Advanced Security Closure of Physical Layouts

[ISPD23 Contest]

Q&A

Last updated: March 21, 2023

This page will be updated with Q&A once they come in; check back regularly. Important Q&A feedback will also be announced as well as shared via email to registered participants.

(Feel free to also check last year's Q&A — some points should still apply also for this year's version contest. In any case, we'll update this site with all relevant Q&A for this year.)

Q&A: ASAP7

Q3: We have encountered a DRC verification problem that hinges on the version of Innovus. We read the same .enc file with Innovus 21.12 and 21.36 respectively, and found that the 21.12 version reports 13 more Minimal_Area violation on the M1 layer. We look into the layout view, but we cannot refer to the x boxes highlighted as minimal area violations. Since the 21.36 version gives result consonant with our manual check, we assume there might be some bugs in drc verification in certain versions of Innovus.

A3: Thanks for reporting this! If possible, please use the same version as we have set up in the backend (21.13), so you can catch and avoid such issues early on in your flow. You can also try the other versions which we have checked ASAP7 for, as mentioned in https://github.com/Centre-for-Hardware-Security/asap7_reference_design At this late

point into the contest, we refrain from upgrading the Innovus version on the backend, as that might have other side-effects we don't know of yet.

Q2: We saw that in the ASAP7 used in the contest, M8 and M9 have extremely large MinArea requirement. We checked the asap7 library and it seems that there was a fix on this (only 5 days ago). https://github.com/The-OpenROAD-Project/asap7/commit/b2ad4e0c4ee180b20add407a0513c682256ee19a In this contest, we will just keep using the current one with large min area?

A2: The changes for M8, M9 in that recent commit by OpenROAD would have little to no impact for this contest and its settings – it is really hard to use these metals for signal routing. Other changes on M6/M7, introduced between Summer 2022 and Feb 2023, are already covered by our revision to the files. In general, recall that our provided versions is an interpretation of what the 7nm rules should look like, with some additional changes made for Innovus compatibility.

In short, we will continue using the techlef as shared previously.

Q1: We found that Innovus will give the following warning in the check log: `**WARN: (IMPSP-377): Center of Cell HB4xp67_ASAP7_75t_L's M1(1) Pin 'Y' does not fall on any existing track, given the current track offset of 0.0000 micron. The expected track offset is 0.1080 micron.` This warning indicates that the pin shape of cell HB4xp67_ASAP7_75t_L on M1 layer cannot be aligned with any track.

To make matters worse, Innovus considers this warning a risk and refuses to use the problematic cells in the opt phase, as shown in the log: `[02/04 17:35:38 137s] Cell 'HB4xp67_ASAP7_75t_L' is marked internal dont-use due to tech site checking failure.`

We would like to know if there is a problem with the track given in the original def and whether we can modify the track set in the def to avoid this warning or not.

A1 (updated March 9): We have encountered the same problem when developing the baseline version of the benchmarks. The issue is not related to a specific cell, it is related to how Innovus interprets the pitches from the techlef. This behavior changes for different versions of innovus.

You can check the reference script that we provide in https://github.com/Centre-for-Hardware-Security/asap7_reference_design/blob/main/scripts/innovus.tcl Look at line 93. There is a series of commands you have to run to make Innovus 21 happy with the tracks.

Note that, if are trying to change the track setting after the design is placed (e.g., 'add_tracks' command is executed after 'defIn') this erases the previous tracks and the tool has no choice rather than removing all the instances since they might not match the new tracks anymore. As you can see in the reference script, we put all the track-related commands in the initial phase, even before the PDN commands. We recommend the same flow be used by the participants.

This also implies that we do not recommend to load the baseline DEF and revise that, but rather you generate your own DEF, by taking the reference flow as starting point and then incorporating your defense techniques in there.

Q&A: Scoring, Evaluation, and Benchmarks

Q12: For the timing violation of trojan insertion. Will it be counted as a violation if inserting a trojan creates negative slacks or if inserting a trojan causes some worse slacks compared to a baseline?

A12: Timing violations for Trojan insertion are based on negative slacks only, not on (positive) slacks that are worse than the baseline.

Q11: For the eco-based trojan insertion at each level(regular, advanced, adadvanced), will you try only one trojan or multiple trojans? If it is multiple, then it is regarded as a failure for this level if only one of the trojan insertions fails or all of the trojan insertions must fail?

A11: We process this the other way around: for each Trojan, we try all the modes separately. Thus, your question whether the mode is considered as fail when one/all Trojans fail does not apply. For the scoring, we then do average, for each Trojan, the results obtained for all modes.

Q10: PDN constraint. We note that die area is one of the scoring metrics. One of our doubts is how to keep the PDN unchanged after the floor plan. Is the latest alpha case

physical synthesis script the same as the GitHub ASAP7 reference flow?

A10: Correct, the script at https://github.com/Centre-for-Hardware-Security/asap7_reference_design/blob/main/scripts/innovus.tcl contains the latest steps for the PDN design. These steps will also be kept throughout the contest, and compliance for these rules is also checked for. So, you're free to explore die area as optimization goal as long as you can follow the provided steps for the PDN design.

Q9: Score and Ranking. It has been mentioned on the website that there will be actual Trojan insertion behaviour during the final round of testing. So, what is the weight of each of the simulated Trojan insertion scores and the current scoring system scores when sorting the final results?

A9: The actual Trojan insertion will cover a set of different Trojans for each benchmark. Each Trojan will contribute equally to the security score, as the challenge imposed by Trojans is difficult to generalize, i.e., depends on the approach and efforts for security closure by teams. More details will be announced in time.

Q8: Will the trojan-insertion evaluator be provided before the final deadline?

A8: We're planning to share the DEF files after Trojan insertion back to the participants, along with all the evaluation scripts and details. However, as in a realistic attack scenario, we will not share the details of the actual Trojans directly. You're free to study the DEFs containing the Trojans to better understand the attack and revise your defense.

Q7: The evaluation metric says the number of free tracks is counted. We are wondering what kind of track will be counted as a free track. Is there a threshold of length or something?

A7: We utilize the command "report_route -include_regular_routes -track_utilization" to generate reports/track_utilization.rpt files. In there, you'll see the number of tracks, track lengths, blocked by what part, and the percentage of available tracks. We consider the last, percentage of available tracks, for scoring. We remain agnostic as to how Innovus counts tracks (considering length thresholds etc or not).

Q6: For the alpha round submission, we wonder if the criteria for passing alpha are no errors and an overall score of less than one. Do the warnings reported also need to be eliminated? (We noticed that submitting the original def and v files will also cause certain warnings)

A6: Correct, for passing the alpha round, only overall scores < 1.0 with some valid submissions are required — valid means no errors. You do not need to fix warnings. Only in case you exceed any warning by +10 over the original layout, this would be considered an error. (In such cases, the related warnings are raised to errors automatically.)

Q5: In the case of timing violations, the performance metric is scored as negative. Is there a problem with this? Or, is there a bug in the scoring of performance?

A5: In case of timing violations, the performance metric is, by definition, not applicable anymore. In general, whenever there are errors, scores are only returned for information, as also emphasized in the notification email ("SCORES ONLY FOR INFORMATION. THIS SUBMISSION IS INVALID DUE TO SOME ERRORS.")

Which parts of the scoring remain applicable/informative and which not depends on the actual error(s). In your example with timing violations, performance score is not, whereas area, power scores, etc. would be. Still, given that the OVERALL score considers all metrics, it is not meaningful anymore for various kind of error(s).

In short, for any error(s), scoring provides only limited information and has to be treated with caution. Such feedback can still be helpful — for example, when there's only 1 DRC violation, fixing that violation shouldn't change the layout and thus the scores much, so the informative scores returned despite such single DRC violation should be a very close estimate of what to expect once the violation is fixed.

Q4: Can commits with timing violations be seen as valid commits?

A4: No.

Q3: We would like to know whether as long as each test case submission contains a result without DRC and scoring other than 1 (which demonstrates that the result is different from the baseline), we will pass the alpha round.

A3: No, not exactly like that. To pass the alpha/qualification round, teams must have at least one submission per benchmark that is returned without errors: no DRCs, yes, but also within the allowed margin (+10 issues) for all other design checks. Furthermore, the score (OVERALL) needs to be improved at least a little, i.e., OVERALL < 1.000000 must be met; OVERALL != 1.0, especially OVERALL > 1.0, is not sufficient.

Note that, to monitor your progress, you are encouraged to submit as many trials as you which and at any point in time. Any trials may contain DRC violations where you would still receive feedback and scores from the evaluation server, albeit labelled as invalid for ranking/passing the alpha round.

Q2: When evaluating the results of physical design, we have encountered the following problem. When executing the evaluation tcl file check,tcl, we encountered an error:
“-include_regular_routes” and “-track_utilization” are not a legal option for command “report_route” .
we have tried the Innovus of versions 20.10 and 21.12, and both fail to execute the command “report_route -include_regular_routes -track_utilization > reports/track_utilization.rpt”.
Besides, we found these options might be the new features in Innovus22.

So we wonder if we can generate the same “track_utilization.rpt” (or a substitute with the same key information) by some basic options or additional operations with an older version of Innovus.

A2: Did you invoke Innovus with Stylus format as mentioned in the README? Like, “innovus -nowin -stylus -files scripts/check.tcl -log check” should be used.

You may use other versions and commands at your end for all checks, but only the scripts provided and tool versions mentioned will be used for official evaluation.

Q1: When we download the alpha test and put it into the virtual machine and unzip it, it reports errors. The error messages are shown below.

```
symlink error: Operation not supported
  _alpha/sha256/ASAP7/asap7_tech_4x_201209.lef -> ../../../_ASAP7/techlef/asap7_
tech_4x_201209.lef
symlink error: Operation not supported
  _alpha/sha256/ASAP7/qrcTechFile_typ03_scaled4xV06 -> ../../../_ASAP7/qrc/qrcTe
chFile_typ03_scaled4xV06
symlink error: Operation not supported
  _alpha/sha256/scripts/check.tcl -> ../../../_scripts/check.tcl
symlink error: Operation not supported
  _alpha/sha256/scripts/mmmc.tcl -> ../../../_scripts/mmmc.tcl
symlink error: Operation not supported
  _alpha/sha256/scripts/lec.do -> ../../../_scripts/lec.do
symlink error: Operation not supported
  _alpha/sha256/scripts/exploitable_regions.tcl -> ../../../_scripts/exploitable
_regions.tcl
symlink error: Operation not supported
  _alpha/sha256/scripts/exploitable_regions.bin -> ../../../_scripts/exploitable
_regions.bin
symlink error: Operation not supported
[master@icpc share]$
```

It seems that this is caused by the use of links in the zip file. What should we do to resolve this issue? Or do you have plans to update the Alpha Test set to fix this bug?

A1: It's correct that the ZIP archive uses symbolic links, but this is on purpose and not a bug. Otherwise the size of the ZIP file would be very big. Please note the README in the release:
> This benchmark suite is part of the ISPD23 contest. Please see https://wp.nyu.edu/ispd23_contest/ for more details.
>
> Note: use of a Linux OS is recommended for handling this zip archive, as it makes use of symbolic links which are not necessarily supported by zip tools in other OS.

So, we suggest you use a Linux in the virtual machine as well.

Q&A: Scope, Threats, General Approach, Tools, etc.

Q2: From what we have seen so far, it seems that Cadence tools Innovus and Genus are the main platforms we should use. While we look into accessing these products, we were wondering the following:
Is there any documentation available to assist with setup and understanding the framework?
Are there any other tools aside from Genus and Innovus you recommend becoming familiar with?

A2: While we recommend Cadence Innovus (Genus is not really needed for you), as we've shared a reference flow for ASAP7 for that, it's not a must to use these tools. If you have icc, icc2, OpenROAD or other tools at hand, you may try them as well. But we haven't tried ASAP7 on them, so we can't really comment, although things should work out there as well.

We do not provide separate documentation for any of these physical design tools, sorry. You'd want to check websites, tutorials, etc by yourself in case you're new to physical design altogether.

Q1: I was wondering if the contest will help the contestant to access the cadence innovus or I should use my own or my university's software?

A1: No, we do not provide direct access to Cadence Innovus. (Only indirectly through the evaluation platform, but you cannot run you own scripts there, only the official scripts will be run automatically there.) Yes, you should make use of your own tools, possibly open source or provided by the University.