KU LEUVEN

Trusted IoT - User group meeting
April 17th, 2023

Nele Mentens, Masoom Rabbani, Jo Vliegen, and Sem Kirkels

WP3: Platform-specific security solutions

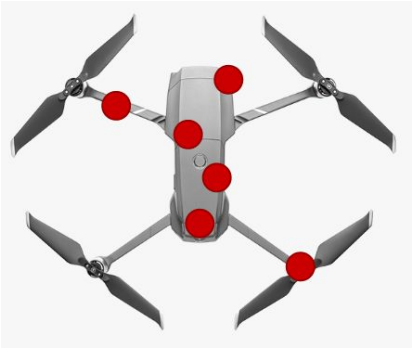
T 3.3 (KU Leuven) **Multi-Core RISC-V** platforms. RISC-V is an open standard that implements the principle of a Reduced Instruction Set Computer (RISC), which comes down to the actual processor on which a system is running. A RISC-V core can be adjusted and/or extended to better fit the application it is hosting. With the fact that more and more different 'processors' are available comes the need to have some form of interaction. This, however, could pose a threat. As the weakest component could succumb to attackers, it might infect other components as well. **Having multiple cores should have a mechanism that they keep an eye on each other.** A typical approach is to provide some **trusted hardware** to each entity (processor) so they are equipped for overcoming this challenge. Having a reconfigurable processor makes this feasible. The results of the examining and comparing the state-of-the-art techniques and implementations and holding them against the established requirements (as done in WP2) will **set out the lines for a proof-of-concept implementation**. This will then be translated to suit the needs for the target use-case in WP4.

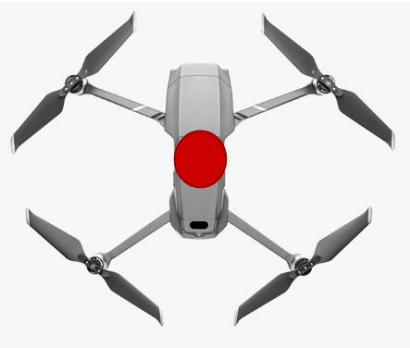
Trusted IoT - WP3 (recap)

Within Trusted IoT - KU Leuven is working on Multi-Core RISC-V platforms

The industrial Use Case will focus on drones, operated by multiple RISC-V cores.

Multiple, isolated microprocessors will be **centralised** on a single **FPGA**



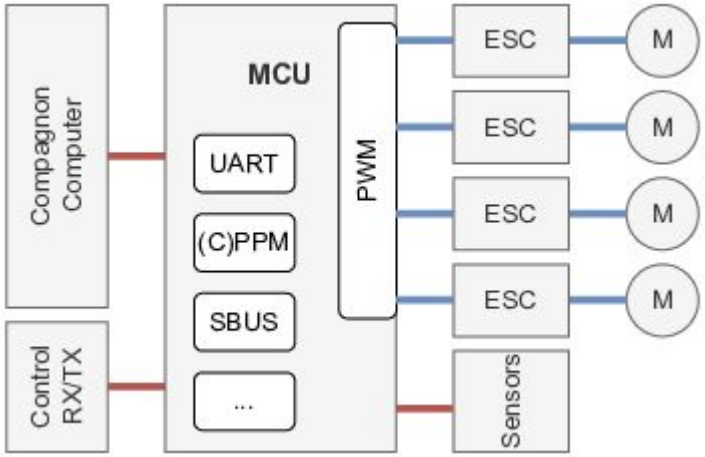


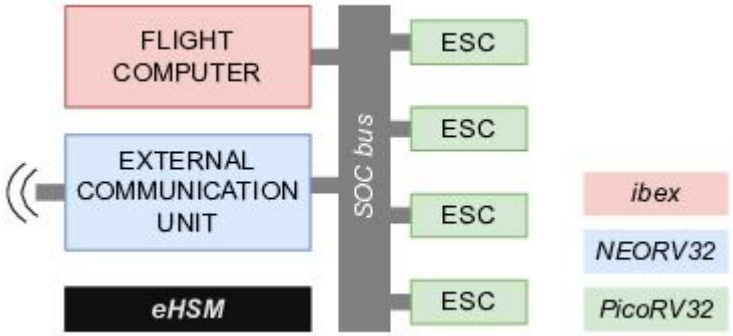
Trusted IoT - WP3

Within Trusted IoT - KU Leuven is working on Multi-Core RISC-V platforms

The industrial Use Case will focus on drones, operated by multiple RISC-V cores.

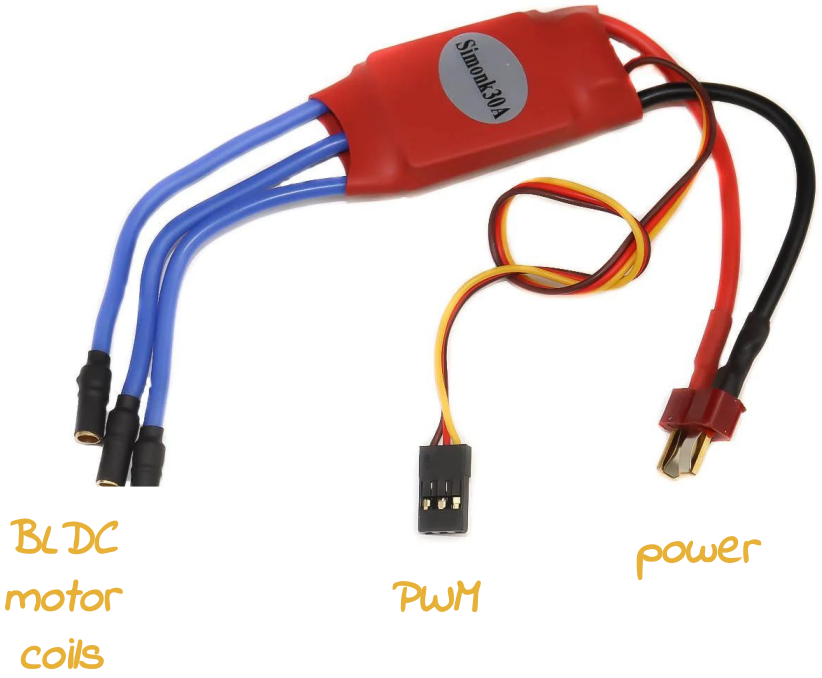
Three different RISC-V implementations will be used





Trusted IoT - WP3

Work on the ESC



There is a processor in the ESC that:

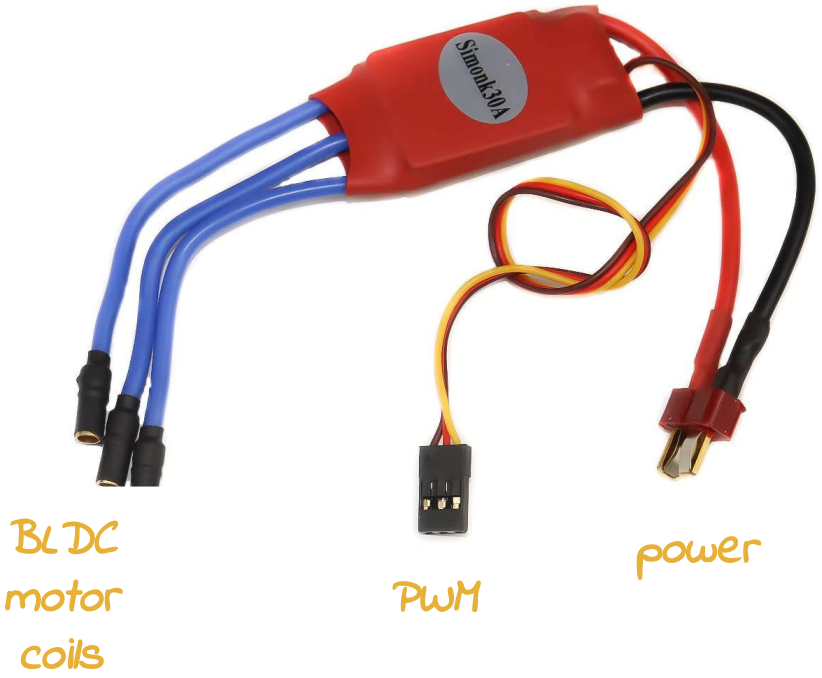
- receives PWM
- transmits coil-steering pattern to the BLDC
- a small **microcontroller** manages

There is "*quite some*" power electronics

We want to get around using the microcontroller

Trusted IoT - WP3

Work on the ESC



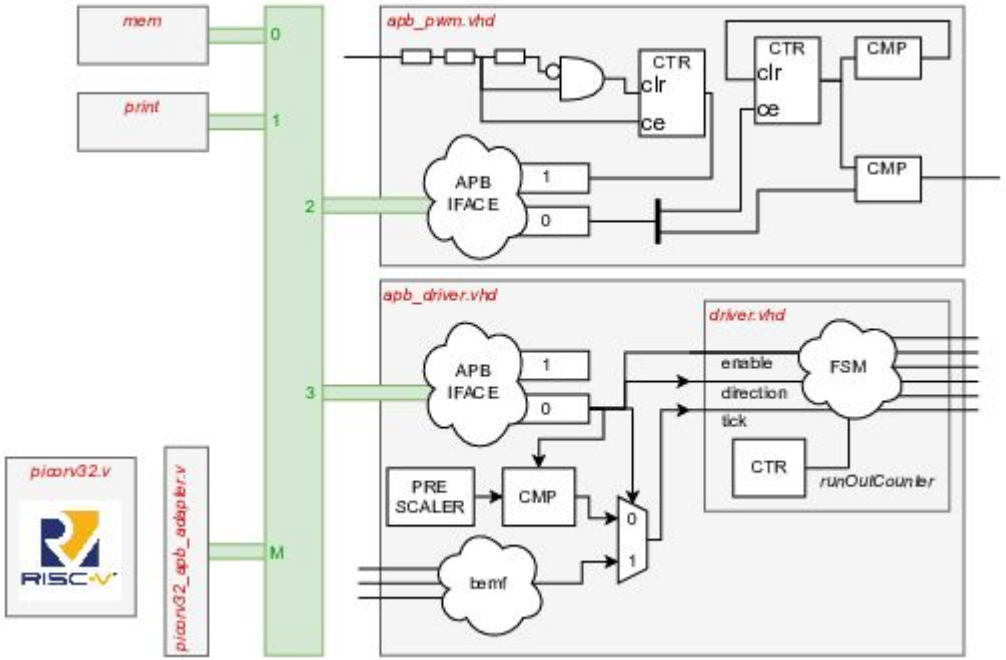
Drone BLDCs are bought

Power electronics has been made

A(n extremely) simple SOC replaces the microcontroller

Trusted IoT - WP3

Work on the ESC



Drone BLDCs are bought

Power electronics has been made

A(n extremely simple) SOC replaces the microcontroller

AXI4-Stream(-like)

“BLDC motor coils”

Trusted IoT - WP3

Work on the COMM

There is a processor in the COMM that:

- sends and receives RF signals
- transmits and receives instructions over PWM
  - can be PWM
  - can be (C)PPM
  - can be SBUS
- a small **microcontroller** manages

We want to get around using the microcontroller

Trusted IoT - WP3

Work on the COMM

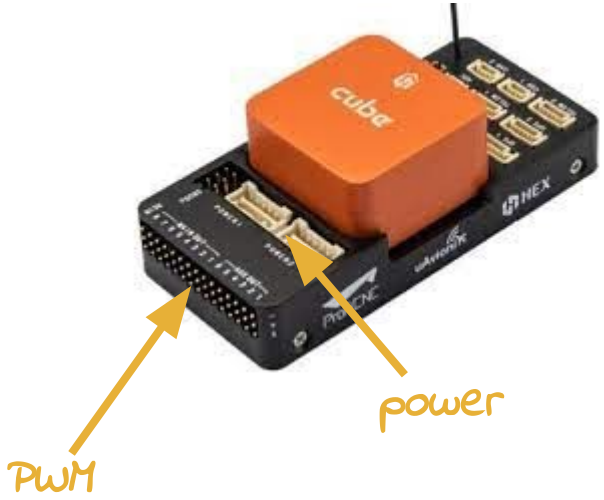
UART

AXI4Stream-like

Trusted IoT - WP3

NOT started with FC

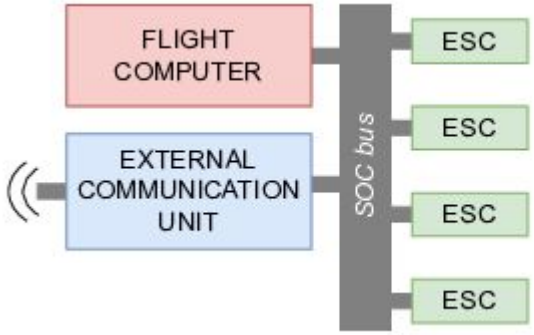
We want to get around using the microcontroller



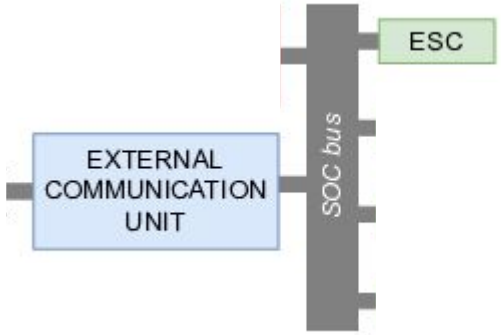
THIS WON'T MAKE IT

Trusted IoT - WP3

Targeted implementation



Current state of implementation



This implementation replaces/represents the “main application”

Trusted IoT - WP3

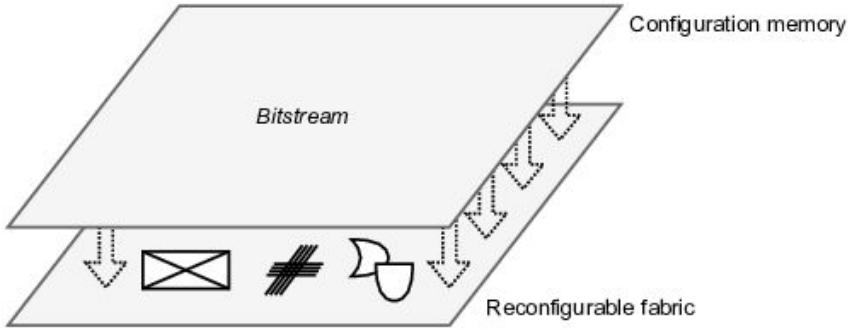
The main application needs to be attested

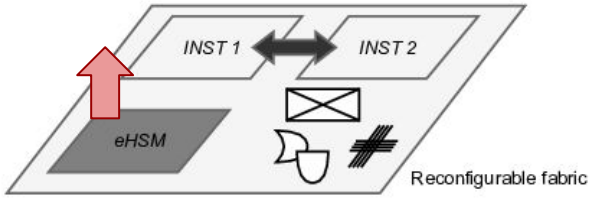
Because the main hackable components are on the FPGA, attestation of the entire FPGA is required.

Trusted IoT - WP3

The main application needs to be attested

Because the main hackable components are on the FPGA, attestation of the entire FPGA is required.



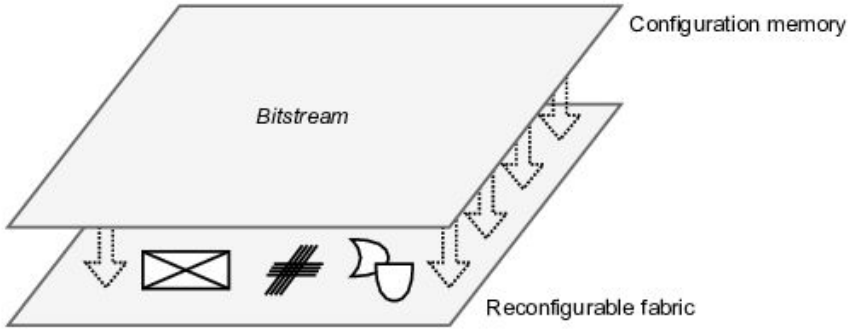


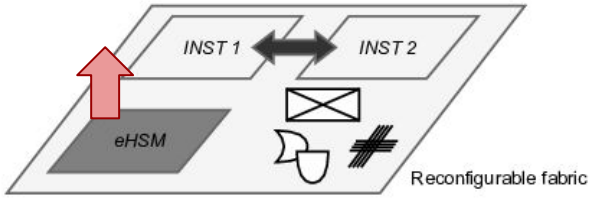
Trusted IoT - WP3

The main application needs to be attested

Because the main hackable components are on the FPGA, attestation of the entire FPGA is required.

Secure communication through LWC winner: ASCON





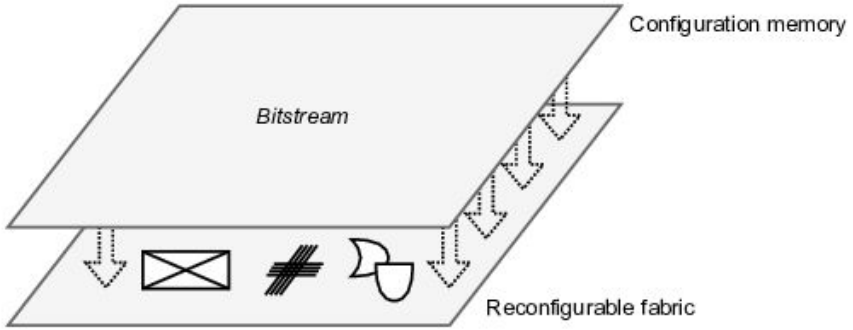
Trusted IoT - WP3

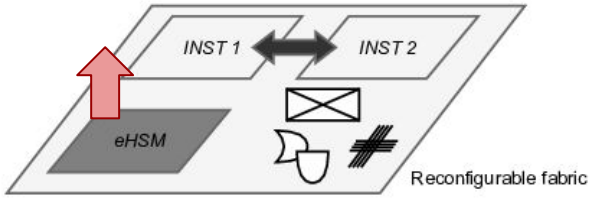
The main application needs to be attested

Because the main hackable components are on the FPGA, attestation of the entire FPGA is required

Secure communication through LWC

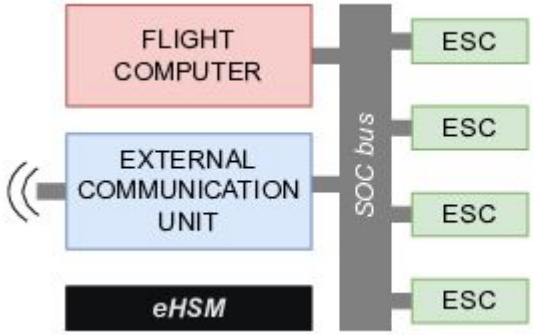
eHSM



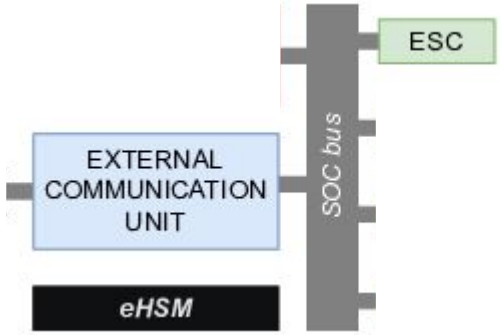


Trusted IoT - WP3

Targeted implementation



Current state of implementation



This implementation (= the drone) replaces/represents the “main application”

Trusted IoT - WP3

Delta w.r.t. November 15th, 2023

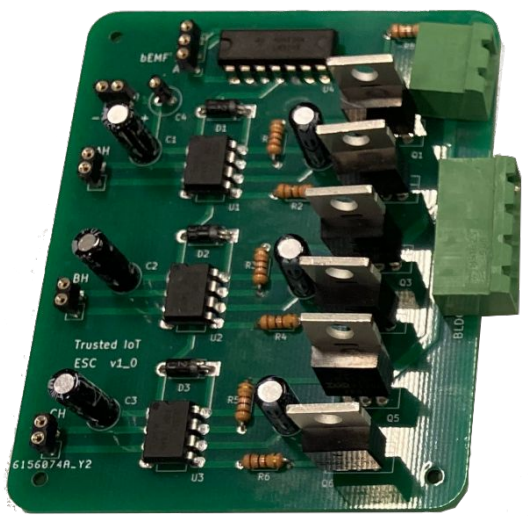
(the yearly Trusted IoT event, organised at IIoTSBOM)

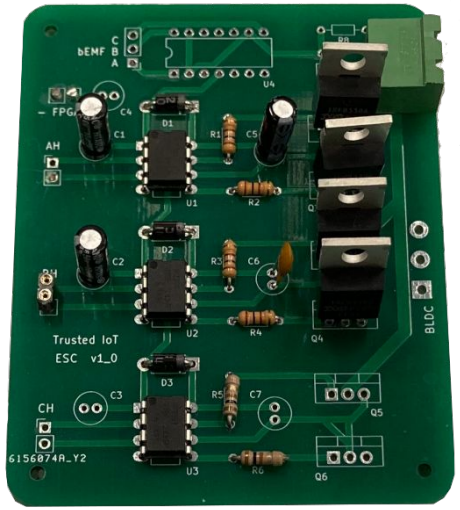
- Testing of PCB
- PCB v2.0
- ASCON Implementation
- eHSM (debugging)

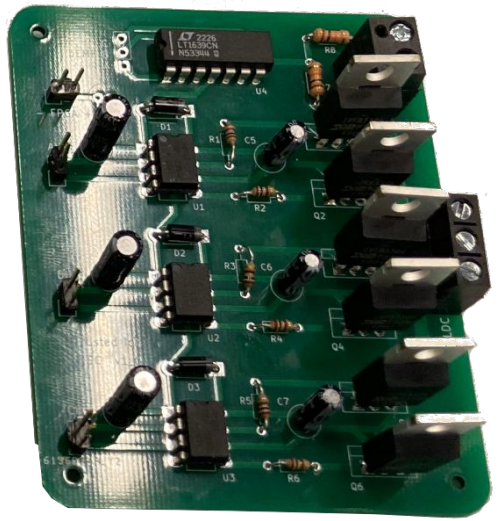
Trusted IoT - WP3

Delta w.r.t. November 15th, 2023: Testing of PCB

Three implementations were made, but didn’t seem to work





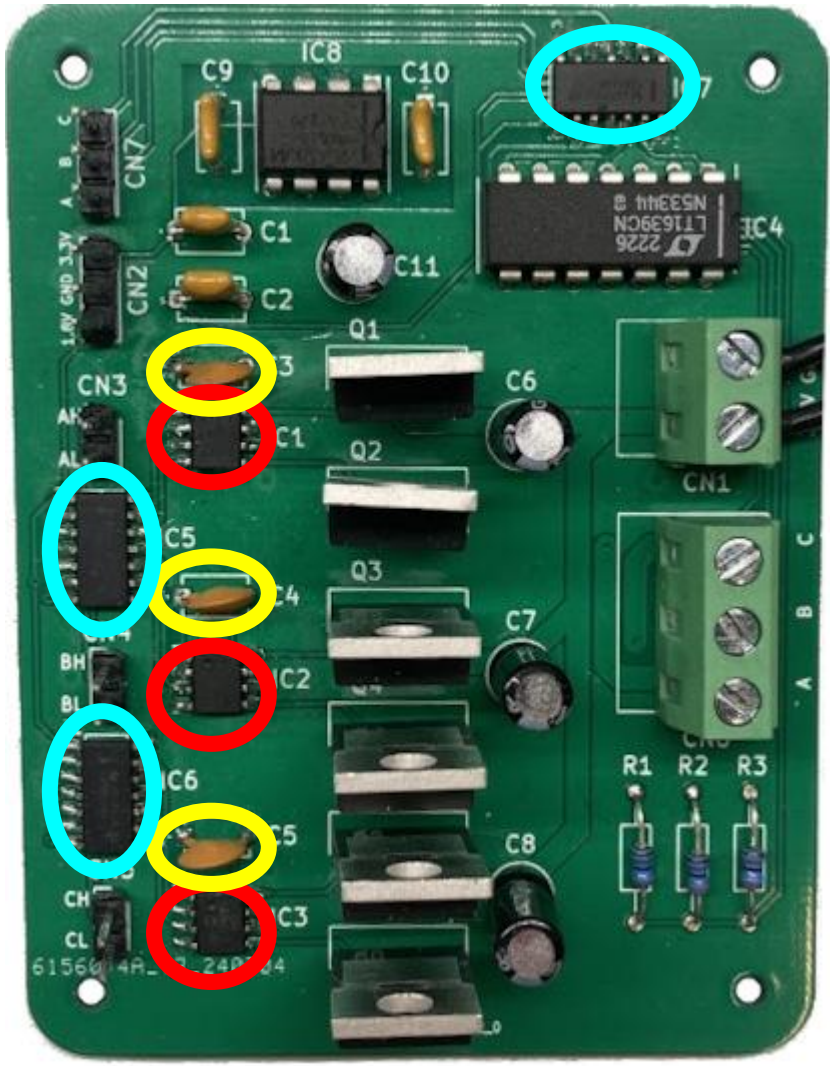


Trusted IoT - WP3

Delta w.r.t. November 15th, 2023: PCB v2.0

Main differences:

- Differently sized capacitors
- Better fitting driver ICs
- Added logical level shifters between FPGA and PCB 1.8 -> 5V
- Boost-converter 3.3V -> 5V

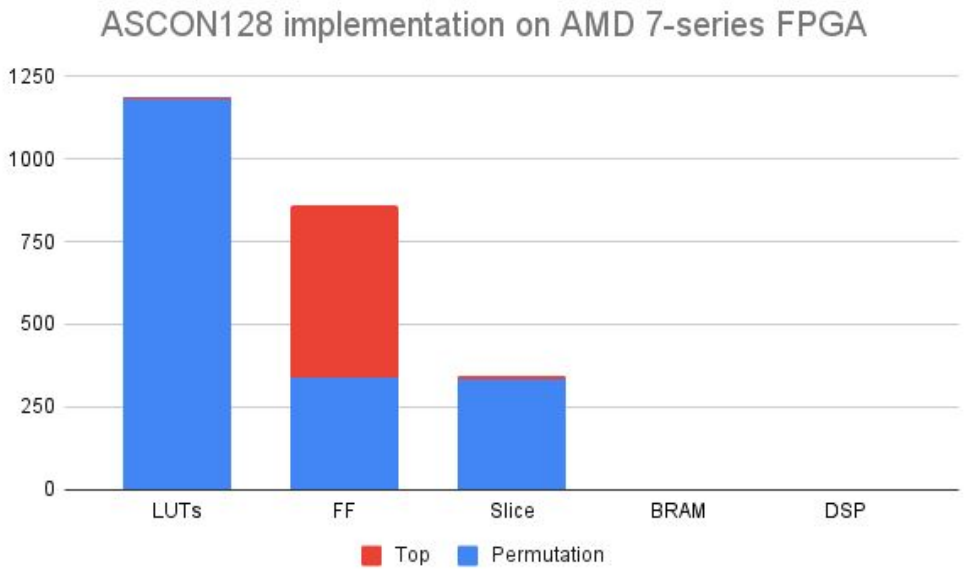


Trusted IoT - WP3

Delta w.r.t. November 15th, 2023: ASCON Implementation

ASCON:

- fully implemented in hardware
- can provide: AEAD
  (Authenticated Encryption with Associated Data)
  - encryption / decryption
  - MAC
  - hashing



F_{max} = 207.25 MHz

Trusted IoT - WP3

Delta w.r.t. November 15th, 2023: eHSM (debugging)

- Blocking issues with ICAP firmware have been fixed
- Read-back of Device ID is done
- Read-back of a single FPGA frame is done

WP4: Industrial Use Case Demonstration

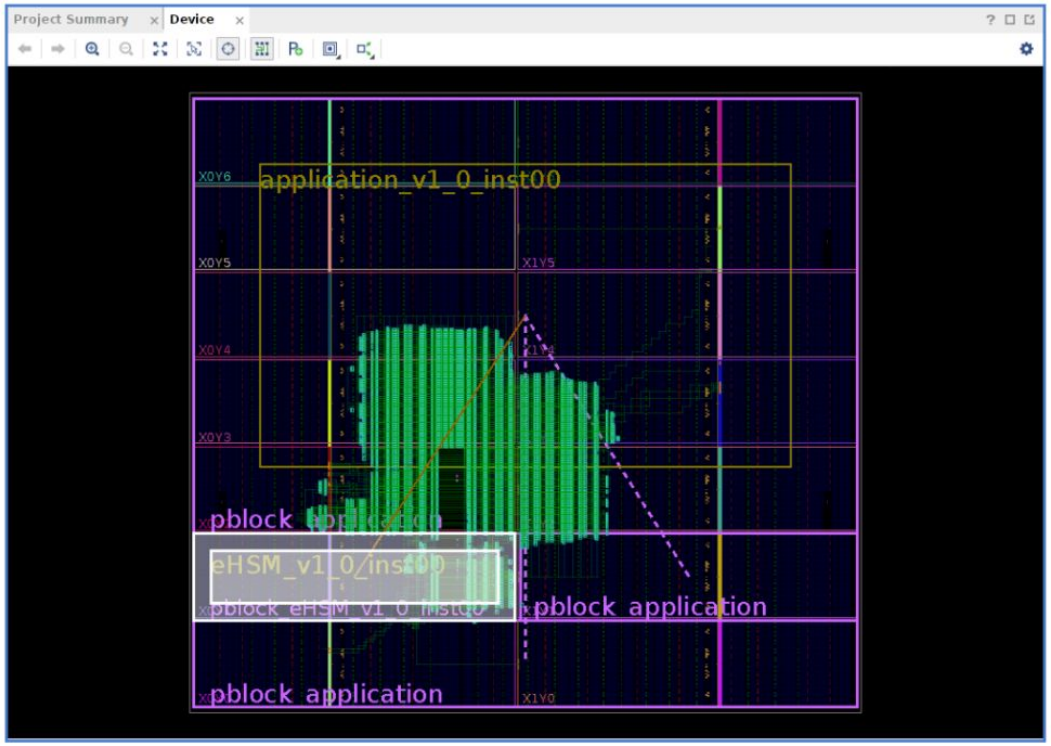
T 4.3 (KUL) Drones 4.4: The brain of the drone is the Flight Computer (FC) which collects output from several modules (e.g. the IMU) and provides input to other modules (e.g. the ESC). All these different modules, either providing or consuming data, are connected to the FC. In this use-case the aim is to **integrate these modules onto a single network-on-chip, consisting of RISC-V** processors, to bring two important benefits: 1) The **throughput** of the intermodule communication can be increased, 2) only **one single chip must be protected against attackers**. The benefit for the individual nodes (of having the possibility to offload work to a coprocessor) is also present for the remote attestation. Computation intensive primites like hash functions can therefore be **offloaded**. Due to the modular approach, unneeded features can be disabled in order to save energy, or could even be removed entirely in some RISC-V's.

Trusted IoT - WP4

WP4: Industrial Use Case Demonstration

Realised work:

- first merge of Application and eHSM
- Resource usage



KU LEUVEN

Trusted IoT - WP4

WP4: Industrial Use Case Demonstration

Remaining work:

- merge ASCON in eHSM
- read-back of entire *application*
- obtaining “the code”
- detect “inserted modification”
- finalise Demonstrator

WP5: Dissemination and Exploitation

T5.1 Dissemination activities: KO, intermediate user meetings, annual meeting

T5.2 Communication activities: project website, scientific papers will be published in conferences and journals, and the project will be made visual on social media (Twitter, LinkedIn,...)

T5.3 Exploitation activities: define internships, master and bachelor theses around the topics of the project, at least one follow-up project, and sharing platform

Trusted IoT - WP5

- T5.1 Dissemination activities:

  KO, intermediate user meetings, annual meeting
- T5.2 Communication activities:

  project website, scientific papers will be published in conferences and journals, and the project will be made visual on social media
- T5.3 Exploitation activities:

  define internships, master and bachelor theses around the topics of the project, at least one follow-up project, and sharing platform

Trusted IoT - WP5

- T5.1 Dissemination activities:

  KO, intermediate user meetings, annual meeting

Trusted IoT - WP5

- T5.1 Dissemination activities
- T5.2 Communication activities:

  project website, ✓

  scientific papers will be published in conferences and journals, ✓

Braeken, A. *et al.* (2024). Trusted Computing Architectures for IoT Devices. In: Skliarova, I., Brox Jiménez, P., Véstias, M., Diniz, P.C. (eds) Applied Reconfigurable Computing. Architectures, Tools, and Applications. ARC 2024. Lecture Notes in Computer Science, vol 14553. Springer, Cham. https://doi.org/10.1007/978-3-031-55673-9_17

J. Vliegen, M. Rabbani, W. Hellemans and N. Mentens, "HAGAR: Hashgraph-based Aggregated Communication and Remote Attestation" In Malicious Software and Hardware in Internet of Things, 7 pages, 2024.

the project will be made visual on social media

Trusted IoT - WP5

- T5.1 Dissemination activities
- T5.2 Communication activities:

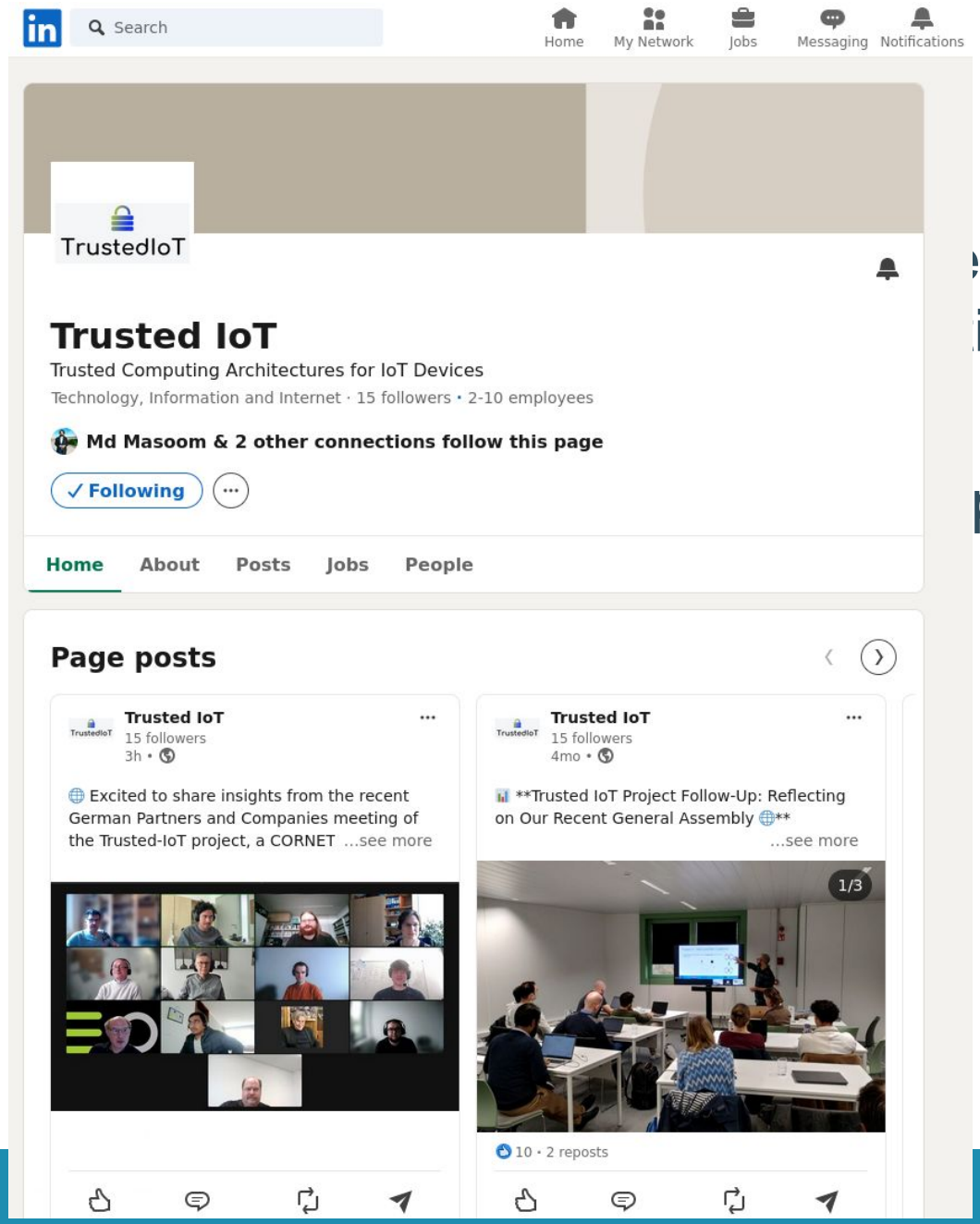
  project website, ✓

  scientific papers will be published in conferences and journals, ✓

Braeken, A. *et al.* (2024). Trusted Computing Architectures for IoT Devices. In: Skliarova, I., Brox Jiménez, P., Véstias, M., Diniz, P.C. (eds) Applied Reconfigurable Computing. Architectures, Tools, and Applications. ARC 2024. Lecture Notes in Computer Science, vol 14553. Springer, Cham. https://doi.org/10.1007/978-3-031-55673-9_17

J. Vliegen, M. Rabbani, W. Hellemans and N. Mentens, "HAGAR: Hashgraph-based Aggregated Communication and Remote Attestation" In Malicious Software and Hardware in Internet of Things, 7 pages, 2024.

  the project will be made visual on social media ✓



es

ies:

published in conferences and journals,

J. Vliegen, M. Rabbani, W. Hellemans and N. Mentens, "HAGAR: Hashgraph-based Aggregated Communication and Remote Attestation" In Malicious Software and Hardware in Internet of Things, 7 pages, 2024.

visual on social media

Trusted IoT - WP5

- T5.1 Dissemination activities
- T5.2 Communication activities
- T5.3 Exploitation activities:

  define internships, ✓

  master and bachelor theses around the topics of the project, ✓

  at least one follow-up project, and

  sharing platform

Horizon Europe project in preparation

Increased Cybersecurity 2024 (HORIZON-CL3-2024-CS-01-01)

?

thank you !!


425