FACING UNCERTAINTY IN COMPLEX CPS DESIGN

-- It's time to talk about the elephant in the room --

Bran Selić

Simula Research Laboratory (Norway)
Malina Software Corp. (Canada)
Zeligsoft (2009) Limited (Canada)
University of Sydney (Australia)
bselic@simula.no

AGENDA

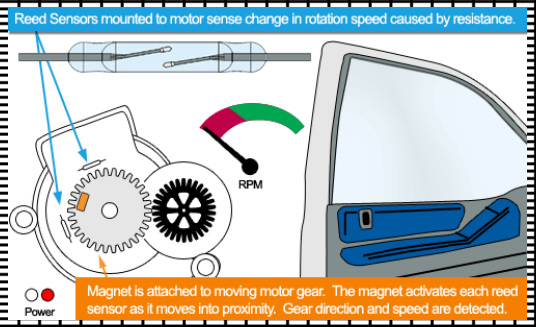
- The problem of uncertainty in system design
- The U-Test H2020 project
- U-Taxonomy: A conceptual model of uncertainty
- Applying the U-Taxonomy to CPS Testing
- Summary

A WHIFF OF THE ELEPHANT: THE "INTEGRATION" PROBLEM

- Occurs when independently defined features interact

	Susp	Brake	Steer	Wheel	Diff	Trans	Clutch	Eng	Driver
Susp		P	P	X+P	P	P	P	P	X+P
Brake	P		P	*X*+P	P	P	P	P	*X*+P
Steer	P	P		*X*+P	P	P	P	P	*X*+P
Wheel	X	X	*X*+P		*X*				
Diff	P	P	P	*X*+P		*X*+P	P	P	
Trans	P	P	P	P	*X*+P		*X*+P	P	P
Clutch		P	P		P	*X*+P		*X*+P	P
Eng	P	P	P	P	P	P	*X*+P		P
Driver	P	*X*+P	*X*+P		P	P	*X*+P	P	

IoT / SAE



Everything is connected to everything else…we cannot model the Universe

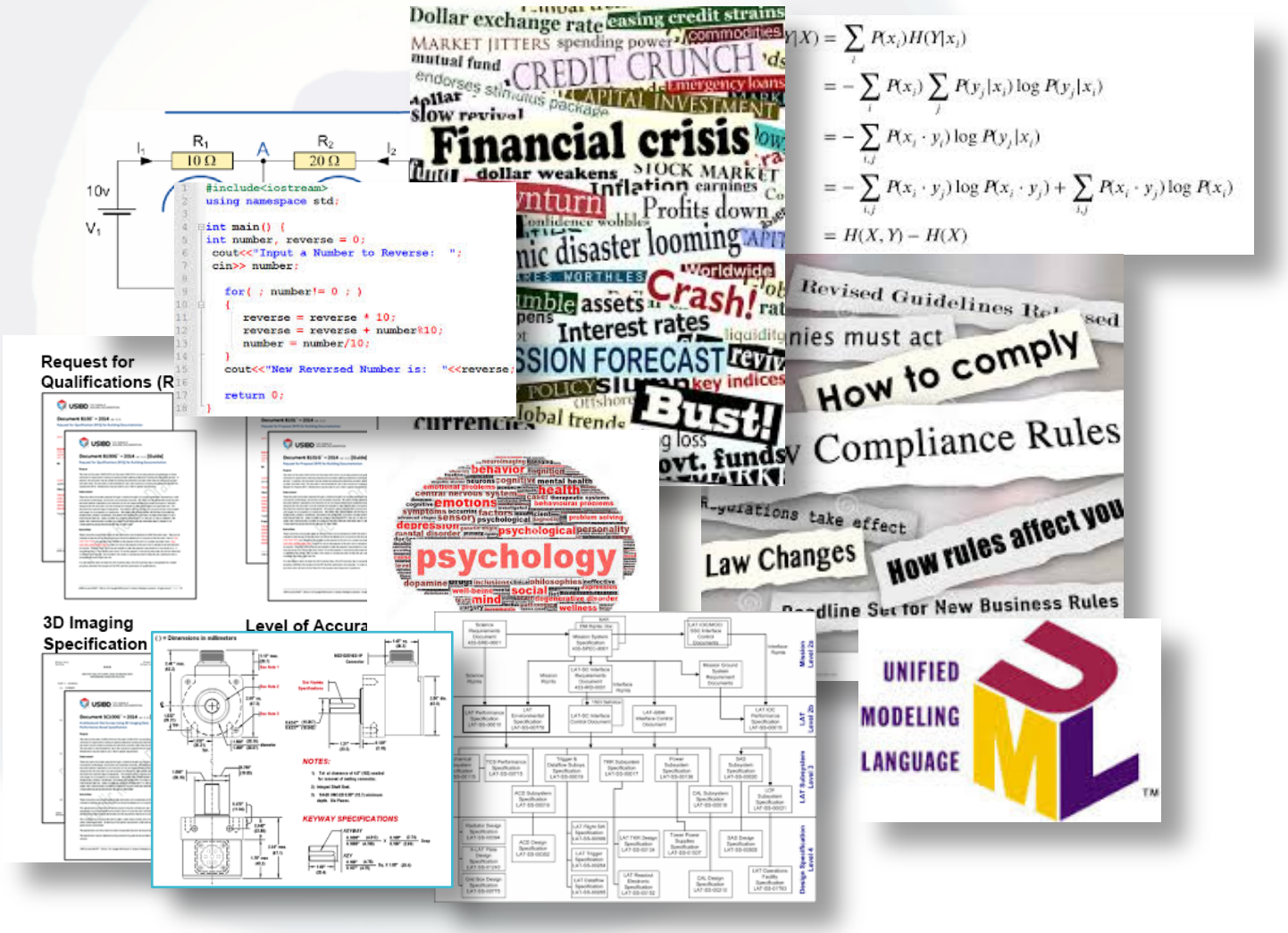
⇒ *engineering problems with greatly increased levels of UNCERTAINTY*

*Table credit of Martin Grimheden, KTH

COMPLEX SYSTEM DESIGN…

- …requires knowledge of many different things…

A COMPLEX SYSTEM



WHERE THE ELEPHANT LIES

RQ: How can we factor this into our design?

A COMPLEX SYSTEM

Risk

Set of all the things we need to know

Set of things we don't know that we don't know

(Unknown Unknowns)

Covered by "conventional" design methods

Set of things we know we don't know

(Known Unknowns)

"Tacit knowledge"

Set of things we don't realize we know

(Unknown Knowns)

Set of things we know we know

(Known Knowns)

AGENDA

- The problem of uncertainty in system design
- The U-Test H2020 project
- U-Taxonomy: A conceptual model of uncertainty
- Applying the U-Taxonomy to CPS Testing
- Summary

THE U-TEST H2020 PROJECT

U-Test: Testing Cyber-Physical Systems under Uncertainty

OBJECTIVE:

To improve the dependability of CPSs, via cost-effective model-based and search-based testing of CPSs under uncertainty, by (1) defining an uncertainty taxonomy and (2) holistic modelling and testing frameworks with considerable reliance on standards.

Duration: 2015 – 2018
Overall funding: € 3.71M
Members: 9

U-TEST CONSORTIUM: MEMBERS

U-Test

1.Research Partners

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

Fraunhofer FOKUS

TU WIEN

2.Case Study Providers

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

ULMA Handling Systems

3.Tool Providers

Fokus! MBT

easy global market

4.Test Bed Provider

NORDIC MEDTEST

5.Exploitation

IK4 IKERLAN Research Alliance

6.Dissemination/ Administration/ Financial

Oslomedtech

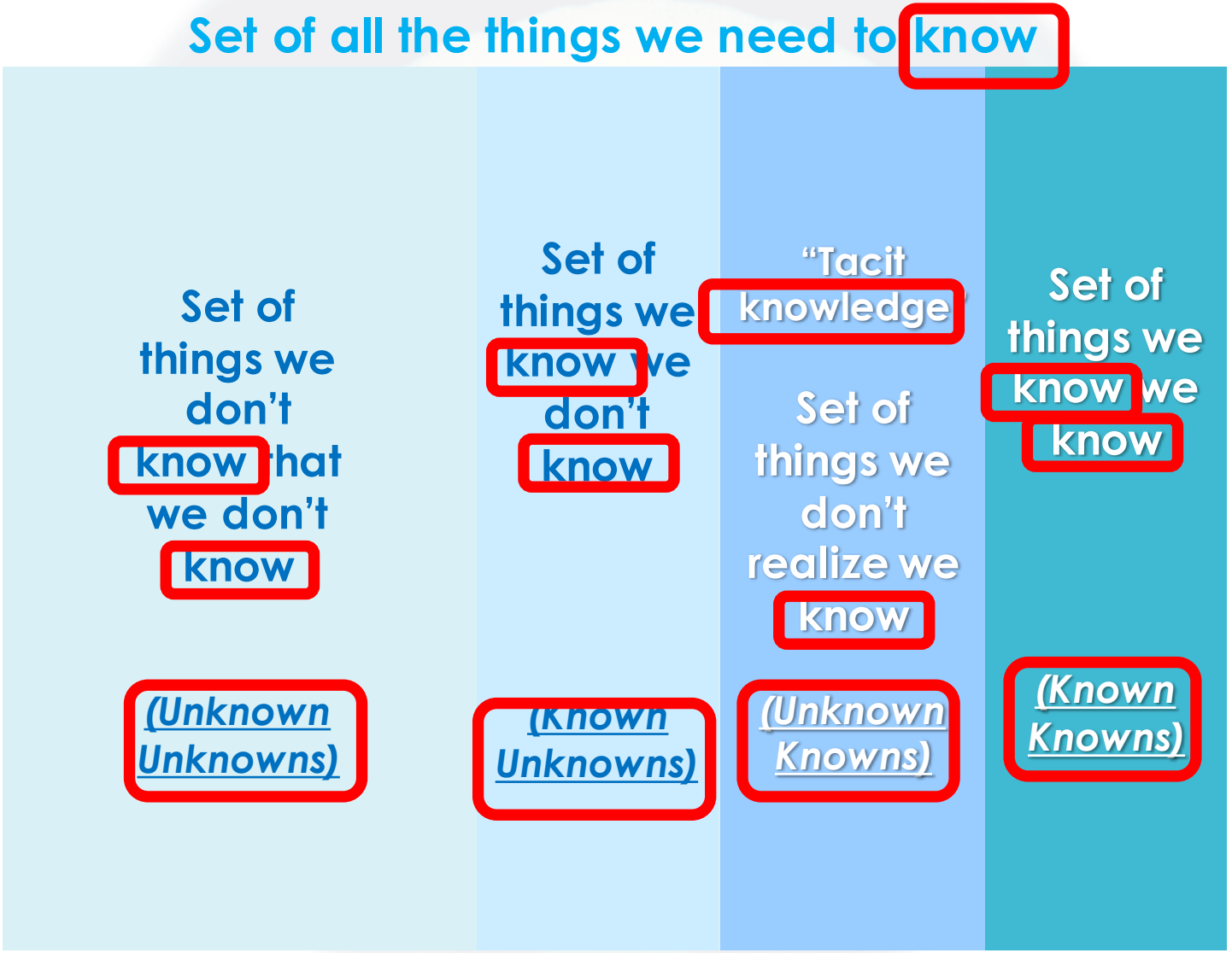
AGENDA

- The problem of uncertainty in system design
- The U-Test H2020 project
- U-Taxonomy: A conceptual model of uncertainty
- Applying the U-Taxonomy to CPS Testing
- Summary

UTEST APPROACH TO UNCERTAINTY

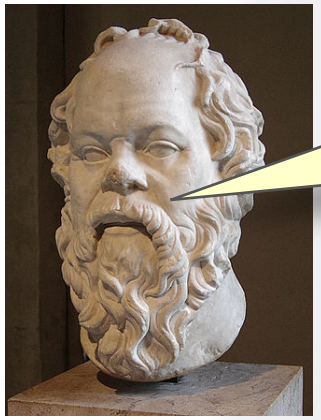
- **Start with a general reference model of uncertainty**
  - ✓ Basis for a common conceptual framework for discussing and reasoning about uncertainty
  - ✓ Includes capability to characterize uncertainty both quantitatively and qualitatively (e.g., for analyses)
- **Foundation for domain-specific specializations**
  - ✓ E.g., testing of CPS

CATEGORIES OF KNOWLEDGE



BUT, WHAT IS "KNOWLEDGE"?

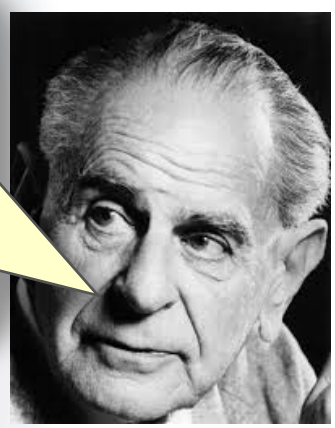
- **Knowledge is an elusive and controversial concept**
  - ✓ Philosophers have been disagreeing on its meaning for centuries
  - ✓ Epistemology = a whole discipline dedicated to the study of knowledge



"I know that I know nothing"

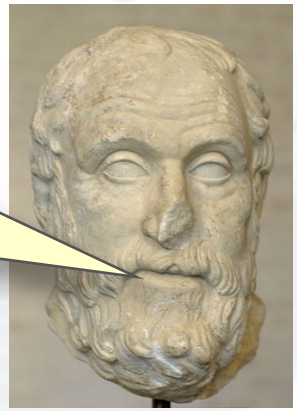
SOCRATES (470-399 BC)

Knowledge is, irreducibly conjectural or hypothetical, *generated by creative imagination* [Wikipedia]



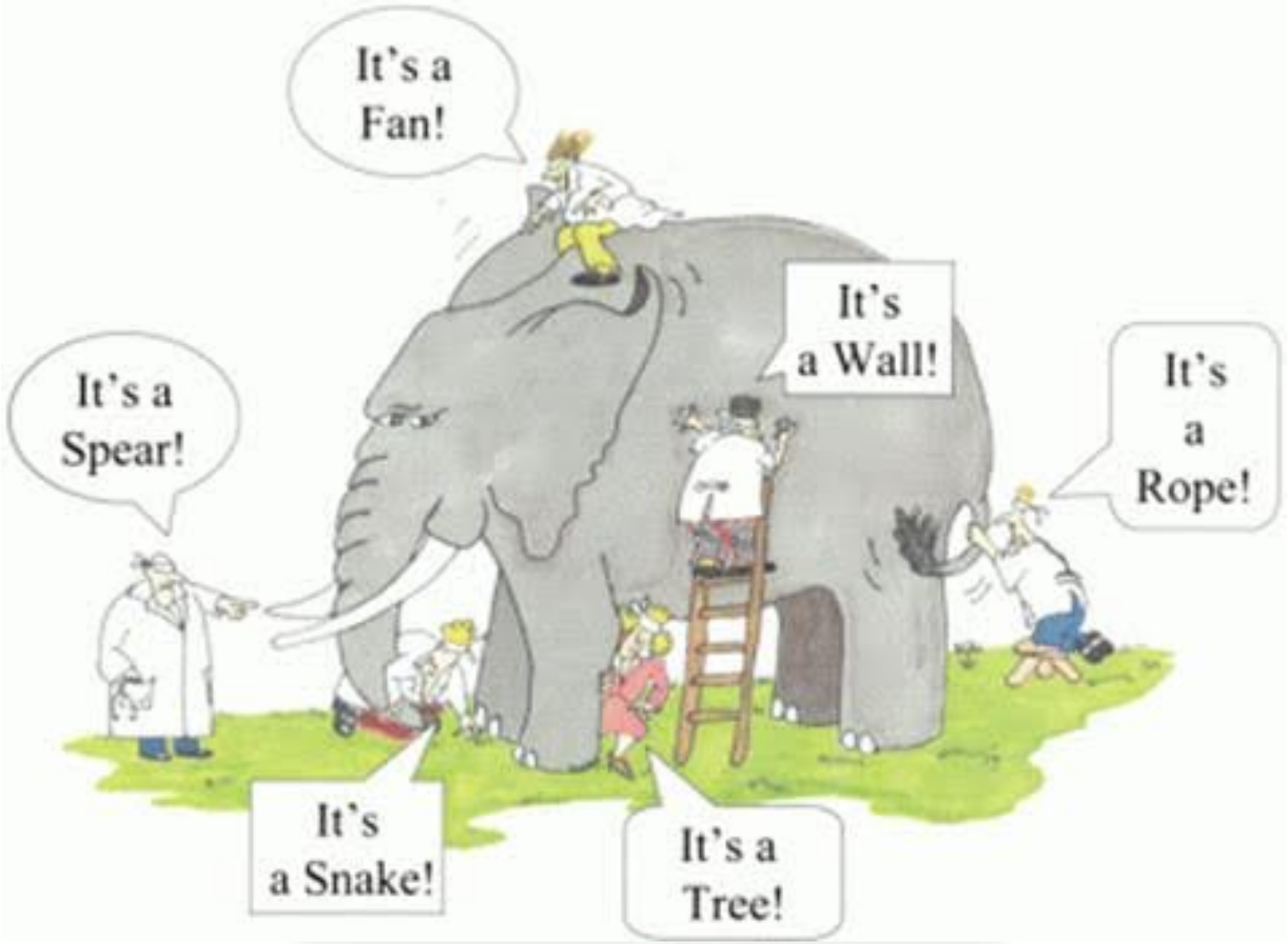
K. POPPER (1902-1994)

"Nothing can be known – not even this"



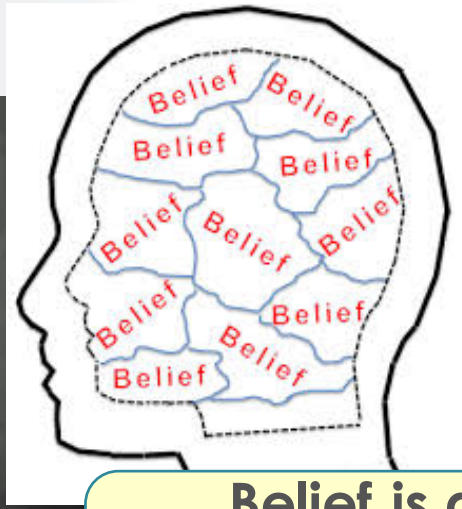
CARNEADES (213-129 BC)

KNOWLEDGE AND TRUTH



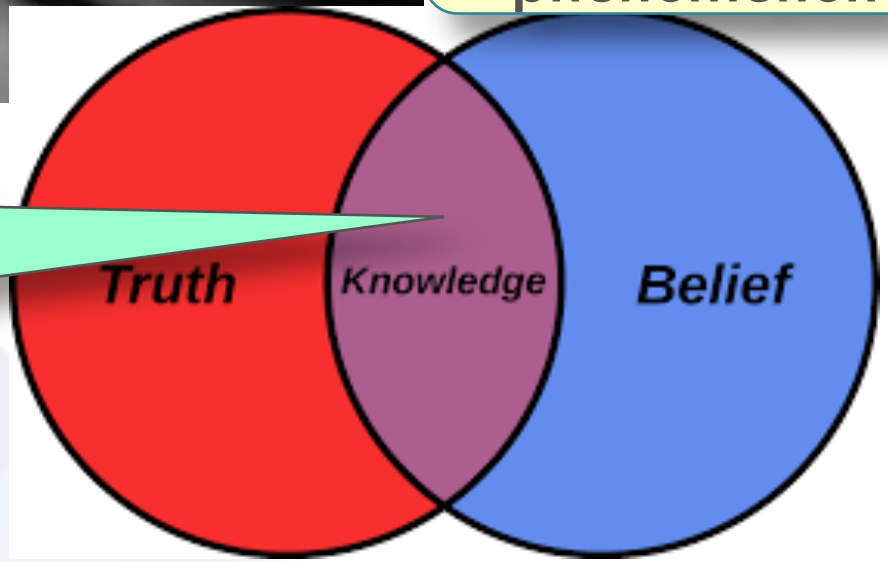
NB: Each statement is based on concrete evidence!

SO, WHAT'S LEFT?

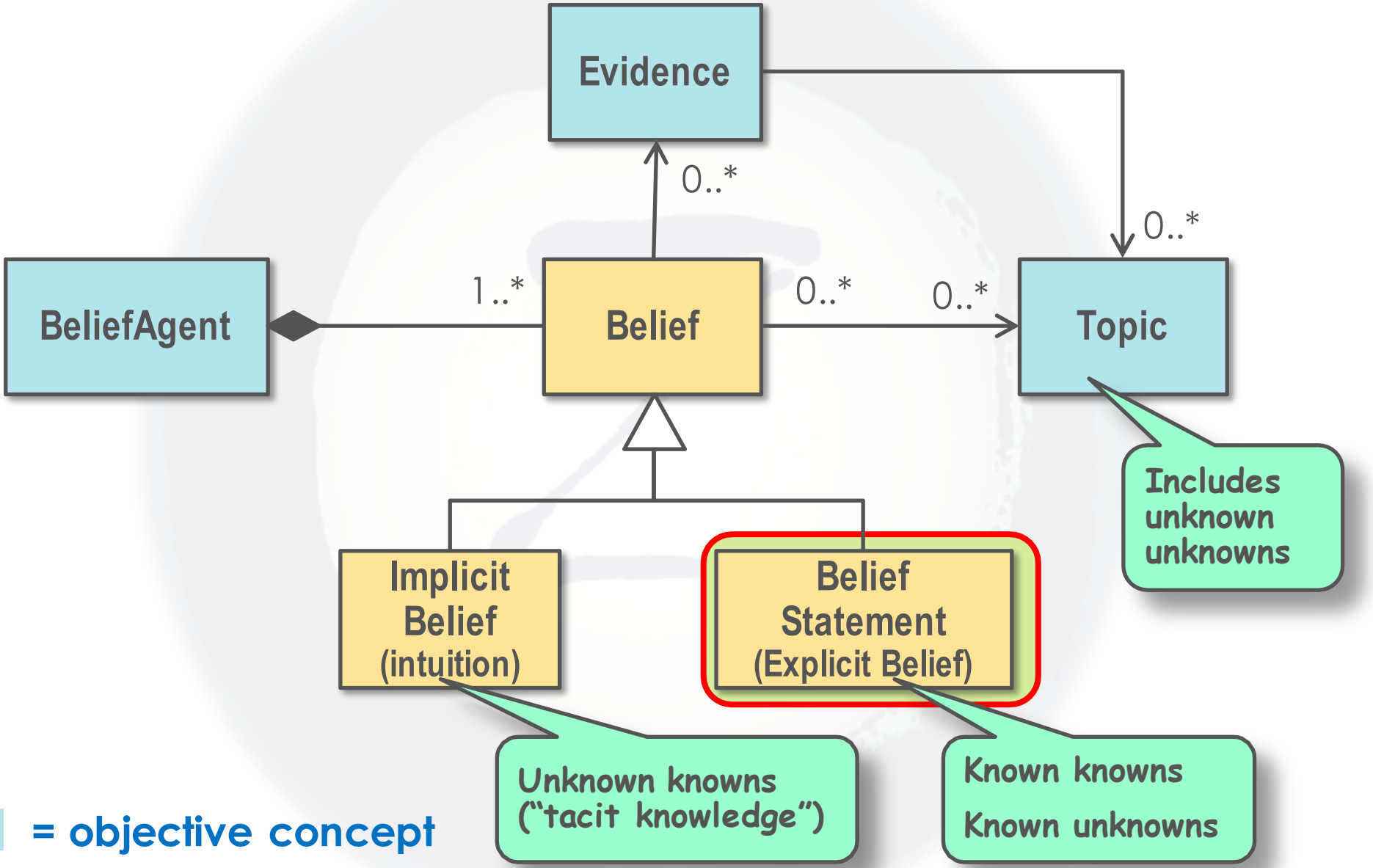


Belief is a *subjective* phenomenon

We cannot even be certain of which of our beliefs corresponds to the truth (and how much)!



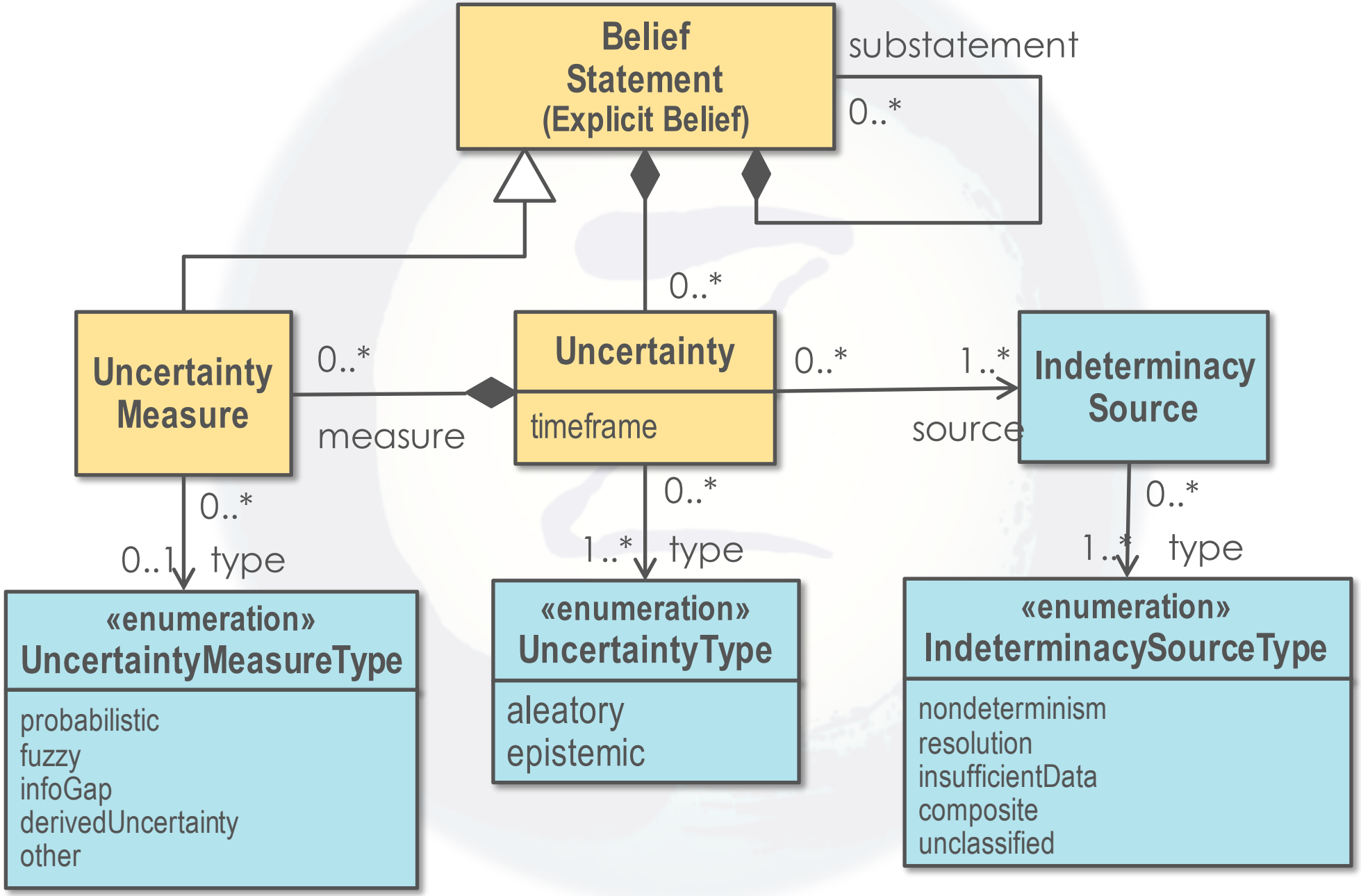
THE U-TAXONOMY BELIEF MODEL



SOME KEY DEFINITIONS

- **Belief Agent**: an individual, group, or mechanism capable of acting or reasoning based on one or more beliefs that it holds
- **Belief**: An implicit or explicit opinion or conviction held by a belief agent
- **Belief Statement**: an explicit formulation of a belief
  - ✓E.g., natural language, mathematical expression, binary code
- **Topic**: some objective phenomenon or concept that may be the subject of beliefs
- **Evidence**: objective information that may be used to justify a belief

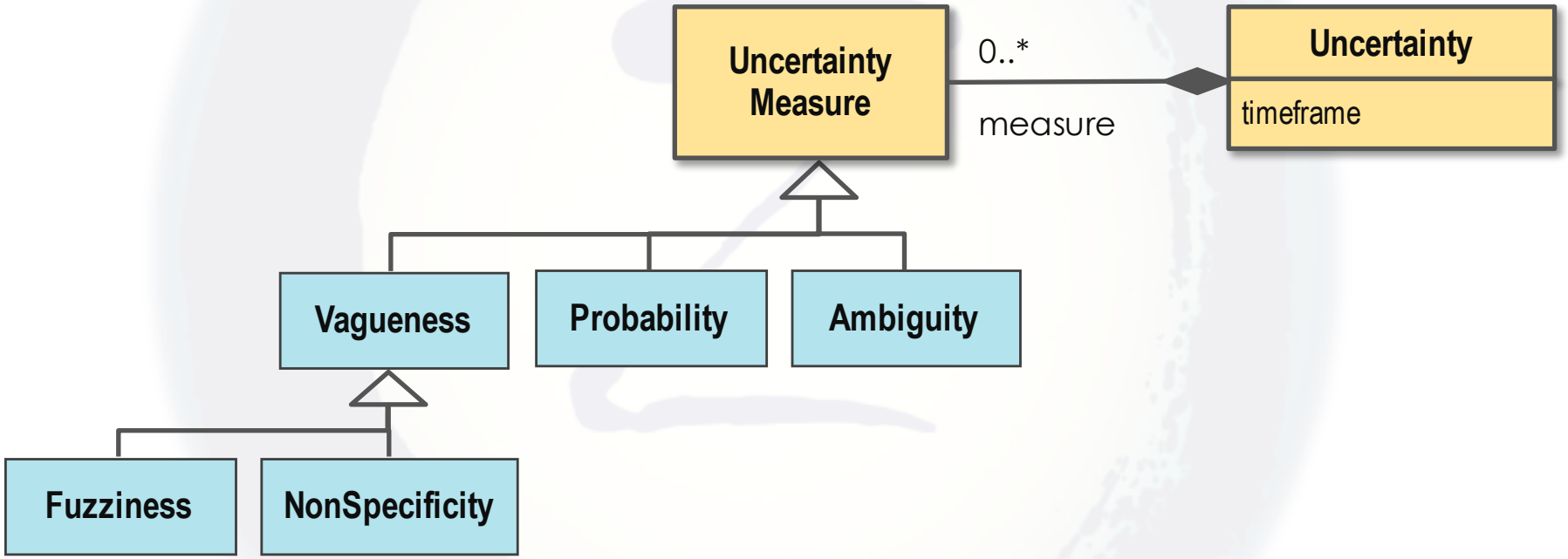
U-TAXONOMY: UNCERTAINTY



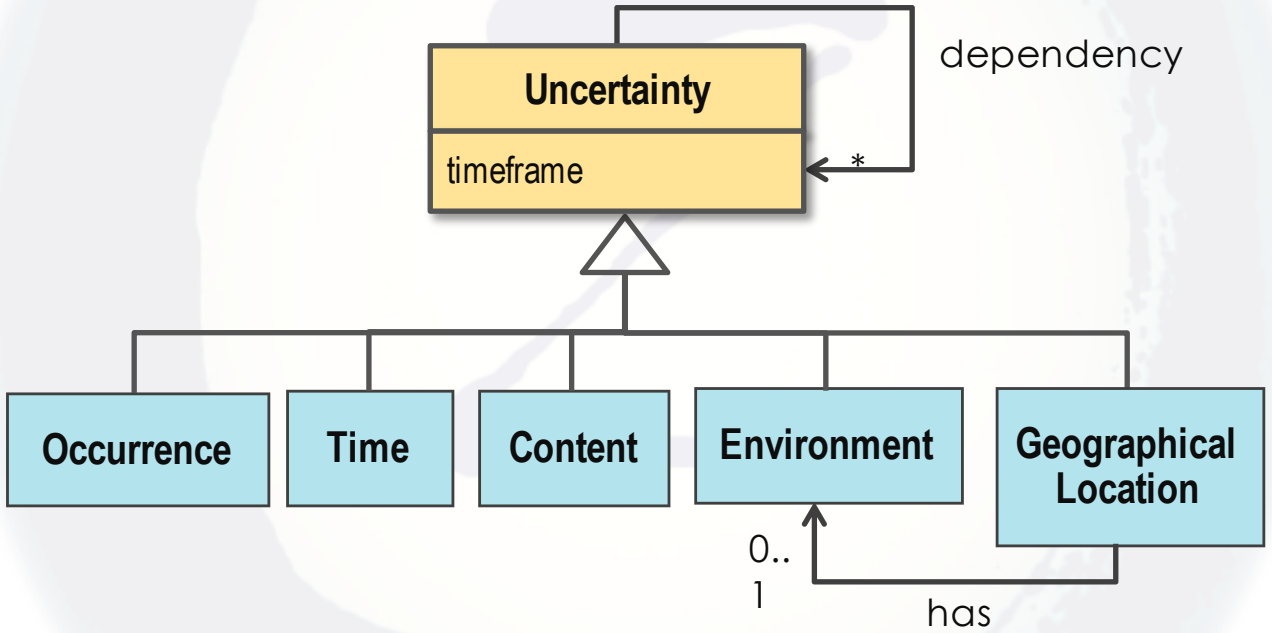
MORE KEY DEFINITIONS

- **Uncertainty**: Lack of confidence by a belief agent in the accuracy (truthfulness) of a belief statement
- **Uncertainty Measure**: An explicit quantified or qualified expression, specified by a belief agent, of the degree of uncertainty (or confidence) associated with a belief statement
  - ✓NB: Not a measure of truthfulness, but of *belief of truthfulness of a statement*
- **Indeterminacy Source**: the direct causes of uncertainties associated with a belief statement
- **Uncertainty Type**:
  - ✓Aleatory – uncertainty due to non-deterministic or variability phenomena
  - ✓Epistemic – uncertainty due to lack of information on the part of the belief agent

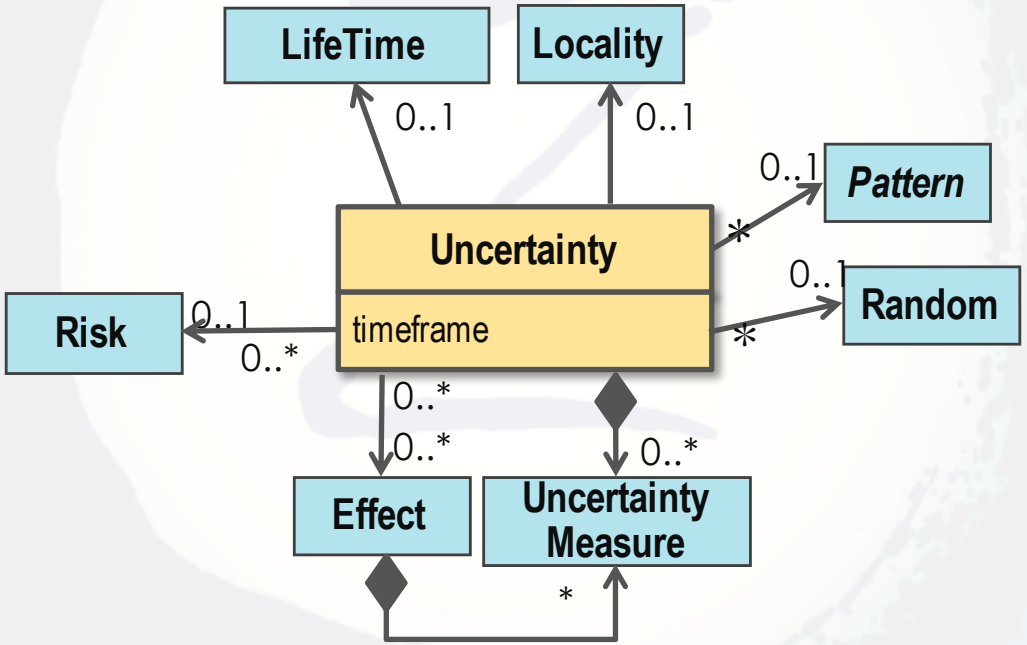
MEASURE MODEL



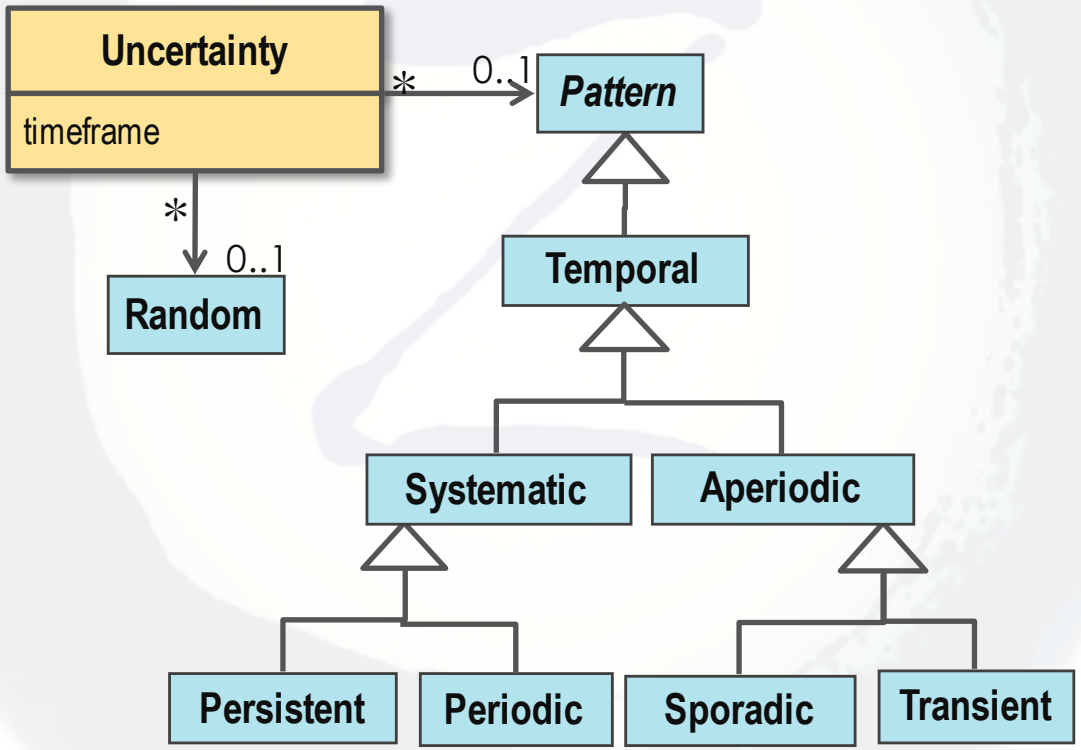
UNCERTAINTY MODEL - CLASSIFICATION



UNCERTAINTY MODEL - CHARACTERIZING UNCERTAINTY



UNCERTAINTY MODEL - PATTERNS OF UNCERTAINTY OCCURRENCE



UNCERTAINTY MODEL – *RISK*

SO, WHAT CAN WE DO WITH THIS?

- **Foundation for purpose-specific specializations**
  - ✓**Systematically identifying, collecting, specifying and discovering uncertainty requirements**
    - **Reference model for asking questions in a structured, precise, and systematic manner**
    - **RUCM-Uncertainty for specifying known uncertainty requirements and automated discovering of unknown uncertainty requirements**
  - ✓**Modeling, analysing and discovering software/system uncertainty behaviours**
  - ✓**Testing software/system under uncertainties**

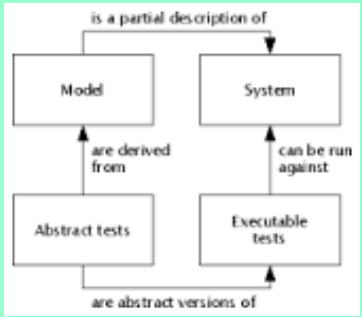
AGENDA

- The problem of uncertainty in system design
- The U-Test H2020 project
- U-Taxonomy: A conceptual model of uncertainty
- Applying the U-Taxonomy to CPS Testing
- Summary

PROPOSED TECHNICAL APPROACH

U-Test

Model-based Testing



- Abstraction
- Complexity management
- Automation
- Systematic approach
- Industry standards

+

Search-based Testing

- Optimization
- "Smart" mechanisms
- Uncovering unknown unknowns
- Genetic algorithms
- …

THE U-TEST H2020 PROJECT

U-Test: Testing Cyber-Physical Systems under Uncertainty

OBJECTIVE:

To improve the dependability of CPSs, via cost-effective model-based and search-based testing of CPSs under uncertainty, by (1) defining an uncertainty taxonomy and (2) holistic modelling and testing frameworks with considerable reliance on standards.

Approach: start with *requirements* as a basis for:

- Specifying uncertainties
- Test case specification

U-TEST: TESTING WITH UNCERTAINTY

- Relinquish full deterministic control of test
- Use search-based testing techniques (combined with genetic algorithms) to explore the "unknown unknown" space and uncover unforeseen situations

Search-based Testing

- Optimization
- "Smart" mechanisms
- Uncovering unknown unkowns
- Genetic algorithms
- …

This research is currently in progress

RUCM: RESTRICTED USE CASE MODELING*

- **A method (and tool) for specifying UML use cases based on restricted natural language**
  - ✓PhD thesis of Dr. Tao Yue at Carleton U. in Canada
  - ✓Facilitates transition from informal domain of user requirements to formal domain of engineering models
    - Automated translation of use cases to UML analysis models
  - ✓Tool and method currently in use by Simula Research Laboratory (Norway) and at the U. of Luxembourg
- **Zen RUCM version of the tool used in the U-Test project by case study providers to specify their use cases**
  - ✓https://ghost.simula.no/publications/Simula.simula.2078

(*) T. Yue, L. Briand, and Y. Labiche, "aToucan: An Automated Framework to Derive UML Analysis Models from Use Case Models", *ACM Trans. On Software Engineering and Methodology* (24, 3), May 2015.

RUCM EXAMPLE

Use Case Name	Withdraw Fund	
Brief Description	ATM customer withdraws a specific amount of funds from a valid bank account.	
Precondition	The system is idle. The system is displaying a Welcome message.	
Primary Actor	ATM customer	
Secondary Actors	None	
Dependency	INCLUDE USE CASE Validate PIN.	
Generalization	None	
Basic Flow	**Steps**	
	1	INCLUDE USE CASE Validate PIN.
	2	ATM customer selects Withdrawal through the system
	3	ATM customer enters the withdrawal amount through the system.
	4	ATM customer selects the account number through the system.
	5	The system VALIDATES THAT the account number is valid.
	6	The system VALIDATES THAT ATM customer has enough funds in the account.
	7	The system VALIDATES THAT the withdrawal amount does not exceed the daily limit of the account.
	8	The system VALIDATES THAT the ATM has enough funds.
	9	The system dispenses the cash amount.
	10	The system prints a receipt showing transaction number, transaction type, amount withdrawn, and account balance.
	11	The system ejects the ATM card.
	12	The system displays Welcome message.
	Postcondition	ATM customer funds have been withdrawn.

RUCM4UNCERTAINTY

- A modified version of the original RUCM tool that incorporates the UTaxonomy

Belief Specification

Use Case Name(Belief)	Monitor Windows and Doors
Brief Description	notify the monitoring personnel about a possible intrusion into the home.
Precondition(Belief)	The windows and doors options are not set.
Primary Actor(Belief)	Intruder
Secondary Actors (Belief)	Home Owner, Personnel, Magnetic Switch
Dependency(Belief)	None
Generalization(Belief)	None
Evidence Description	REF Experience
IndeterminacySource Description	REF Unpredicted intrusion, behavior
Belief Degree	Probability::80%
Belief Agent	Fancisco Rojas
Stated Time	03-06-2209, unknown

Basic Flow (Belief)	Steps
	1 IF Home Owner is outside TH
	2 Home Owner enables the
	3 The system enables the n
	4 DO
	5 The system invokes the
	6 The system VALIDATES THAT the status of windows and doors is normal.
	7 UNTIL Home Owner disables the monitoring of windows and doors
	8 ENDIF
	Postcondition (Belief): None

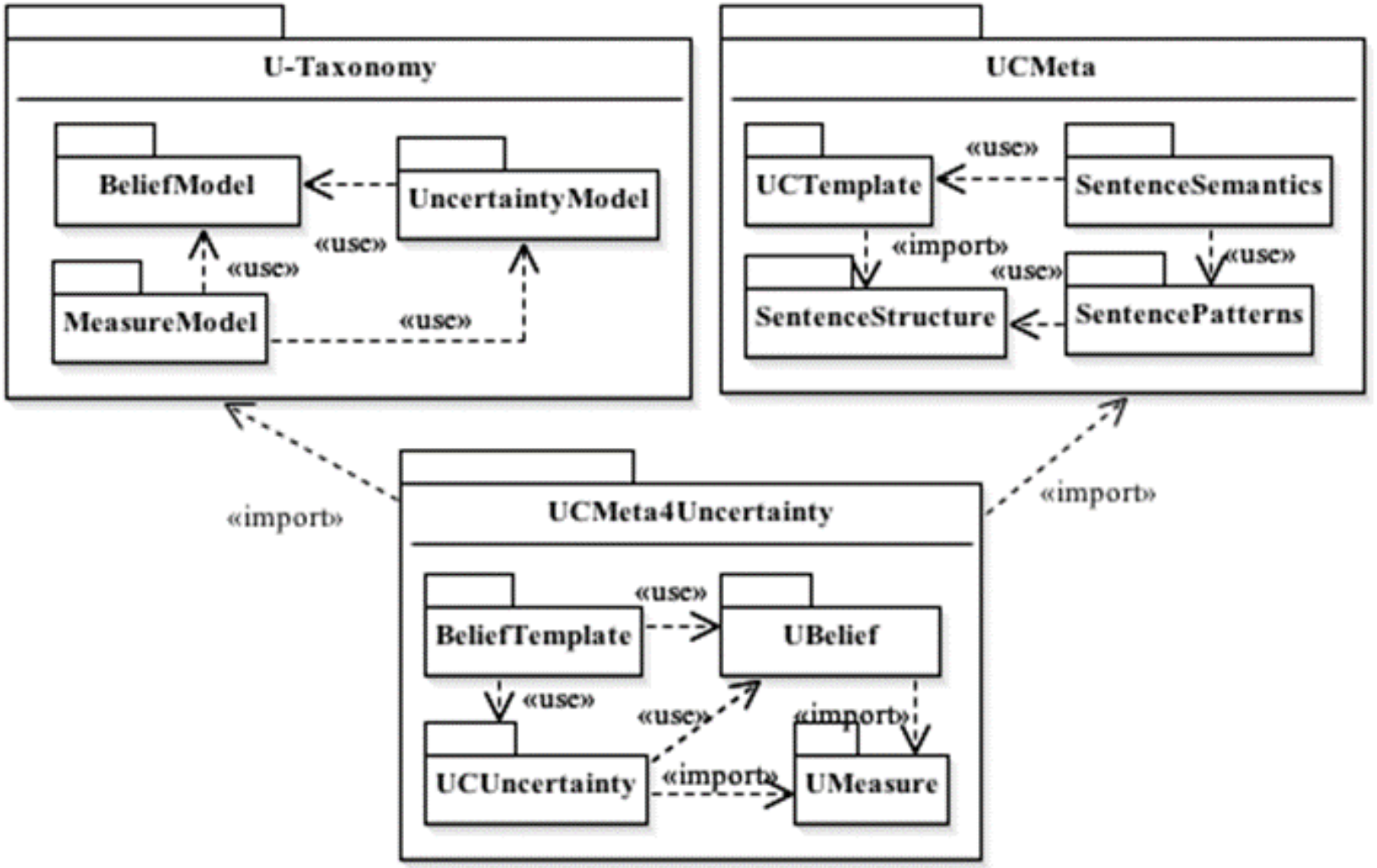
	URFS 5-6
	Intruder breaks the windows or doors.
	Magnetic Switch detects the intruder.
	The system VALIDATES THAT the status of windowws and doors is abnormal.
	Magnetic Switch alters the system to send a notification to the Monitroing personnel.
	The system sends the intrusion notification to Monitoring personnel MEANWHILE the system alarms bell.
	3 Monitoring personnel phones the police.
	4 ABORT.
	Postcondition (Belief): Intruder run away.

The entire use case (and/or individual steps) can be treated as a specific kind of Belief Statement with its own uncertainty characteristics and measures

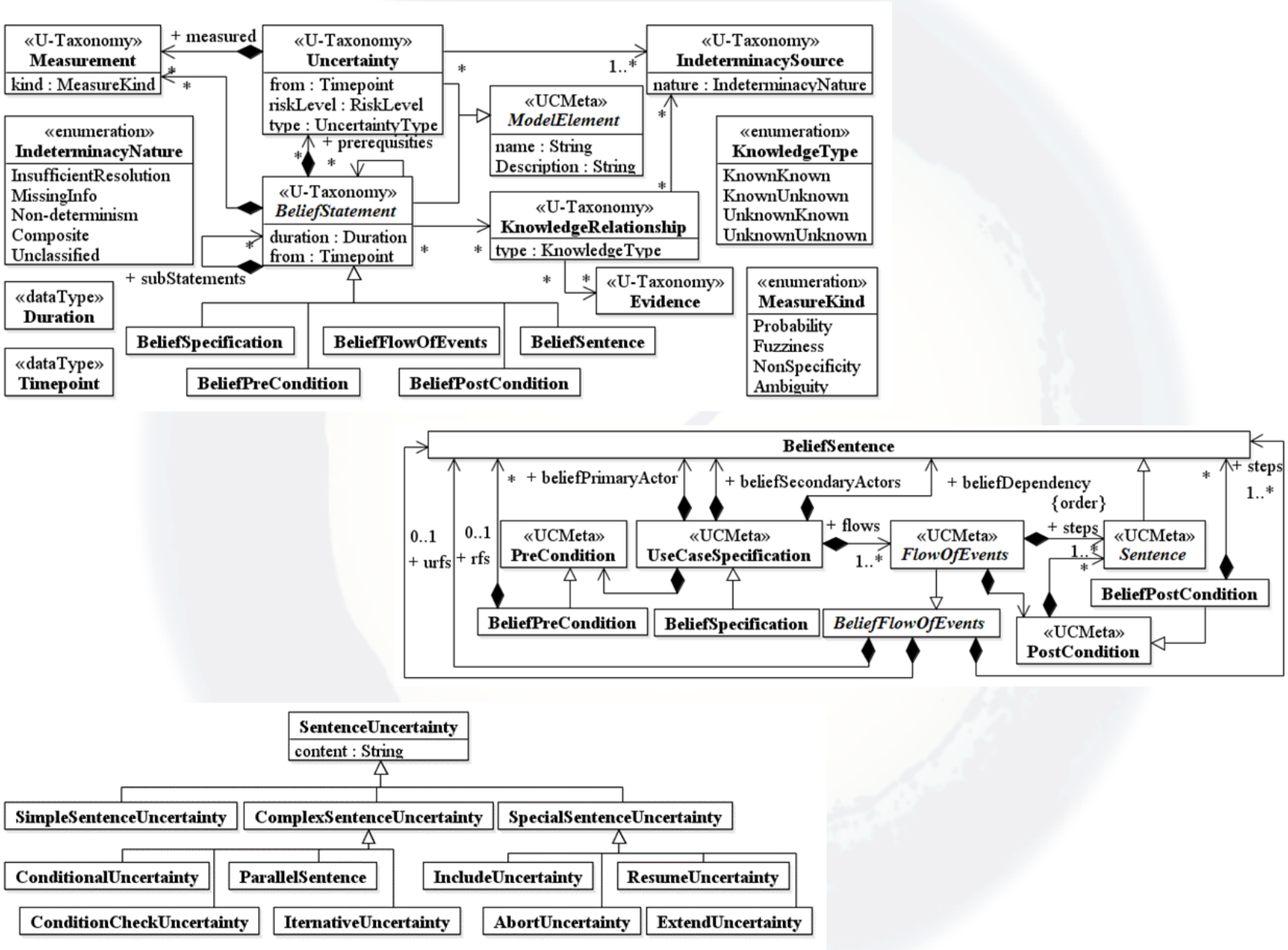
Belief statements can be characterized (e.g., trustworthiness)

RUCM FOR THE U-TAXONOMY

- For this to work, it was necessary to merge two domain-specific languages:



MERGED METAMODEL



AGENDA

- The problem of uncertainty in system design
- The U-Test H2020 project
- U-Taxonomy: A conceptual model of uncertainty
- Applying the U-Taxonomy to CPS Testing
- Summary

UNCERTAINTY AS PRIMARY DESIGN CONCERN

- Methods that explicitly address uncertainty

Set of all the things we need to know

Set of things we don't know that we don't know

(Unknown Unknowns)

Covered by "conventional" design methods

Set of things we know we don't know

(Known Unknowns)

Embracing Uncertainty

Implies:

- *Utility vs. Correctness*
- *Approximation vs. Precision*
- *Closed-loop systems*

New research challenges:

- *New design methods*
- *New formal methods and tools*
- *New testing methods*
- *…*

THE U-TEST H2020 PROJECT

U-Test

- **Primary focus on testing CPS in the presence of uncertainty**
- **Objectives:**
  - ✓ An extensible conceptual framework for representing and reasoning about uncertainty (the U-Taxonomy)
    - Status: Initial proposal available
    - Potentially reusable beyond the testing context
  - ✓ New methods for testing (initial work commencing)
    - Status: Experimental testbed and tool under construction
    - Status: Industrial case studies in development

THANK YOU!

An Uncertainty Taxonomy to Support Model-Based Uncertainty Testing of Cyber-Physical Systems
MAN ZHANG, BRAN SELIC, SHAUKAT ALI, TAO YUE, OSCAR OKARIZ AND ROLAND NORGREN
Technical Report TR 2015-3, Simula Research Laboratory
https://www.simula.no/publications/uncertainty-taxonomy-support-model-based-uncertainty-testing-cyber-physical-systems