CISPA
HELMHOLTZ CENTER FOR INFORMATION SECURITY

TwinFuzz: Differential Testing of Video Hardware Acceleration Stacks

Matteo Leonelli, *Addison Crump, Meng Wang, Florian Bauckholt, Keno Hassler, Ali Abbasi, Thorsten Holz*

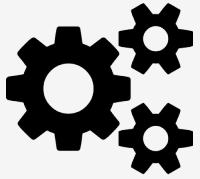
NDSS SYMPOSIUM

NDSS 2025 | CISPA Helmholtz Center for Information Security

Software Fuzzing

image: Flaticon.com

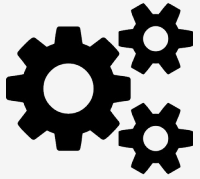
Software Fuzzing



Fuzzer

image: Flaticon.com

Software Fuzzing



Fuzzer

Instrumented
Binary

image: Flaticon.com

Software Fuzzing

 image: Flaticon.com

Software Fuzzing

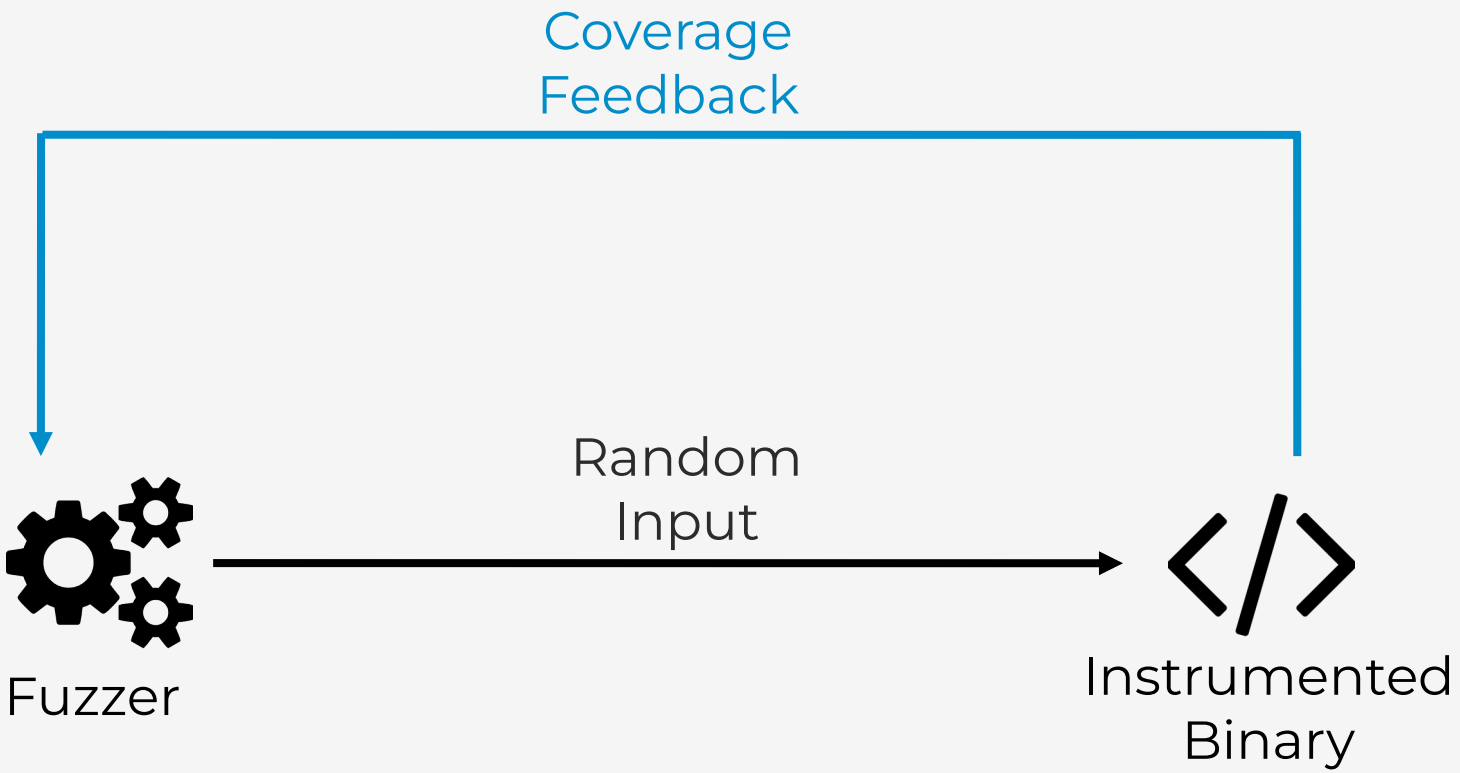


 image: Flaticon.com

Software Fuzzing

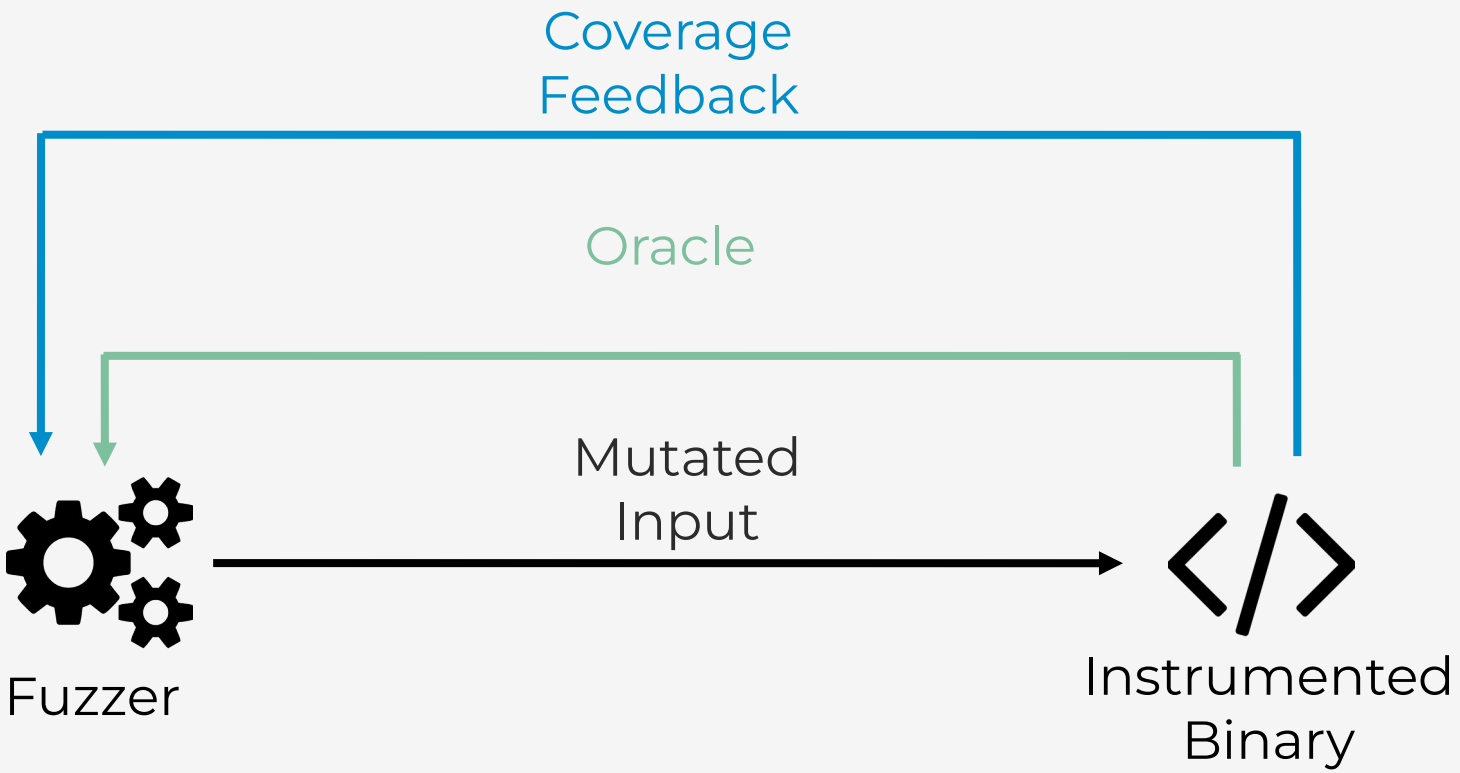


 image: Flaticon.com

Software Fuzzing

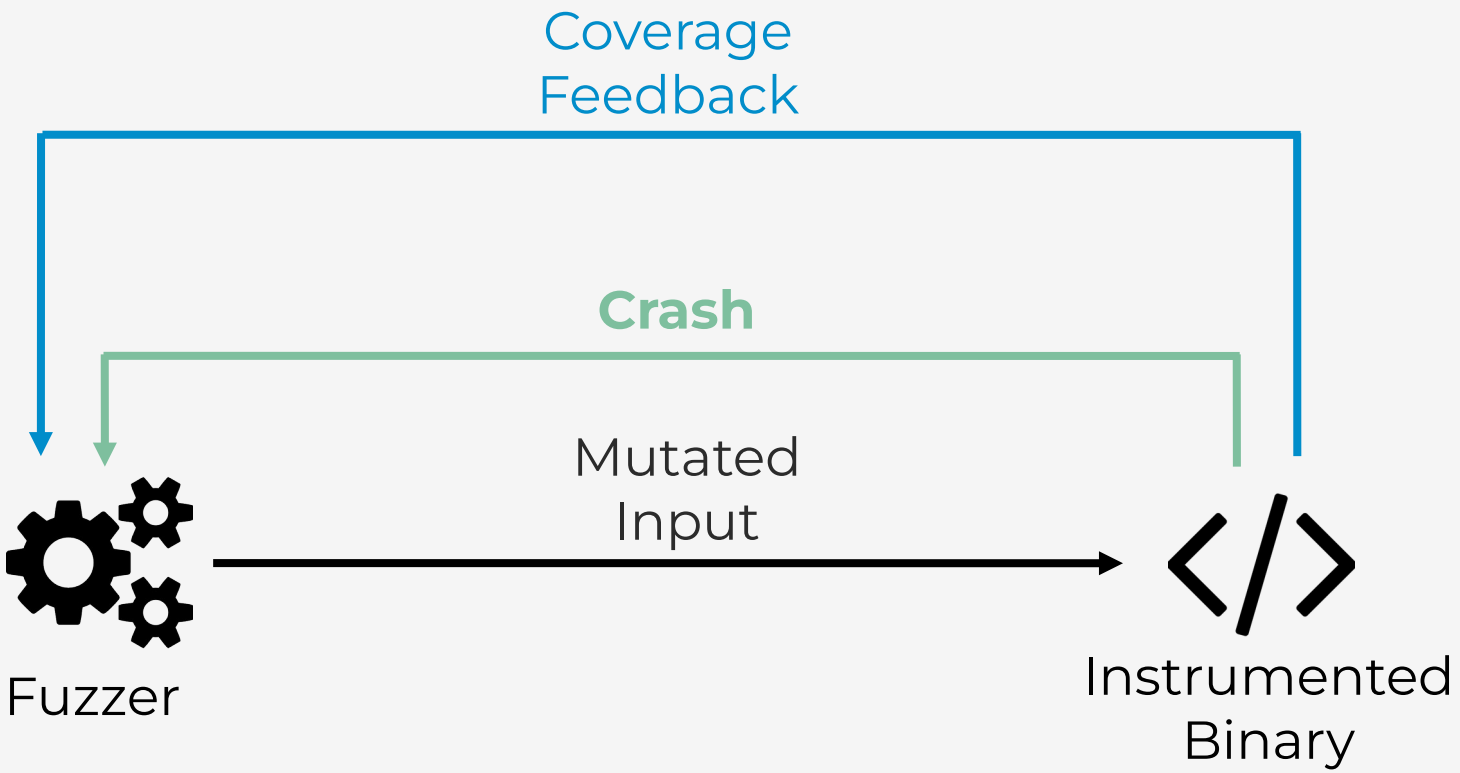
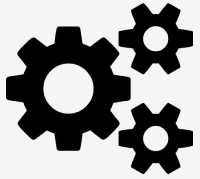


 image: Flaticon.com

Hardware Fuzzing

 image: Flaticon.com

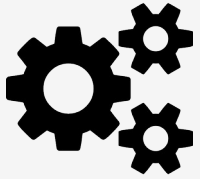
Hardware Fuzzing



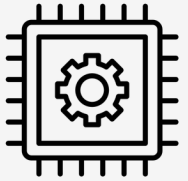
Fuzzer

image: Flaticon.com

Hardware Fuzzing



Fuzzer



Black-Box
Hardware

image: Flaticon.com

Hardware Fuzzing

image: Flaticon.com

Hardware Fuzzing

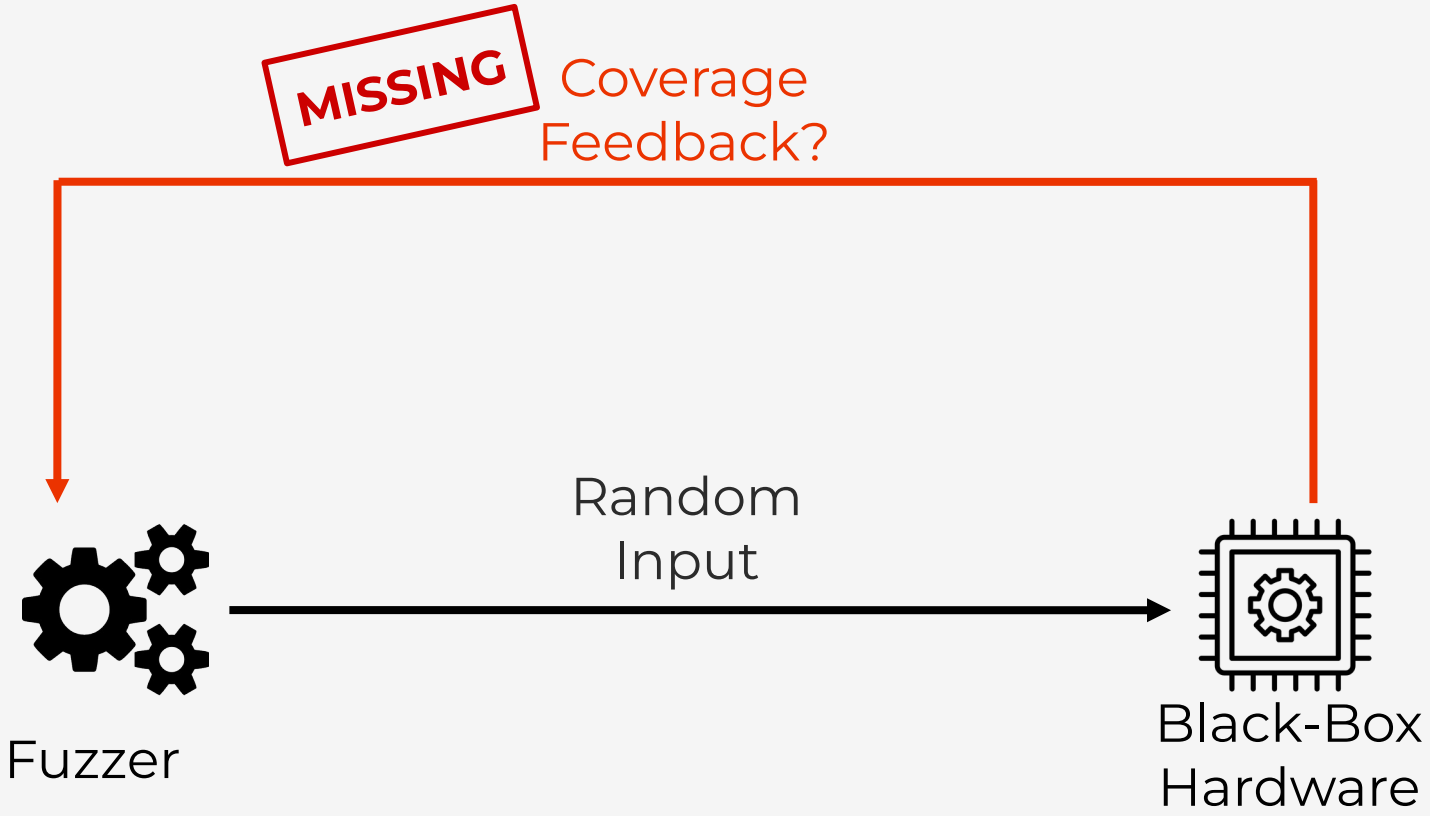


image: Flaticon.com

Hardware Fuzzing

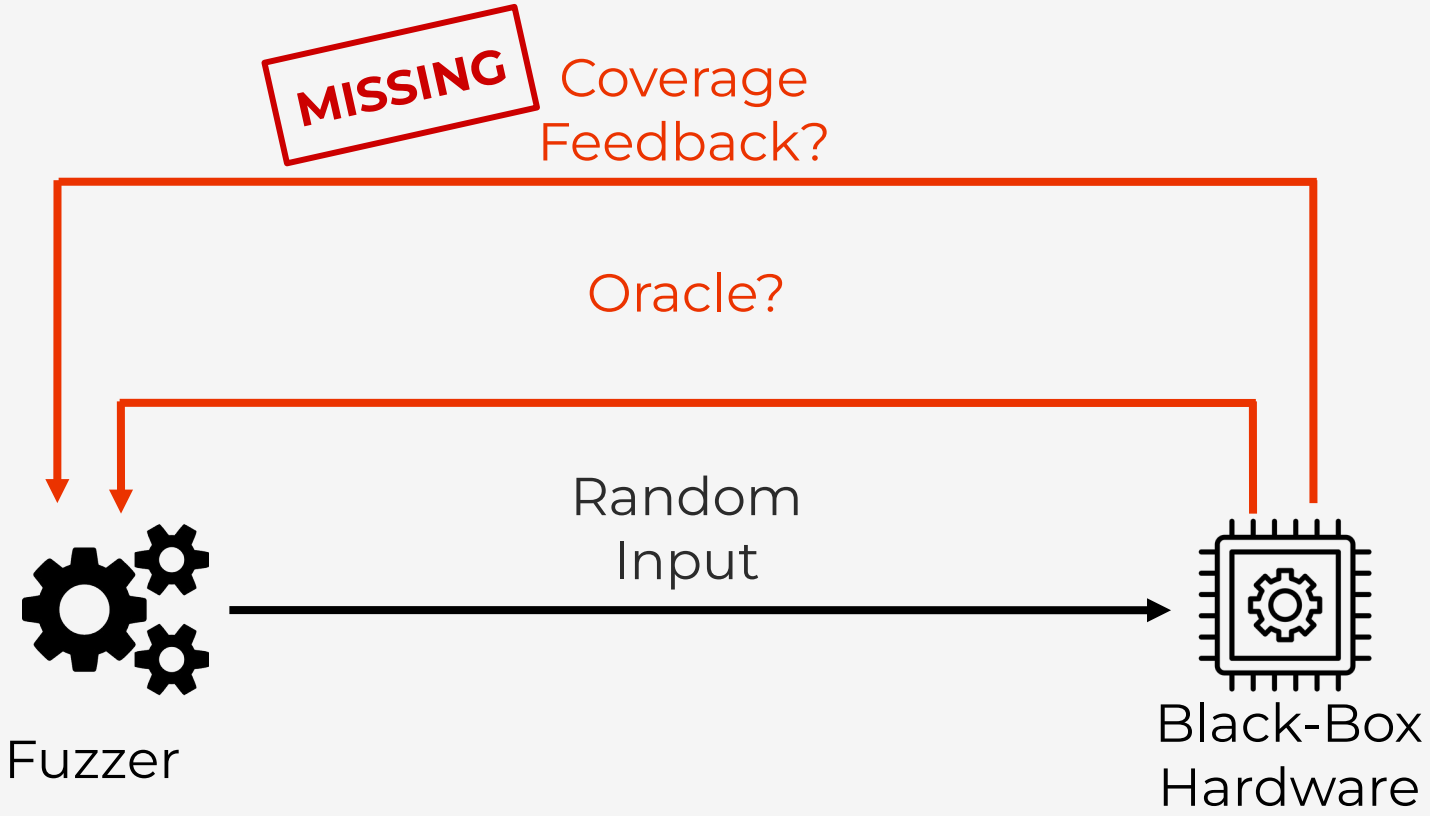


image: Flaticon.com

Hardware Fuzzing

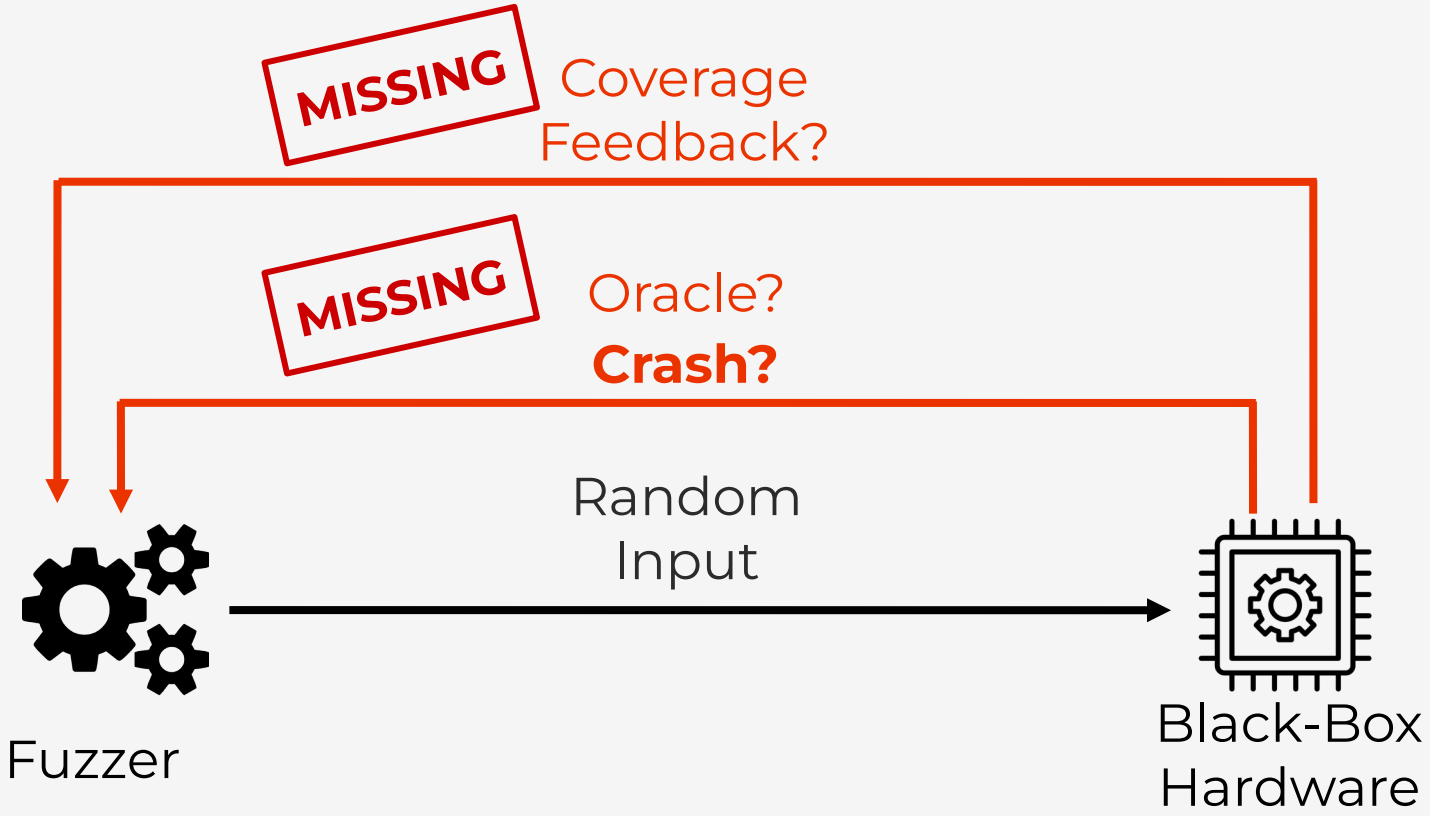
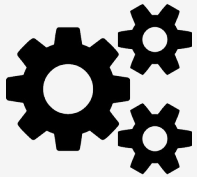


image: Flaticon.com

Differential Testing

image: Flaticon.com

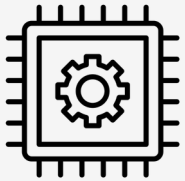
Differential Testing



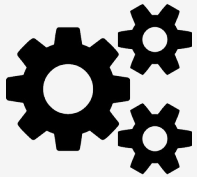
Fuzzer

image: Flaticon.com

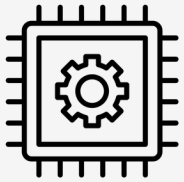
Differential Testing



Hardware’



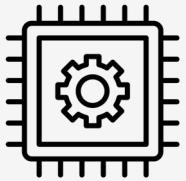
Fuzzer



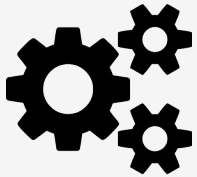
Hardware’’

image: Flaticon.com

Differential Testing

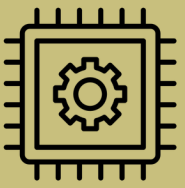


Hardware’



Fuzzer

Reference Model



Hardware’’

image: Flaticon.com

Differential Testing

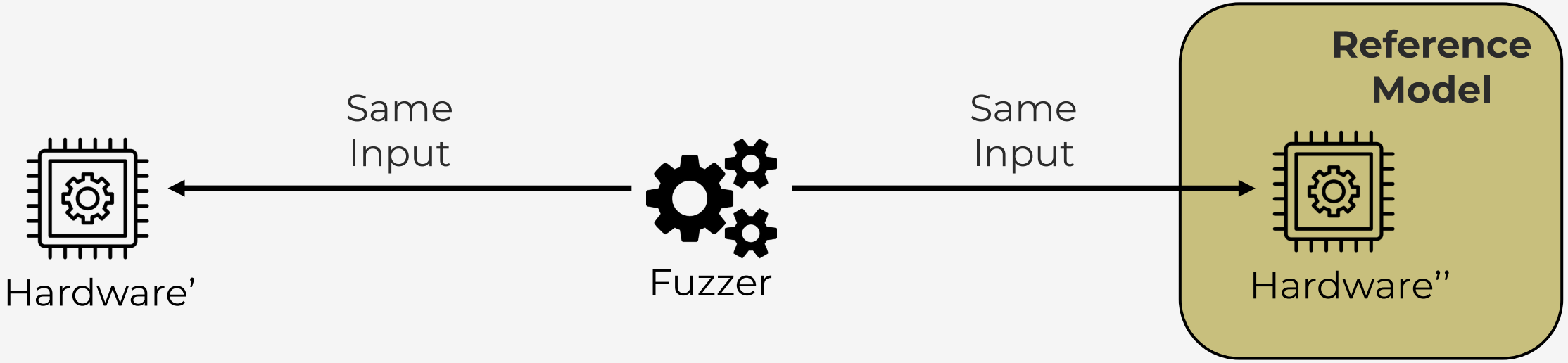


 image: Flaticon.com

Differential Testing

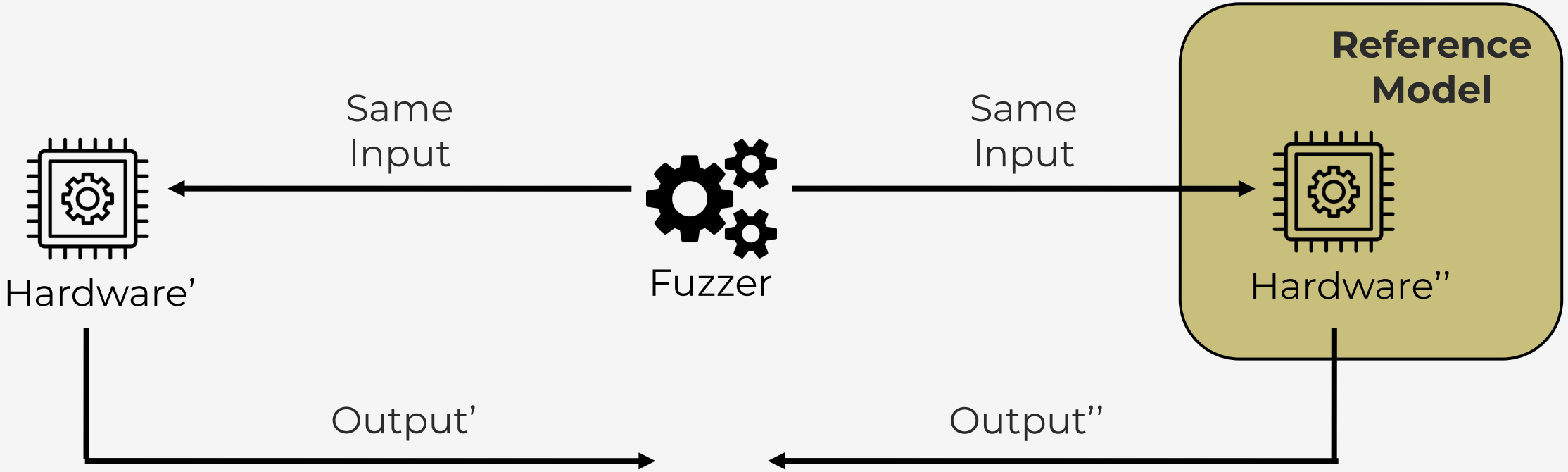


image: Flaticon.com

Differential Testing

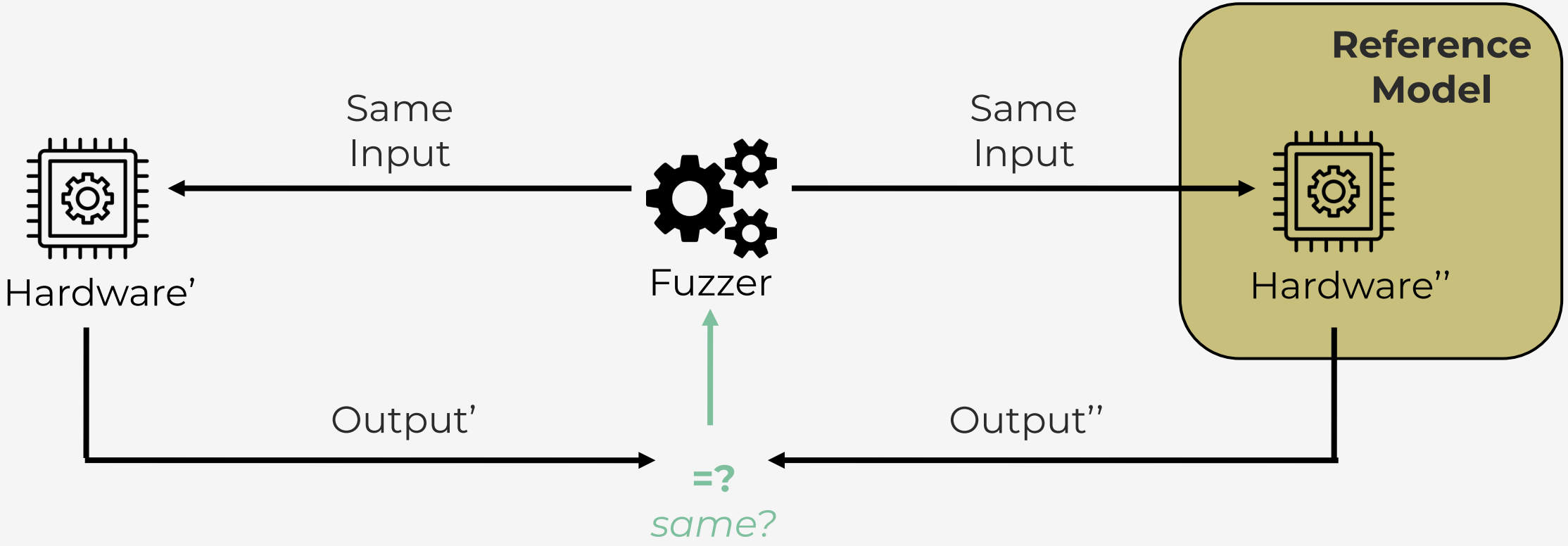
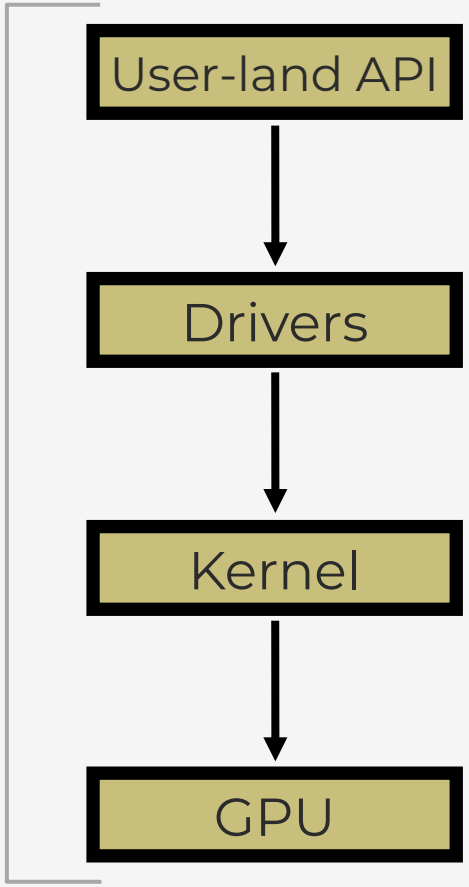


image: Flaticon.com

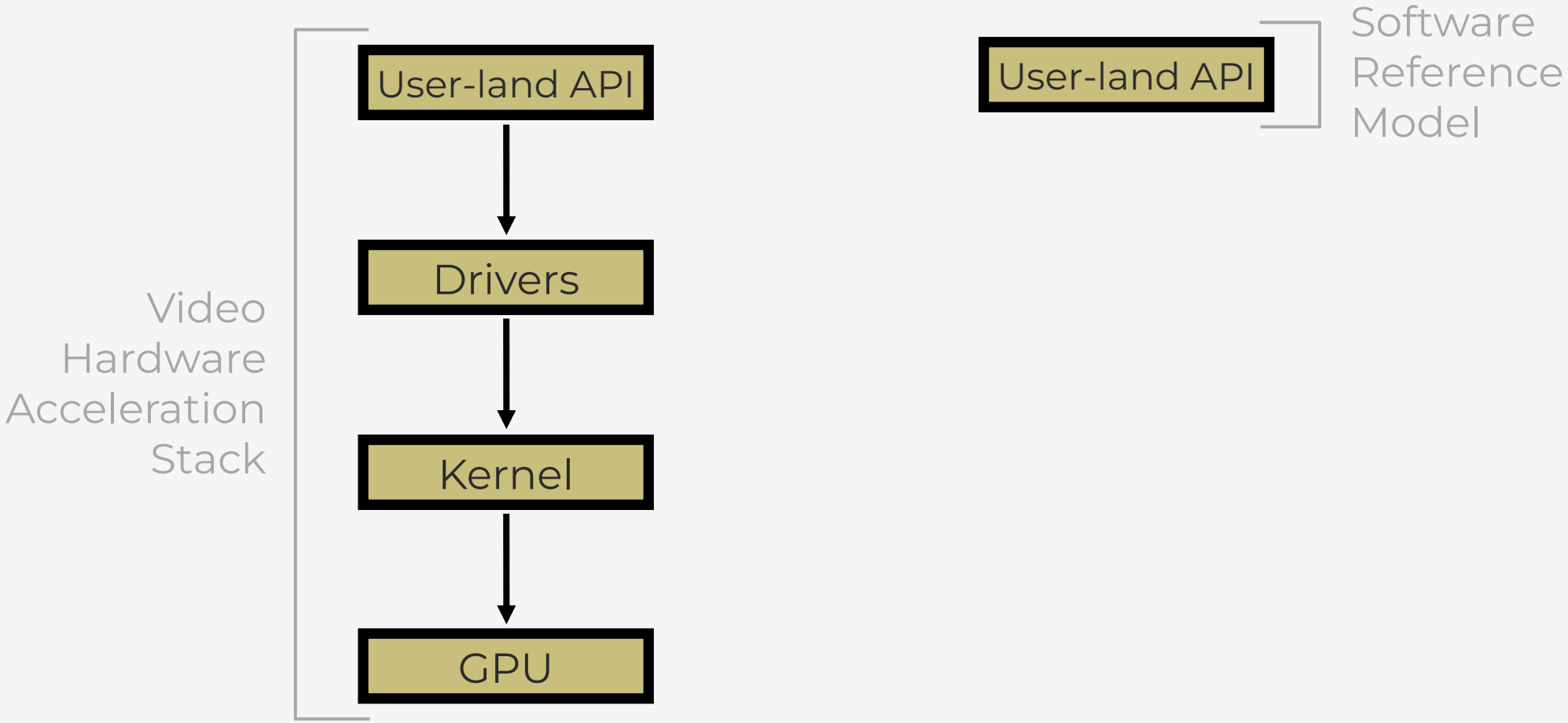
Video Decoding Models

Video Decoding Models

Video Hardware Acceleration Stack



Video Decoding Models



TwinFuzz Challenges

TwinFuzz Challenges

CH 1

Define a **new oracle** for hardware-accelerated stack

TwinFuzz Challenges

CH 1

Define a **new oracle** for hardware-accelerated stack

CH 2

Define a **feedback mechanism** for hardware-accelerated stack

TwinFuzz Challenges

CH 1 — Define a **new oracle** for hardware-accelerated stack

CH 2 — Define a **feedback mechanism** for hardware-accelerated stack

CH 3 — Analyze the **observable differences**

CH 1: Differential Oracle for Video Hardware Acceleration Stack

image: Flaticon.com

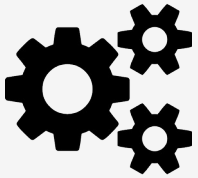
CH 1: Differential Oracle for Video Hardware Acceleration Stack

CH 1

Define a **new oracle** for hardware-accelerated stack

image: Flaticon.com

CH 1: Differential Oracle for Video Hardware Acceleration Stack



Fuzzer

image: Flaticon.com

CH 1: Differential Oracle for Video Hardware Acceleration Stack

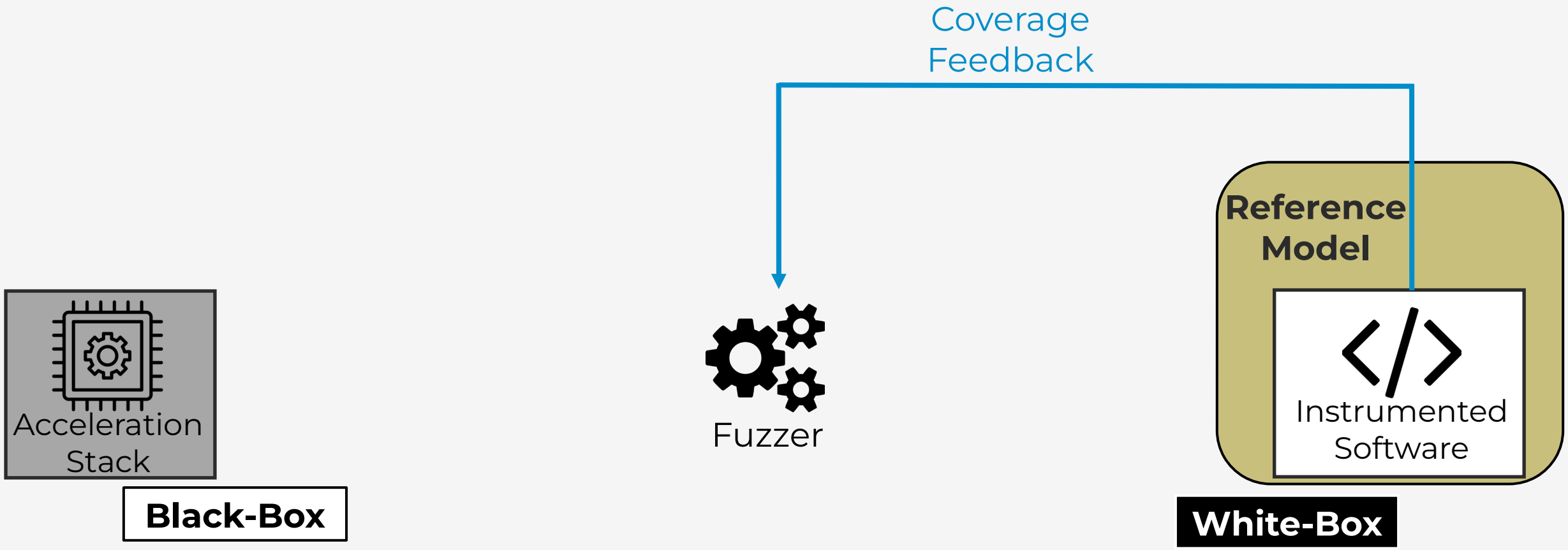


image: Flaticon.com

CH 1: Differential Oracle for Video Hardware Acceleration Stack

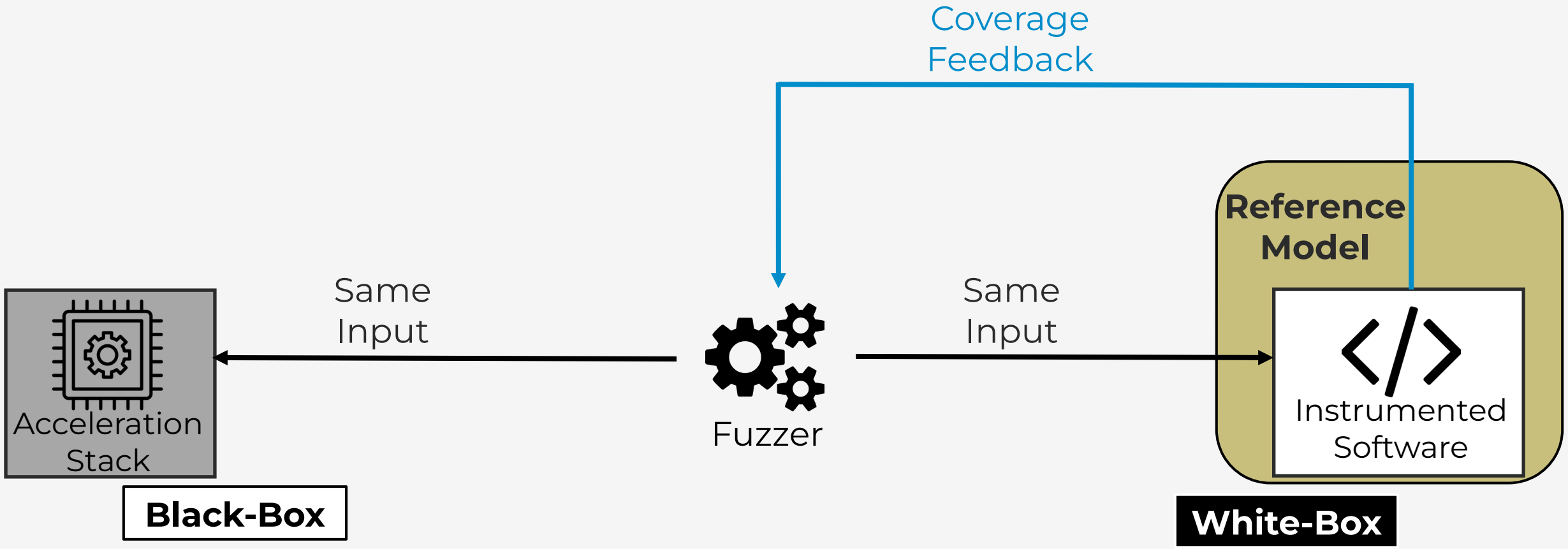


image: Flaticon.com

CH 1: Differential Oracle for Video Hardware Acceleration Stack

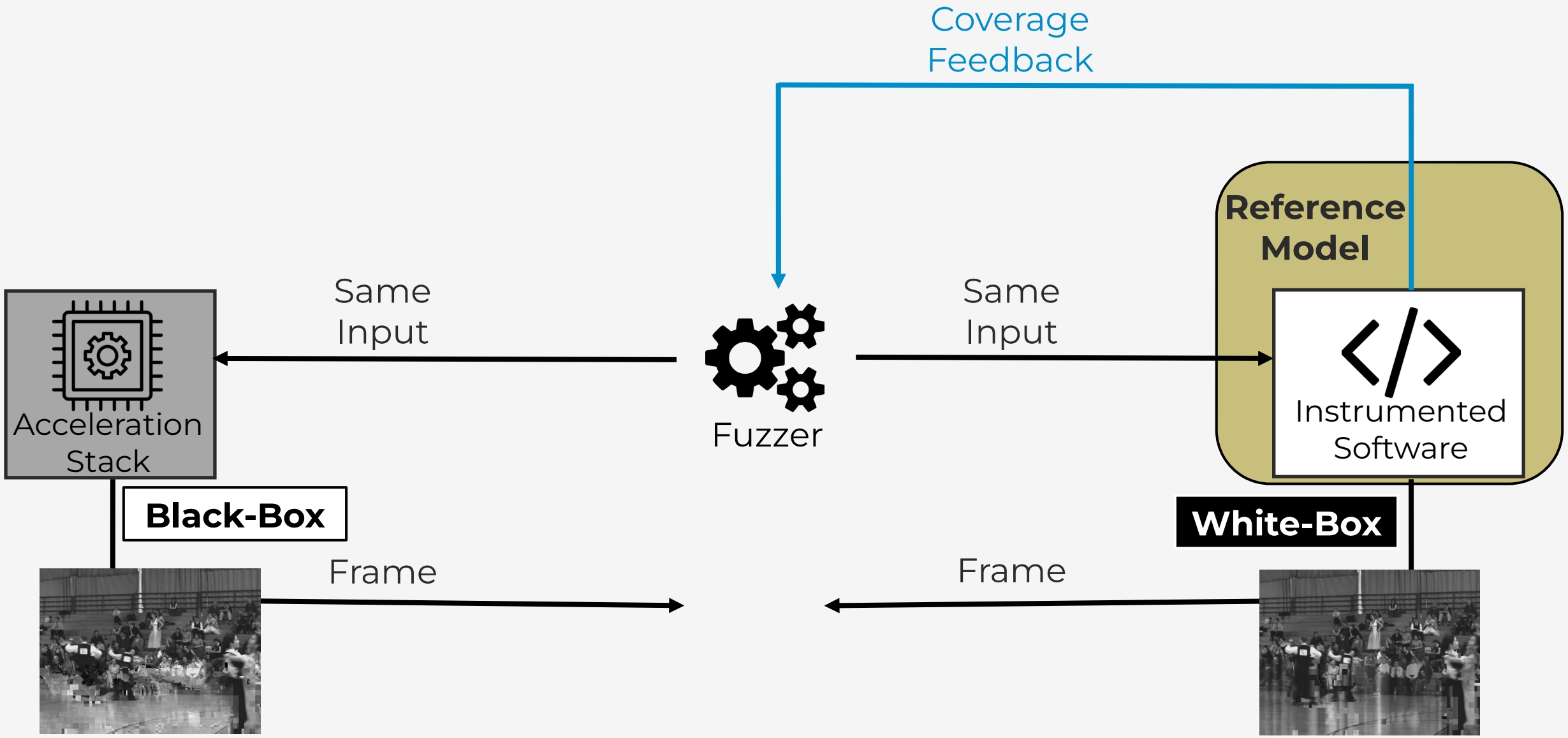


image: Flaticon.com

CH 1: Differential Oracle for Video Hardware Acceleration Stack

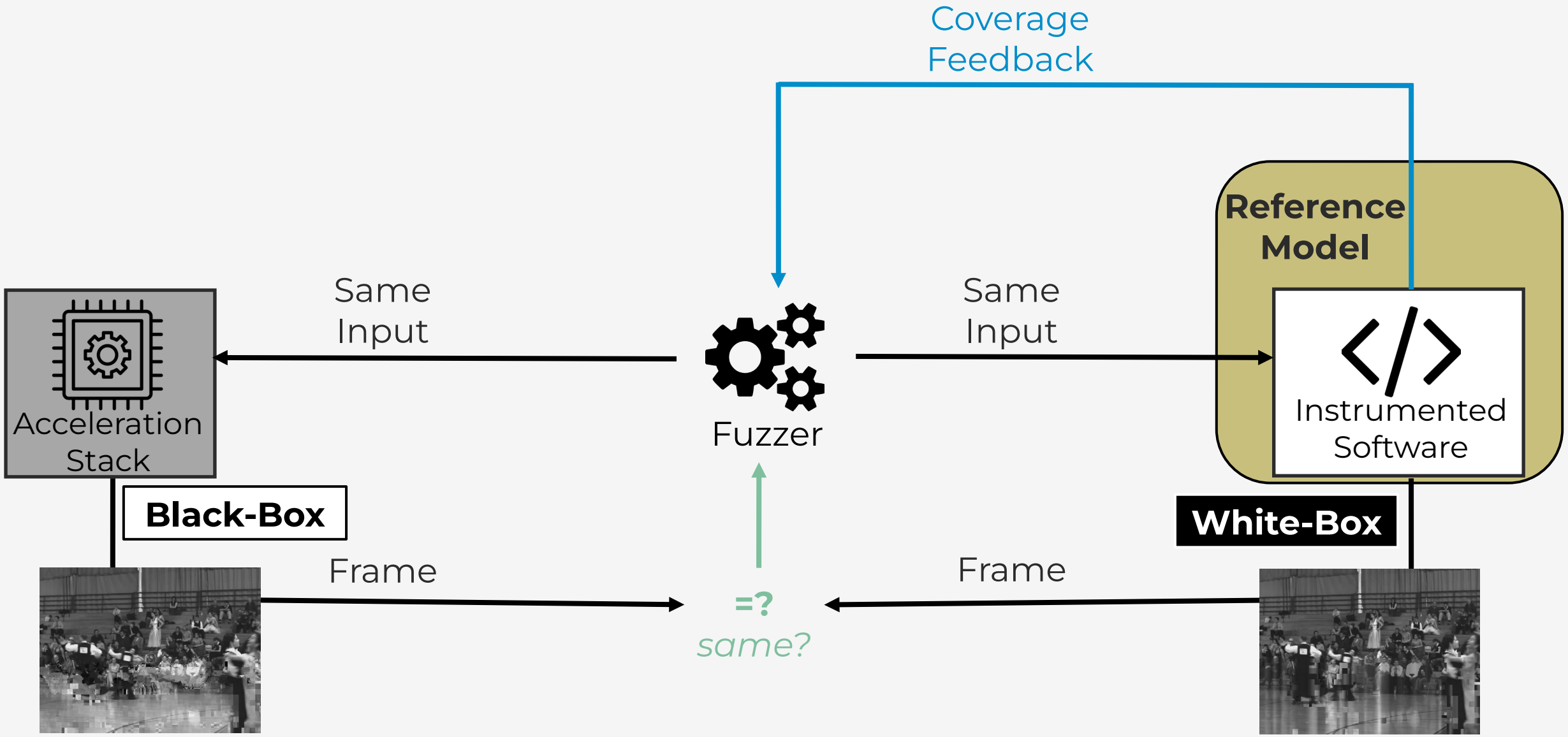


 image: Flaticon.com

Observable Differences

Observable Differences

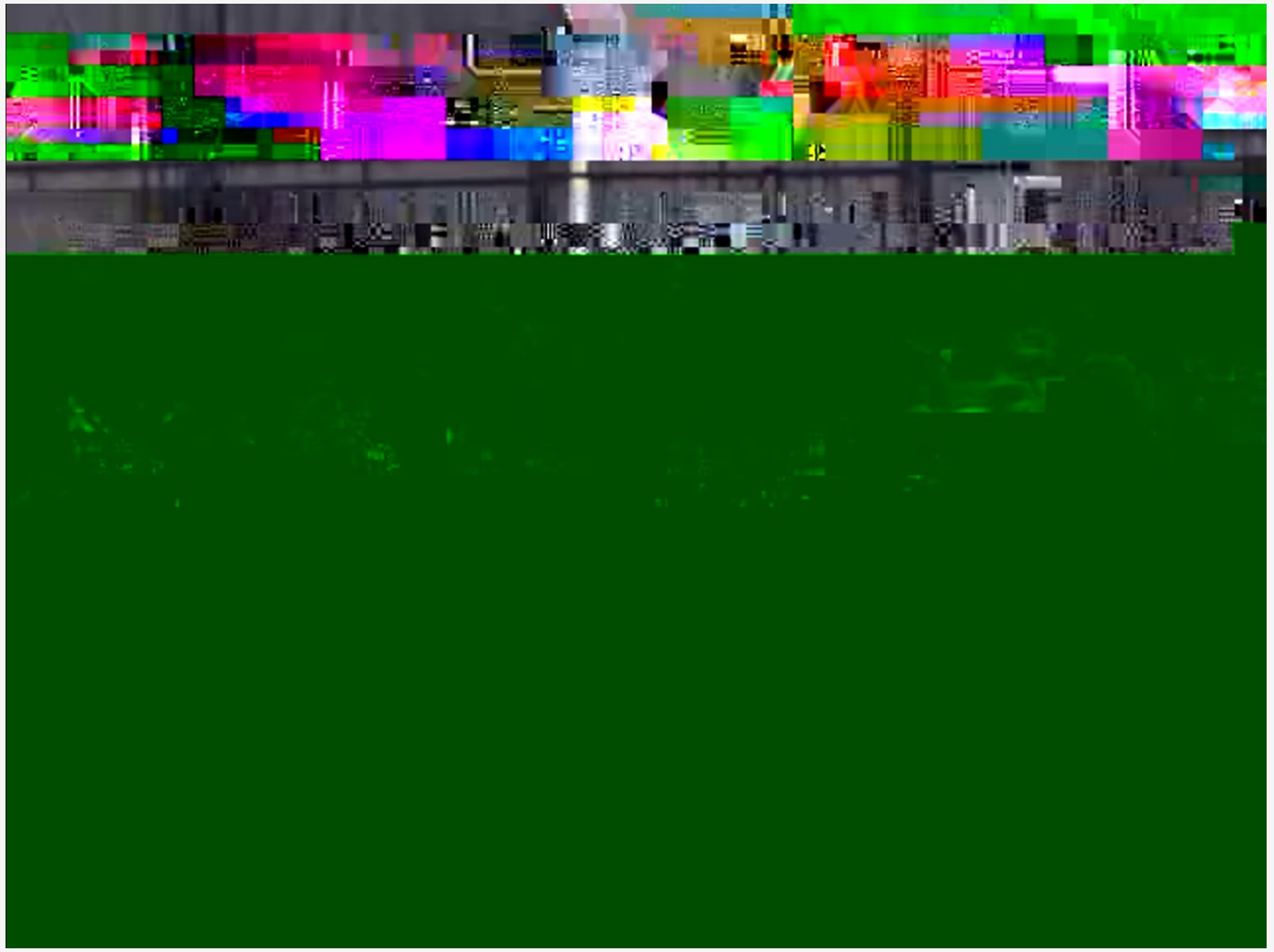
HW Output Frame

Observable Differences

HW Output Frame

SW Output Frame

Frame Rendered in Web Browser



Frame rendered using
hardware acceleration

CH 2: Indirect Proxy Coverage

CH 1

Define a **new oracle** for hardware-accelerated stack

CH 2: Indirect Proxy Coverage

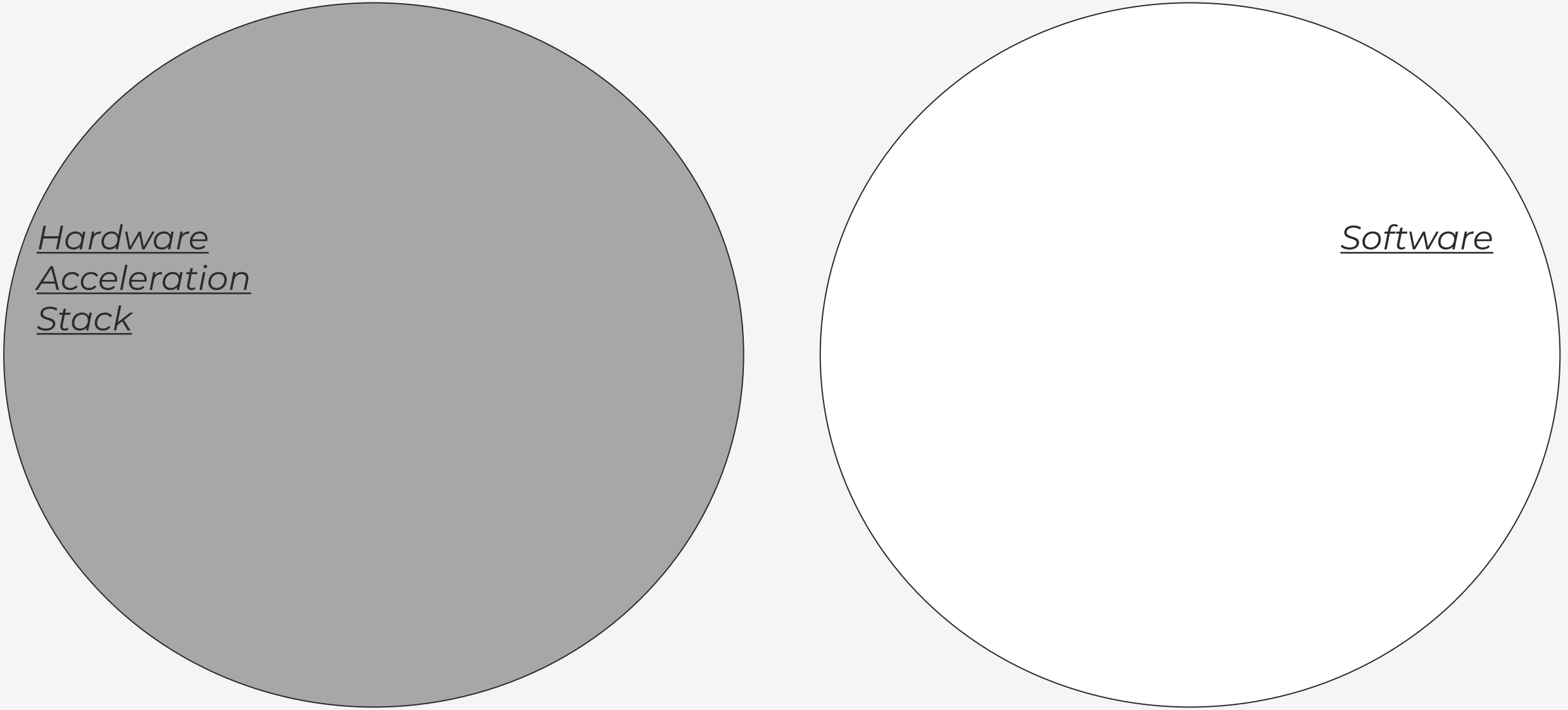
CH 1

Define a **new oracle** for hardware-accelerated stack

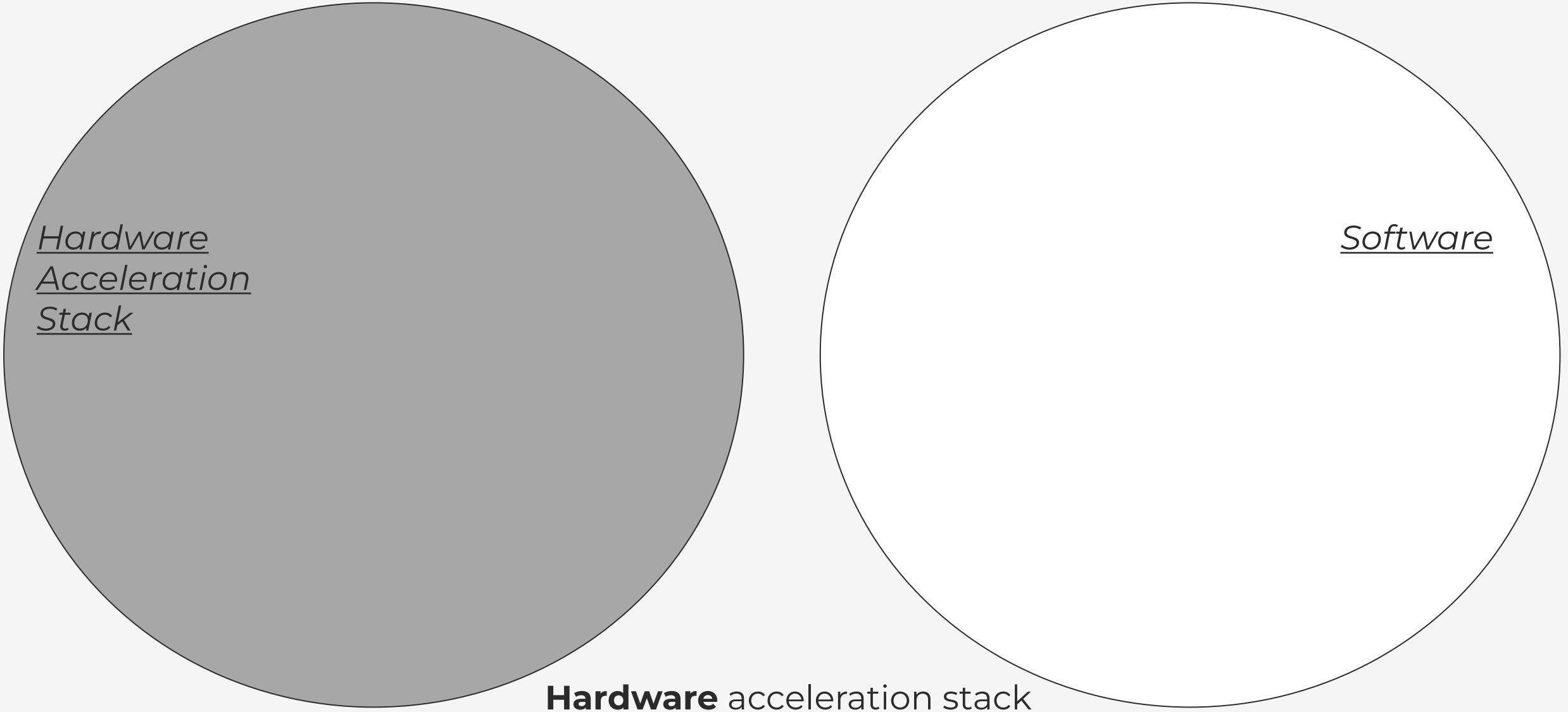
CH 2

Define a **feedback mechanism** for hardware-accelerated stack

CH 2: Indirect Proxy Coverage

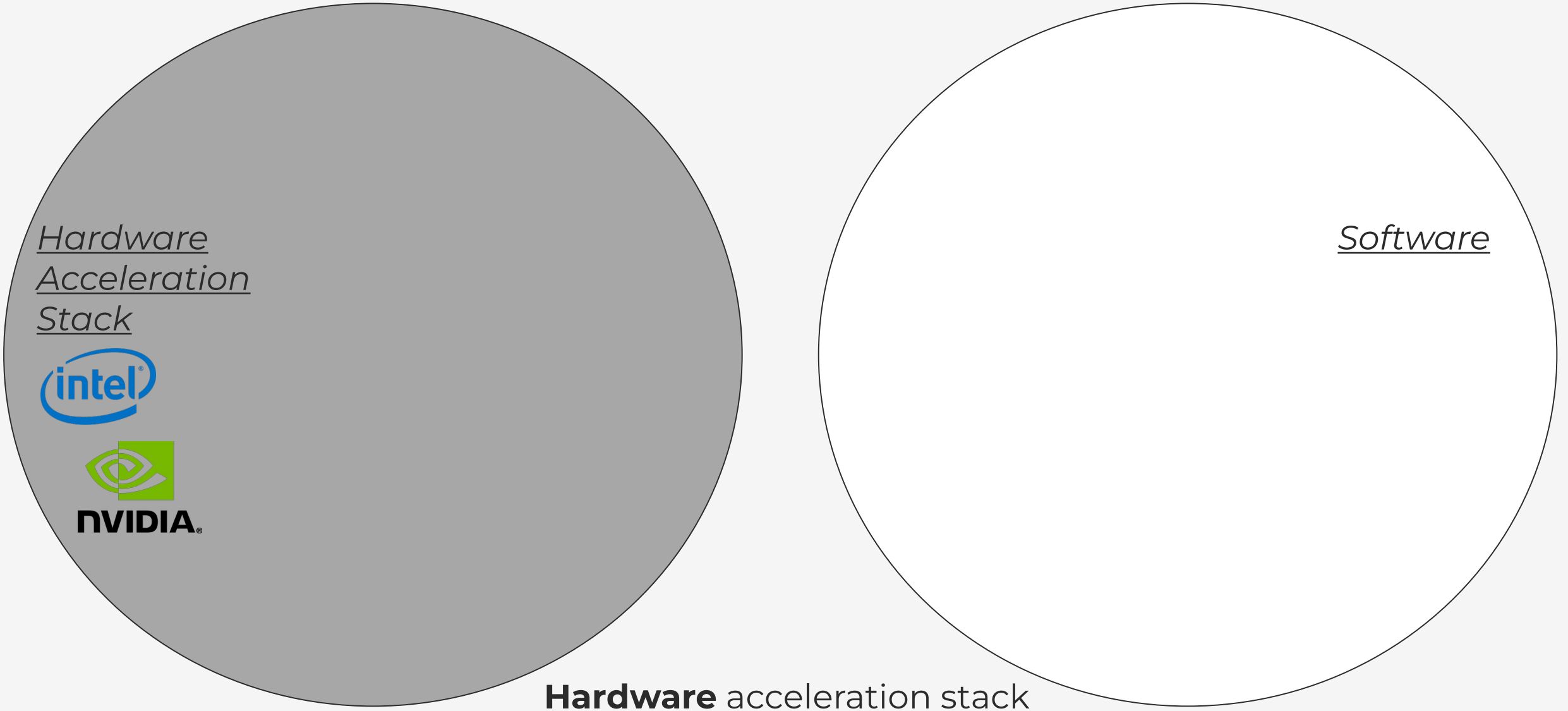


CH 2: Indirect Proxy Coverage



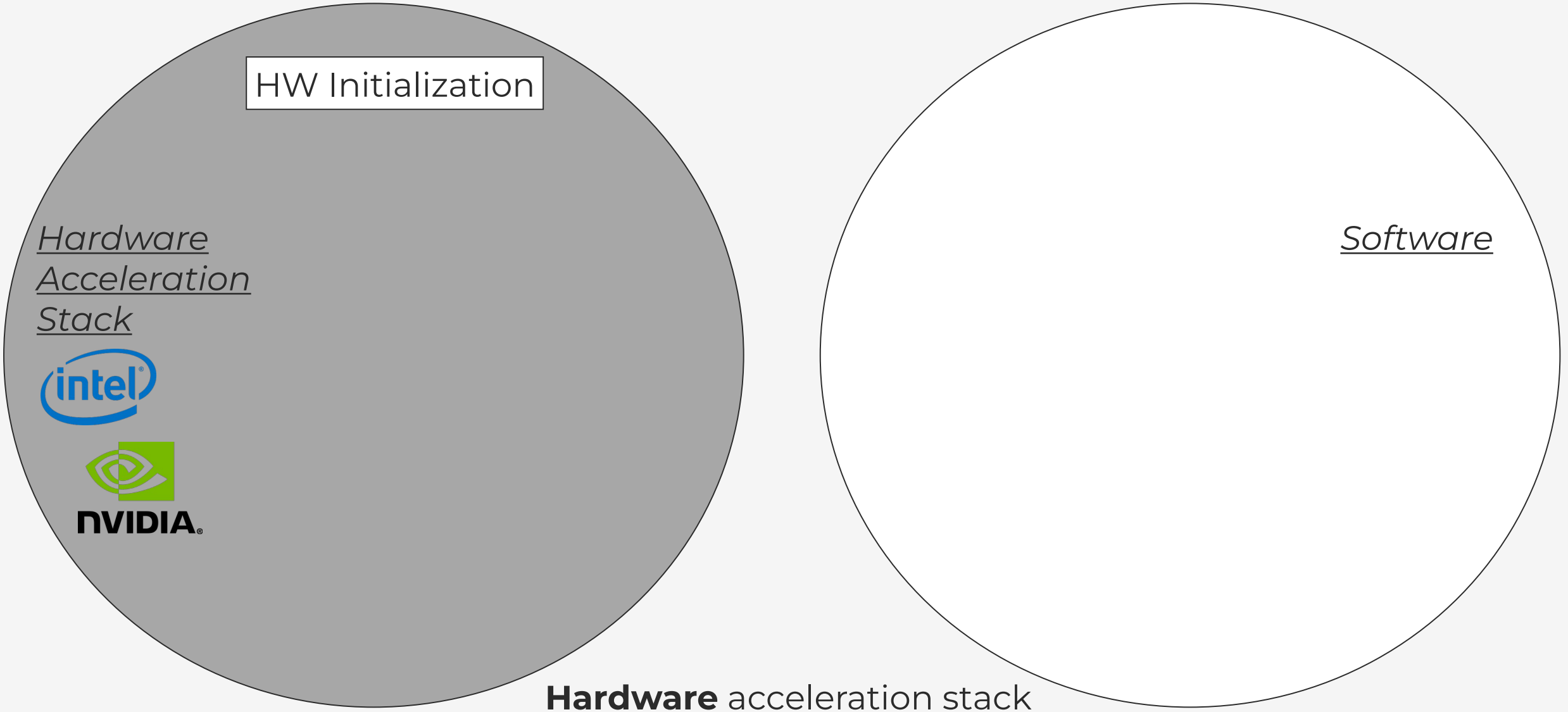
Hardware acceleration stack should **behave as closely** as possible to **software** stack

CH 2: Indirect Proxy Coverage



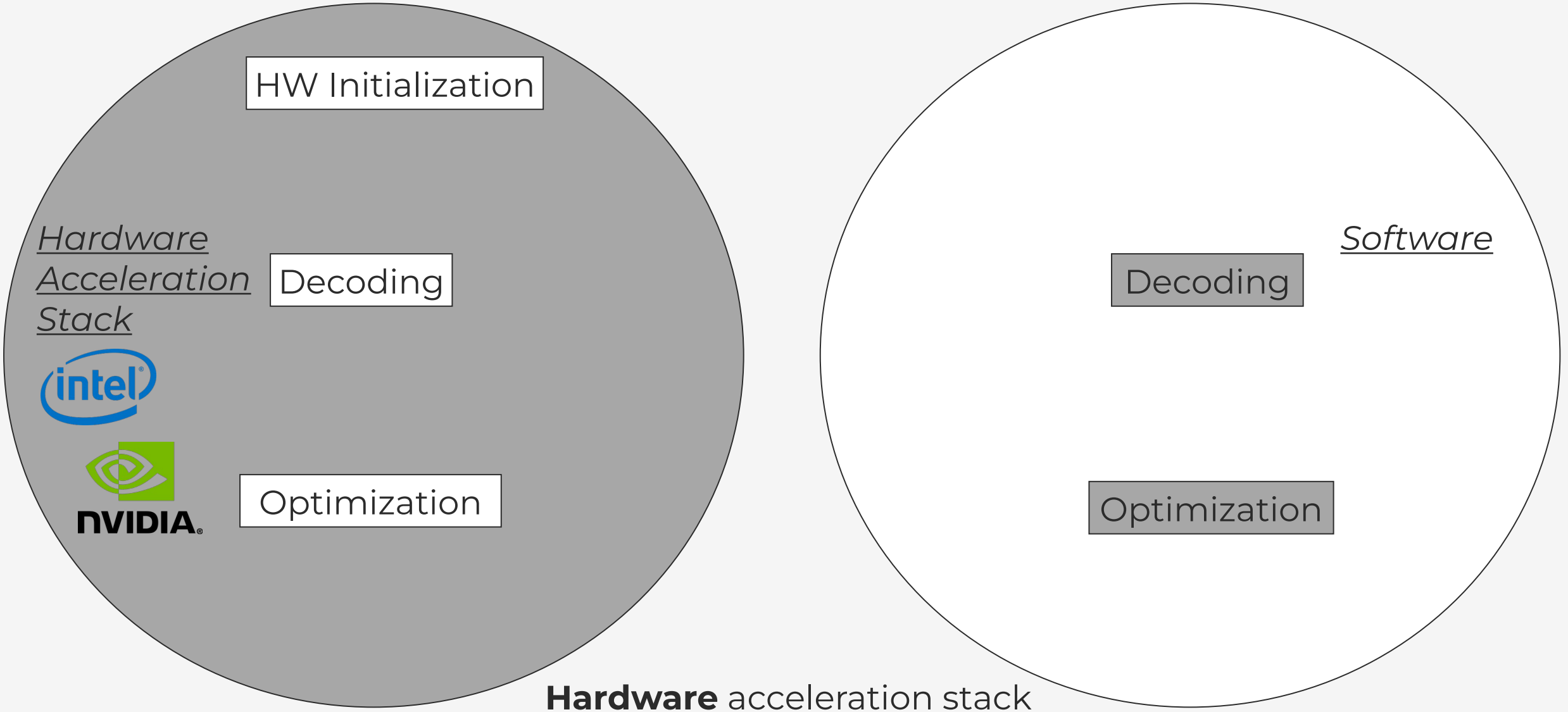
Hardware acceleration stack should **behave as closely** as possible to **software** stack

CH 2: Indirect Proxy Coverage



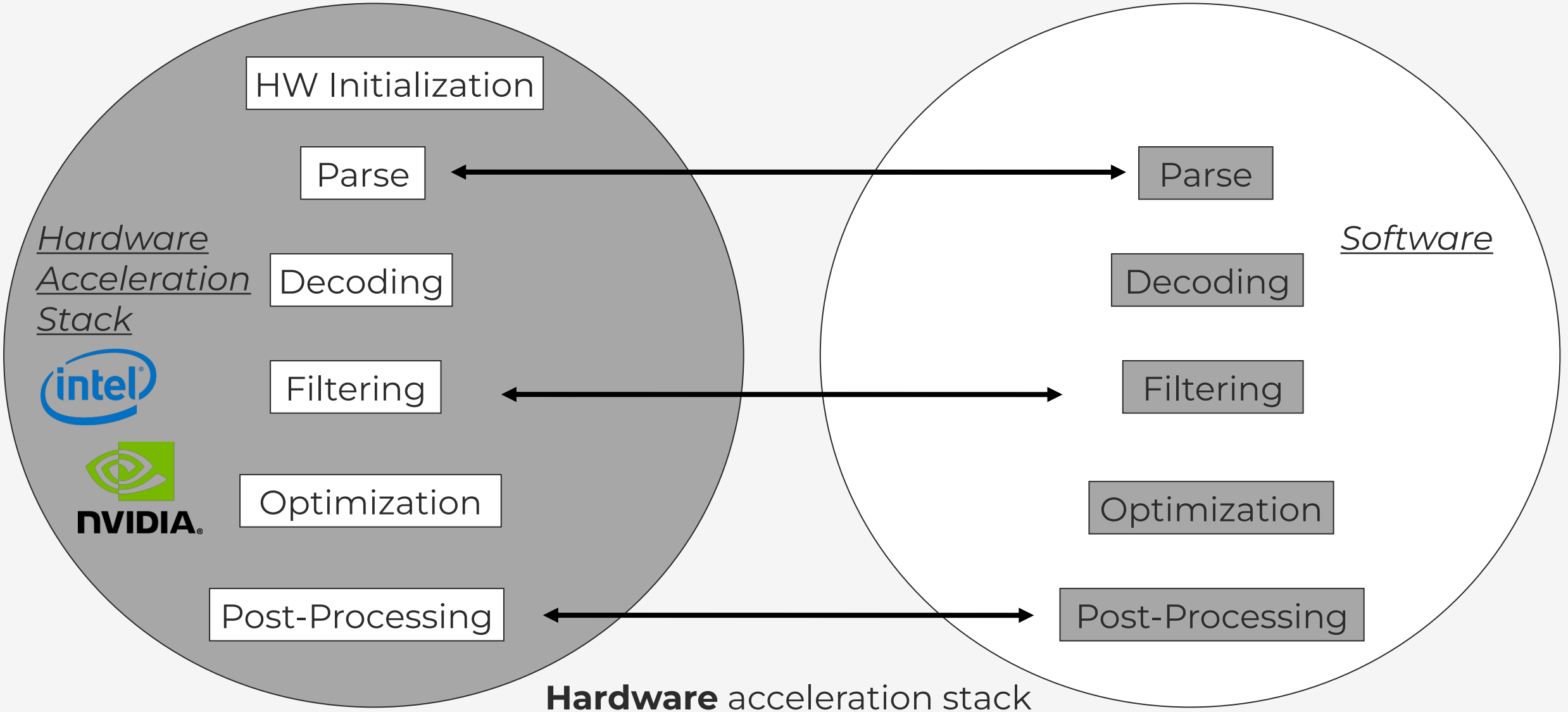
Hardware acceleration stack should **behave as closely** as possible to **software** stack

CH 2: Indirect Proxy Coverage



Hardware acceleration stack should **behave as closely** as possible to **software** stack

CH 2: Indirect Proxy Coverage



Hardware acceleration stack should **behave as closely** as possible to **software** stack

CH 3: Root Cause with Hardware-accelerated Stack

CH 1 — Define a **new oracle** for hardware-accelerated stack

CH 2 — Define a **feedback mechanism** for hardware-accelerated stack

CH 3: Root Cause with Hardware-accelerated Stack

CH 1 — Define a **new oracle** for hardware-accelerated stack

CH 2 — Define a **feedback mechanism** for hardware-accelerated stack

CH 3 — Analyze the **observable differences**

CH 3: Root Cause with Hardware-accelerated Stack

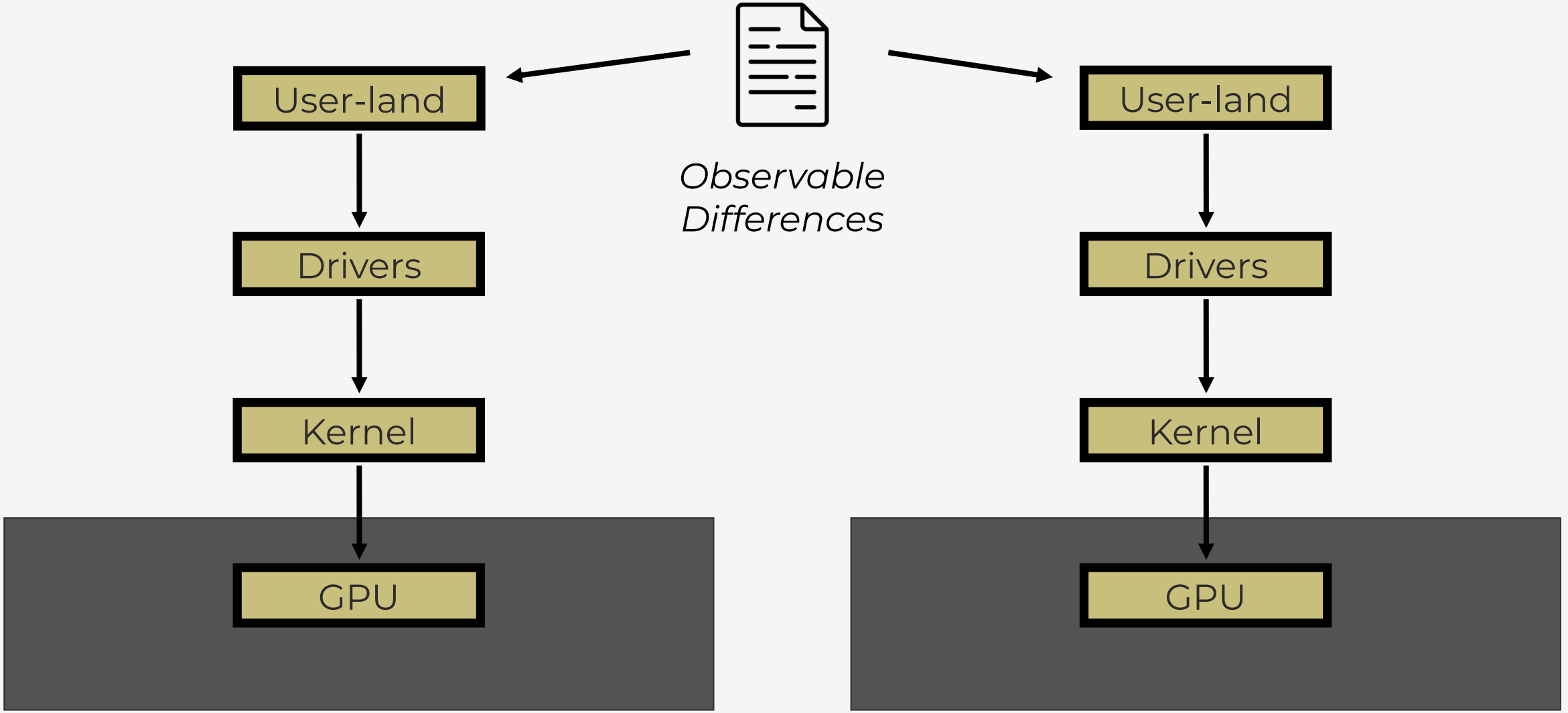


 image: Flaticon.com

CH 3: Root Cause with Hardware-accelerated Stack

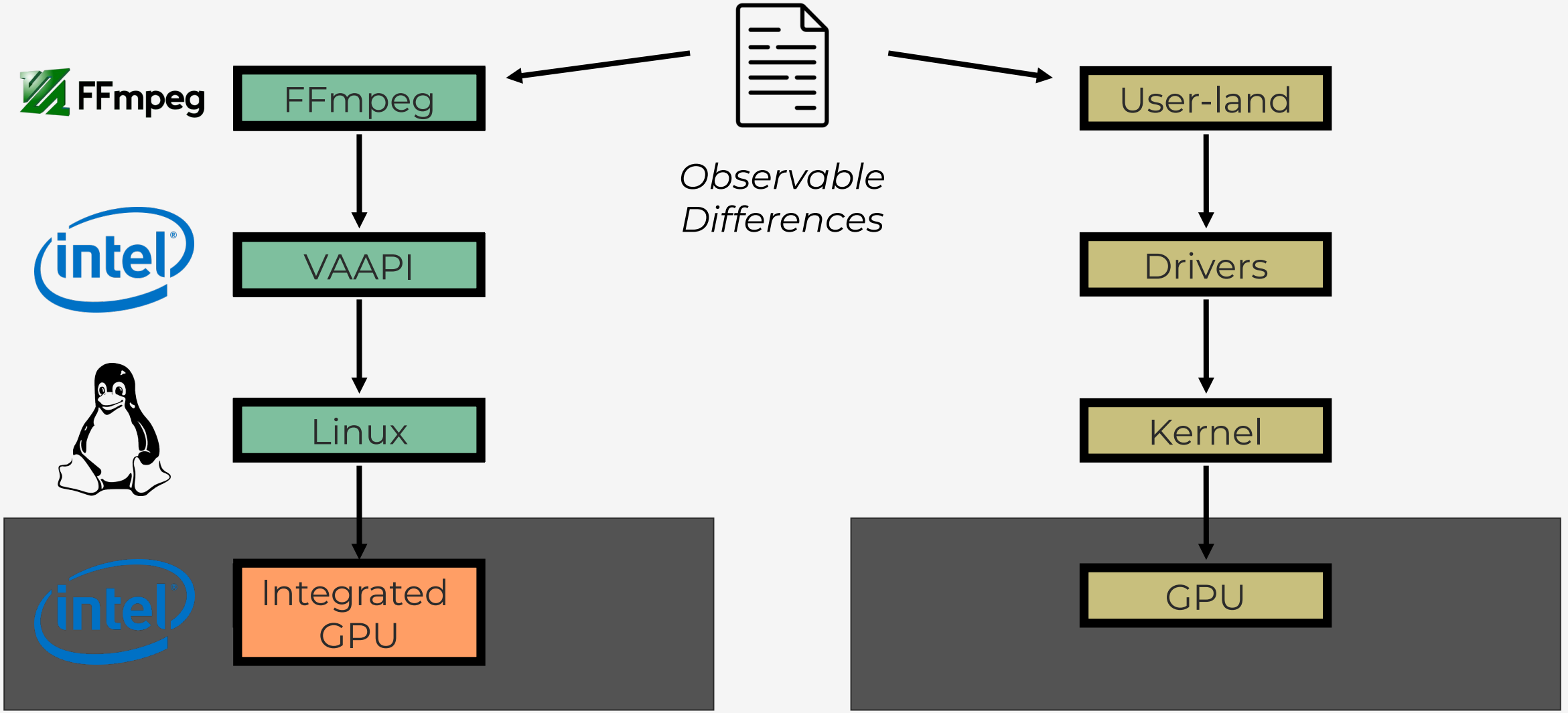


image: Flaticon.com

CH 3: Root Cause with Hardware-accelerated Stack

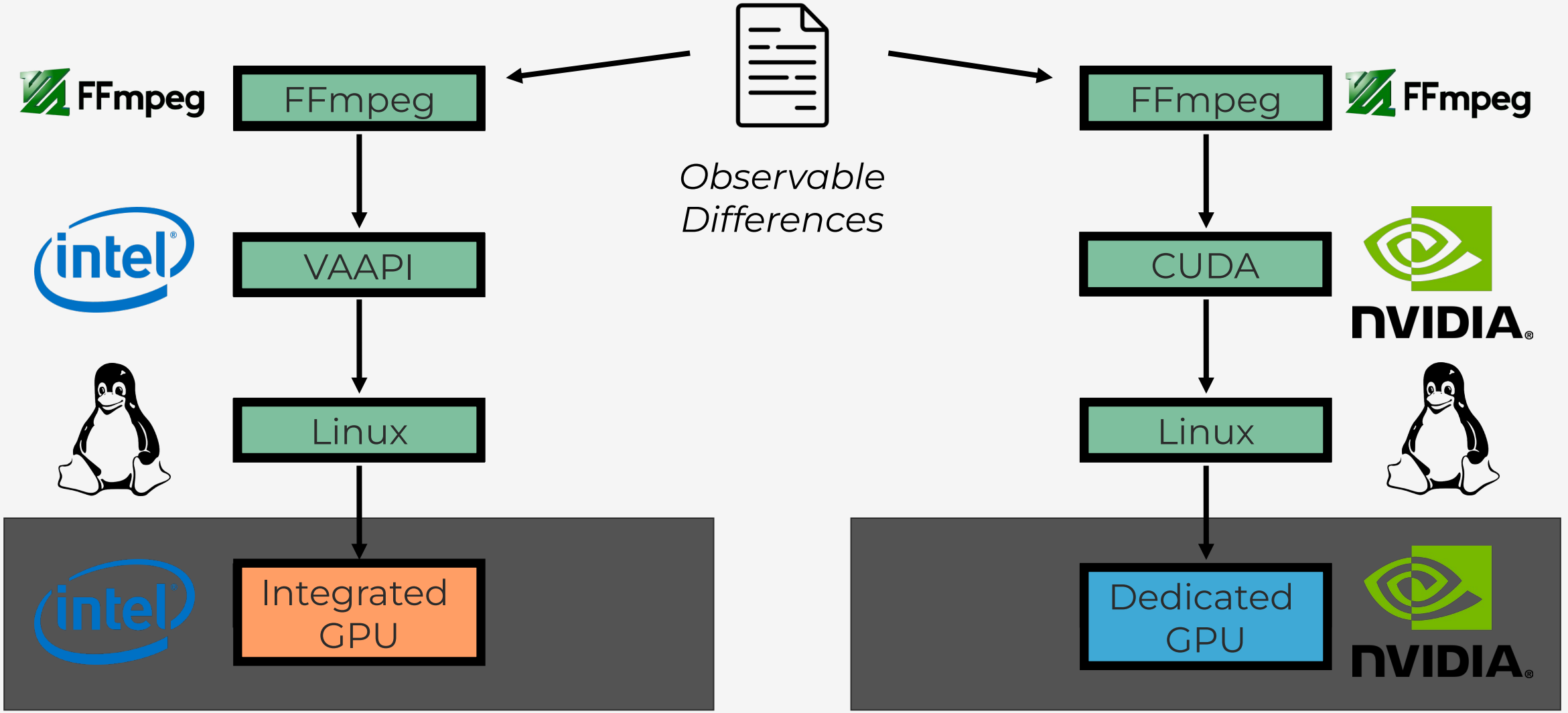


image: Flaticon.com

Bug Findings

Bug ID	Platform	Description	CWE IDs [45]	Layer	Discovery Method	Status
1.a-d	All platforms	Observable difference	204, 474	Undetermined	Fuzzing	Unconfirmed
2	*linux-intel*	Timing-dependent observable difference	204, 362, 474	Undetermined	Fuzzing	Unconfirmed
3	*linux-intel*	Global buffer overflow	126	Application	Fuzzing	Patched
4	*linux-intel*	Heap buffer overflow	122, 787	Driver	Fuzzing	Patched w/ bounty
5	*linux-intel*	Wild pointer dereference	824	Driver	Fuzzing	Disputed
6	*linux-nvidia*	Invalid pointer free	415	Application	Fuzzing	Patched before report
7	*linux-nvidia*	Near-null pointer dereference	824	Application/Driver	Fuzzing	Patched
8	*windows-nvidia*	Information leak on Firefox	908	Application/Driver	Input replay	Confirmed
9	*windows-nvidia*	Windows driver interaction with VLC	476	Application/Driver	Input replay	Reported

Bug Findings

Bug ID	Platform	Description	CWE IDs [45]	Layer	Discovery Method	Status
1.a-d	All platforms	Observable difference	204, 474	Undetermined	Fuzzing	Unconfirmed
2	*linux-intel*	Timing-dependent observable difference	204, 362, 474	Undetermined	Fuzzing	Unconfirmed
3	*linux-intel*	Global buffer overflow	126	Application	Fuzzing	Patched
4	*linux-intel*	Heap buffer overflow	122, 787	Driver	Fuzzing	Patched w/ bounty
5	*linux-intel*	Wild pointer dereference	824	Driver	Fuzzing	Disputed
6	*linux-nvidia*	Invalid pointer free	415	Application	Fuzzing	Patched before report
7	*linux-nvidia*	Near-null pointer dereference	824	Application/Driver	Fuzzing	Patched
8	*windows-nvidia*	Information leak on Firefox	908	Application/Driver	Input replay	Confirmed
9	*windows-nvidia*	Windows driver interaction with VLC	476	Application/Driver	Input replay	Reported

Bug Findings

Bug ID	Platform	Description	CWE IDs [45]	Layer	Discovery Method	Status
1.a-d	All platforms	Observable difference	204, 474	Undetermined	Fuzzing	Unconfirmed
2	*linux-intel*	Timing-dependent observable difference	204, 362, 474	Undetermined	Fuzzing	Unconfirmed
3	*linux-intel*	Global buffer overflow	126	Application	Fuzzing	Patched
4	*linux-intel*	Heap buffer overflow	122, 787	Driver	Fuzzing	Patched w/ bounty
5	*linux-intel*	Wild pointer dereference	824	Driver	Fuzzing	Disputed
6	*linux-nvidia*	Invalid pointer free	415	Application	Fuzzing	Patched before report
7	*linux-nvidia*	Near-null pointer dereference	824	Application/Driver	Fuzzing	Patched
8	*windows-nvidia*	Information leak on Firefox	908	Application/Driver	Input replay	Confirmed
9	*windows-nvidia*	Windows driver interaction with VLC	476	Application/Driver	Input replay	Reported

Bug Findings

Bug ID	Platform	Description	CWE IDs [45]	Layer	Discovery Method	Status
1.a-d	All platforms	Observable difference	204, 474	Undetermined	Fuzzing	Unconfirmed
2	*linux-intel*	Timing-dependent observable difference	204, 362, 474	Undetermined	Fuzzing	Unconfirmed
3	*linux-intel*	Global buffer overflow	126	Application	Fuzzing	Patched
4	*linux-intel*	Heap buffer overflow	122, 787	Driver	Fuzzing	Patched w/ bounty
5	*linux-intel*	Wild pointer dereference	824	Driver	Fuzzing	Disputed
6	*linux-nvidia*	Invalid pointer free	415	Application	Fuzzing	Patched before report
7	*linux-nvidia*	Near-null pointer dereference	824	Application/Driver	Fuzzing	Patched
8	*windows-nvidia*	Information leak on Firefox	908	Application/Driver	Input replay	Confirmed
9	*windows-nvidia*	Windows driver interaction with VLC	476	Application/Driver	Input replay	Reported

Limitations

- ❏ Uses **unspecialized** fuzzer
- ❏ Targets hardware-accelerated **post-silicon video decoding**
- ❏ **Limited** root-cause analysis on observable differences
- ❏ Drivers and GPUs are **bundled**

Take Away

- We present a **new method for testing video hardware acceleration stacks**. We derive a **differential oracle** that may indicate the presence of both correctness and security-relevant faults
- We propose a technique for **indirectly guiding** an unmodified **fuzzer** to abstract **over a hardware acceleration stack** that is otherwise difficult to introspect
- We **implement a prototype called TwinFuzz** capable of fuzzing a specific hardware acceleration stack

https://github.com/CISPA-SysSec/twinfuzz

matteo.leonelli@cispa.de