3rd national RISC-V student contest 2022-2023

Sponsored by Thales, the GDR SOC² and the CNFM

CV32A6 RISC-V soft-core hackathon

You are students and like new challenges.
You are interested in electronics, computer architectures and embedded cybersecurity. You want to participate in the adventure of a renowned OpenHW processor core.
Then join this contest and win up to € 5,000!

Context

Thales is a world leader for mission critical information systems for the security, defense, space, aerospace and ground transportation domains. It employs 81,000 people in 68 countries. Following the success of two national RISC-V student contest (2020-2021, 2021-2022), Thales Research & Technology France, together with the GDR SOC² and the CNFM, are proud to announce the co-organization of the 3rd edition of the contest (2022-2023). This new contest will focus on the **security** of the CV32A6 RISC-V soft-core.

RISC-V is a recent open ISA that is gaining every day more attraction. From this ISA, ETH Zürich has designed a mid-range open-source application core named **ARIANE**. It has the capacity to execute rich operating systems and integrates an MMU function and several privilege levels. In 2019, the **OpenHW Group** was created with the ambition to design industrial-grade RISC-V processors. It has integrated the ARIANE core as its new 64-bit application core under the name CV64A6. Thales engineers have created a more compact 32-bit version from the original design, named **CV32A6**. CV32A6 and CV64A6 share the same source code and are together referred to as CVA6.

This year, the students are tasked to defeat several cyber attacks on the CV32A6 core geared with the Zephyr RTOS and running test applications. Winning teams will be those who defeat the more attacks. Teams can act at several levels: modify the CV32A6 core, the Zephyr RTOS and/or the compiler.

Targeted participants

You are a team of students:

- 2 to 4 **Master 2 students** (or equivalent: final year in engineering schools)[1]
- Registered in a **French engineering school or university**
- Coached by one or several **supervisors** (teachers, assistant professors, professors)
- A PhD student can additionally provide some coaching.

You have the following skills or will get some or all of them:

- Digital electronics
- HDL languages
- Digital simulation
- Computing architecture
- Embedded programming and RTOS
- Embedded security
- FPGA design and tools

The broad timeline of the contest should make it a good fit for your last-year university/school project. You can start a few months after the official kick-off date or submit results weeks or months before the deadline, e.g. before you start an internship.

Description of the contest

Inputs

Thales will prepare a kit composed of:

- A testbench to simulate the CV32A6 in its RTL form;
- The parameters of the CV32A6 core to consider;
- Scripts for synthesis of the baseline core;
- A BSP;
- A reference design to run the CV32A6 core on an FPGA development board
- Zephyr RTOS ported to CV32A6
- Zephyr running on a QEMU-RISCV emulator (for faster investigations than RTL simulations)
- HOPE-RIPE attacks ported to Zephyr and CV32A6
- Various applications to run on the processor core and check they were not broken by your modifications.

The kit will be obtained from a Thales GitHub repository. The repository address will be communicated through the Discord platform (see next section).

You will get support from your university/school and coaching from your supervisor. The organizers (Thales, GDR SOC², CNFM) will remain in contact with the teams and the supervisors.

Communication and support

Supervisors, together with the university/school staff, will provide level 1 support to the team. Level 2 support may only be exercised if the issue cannot be solved at level 1.

A Discord place will be created by the organizers to:

- Communicate announcements and practical information;
- Allow level 2 support;
- Host forums and discussions open to all participants.

[1] Although the contest does not primarily target M1 students, they are also accepted.

The Discord place will log messages so that teams, which will start later, can recover past information. No mailing list will be maintained; all messages will go through Discord after the team is registered. The invitations to the Discord place will be sent when the registration is accepted.

The French language will be used on Discord and during the interim event. Results can be reported in French or English.

Prerequisites

Most parts of CVA6 are written in **SystemVerilog**, a language widely adopted by the industry. You will have to use this language if you intend to modify the core.

Zephyr RTOS is written in C language; you will have to use it if you intend to modify the operating system.

The list of CAD tools and the FPGA board are unchanged w.r.t. the previous editions, so that schools/universities having participated last year may have the pre-requisite for this contest.

The **FPGA development board** selected for this context is the Digilent Zybo Z7-20.

Because of the current tensions on supply chains, you should **anticipate as soon as possible the provisioning of the mandatory FPGA development environment** to avoid unnecessary delays. The list of necessary material is:

Reference	URL	Remark
Zybo Z7-20	https://store.digilentinc.com/zybo-z7-zynq-7000-arm-fpga-soc-development-board/	Zybo Z7-10 is too small for CVA6.
Pmod USBUART	https://store.digilentinc.com/pmod-usbuart-usb-to-uart-interface/	Used for the console output
JTAG-HS2 Programming Cable	https://store.digilentinc.com/jtag-hs2-programming-cable/	
Connectors	https://store.digilentinc.com/pmod-cable-kit-2x6-pin-and-2x6-pin-to-dual-6-pin-pmod-splitter-cable/	At least a 6-pin connector Pmod is necessary; other references may offer it.

Supervisors must **make sure the student teams will have this FPGA environment**. They can order the complete set from CNFM (contact: fpga@cnfm.fr).

The Siemens EDA (formerly Mentor Graphics) **Questa** digital simulator will be needed if you modify the CV32A6 core and will be supported by Thales. Questa licenses can be obtained through CNFM. As the Questa licence tokens are hosted on a CNFM server, you will likely need support from your IT (e.g. configure a firewall, communicate IP address with CNFM…).

Xilinx Vivado will be used for the synthesis and place & route to port CV32A6 to the FPGA board. Participants can use evaluation licenses or the Xilinx University Program (XUP).

The kit prepared by Thales will run on Linux Ubuntu 20/04. You can use other host OSes, but you will not receive IT support by the organizers.

CAD tools are available in schools/universities through CNFM. For any information, supervisors can get in touch with cao@cnfm.fr.

From last year experience, you should **anticipate the provisioning of CAD licences and FPGA board, and the setup of the IT infrastructure** to avoid delays.

Work to perform and constraints

Your goal is to defeat as many HOPE-RISCV attacks as possible on the CV32A6 core geared with the Zephyr RTOS and running test applications.

To defeat RIPE attacks, you have to modify the CV32A6 core, the Zephyr RTOS and/or the compiler.

Your creativity should prevail as long as these constraints are fulfilled:

- The size of your hardware design fits in the FPGA.
- The test applications run correctly on FPGA when you apply your security solution (no false positives).

- You do not alter the source code of the test applications.
- The execution time of the test applications does not increase more than 100%.
- The memory footprint of your solution (including the OS, the application and the data) does not increase more than 100%.
- You do not replace the CV32A6 by another core (but you can modify it).
- You do not replace Zephyr RTOS by another OS (but you can modify it).
- You may not modify the test applications nor the RIPE tests running on Zephyr OS.

The QEMU emulation environment is provided to help you design the software part of your solution. However the results have to be demonstrated on the FPGA board.

Outputs

You shall provide:

- A 6-page report presented as a scientific paper, in French or English, with illustrations[2]
- A 10-minute recorded video, that will be presented during the defense session (and during the prize ceremony for the winning teams), in French or English
- A link to your new source code and results uploaded on GitHub (under Apache 2.0 or Solderpad 2.0 licenses)
- The reports from the tools that justify the results presented in the report.

During the course of the contest, the organizers will provide additional instructions with a standardized way to report results, according to the defined criteria.

Contributions to the OpenHW Group

Thales may promote some of the student open-source contributions to the OpenHW Group. The OpenHW Group criteria for accepting contributions may differ from those used in this contest.

Prizes and jury's criteria

To be eligible for the final selection, your solution must work on the FPGA board, defeat one or more attacks, correctly execute the test applications and fulfill the constraints listed above.

The jury will then **rank the results based on the number of defeated attacks** of the solutions compared to the original design delivered in the kit.

If there are ties, i.e. teams defeat the same number of attacks, the results will be separated according to the execution time of one of the test applications.

Thales will award **€ 5,000** to the winning team and **€ 2,000** to the second best team (both prizes will be shared among the team members).

The winning teams will present their video at an event organized by Thales and/or the GDR SOC². In addition to the prize, they will get a diploma.

Registration

Teams may register anytime until **2023-01-31** and run the contest at their own pace. They will recover past information from the Discord server.

Teams from a same university/school will register separately and can start at different dates.

Teams may deliver their results at any time before the end of the contest (**2023-05-12**). For instance, they can deliver their results in February if students start their internships in March.

To register, the supervisor will send an email to Jérôme Quévremont, Sébastien Pillement and Pascal Benoit (addresses below) with the following details:

[2] An IEEE template is recommended: https://www.ieee.org/conferences/publishing/templates.html.

- Name of the university/school
- Name of the team[3]
- Supervisor: Name, position (e.g. assistant professor), email address
- For each student: Name, option/major/"filière", Master 1 / Master 2, email address

The organizers will then check whether the registration is valid and send Discord invitations to the students and the supervisors.

A few additional rules:

- Individual candidates and teams without a supervisor are not accepted.
- If you are more than 4 students, register as several teams.
- There may be several teams from a given university/school. A team may include students from different options/majors/"filières".
- A student may not be in more than one team.
- A supervisor may supervise several teams and ensure no co-operation between these teams on their technical solutions. Joint teaching/learning (e.g. SystemVerilog, ISA, RTOS courses) is of course accepted and encouraged.
- The supervisor may be replaced during the project.
- Once the team is registered, the list of students shall not change (except under exceptional circumstances, with the organizers' agreement).
- The organizers will consider specific situations (if not clearly defined in the rules) while maintaining the fairness with other teams.

Abbreviations

ASIC	Application-Specific Integrated Circuit
BSP	Board Support Package
CAD	Computer-Aided Design
CNN	Convolutional Neural Network
FPGA	Field-Programmable Gate Array
HDL	Hardware Description Language
IC	Integrated Circuit
ISA	Instruction Set Architecture
OS	Operating System
RIPE	Runtime Intrusion Prevention Evaluator
RISC	Reduction Instruction Set Computer
M1/M2	Master 1 / Master 2
MMU	Memory Management Unit
RTOS	Real-Time Operating System
TBA	To be announced
XUP	Xilinx University Program

Planning

	Thales	GDR SOC[2]	CNFM	Teams and universities/schools
October 17th, 2022	Launch the contest			You can register teams as soon as you read this document. You can anticipate the contest by gaining knowledge on CV32A6, Zephyr, RIPE… No support from the organizers until the kit is delivered.

[3] It is important if several teams from a same university/school register. If only one team registers, it can have the name of its university/school. The team name will be printed on the winners' diploma.

	Thales	GDR SOC²	CNFM	Teams and universities/schools
First half of November 2022	Deliver the kit as a GitHub repo.			The teams can start later than this date.
November-May	Level 2 support (fix bugs in the kits…)			Run the project. Supervisors provide level 1 support to the student team.
January 10th, 2023 14:00	Organize an online event: teams' introduction, guidelines to prepare submission, Q&A…			Participate to the event
January 31st, 2023				Deadline to register teams
May 12th, 2023 at 23:59				**Deadline to submit results in a GitHub repository (reports, source code…)**. The teams can submit results sooner. The defense videos will have to be provided about one week after.
End of May 2023 (TBA)	Organize the online defense session as online meeting(s)			Attend the online defense session: recorded video (10') + live Q&A (5')
June 12th-14th, 2023	Final event at Colloque GDR SOC² in Lyon: prize announcement, presentation by the winning teams (recorded videos).			Representatives of each winning team are welcome to receive the diploma and applauses.

Contacts

Thales Research and Technology	Jérôme Quévremont	jerome.quevremontⓐthalesgroup.com
GDR SOC²	Sébastien Pillement	sebastien.pillementⓐuniv-nantes.fr
CNFM	Pascal Benoit	pascal.benoitⓐlirmm.fr