An Automated Pre-silicon IP Trustworthiness Assessment for Hardware Assurance

J. Hallman, D. Landoll, S. Marchese, S. Beyer - OneSpin Solutions
G. Chan, S. Zantout, V. Rao – Aerospace Corporation

accellera SYSTEMS INITIATIVE™

2020 DESIGN AND VERIFICATION™ DVCON CONFERENCE AND EXHIBITION EUROPE

CAN YOU TRUST THIRD-PARTY IPs?

Using (third-party) IPs is crucial for cost-effective IC and SoC design

Risks

- IPs could contain security vulnerabilities and undocumented, malicious logic
- Hardware Trojans can be inserted at various stages during the IP design cycle

In security- and safety-critical chips these risks must be managed

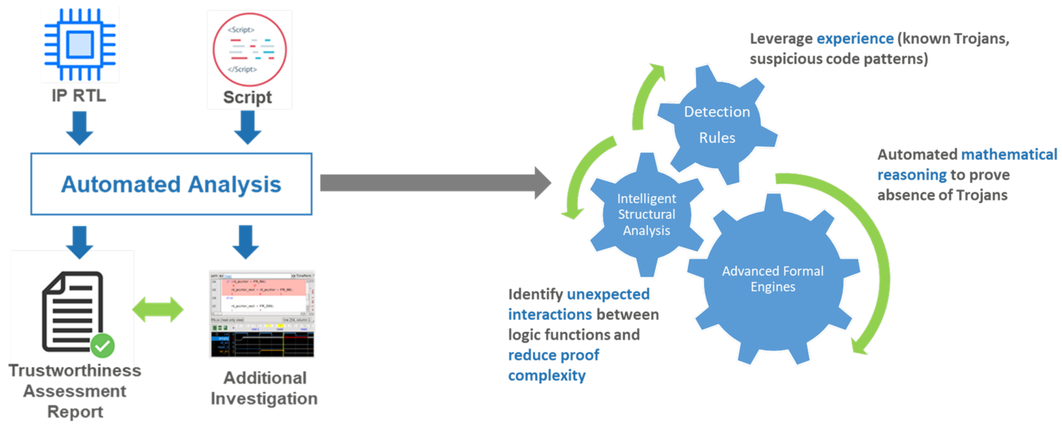
Challenges

- IPs are complex – SoC Integrators don't know the details
- RTL code review is effort-intensive and likely to miss issues
- Limited engineering resources, expertise, tools

AUTOMATED TRUSTWORTHINESS ASSESSMENT

Highlights

- No trusted/independent IP model is required
- No formal verification or IP expertise required
- Automated, repeatable, objective assessment process
- Leverage unique technology and expertise under-the-hood



RESULTS

Test suite

- 90 designs with and without Trojans inserted
- Size range: 100 to 100K FFs

Source	Name	Runtime	Issues Reported	Trojan Inserted	Automatic Detection
TrustHub*	AES	11 hours	260	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***

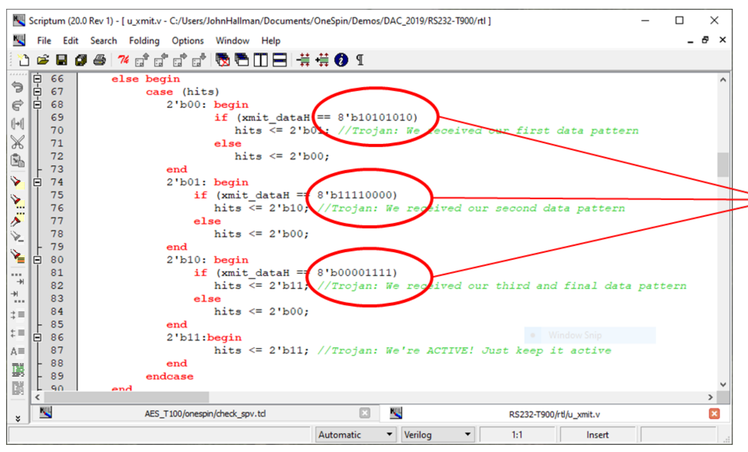
* TrustHub designs averaged results over multiple articles
** Aerospace designs contained 1 golden, 3 with Trojans
*** Leon3 articles consisted of 3 Trojan designs, 1/3 Trojans discovered

Results

- Representative selection of IP designs
- Few trigger-type issues reported
- Numerous reliability issues reported
- Very few false alarms
- Some Trojans have been missed
- Runtime is short

EXAMPLE OF DETECTED TROJAN

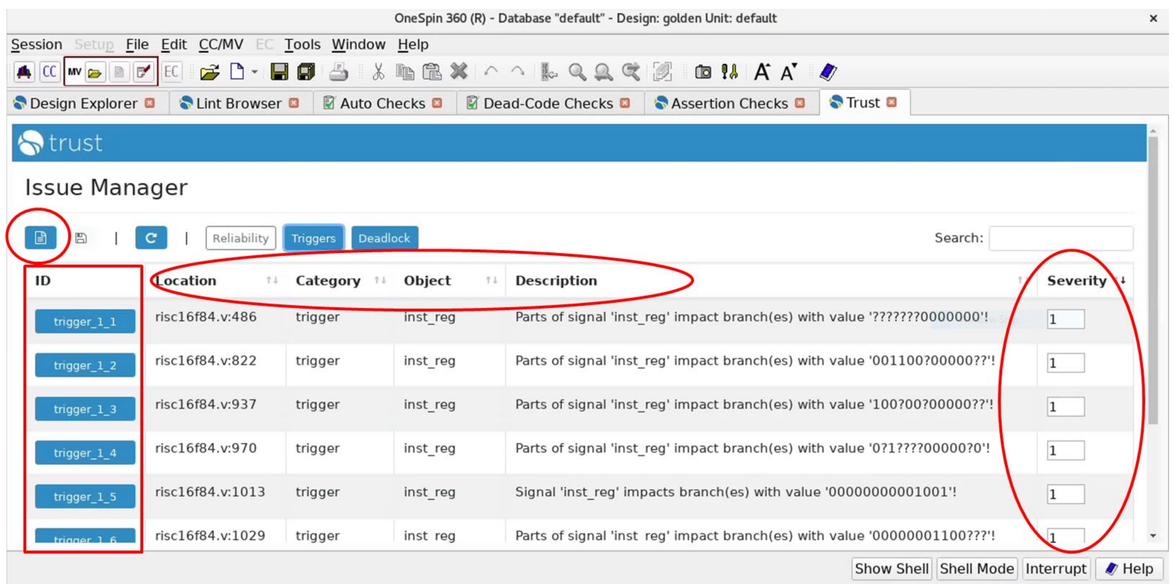
- Triggers based on deep counters
- Specific sequences of events triggering unusual control action
- FSM with malicious logic monitoring the occurrence of specific data sequence



Trojan triggers on data sequence 0xAA, 0xF0, 0x0F

SIGNOFF ASSESSMENT REPORT

Concise - Actionable - Customizable - Issues linked to IP model



CONCLUSION

IP trustworthiness is a rising concern

- A vulnerability or hardware Trojan can compromise the security of the entire system

Automated trustworthiness assessment

- Provides a low-effort, objective approach to increase confidence that IP is trustworthy
- Does not require additional IP model or detailed IP knowledge
- Algorithms need continuous improvement
- Low noise level (false alarms) is key

Process limitations

- No trustworthiness metric (open industry topic)
- Detects Trojans, but cannot prove absence of all functional Trojans

AEROSPACE

To learn more contact
john.hallman@onespin.com

onespin