osmosis

onespin meeting on solutions, innovation, & strategy

Presented by OneSpin: A Siemens Business

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 **be available for use when needed**

never **go off unless authorized**

A Transition…

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"

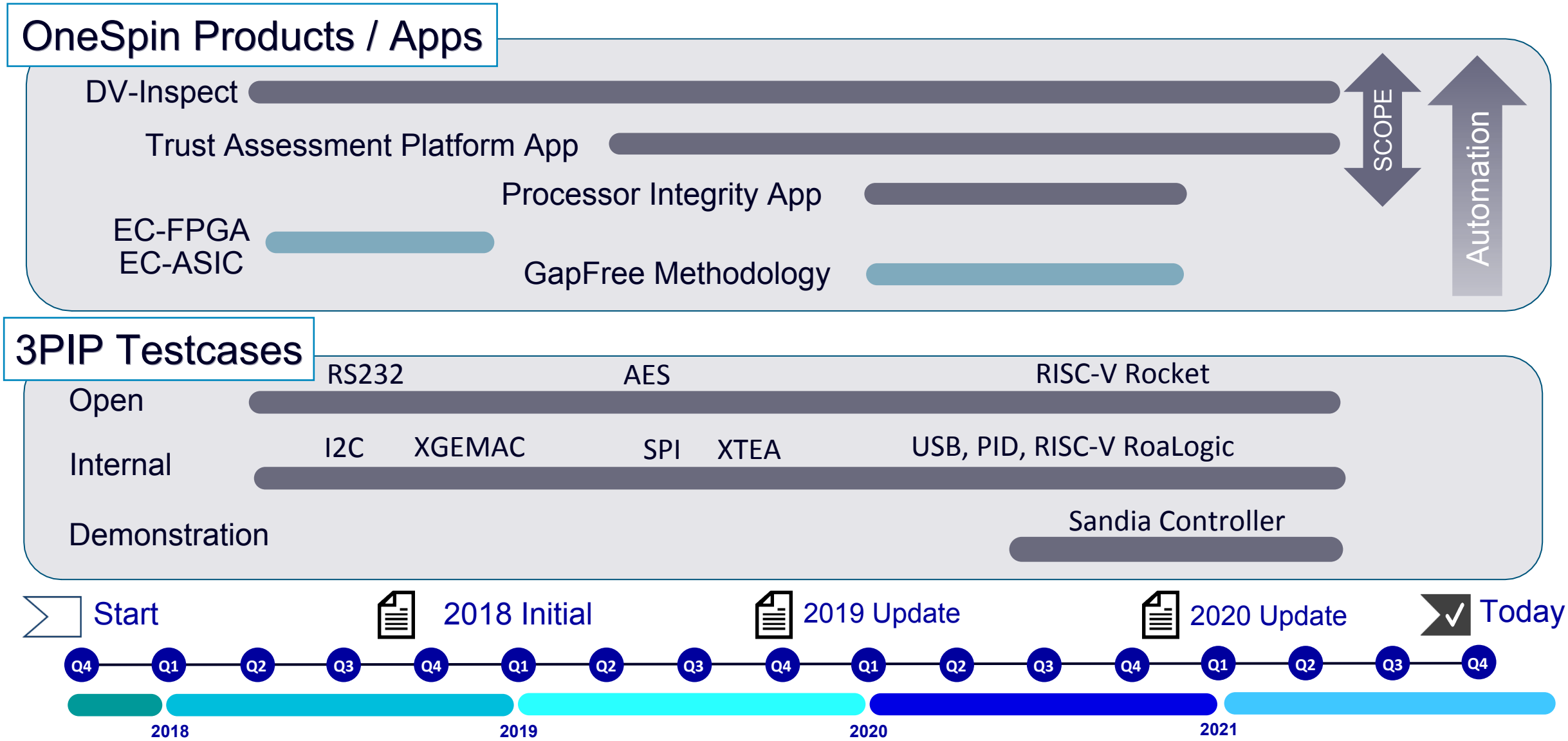
- **3PIP is not encrypted**
- **3PIP can be parsed by analysis tools**
- **Automation**
- ***Evaluator has limited design knowledge***
- ***There is no "golden" model (known good)***

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)***

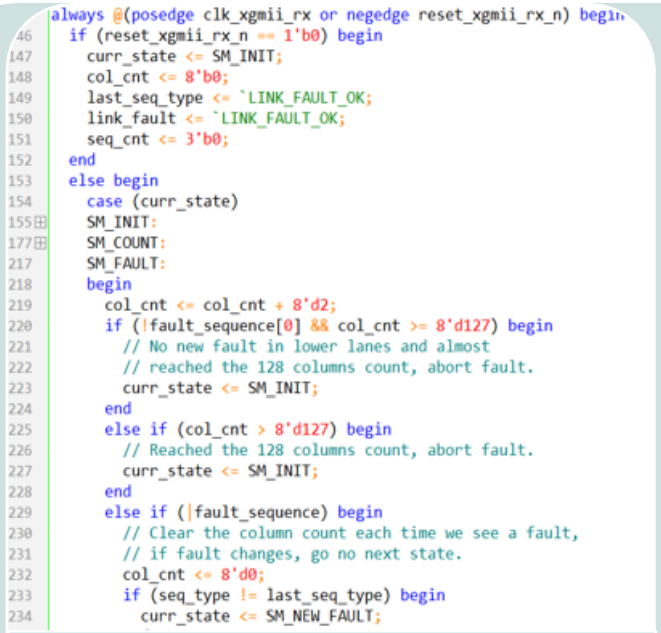
Evaluating OneSpin Tools for Assurance of 3PIP



How is 3PIP provided?

OneSpin tools most useful here

1 – based on ethernet MAC
2 – based on RISC-V RocketCore



HDL

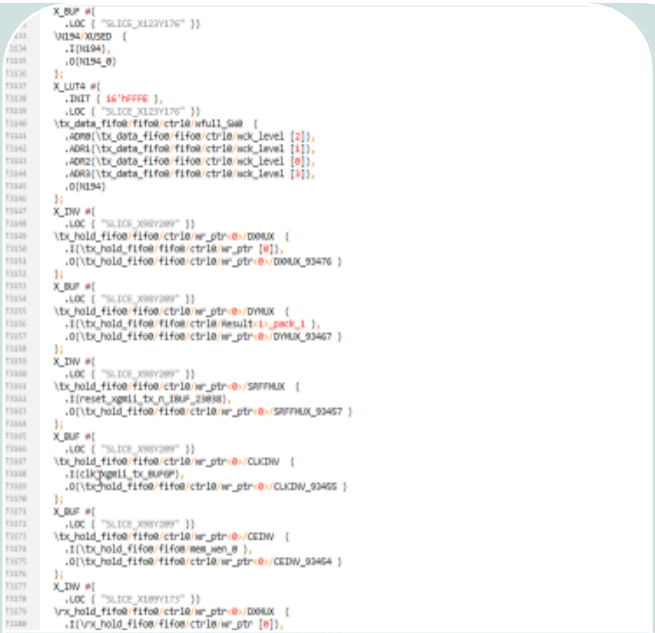
28

state bits/line of code[1]

Generated HDL

0.4

state bits/line of code[2]

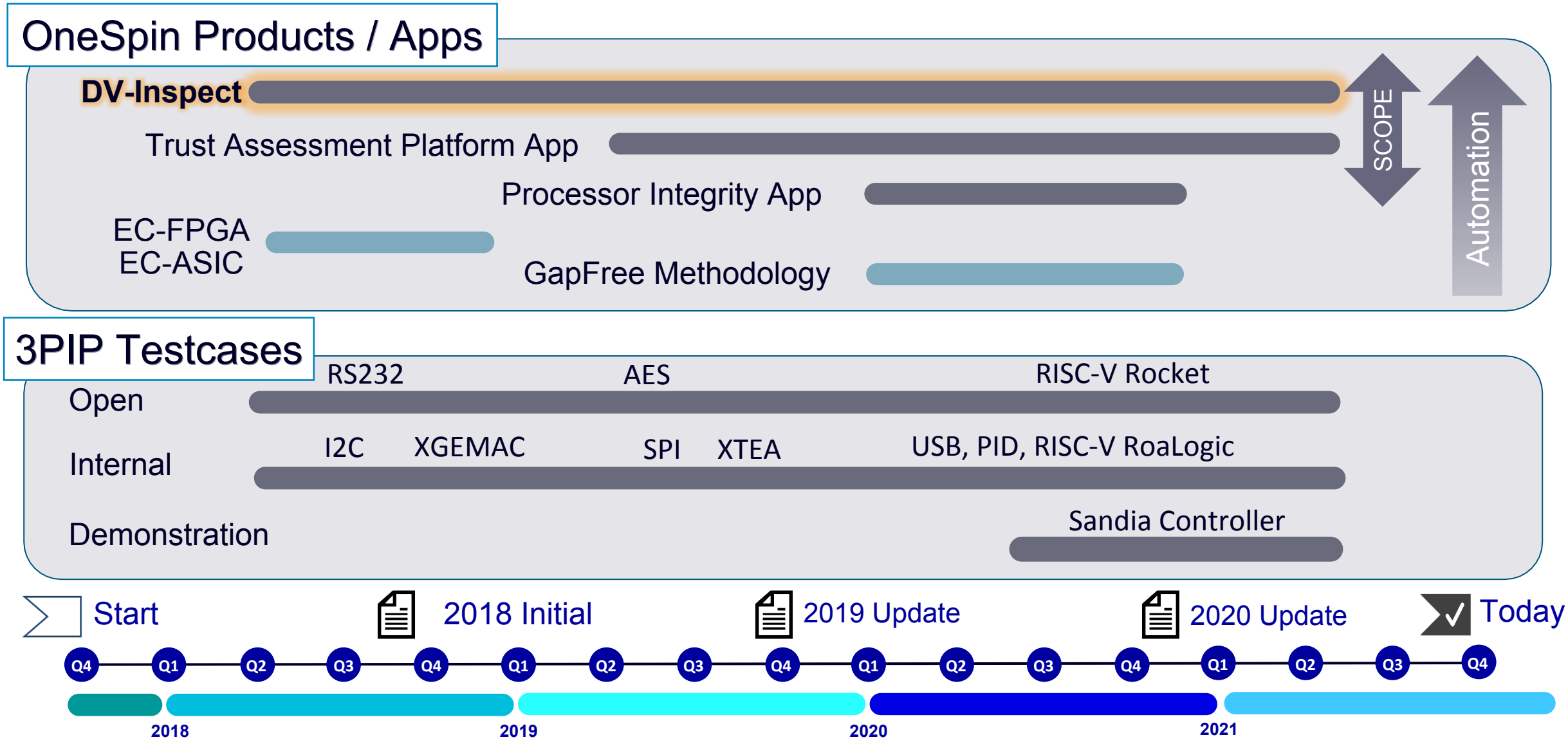


Netlist

1.3

state bits/line of code[1]

Evaluating OneSpin Tools for Assurance of 3PIP



DV-Inspect Autochecks

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

DV-Inspect Autochecks

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

Useful as a first step

Enforces good coding habits

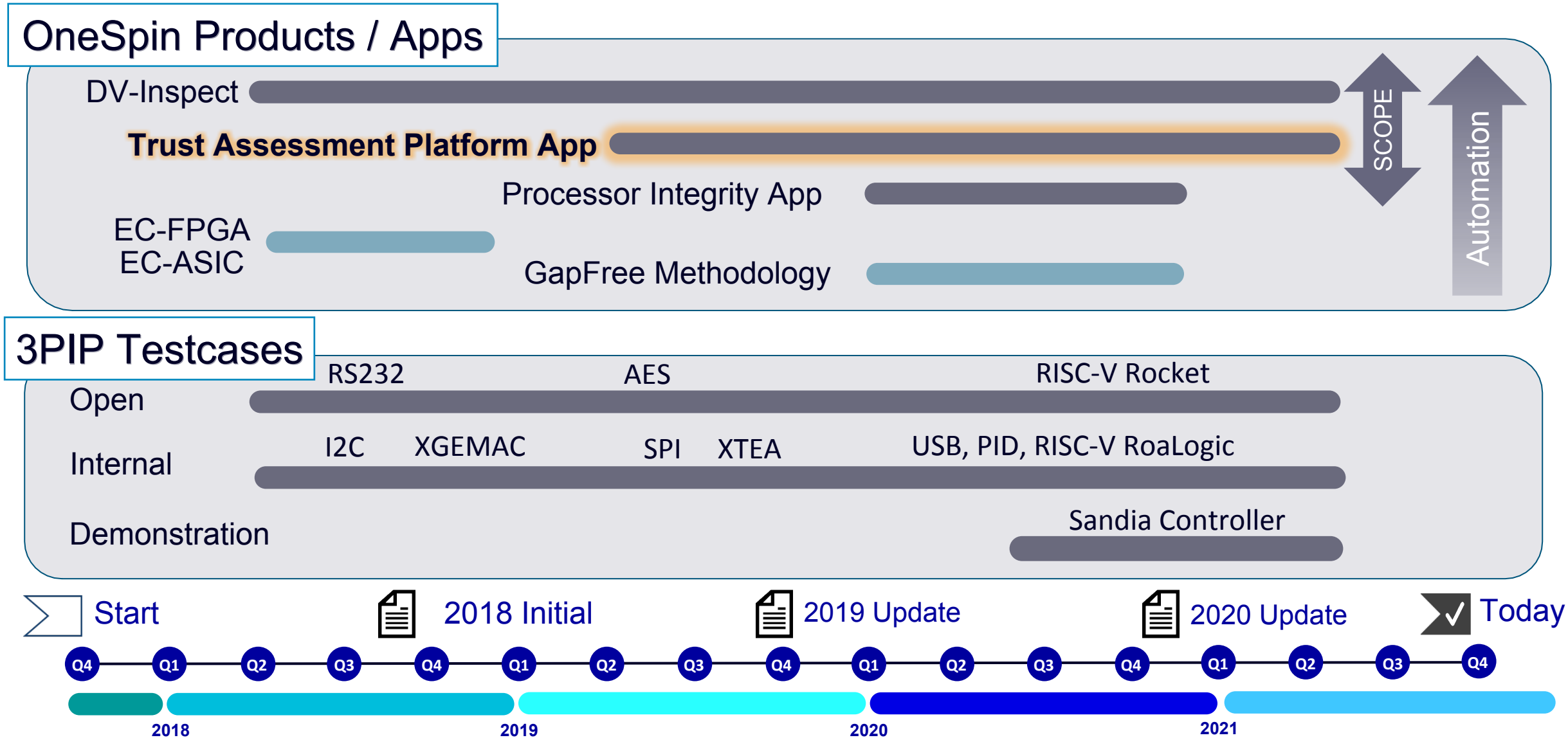
Which of these checks are assurance-relevant?

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.

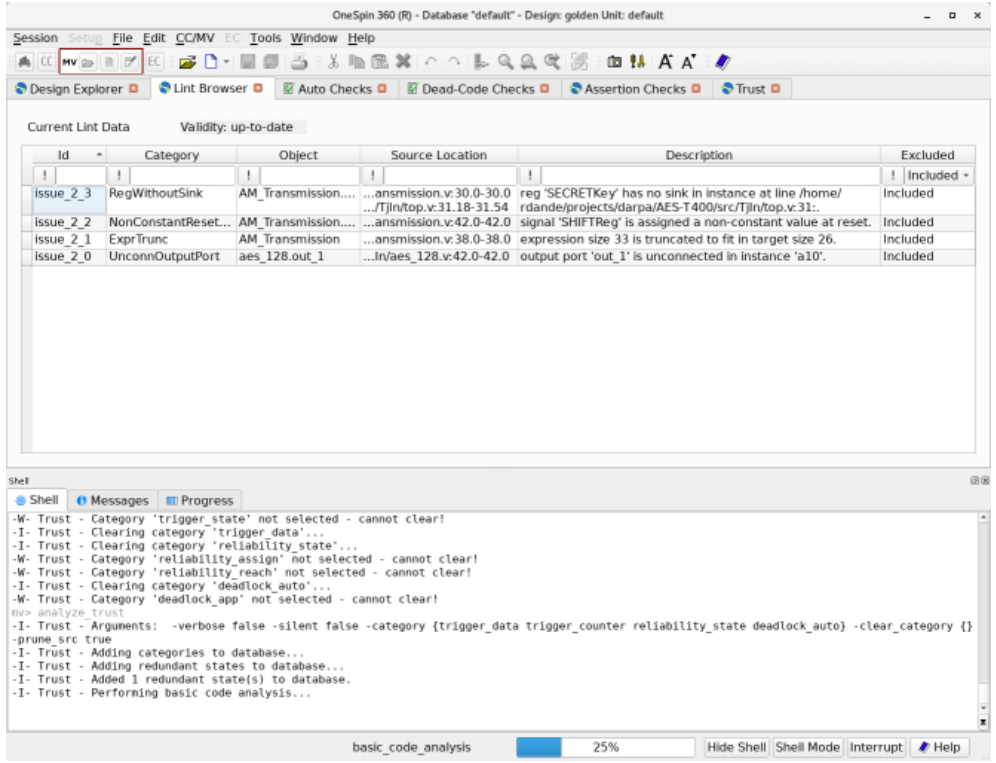
Evaluating OneSpin Tools for Assurance of 3PIP



Trust Assessment Platform (TAP) v2021.1.0

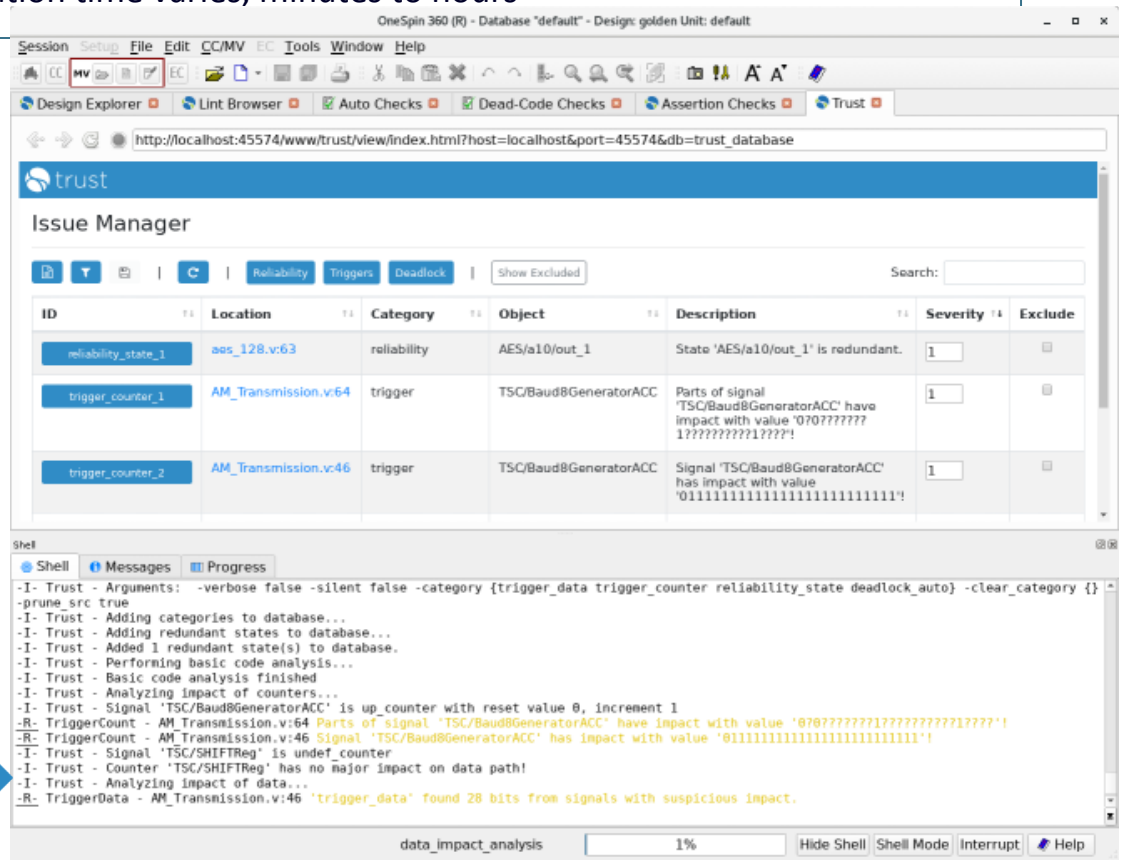
Lint browser (DV-Inspect)

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



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***

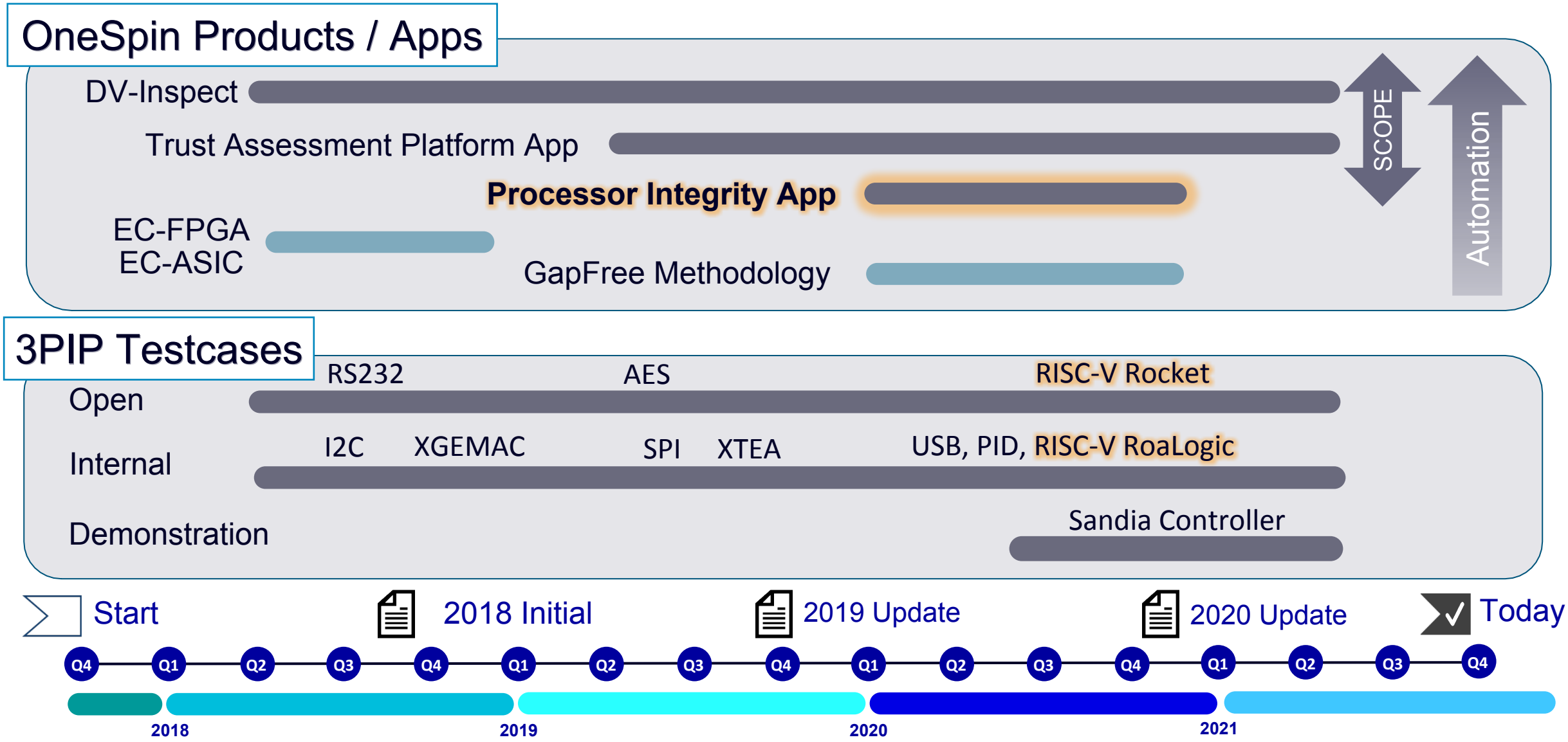
* TrustHub designs averaged results over multiple articles
** Aerospace designs contained 1 golden, 3 with Trojans
*** Leon3 articles consisted of 3 Trojan designs, 1/3 Trojans discovered
(Results were from OneSpin TAP ~~2020~~ 2020.2

- 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

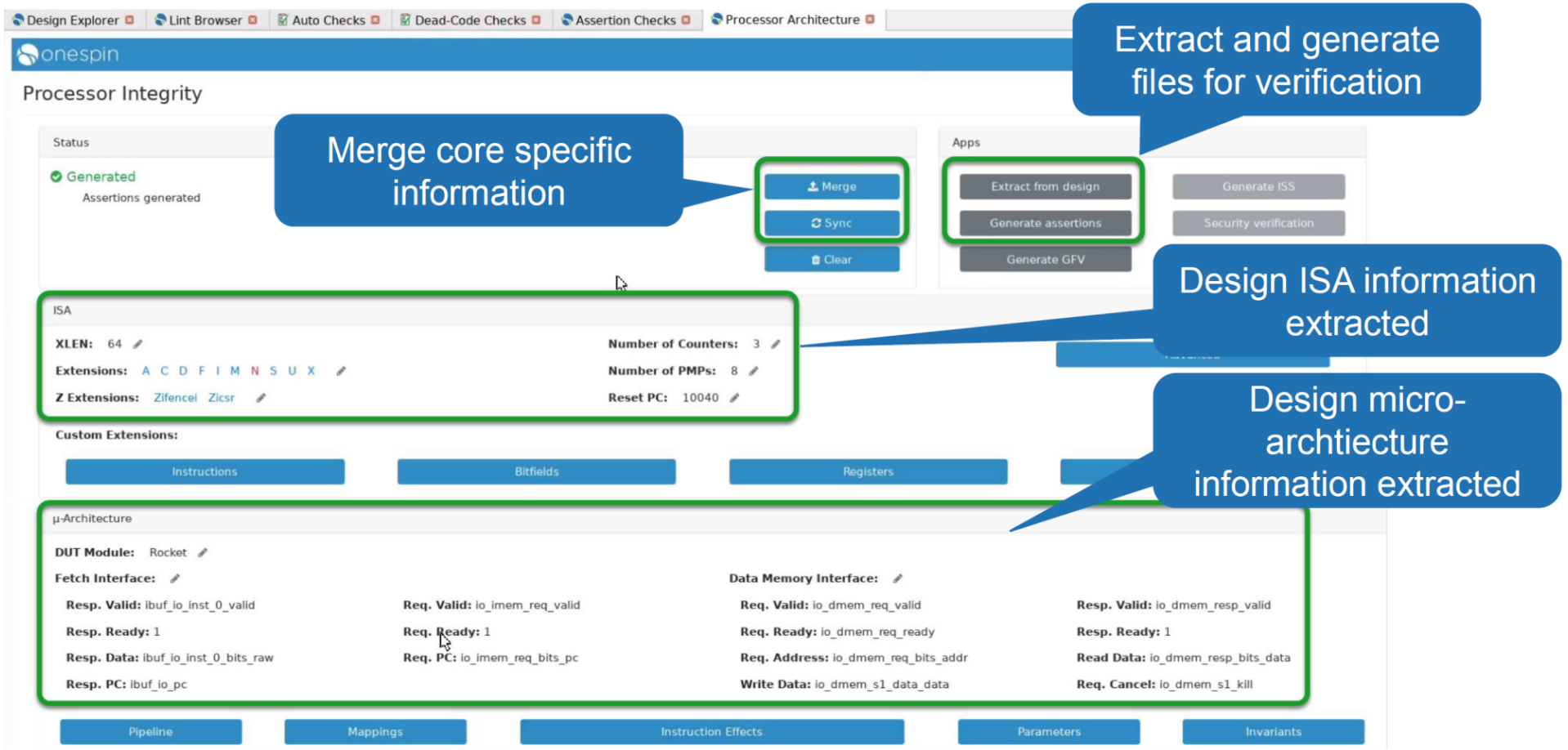
Evaluation of OneSpin Trust Assessment for Hardware Trojan Detection. Chan, Garrett and Rao, Vikram. Aerospace. Osmosis for DoD 2020.

- 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

Evaluating OneSpin Tools for Assurance of 3PIP



Processor Integrity App v2020.2



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	Witness Status	Prover	Runtime
!	! <any status>	! <any s		
Properties				
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	
RV_chk.ops.RV32I.Branch_a	hold	pass (2)		
RV_chk.ops.RV32I.CallBreak_a	fail (7)	pass (2)	disprover1	00:06:09
RV_chk.ops.RV32I.CSR_a	fail (2)	pass (2)	disprover3	00:02:11
RV_chk.ops.RV32I.FENCE_a	hold	pass (2)	approver1:0	00:00:34
RV_chk.ops.RV32I.FENCE_I_a	fail (2)	pass (2)	disprover3	00:01:28
RV_chk.ops.RV32I.Jump_a	hold		approver1:0	00:02:52
RV_chk.ops.RV32I.LUI_a	hold	pass (2)		
RV_chk.ops.RV32I.Mem_a	hold	pass (2)	approver1:0	
RV_chk.ops.RV32I.RET_a	hold	pass (2)	approver1:0	00:00:34
RV_chk.ops.RV32I.Supervisor.SFENCE_VMA_a	hold	pass (2)	approver1:0	00:01:14
RV_chk.ops.RV32M.all_a	hold	pass (2)	approver1:0	00:01:27
RV_chk.ops.RV64A.all_a	hold	pass (2)	approver1:0	00:01:13
RV_chk.ops.RV64D.all_a	hold	pass (7)	approver1:0	00:01:06
RV_chk.ops.RV64F.all_a	hold	pass (7)	approver1:0	00:00:53
RV_chk.ops.RV64I.Arith_a	hold	pass (2)	approver1:0	00:03:41
RV_chk.ops.RV64I.Mem_a	hold	pass (2)	approver1:0	00:02:18
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

RISC-V Testcase Support Dec 2020

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

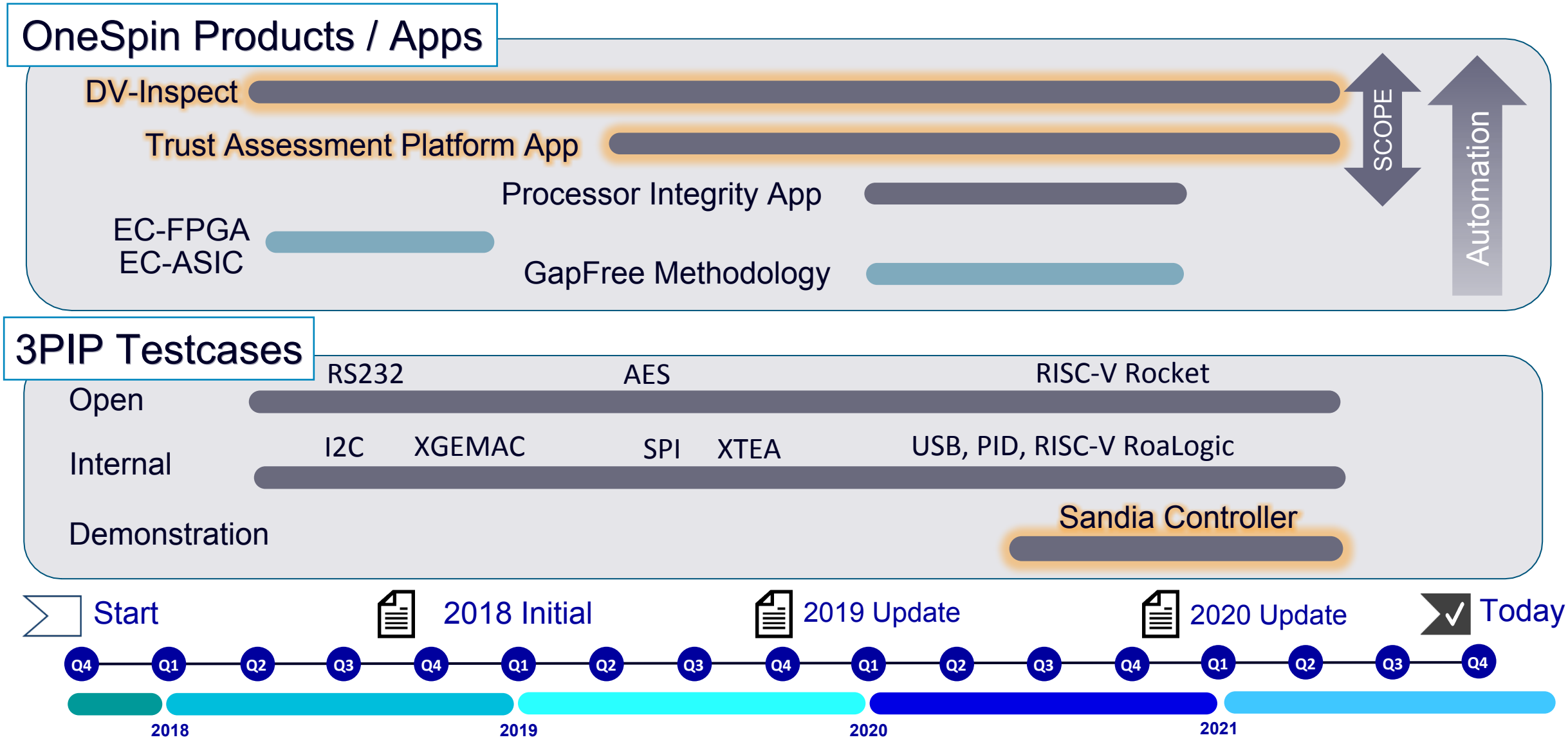
https://github.com/RoaLogic/RV12

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

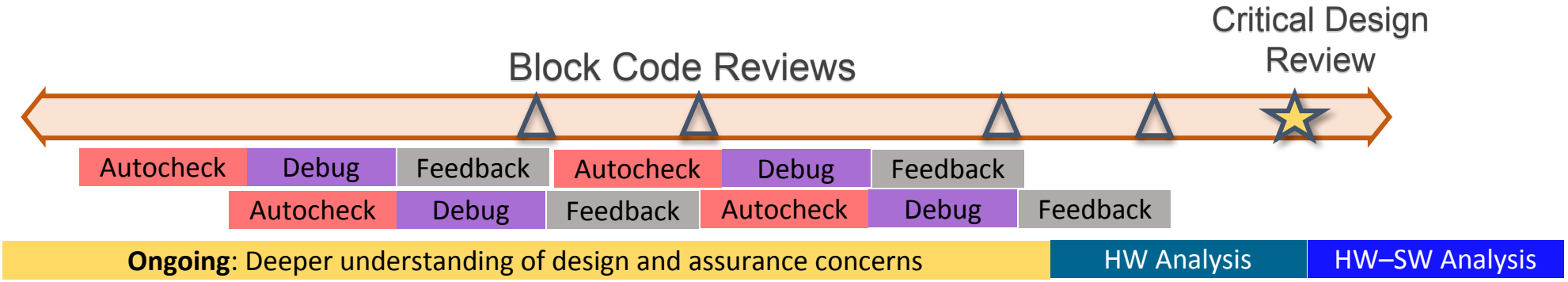
→ ***Others should expect to work with OneSpin for new processor configurations***

** 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



Tool Workflow in Practice



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

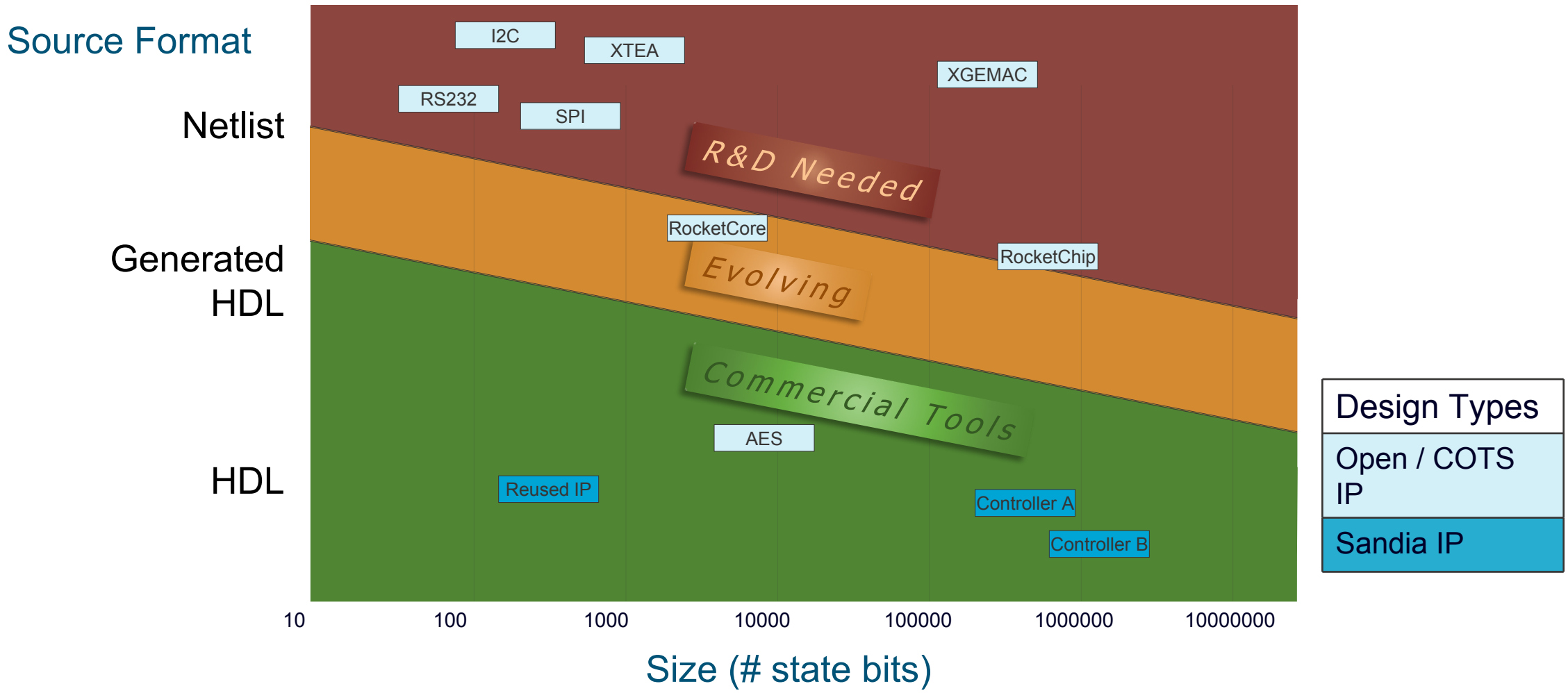
- **Caveats**: Many ways to configure 3PIP to violate constraints, assumptions. Need capabilities for HW-SW analysis.

Level of experience and training matters

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

Application and integration of IP matters

State of the Practice for 3PIP Assurance



What's Next?

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)

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