

Hardening NVIDIA's Confidential Computing

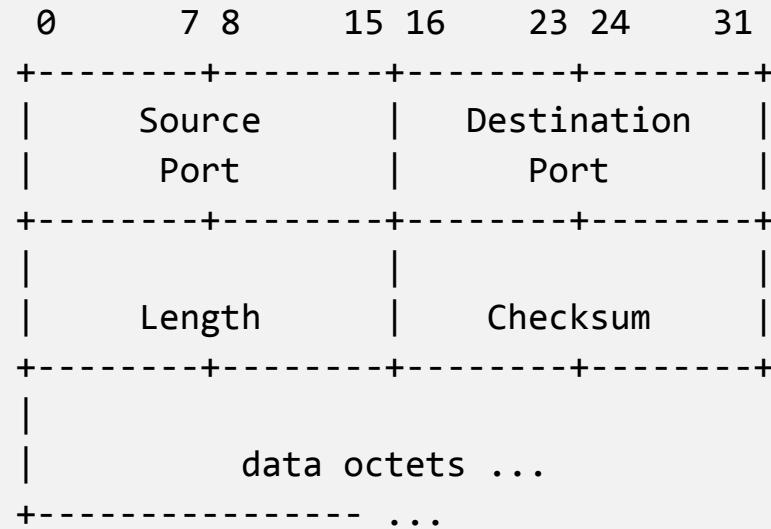
A Formally Verified Implementation of the SPDM Device Attestation Protocol

Tobias Reiher

Mar 28, 2024



A fairly simple protocol: UDP



User Datagram Header Format

“Length is the length in octets of this user datagram including this header and the data.” RFC 768



Typical representation with a C struct

UDP

00	01	02	03	04	05	06	07	08	09	10	11	12	...	1023
source_port <code>uint16_t</code>	dest_port <code>uint16_t</code>	length <code>uint16_t</code>	checksum <code>uint16_t</code>								data[] <code>uint8_t</code>			



Typical representation with a C struct

UDP

00 01 02 03 04 05 06 07 08 09 10 11 12 ... 1023

source_port uint16_t	dest_port uint16_t	length uint16_t	checksum uint16_t	data[] uint8_t							
---------------------------------------	-------------------------------------	----------------------------------	------------------------------------	---------------------------------	--	--	--	--	--	--	--

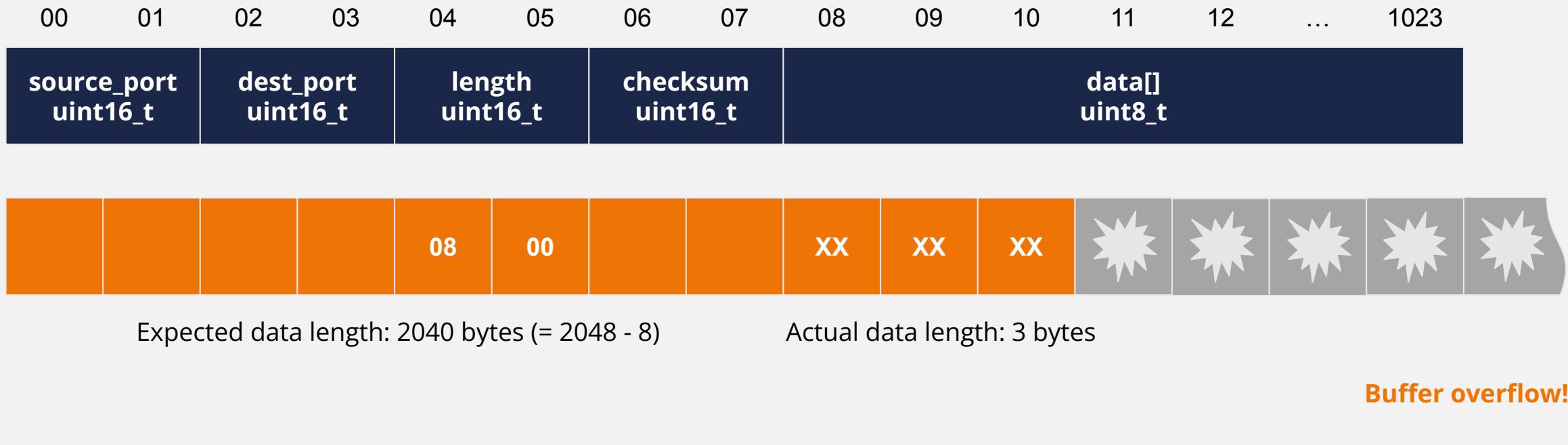


Expected data length: 3 bytes (= 11 - 8)

Actual data length: 3 bytes

What could go wrong?

UDP



What could go wrong?

UDP

00 01 02 03 04 05 06 07 08 09 10 11 12 ... 1023

source_port uint16_t	dest_port uint16_t	length uint16_t	checksum uint16_t	data[] uint8_t
-------------------------	-----------------------	--------------------	----------------------	-------------------



Expected data length: 65528 bytes (= 0 - 8)

Integer underflow!

Actual data length: 3 bytes

Buffer overflow!



Real consequences and huge costs

The Guardian: BrakTooth vulnerability - Bluetooth users are warned some devices are unpatched. White-hat hackers have disclosed vulnerabilities, dubbed BrakTooth, in billions of Bluetooth devices - and are raising some vendors' unwillingness to patch them.

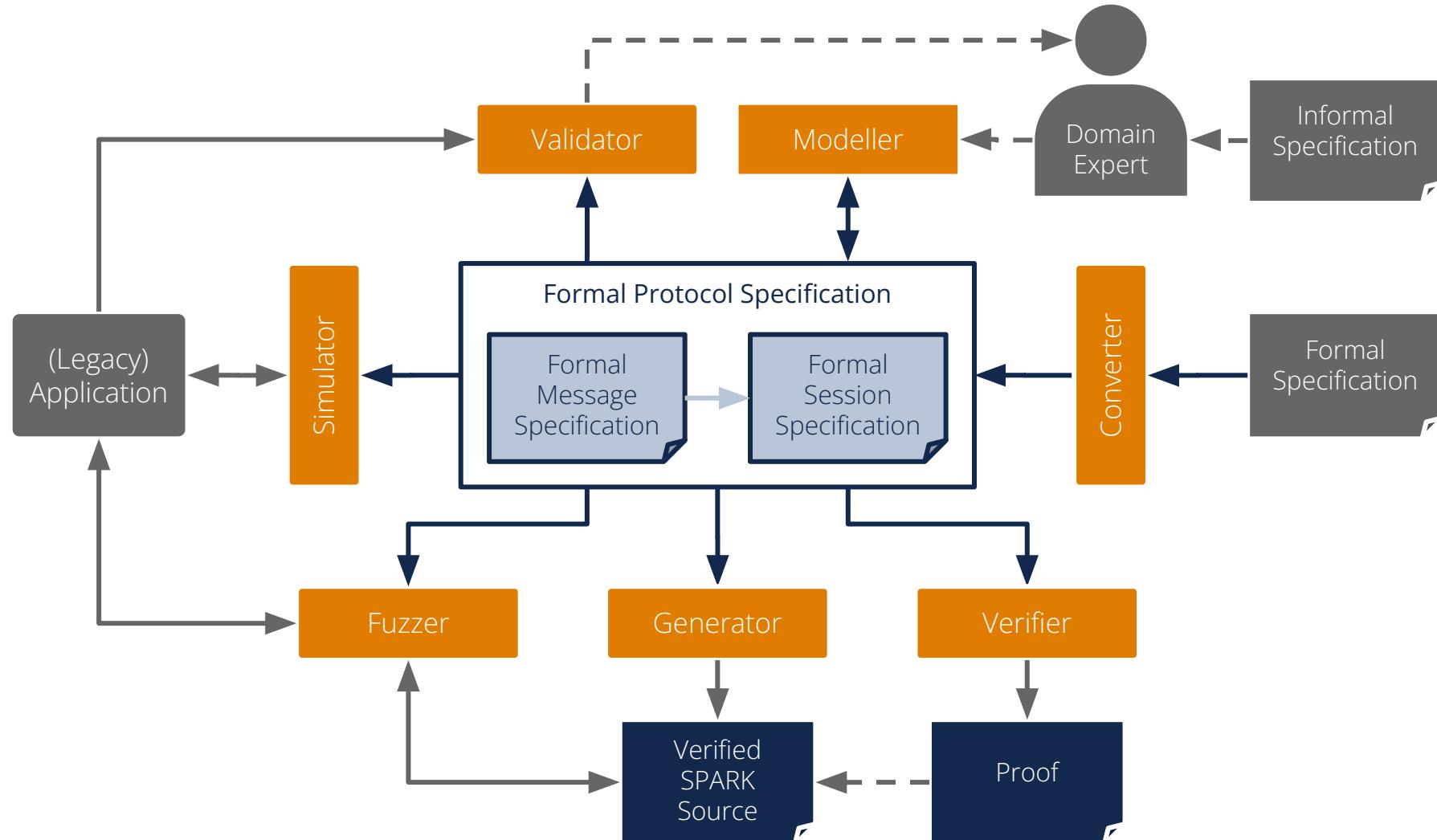
BleepingComputer: BlueBorne Vulnerabilities Impact Over 5 Billion Bluetooth-Enabled Devices. Security researchers have discovered vulnerabilities — codenamed BlueBorne — in the Bluetooth protocol used by billions of devices.

ZDNet: Ripple20 vulnerability will haunt the landscape for years to come. Security researchers discovered a critical flaw in a TCP/IP library that impacts many IoT products.

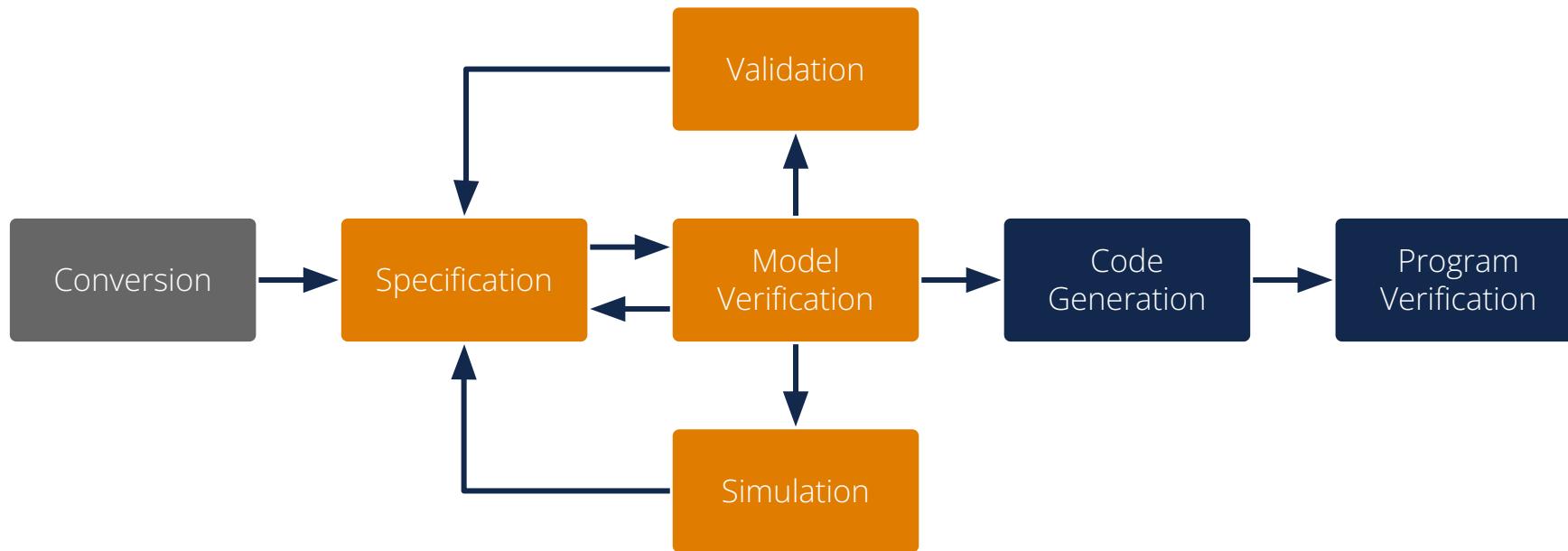
Medical Device Network: URGENT/11 vulnerability could let cyberattackers take over medical devices. The URGENT/11 vulnerability allows attackers to remotely take over industrial devices, bypassing perimeter measures such as firewalls.

The Hacker News: Amnesia:33 – Critical TCP/IP Flaws Affect Millions of IoT Devices. The Amnesia:33 vulnerability affects millions of IoT devices, including routers, switches, and firewalls, potentially allowing attackers to gain unauthorized access to networks.

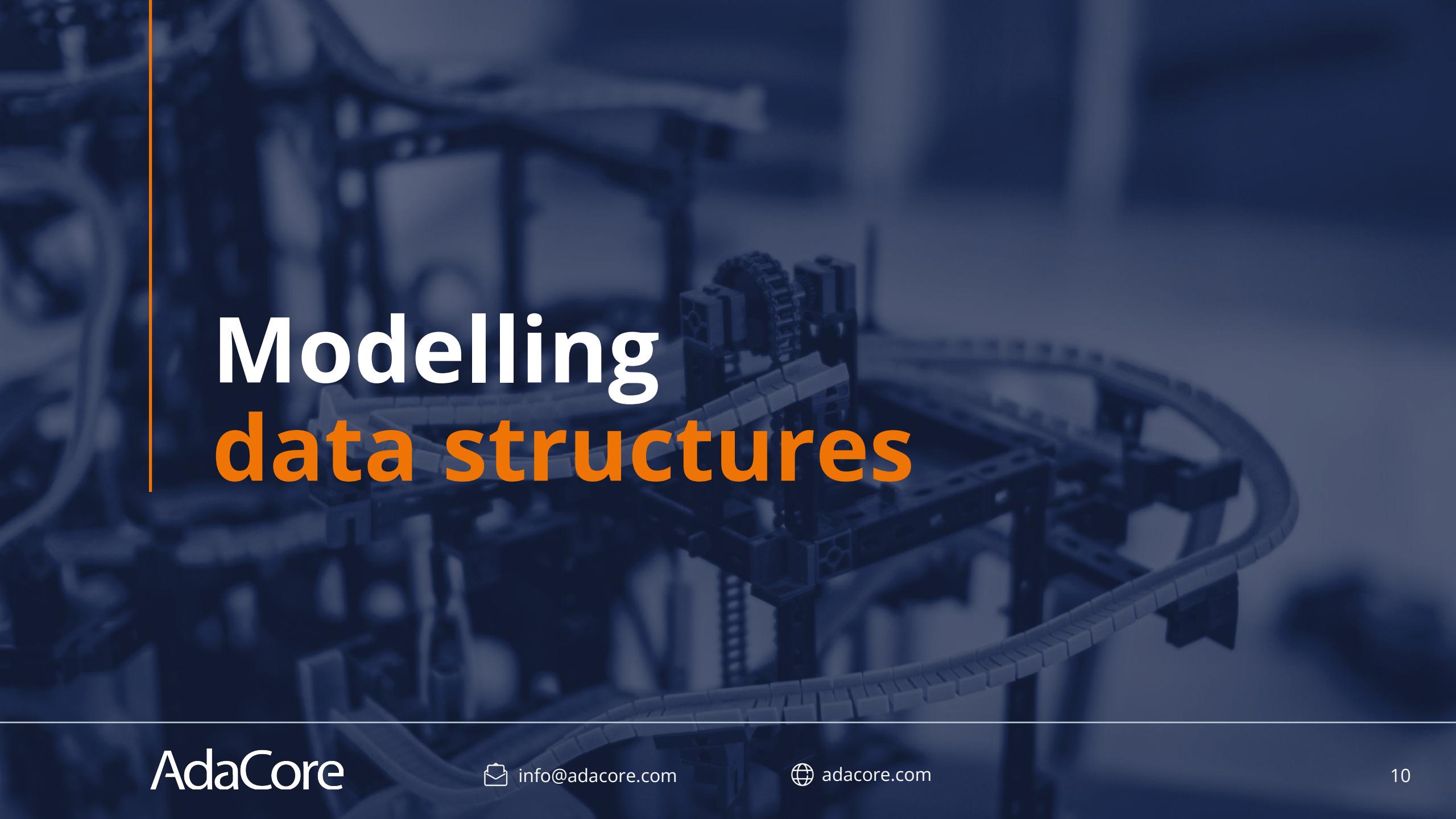
RecordFlux toolset



RecordFlux workflow

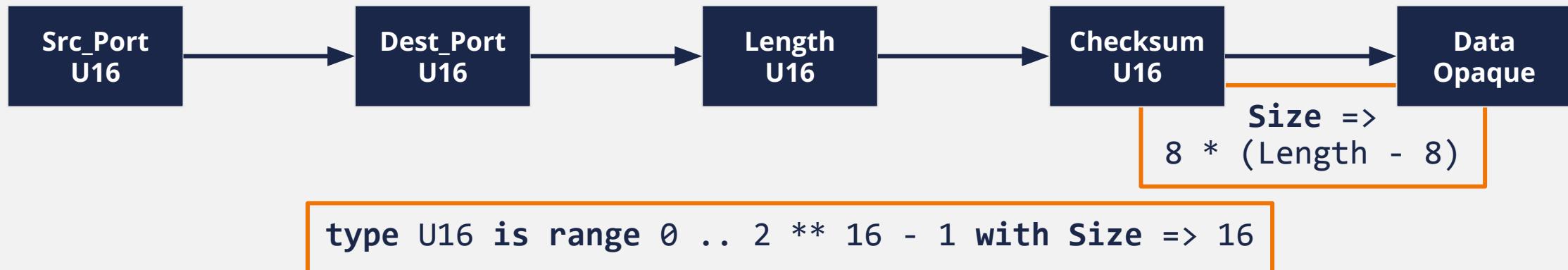


Modelling data structures



Formal message specification

UDP



Proofs on the model level

UDP



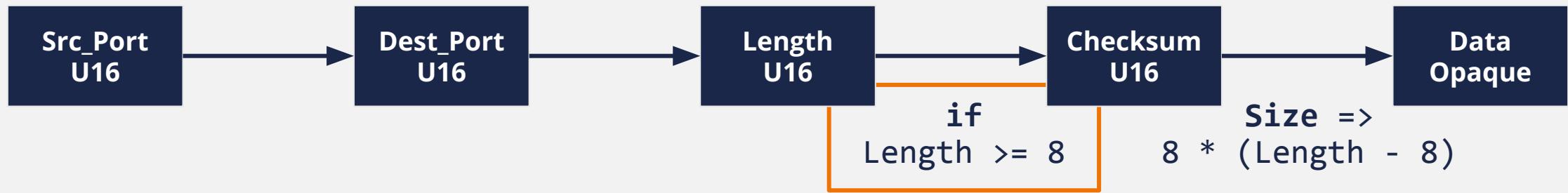
```
type U16 is range 0 .. 2 ** 16 - 1 with Size => 16
```

```
model: error: negative size for field "Data"  
(Src_Port -> Dest_Port -> Length -> Checksum -> Data)
```



Option #1: Introduce explicit invariant

UDP



```
type U16 is range 0 .. 2 ** 16 - 1 with Size => 16
```



Option #2: Use constraint length type

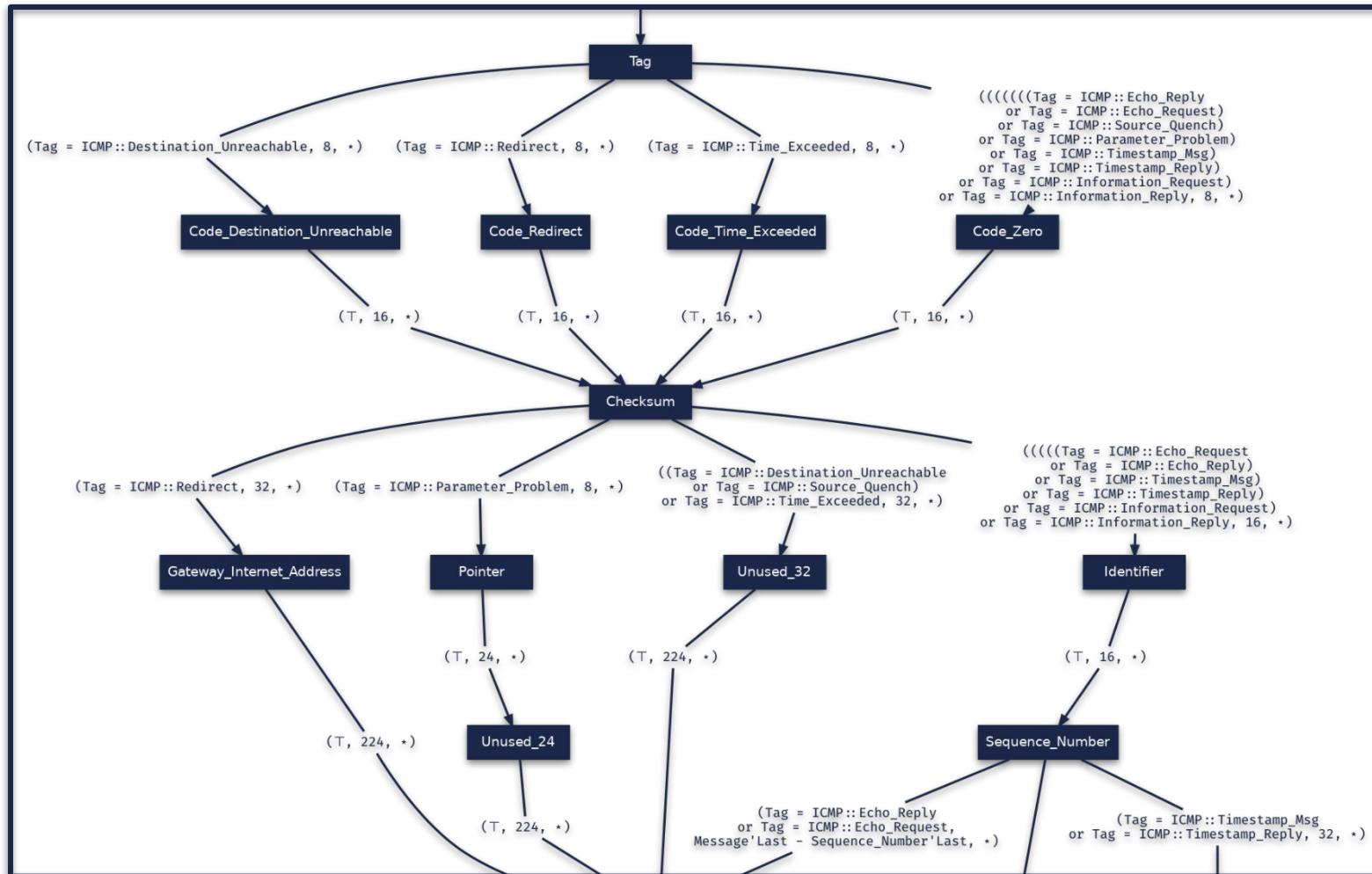
UDP



```
type U16 is range 0 .. 2 ** 16 - 1 with Size => 16
```

```
type Length_T is range 8 .. 2 ** 16 - 1 with Size => 16
```

A fragment of an ICMP message model



A large, modern building with a distinctive glass and steel facade. The glass panels are arranged in a grid pattern, creating a series of triangles. An orange vertical line runs along the left edge of the slide.

Guarantees from message verification

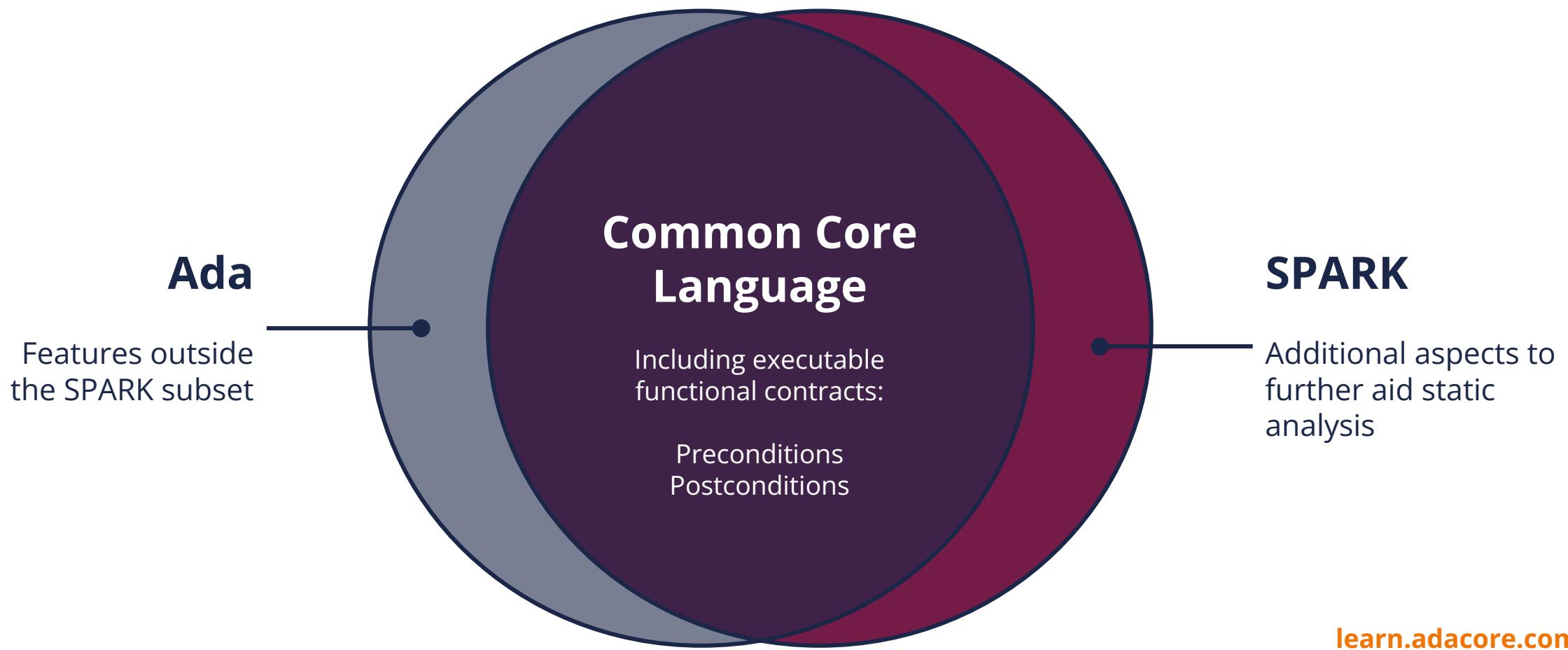




How do we bridge the gap between specification and implementation?



SPARK as our target language



learn.adacore.com

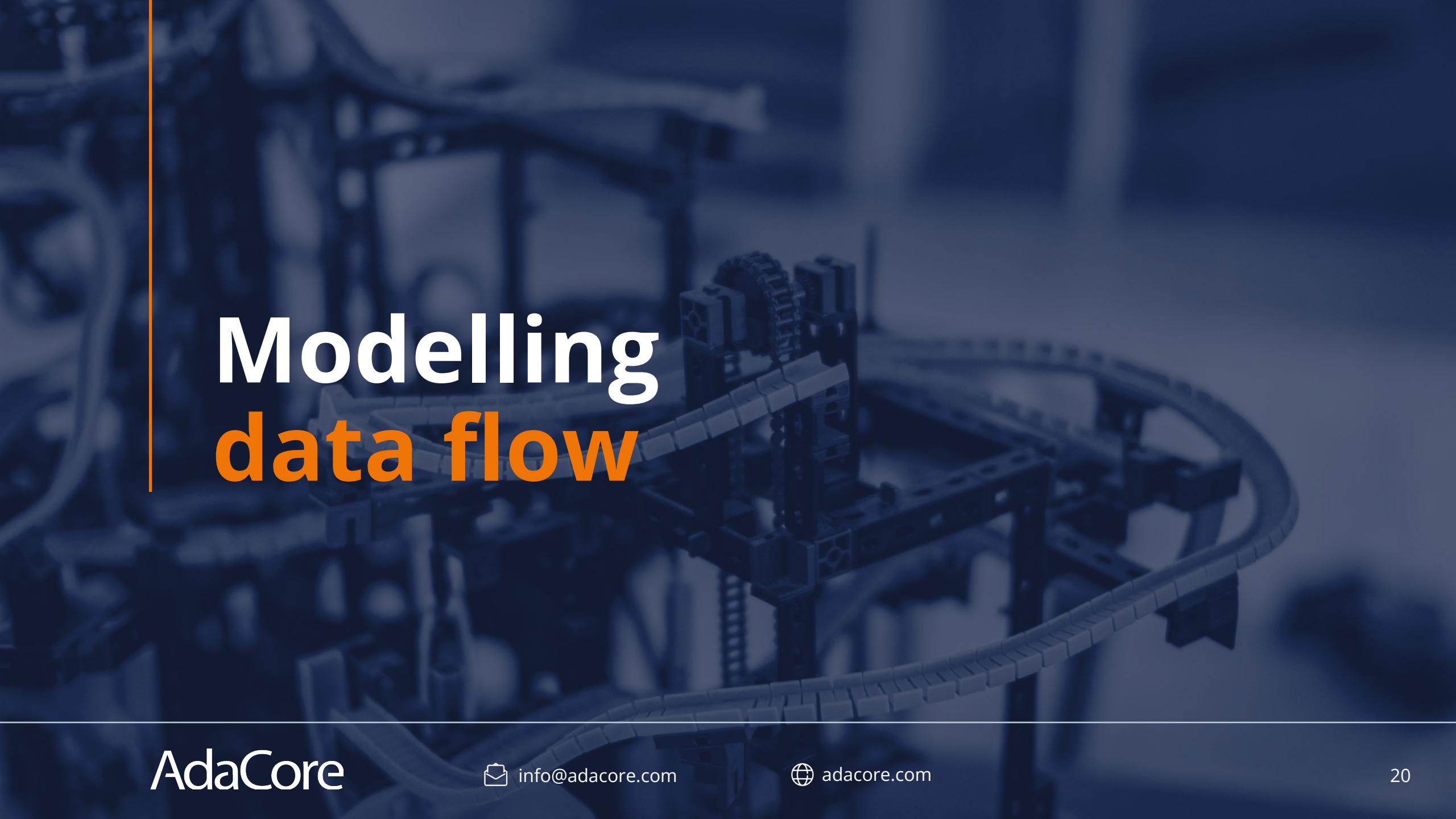




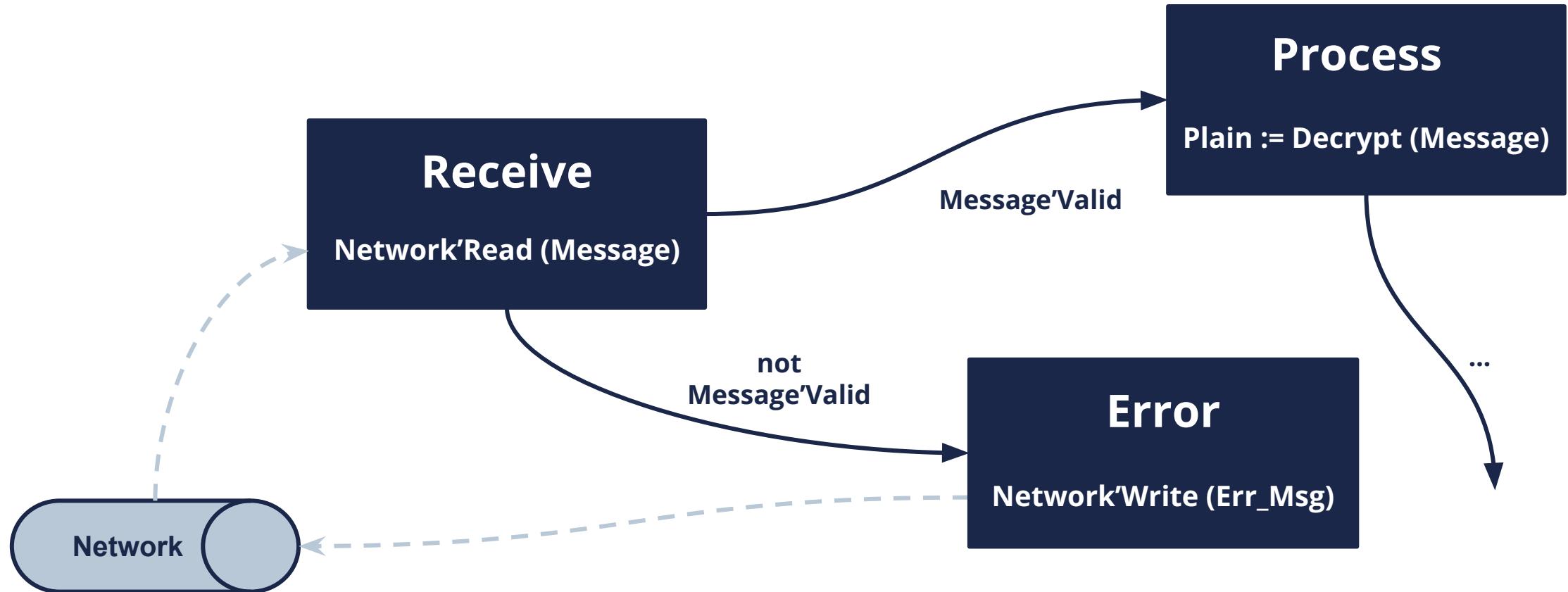
Guarantees from program verification



Modelling data flow



Interacting FSMs with context



A large, modern building with a distinctive glass and steel facade. The glass panels are arranged in a grid pattern, creating a series of triangles. An orange vertical bar runs along the left edge of the slide.

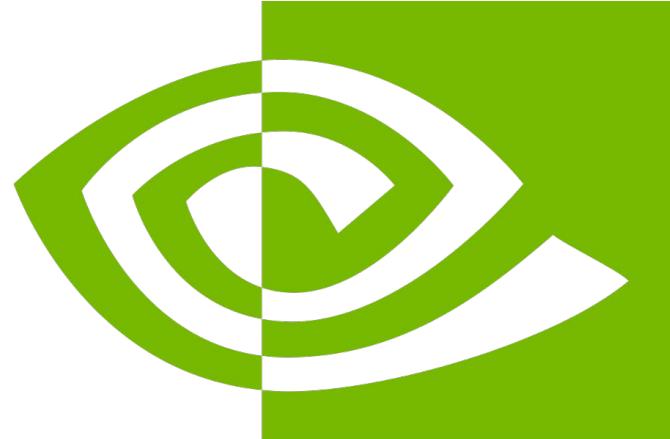
Guarantees from session verification



Hardening NVIDIA's Confidential Computing



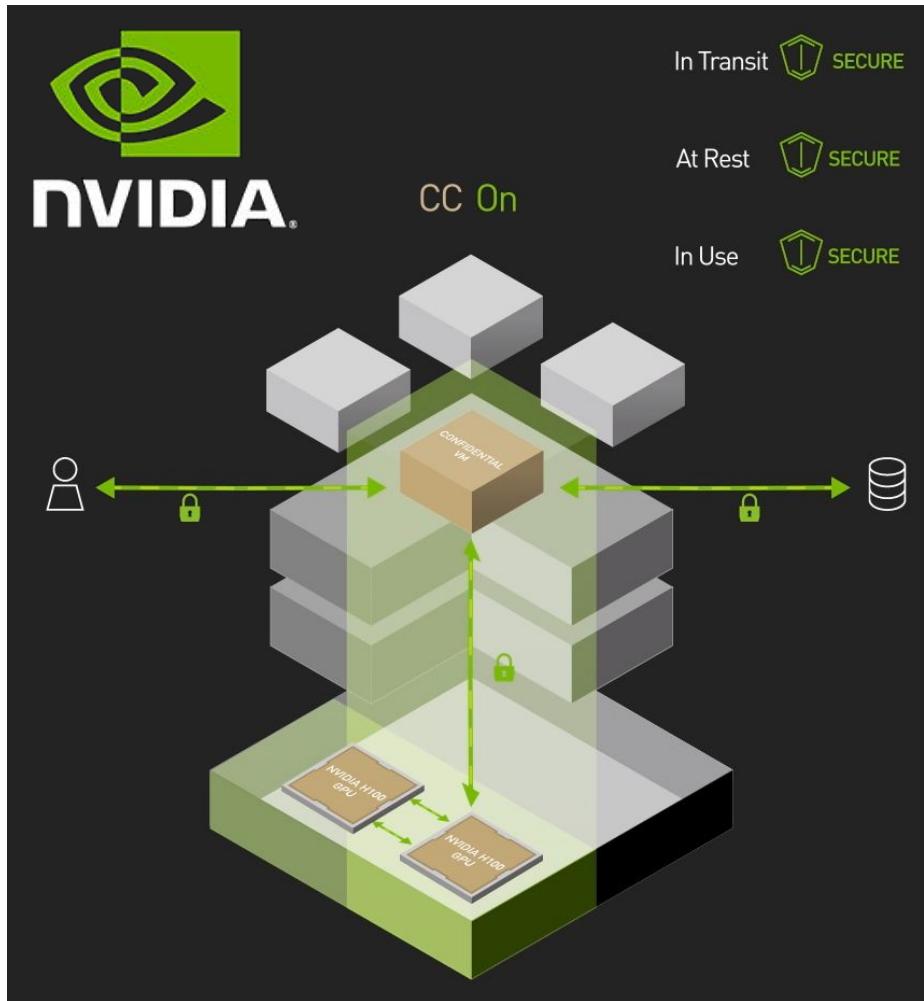
NVIDIA adopts SPARK for critical firmware



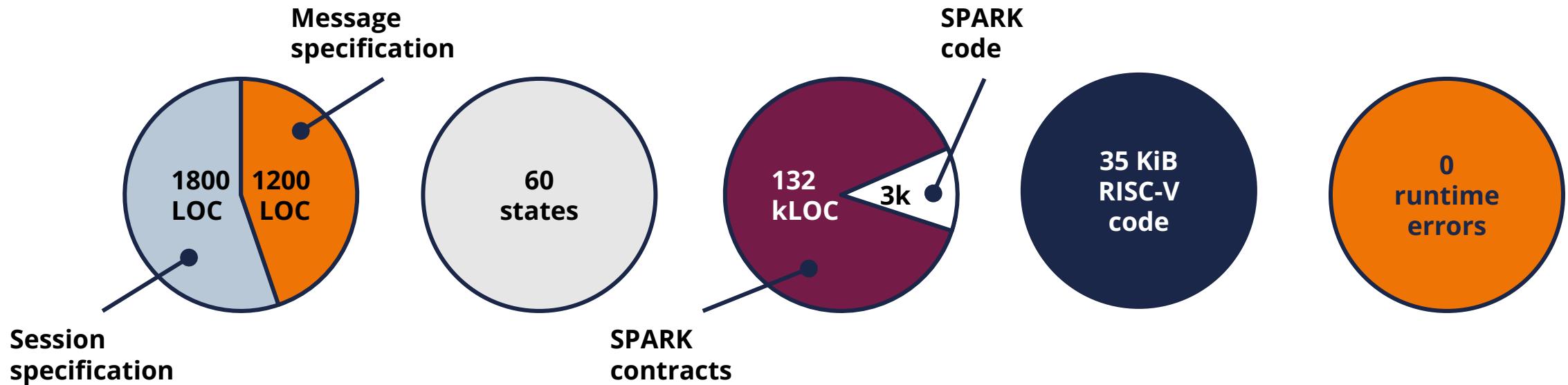
nVIDIA®

adacore.com/nvidia

Security Protocol and Data Model (SPDM)



SPDM formalization with RecordFlux



RecordFlux/SPARK SPDM implementation:
github.com/AdaCore/spdm-recordflux

The Future



adacore.com/recordflux

Tobias Reiher
reiher@adacore.com