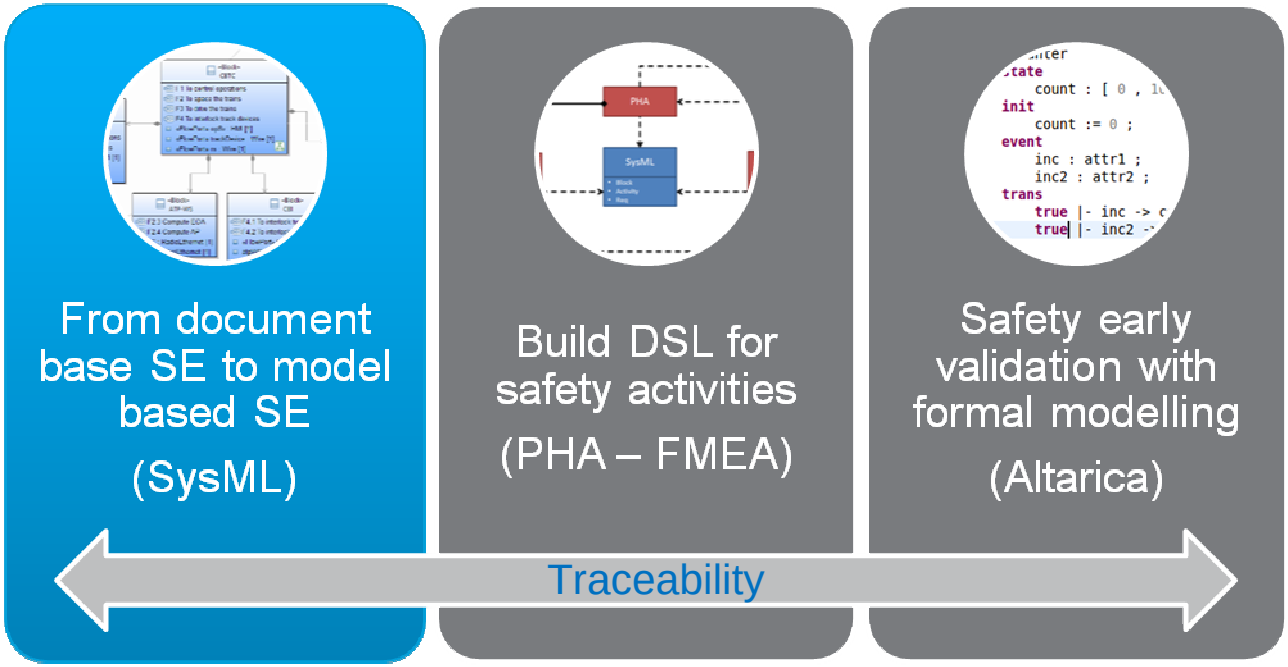
Safety critical development process: “Traditional V-Cycle”



Context: Railway signalling system development

Safety critical development process: "Safety Activities"

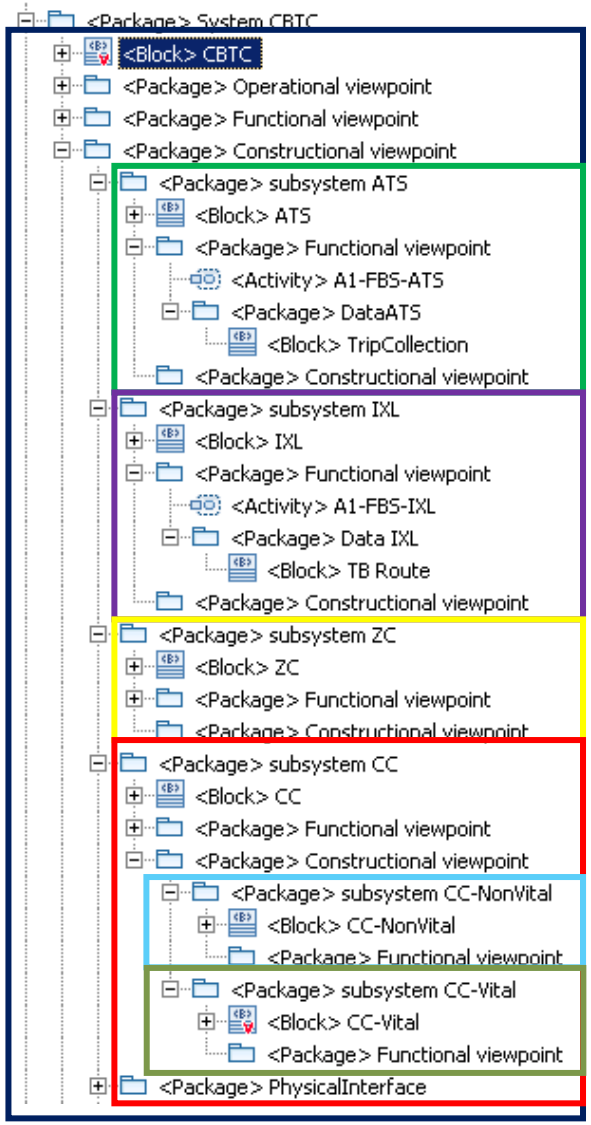




Model Based Approach

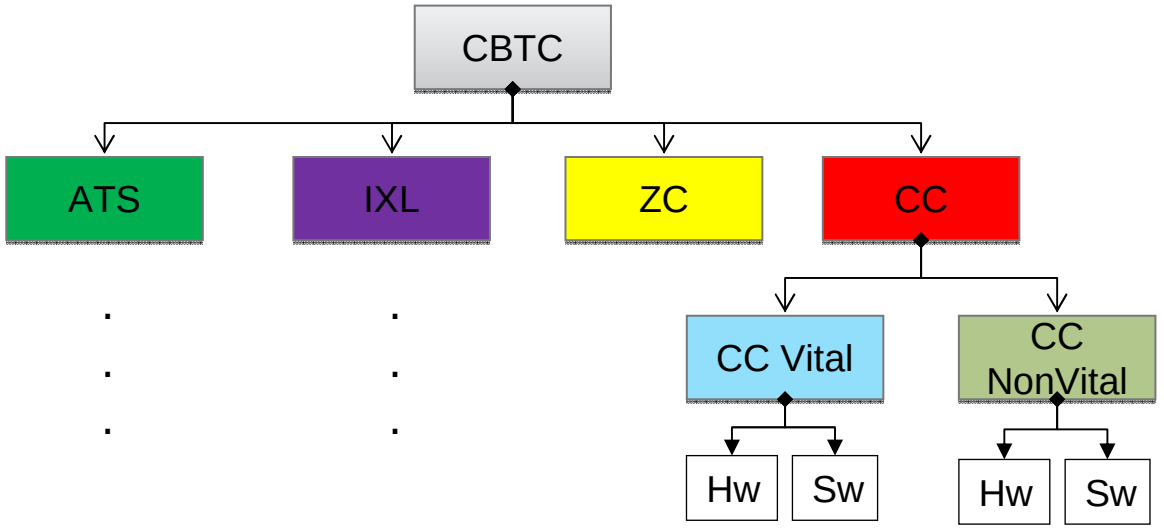
System Design with SysML

Specification with SysML



Three viewpoints
- Operational
- Functional : Activities Hierarchy
- Constructional: Blocks Hierarchy

Allocation

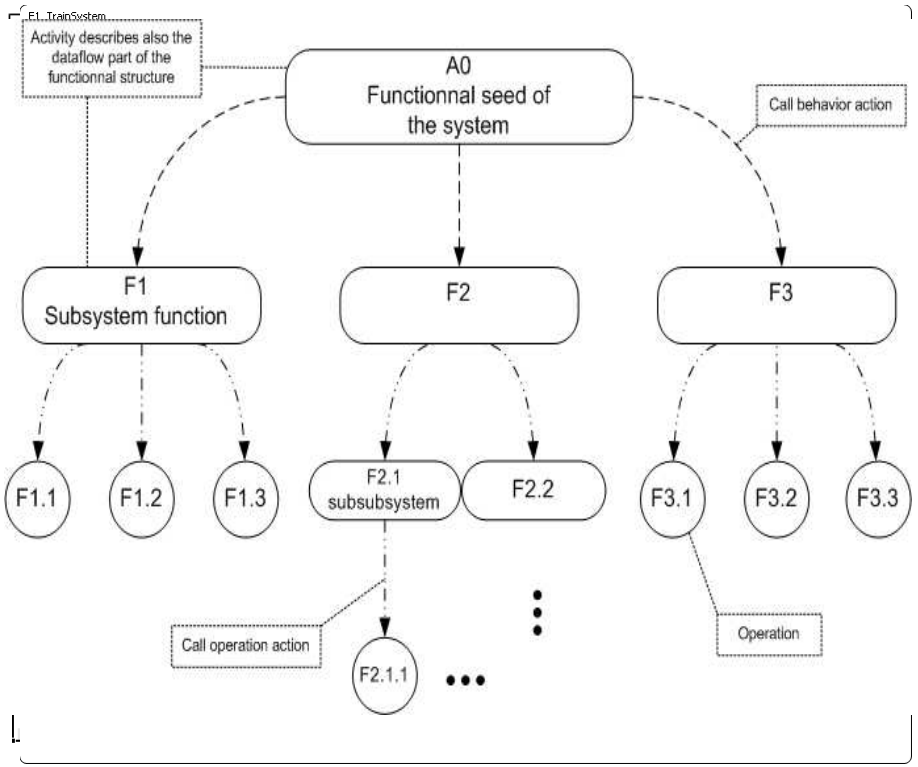


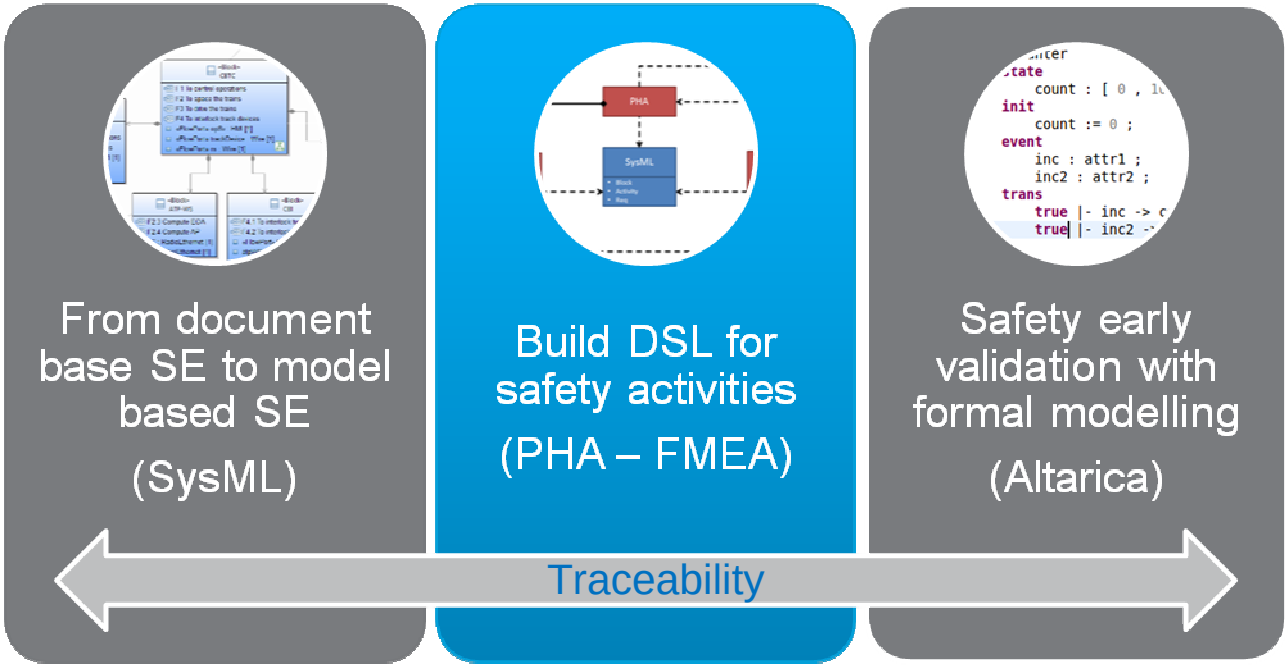
Iterative process over the constructional hierarc

Illustration of System Eng. Concepts in SysML

SysML representation of SE concepts

- Operational viewpoint
  - Environment of the system
  - Context of use
- Functional viewpoint (Function = Activity)
  - FBS
  - Functions behaviour

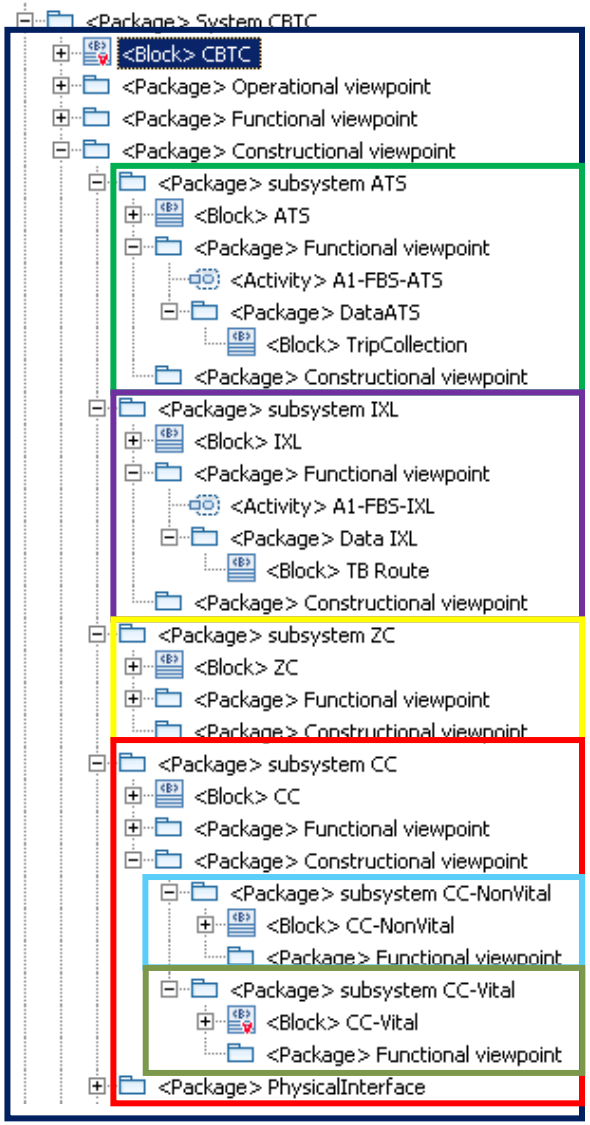


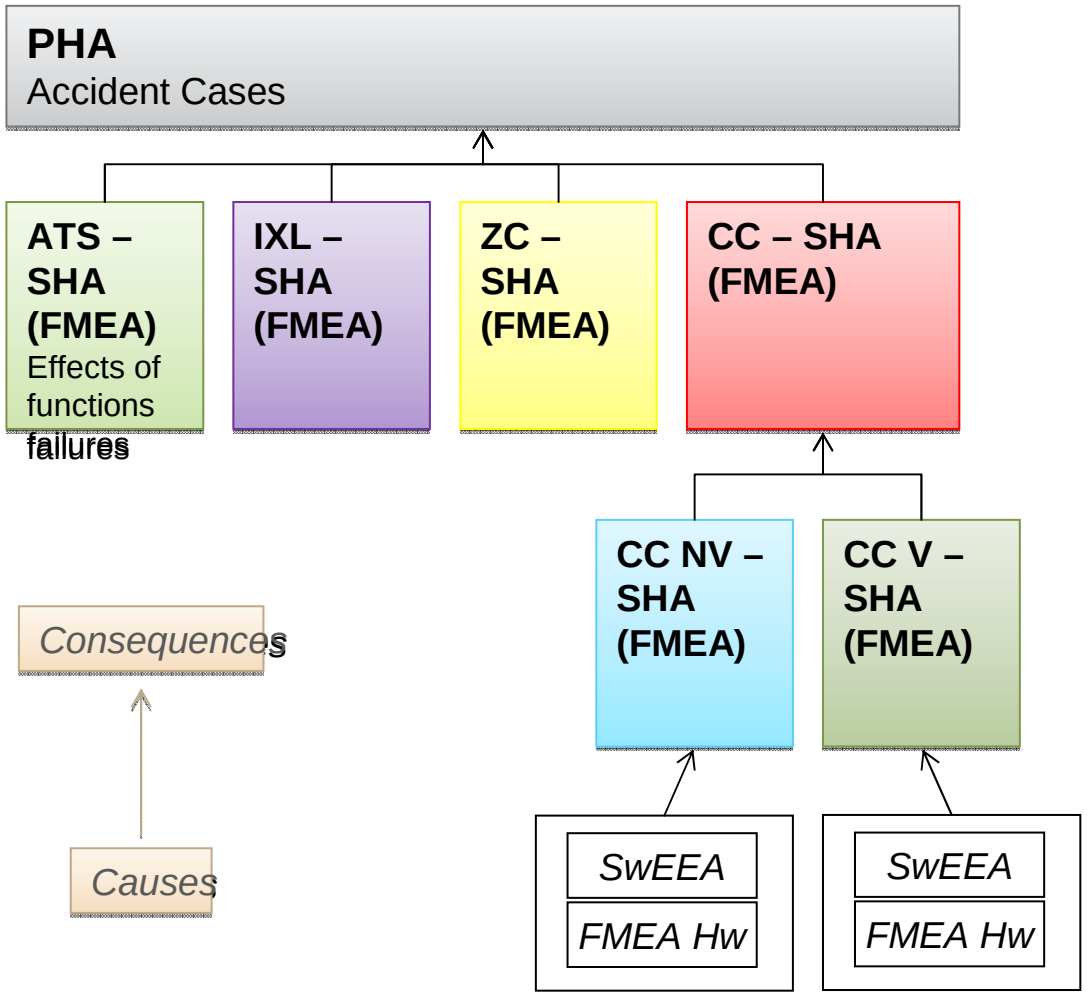


Model Based Approach

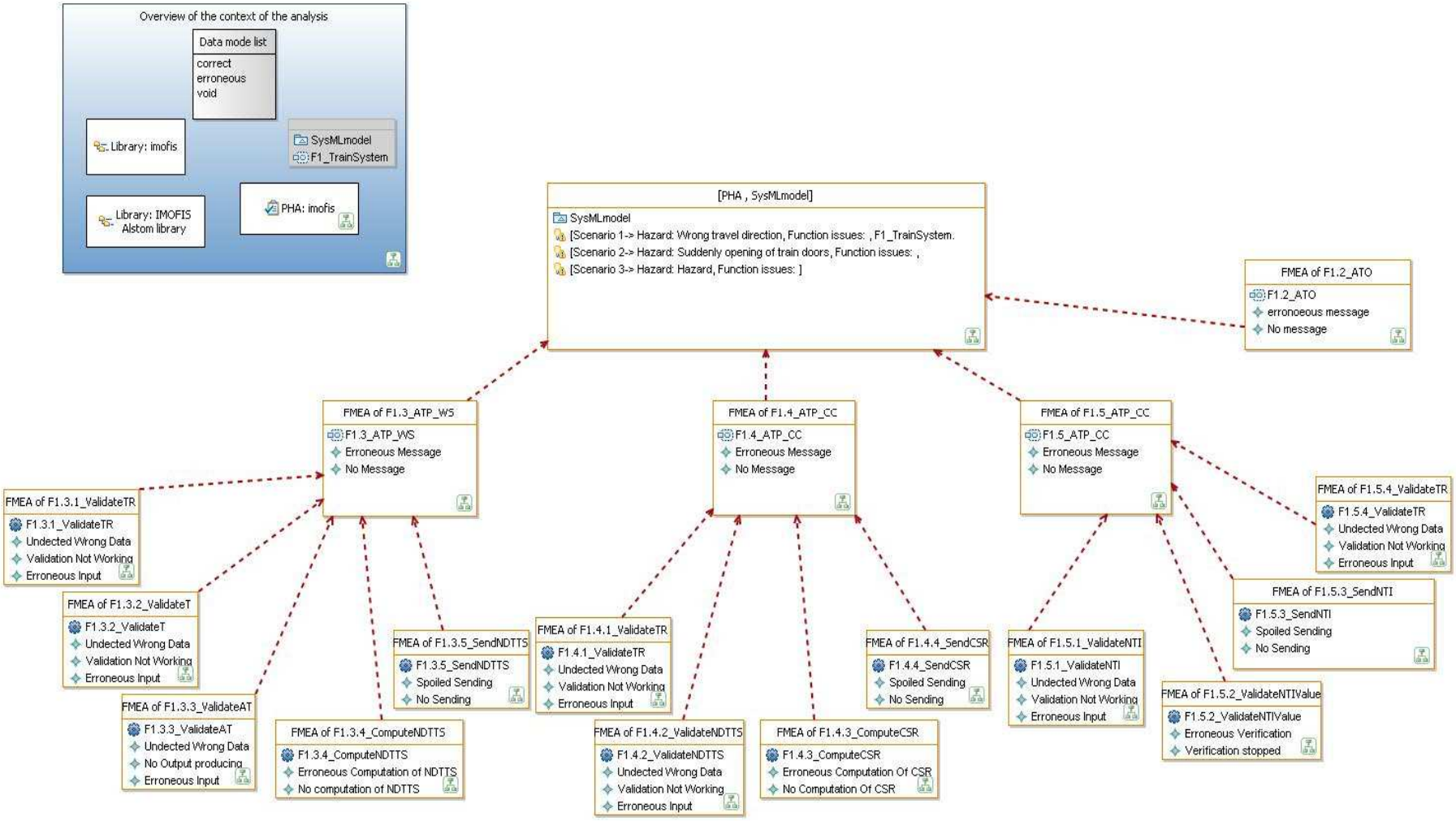
Safety Process & Safety DSL

Hazards Analysis on SysML System Specification





Hazard analysis with the DSL



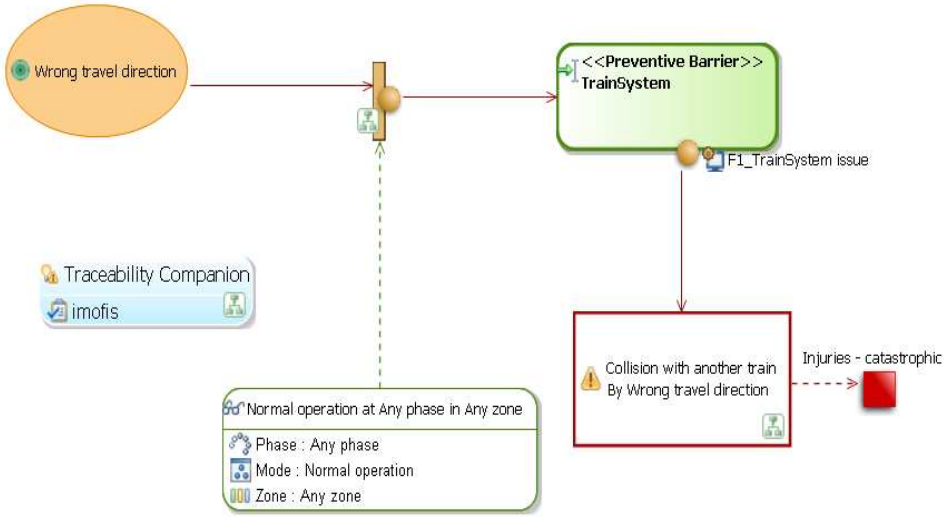
PHA – SHA modelling concepts

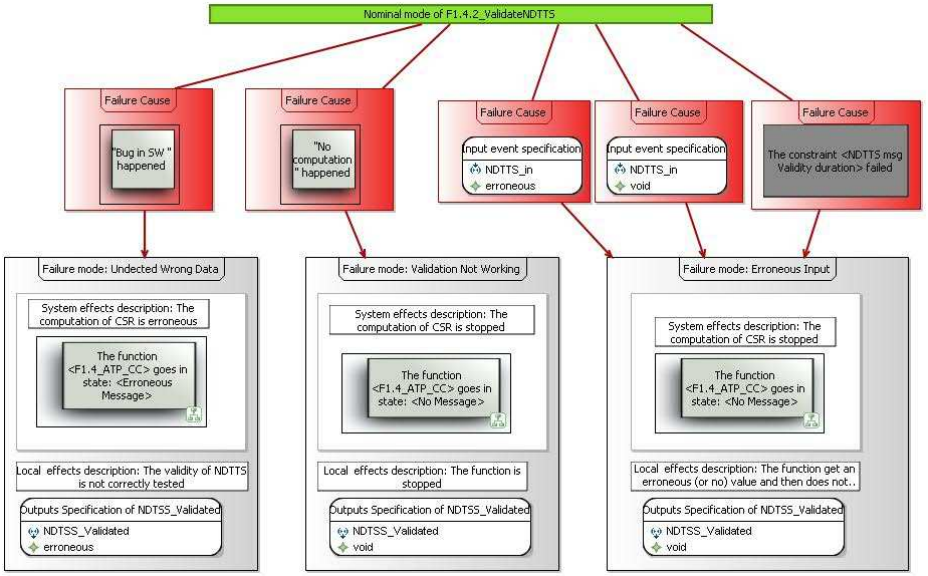
PHA

- Identify accident scenarios

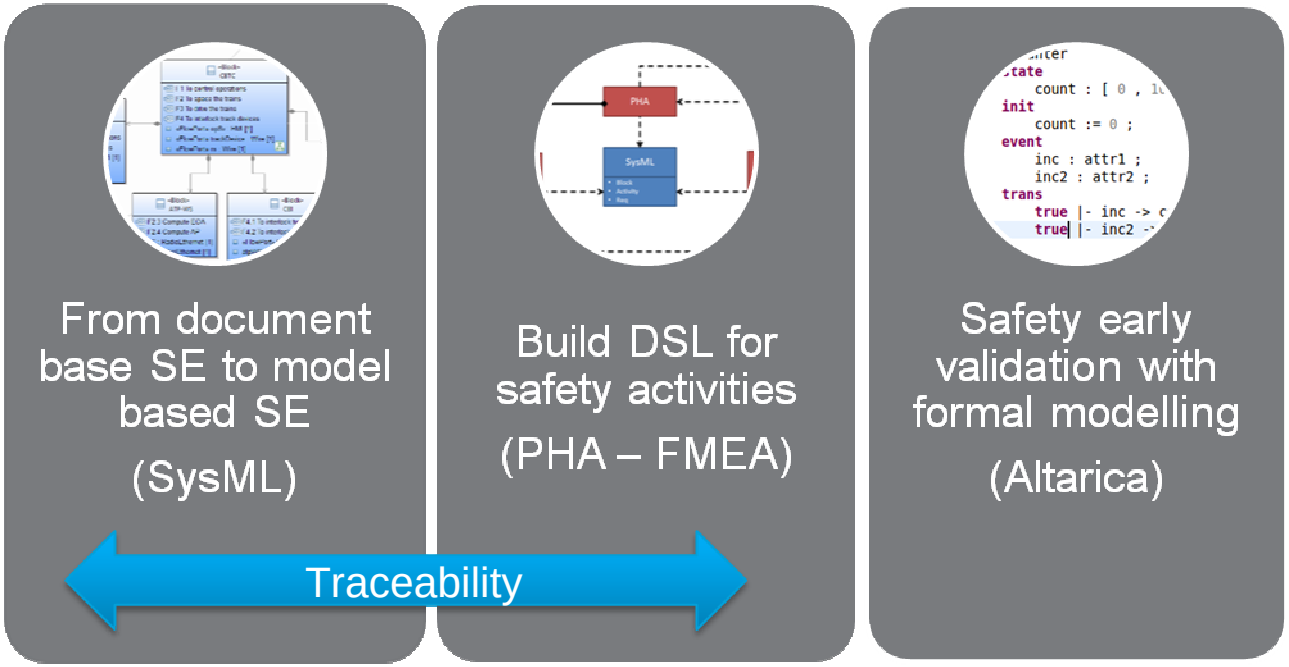
SHA

- Exhaustive analysis of all function failures





DSL for PHA & SHA interoperable with SysML



Model Based Approach

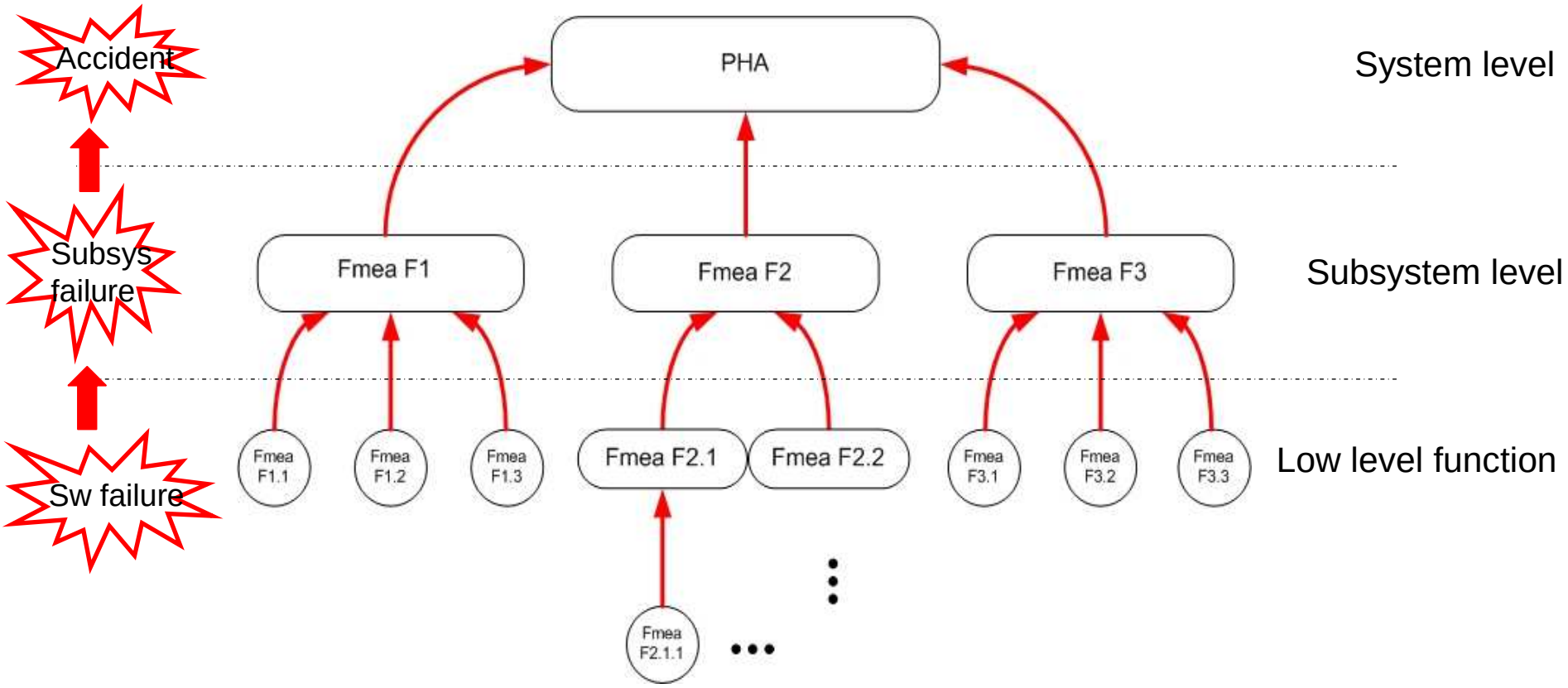
Traceability between SysML and Safety DSL

Modelling artefacts Traceability: System to Safety

System		Safety
Block	⟺	Barrier
Activity	⟺	Function Fmea
Operation	⟺	Low level function Fmea
Requirement	⟺	Safety requirement
Port/Parameter	⟺	Function input/output
Constraint (VSL)	⟺	Condition of failure

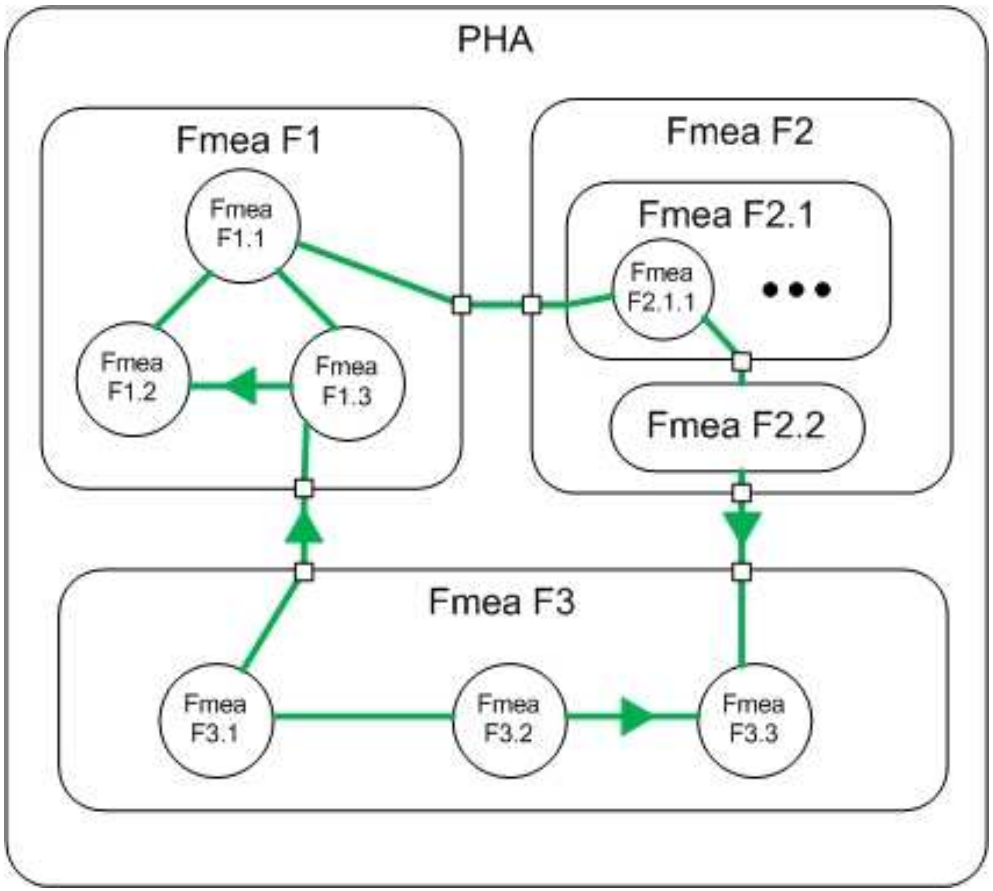
Traceability inside Safety model : Failure decomposition

Failures of low level functions develop to system accidents:



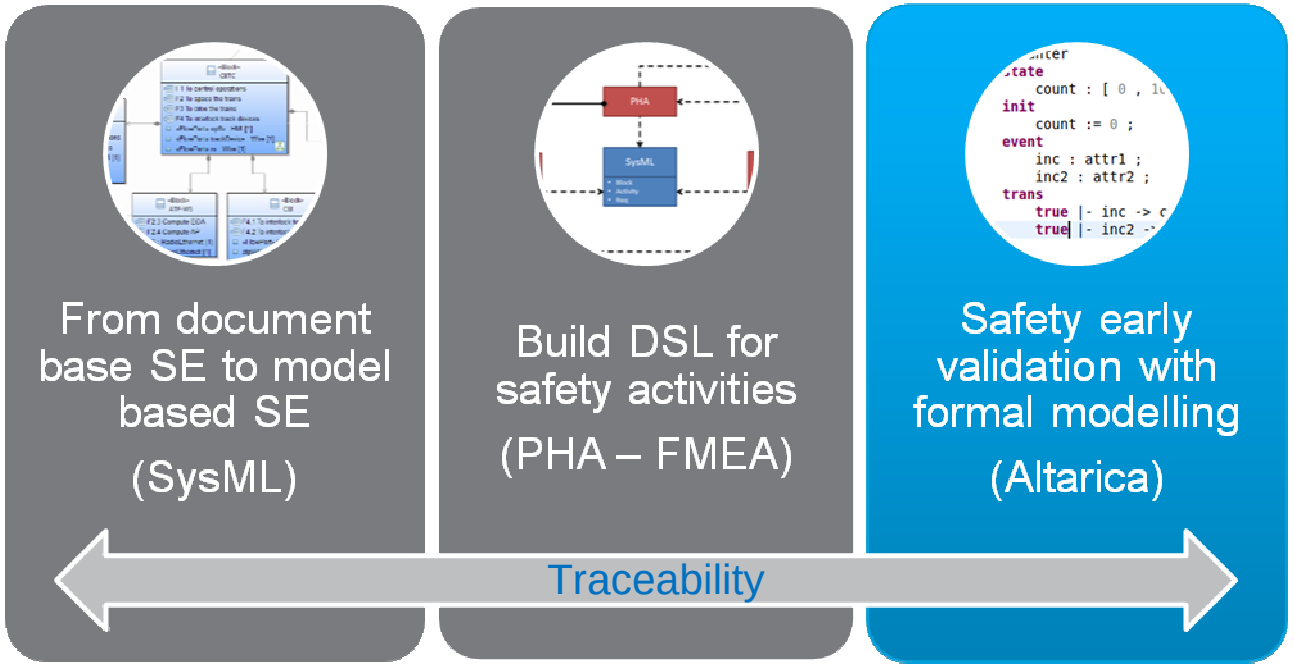
Failures at level i+1 are causes of failures at le

Propagation of errors



Error are propagated through dataflow links

An erroneous value as input can be the cause of a failure



Model Based Approach

Formal semantic for safety DSL

Automatic translation

Formal semantic for Safety DSL

Why?

- To generate the fault trees,
- To compute the sequences,
- To preform early validation of the system safety;

What?

- Guarded Transition System: Altarica (Thesis – Point, G. 2000)

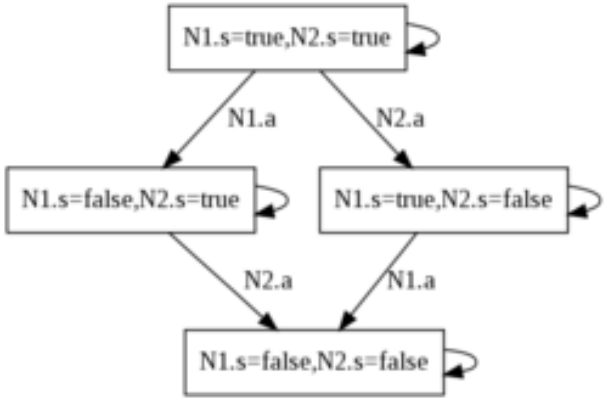
How?

- Control flow (event, guard): to model the occurrences of failures,
- Data flow: to study errors propagation;

Altarica overview

Textual Syntax to describe GTS

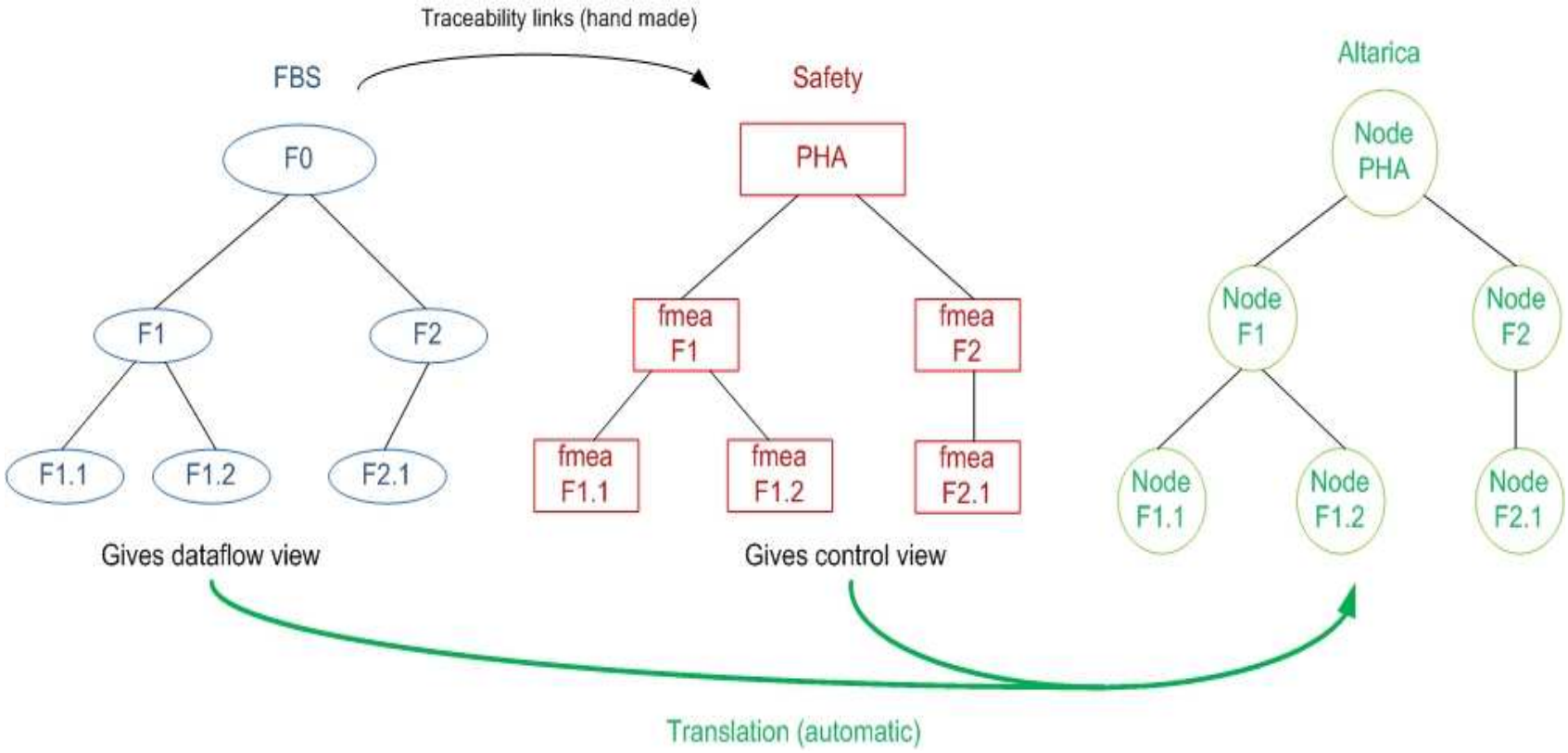
- Hierarchy of Nodes
  - Node
    - Sub-Nodes
    - Data Flow connectors (in/out)
    - Events
    - States
    - Transitions
    - Assertions




```
1  node N
2    event a;
3    state s : bool;
4    init s := true;
5    trans s |- a -> s := not s;
6  edon
7
8  node Main
9    sub
10     N1, N2 : N;
11 edon
```

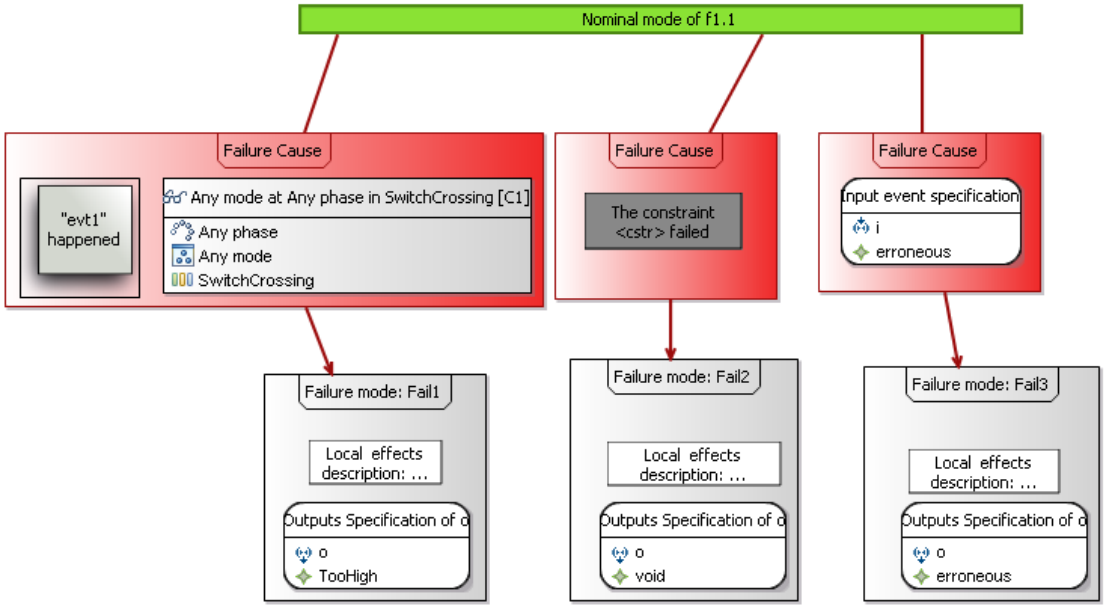
http://altarica.labri.fr

Translation - Overview



Translation of leaf FMEA

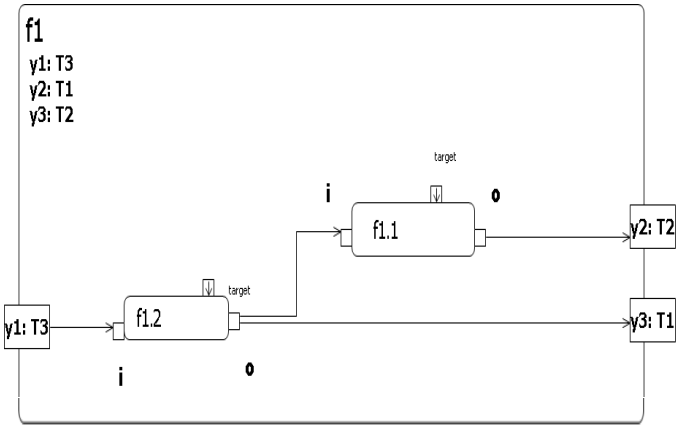
- f1.1(in i : T1, out o : T2)

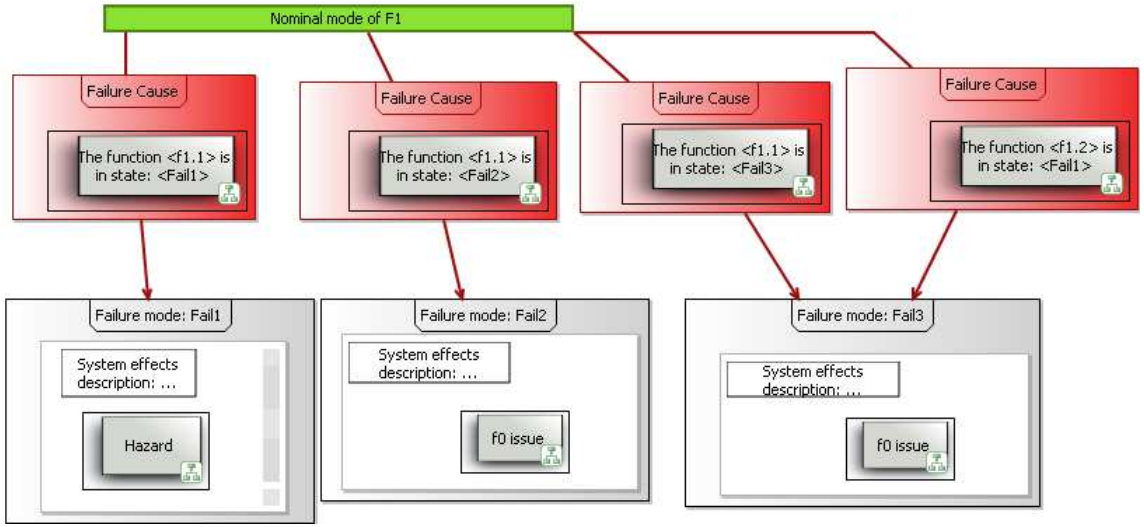



```
Node f1_1
    flow
      ctxt : ContextType : in;
      i : DysData : in;
      o : DysData : out;
    event
      evt1,cstr_fail;
    state

    st:{Nominal,Fail1,Fail2,Fail3};
    trans
        ctxt=c1 |- evt1 ->st:=Fail1;
        true |-cstr_fail -> st:=Fail2;
        i=erroneous|- -> st:=Fail3;
    assert
        case{ st = Nominal :
    o=correct,
                st = Fail1 :
    o=TooHigh,
                 st = Fail2 : o=Void,
                st = Fail3 :
    o=erroneous};
```

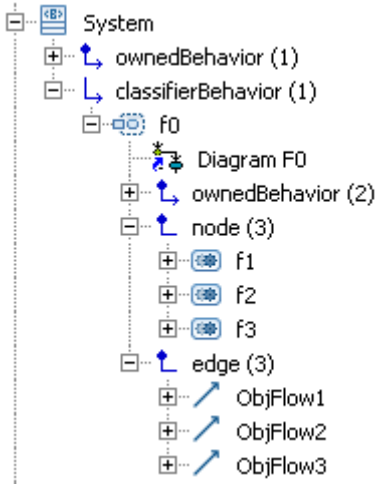
Translation of intermediary FMEA

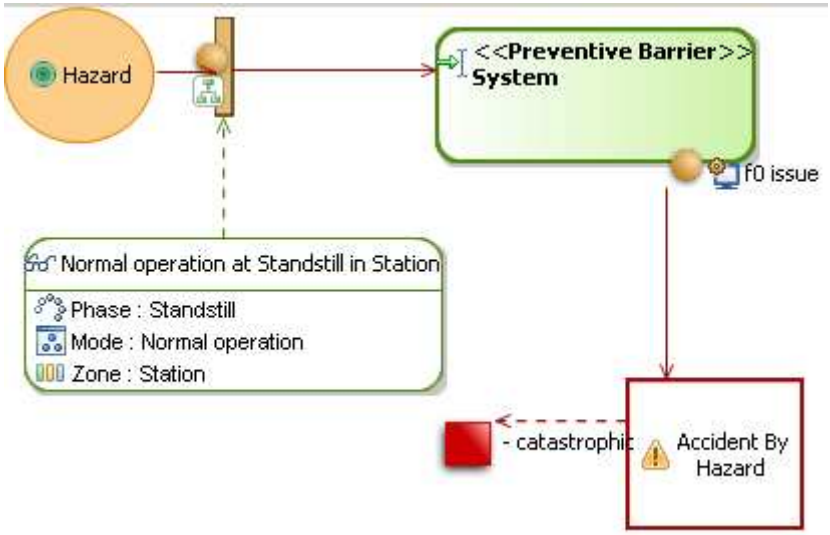





```
Node f1
    sub
      f11Inst : f1_1;
      f12Inst : f1_2;
    flow
      ctxt : ContextType : in;
      y1 : DysData : in;
      y2,y3 : DysData : out;
    state
      st:{Nominal,Fail1,Fail2,Fail3};
    trans
      f11Inst.st=Fail1|- ->st:=Fail1
      f11Inst.st=Fail2|- ->st:=Fail2
      f11Inst.st=Fail3 or
    f12Inst.st=Fail1
          |- -> st:=Fail3
    assert
    f11Inst.ctxt=ctxt; f12Inst.ctxt=ctxt
    y1 = f12inst.i;
    f12Inst.o= f11Inst.i
    y2 = f11Inst.o; y3 = f12Inst.o;
```

Translation of PHA

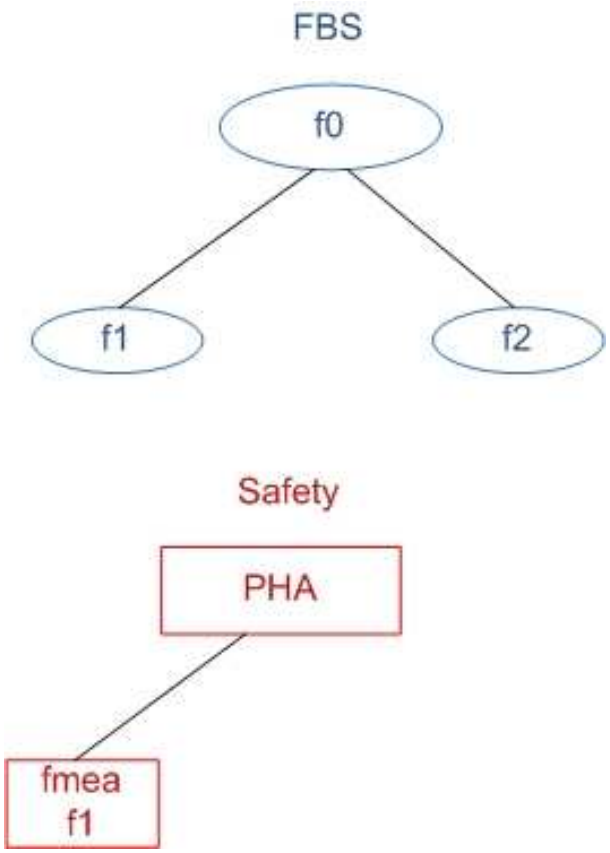


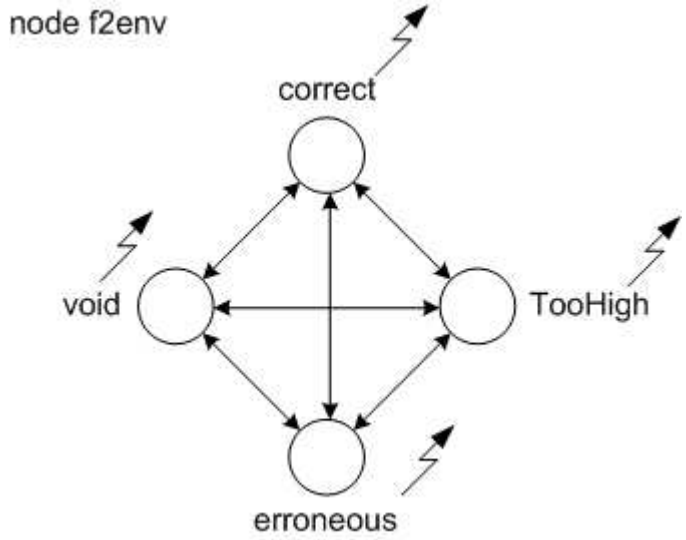


Node PHA
sub
f1Inst : f1; f2Inst : f2;
f3envInst:f3env;
Ctxtinst:CtxtNode;
state
Accident:{No,AccByHazard};
trans
ctxt=c1 and
(f1Inst.st= fail1 or …) and
(f2Inst.st=Fail2 or …) |-
->Accident=AccByHazard;
assert
f3envInst.z= f1Inst.y1;
f2Inst.w1= f1Inst.y2;
f2Inst.w2=f1inst.y3;
Ctxtinst.ctxt=f2Inst.ctxt;
Ctxtinst.ctxt=f1Inst.ctxt;

Automatic Environment generation

The function f2 is not dysfunctionally specified yet





A generic node is created to close the model (wrt datafl

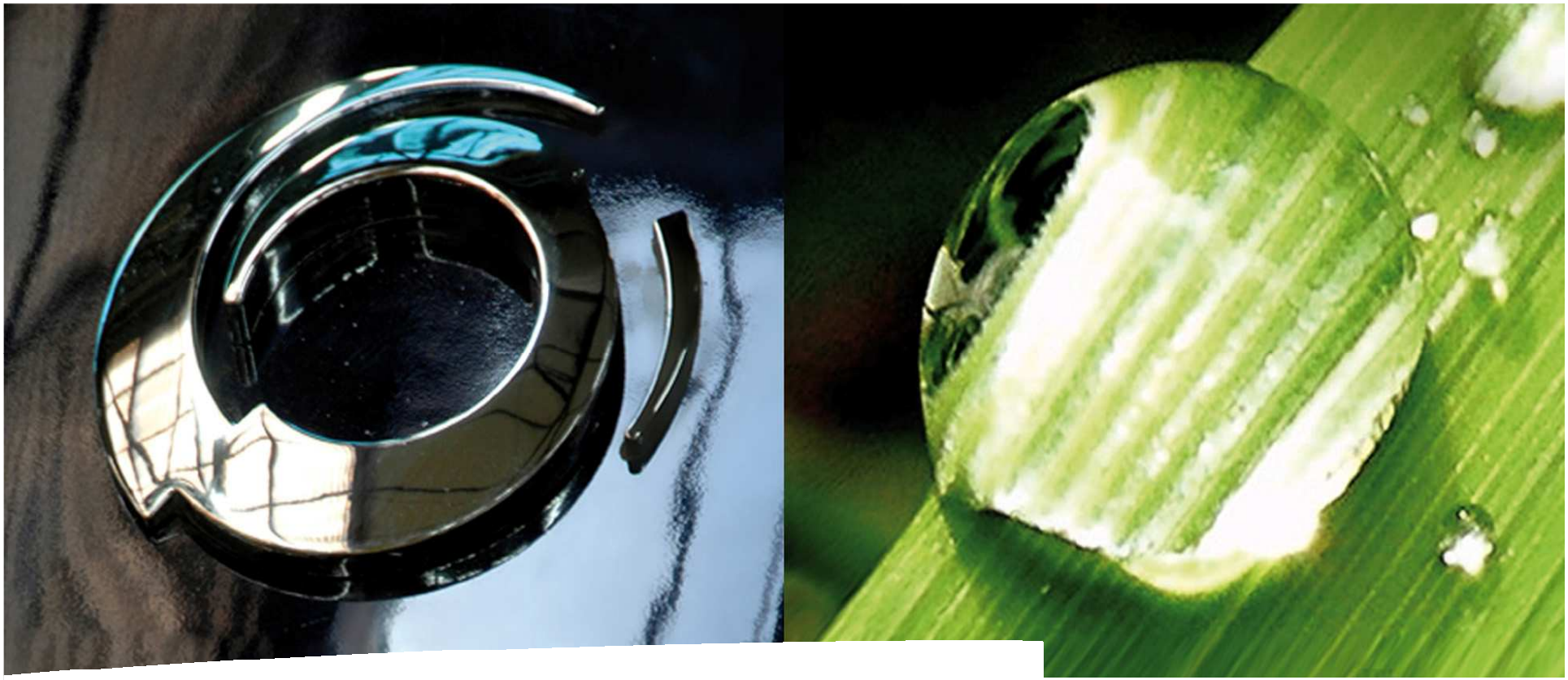
Conclusion

Achieved work

- MBSE process that integrates both system and safety
- DSL for PHA & FMEA on EMF (Obeo Designer)
- Model transformation from DSL & SysML to Altarica
- Computation of accident sequences on a sample model (SD9)

Benefits

- Traceability links between system and safety models
- Formalize the safety analysis with GTS semantic
- Generate complicated Fault trees and Accident Sequences



Alstom Transport