Testing Applications of Cyber-Physical Systems in the Presence of Uncertainty

Martin A. Schneider

Fraunhofer FOKUS, Berlin, Germany

October 10th, STV Workshop, Berlin, Germany

Project facts:

Total cost: EUR 3 713 233,75

EU contribution: EUR 3 713 233,75

Coordinator: Oslo Medtech, Norway

Topic(s):ICT-01-2014 - Smart Cyber-Physical Systems

Funding scheme: RIA - Research and Innovation action

Overall project objective:

Improving CPS dependability via systematic and automated testing of Uncertainty in CPS

The consortium

[simula . research laboratory]
- by thinking constantly about it

Fraunhofer FOKUS

TU WIEN

ULMA Handling Systems

IK4 IKERLAN Research Alliance

future position | 60°40'17" North 17°06'29" East 213.141.90.204

Fokus! MBT

easy global market

NORDIC MEDTEST

OSLO MED TECH

Results and methods

Key expected results:

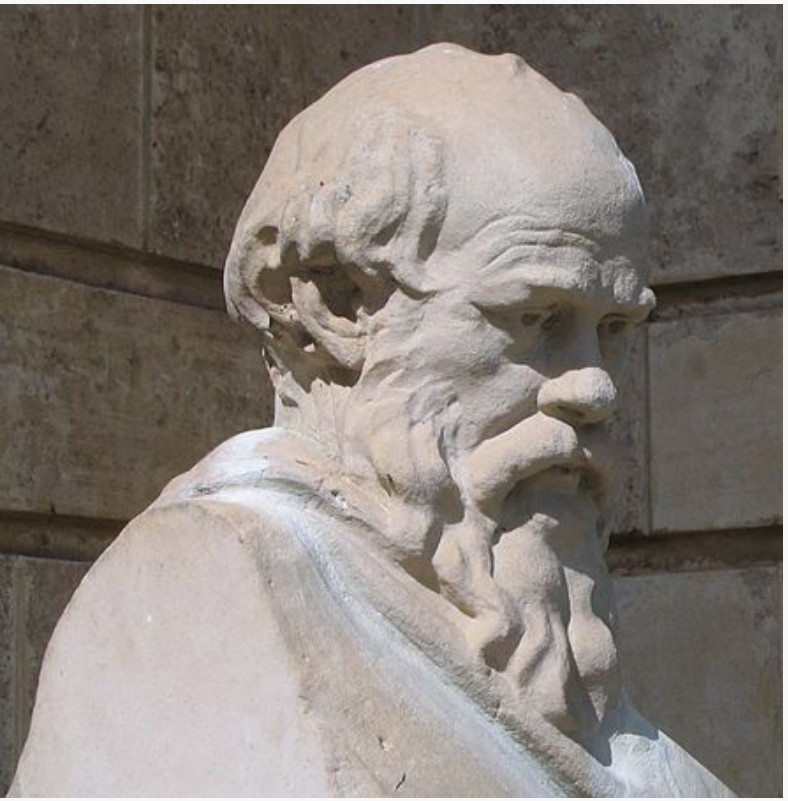
- Understanding Uncertainty (U-Taxonomy)
- Modeling Framework
  - Extensible and Configurable
- Testing Framework
  - Extensible and Configurable
- Tools implementing Taxonomy and Frameworks
- Standards (Crosscutting)

Model-Based Testing:

- Abstraction
- Managing Complexity
- Automation
- Systematic

Search-Based Testing

- Optimization
- Smart Mechanisms
- Discovering unknown uncertainties
- Genetic Algorithms.....



© Photograph by Greg O'Beirne. Cropped by User:Tomisti / Wikimedia Commons / CC-BY-SA-3.0 / GFDL

Socrates

»I know that I know nothing«

»I know that I don't know«

»I know that I don't know with certainty«

Agenda

1. **Uncertainty and Cyber-Physical Systems**
2. Uncertainty Taxonomy
3. Uncertainty Modelling
4. Uncertainty Testing

© Fraunhofer FOKUS

Uncertainty

“any deviation from the unachievable ideal of completely deterministic knowledge of the relevant system”

Walker et al. (2003): Defining uncertainty: a conceptual basis for uncertainty management in model-based decision support

„system state of incomplete or inconsistent knowledge such that it is not possible […] which of two or more alternative environmental or system configurations hold at a specific point”

A. J. Ramirez et al. (2012): A taxonomy of uncertainty for dynamically adaptive systems.

© Fraunhofer FOKUS

Uncertainty in Cyber-Physical Systems

- Cyber-physical systems are **connected embedded systems** that integrate **computation, networking and physical processes**.

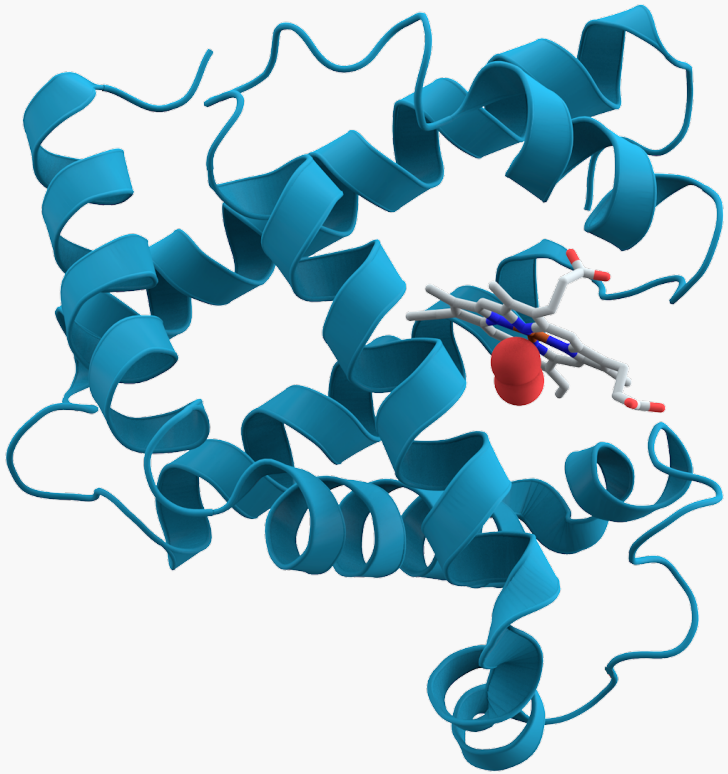
- **Uncertainty** arises from interaction between
  - elements of the CPS‘s infrastructure — Infrastructure Level
  - application(s) and the infrastructure of the CPS — Integration Level
  - humans and the environment with the CPS — Application Level

© Fraunhofer FOKUS

CPS may be not dependable

- **undesired behaviour** of a CPS is observed at runtime
  - due to uncertainty in the *digital x physical* environment

- **Challenge**
  - How to find find such scenarios **efficiently** in the **infinite and complex space of the scenarios**?
- **Solution**
  - Search algorithms



Use Cases for Uncertainty Testing

© ULMA Handling Systems, Spain

Automated Warehouse

- automatically stores and unloads goods
- manual intervention sometimes required
  - handling goods
  - updating database

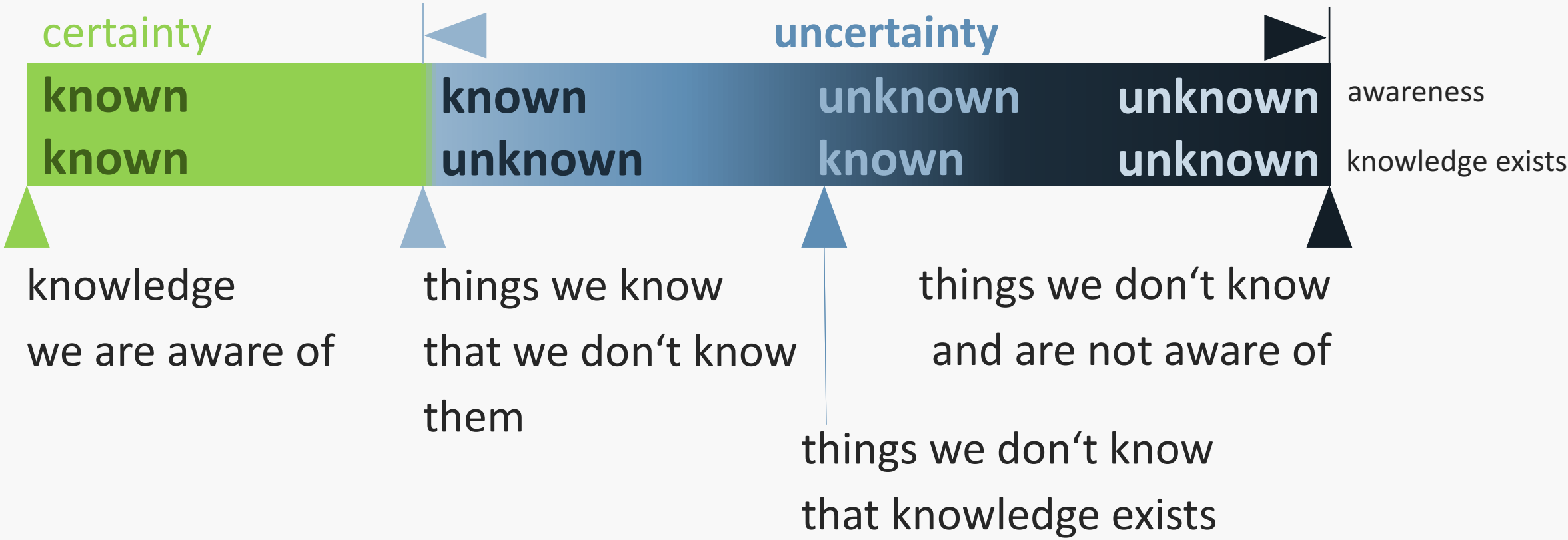
© FuturePositionX, Sweden

GeoSports

- automatically tracks all kinds of movements during a match (positioning via triangulation)
- improving performance of athletes
- athlete wears a device that constantly communicates with locating infrastructure

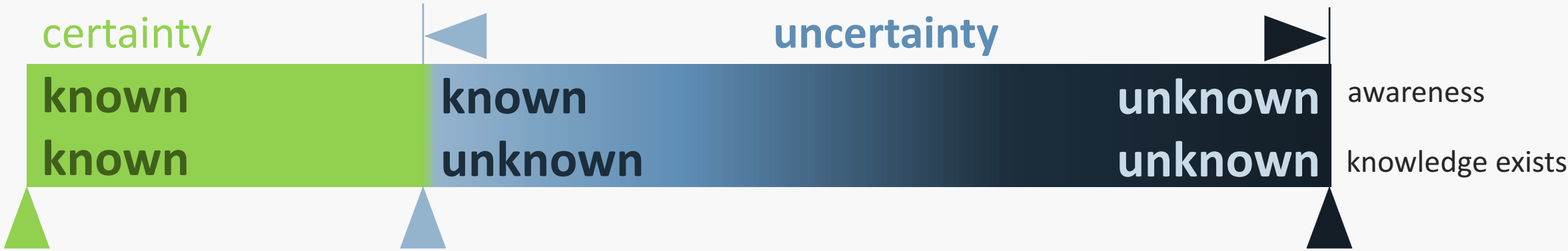
© Fraunhofer FOKUS

Uncertainty and Knowledge



© Fraunhofer FOKUS

Uncertainty and Knowledge



knowledge we are aware of

provided by use cases, observed in the field

goal of U-Test to find such uncertainties

© Fraunhofer FOKUS

Uncertainty and Risk

- uncertainty w.r.t. to the occurrence (likelihood) of a risk
- uncertainties do not have a probability assigned
- uncertainty covers positive and negative outcomes while risk focusses on negative outcomes, e.g., threats

- uncertainty as a source of risk
  - uncertain behavior: manifestation of an uncertainty as an behavior of the CPS with a negative impact on its dependability

© Fraunhofer FOKUS

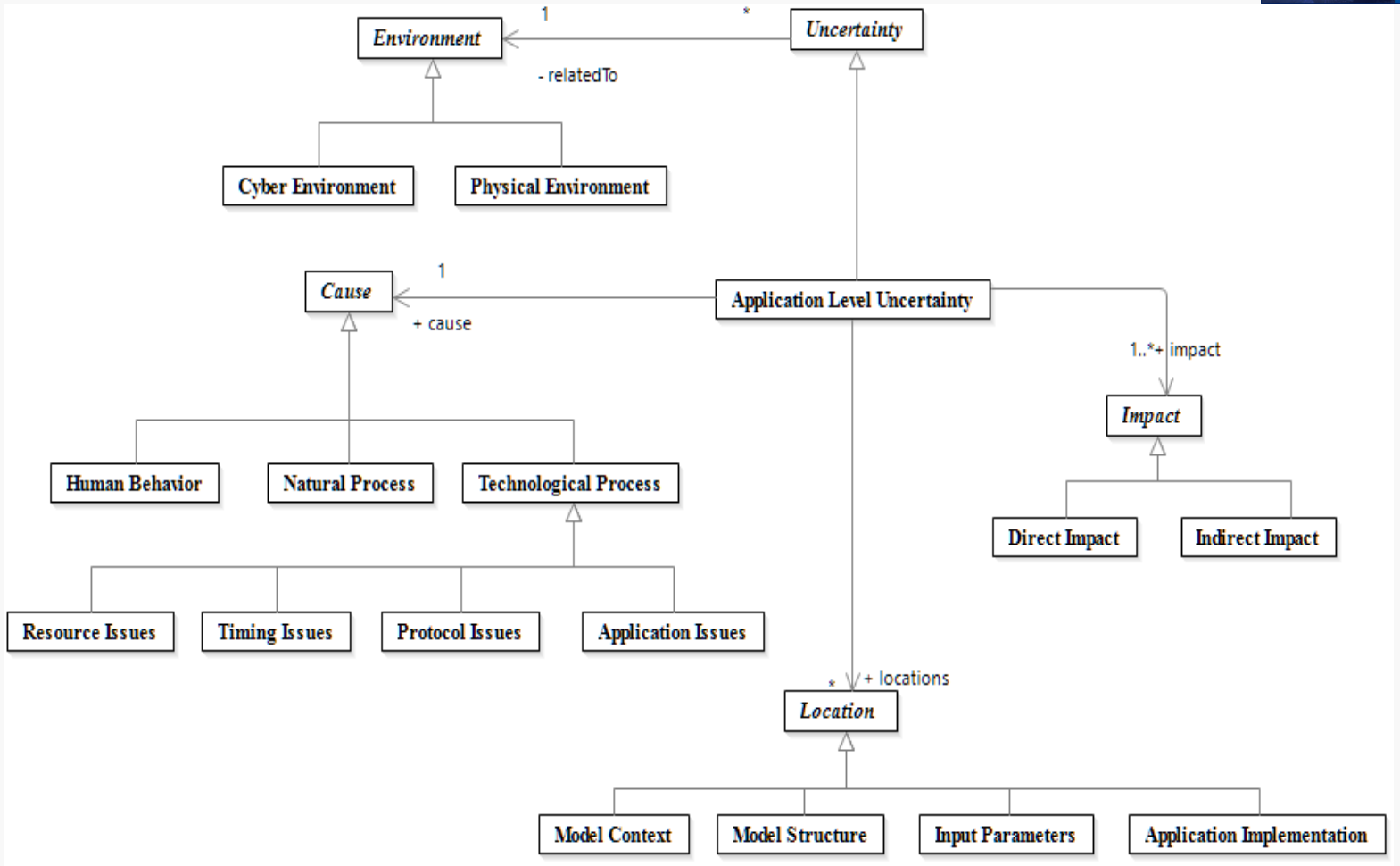
Agenda

1. Uncertainty and Cyber-Physical Systems
2. **Uncertainty Taxonomy**
3. Uncertainty Modelling
4. Uncertainty Testing

© Fraunhofer FOKUS

Uncertainty Taxonomy (Excerpt)

- **nature**
  - epistemic
  - aleatoric
- **environment**
  - cyber environment
  - physical environment
- **cause**
  - human behavior
  - natural process
  - technological process
- **impact**
  - direct
  - indirect
  - impacted element



© Fraunhofer FOKUS

Agenda

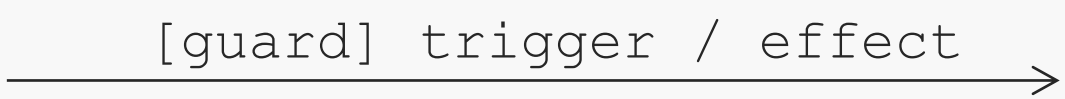
1. Uncertainty and Cyber-Physical Systems
2. Uncertainty Taxonomy
3. **Uncertainty Modelling**
4. Uncertainty Testing

© Fraunhofer FOKUS

Uncertainty Modelling

Uncertainy Modelling Framework (UMF)

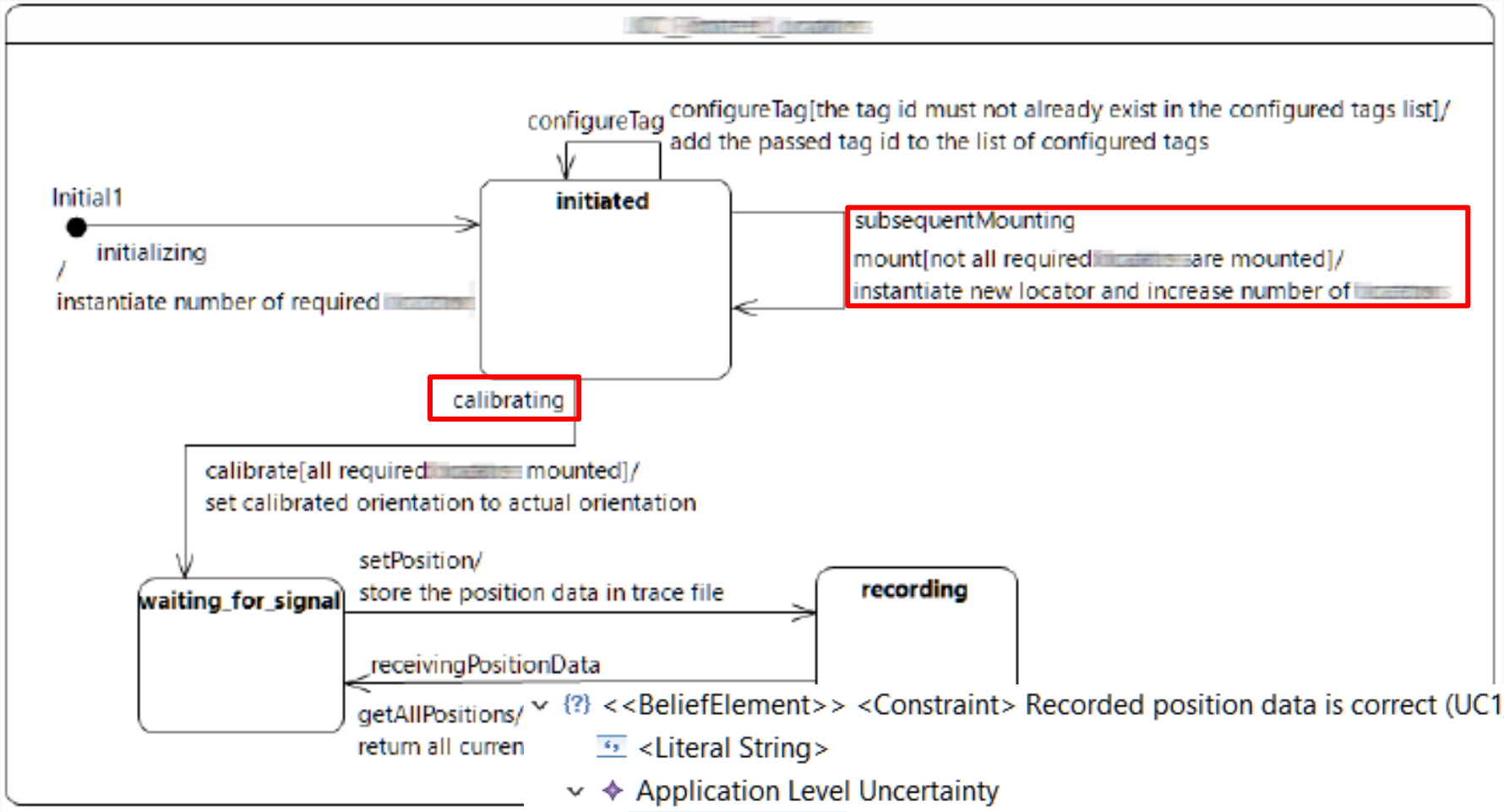
- State Machines
  - describe the expected input/output behavior of the SUT
  - from the perspective of SUT



- Uncertainties
  - characterization of uncertainties in terms of the UMF
  - that are related to the model

© Fraunhofer FOKUS

GeoSports State Machine



{?} <<BeliefElement>> <Constraint> Recorded position data is correct (UC1_APP_3_QUUPPA)

- <Literal String>
- Application Level Uncertainty
  - Impact Direct
  - Natural Process
  - Human Behavior

Property	Value
Impacted Element	<Operation> mount (orientation : Integer, locatorID : String) : Boolean
Impact Kind	Direct

© Fraunhofer FOKUS

Agenda

1. Uncertainty and Cyber-Physical Systems
2. Uncertainty Taxonomy
3. Uncertainty Modelling
4. **Uncertainty Testing**

© Fraunhofer FOKUS

Search-based Uncertainty Testing

- **cover known uncertainties described by use case providers**
  - by using use case descriptions (state machines)
  - by using information from modelled uncertaintes
- **discover unknown uncertainties**
  - by exploiting information from known uncertainties (coupling effect)
  - by recombining uncertainties

© Fraunhofer FOKUS

Search-based Uncertainty Testing

- genetic algorithm

- **individual**: state machines representing use cases
- **mutation**: applying mutation operators to state machines
  - first generation: apply mutation operators solely based on uncertainty information
  - further generations: increase amount of mutations not related to modelled uncertainties
- **crossover**: combination of uncertainties

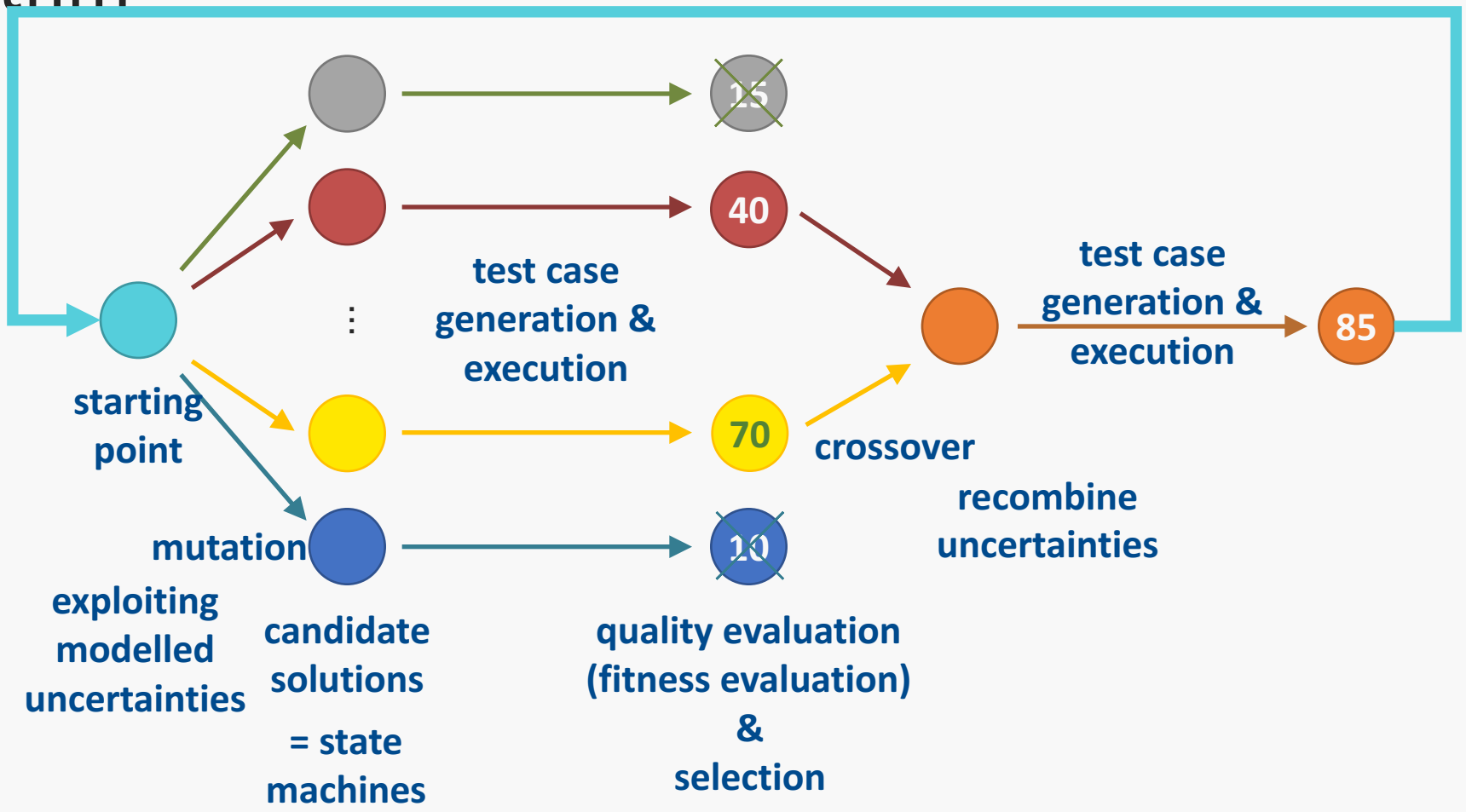
© Fraunhofer FOKUS

Mutation Operators

Mutation Operator	Description	Constraints/Comments
Add Transition	Adds a new transition by duplicating an existing one and setting a new source and target state.	
Remove Transition	Completely removes the transition.	Transitions having an initial state as source or a final node as target must not be removed.
Remove Transition (with State Merge)	Completely removes the transition. Merges the source and target state if the removed transition is the only one connecting them (optional: with the same direction). This avoid mutilated state machines which inhibit generating test cases.	Equivalent to 'Change Guard: replace expression with false'. Transitions having an initial state as source or a final node as target must not be removed. Equivalent to 'Change Guard: replace expression with false'.
Reverse Transition	Swaps source and target of the transition.	Transitions having an initial state as source or a final node as target must not be reversed. Optional: Transitions being the only one that connect source and target state must not be removed (optional: with the same direction). This avoid mutilated state machines which inhibit generating test cases.
Change Source/Target	Move the source or the target of the transition to any other state.	In case the target state of the transition is changed, the target must not be the initial state. In case the source state of the transition is changed, the source must not be the final node.

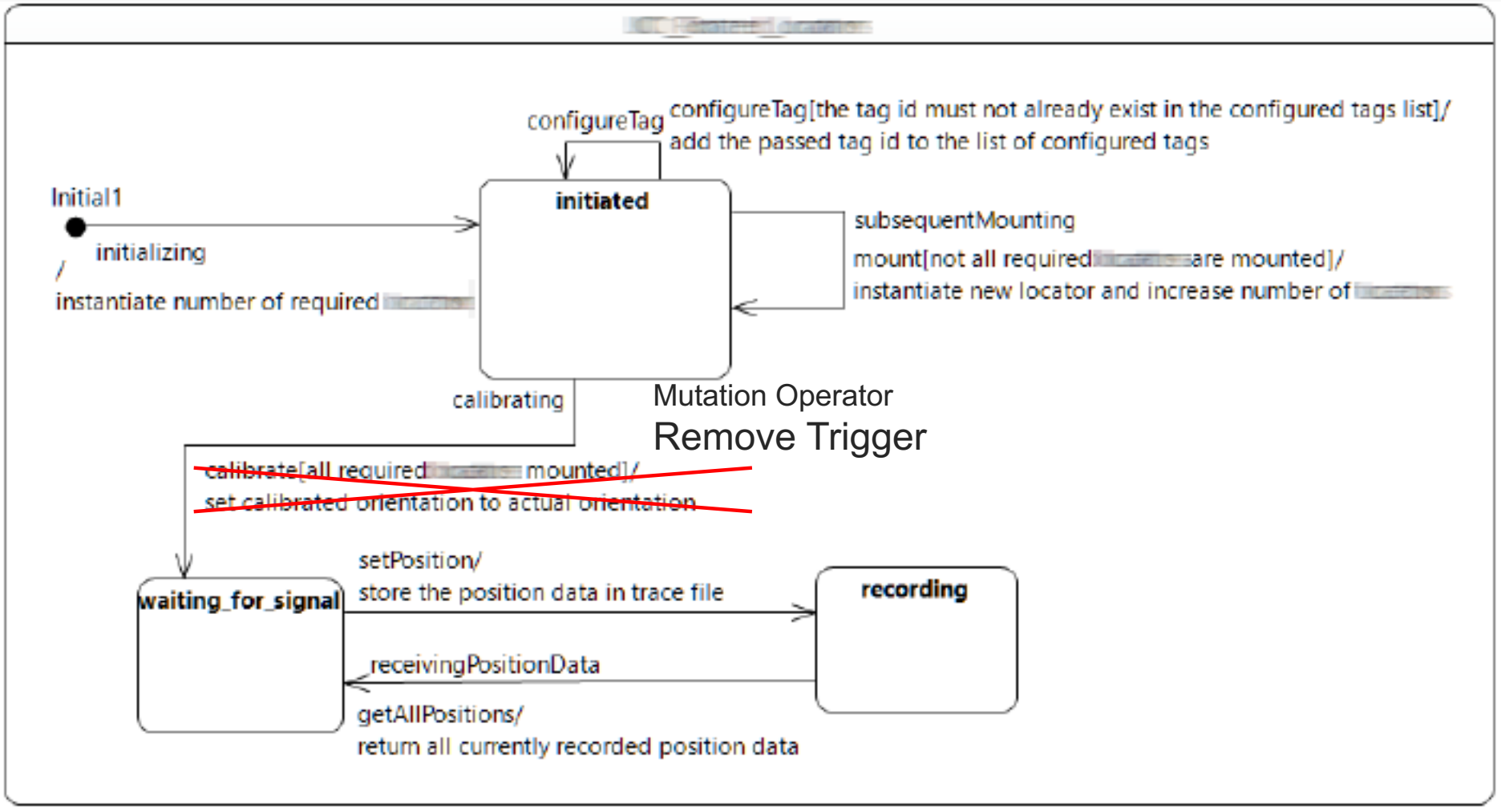
Mutation Operator	Description	Constraints/Comments
Remove Trigger	Transforms the transition to a completion transition.	
Remove Guard	Removes the guard of a transition completely.	Equivalent to 'Change Guard: replace expression with true'
Remove Effect	Removes the effect of a transition completely.	
Change Trigger Operation	Changes the operation to another one of the same interface of the original operation.	
Change Guard/ Change Effect	**- replace expression with true/false** **- negate expression** **- replace subexpression with true/false** **- negate subexpression** **- change logical operator** **- change relational operator** **- change arithmetic operator** **- change set operator** **- change quantifier** **- replace operand** **guard/effect mutation operators** **- remove statement** **- move statement** **- fix parameter/property of a called method or sent signal** **- change called method or sent signal** **- change operator** **- fix operand (replace it with a literal)** **- change operand (replace with variable, call parameter or signal property of the same type)** **- replace result: replace right-hand-side (RHS) expression with default value of left-hand-side (LHS)**	Guards and effects are written in C#.

Search-based Testing with a Genetic Algorithm



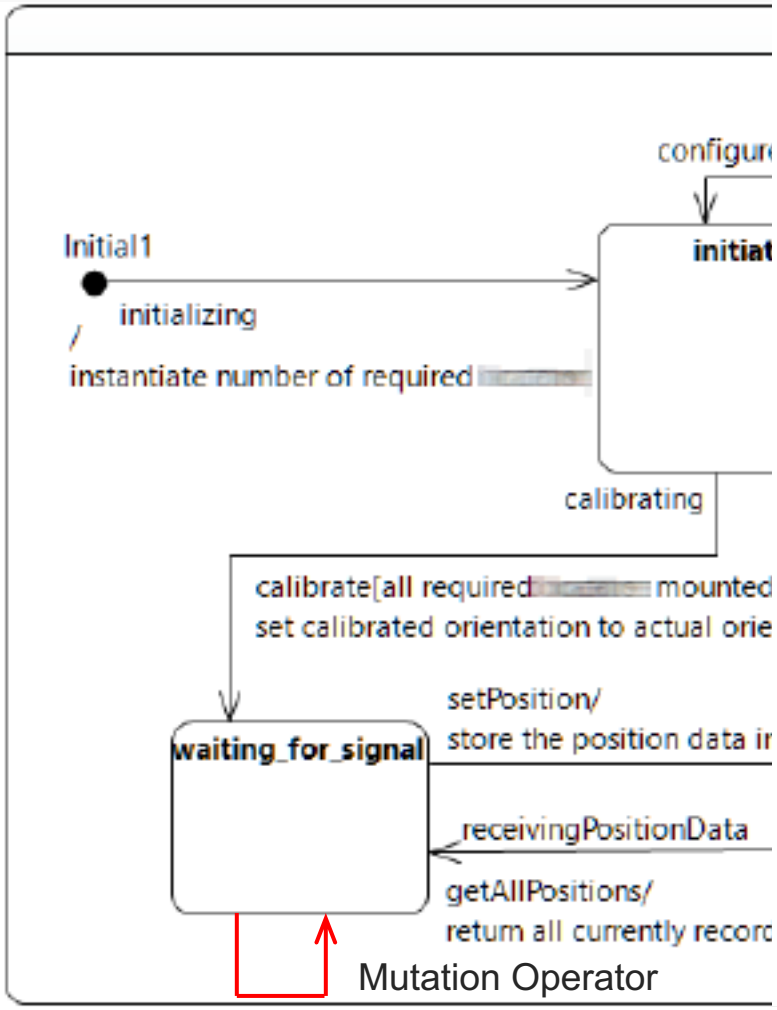
© Fraunhofer FOKUS

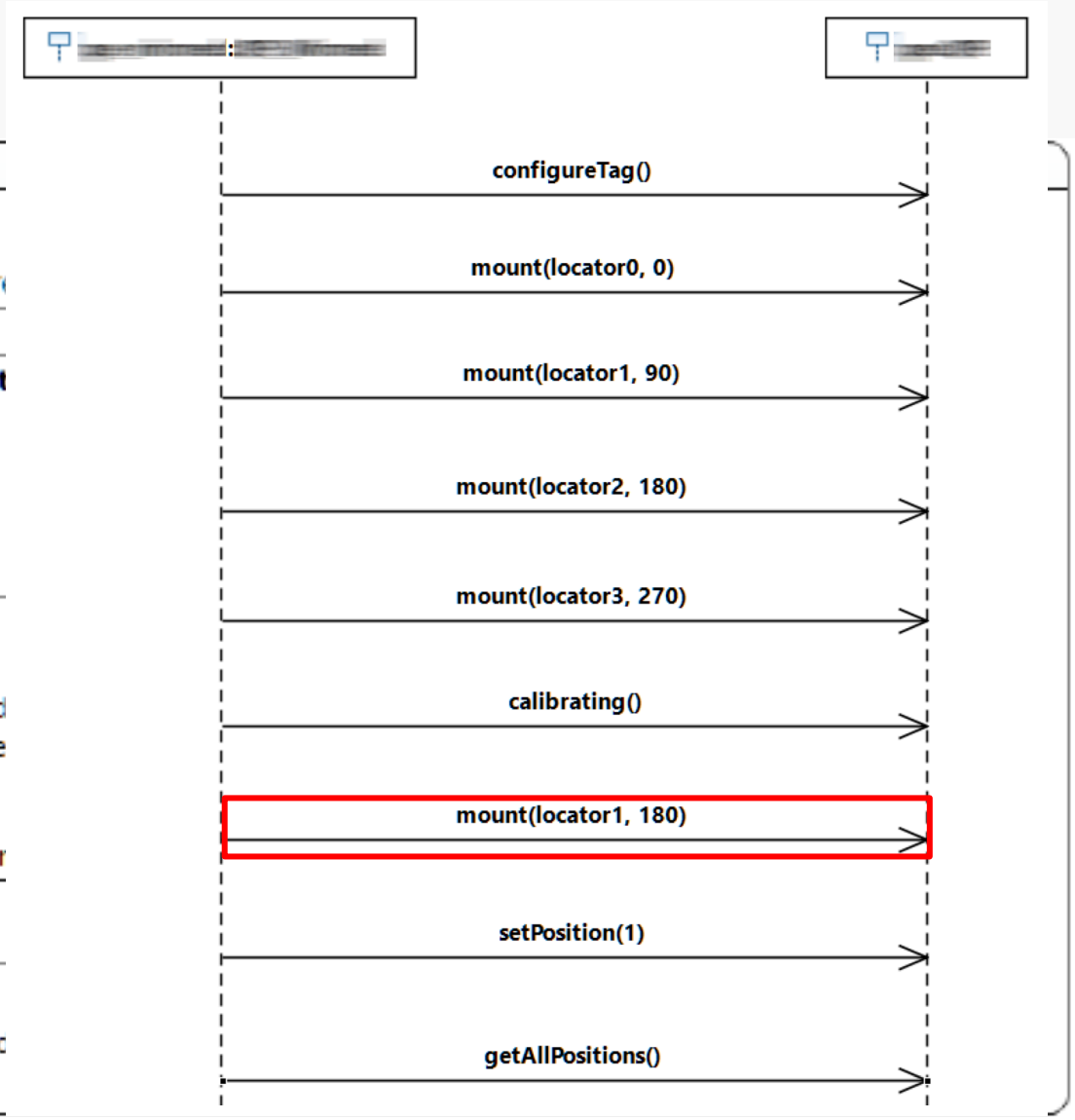
Example



© Fraunhofer FOKUS

Example





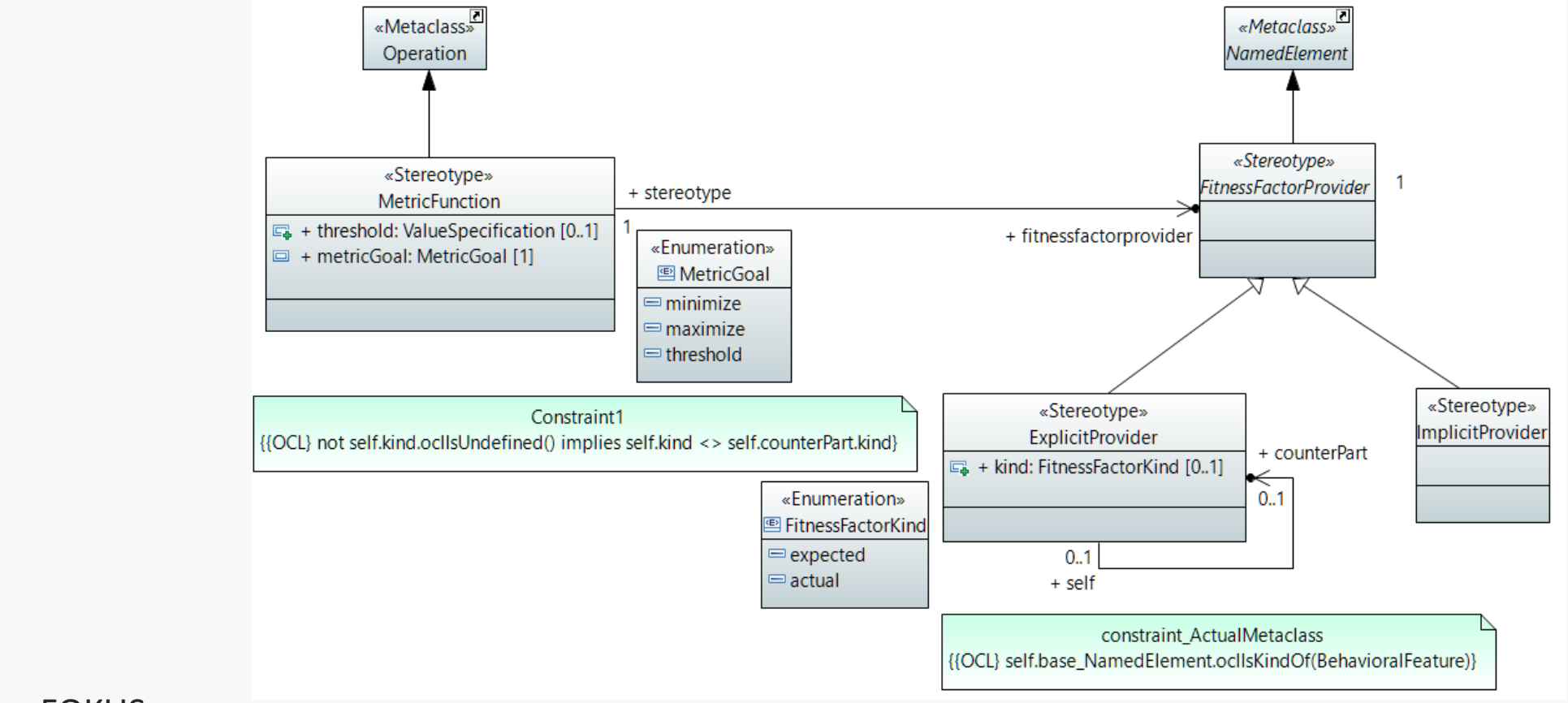
Mutation Operator

Add Transition

© Fraunhofer FOKUS

Search-based Uncertainty Testing: Fitness Factors

- generic, simple, model-based profile for fitness factors



© Fraunhofer FOKUS

Coverage Criteria

- **Traditional Transition Coverage** (state machine) $\frac{\#transitions_{covered}}{\#transitions_{all}}$
- **Uncertainty Coverage** (model) $\frac{\#uncertainties_{covered}}{\#uncertaities_{modelled}}$
- **Mutation Transition Coverage** (state machine) $\frac{\#mutations_{covered}}{\#mutations_{all}}$
- **Known Uncertainty Space Coverage** (all generations related to a single uncertainty)

$$\frac{\#mutations}{\#states \times (\#states - 1) \times \#operations \times 2}$$

© Fraunhofer FOKUS

A few, early numbers…

Mutation Operator	#Test Cases	#Removed Test Cases		#Remaining Test Cases
		Complete Path	Mutated Transition Coverage	
ChangeTransitionTarget	51	0	0	51
ChangeTransitionSource	5	5	0	0
RemoveTransition	5	0	0	5
AddTransition	51	0	51	0
RemoveEffect	5	5	0	0
RemoveGuard	252	1	0	251
RemoveTrigger	51	0	0	51

[1] Test cases generated by MS SpecExplorer based on the mutated state machines by traversing the state machines.
[2] Test cases generated by MS SpecExplorer do not necessarily end in a final state. Hence, first all complete paths starting from an initial state and ending in a final state are selected in the first stage.

Conclusions & Future Work

- small effort for testers
  - start from functional models (state machines)
  - add declarative uncertainty descriptions
- reduction of search space
  - search is guided by modelled uncertainties
- configurable and extendable
  - by modelled uncertainties
  - and model-based fitness factors
- empirical evaluation on the case studies

Thank you for your attention!

www.u-test.eu

@utesth2020

U-test.eu