EXTENDING AN EXISTING CONFORMANCE TEST SYSTEM WITH THE ABILITY OF NEGATIVE TESTING

Steffen Lüdtke, October 2017

Fraunhofer FOKUS

Engineering a Connected World

Agenda

- Conformity and interoperability testing of HL7 and IHE
- Fuzztesting
- Heuristics for HL7
- Prototype
- Case Study

CONFORMITY AND INTEROPERABILITY TESTING OF HL7 / IHE

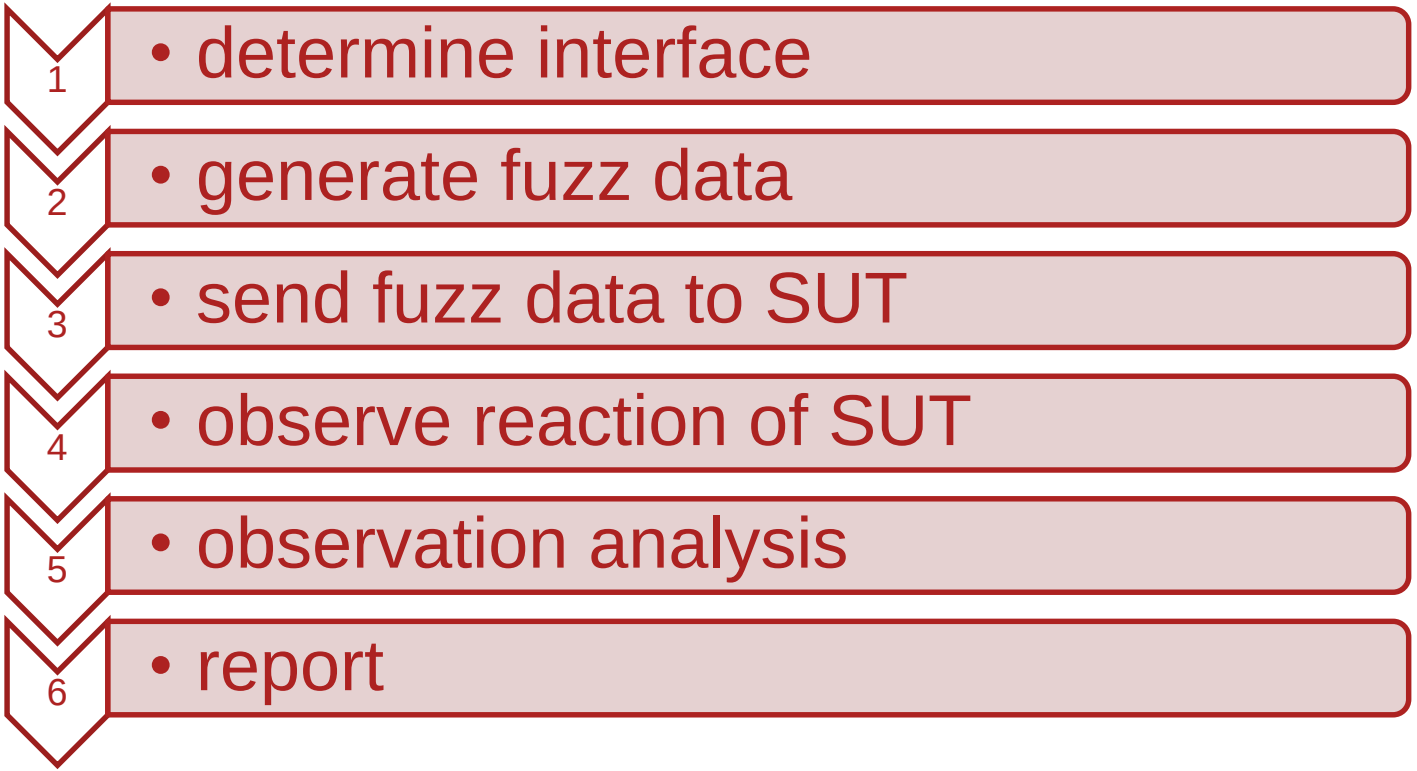
- HL7 is standard for information exchange in medical domain
- version 2 is simple and text-based
- HL7 defines message structure, IHE application scenarios and sequences

```
MSH|^~\&|ADT1|CUH|LABADT|CUH|198808181127|SECURITY|ADT^A01^ADT_A01|MSG00001|P|2.3|
EVN|A01|198808181122||
PID|||PATID1234^5^M11||RYAN^HENRY^P||19610615|M||2054-5|1200 N ELM STREET^^GREENSBORO^NC^27401-1020|...
NK1|JOHNSON^JOAN^K|WIFE|||||1|||NK^NEXT OF KIN
PV1|1|I|2000^2053^01||||004777^FISHER^BEN^J.|||SUR||||ADM|A0|
```

Fuzztesting

- Fuzz testing or fuzzing is a technique in the area of security testing
- A system is executed with unexpected, invalid inputs or messages sequences
- Fuzz tests are characterized by a high degree of automation and a big number of test cases
- Test oracle observes SUT and evaluates reaction

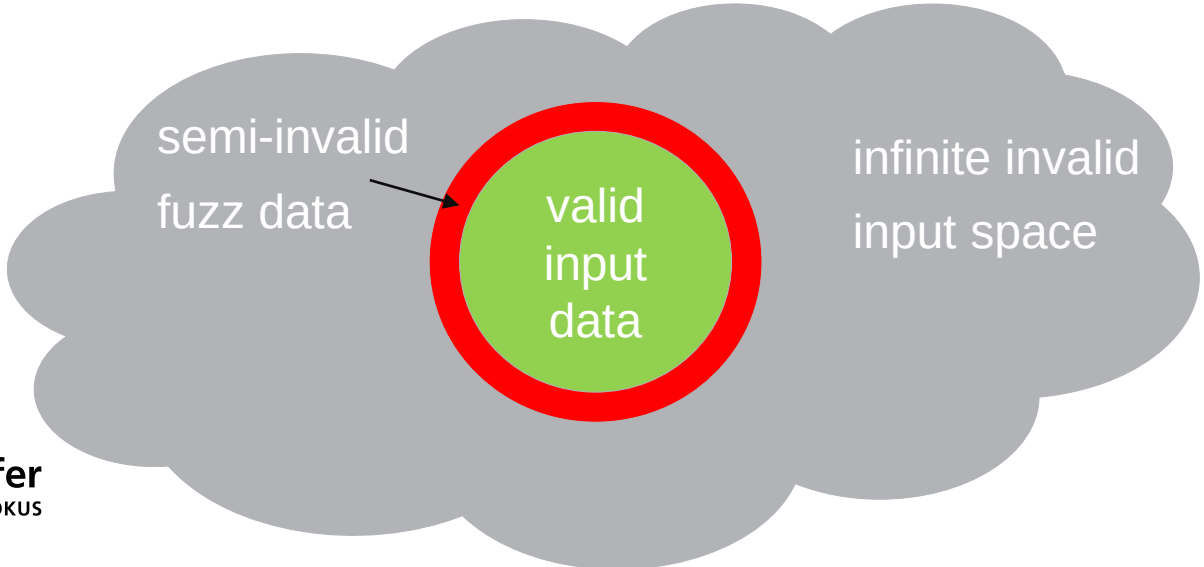
Fuzztesting - Phases



Fraunhofer FOKUS

Heuristics

- The infinity input space of the (invalid) input data makes a constructive limitation of the test data necessary
- Test data for fuzz tests are created heuristically
- Heuristics create with guidelines semi-invalid test data



Heuristics

- Realization of heuristics in Fuzzino

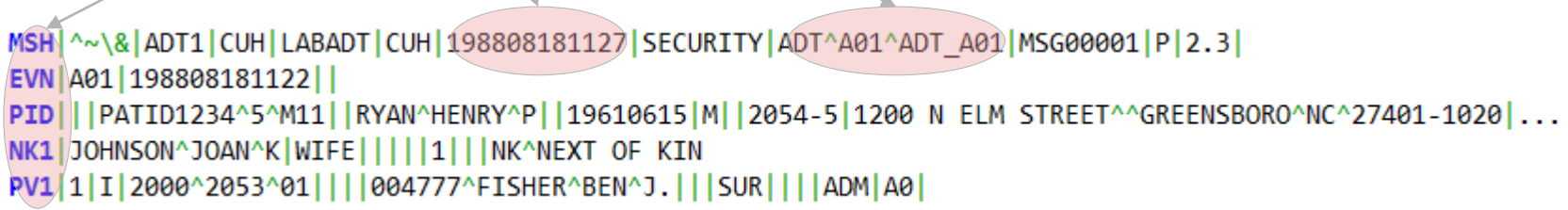
- Example heuristic: 29. February
  - take all 29. February of the years 0000 to 9999
  - Remove all leap years
  - Result: 7562 data sets with non-existing 29. February

Heuristics

heuristic for a data field

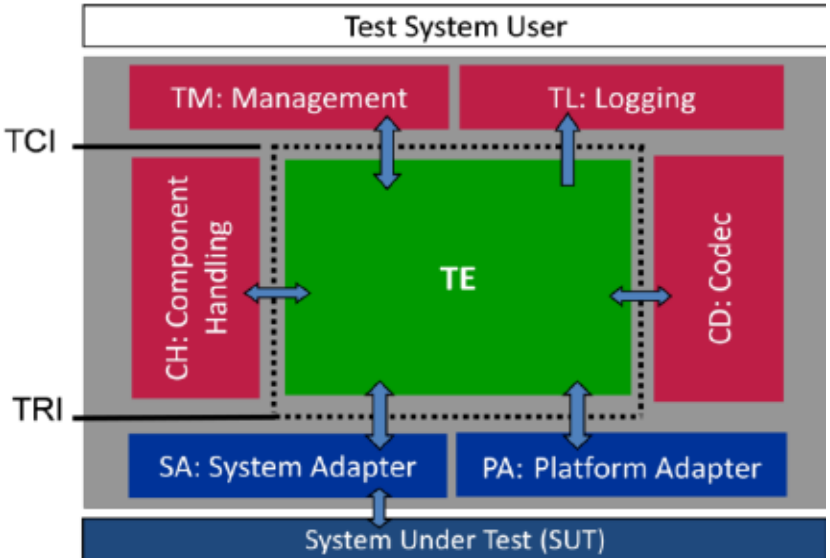
heuristic for a structured field

heuristic for message structure

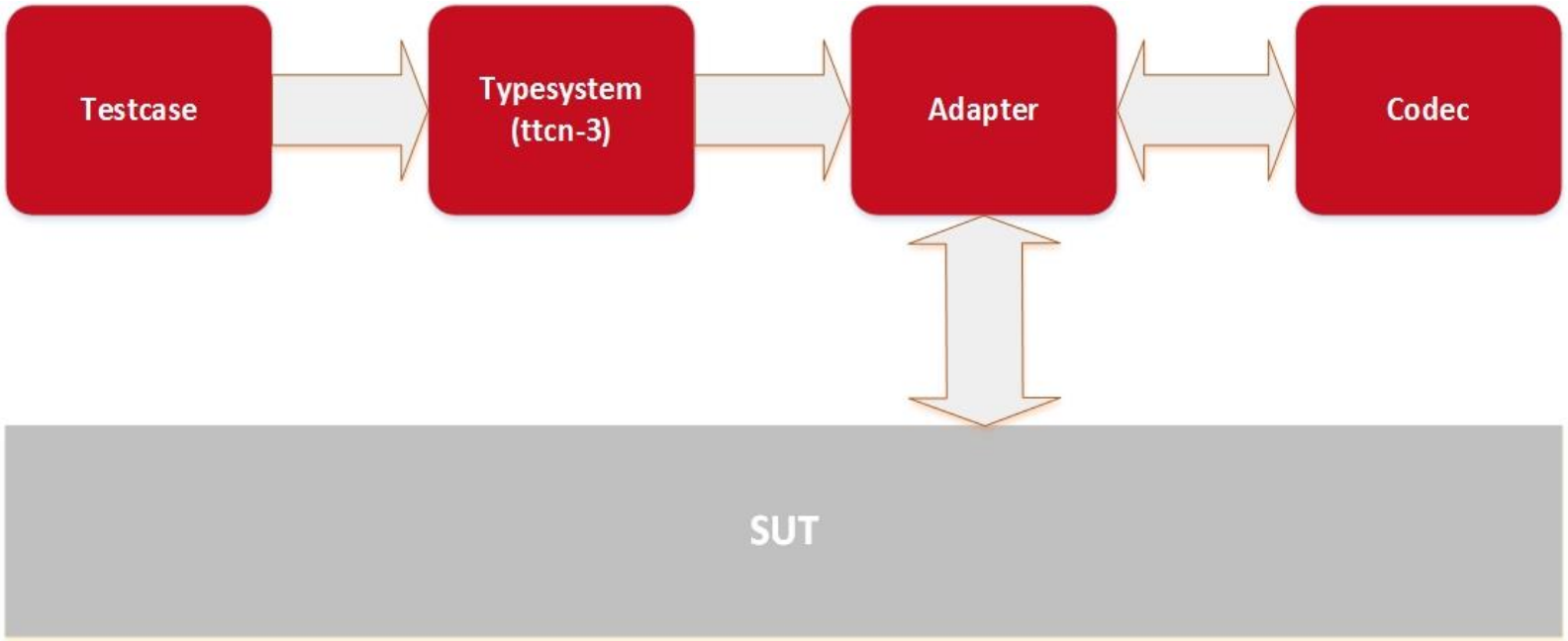


TTCN-3 Standard Architecture

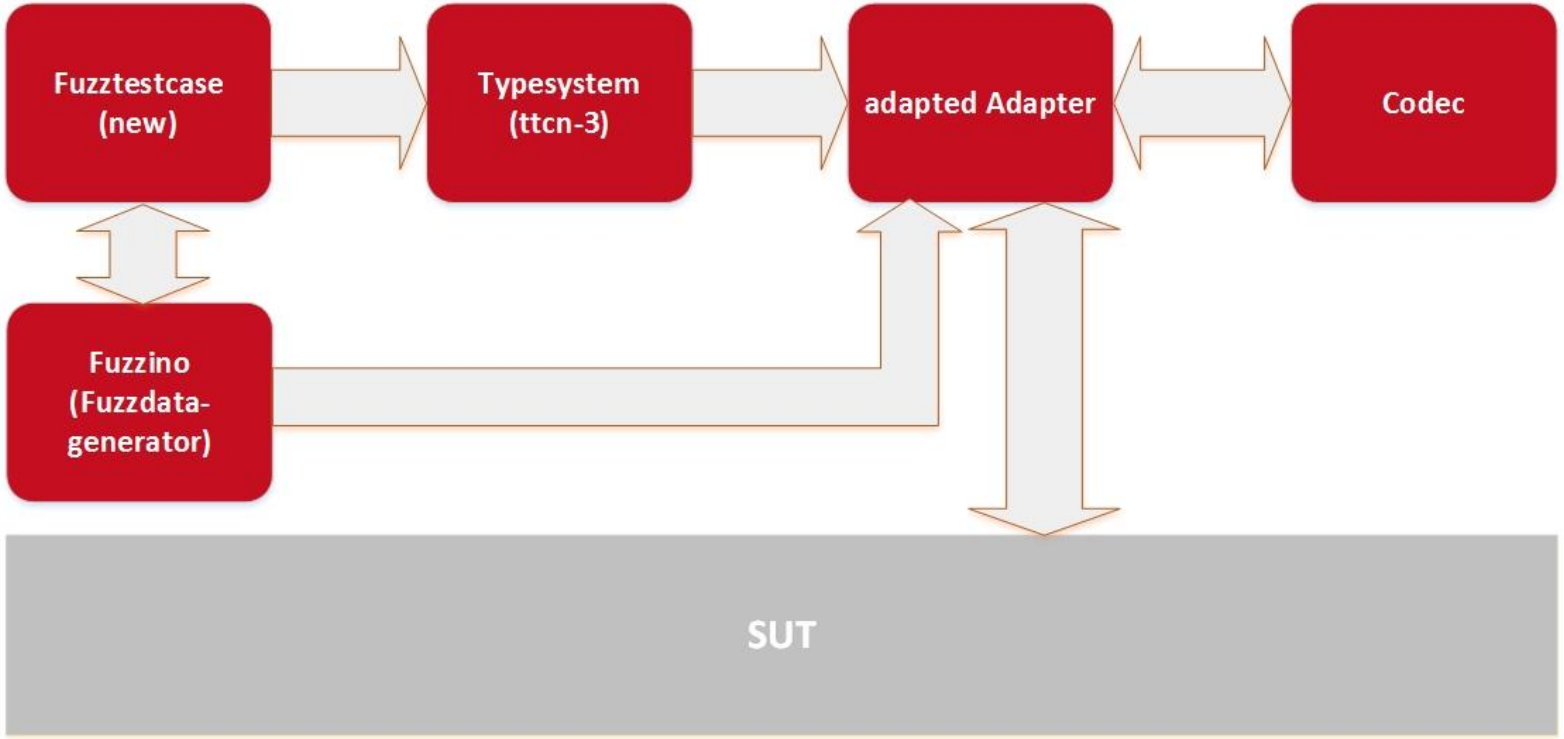
- Example test system for HL7 is developed in TTCN-3
- TTWorkbench by Spirent is used as tool



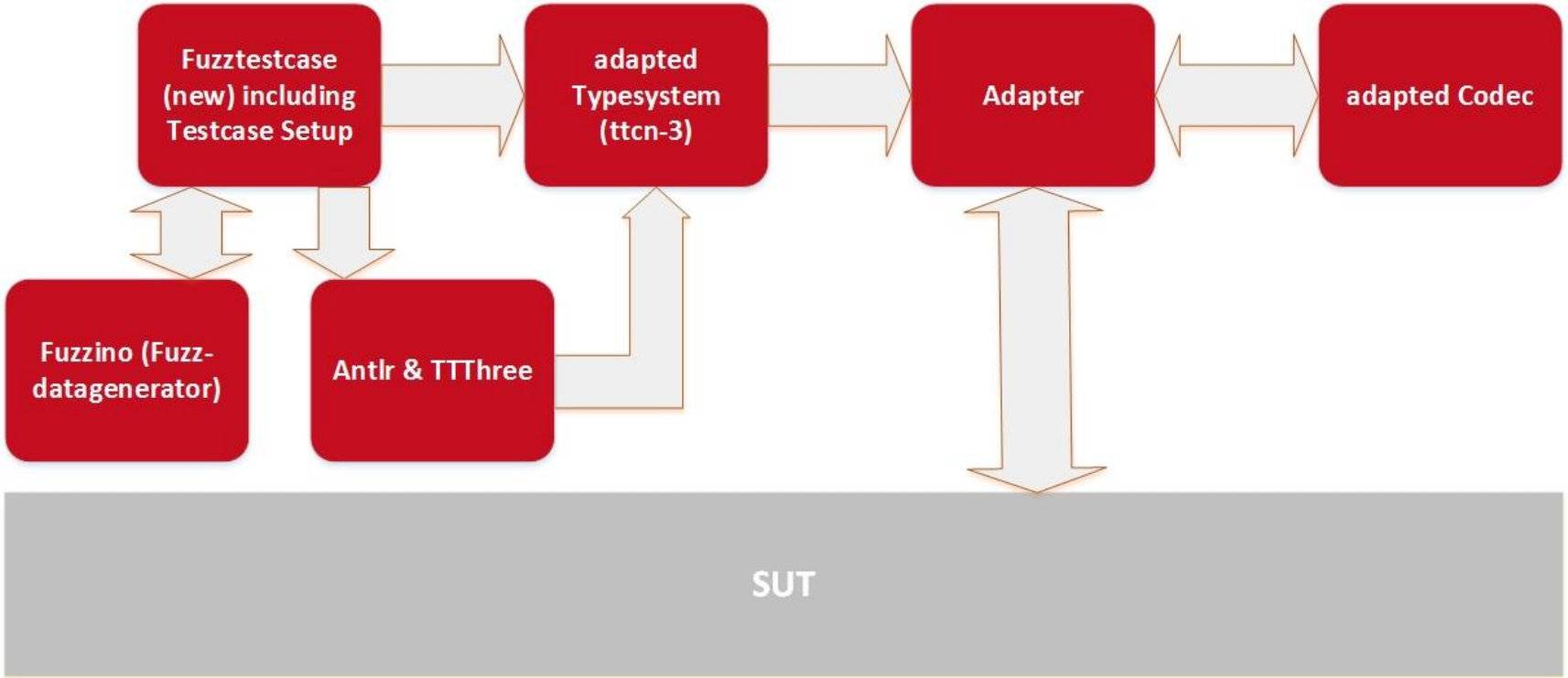
Tecnical Realisation 1



Technical Realisation 1



Tecnical Realisation 2

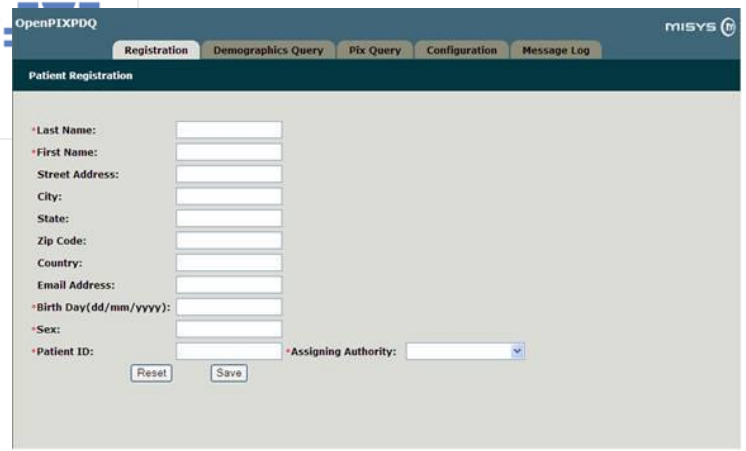


DEMO

1. HL7 conformance test case
2. HL7 fuzz test case
3. setup test case (adaption of type system)
4. HL7 fuzz test case

Case Study

- 2 SUTs:
- 4 different testcase
- 17 heuristics
- 540.000 executed fuzz test cases



Case Study

- Crash
- No answer of SUT
- inconsistent database
- memory consumption

Finding	SUT Initiate	SUT Open PIX PDQ
crash	heuristic „invalid string“, area datafuzzing	-
no answer	-	heuristic „remove mandatory segment“, area messagefuzzing heuristic „invalid string“, area Datafuzzing
unexpected message from SUT	heuristic „invalid string“, area structurfuzzing (HD)	heuristic „invalid string“, area structurfuzzing (MSG)
inconsistent database	-	heuristic „29. February“, area datafuzzing and other heuristics for field TS
memory consumption	-	heuristic „29. February“, area datafuzzing

Thank you for your attention

Fraunhofer FOKUS