A Fuzzing-Based Test-Creation Approach for Evaluating Digital TV Receivers via Transport Streams

Fabricio Izumi, Eddie Filho, Lucas Cordeiro, Orlewilson Maia,
Romulo Fabricio, **Bruno Farias**, Aguinaldo Silva

bruno.farias@manchester.ac.uk
University of Manchester

29th May 2024

Overview

Challenges on Digital TV systems

Misconfigured headend **equipment**

Incorrect data structures and protocols formats

Receiver malfunctions and field problems caused by incorrect information in Transport Streams

Proposed approach

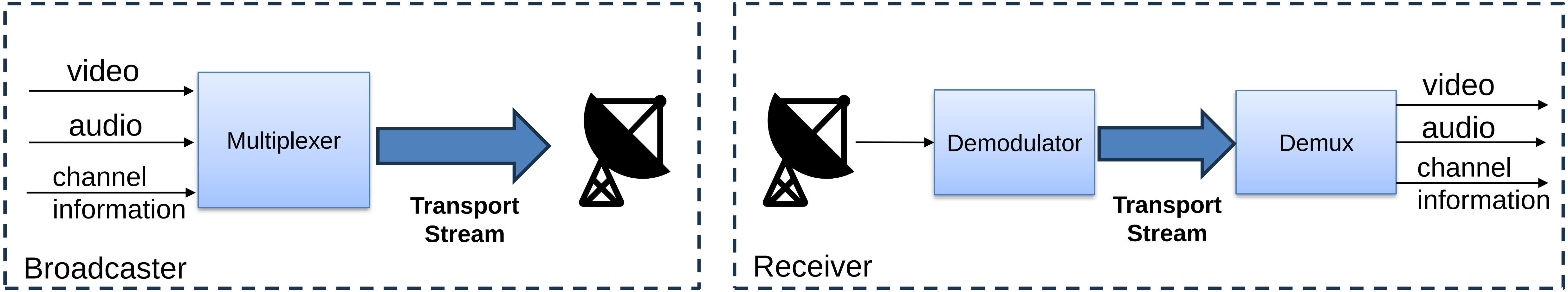
Robustness evaluation using **grammar-based guided fuzzing**

Goals

Test receivers under unforeseen conditions

Enhance operational reliability and robustness in commercial DTV platforms

Terrestrial DTV Systems Architecture



Broadcaster

video

audio

channel information

Multiplexer

Transport Stream

Receiver

Demodulator

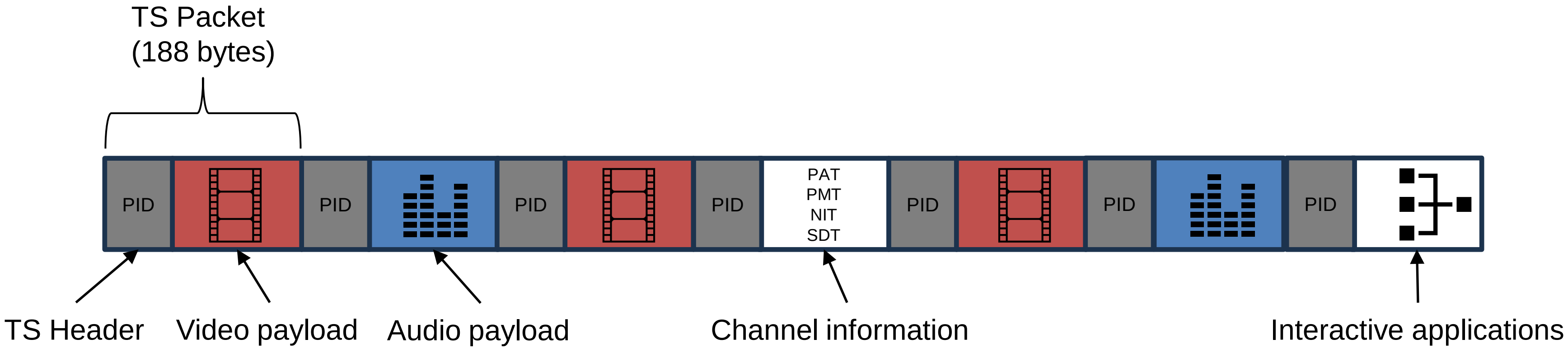
Transport Stream

Demux

video

audio

channel information



TS Packet (188 bytes)

PID

PAT PMT NIT SDT

TS Header

Video payload

Audio payload

Channel information

Interactive applications

Field-problems analysis

Error Sources

- Media-related encoding data
  - Wrong size information in **H.264 packet headers**
  - Wrong audio format announced in tables
- System-related
  - **Wrong clock references** affecting medias synchronization
  - Intervals between tables (configuration) data larger than recommended
- Data-related
  - Conditional access information transmitted without protection
  - Non-existent services listing
  - Inconsistent encoding of audio and video streams

Symptons of failing receivers

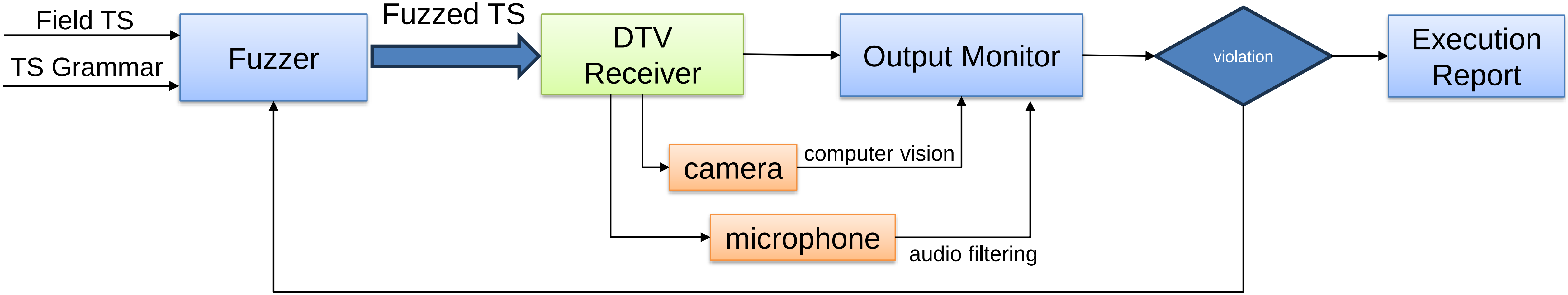
- Video freezing or flickering
- Frame skipping

Image source: Adobe (https://t.ly/6LtUf)

- Abscence of audio

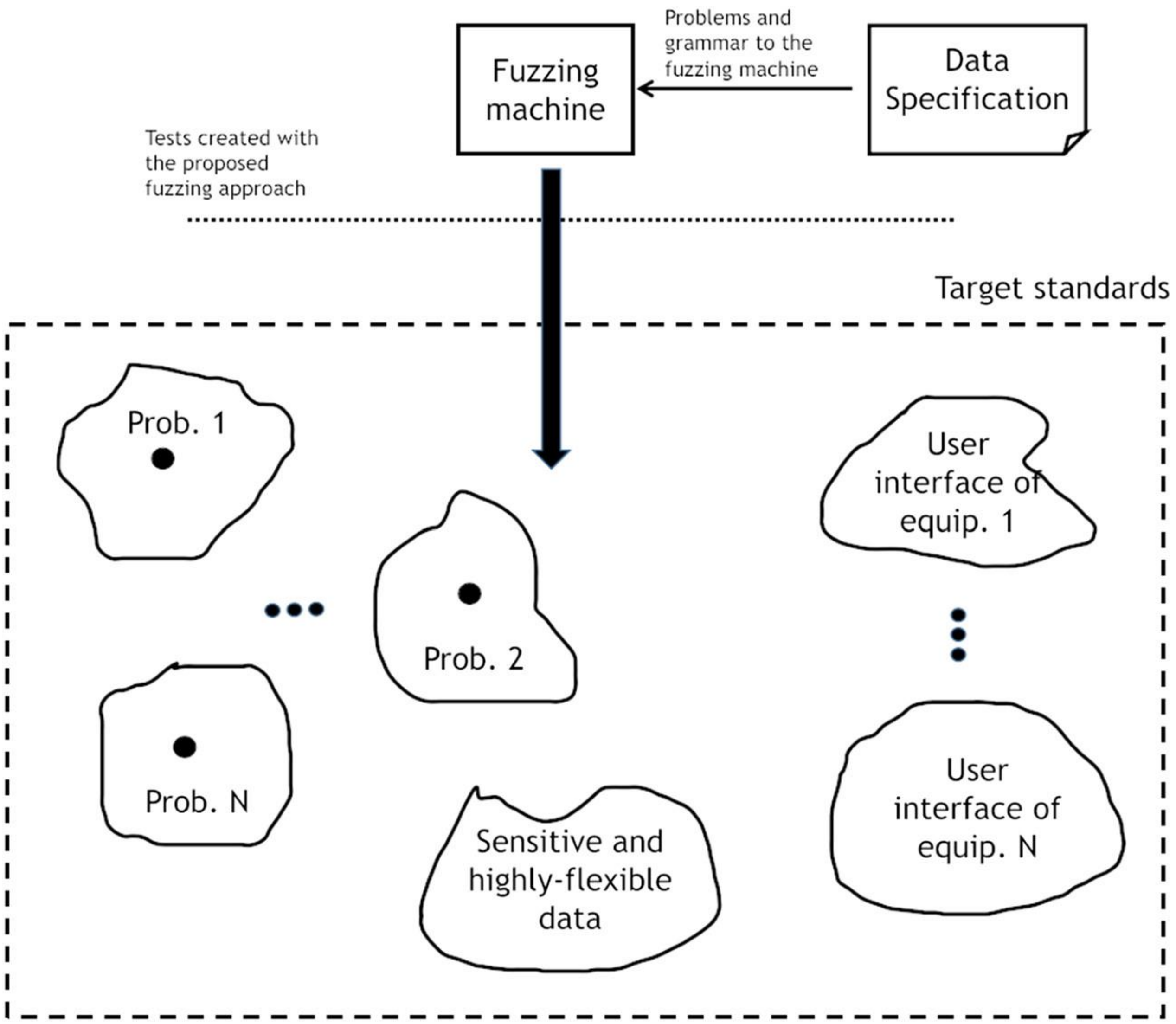
MANCHESTER
1824
The University of Manchester

DTV-oriented smart fuzzer



- Generation-based: Inputs from MPEG-2 TS specification
- Mutation-based: Variations from field problems and execution results
- Execution monitoring through video and audio outputs

Fuzzing DTV Receivers


Fuzzing machine
Problems and grammar to the fuzzing machine
Data Specification
Tests created with the proposed fuzzing approach
Target standards
Prob. 1
Prob. 2
Prob. N
Sensitive and highly-flexible data
User interface of equip. 1
User interface of equip. N

Grammar based on MPEG-2 TS format

```
program_number = ‘original_network_id’,
service_type,
service_number;
service_type = ‘01’|‘10’|‘11’;
service_number = ‘001’ |‘010’|‘011’|‘100’
                  |‘101’|‘110’|‘111’;
```

Grammar for *program_number* field

```
component_descriptor = ‘01010000’,
   ‘00000110’,
   stream_content_ext,
   stream_content_and_component_type,
   component_tag,
   ISO_639_language_code;
stream_content_ext = 4 ∗ binary_digit;
stream_content_and_component_type = ‘000100000000’
| (‘0000’, component_type);
component_type = 8 ∗ binary_digit;
binary_digit = ‘0’|‘1’
```

Grammar for *component_descriptor* field

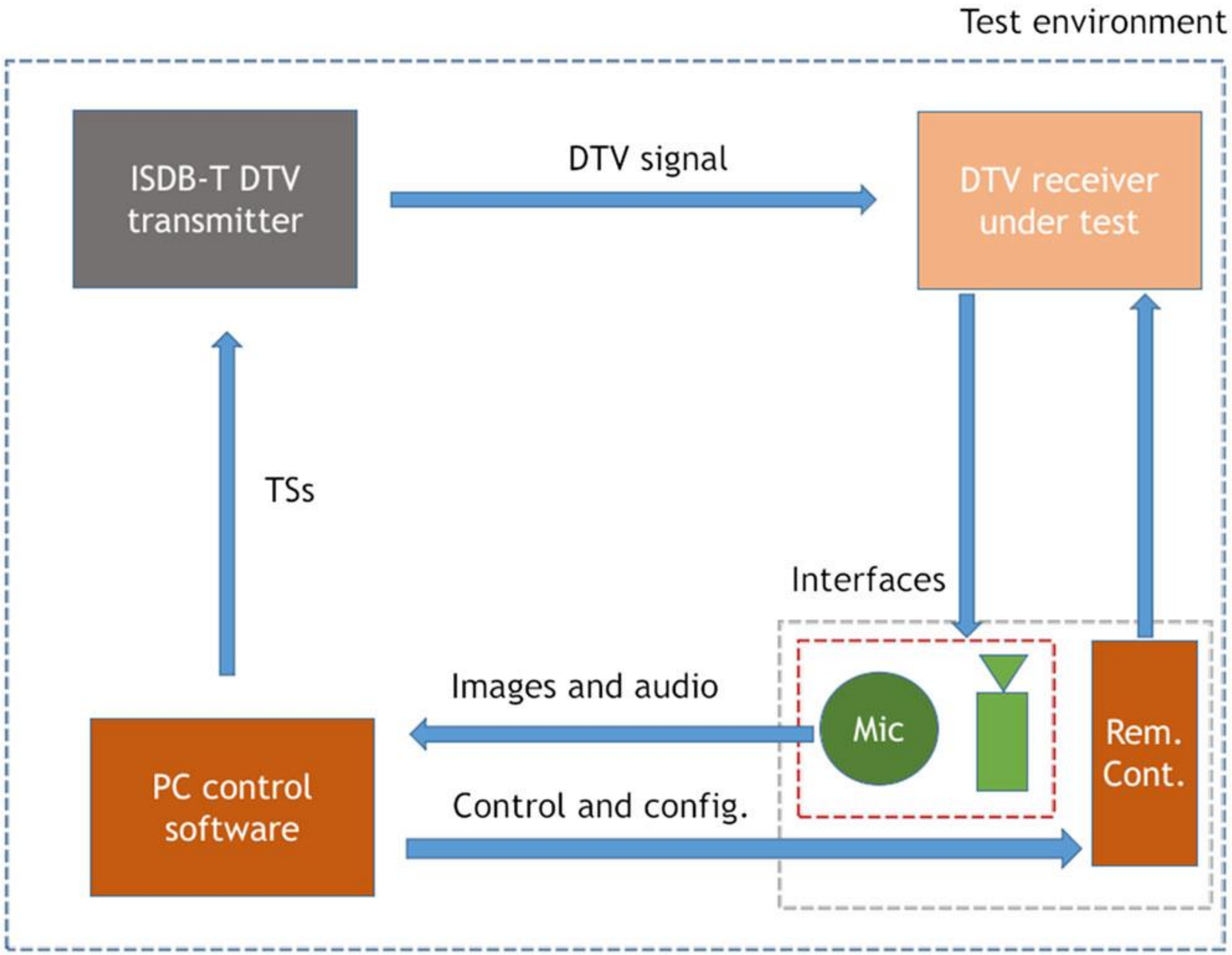
Fuzzing tool

Transport Stream generation

- FFMPEG: Audio and video
- OpenCaster library
  - Channel configuration from text files
  - TS multiplexing

Remote control module

- USB Infrared transmitter
- Linux Infrared Remote Control (LIRC)



MANCHESTER 1824
The University of Manchester

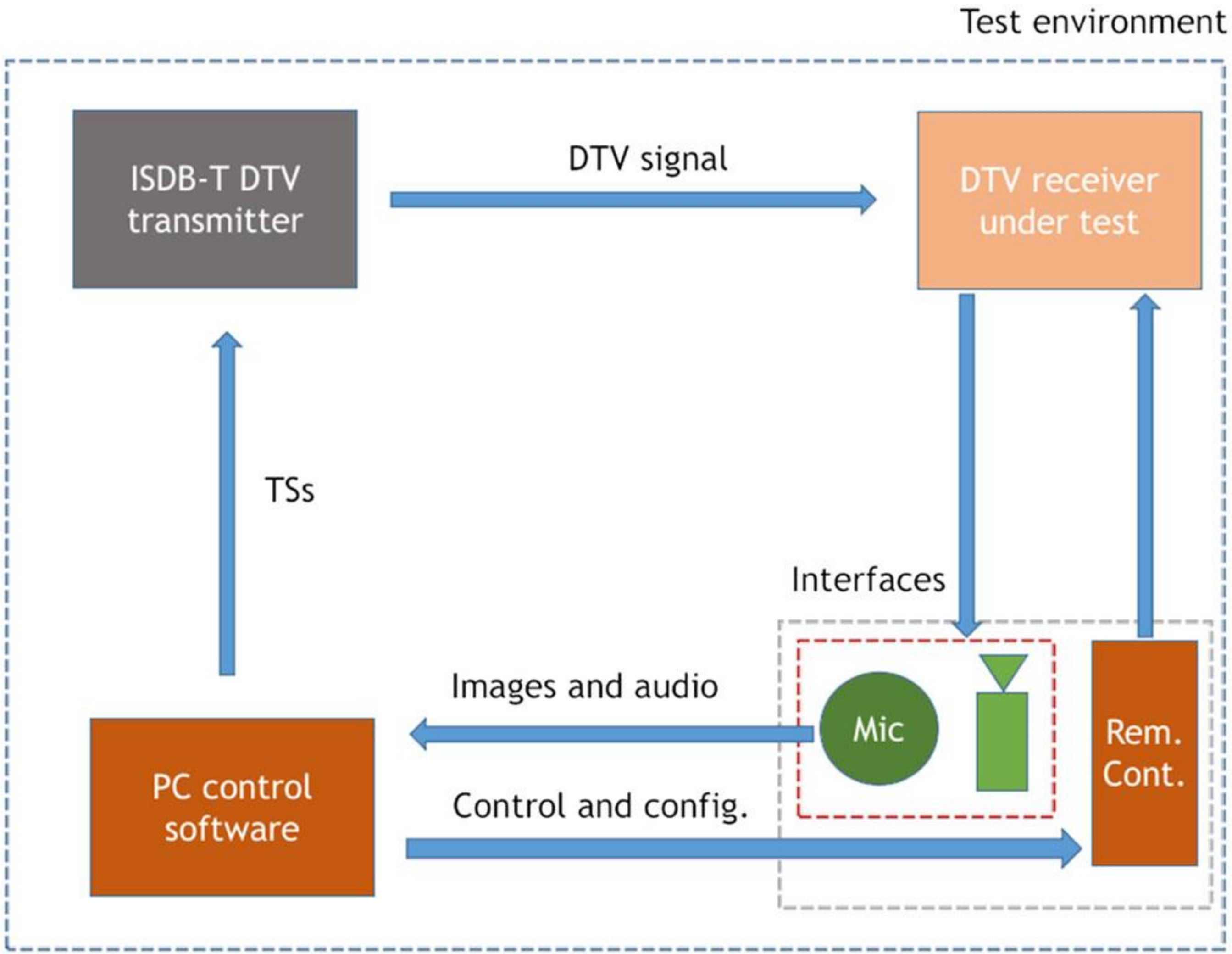
Fuzzing tool

<u>Image processing module</u>

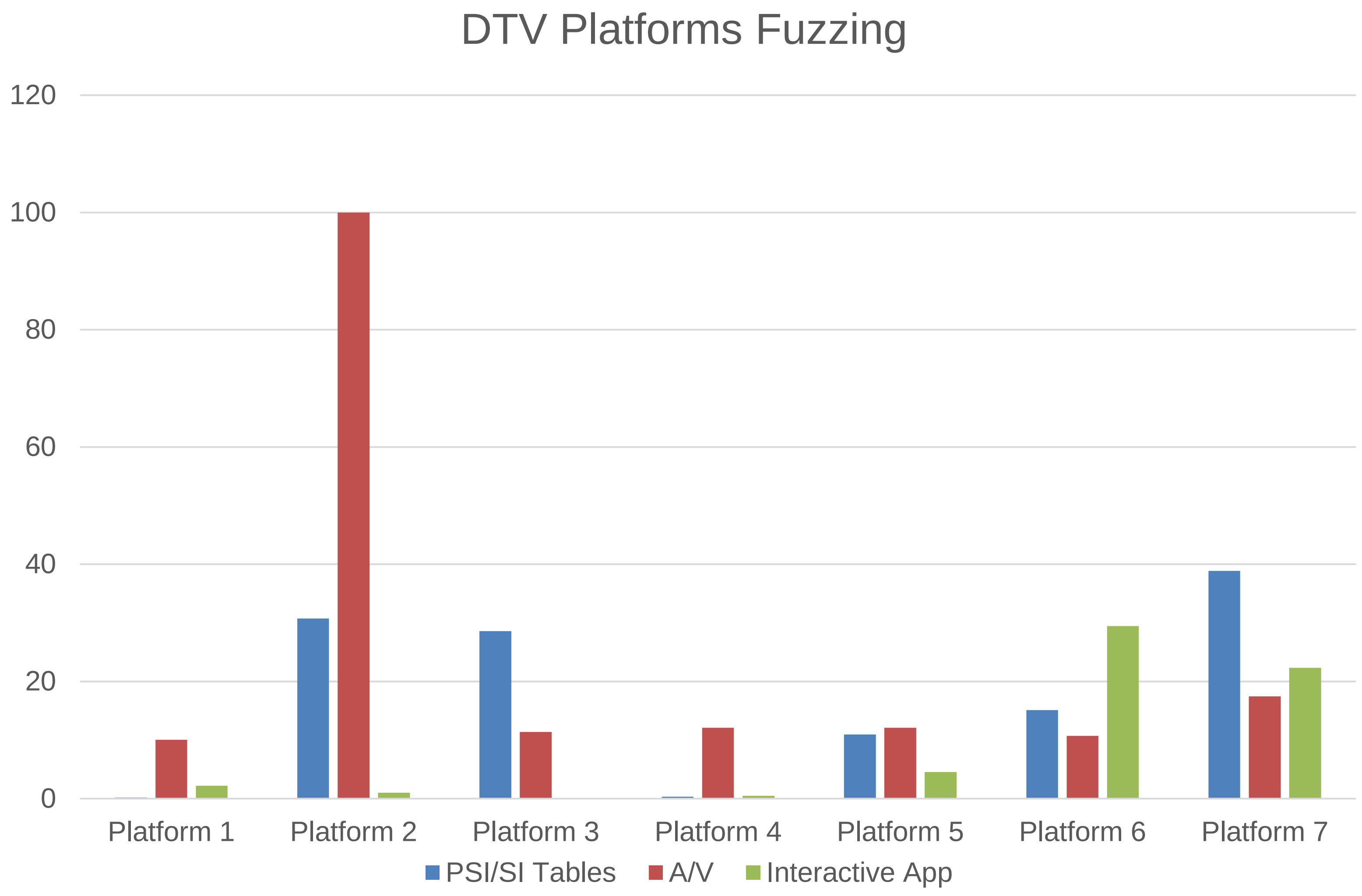
- Screen detection algorithm
- Freezing and flickering detection
  - Histograms
  - Structural Similarity Index (SSIM)
  - OpenCV framework

<u>Audio analysis module</u>

- Amplitude verification
- ALSA library



Experimental Results



Evaluations on 7 commercial platforms

Most issues are concentrated in PSI/SI and A/V

Bug fixes in DTV receiver software impacting millions of users

Enhancements to devices and transmission setups

Conclusion and Future Work

- Our work presents a **collection of real field problems** identified in DTV networks and outlines **a scheme for non-compliance insertion** that performs **grammar-based guided fuzzing**.

- The experimental results showed that our methodology is **effective on finding real problems** on comercial Digital TV platforms.

- In terms of fuzzing technique, we envision future work on applying machine learning algorithms that provide adaptability toward known fragile parts.

MANCHESTER 1824
The University of Manchester

TPV

UFAM

A Fuzzing-Based Test Creation Approach for Evaluating Digital TV Receivers via Transport Streams

Bruno Farias

bruno.farias@manchester.ac.uk
University of Manchester

29th May 2024