



Evaluating Capabilities for Assurance of Third Party Intellectual Property

Vivian Guzman Kammler | R&D Cybersecurity Lead

Virtual Event | November 4, 2021



Sandia National Laboratories

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

This presentation describes objective technical results and analysis. Any subjective views or opinions that might be expressed in the presentation do not necessarily represent the views of the U.S. Department of Energy or the United States Government.

Presenting an evaluation of tools. This does not constitute an endorsement.



SANDIA IS A FEDERALLY FUNDED RESEARCH AND DEVELOPMENT CENTER(FFRDC) MANAGED AND OPERATED BY

National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc.

Government owned, contractor operated

FFRDCs are long-term strategic partners to the federal government, operating in the public interest with objectivity and independence and maintaining core competencies in missions of national significance

The nuclear deterrent should

Always

NEVER

always be available for use when needed

never go off unless authorized

Zero Trust and Quantifiable Assurance

Hardware Assurance

An activity to ensure a level of confidence that microelectronics (also known as microcircuits, semiconductors, and integrated circuits, including its embedded software and/or **intellectual property**) function as intended and are **free of known vulnerabilities**, either intentionally or unintentionally designed or inserted as part of the system's hardware and/or its embedded software and/or intellectual property, **throughout the life cycle**.

DAU Glossary



Defining Constraints & Success Criteria



Constraints

“activity to ensure a level of confidence”

- **3PIP is not encrypted**
- **3PIP can be parsed by analysis tools**
- **Automation**
- ***Evaluator has limited design knowledge***
- ***There is no “golden” model (known good)***

Success Criteria

3PIP is “free of known vulnerabilities”

- **Verified functionality**
 - Available or provided functional checks pass
- **Detection of Hardware Trojans**
- ***Verified absence of vulnerabilities based on prior knowledge (catalogs, databases)***

Evaluating OneSpin Tools for Assurance of 3PIP

OneSpin Products / Apps

DV-Inspect

Trust Assessment Platform App

Processor Integrity App

EC-FPGA
EC-ASIC

GapFree Methodology

SCOPE

Automation

3PIP Testcases

Open

RS232

AES

RISC-V Rocket

Internal

I2C

XGEMAC

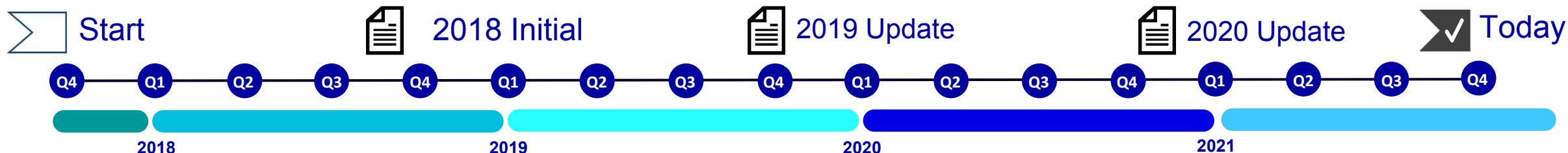
SPI

XTEA

USB, PID, RISC-V RoaLogic

Demonstration

Sandia Controller



How is 3PIP provided?

← OneSpin tools most useful here →

1 – based on ethernet MAC

2 – based on RISC-V RocketCore

```

always @ (posedge clk_xgmii_rx or negedge reset_xgmii_rx_n) begin
  if (reset_xgmii_rx_n == 1'b0) begin
    curr_state <= SM_INIT;
    col_cnt <= 8'b0;
    last_seq_type <= `LINK_FAULT_OK;
    link_fault <= `LINK_FAULT_OK;
    seq_cnt <= 3'b0;
  end
  else begin
    case (curr_state)
      SM_INIT:
      SM_COUNT:
      SM_FAULT:
      begin
        col_cnt <= col_cnt + 8'd2;
        if (!fault_sequence[0] && col_cnt >= 8'd127) begin
          // No new fault in lower lanes and almost
          // reached the 128 columns count, abort fault.
          curr_state <= SM_INIT;
        end
        else if (col_cnt > 8'd127) begin
          // Reached the 128 columns count, abort fault.
          curr_state <= SM_INIT;
        end
        else if (!fault_sequence) begin
          // Clear the column count each time we see a fault,
          // if fault changes, go no next state.
          col_cnt <= 8'd0;
          if (seq_type != last_seq_type) begin
            curr_state <= SM_NEW_FAULT;
          end
        end
      end
    end
  end
  SM_NEW_FAULT:

```

HDL

28
state bits/line of code¹

Generated HDL

0.4
state bits/line of code²

Netlist

state bits/line of code

Evaluating OneSpin Tools for Assurance of 3PIP

OneSpin Products / Apps

DV-Inspect

Trust Assessment Platform App

Processor Integrity App

EC-FPGA
EC-ASIC

GapFree Methodology

SCOPE

Automation

3PIP Testcases

Open

RS232

AES

RISC-V Rocket

Internal

I2C

XGEMAC

SPI

XTEA

USB, PID, RISC-V RoaLogic

Demonstration

Sandia Controller



Low Effort: 20 minutes

Check Type	Number of Checks	Number of Holds	Number of Fails	Number of Opens
Array Index	792	784	8	0
Truncation	452	36	114	302
Resolution-X	400	0	400	0
Signal-Domain	64	64	0	0
Init	78312	6816	71496	0
Dead-Code	23672	11987	2908	8777
Stick	56170	17374	3876	34920
Integer	2788	2303	14	471
Total	162650	39364	78816	44470

Useful as a first step

Enforces good coding habits

Which of these checks are assurance-relevant?

DV-Inspect autochecks run on MIT-LL Common Evaluation Platform (CEP) containing Rocket Core. <https://github.com/mit-ll/CEP>

DV-Inspect Autochecks



Normal Effort: 3 hrs, 13 min

Check Type	Number of Checks	Number of Holds	Number of Fails	Number of Opens
Array Index	792	784	8	0
Truncation	452	42 (+6)	124 (+10)	286 (-16)
Resolution-X	400	0	400	0
Signal-Domain	64	64	0	0
Init	78312	6816	71496	0
Dead-Code	23672	11987	3007 (+99)	8678 (-99)
Stick	56170	17374	3876	34920
Integer	2788	2303	14	471
Total	162650	39370 (+6)	78925 (+109)	44355 (-115)

(+/-) compared to Low Effort

Useful as a first step

Enforces good coding habits

Which of these checks are assurance-relevant?

DV-Inspect autochecks run on MIT-LL Common Evaluation Platform (CEP) containing Rocket Core. <https://github.com/mit-ll/CEP>

Normal Effort +: 1 day, 12 hrs, 50 min

Check Type	Number of Checks	Number of Holds	Number of Fails	Number of Opens
Array Index	792	784	8	0
Truncation	452	42	124	286
Resolution-X	400	0	400	0
Signal-Domain	64	64	0	0
Init	78312	6816	71496	0
Dead-Code	23672	12398 (+411)	4075 (+1068)	7199 (-1479)
Stick	56170	18099 (+725)	4193 (+317)	33878 (-1042)
Integer	2788	2303	14	471
Total	162650	40506 (+1136)	80310 (+1385)	41834 (-2521)

(+/-) compared to Normal Effort

What does this mean? When are we done?

DV-Inspect autochecks run on MIT-LL Common Evaluation Platform (CEP) containing Rocket Core. <https://github.com/mit-ll/CEP>

- Reached out to OneSpin to assist with interpretation of results, prover/disprover modifications, targeting only dead-code and stick checks. No finite state machines were automatically recognized.

Evaluating OneSpin Tools for Assurance of 3PIP

OneSpin Products / Apps

DV-Inspect

Trust Assessment Platform App

EC-FPGA
EC-ASIC

Processor Integrity App

GapFree Methodology

SCOPE

Automation

3PIP Testcases

Open

RS232

AES

RISC-V Rocket

Internal

I2C

XGEMAC

SPI

XTEA

USB, PID, RISC-V RoaLogic

Demonstration

Sandia Controller



Trust Assessment Platform (TAP) v2021.1.0

Lint browser (DV-Inspect)

- basic lint check, automatically performed on read-in designs

The screenshot shows the OneSpin 360 R software interface. The top menu bar includes Session, Setup, File, Edit, CC/MV, EC, Tools, Window, and Help. The toolbar contains various icons for file operations, search, and analysis. The main window has tabs for Design Explorer, Lint Browser, Auto Checks, Dead-Code Checks, Assertion Checks, and Trust. The Design Explorer tab is active, displaying a table of current lint data. The Shell tab is also visible, showing a command-line history and analysis results.

Design Explorer (Active Tab)

Current Lint Data Validity: up-to-date

Id		Category	Object	Source Location	Description	Excluded
issue_2_3	RegWithoutSink	AM_Transmission....	...ansmission.v:30.0-30.0	reg 'SECRETKey' has no sink in instance at line /home/rdande/projects/darpa/AES-T400/src/Tjntop.v:31:	Included	
issue_2_2	NonConstantReset...	AM_Transmission....	...ansmission.v:42.0-42.0	signal 'SHIFTReg' is assigned a non-constant value at reset.	Included	
issue_2_1	ExprFunc	AM_Transmision	...ansmission.v:38.0-38.0	expression size 33 is truncated to fit in target size 26.	Included	
issue_2_0	UnconnOutputPort	aes_128.out_1	...In/aes_128.v:42.0-42.0	output port 'out_1' is unconnected in instance 'a10'.	Included	

Shell

Shell Messages Progress

```

-W- Trust - Category 'trigger_state' not selected - cannot clear!
-I- Trust - Clearing category 'trigger_data'...
-I- Trust - Clearing category 'reliability_state'...
-W- Trust - Category 'reliability_assign' not selected - cannot clear!
-W- Trust - Category 'reliability_reach' not selected - cannot clear!
-I- Trust - Clearing category 'deadlock_auto'...
-W- Trust - Category 'deadlock_app' not selected - cannot clear!
mv analyze trust
-I- Trust - Arguments: -verbose false -silent false -category {trigger_data trigger_counter reliability_state deadlock_auto} -clear_category {trigger_state reliability_assign reliability_reach deadlock_app}
-prune src true
-I- Trust - Adding categories to database...
-I- Trust - Adding redundant states to database...
-I- Trust - Added 1 redundant state(s) to database.
-I- Trust - Performing basic code analysis...

```

analyze_trust (TAP)

- runs a suite of tests and presents a list of discovered issues
- the user can view the source of issues by clicking the list item
- execution time varies, minutes to hours

TAP Continues to Evolve

Hardware Trojan R&D

EDA Tool Evaluation

Experimental Results

Source	Name	Runtime	Issues Reported	Trojan Inserted	Automatic Detection
TrustHub*	AES	11 hours	2	Yes	Yes
TrustHub	PIC16	<1 min	72	Yes	Yes
TrustHub	RS232	<1 min	3	Yes	Yes
TrustHub	BasicRSA	<1 min	17	Yes	Yes
GitHub	RISC-V Rocketcore	28 min	12	No	Yes
OneSpin	UART	<1 min	10	Yes	Yes
Aerospace**	SpaceWire	<1 min	3	No/Yes	No
Aerospace	RISC-V Taiga	13 min	46	No/Yes	No
Aerospace	Leon3	6 hours	423	No/Yes	Yes***

* TrustHub designs averaged results over multiple articles

** Aerospace designs contained 1 golden, 3 with Trojans

*** Leon3 articles consisted of 3 Trojan designs, 1/3 Trojans discovered

(Results were from OneSpin TAP ~~2020~~ 2020.2



- Test suite
 - 90 designs with and without Trojans inserted
 - Size range: 100 to 100K FFs
- Results
 - Representative selection of IP designs shown in table
 - Few trigger-type issues reported
 - Numerous reliability issues reported
 - Very few false alarms
 - Some Trojans have been missed
 - Runtime is short

© 2020 OneSpin Osmosis | Page 18

Our RISC-V results consistent with Aerospace once we synced on same version

TAP helps filter results

TAP does not accelerate results

Best working with HDL

Evaluation of OneSpin Trust Assessment for Hardware Trojan Detection. Chan, Garrett and Rao, Vikram. Aerospace. Osmosis for DoD 2020.

Evaluating OneSpin Tools for Assurance of 3PIP

OneSpin Products / Apps

DV-Inspect

Trust Assessment Platform App

Processor Integrity App

EC-FPGA
EC-ASIC

GapFree Methodology

SCOPE

Automation

3PIP Testcases

Open

RS232

AES

RISC-V Rocket

Internal

I2C

XGEMAC

SPI

XTEA

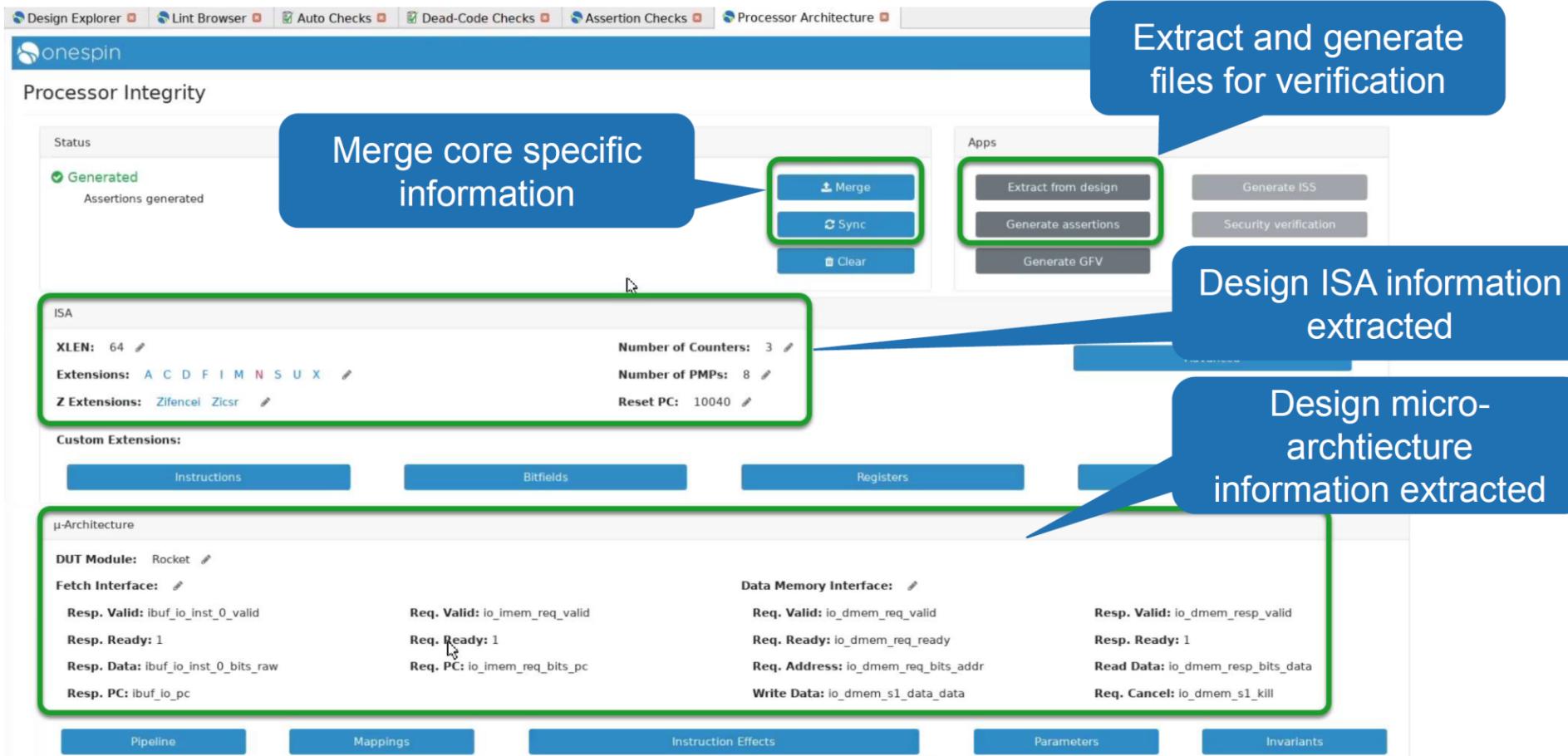
USB, PID, RISC-V RoaLogic

Demonstration

Sandia Controller



Processor Integrity App v2020.2



The screenshot shows the Processor Integrity App interface. The top navigation bar includes Design Explorer, Lint Browser, Auto Checks, Dead-Code Checks, Assertion Checks, and Processor Architecture. The main window has tabs for Status, ISA, Custom Extensions, μ-Architecture, and Apps. The Apps tab is active, showing buttons for Merge, Sync, Clear, Extract from design, Generate assertions, Generate ISS, Generate GFV, and Security verification. Callouts highlight the following features:

- Merge core specific information (points to the Merge button)
- Extract and generate files for verification (points to the Extract from design button)
- Design ISA information extracted (points to the ISA section)
- Design micro-architecture information extracted (points to the μ-Architecture section)

ISA

- XLEN: 64
- Extensions: A C D F I M N S U X
- Z Extensions: Zifencei Zicsr

Custom Extensions:

- Instructions
- Bitfields
- Registers

μ-Architecture

DUT Module: Rocket

Fetch Interface:

- Req. Valid: ibuf.io_inst_0_valid
- Req. Ready: 1
- Req. Data: ibuf.io_inst_0_bits_raw
- Req. PC: ibuf.io_pc

Data Memory Interface:

- Req. Valid: io_imem_req_valid
- Req. Ready: 1
- Req. PC: io_imem_req_bits_pc
- Req. Address: io_dmem_req_bits_addr
- Write Data: io_dmem_s1_data_data
- Resp. Valid: io_dmem_resp_valid
- Resp. Ready: 1
- Read Data: io_dmem_resp_bits_data
- Req. Cancel: io_dmem_s1_kill

Tool Buttons (Apps tab):

- Merge
- Sync
- Clear
- Extract from design
- Generate assertions
- Generate ISS
- Generate GFV
- Security verification

Open-source RISC-V instruction set architecture and Processor Integrity App enables access to GapFreeVerification™ rigor via automation

RISC-V Property Checks

Name	Proof Status	Vitness Status	Prover	Runtime
Properties	<any status>	<any s>		
RV_chk.ops.bubble_a	hold	pass (1)	approver1:0	00:00:55
RV_chk.ops.flush_a	hold	pass (3)	approver1:0	00:00:25
RV_chk.ops.interrupt_handle_a	fail (7)	pass (2)	disprover1	00:03:34
RV_chk.ops.mispred_a	hold	pass (3)	approver1:0	00:00:13
RV_chk.ops.RV32A.all_a	hold	pass (2)	approver1:0	00:01:22
RV_chk.ops.RV32D.all_a	hold	pass (7)	approver1:0	00:01:45
RV_chk.ops.RV32F.all_a	hold	pass (7)	approver1:0	00:01:05
RV_chk.ops.RV32I.ADD_a	hold	pass (2)	approver1:0	00:04:31
RV_chk.ops.RV32I.Arith_a	hold	pass (2)	approver1:0	00:07:30
RV_chk.ops.RV32I.AUIPC_a	hold	pass (2)	approver1:0	00:01:10
RV_chk.ops.RV32I.Branch_a	fail (7)	pass (2)	approver1:0	00:06:09
RV_chk.ops.RV32I.CallBreak_a	fail (2)	pass (2)	disprover1	00:02:11
RV_chk.ops.RV32I.CSR_a	hold	pass (2)	approver1:0	00:00:34
RV_chk.ops.RV32I.FENCE_a	fail (2)	pass (2)	disprover3	00:01:28
RV_chk.ops.RV32I.FENCE_I_a	hold	pass (2)	approver1:0	00:02:52
RV_chk.ops.RV32I.Jump_a	hold	pass (2)	approver1:0	00:00:46
RV_chk.ops.RV32I.LUI_a	hold	pass (2)	approver1:0	00:00:34
RV_chk.ops.RV32I.Mem_a	hold	pass (2)	approver1:0	00:01:14
RV_chk.ops.RV32I.RET_a	hold	pass (2)	approver1:0	00:01:27
RV_chk.ops.RV32I.Supervisor.SFENCE_VMA_a	hold	pass (2)	approver1:0	00:00:53
RV_chk.ops.RV32M.all_a	hold	pass (2)	approver1:0	00:03:41
RV_chk.ops.RV64A.all_a	hold	pass (2)	approver1:0	00:02:18
RV_chk.ops.RV64D.all_a	hold	pass (7)	approver1:0	00:01:13
RV_chk.ops.RV64F.all_a	hold	pass (7)	approver1:0	00:01:06
RV_chk.ops.RV64I.Arith_a	hold	pass (2)	approver1:0	00:00:53
RV_chk.ops.RV64I.Mem_a	hold	pass (2)	approver1:0	00:03:41
RV_chk.ops.RV64M.all_a	hold	pass (2)	approver1:0	00:01:14
RV_chk.ops.RVC.Arith_a	hold	pass (2)	approver1:0	00:16:50
RV_chk.ops.RVC.Branch_a	hold	pass (2)	approver1:0	00:00:45
RV_chk.ops.RVC.Jump_a	hold	pass (2)	approver1:0	00:01:05
RV_chk.ops.RVC.Mem_a	hold	pass (2)	approver1:0	00:01:53
RV_chk.ops.replay_a	hold	pass (2)	approver1:0	00:00:35
RV_chk.ops.replay_mem_a	hold	pass (2)	approver1:0	00:02:19
RV_chk.ops.replay_wb_a	hold	pass (2)	approver1:0	00:01:55
RV_chk.ops.reset_a	hold	pass (1)	approver1:0	00:00:11
RV_chk.ops.xcpt_fetch_dec_a	fail (2)	pass (2)	disprover3	00:01:52
RV_chk.ops.xcpt_mem_a	fail (12)	pass (7)	disprover1	00:31:15
RV_chk.ops.xcpt_wb_a	fail (7)	pass (2)	disprover1	00:14:14

Semi-automated to get to this point
Extract and map ISA registers,
custom extensions, exceptions,
interrupts

SUPPORTED

Rocket / MIT-LL CEP

<https://github.com/mit-ll/CEP>

- OneSpin had previously identified bugs contained in our version
 - Illegal instruction exception not raised when expected**
- Our CEP (v2.2) implementation had outdated Rocket Core
 - Issues have been closed since this finding

→ Identified processor integrity and provenance tracking issues

NOT YET SUPPORTED

Roa Logic

<https://github.com/RoaLogic/RV12>

- Full automated extraction not possible
- Custom JSON configuration file needed
- Modifications to internal SV files needed
- Did not pursue further

→ ***Others should expect to work with OneSpin for new processor configurations***

** <https://github.com/mit-ll/CEP/issues/8>
<https://github.com/chipsalliance/rocket-chip/issues/1861>
<https://github.com/chipsalliance/rocket-chip/issues/1949>

Evaluating OneSpin Tools for Assurance of 3PIP

OneSpin Products / Apps

DV-Inspect

Trust Assessment Platform App

Processor Integrity App

EC-FPGA
EC-ASIC

GapFree Methodology

SCOPE

Automation

3PIP Testcases

Open

RS232

AES

RISC-V Rocket

Internal

I2C

XGEMAC

SPI

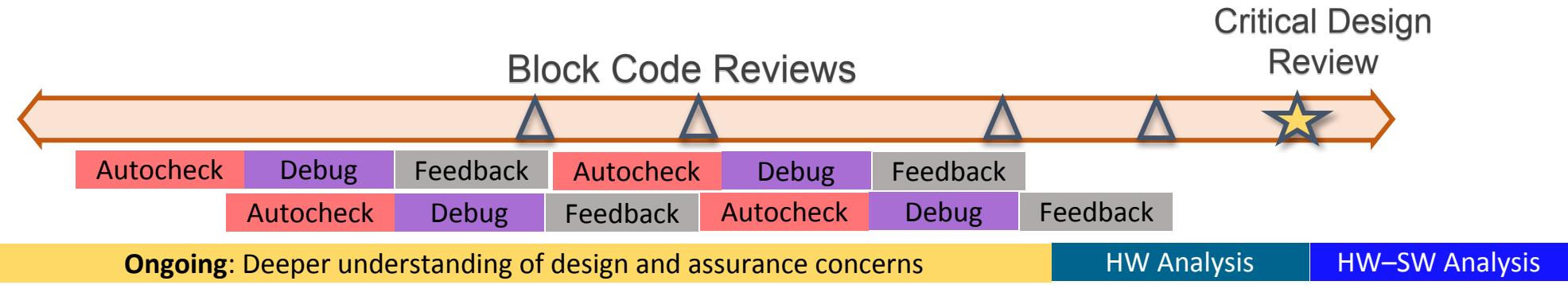
XTEA

USB, PID, RISC-V RoaLogic

Demonstration

Sandia Controller





Three teams: Design, Verification, and Independent Assessment

Autochecks save time, but should not define “done”

- Need tips and tricks for getting through dead-code and FSM analysis.

Formal verification does HW integrity really well

- **Caveats:** Many ways to configure 3PIP to violate constraints, assumptions. Need capabilities for HW-SW analysis.

Level of experience and training matters

- We were more effective and knowledgeable of design as time went on. Don't always have that time.

Application and integration of IP matters

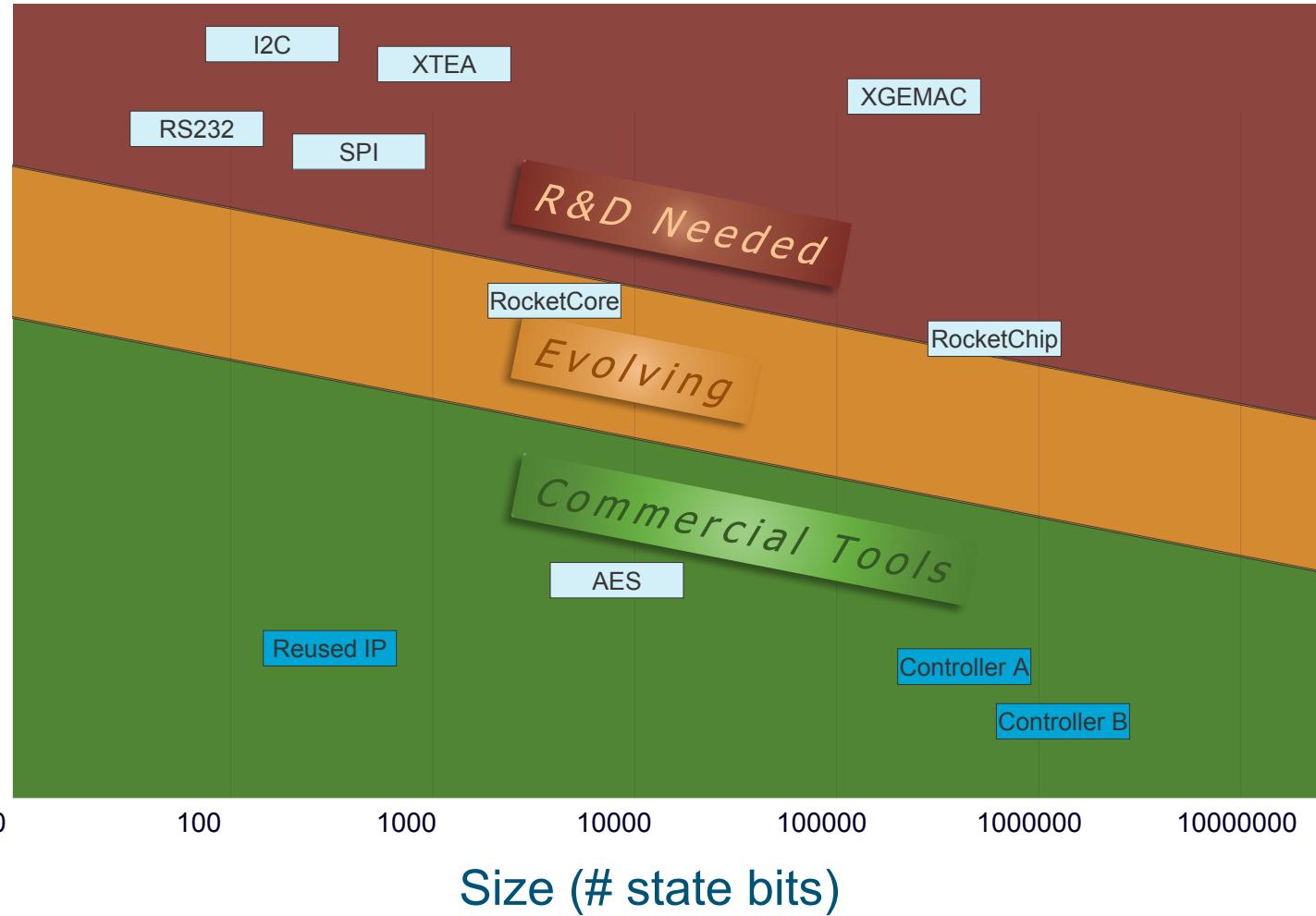
State of the Practice for 3PIP Assurance

Source Format

Netlist

Generated
HDL

HDL





Track Developments

Accellera Systems Initiative:
Security Assurance for Electronic
Design Integration Standard

(rev 1.0, July 2021)



Target Relevant 3PIP

Inform best practices for
Quantifiable Assurance (5200.xx)



Evaluate Tools

Incorporate tools into assessment
workflows

Joint Federated Assurance Center (JFAC)



The JFAC is a federation of DoD organizations that promotes and enables software and hardware assurance by providing expertise and support to defense acquisition programs and supporting activities.

JFAC Portal:

<https://jfac.navy.mil>

SharePoint Site:

<https://intelshare.intelink.gov/sites/jfac>

Contact

Vivian Guzman Kammler | R&D Cybersecurity Lead | Sandia National Laboratories

vgkamml@sandia.gov | +1 505 284 3528