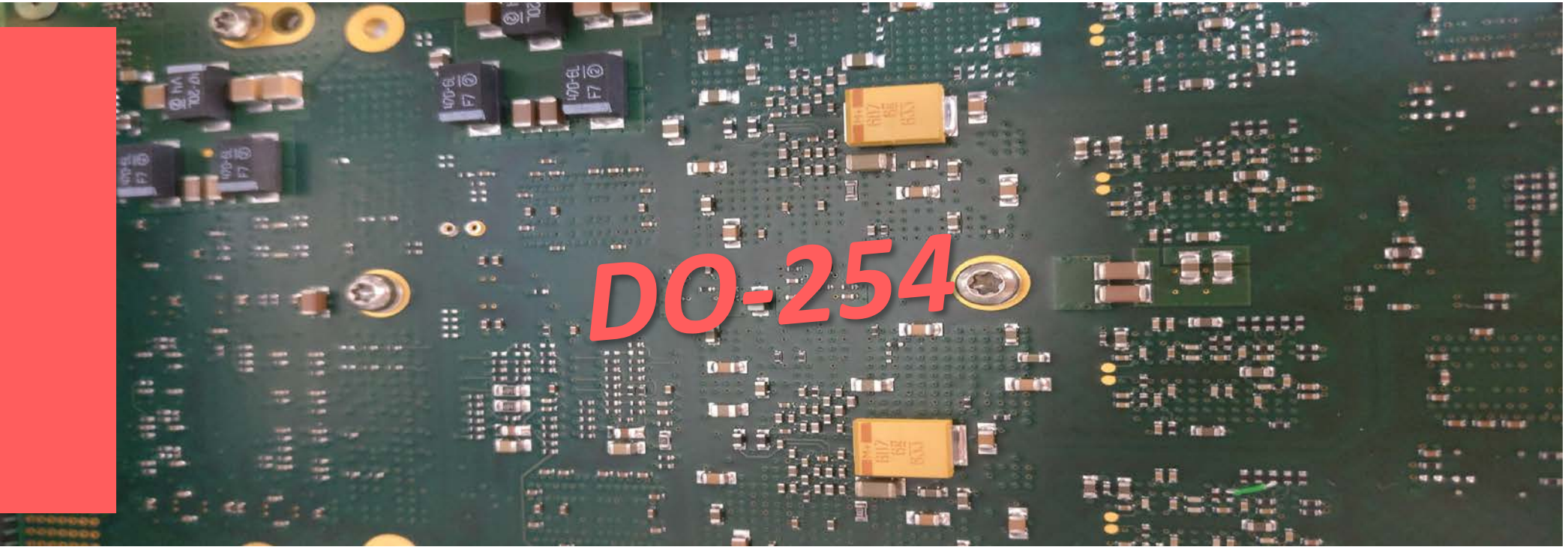
Fachhochschule Nordwestschweiz
Hochschule für Technik

FPGA-Developement for safety critical application

Christoph Meyer & Rafael Reimann

Institute of Microelectronics



Intro

- Safety critical devices for avionics
  - Why DO-254?
  - What is DO-254?
- Development Process
  - Requirements Capture
  - Design
  - Verification
  - Validation
- Costs & Benefits

We want safe planes

No dangerous situations

No crashes

How can we be sure a plane is safe?

How can we guarantee a plane is safe?

DO-254

DO-254 applies for development of complex components

DO-254 does not define how to implement

DO-254 defines the development process

DO-254 defines Teams

DO-254 defines Documents

DO-254 defines Reviews

DO-254 defines Interactions with Authorities

DO-254 makes development transparent

DO-254 helps to avoid errors

Nothing can be 100% safe

No device has Zero failure rate

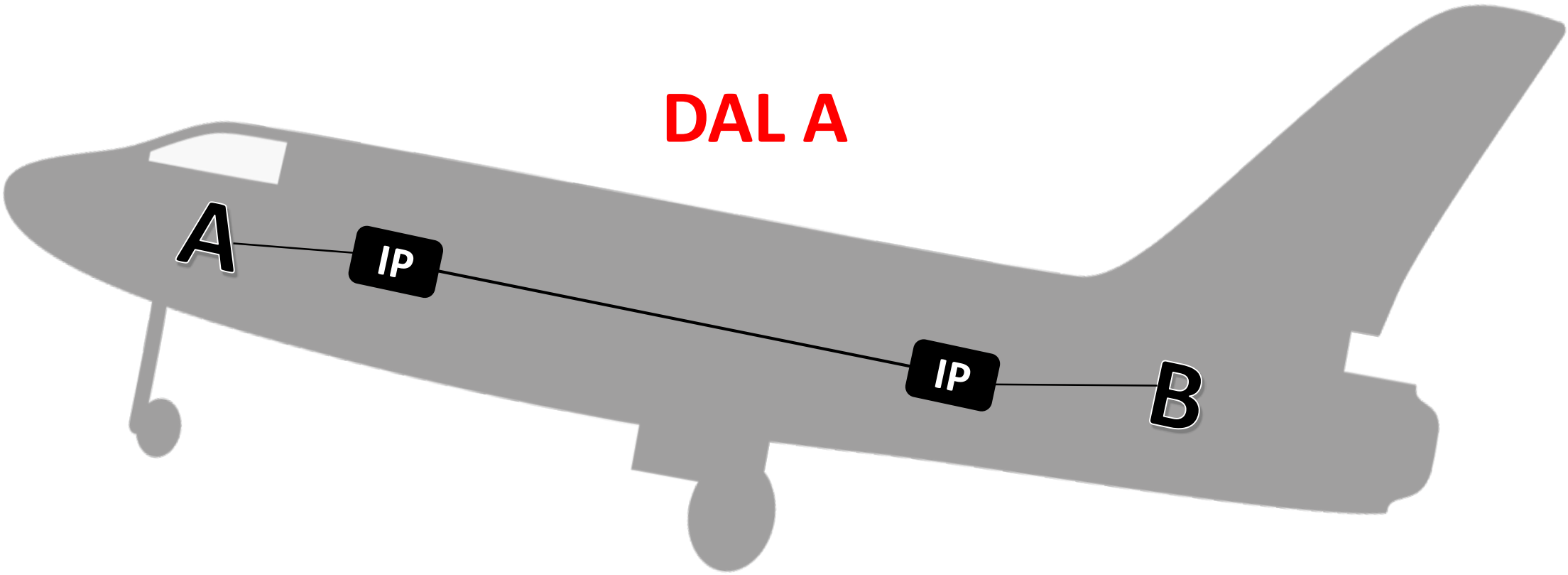
No Development is 100% free of errors

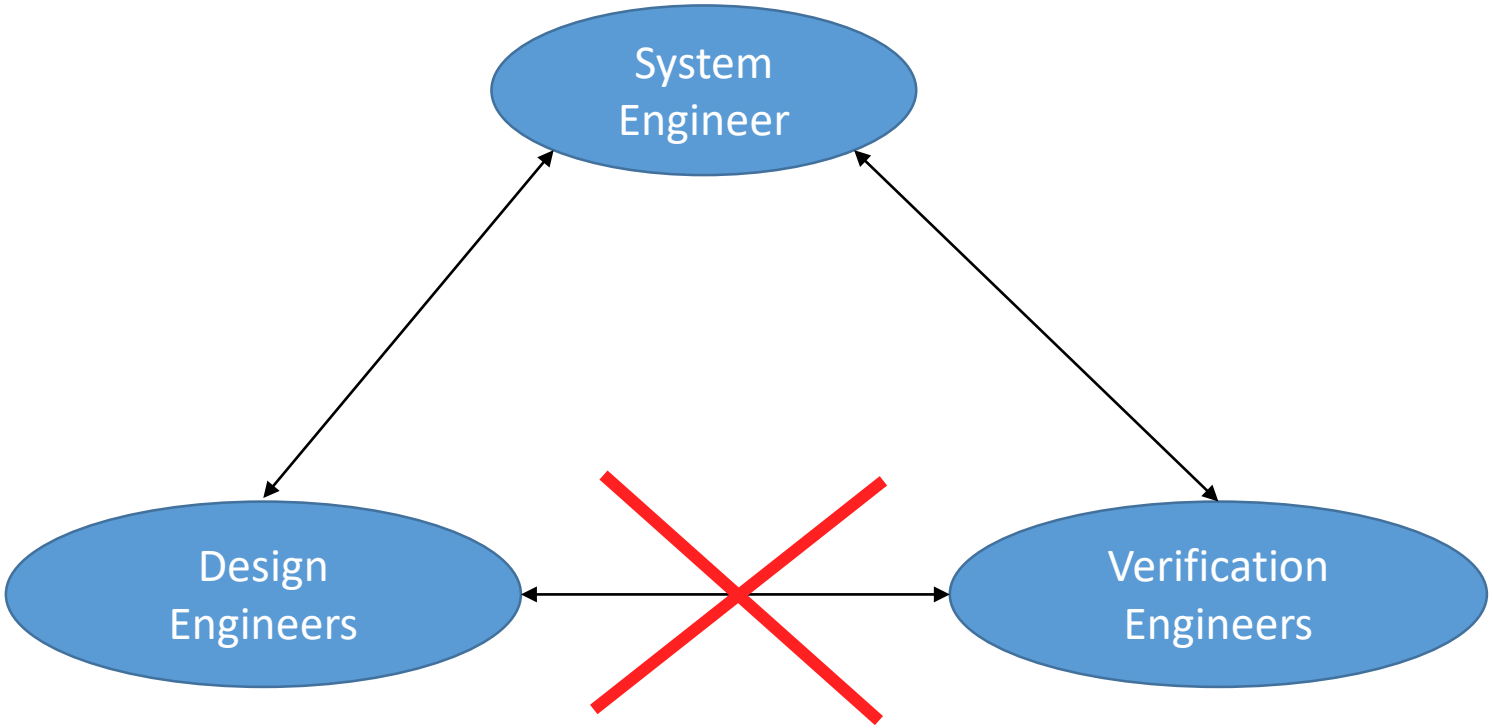
Not all possibilities can be forseen and tested

What failure rate is acceptable?

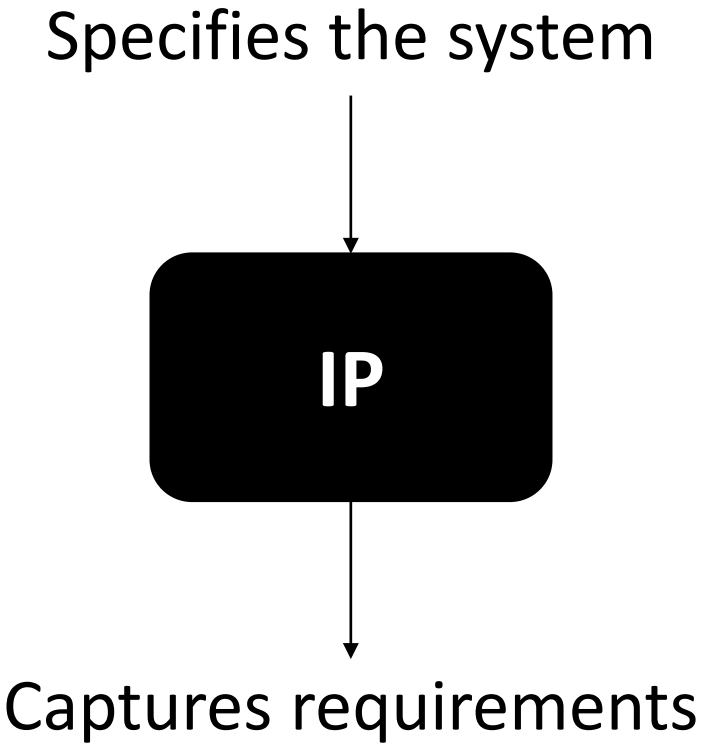
Design Assurance Level (DAL)	Description	Target System Failure Rate	Example System
Level A (Catastrophic)	Failure causes crash, deaths	$< 1 \times 10^{-9}$	Flight controls
Level B (Hazardous)	Failure may cause crash, deaths	$< 1 \times 10^{-7}$	Braking systems
Level C (Major)	Failure may cause stress, injuries	$< 1 \times 10^{-5}$	Backup systems
Level D (Minor)	Failure may cause inconvenience	No safety metric	Ground navigation systems
Level E (No Effect)	No safety effect on passeger/crew	No safety metric	Passenger entertainment

Our Project




System
Engineer
Design
Engineers
Verification
Engineers

System Engineer



The Requirement should be uniquely identified

The Requirement should be understandable

The Requirement should be testable

~~The IP interface shall be easy to address~~

~~Wrong messages shall be discarded~~

After the system reset is applied, the IP shall set the FIFO “X” to empty.

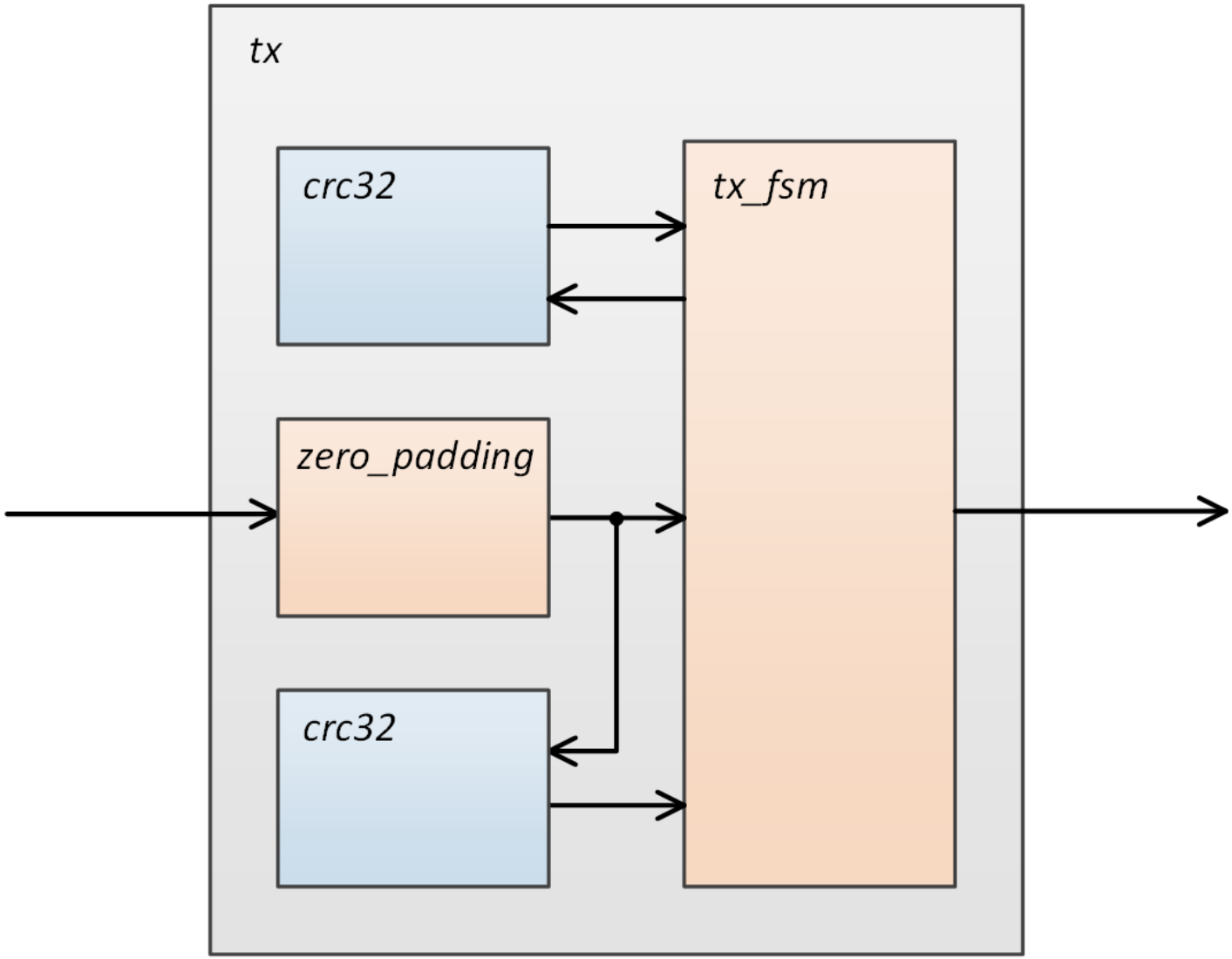
After the system reset is applied, the IP shall set the FIFO “X” to empty, if its value is read, then the IP shall return the value 0xFFFFFFFF.

~~The System shall complete a short Ethernet frame by byte padding.~~

The System shall complete the Ethernet frame by byte padding when the message to send is shorter than 100 bytes.

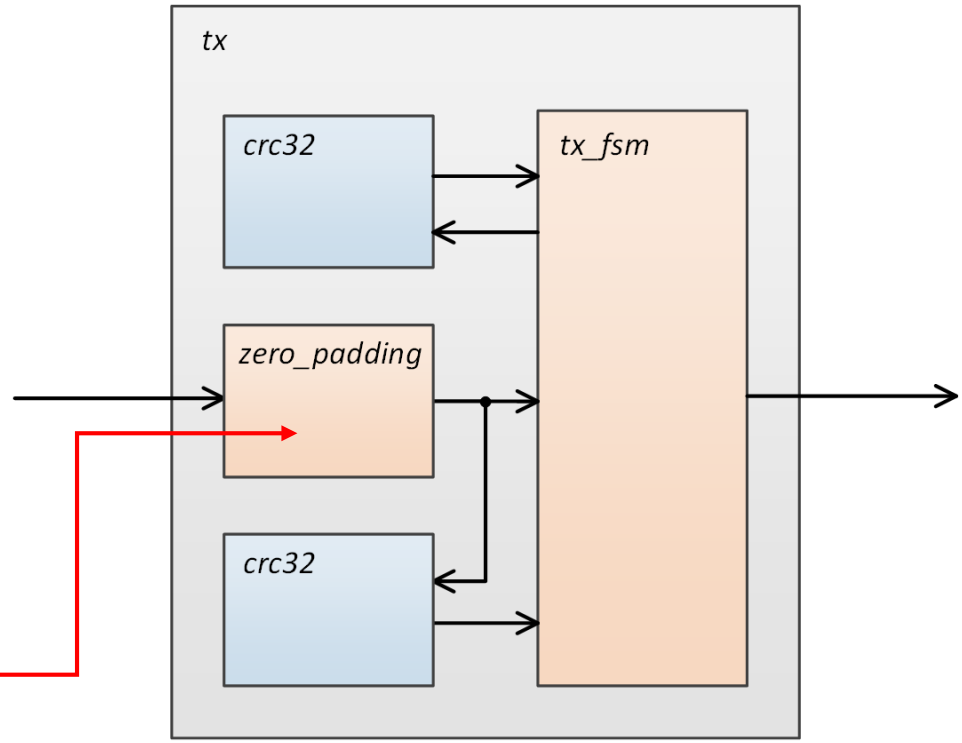
Design Engineer

Concept for the Design


tx
crc32
tx_fsm
zero_padding
crc32

Main Functions:

- Forward byte stream
- Check frame length
- Extend byte stream if needed



Design Item

DI_012_b:

The block zero_padding is extending the byte stream for frames smaller than 100 bytes by keeping the valid signal high and setting the data signal to zero until the frame reaches 100 bytes.

Covers Req_002_a

Req_002_a:

The System shall complete the Ethernet frame by byte padding when the message to send is shorter than 100 bytes.

Design Items cover Requirements

Design Items are covered in the Code

Coverage 100 %

```
-- make sure the data line is all zeros if no valid data is being sent
-- Implements DI_012_b
tx_mac_data_p   <=  tx_mac_data WHEN tx_mac_valid = '1'
                                ELSE (OTHERS => '0');
```

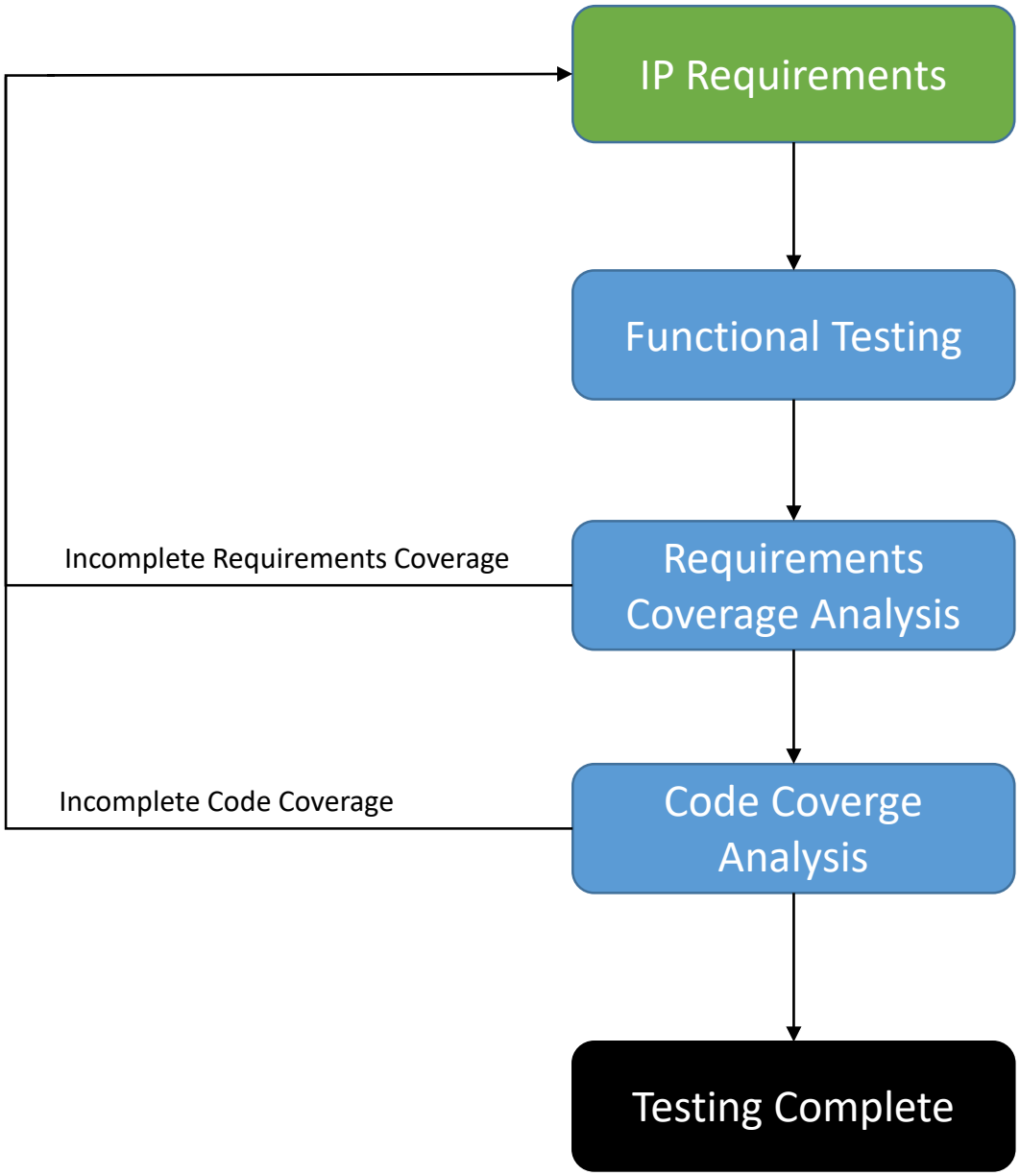
DI_012_b:

The block zero_padding is extending the byte stream for frames smaller than 100 bytes by keeping the valid signal high and setting the data signal to zero until the frame reaches 100 bytes.

Covers Req_002_a

Verification Engineer

Verification ensures that the device performs the intended function as specified by the requirements


IP Requirements
Functional Testing
Incomplete Requirements Coverage
Requirements Coverage Analysis
Incomplete Code Coverage
Code Coverge Analysis
Testing Complete

For each Requirement there is at least one Test Procedure

TC_133_b:

Sending a message that is shorter than 100 bytes and sending a message that is longer than 100 bytes.

Tests Req_002_a

Req_002_a:

The System shall complete the Ethernet frame by byte padding when the message to send is shorter than 100 bytes.

TC_133_b

Sending a message that is shorter than 100 bytes and sending a message that is longer than 100 bytes.

Req_002a

Step 0	Send a message with 45 bytes	Expecting a message with byte padding
Step 1	Send a message with 99 bytes	Expecting a message with byte padding
Step 2	Send a message with 100 bytes	Expecting a message without byte padding
Step 3	Send a message with 125 bytes	Expecting a message without byte padding

Validation

Validation ensures that the requirements are correct

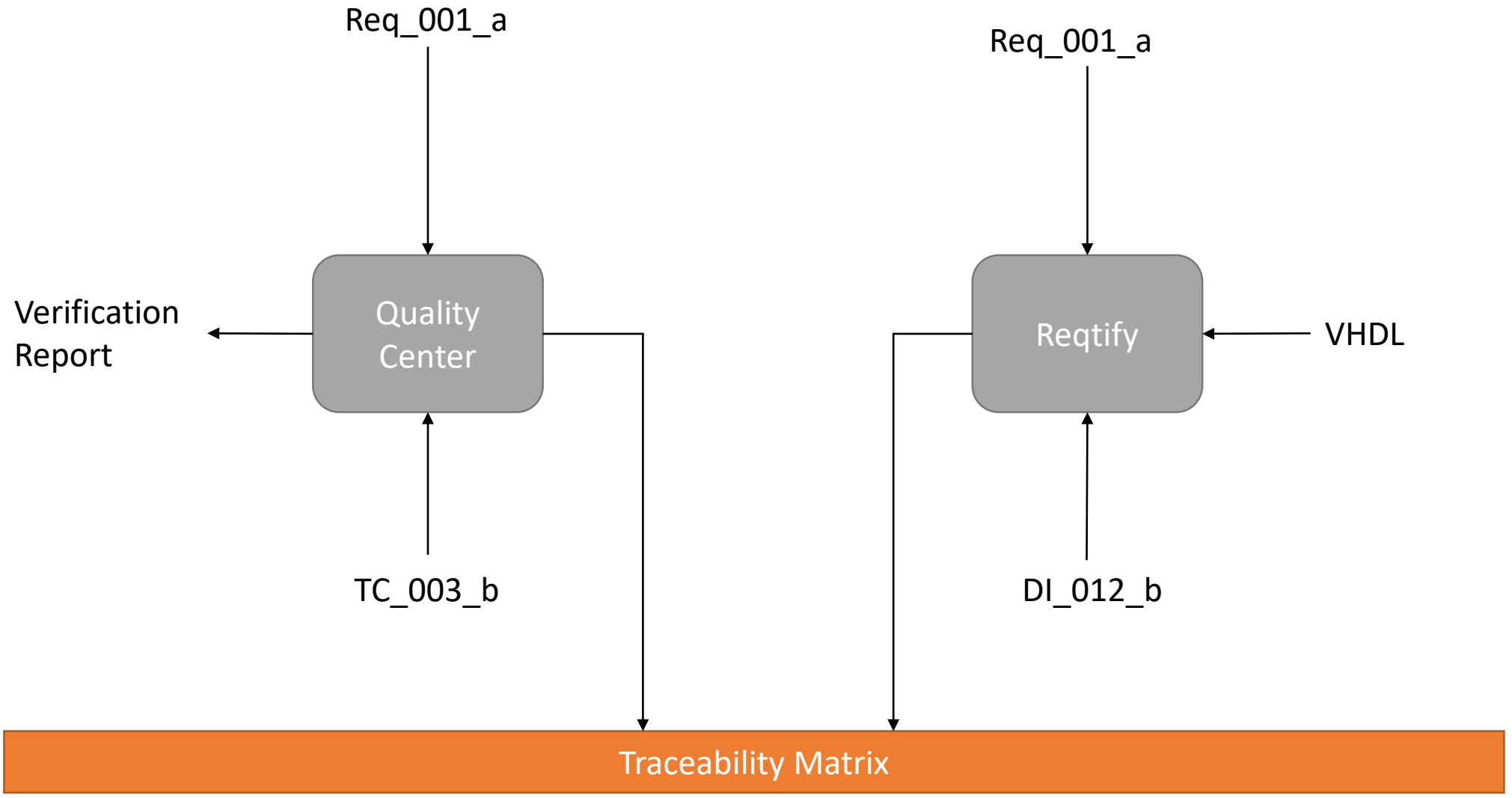
Validation ensures that the requirements are complete

Validation ensures that the requirements are verifiable

Requirements	Design Items
Req_001_a	DI_012_b DI_001_c
Req_002_a	DI_022_a

Requirements	Test Cases
Req_001_a	TC_003_b TC_017_a
Req_002_a	TC_133_c
Req_003_a	TC_133_c TC_051_a TC_52_b

Tools


Req_001_a
Req_001_a
Verification
Report
Quality
Center
Reqtify
VHDL
TC_003_b
DI_012_b
Traceability Matrix

DAL-A

How did we reach a failure rate of 10^{-9}

Less than 1 failure in 10^9 hours

Less than 1 failure in 10^5 years

Single Event Upset due to Neutron Flux

Depends on Location

Depends on Altitude

Depends on Device

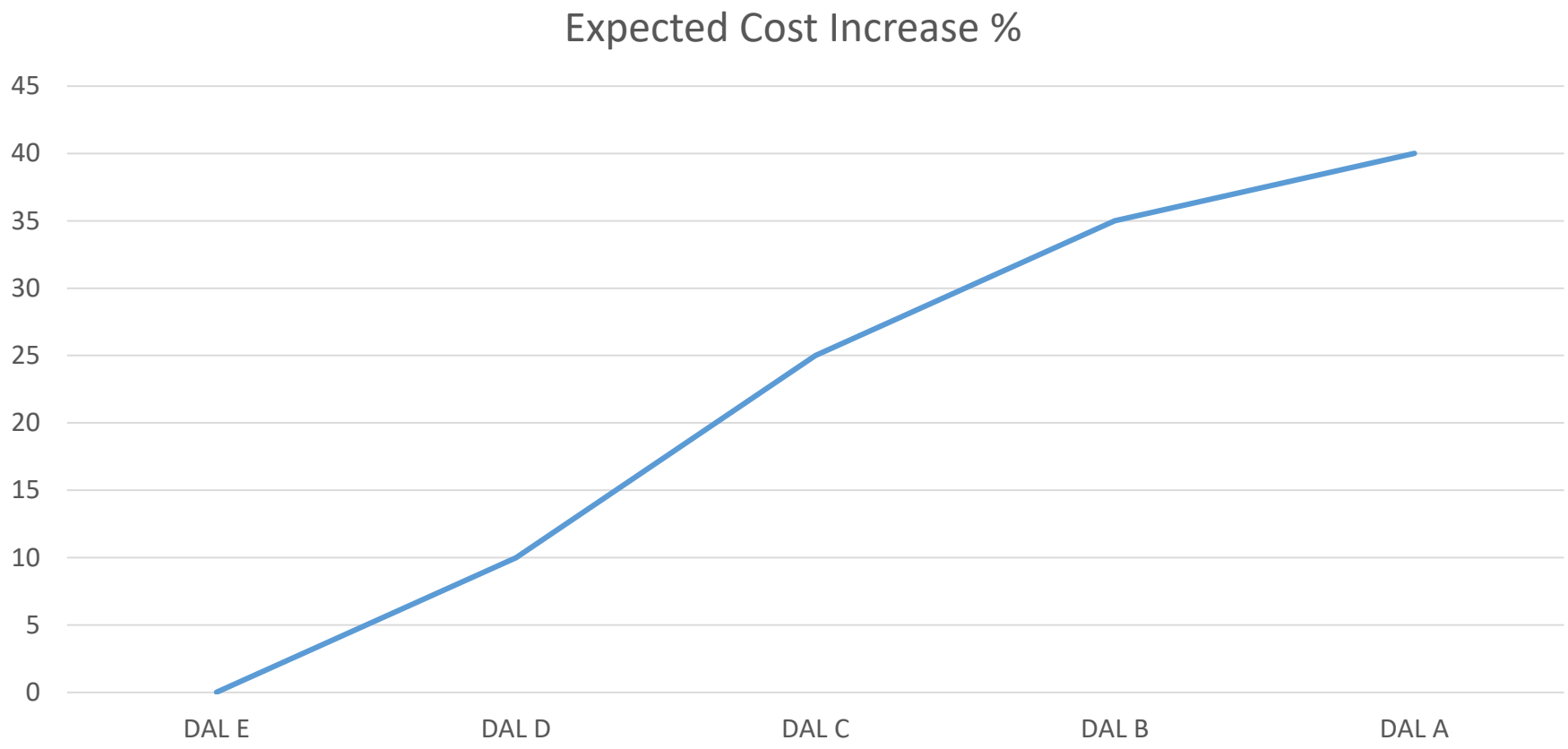
Depends on Technology

Depends on Sun Activity

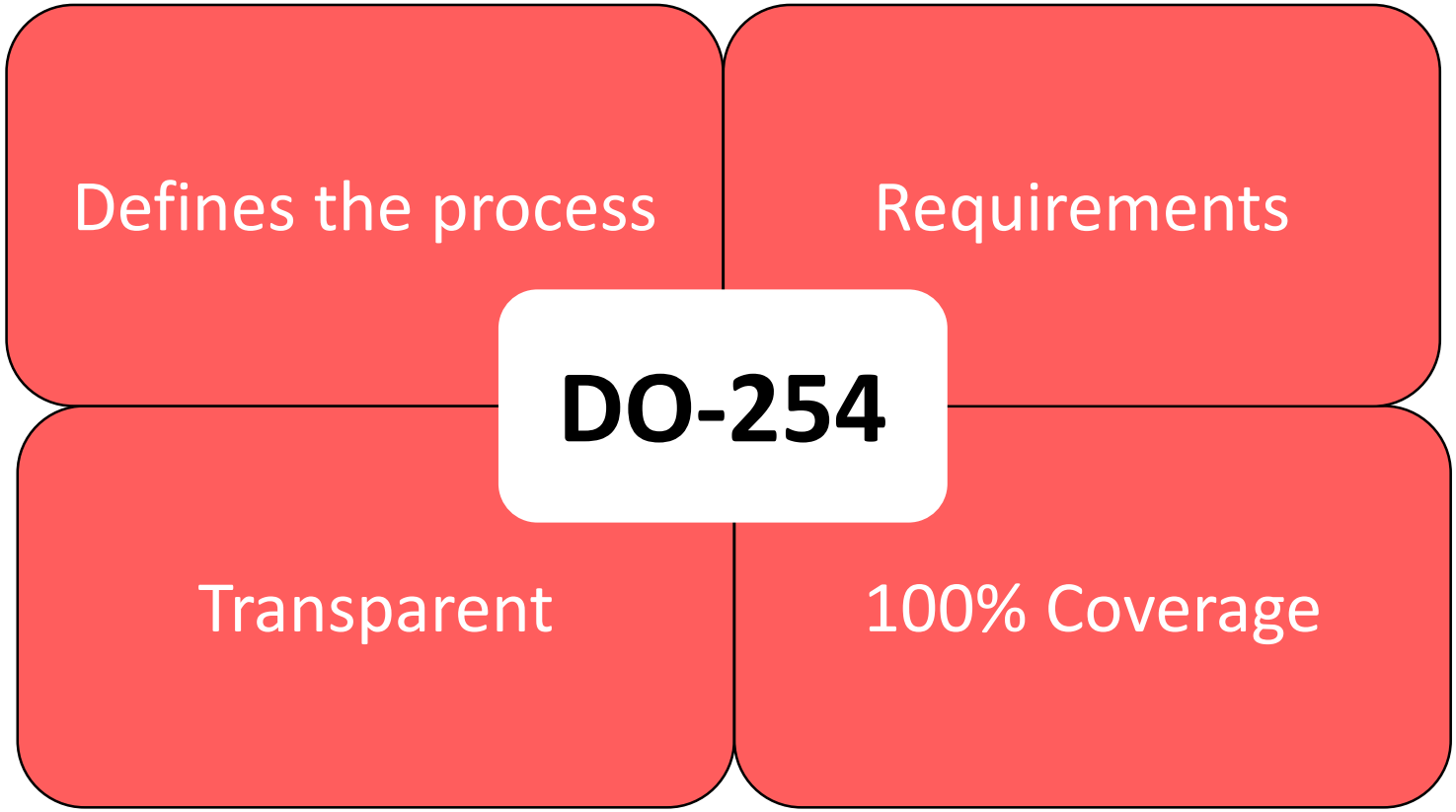
Worst Case for one Flip-Flop: $0.72 * 10^{-9}$

Error Detection

Error Correction



Industry average: 75…150%


Defines the process
Requirements
DO-254
Transparent
100% Coverage

Fachhochschule Nordwestschweiz
Hochschule für Technik

Thank you

Christoph Meyer & Rafael Reimann

Institute of Microelectronics