SNETP
Sustainable Nuclear Energy Technology Platform

Simulation Assisted Requirements and Systems Engineering

Conciliating Safety, Innovation and Engineering Efficiency

Thuy NGUYEN
June 2nd, 2022

Who Am I?

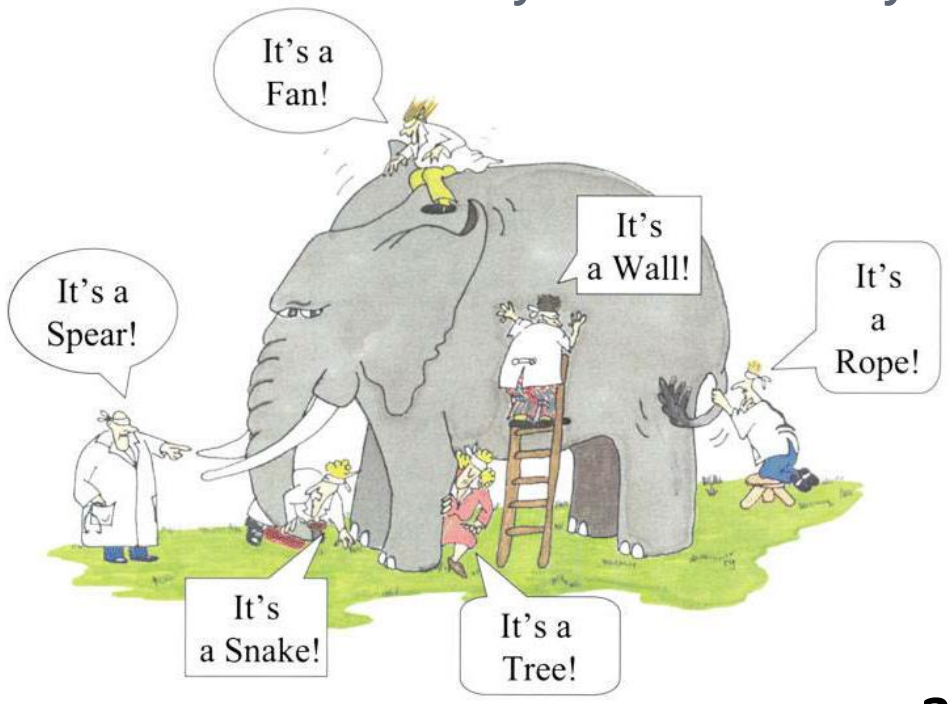
- 1975 - 1994: Software engineer and architect in the general software industry
- 1994 - 2021: Senior research engineer at EDF on digital I&C systems
  - Since 1994: Formal software verification
  - Since 1999: FPGAs for safety applications
  - Since 2007: Simulation assisted requirements and systems engineering
  - Since 2016: NUWARD I&C architect
    - SMR co-designed by EDF, CEA, Technicatome and Naval Group
- Since June 2021: Retired
  - But still active on my favourite subjects of interest

Context

- Nuclear power plants need to be economically competitive
  - In the face of increasingly cost-effective other sources of energy
- Nuclear must innovate while still ensuring high safety levels
  - In a world-wide market but non-harmonized nuclear regulatory landscape
- To this end, efficient engineering is a necessity
  - All along power plants life cycle, from conceptual studies to deconstruction

Systems Engineering (SE) is Important

- Complex systems cannot be understood by single teams and disciplines
  - Coordination of many is necessary



- The later an error is revealed, the more expensive and severe the consequences

and also Logistics, Geography, Weather & Climate, Prospective studies, ...

SNETP
Sustainable Nuclear Energy Technology Platform

Requirements Engineering (RE) is Important

- Defence against CCF
  - Faults in requirements could defeat redundancy, defence-in-depth and diversity (even with functional diversity)
- Confirmed by studies with EPRI
  - For 1E I&C systems, faults in requirements are several times more frequent than faults in software
- Confirmed by OECD COMPSIS

> "Weaknesses in requirements are one of the most significant contributors to systems and software failing to meet the intended goals. A better analysis is needed to understand the software's interfaces with the rest of the system and discrepancies between the documented requirements for a correct functioning system."
> [OECD COMPSIS Project Report – Nov 2011]

- Confirmed by events from all industrial sectors
  - E.g., the civil aviation industry

Need for Improvements in RE & SE

- Dissatisfaction with most mainstream RE approaches
  - Do not address requirements elicitation and validation
  - Do not address requirements meaning and semantics
  - Need to take full account of systems operational environment
- Dissatisfaction also with most mainstream SE approaches
  - Do not fully address development
  - Do not address operation
  - Do not address complexity
  - Do not address RE
  - Ignore techniques as fundamental as simulation
  - Ignore needs as essential as maintenance of engineering and safety knowledge about a system all along its life time

SNETP
Sustainable Nuclear Energy Technology Platform

Defects in Requirements

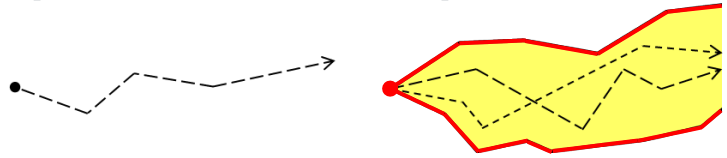
- Inadequacy
  - Where, in some situations, what is specified is woefully inappropriate
- Ambiguity
  - Where different people concerned could interpret what is specified differently
- Apathy
  - Where thre is no difference between what is genuinely needed and what is barely tolerated
- Over-ambition
  - Where what is specified leads to excessive complexity
- Over-specification
  - Where what is specified is not the problem but a technical solution
- Intangibility
  - Where what is specified has no concrete, verifiable acceptance criteria
- Impossibility
  - Where what is specified is not achievable

SNETP
Sustainable Nuclear Energy Technology Platform

Rigorous Requirements Engineering

- To eliminate these defects, one needs to consider the meaning of requirements
- For large and complex systems, manual verification is ineffective and insufficient
- Tool-supported verification needs requirements to be formally specified
  - Simulation, formal verification
  - But models must also be understood by all those concerned

- To avoid over-specification, need for constraint-based requirements specification



- Requirements adequacy depends on assumptions
- A requirement may be adequate in some situations, but not in others
  - Need to explore the set of situations the system may face during its life time

SNETP
Sustainable Nuclear Energy Technology Platform

Modelling

- Many different types of models
  - Requirements models
  - Functional models
  - Probabilistic models
  - Economic models
  - Operational procedures
  - Task scheduling models
  - Process & multi-physics models
  - …

Behavioural modelling (dynamic phenomena)

BASAALT: Behaviour Analysis & Simulation All Along systems Life Time

FORM-L: FOrmal Requirements Modelling Language

- Geometric & Topological models
- Geographic models
- Engineering databases
- …

Other forms of modelling

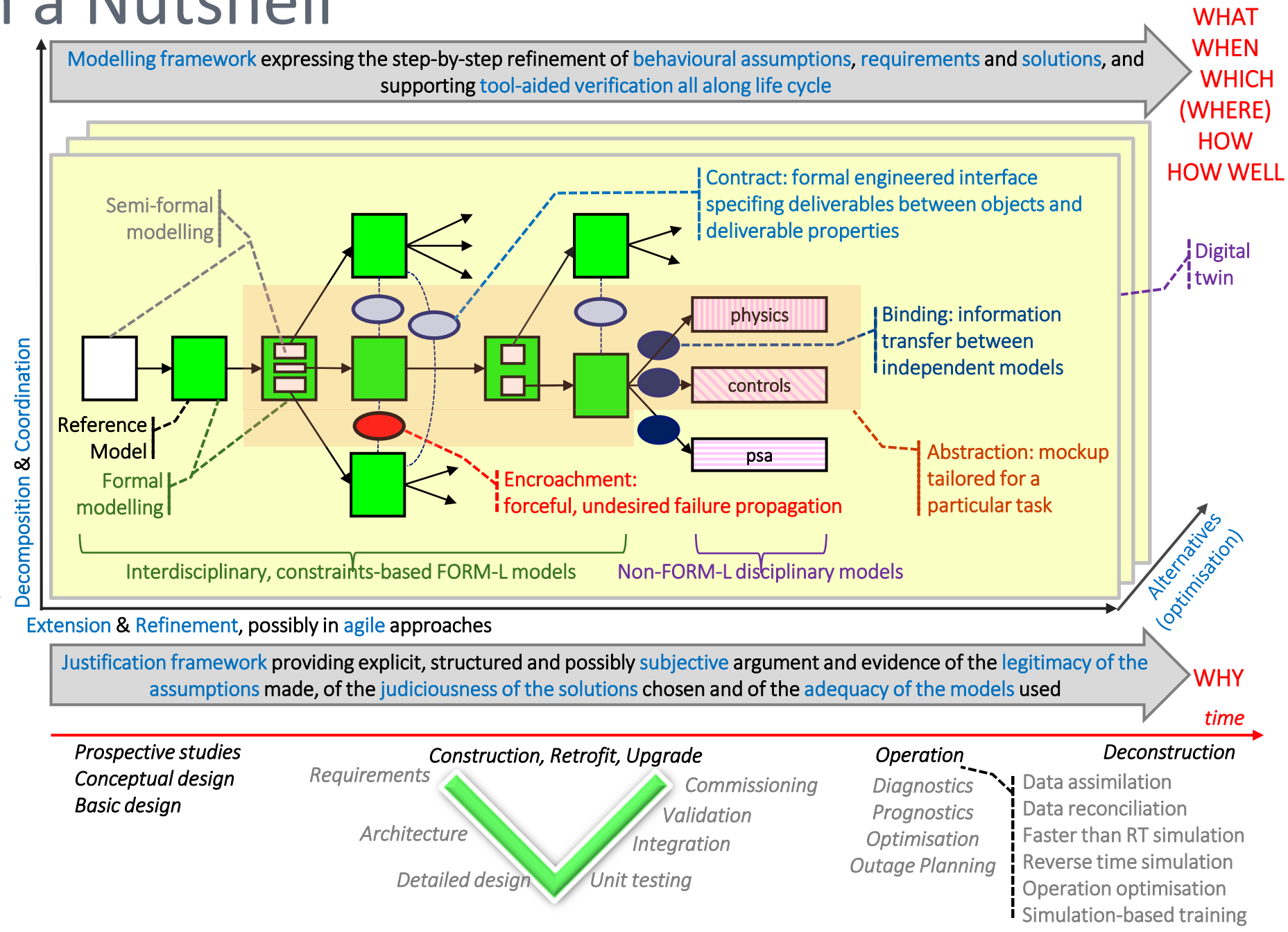
MESKAAL: Maintenance of the Engineering and Safety Knowledge about a system All Along its Life time

- Modelling thriftiness
- Model-assisted teams coordination

SNETP
Sustainable Nuclear Energy Technology Platform

BASAALT in a Nutshell

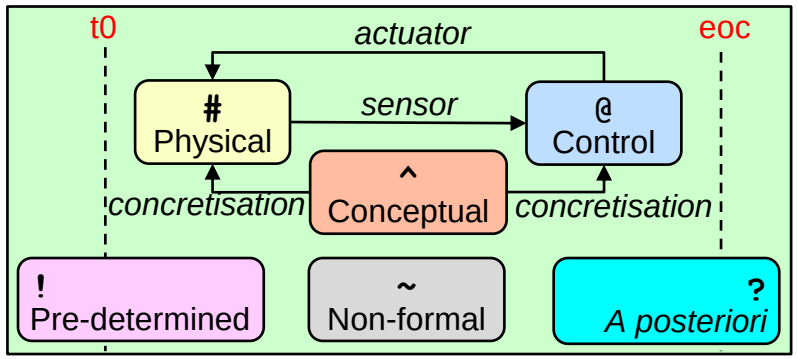
- Modelling **modularity**
  - Keeping track of **engineering progress** along life time
  - Enabling **teams coordination**
  - Expressing **system decomposition**
- Models used for development are an **investment** for operation, upgrades and deconstruction



SNETP
Sustainable Nuclear Energy Technology Platform

FORM-L in a Nutshell

Determiners



Behavioural Items

- **Variables** (Booleans, statecharts, Integers, Reals, quantities, Strings)
- **Events**
- **Sets** (of items or of values)
- **Properties**, Assumptions, Objectives, Requirements, Guarantees, Guards
- **Objects** (static, or dynamic creation / deletion)

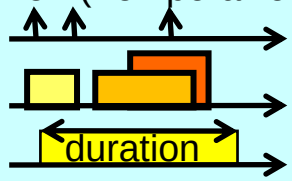
Time Domains (in Newtonian time)

One single **Continuous Time Domain** for physical processes & human actions

Multiple **Discrete Time Domains** for Globally Asynchronous but Locally Synchronous (GALS) digital systems

Elementary Instructions

When (Temporal locators)



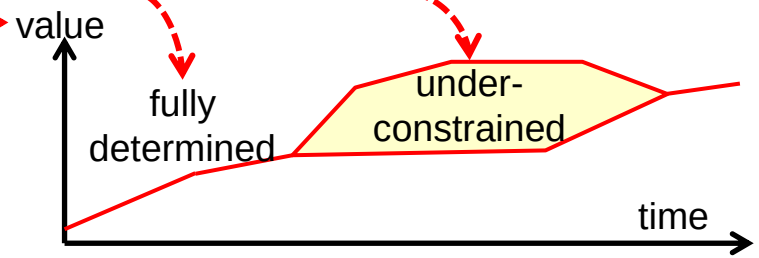
Who / Which (Selectors: universal or existential quantifiers)

Where (Spatial locators)

What, How, How well

- Dynamic object creation
- Dynamic object deletion
- Assignments

A posteriori constraints	Invariance	Achievement
Operation-time constraints	Invariance constraints	Achievement constraints
Systematic constraints	*ensure*	achieve
Capability constraints	*assert* X, Y *can ensure*	*assert* X, Y *can achieve*



Composite Instructions

Time exclusion	**Sequence**
Set exclusion	**Concurrence**
Selection	**Iteration**
(Boolean or probabilistic)	

Interfaces (coordination, co-simulation)

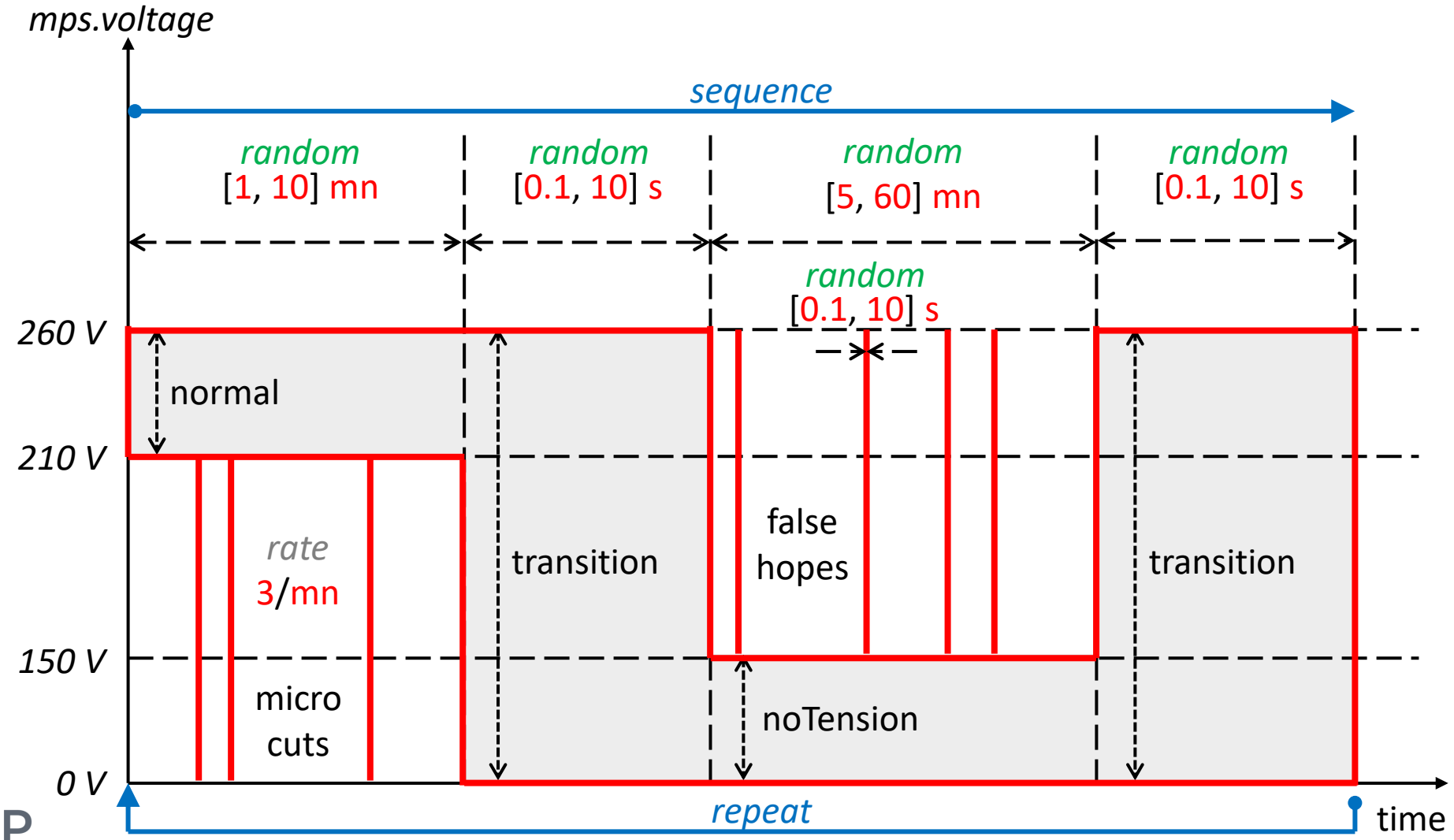
Contracts (Engineered, mutually agreed interfaces between concerned parties)

Party
- Deliverables (variables, events, sets, objects)
- Properties of deliverables

Encroachments (Undesired, forceful failure propagation)

Bindings (enabling co-simulation of FORM-L models developed independently or with non FORM-L models)

Example of Envelope
Electric Voltage at a Power Supply Terminals



SNETP
Sustainable Nuclear Energy Technology Platform

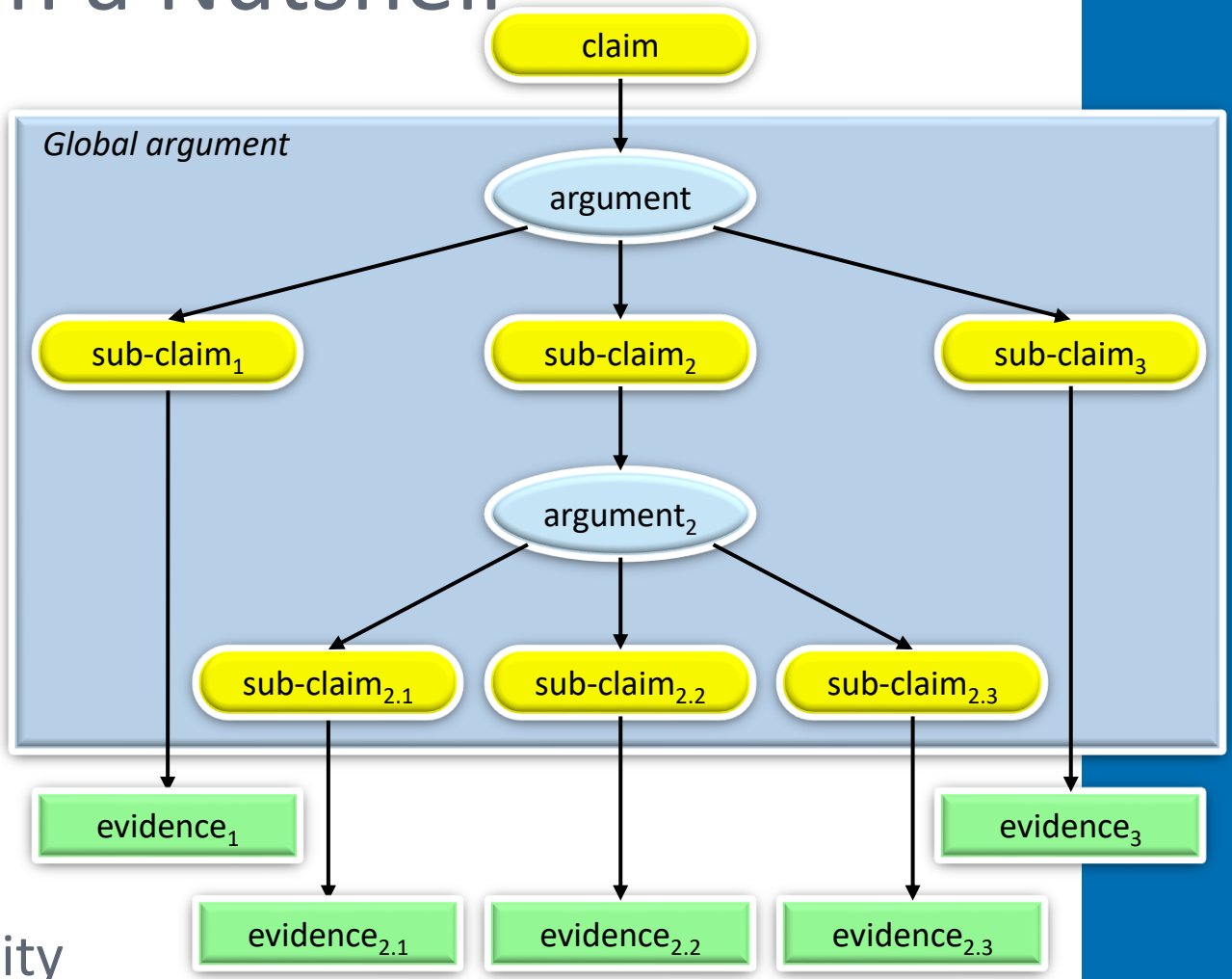
Example of Envelope
Electric Voltage at a Power Supply Terminals

```
mps.voltage begin
  private Event eMicroCut "Micro cuts or false hopes": rate is 3/mn;
  from t0 repeat sequence
    during random (1, 10)*mn
      from eMicroCut during random (0.1, 10)*s Assumption microCut is
        ensure                                 derivative in [-1000, 1000]*V/s
      otherwise Assumption normalTension is
        ensure value in [210, 260]*V and derivative in [  -10,   10]*V/s;
    during random (0.1, 10)*s Assumption transition is
        ensure                                 derivative in [-1000, 1000]*V/s;
    during random (5, 60)*mn
      from eMicroCut during random (0.1, 10)*s Assumption falseHope is
        ensure                                 derivative in [-1000, 1000]*V/s
      otherwise Assumption noTension is
        ensure value in [  0, 150]*V and derivative in [ -100,  100]*V/s;
  end sequence;
end mps.voltage;
```

SNETP
Sustainable Nuclear Energy Technology Platform

Justification Framework in a Nutshell

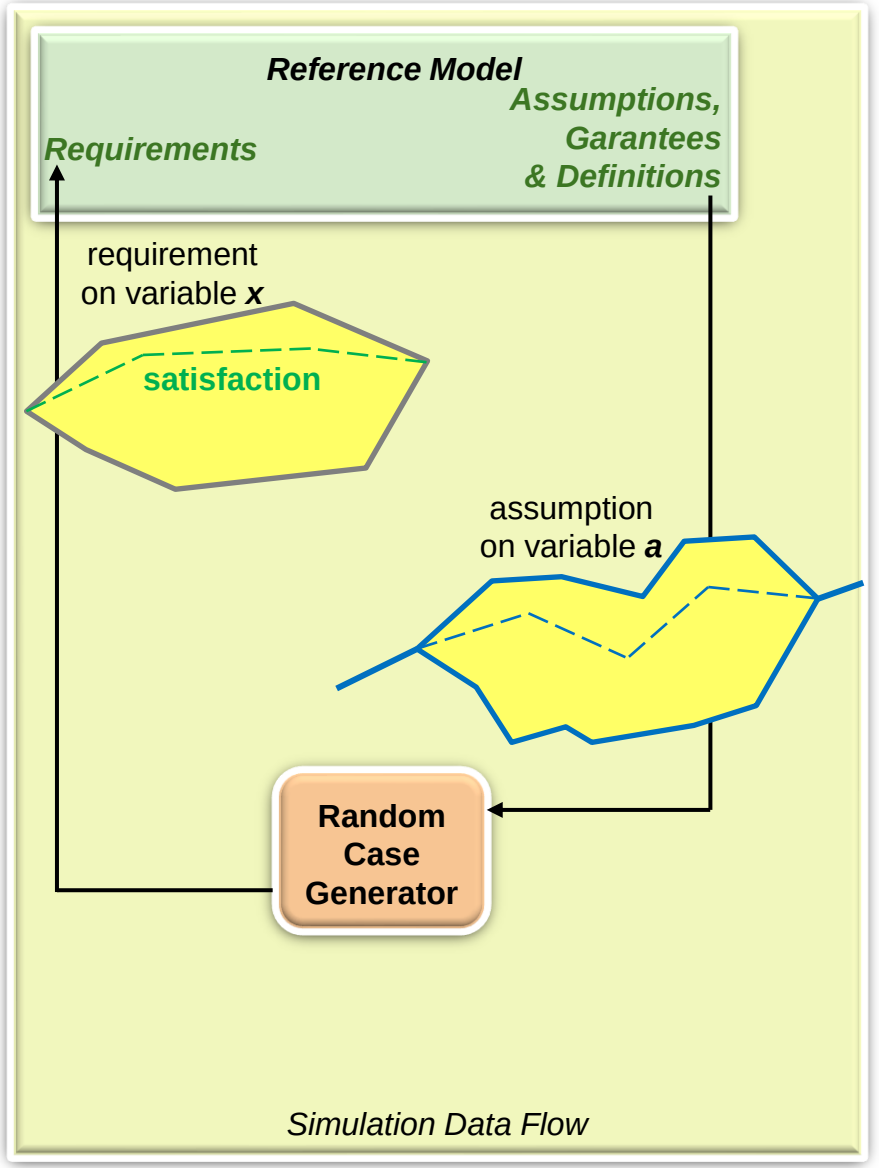
- May be used to express in a structured manner the rationales behind decisions
  - Can express rigorous and objective, qualitative and subjective aspects
  - More informative than simple traceability links
- Complementary to the modelling framework
  - ISO - IEC - IEEE 15026-2 (2011)
  - EURATOM project HARMONICS (Harmonised Assessment of Reliability of MOdern Nuclear Instrumentation and Control Software, 2011-2015)



SNETP
Sustainable Nuclear Energy Technology Platform

Simulation of Constraint-Based Models

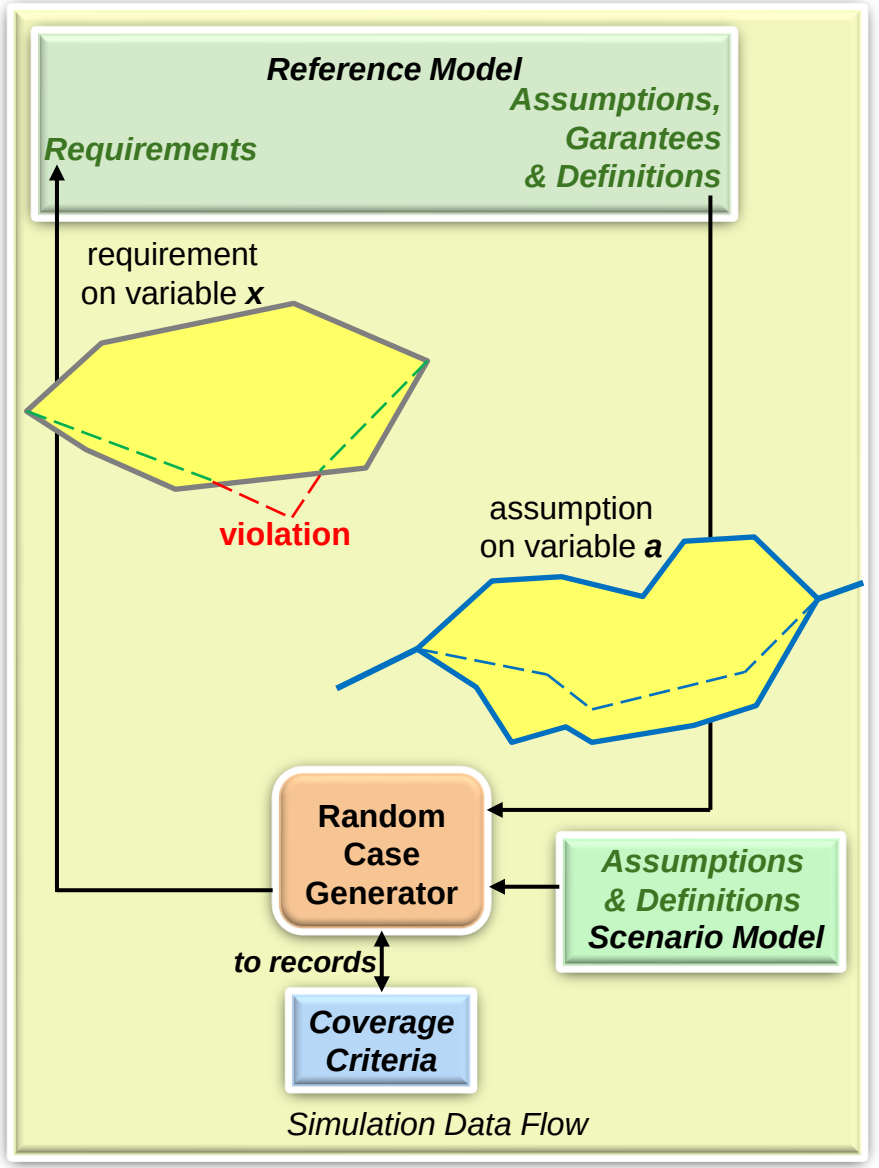
- Tools like StimuLus can randomly generate any number of different test cases consistent with definitions and constraints
  - To automatically explore large sets of possible situations arising from the full operational context
  - Taking account of normal and failure behaviours
  - Including human actions and errors



SNETP
Sustainable Nuclear Energy Technology Platform

Simulation of Constraint-Based Reference Models

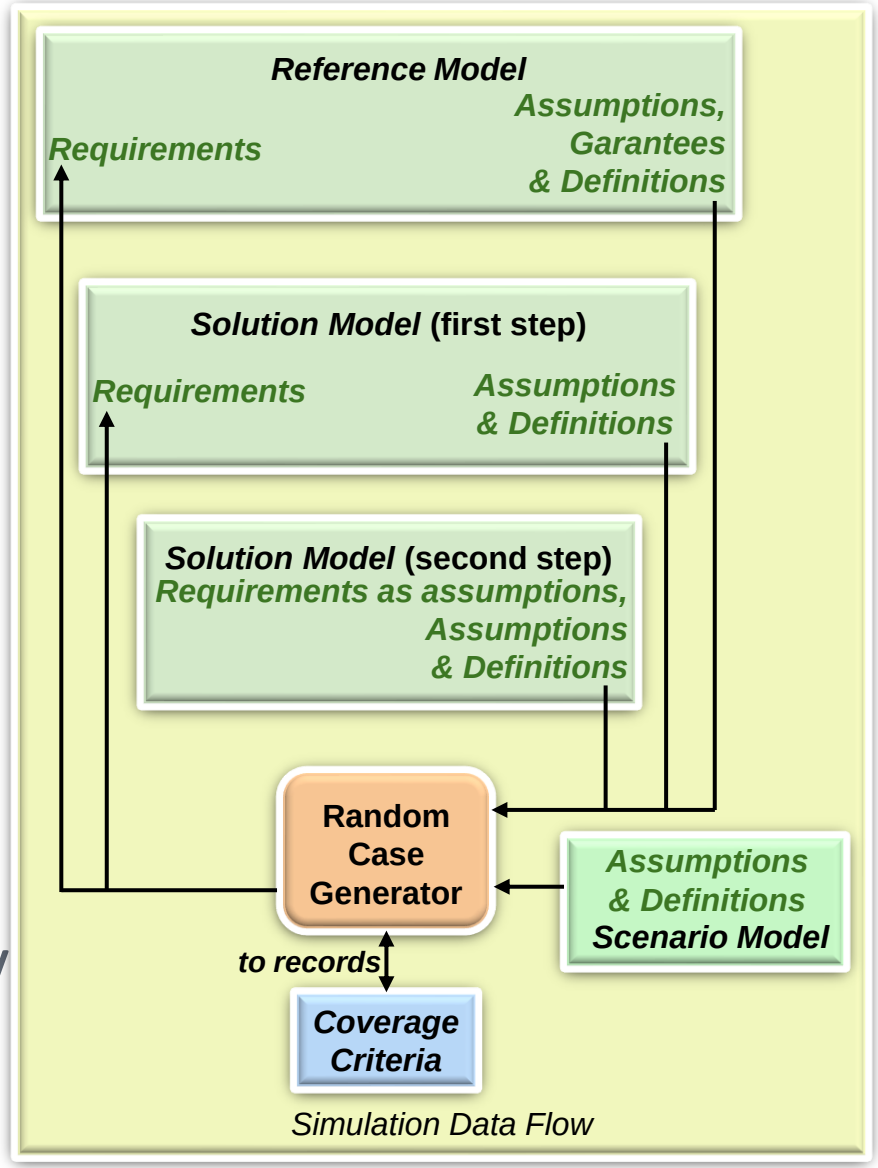
- Tools like StimuLus can randomly generate any number of different test cases consistent with definitions and assumptions
- Scenario Models may be used to guide the generator towards cases of interest
- Coverage criteria may be used to help ensure that models are sufficiently tested



SNETP
Sustainable Nuclear Energy Technology Platform

Simulation of Constraint-Based Solution Models

- Solution models may be validated step-by-step against the requirements of earlier models
- Even for relatively simple systems, the number of cases to consider is a challenge for purely manual techniques
- Automated verification may be reapplied at limited cost and delay after each modification
- Alternative solutions (optimisation) may also be assessed at limited cost and delay



SNETP
Sustainable Nuclear Energy Technology Platform

Conclusion

- BASAALT and FORM-L are still works in progress
  - Formal specification of FORM-L grammar and semantics
  - Development of translators towards existing modelling languages that already have support tools
    - E.g., StimuLus, Modelica, Scade, Figaro, ...
  - Development of variants other than the English variant
    - E.g., French, German, Swedish variants
  - Development of a graphical FORM-L representation
  - Development of appropriate test coverage criteria
  - Introduction of spatial locators in 3D, 2D and 1D spaces
    - Einsteinian, relativistic space-time could also be considered, but that could add significant complexity to the language

Thank you for your attention

Questions ?

SNETP
Sustainable Nuclear Energy Technology Platform