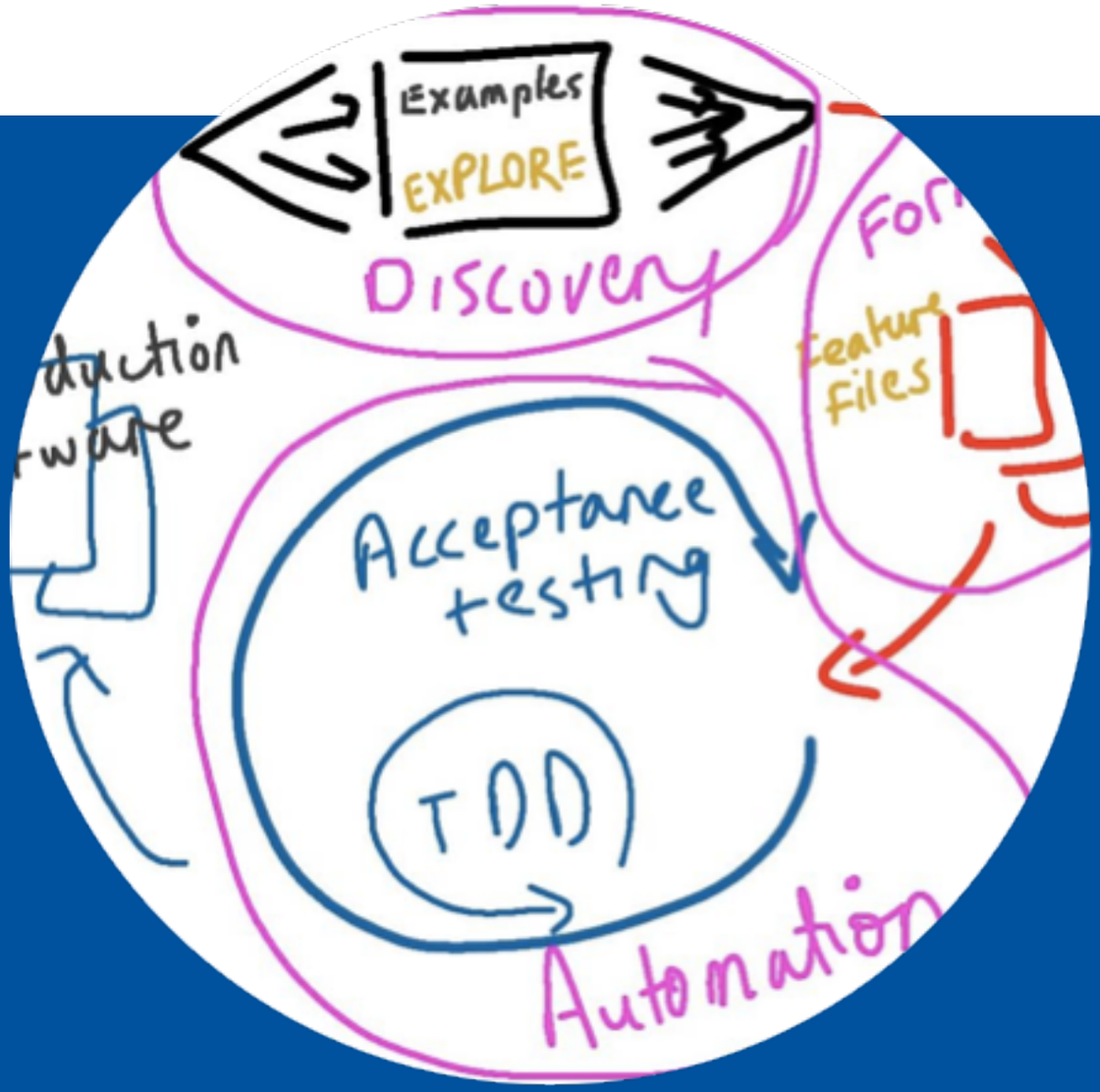
University of Stuttgart

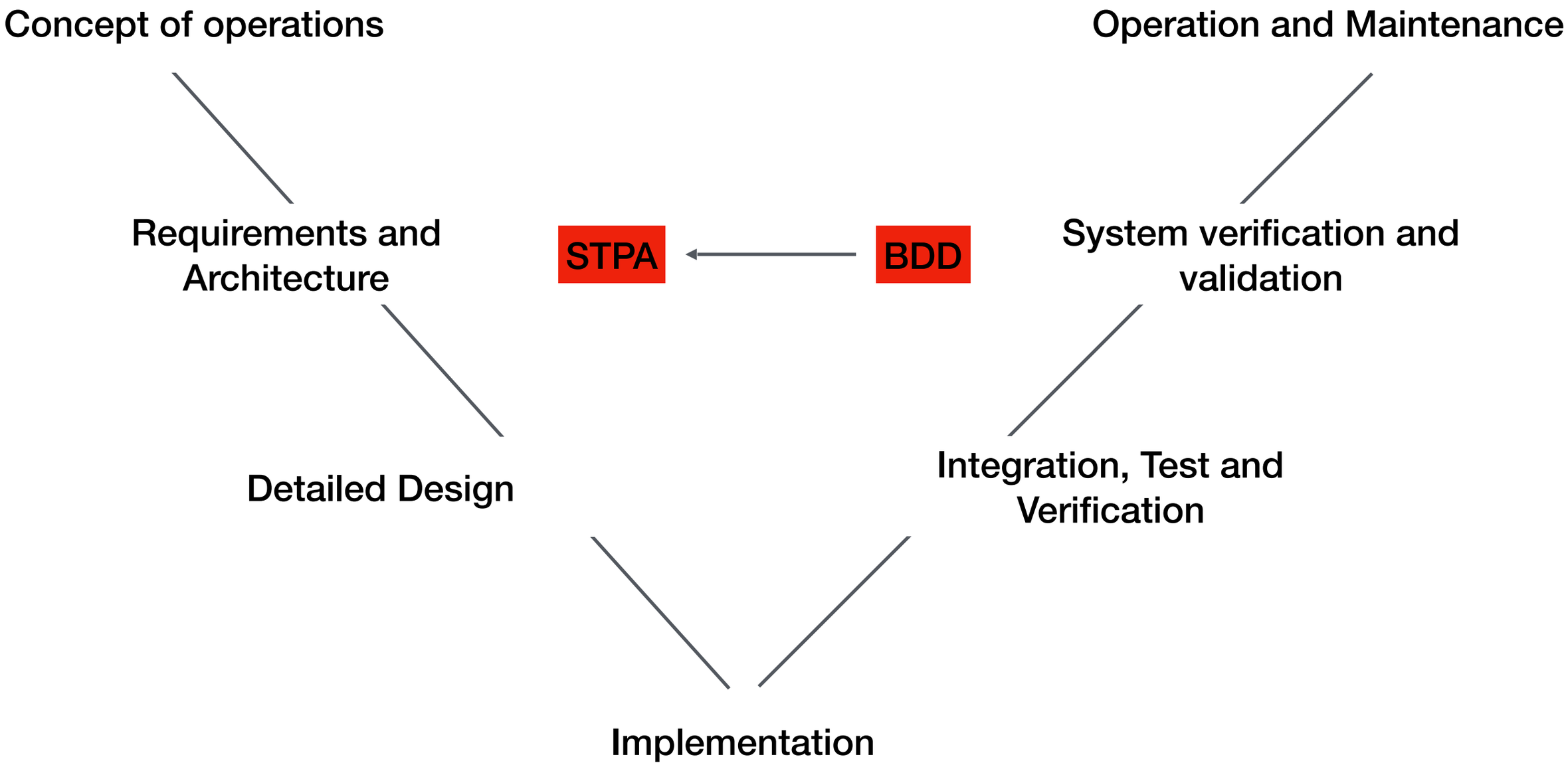
Combining STPA and BDD for Safety Analysis and Verification



Yang Wang
Joint work with Stefan Wagner
STAMP Workshop MIT, March 29, 2018

Papers will be published in:
the 19th International Conference on Agile Software Development, from May 21 to May 25, Porto, Portugal.
the 40th International Conference on Software Engineering Companion, from May 27 to June 3, Gothenburg, Sweden.

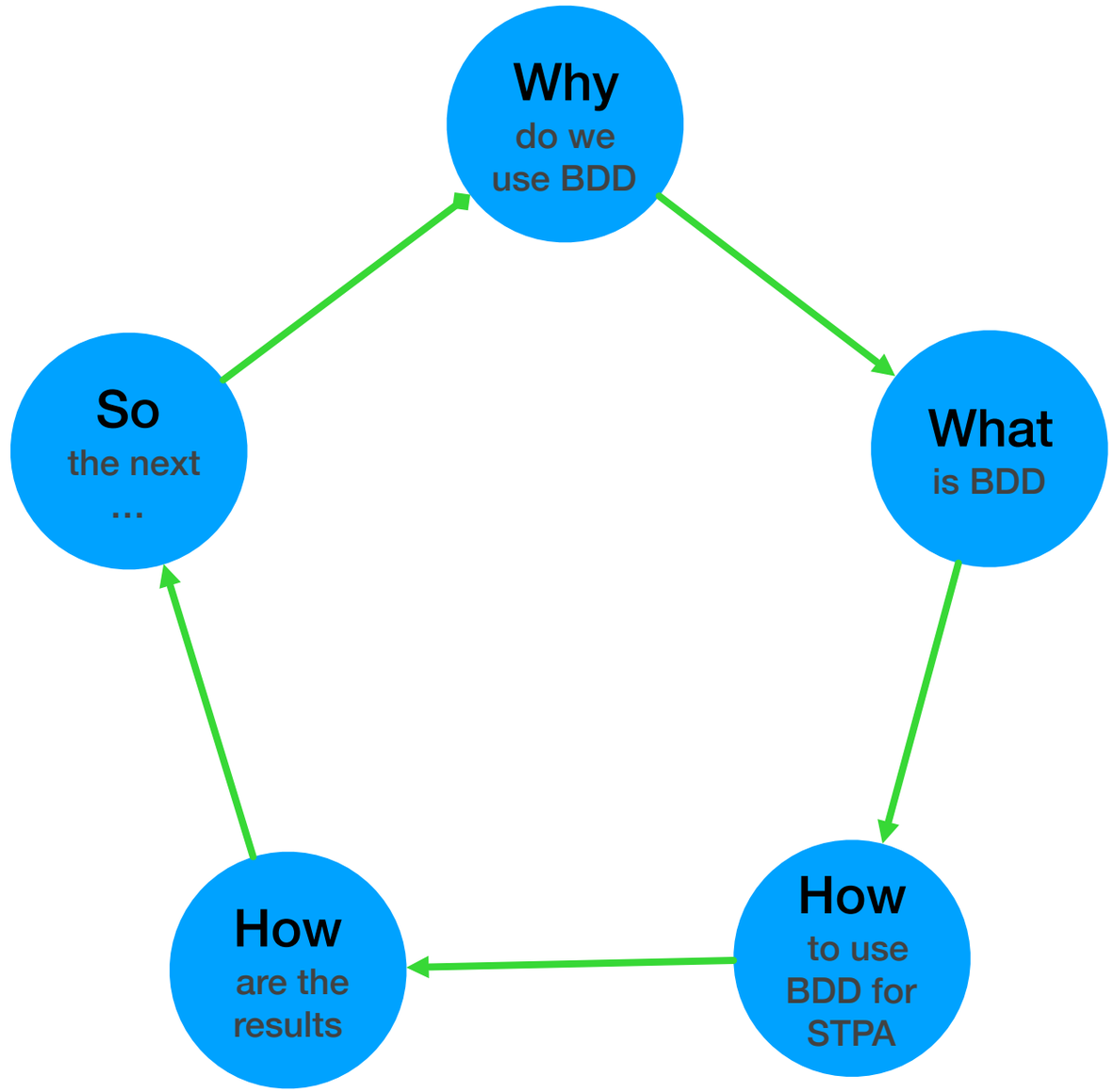
What we will talk about?



University of Stuttgart © Copyright Yang Wang | yang.wang@informatik.uni-stuttgart.de

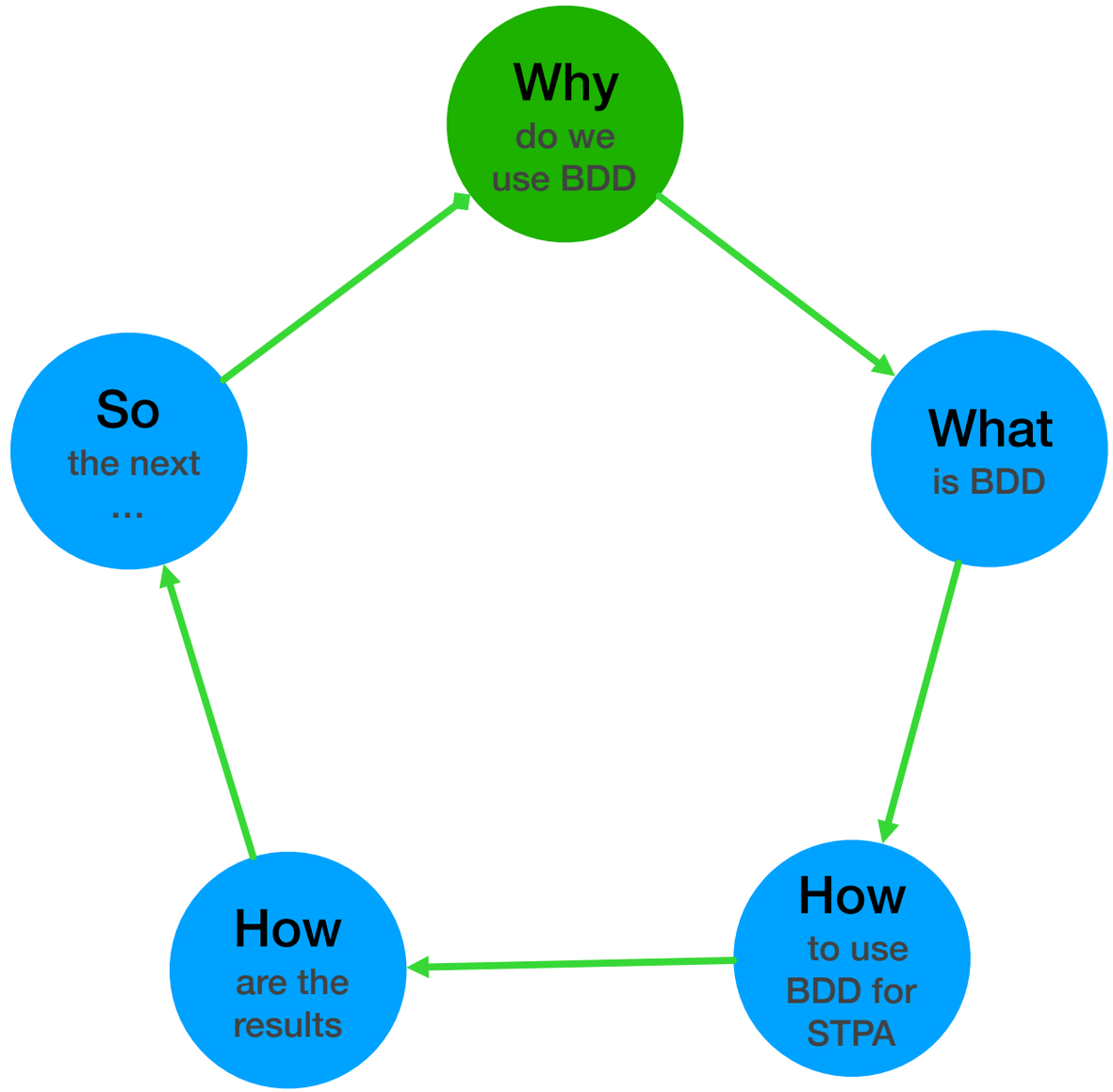
Agenda

1. **Motivation**
2. **BDD**
3. **STPA-BDD**
4. **Evaluation**
5. **Conclusion & Future Work**



Agenda

1. **Motivation**
2. **BDD**
3. **STPA-BDD**
4. **Evaluation**
5. **Conclusion & Future Work**



Existing safety verification

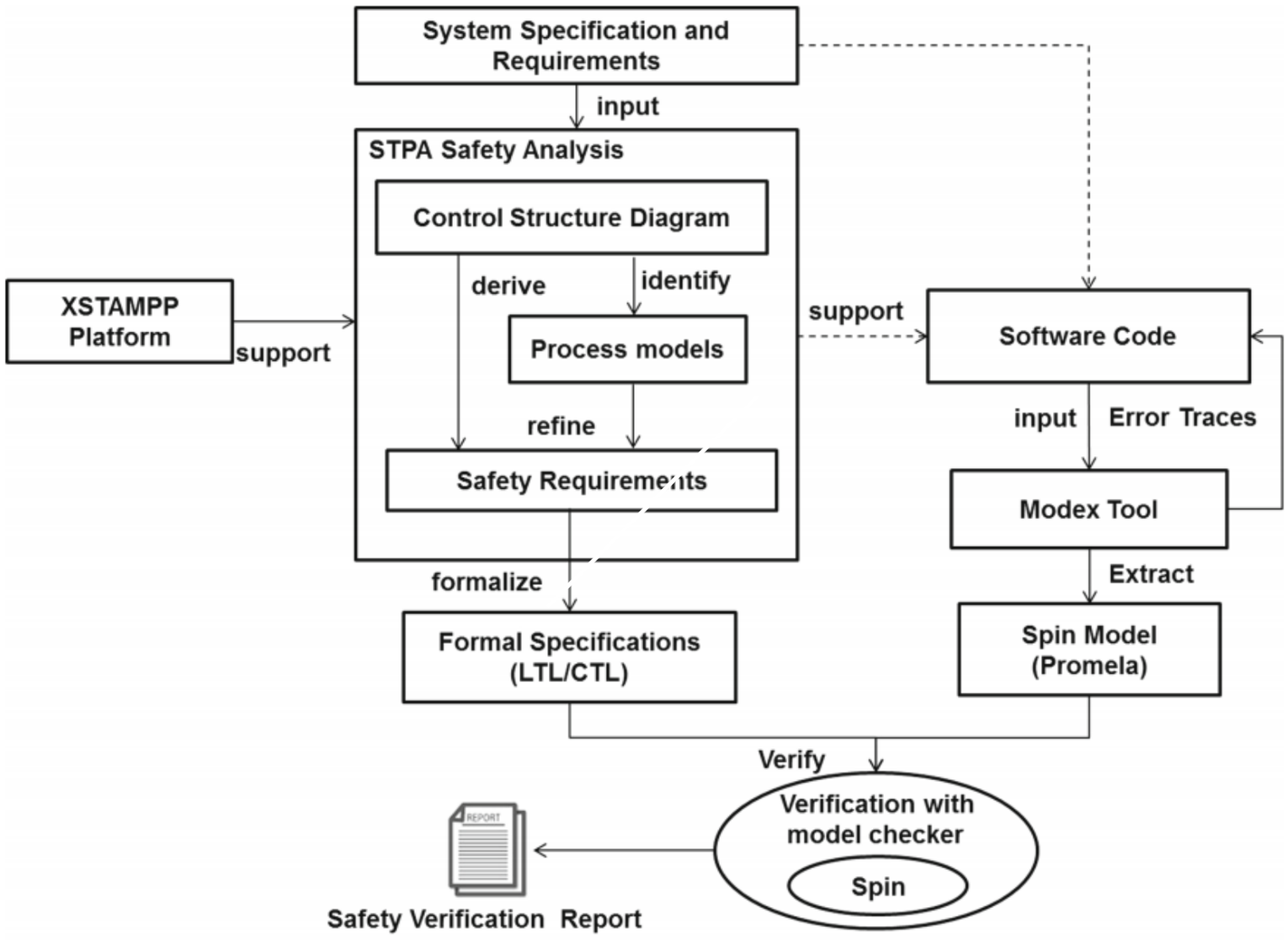
5

In industries, the prevalent method for verifying safety is testing (i.e. UAT).

Usually, UAT happens in a conference or war room sort of a set up where the users, PM, QA team representatives all sit together for a day or two and work through all the acceptance test cases.

University of Stuttgart © Copyright Yang Wang | yang.wang@informatik.uni-stuttgart.de

STPA + Model Checking



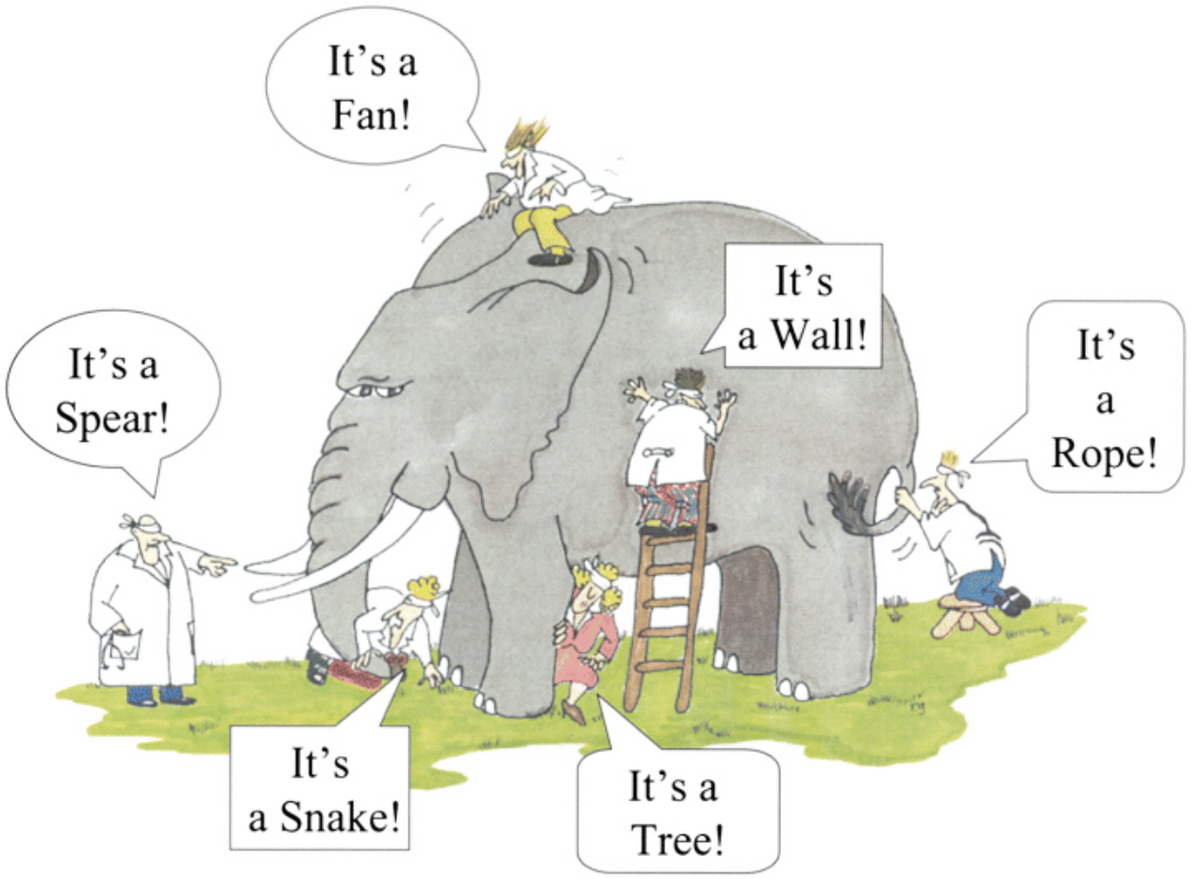
Integrated Safety Analysis Using Systems-Theoretic Process Analysis and Software Model Checking, Asim Abdulkhaleq and Stefan Wagner, 2016

University of Stuttgart © Copyright Yang Wang | yang.wang@informatik.uni-stuttgart.de

Problem Statement

8

“Weak communication between requirements engineers and test engineers often leads to confusing features.” - E. Bjarnason, P. Runeson, M. Borg et al.

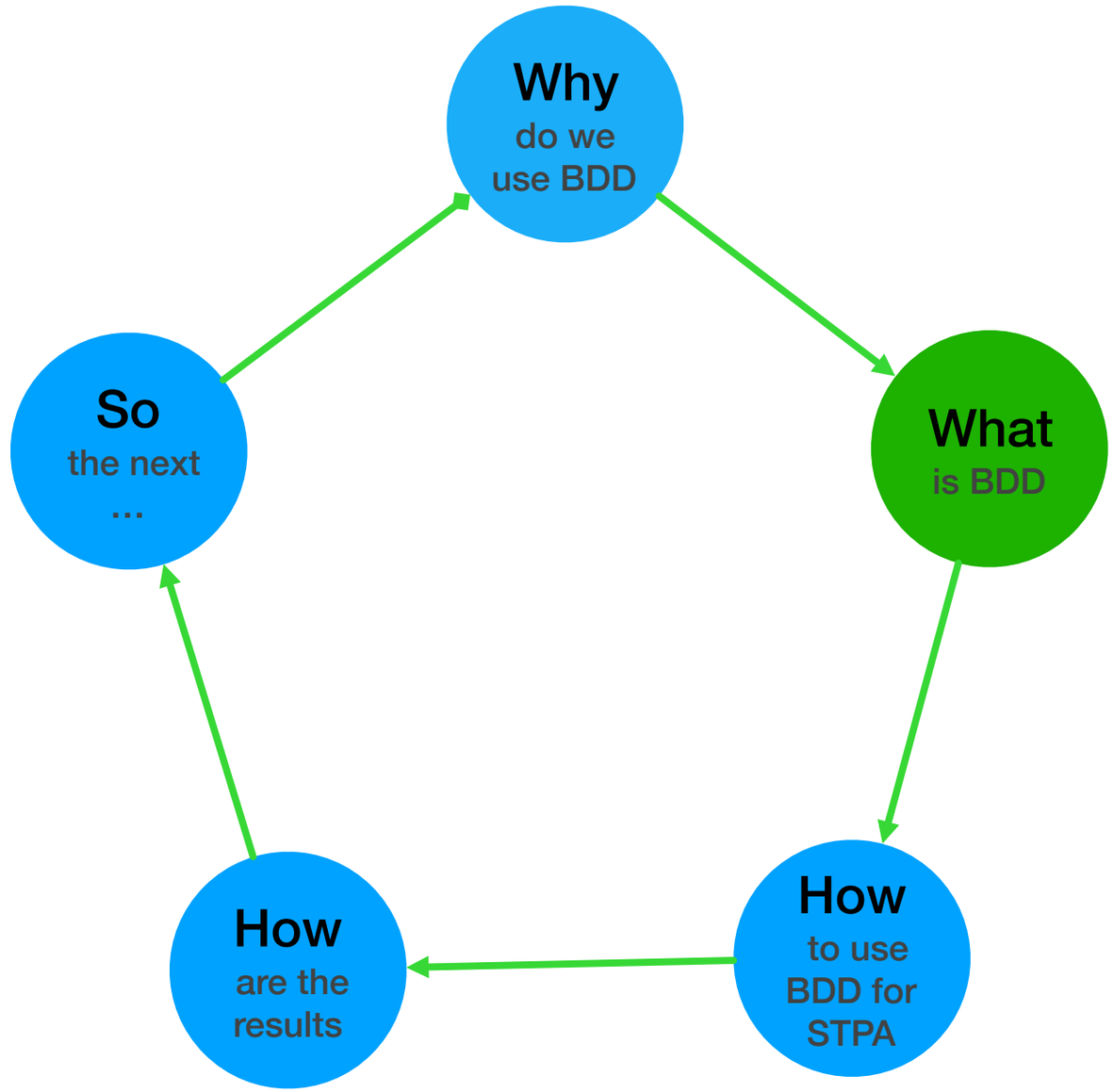


The safety verification needs to support ***communication.***

University of Stuttgart © Copyright Yang Wang | yang.wang@informatik.uni-stuttgart.de

Agenda

1. **Motivation**
2. **BDD**
3. **STPA-BDD**
4. **Evaluation**
5. **Conclusion & Future Work**



“ Behaviour-Driven Development (BDD) builds upon **Test-Driven Development** … The best practitioners work from the outside-in, starting with a failing customer acceptance test that describes the **behaviour** of the system from the customer’s point of view …We make a deliberate effort to develop a shared, **ubiquitous language** for talking about the system.”

- Matt Wynne et al.

11

Behaviour-Driven Development (BDD)

In the family of Test-Driven Development

Relies on testing system behaviour

Implements a template for generating test scenarios and test cases

Has been used for verifying non-functional requirements

Behaviour-Driven Development (BDD)

- Add a test
- Run all tests and see if the new test fails
- Write the code
- Run tests
- Refactor code
- Repeat

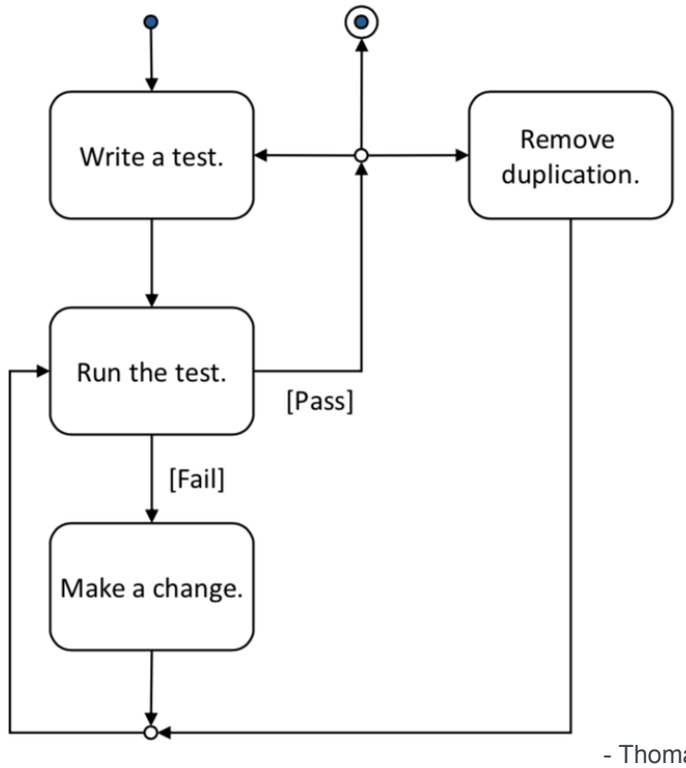
- Kent Beck

Relies on testing system behaviour

Implements a template for generating test scenarios and test cases

Has been used for verifying non-functional requirements

Behaviour-Driven Development (BDD)



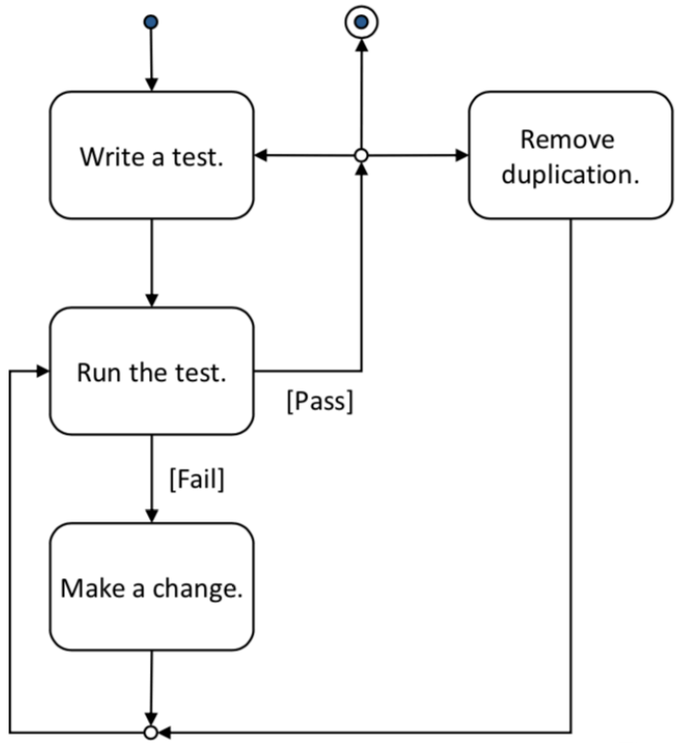
- Thomas Dohmke

Relies on testing system behaviour

Implements a template for generating test scenarios and test cases

Has been used for verifying non-functional requirements

Behaviour-Driven Development (BDD)



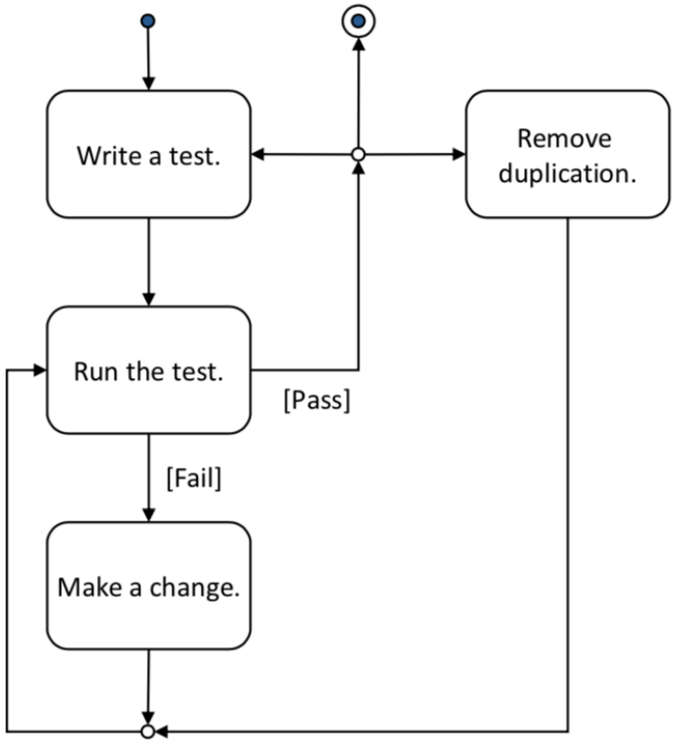
- Thomas Dohmke

TDD creates well-written unit of code
ATDD emphasises on developer-tester-business customer collaboration

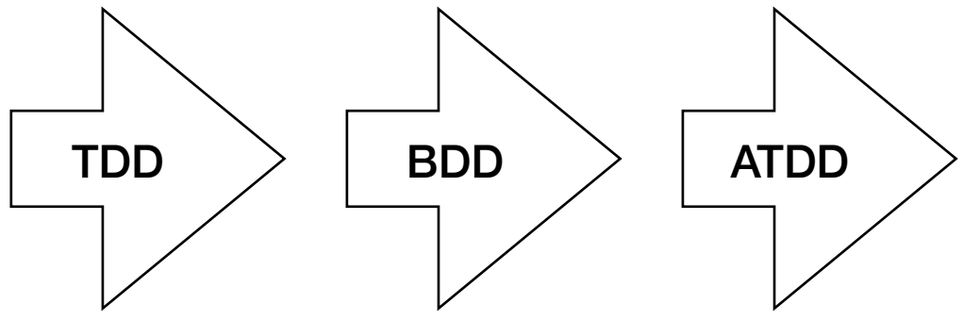
Implements a template for generating test scenarios and test cases

Has been used for verifying non-functional requirements

Behaviour-Driven Development (BDD)



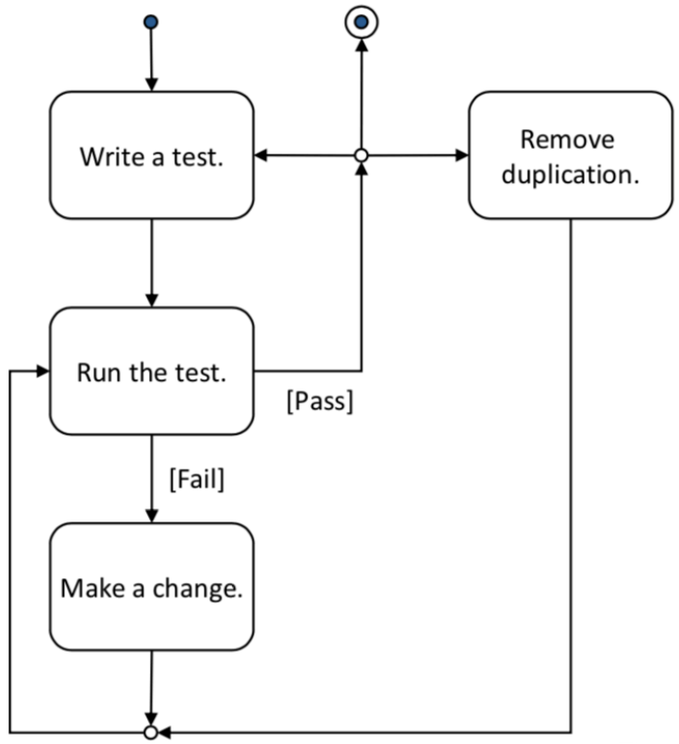
- Thomas Dohmke



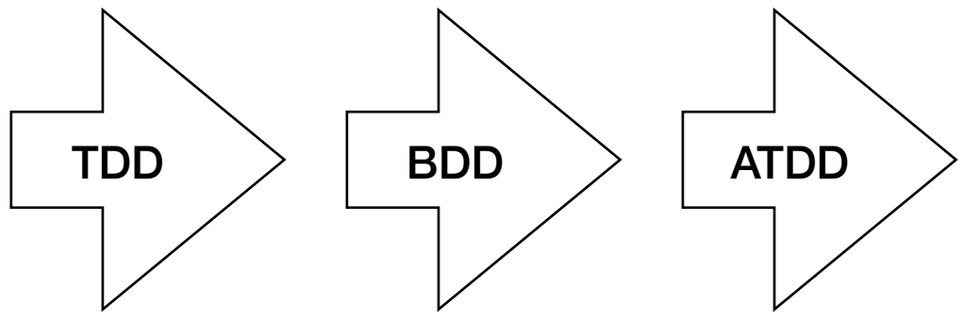
Implements a template for generating test scenarios and test cases

Has been used for verifying non-functional requirements

Behaviour-Driven Development (BDD)



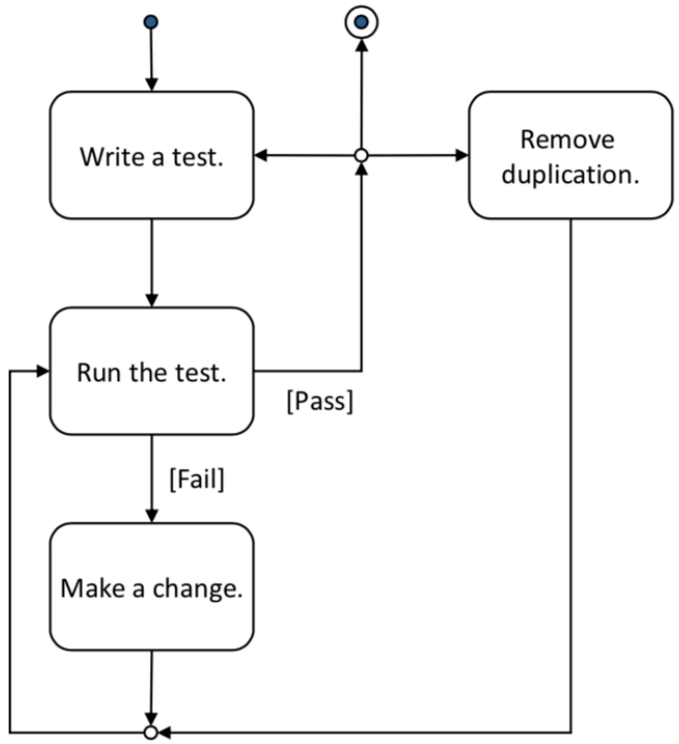
- Thomas Dohmke



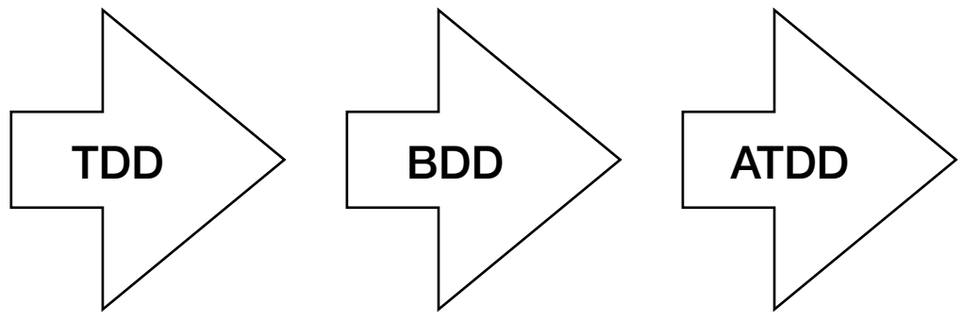
Given the initial context
When an event occurs
Then ensure some outcomes

Has been used for verifying non-functional requirements

Behaviour-Driven Development (BDD)



- Thomas Dohmke



Given the initial context
When an event occurs
Then ensure some outcomes

Scenario: Present the login form over an HTTPS connection

Given a new browser instance

And the login page is displayed

…

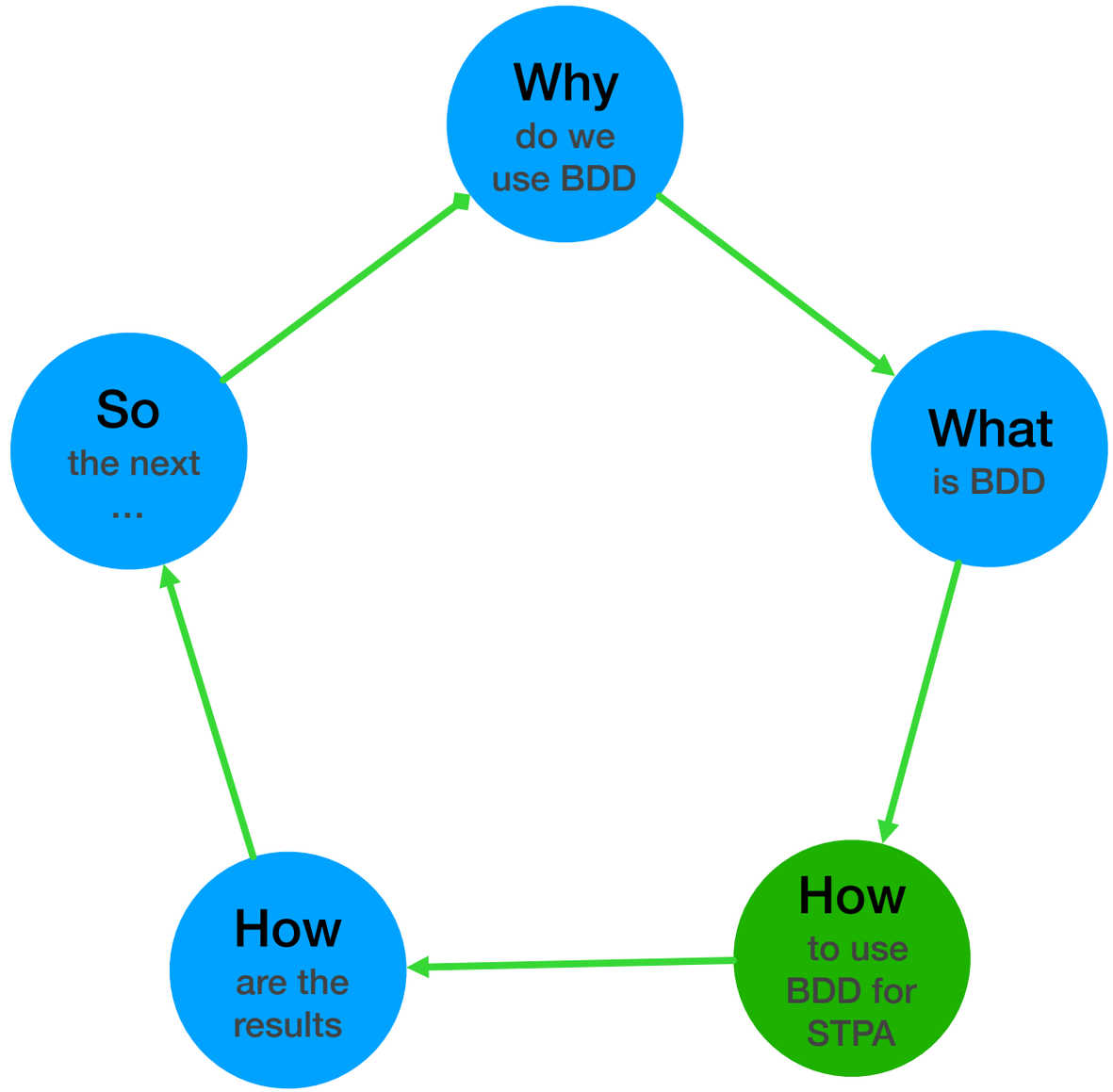
When the HTTP request-response containing the login form

Then the protocol should be HTTPS

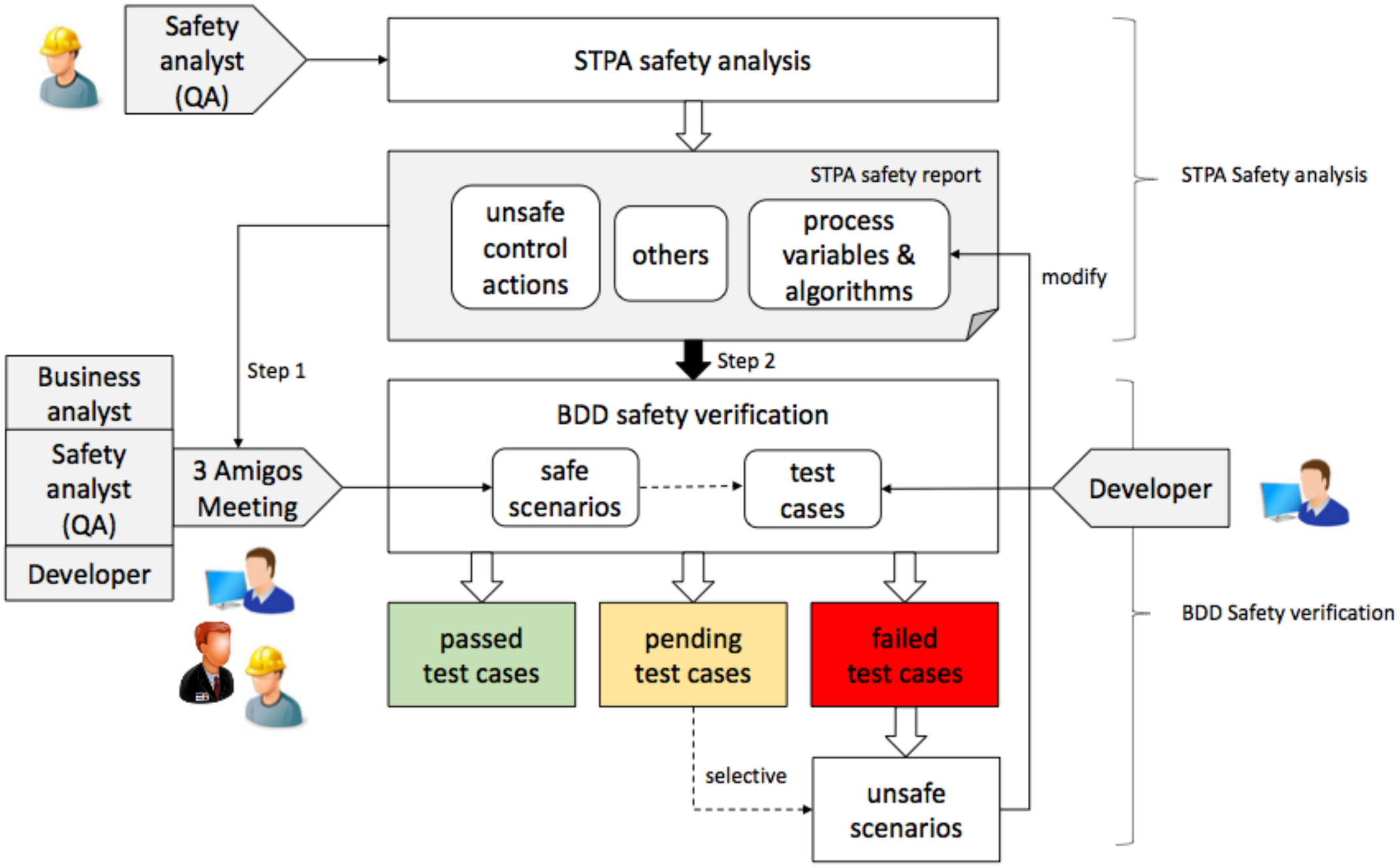
- continuumsecurity

Agenda

1. **Motivation**
2. **BDD**
3. **STPA-BDD**
4. **Evaluation**
5. **Conclusion & Future Work**



STPA - BDD



University of Stuttgart © Copyright Yang Wang | yang.wang@informatik.uni-stuttgart.de

Test Scenario Sample

BDD safety verification test scenario – sample

Narrative:
UCA: During auto-parking, the autonomous vehicle does not stop immediately when there is an obstacle upfront

A test scenario: The ultrasonic sensor provides right or wrong value

Given the autonomous vehicle is auto-parking
When the ultrasonic sensor provides the feedback that the forward distance <= threshold (means there is an obstacle upfront)
Then the autonomous vehicle stops immediately

University of Stuttgart © Copyright Yang Wang | yang.wang@informatik.uni-stuttgart.de

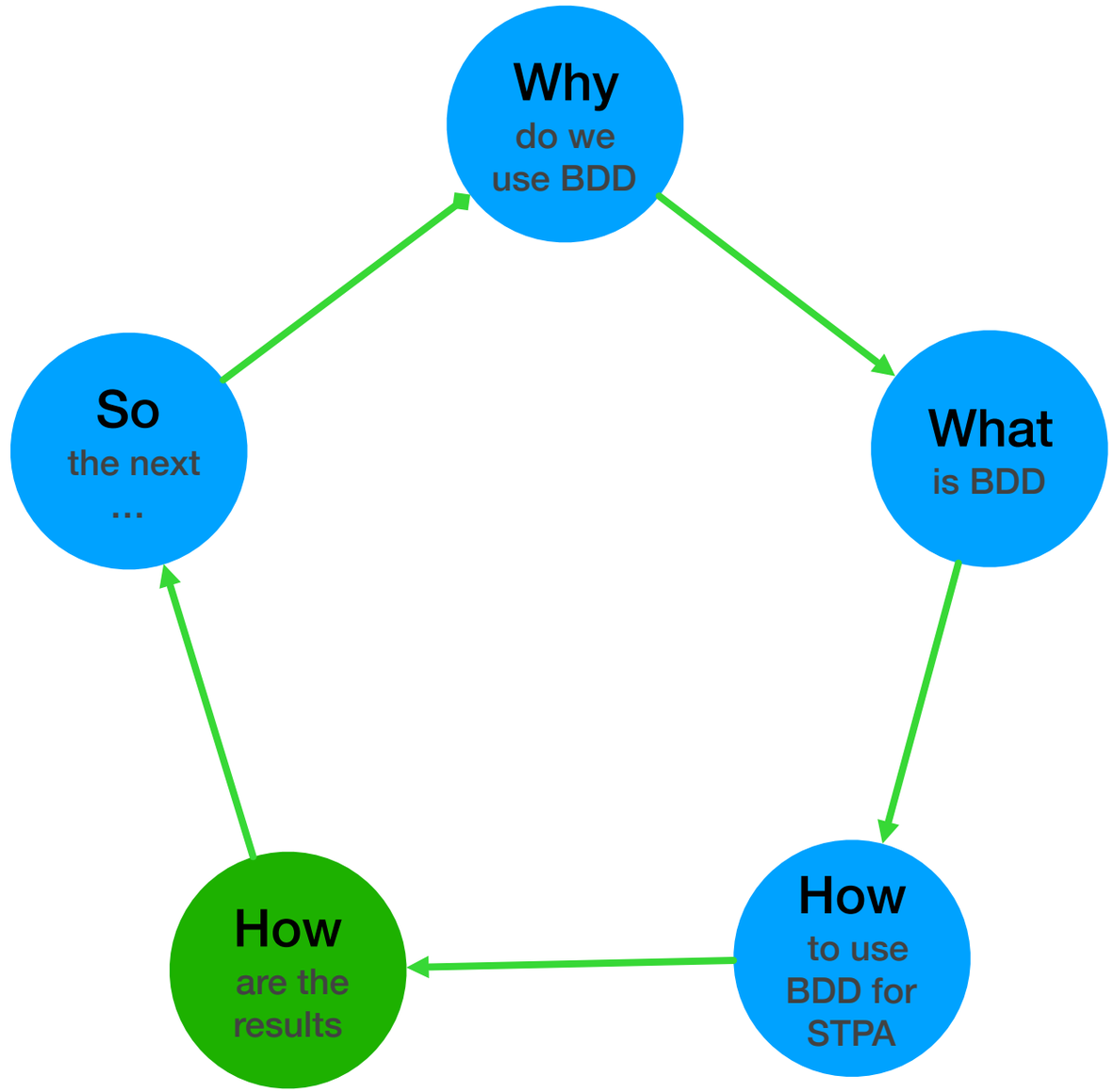
Test Case Sample

```
@Given("the autonomous vehicle is $auto-parking")
public void theAutonomousVehicleIsAutoParking () {
        vehicle.autoParking(); }

@When("the ultrasonic sensor provides the feedback
that the forward distance <= threshold (means there is an
obstacle upfront)")
public void theDistanceLessThanThreshold() {
        if (distance <= threshold) {vehicle.setSpeed (0);} }

@Then("the autonomous vehicle $stops immediately")
public void theAutonomousVehicleStopsImmediately() {
        assertEquals(motor.mode, Stop); }
```


University of Stuttgart © Copyright Yang Wang | yang.wang@informatik.uni-stuttgart.de

Agenda

1. **Motivation**
2. **BDD**
3. **STPA-BDD**
4. **Evaluation**
5. **Conclusion & Future Work**

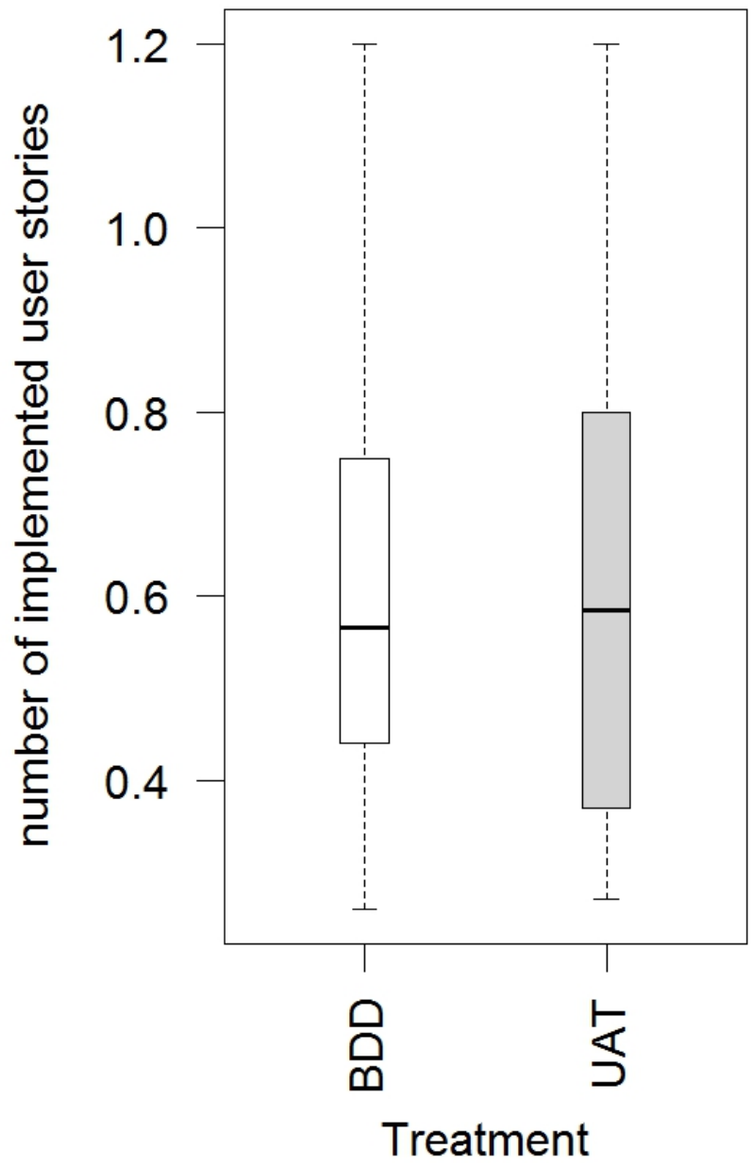


Preliminary Evaluation

University of Stuttgart © Copyright Yang Wang | yang.wang@informatik.uni-stuttgart.de

Productivity

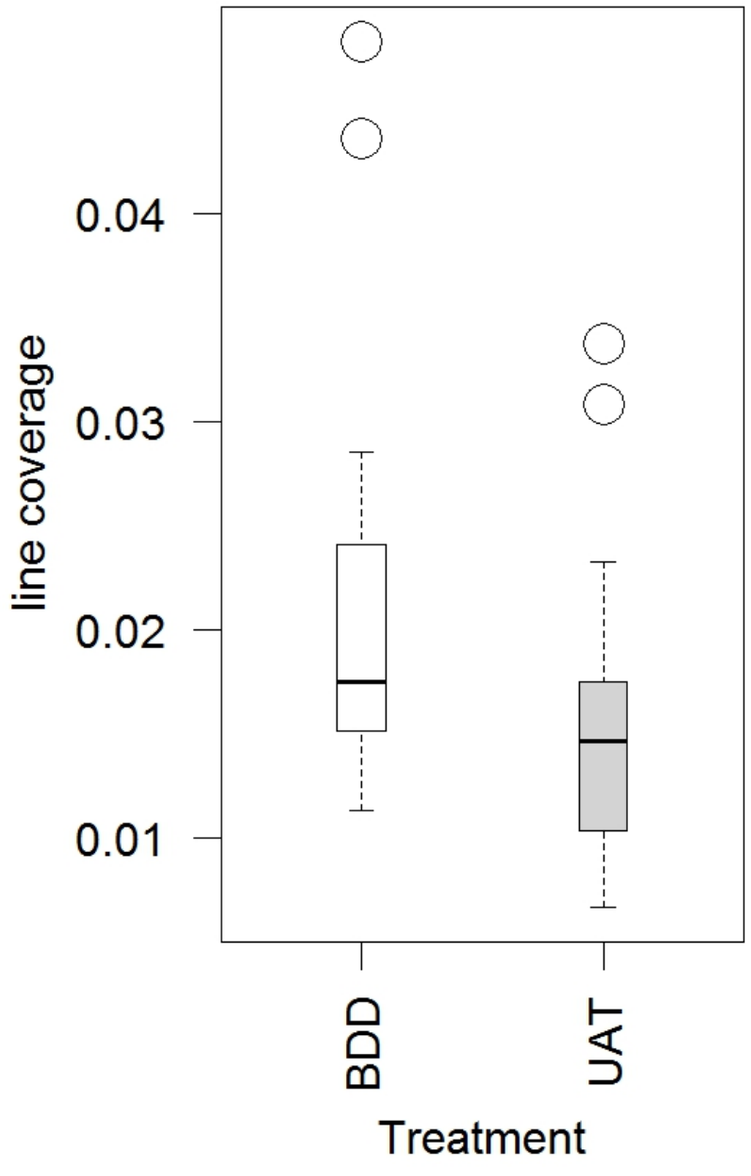
We test how many safety requirements can be written into test cases within a limited time slot.

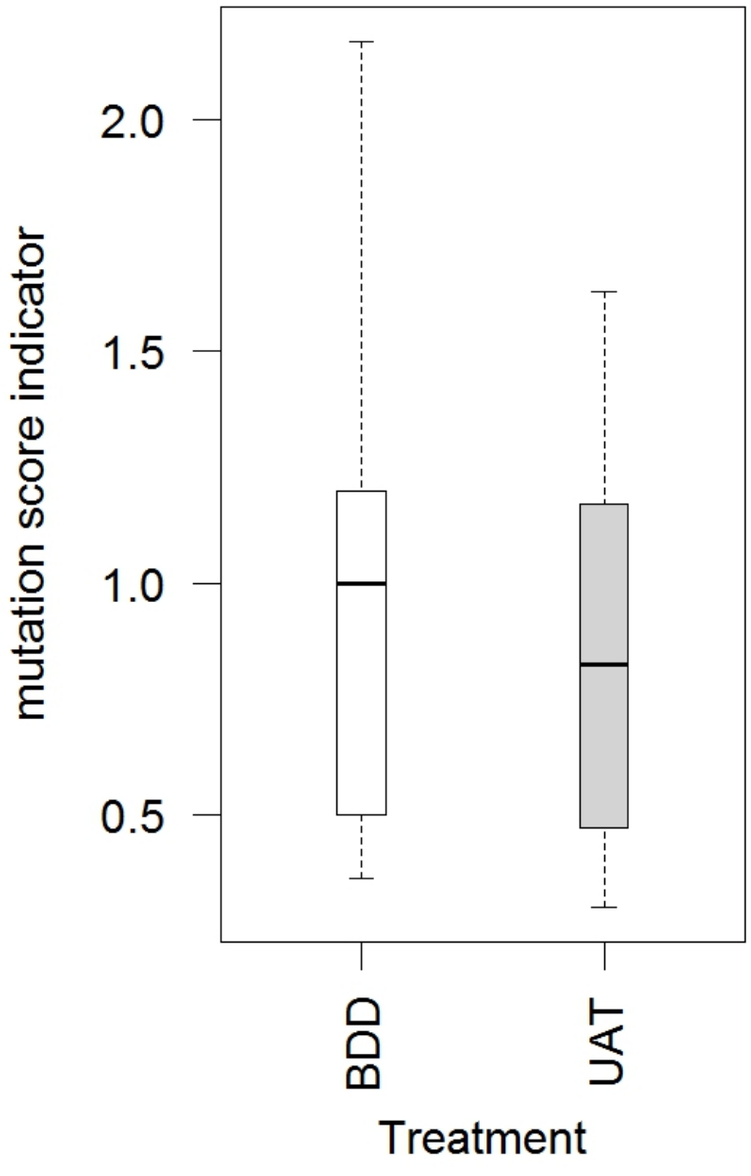


University of Stuttgart © Copyright Yang Wang | yang.wang@informatik.uni-stuttgart.de

Quality

We test the quality through the automated test reports from Eclipse and PIT.





University of Stuttgart © Copyright Yang Wang | yang.wang@informatik.uni-stuttgart.de

Communication

The participants portray as business analysts and developers to discuss the STPA-BDD test cases and test results.

From the developer's perspective:

- BDD has a clear documentation.
- The developers could flush out functional gaps before development.
- The developers have a good understanding of the business requirements.
- BDD test cases have a good organisation and structure.
- Realistic examples make the developers think harder.
- There is an obvious glue between test cases and code.

University of Stuttgart © Copyright Yang Wang | yang.wang@informatik.uni-stuttgart.de

Communication

The participants portray as business analysts and developers to discuss the STPA-BDD test cases and test results.

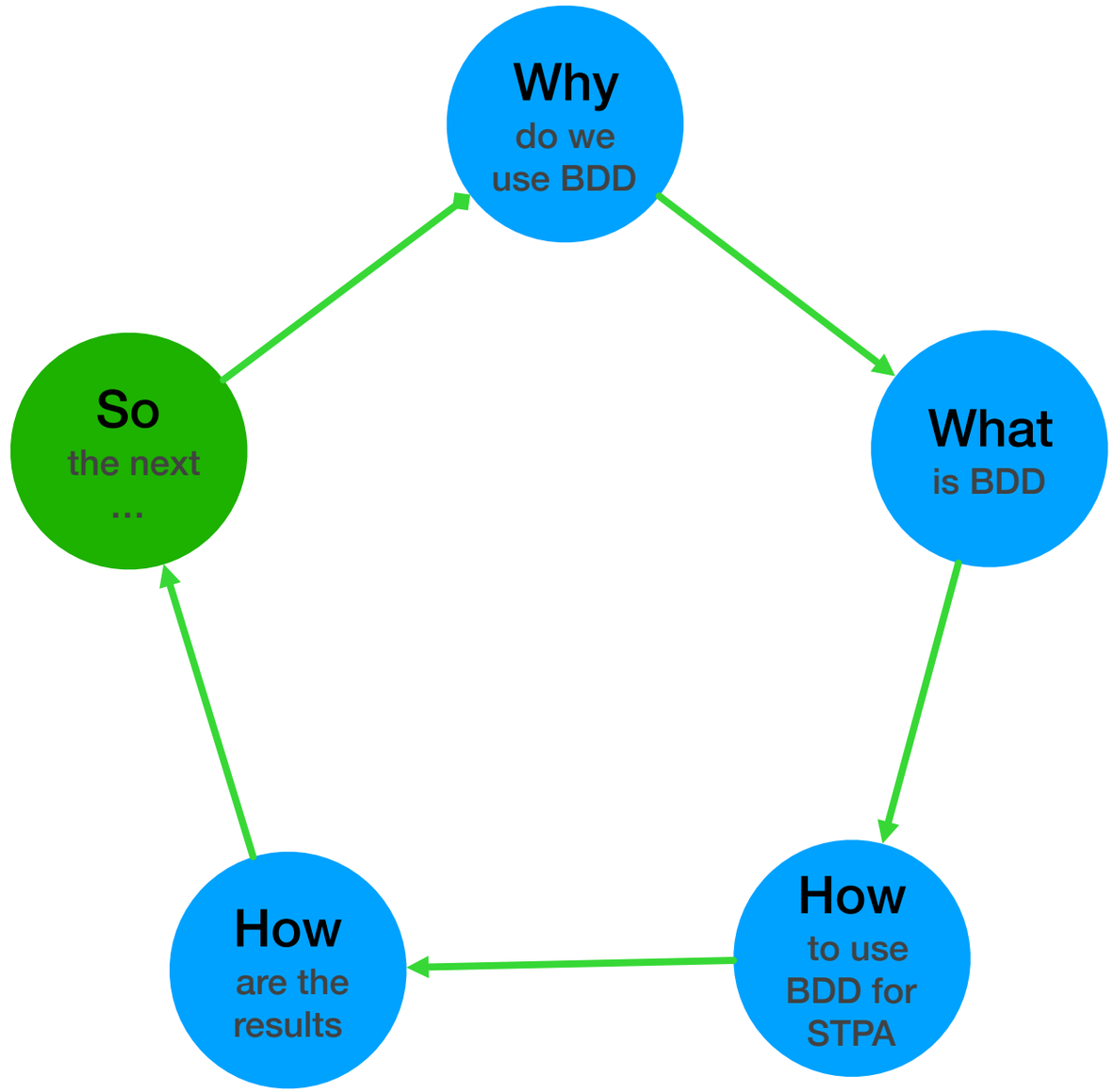
From the business analyst’s perspective:

- The developers consider the safety requirements deeply and initiatively.
- The business analysts are more confident about the test cases.
- It becomes easier to identify conflicts in business rules and test cases.
- The business analysts are clear about the status of acceptance testing.
- The business analysts could spend less time on sprint-end acceptance tests.

University of Stuttgart © Copyright Yang Wang | yang.wang@informatik.uni-stuttgart.de

Agenda

1. **Motivation**
2. **BDD**
3. **STPA-BDD**
4. **Evaluation**
5. **Conclusion & Future Work**



Conclusion

BDD seems to be a possible way for STPA to verify safety requirements.

- It verifies system behaviours.
- It can start at an early stage.
- It supports communication.

University of Stuttgart © Copyright Yang Wang | yang.wang@informatik.uni-stuttgart.de

Future Work

- Combine BDD with STPA requirements specification.
- Test automation of BDD.
- Evaluation with professionals.

University of Stuttgart © Copyright Yang Wang | yang.wang@informatik.uni-stuttgart.de

University of Stuttgart

Thanks!

Yang Wang, PhD candidate

e-mail yang.wang@informatik.uni-stuttgart.de

phone +49 (0) 711 685-88342

www. iste.uni-stuttgart.de/en/se/people/yang-wang.html

University of Stuttgart
Institute of Software Technology