Certification Aspects in Critical Embedded SW Development with Model Based Techniques

DETECTION OF UNINTENTED FUNCTIONS

INNOVATING SOLUTIONS

European Aviation Safety Agency (EASA). Objective:

Safety implications in performing **SO**ftware **M**odel **C**overage **A**nalysis

CONTEXT

EASA

CERTIFICATION

V&V COVERAGE

EASA regulatory framework, get airworthiness type certification.

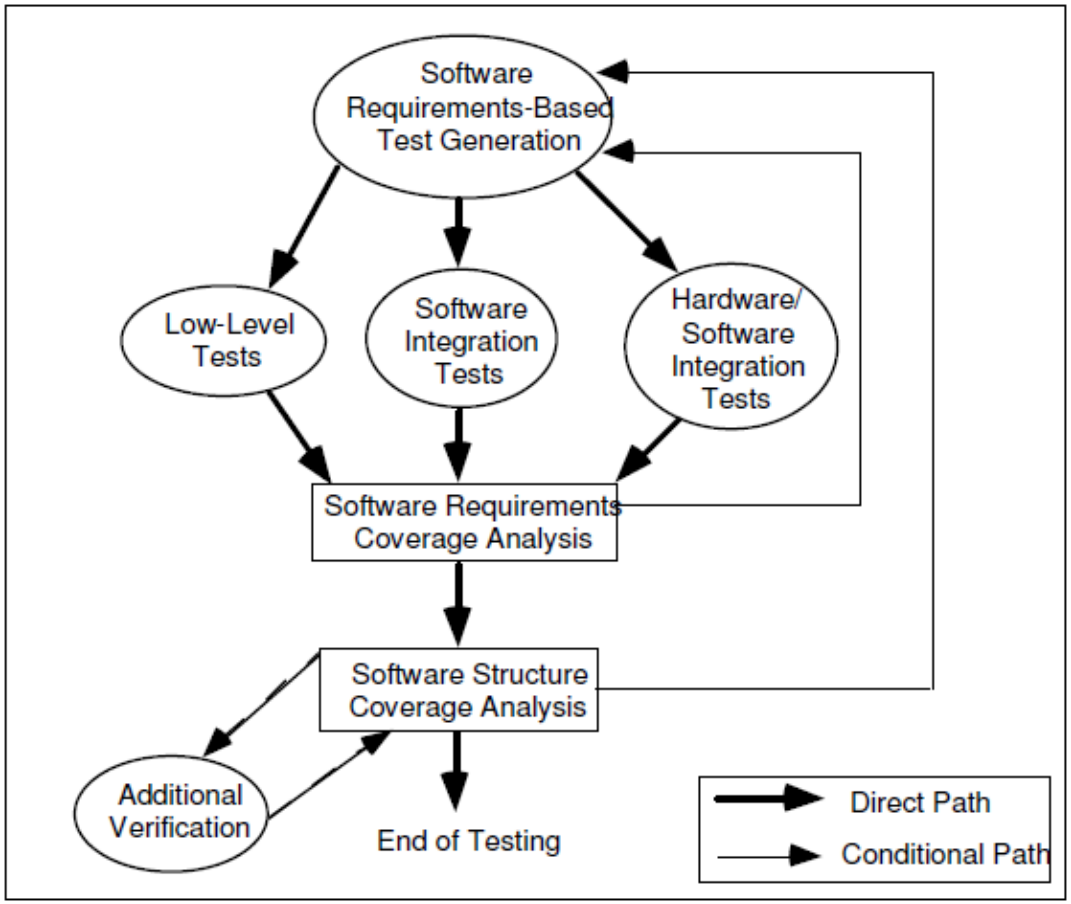
Certification Specification CS 25.1309

The aeroplane equipment and systems must be designed and installed so that those required for type certification or by operating rules, or whose improper functioning would reduce safety, ***perform as intended*** *under the aeroplane operating and environmental conditions*

AMC 25.1309 recognises
ED-12B / RTCA DO-178B

ED-12B/DO-178B

- Product **Assurance** + Verification **coverage** criteria.
- SW Testing Process: Test Coverage Analysis



Source: RTCA DO-178B

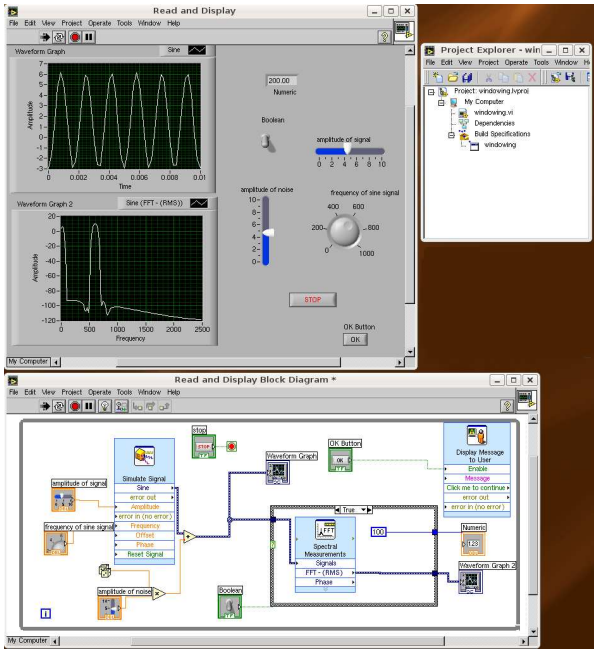
DO-178B Test Coverage Criteria

	Objective		Applicability by SW Level				Output		Control Category by SW level			
	Description	Ref.	A	B	C	D	Description	Ref.	A	B	C	D
1	Test procedures are correct.	6.3.6b	Δ	B	B		Software Verification Cases and Procedures	11.13	②	②	②	
2	Test results are correct and discrepancies explained.	6.3.6c	Δ	B	B		Software Verification Results	11.14	②	②	②	
3	Test coverage of high-level requirements is achieved.	6.4.4.1	Δ	B	B	B	Software Verification Results	11.14	②	②	②	②
4	Test coverage of low-level requirements is achieved.	6.4.4.1	Δ	B	B		Software Verification Results	11.14	②	②	②	
5	Test coverage of software structure (modified condition/decision) is achieved.	6.4.4.2	Δ				Software Verification Results	11.14	②			
6	Test coverage of software structure (decision coverage) is achieved.	6.4.4.2a 6.4.4.2b	Δ	Δ			Software Verification Results	11.14	②	②		
7	Test coverage of software structure (statement coverage) is achieved.	6.4.4.2a 6.4.4.2b	Δ	Δ	B		Software Verification Results	11.14	②	②	②	
8	Test coverage of software structure (data coupling and control coupling) is achieved.	6.4.4.2c	Δ	Δ	B		Software Verification Results	11.14	②	②	②	

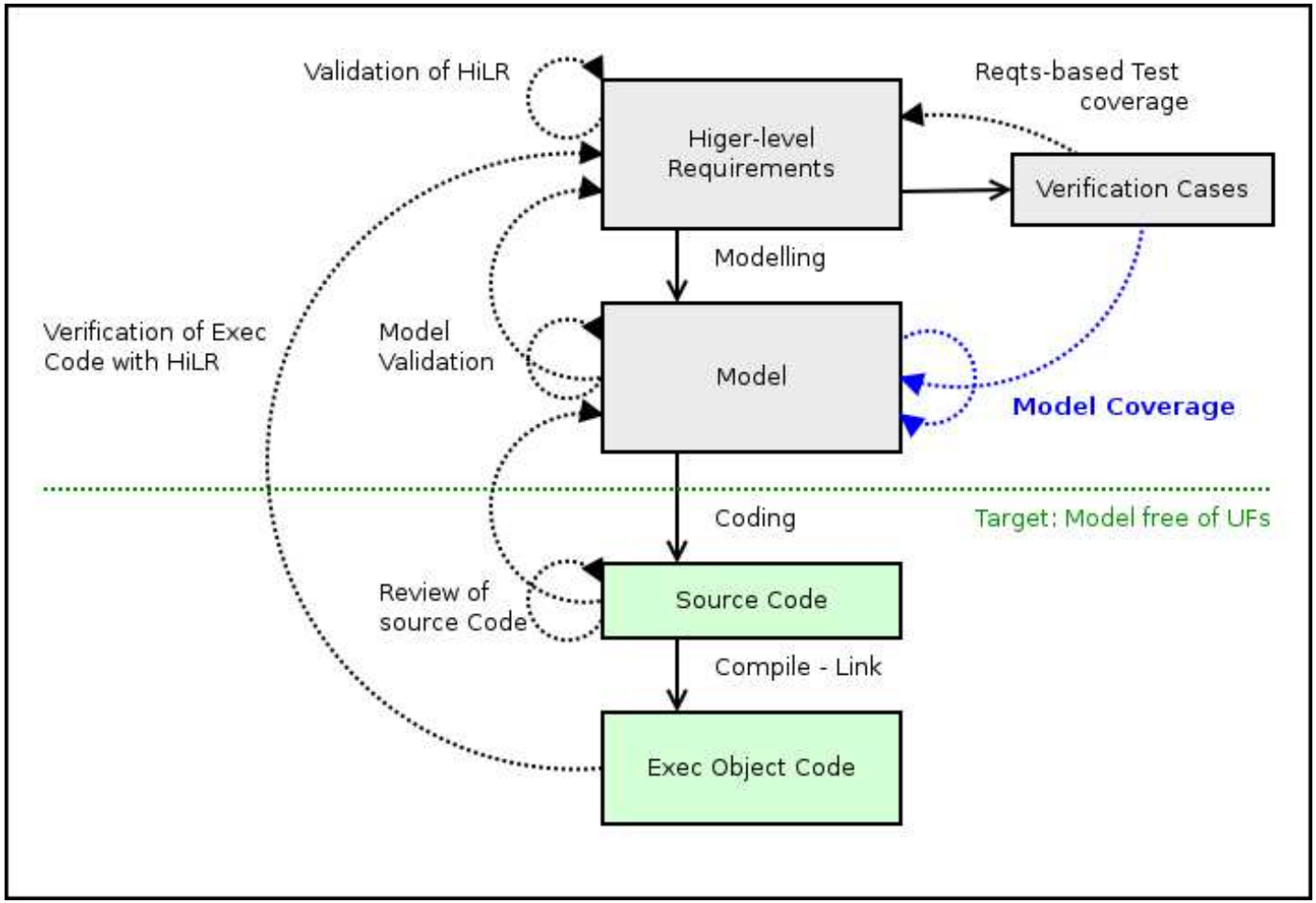
Source: RTCA DO-178B

Modelling Formalisms

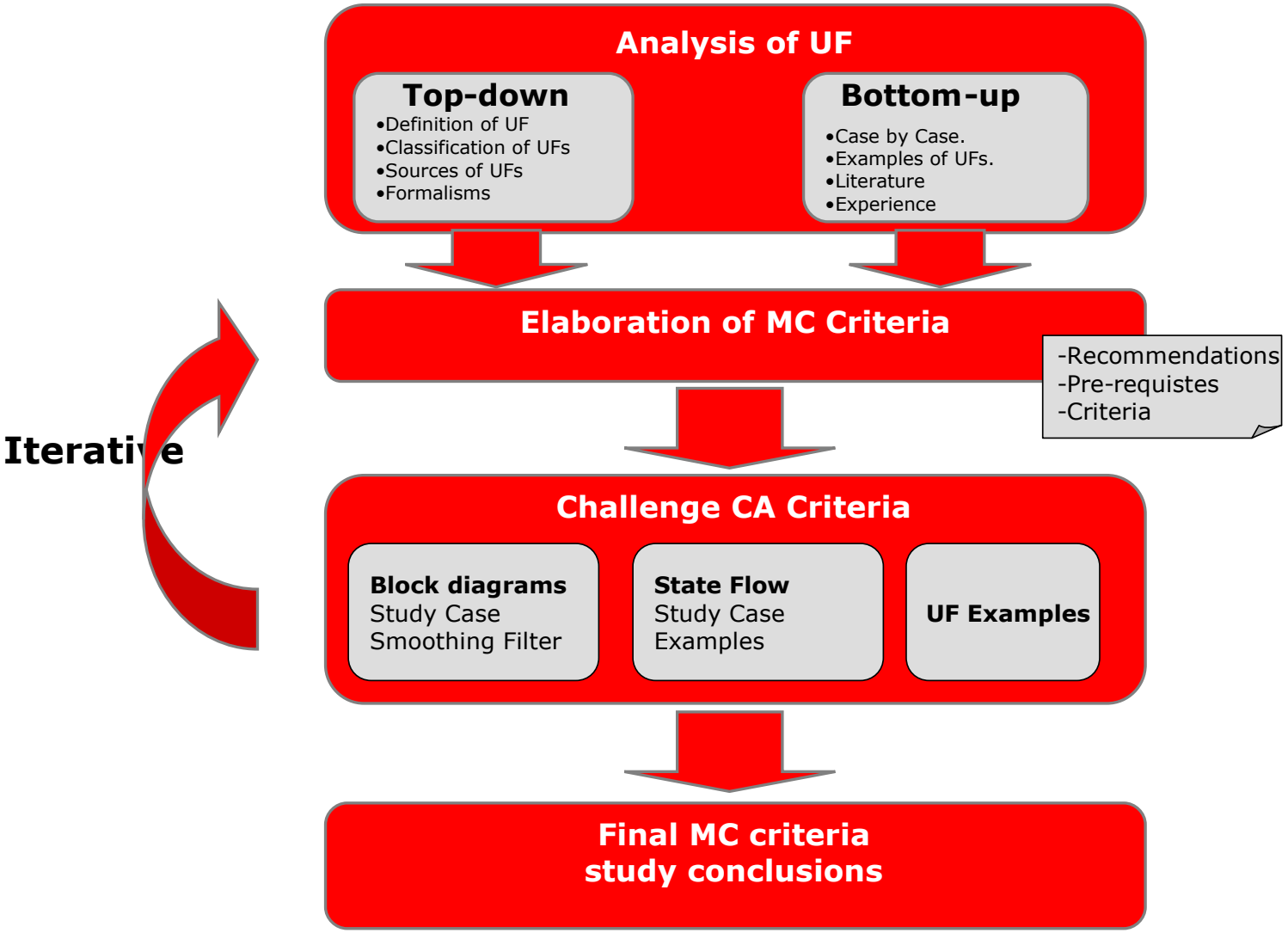
- MBD is currently being used for airborne software
  - Notations for Formalized Requirements & Designs
  - Each toolset implements its own notation:
    - **State Diagrams**
    - **Block Diagrams**
  - Most widely used for Formalized Designs analysed:
    - **SCADE** Suite
    - Simulink / Stateflow
- Each MBD toolset implements different notations
  - Each notation provide different features and properties
  - Differences in code generation
  - Different model coverage criteria



Verification and Validation process of a Formalized Design within **Model-Based development** workflow

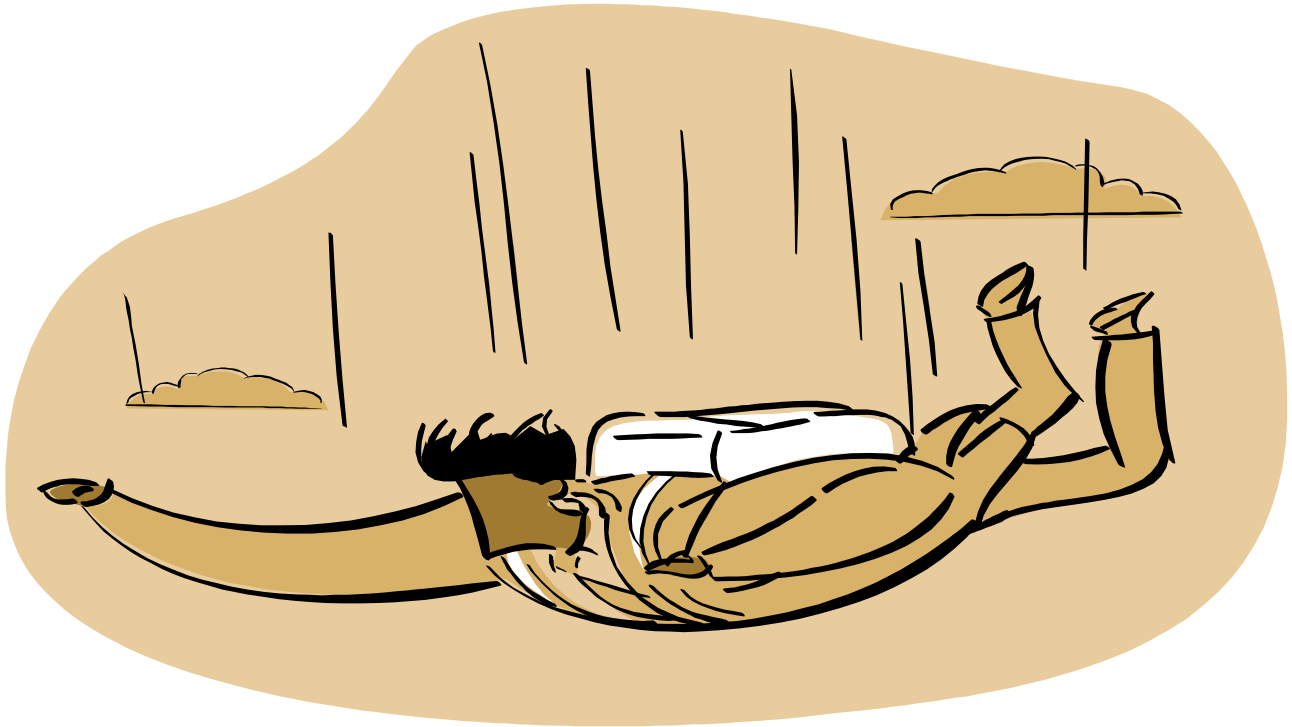


Study approach (SOMCA)



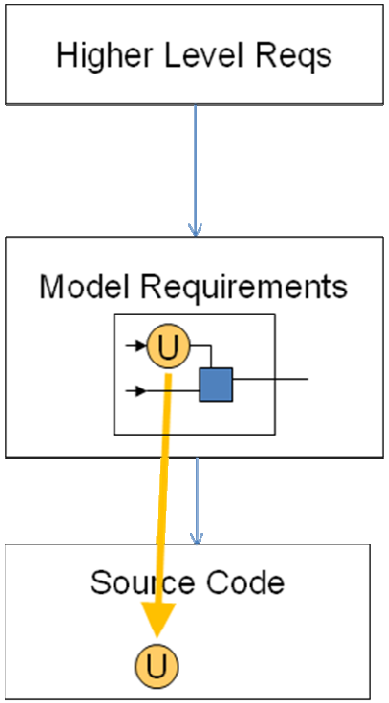
http://easa.europa.eu/safety-and-research/research-projects/large-aeroplanes.php

Unintended Functions



Definition of Unintended Functions

An **Unintended Function** is any *unspecified* —not defined in the higher-level requirements— and *uncontrolled* behaviour of the software under the aeroplane operating and environmental conditions



- Transmission of **Unintended Functions** from **Model** to **Source Code**

Unintended Functions in MBD: SOURCES

Activities that could directly **inject UFs** into the system, development activities

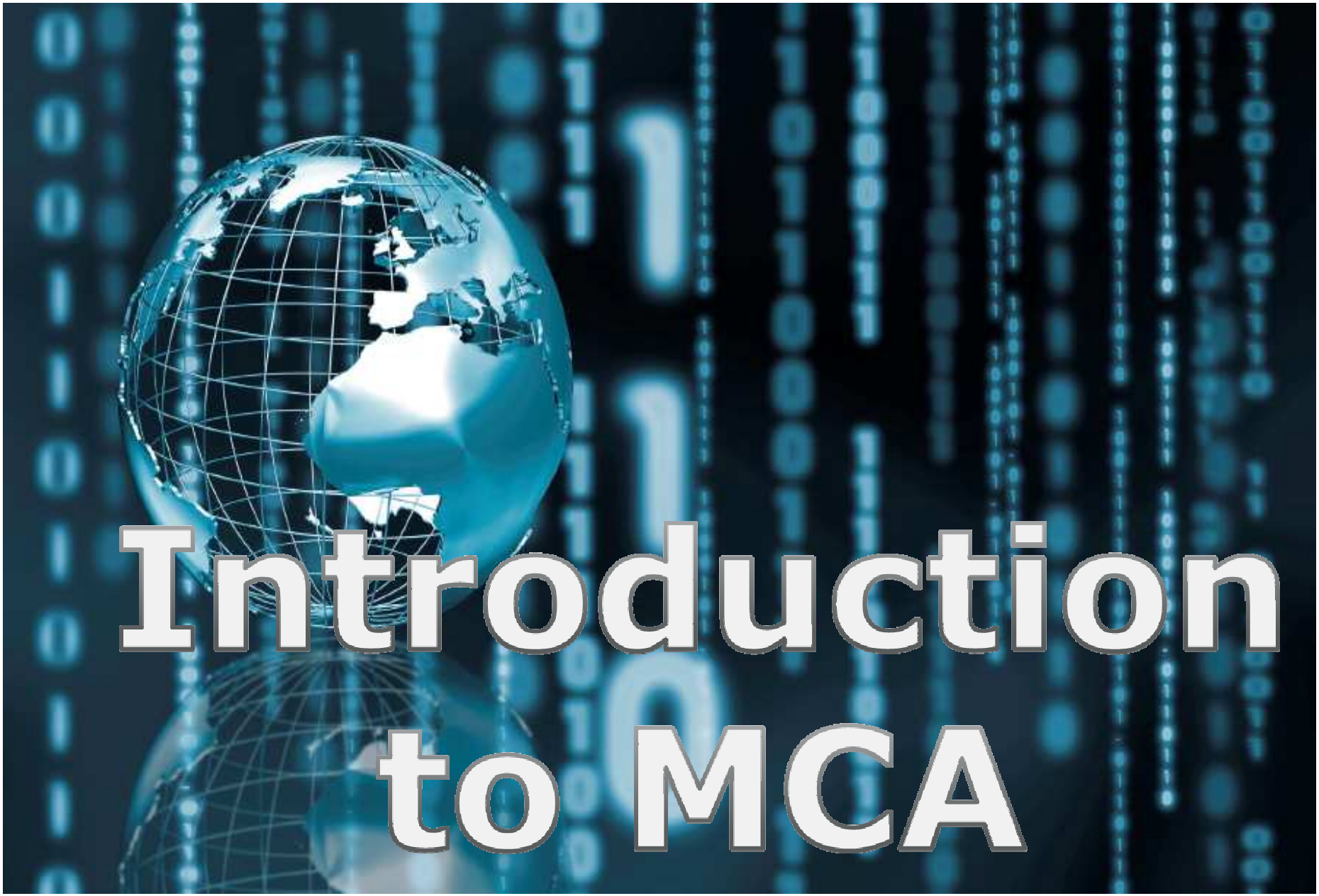
Activities aimed at **detecting** defects or errors in the specification and/or system, verification and validation activities. **UF misdetection**.

INJECTION

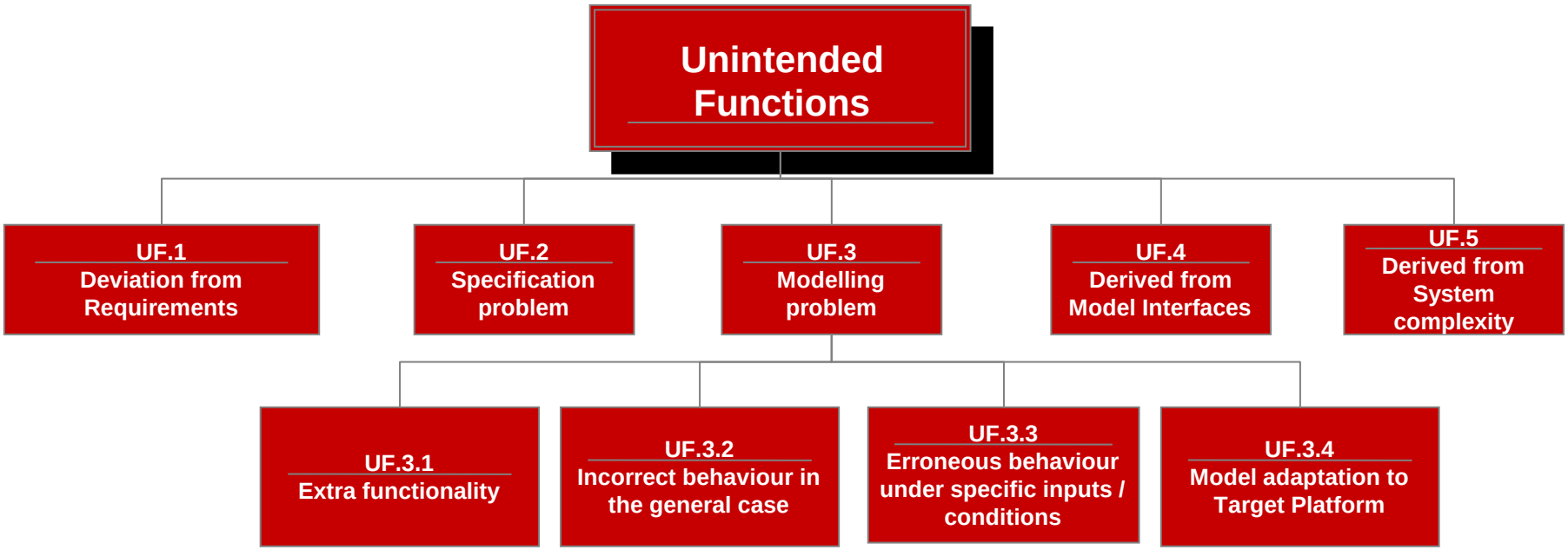
- **Modelling mistakes**
  - Wrong understanding of requirements
  - Incorrect subsystem usage
  - Wrong configuration
  - System-level interactions
  - Coupling of logical and numerical flows
  - Assumptions in model reuse
  - Partial use of existing block due to model reuse
- **Formalism or Toolset issues**
  - Error-prone language constructions
  - Non-formalized language semantics
  - Use of obscure tool features
  - Inadequate formalism
- **Aspects external to the model**
  - Inappropriate selection of the modelled requirements
  - Inaccurate modelling of target platform
  - Interfacing with components external to the model
  - Synchronisation between the model and the generated source code
  - Configuration Management of the modelling tools

MISDETECTION

- **Incomplete validation/verification of the model**
- **Inadequate configuration**
- **Inadequate sample time**
- **Bugs in the simulator**



TAXONOMY

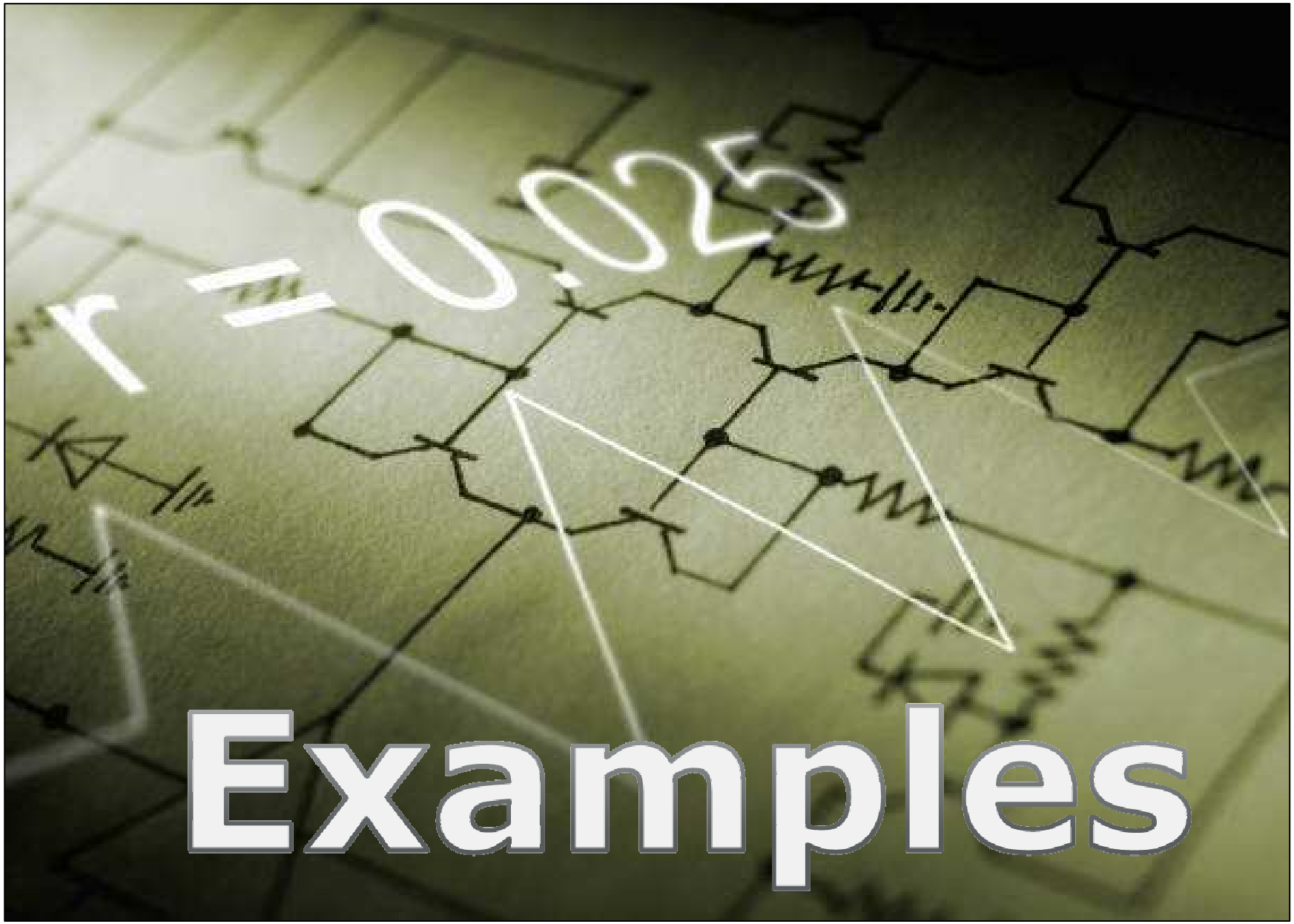


SOMCA MCA

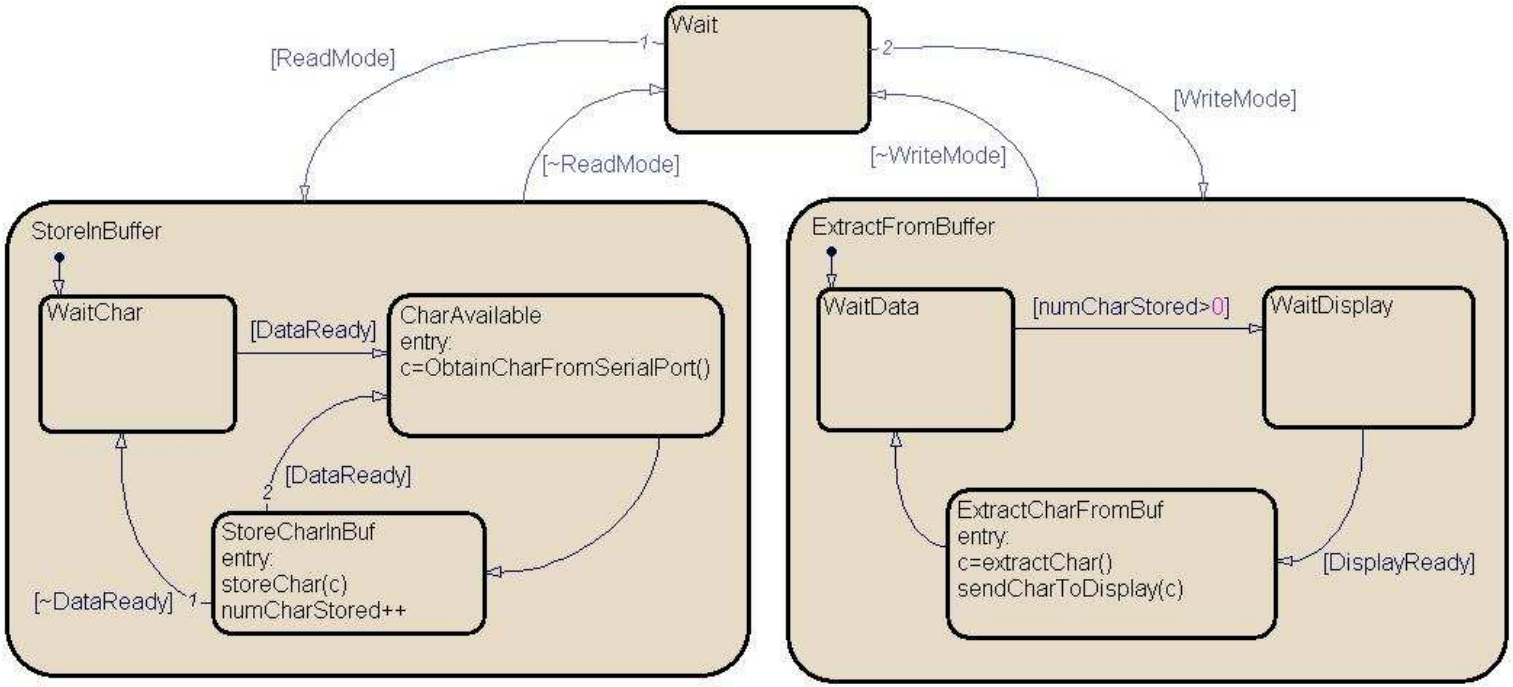
- Effective technique for V&V assessment
  - Demonstrate all relevant features exercised
  - MCA required for some types of UF detection

- All UF sources & categories
- Specific criteria for State Diagrams & Block Diagrams
- Specific criteria for each criticality level

- SOMCA MCA:
  - 14 Criteria
  - 22 Prerequisites
  - 25 Recommendations



Serial Port Controller State Machine



- **Transition Coverage Criteria:** All transitions of the diagram have been exercised
- **Parent State Coverage** Criterion defined for State Machines

Real environment about **0.1%** of the characters were surprisingly lost

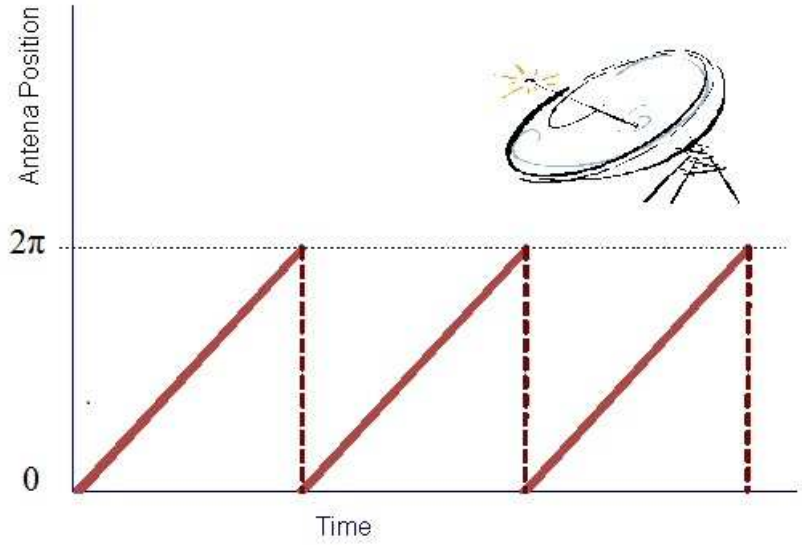
Parent State Coverage Criterion defined for State Machines

- ***All states and sub-states have been entered and exited (except for those without exit transitions), and all sub-states have been active at least once when parent state exits***.
- It was discovered that the mode *StoreInBuffer* could be interrupted when any of the sub-modes is active creating uncontrolled consequences like the loss of data.
- This behaviour was neither considered during the design nor in the test definition.

Antenna Position

- Subsystems that have been designed and tested in **isolation.**
- Subsystem providing the position of an antenna (angle of rotation).
- Successfully:
  - Validated in isolation covering the valid range
  - integrated and verified
- BUT…….

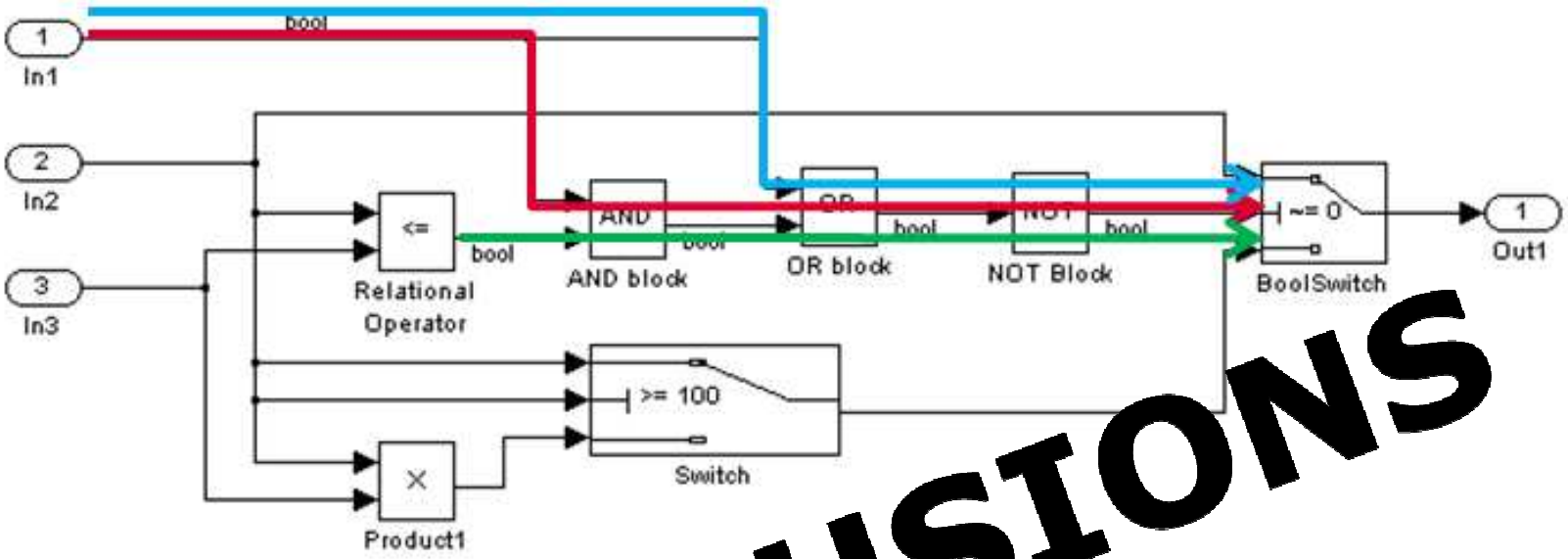
Real environment became unstable



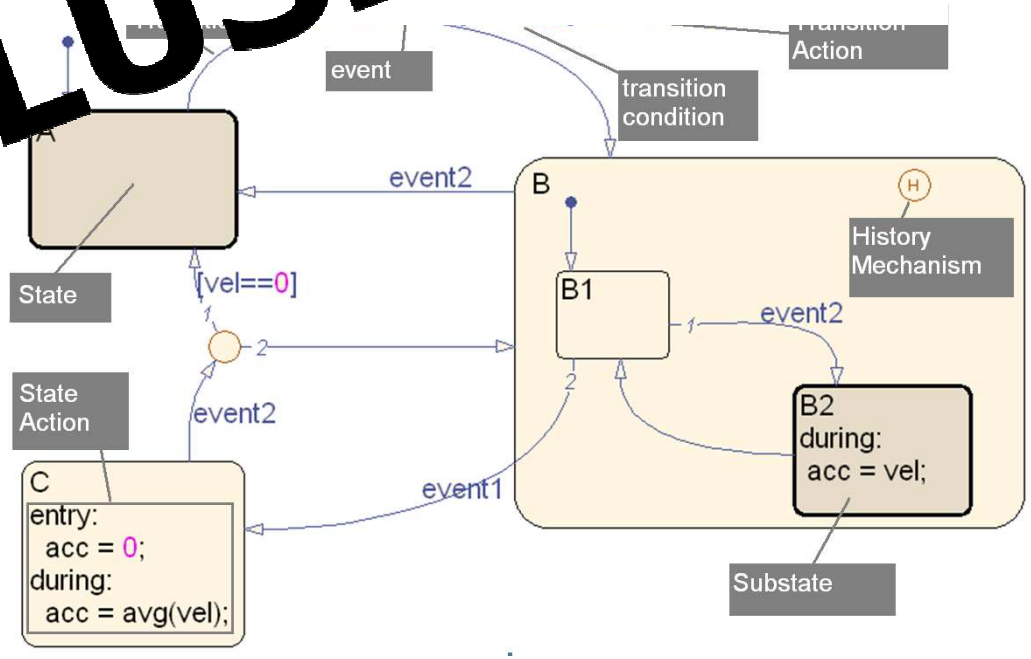
- **Range Coverage**

Range Coverage Criterion

- Rolling angle presented a discontinuity on every complete turn of the antenna, when the output value changes from 2π to 0.
- Necessary to check that the validity of the input/output range **AND**.. other characteristics of the input signal like dynamics, chronological evolution, periodicity, etc
- ***Range Coverage Criteria:*** *All the significant values of the inputs and outputs of each model component must be exercised.*
- *Also Considers:*
  - *All singular points of the functional components and algorithms*
  - *All equivalence classes (valid/in-range and invalid/out-of-range classes), including internal data types*
  - *Continuous and discontinuous input signals, including transitions between the maximum and minimum in-range values and periodic signals (e.g. angle between [0 .. 2 • pi))*



CONCLUSIONS



MCA is an efficient way of dectecting UFs at Formalized Design.

ADDED VALUE for V&V process with MDB

But…

Future Work

- Equivalence between Structural Coverage Analysis and Model Coverage Analysis and under which conditions could be possible.
- Applicability of MCA criteria for the certification
- Investigate Formal Specification and Verification Methods and their contribution to UF detection.
- Automation of MCA criteria in commercial tools
- Application of MCA criteria to a real project under certification process….


Thank you!
Amaya Atencia Yépez
aatencia@gmv.com
www.gmv.com
gmv
INNOVATING SOLUTIONS