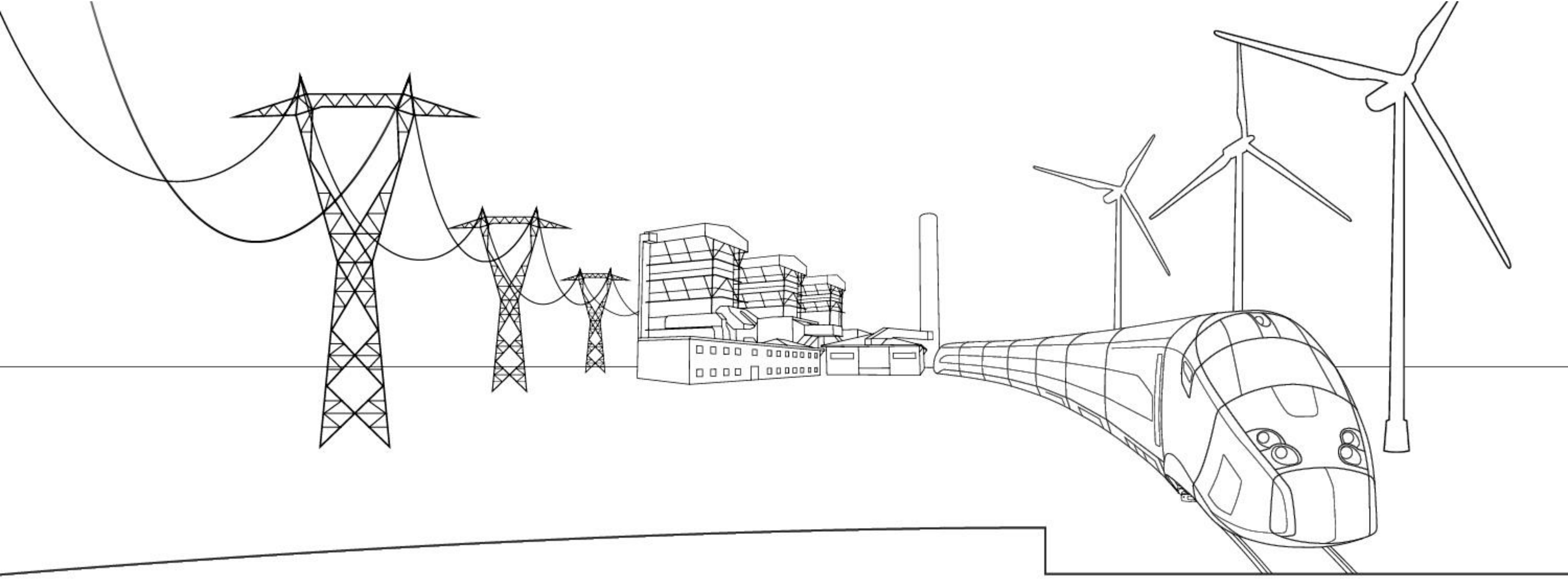


New modelling approach to construct Test model for railway embedded systems

Amine Mechraoui, Pascal Poisson, Elie Soubiran

UCAAT 2013

23/09/2013

Agenda

- **Introduction of ALSTOM Company and Industrial context**
- **Operational constraints: Safety and test quality**
- **Proposed methodology**
- **Implementation within a MBT framework : Results and limitations**
- **Ongoing development**

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

Signaling systems are safety critical

Ruled by Cenelec Norm:

- Excerpt:
  - "*The Assessor shall assess* […] *that the validation responds correctly to safety issues derived from the System Safety Requirements Specification.*"
  - "[…] *Verify the evidences* […] *appropriate set of techniques* […] *for the intended development*"

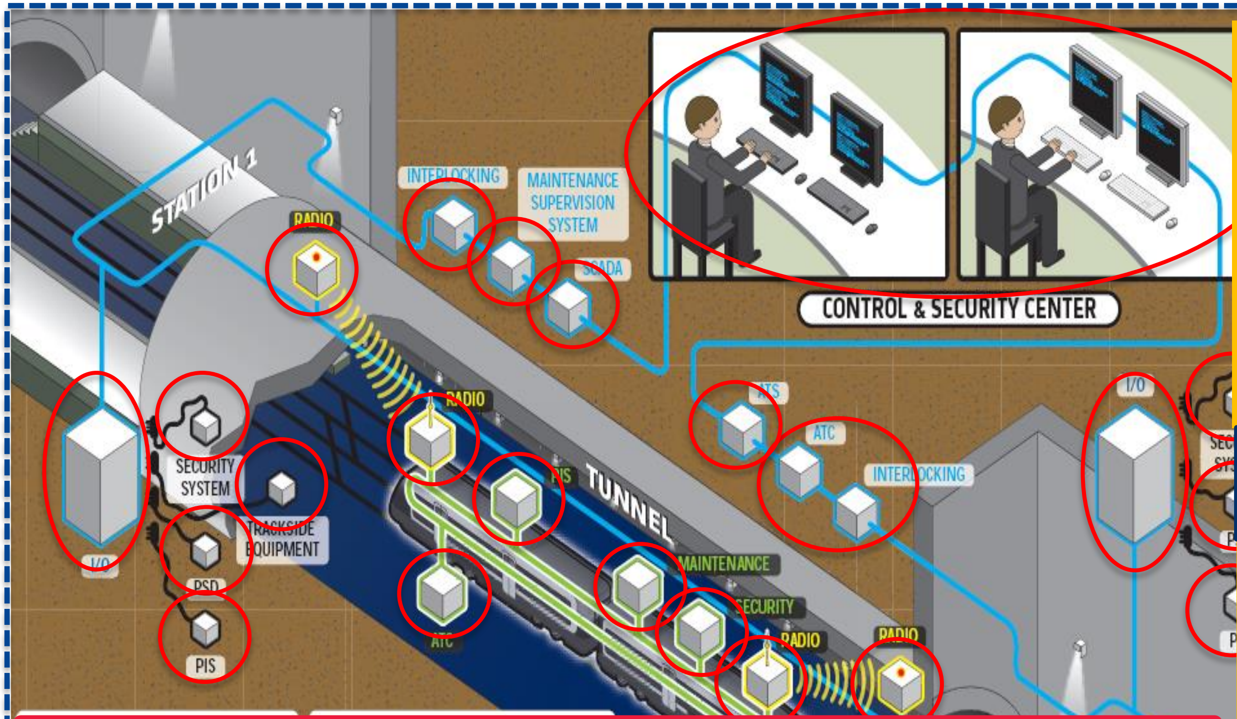
= A big bunch of work !

Platform, Concurrent Engineering, rework…….

The whole assessment cannot be redone each time: Impact analysis is done

Deterministic test case generation must be applied to cope with the objectives and constraints

Signalling system are complex



In this complex system context Test coverage can be broadened only by dynamic test case generation … at an affordable cost

- Specific exploitation rules
- Local or national signaling rules
- Specific topology
- Specific Rolling Stock

This is Thousands of parameters

- Defining the system behavior
- Characterizing the environment

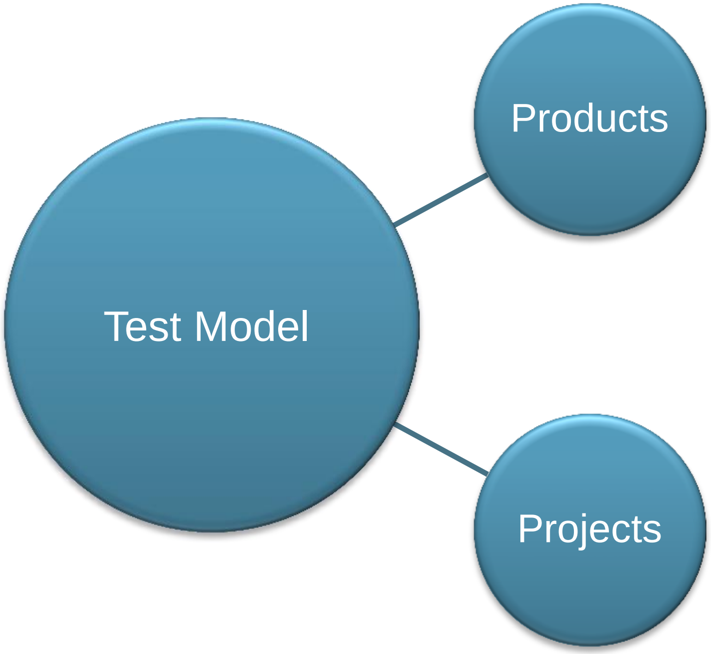
Proposed Methodology : Modularity

Re-use of models

- **Capitalize environments and sub-system models**
- **Combine them regarding the validation phase**

- **Products validation**: Combine sub-system model with a stochastic environment model.
  - Validate the product regarding a wide range of randomly generated environment.

- **Projects validation**: Combine sub-system model with static environment models (one per project).
  - Consolidate the product regarding a specific topology



- Sub-system 1
- Sub-system 2
- …
- Sub-system n

- Environment 1
- Environment 2
- …
- Environment m

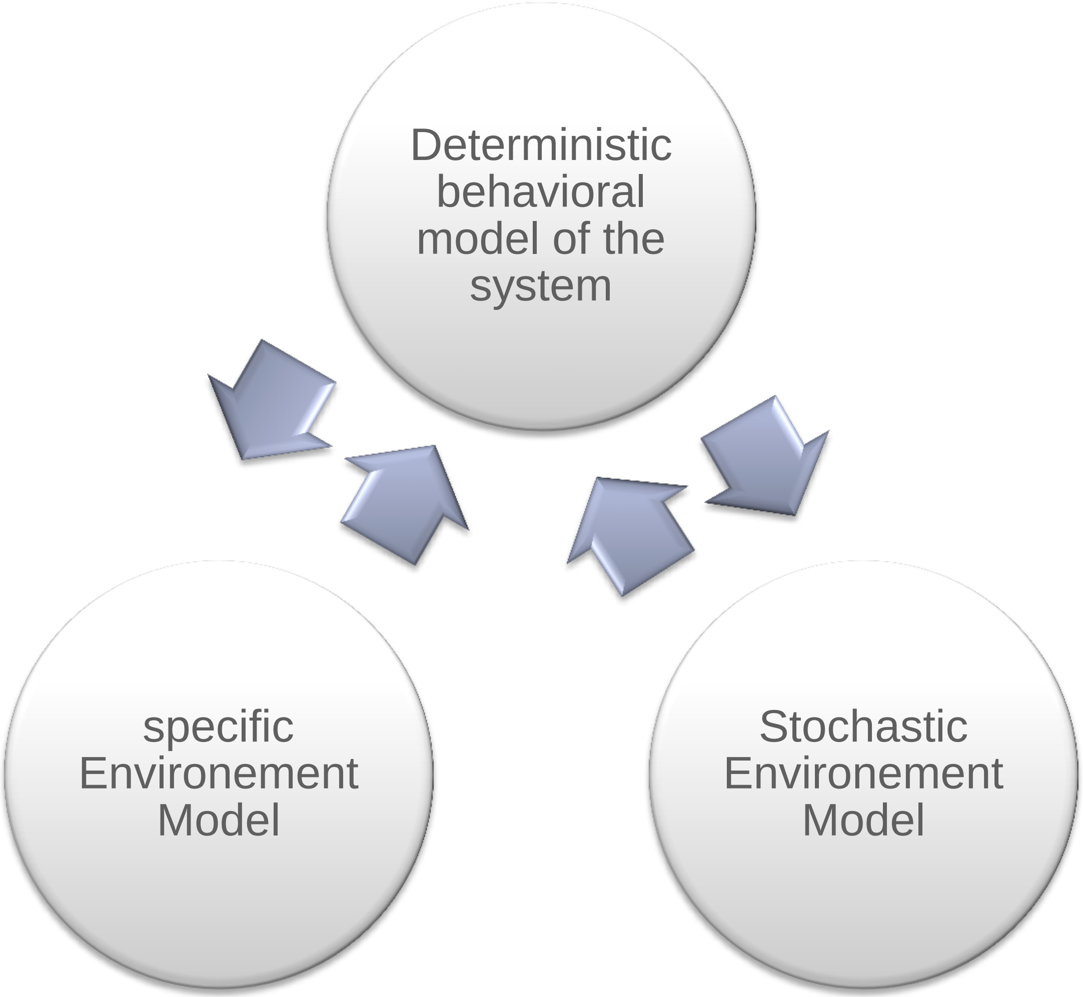
Proposed Methodology : Handle complexity and safety

Combine Determinism and Randomness

- Why deterministic generation?
  - ✓ Safety critical systems: safety function reacts deterministically relatively to a safety issue
  - ✓ Operational behavior: given a context the system always acts as intended by the operator
  - ✓ Deterministic generation: minimize the impact on safety assessment regarding changes and iterations.

- Why random generation?
  - ✓ Support the exponential combination of parameters specific to signalling system
  - ✓ Generate randomly operational contexts to stimulate the SUT and then to detect a maximum number of errors

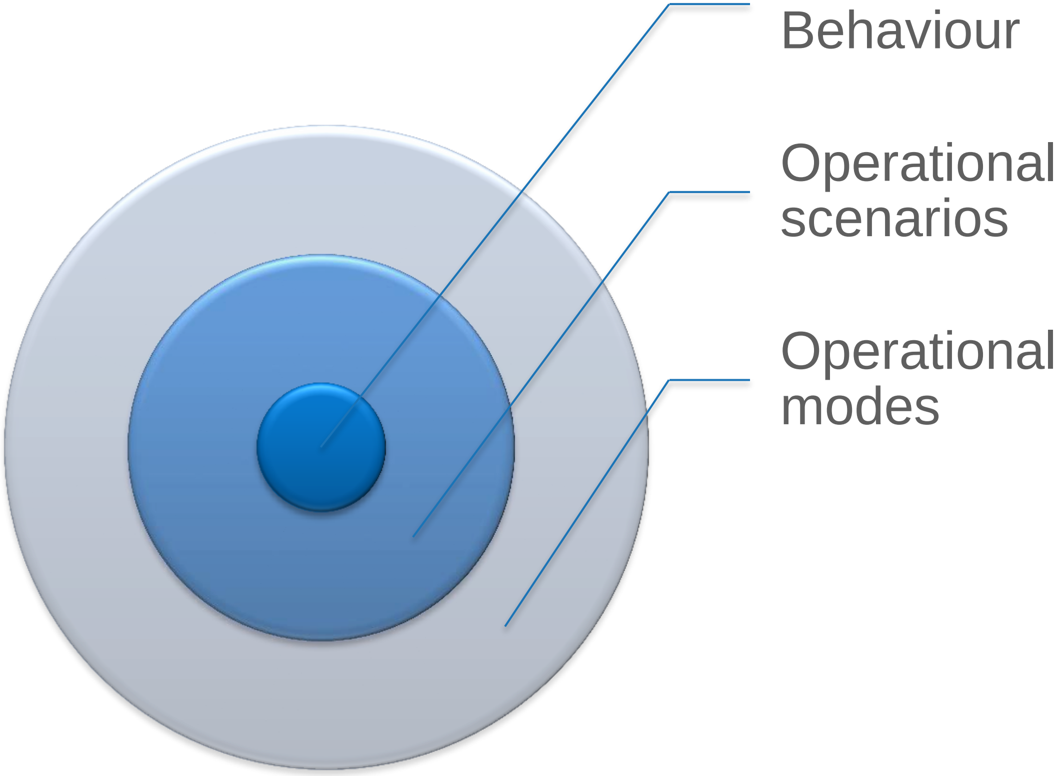
Target generic or specific systems


Deterministic behavioral model of the system
specific Environement Model
Stochastic Environement Model

Proposed Methodology : Operational first

Test Model

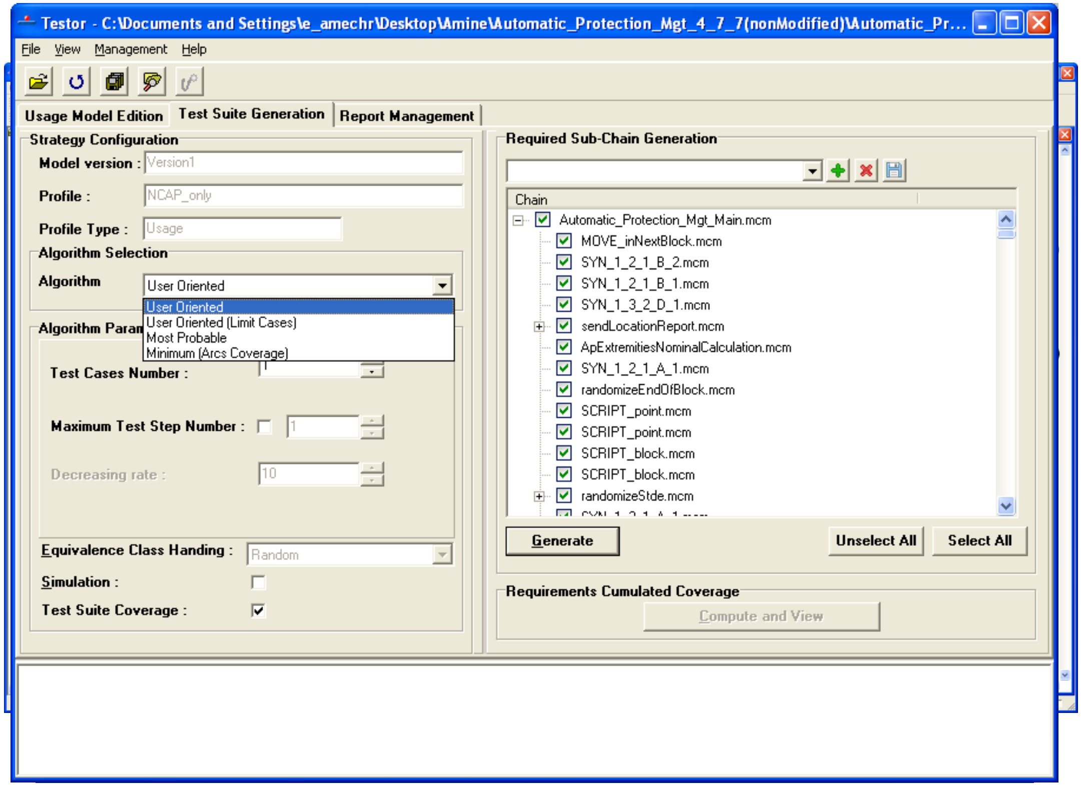
- For the environement:
  - What are the operational contexts?
- For the System:
  - What are the operational modes?
  - What are the operational scenarios for each operational mode?
  - How it will behave according to each oparational context and to each operational mode?



Implementation within MBT framework

MaTeLo implementation

- Each Level of the Modelling Diagram is represented in MaTeLo with an hierarchical level (Sub-chains)
- The operational scenarios are modelled using the concept of « conditions »
- Missions behavior include Scilab functions & Expected Results
- Radom generation is performed using Radom Algorithms proposed within MaTeLo



Testor - C:\Documents and Settings\e_amechr\Desktop\Amine\Automatic_Protection_Mgt_4_7_7(nonModified)\Automatic_Pr...

Strategy Configuration

Model version : Version1

Profile : NCAP_only

Profile Type : Usage

Algorithm Selection

Algorithm: User Oriented

- User Oriented
- User Oriented (Limit Cases)
- Most Probable
- Minimum (Arcs Coverage)

Algorithm Param

Test Cases Number : 1

Maximum Test Step Number : □ 1

Decreasing rate : 10

Equivalence Class Handing : Random

Simulation : □

Test Suite Coverage : ☑

Required Sub-Chain Generation

Chain

- ☑ Automatic_Protection_Mgt_Main.mcm
  - ☑ MOVE_inNextBlock.mcm
  - ☑ SYN_1_2_1_B_2.mcm
  - ☑ SYN_1_2_1_B_1.mcm
  - ☑ SYN_1_3_2_D_1.mcm
  - ☑ sendLocationReport.mcm
  - ☑ ApExtremitiesNominalCalculation.mcm
  - ☑ SYN_1_2_1_A_1.mcm
  - ☑ randomizeEndOfBlock.mcm
  - ☑ SCRIPT_point.mcm
  - ☑ SCRIPT_point.mcm
  - ☑ SCRIPT_block.mcm
  - ☑ SCRIPT_block.mcm
  - ☑ randomizeStde.mcm

Results and tool limitations

Structuring Methodology →

✓ Share a common understanding of validation model
✓ Minimise modelling errors
✓ Facilitate impact analysis

Stochastic model of environment →

✓ Increase test coverage at product validation phase
✓ Avoid a maximum of iteration during projects

Deterministic models →

✓ Cover safety and operational scenario
✓ Validate sub-system on a specific environment

Modularity →

✓ Facilitate re-use
✓ Save time, reduce cost

Model Construction →

○ Consume Effort & Time

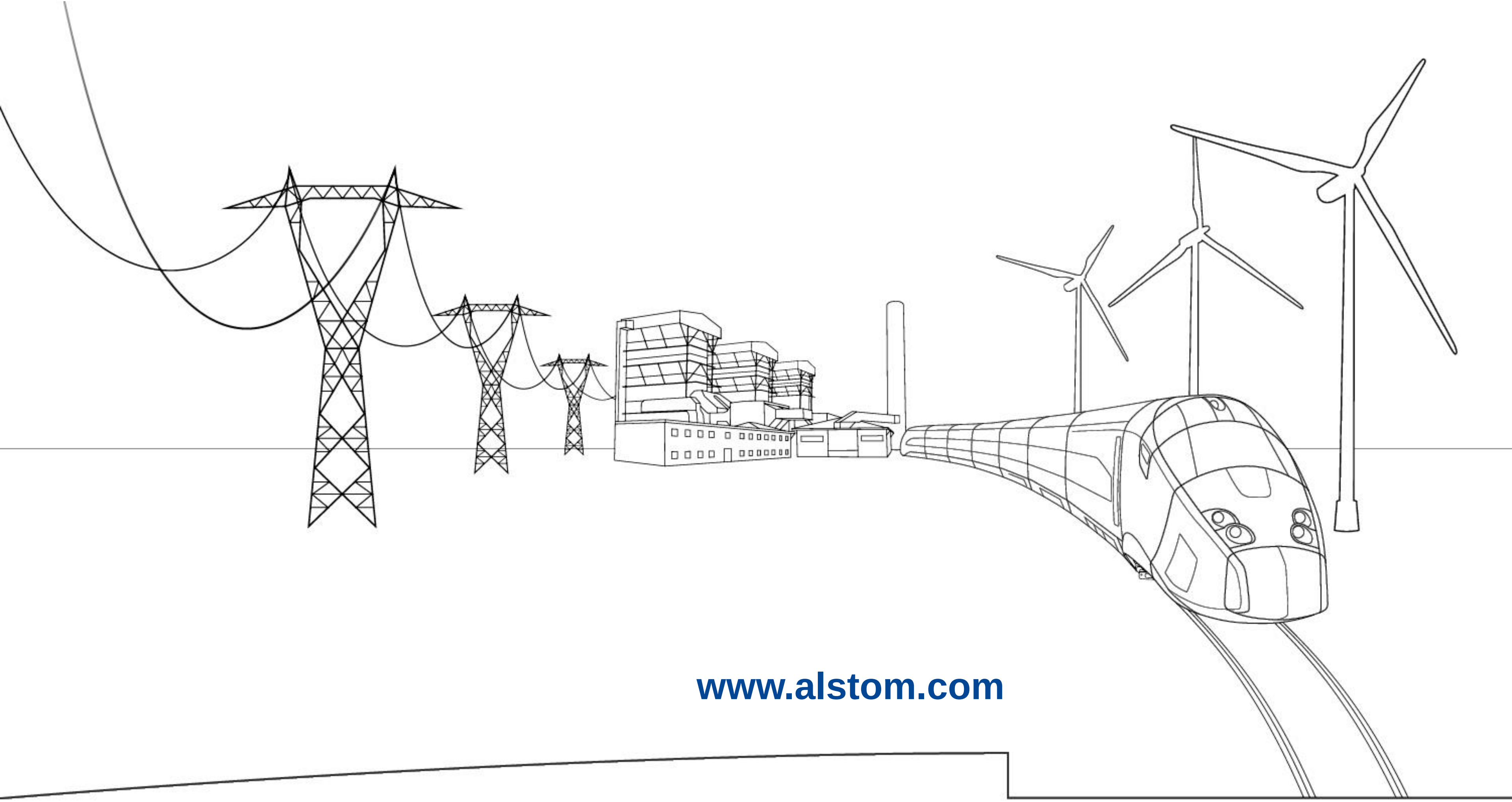
Tool Limitation →

○ Combining Random and deterministic approaches is not well integrated in tools
○ Covering paths does not apply covering safety and operational objectives

Ongoing Developpements

Large test base versus precise test objectives: how to?

- Deciding whenever a generated test base covers precise safety and operational objectives is a hard problem.
- **Idea**: Formalise operational use case, equivalence classes, boundaries constraints, dysfunctional scenario… as formal statements and then model check your test base.
- **Advantages:**
  - Powerful modal logic to formalise dynamic scenario
  - Not intrusive, keep your behavioural model simple
  - Discriminate test cases regarding objectives (and not path of your model)
- Tools: MaTeLo for TCG and Artimon (CEA) for analysis



www.alstom.com

ALSTOM
Shaping the future