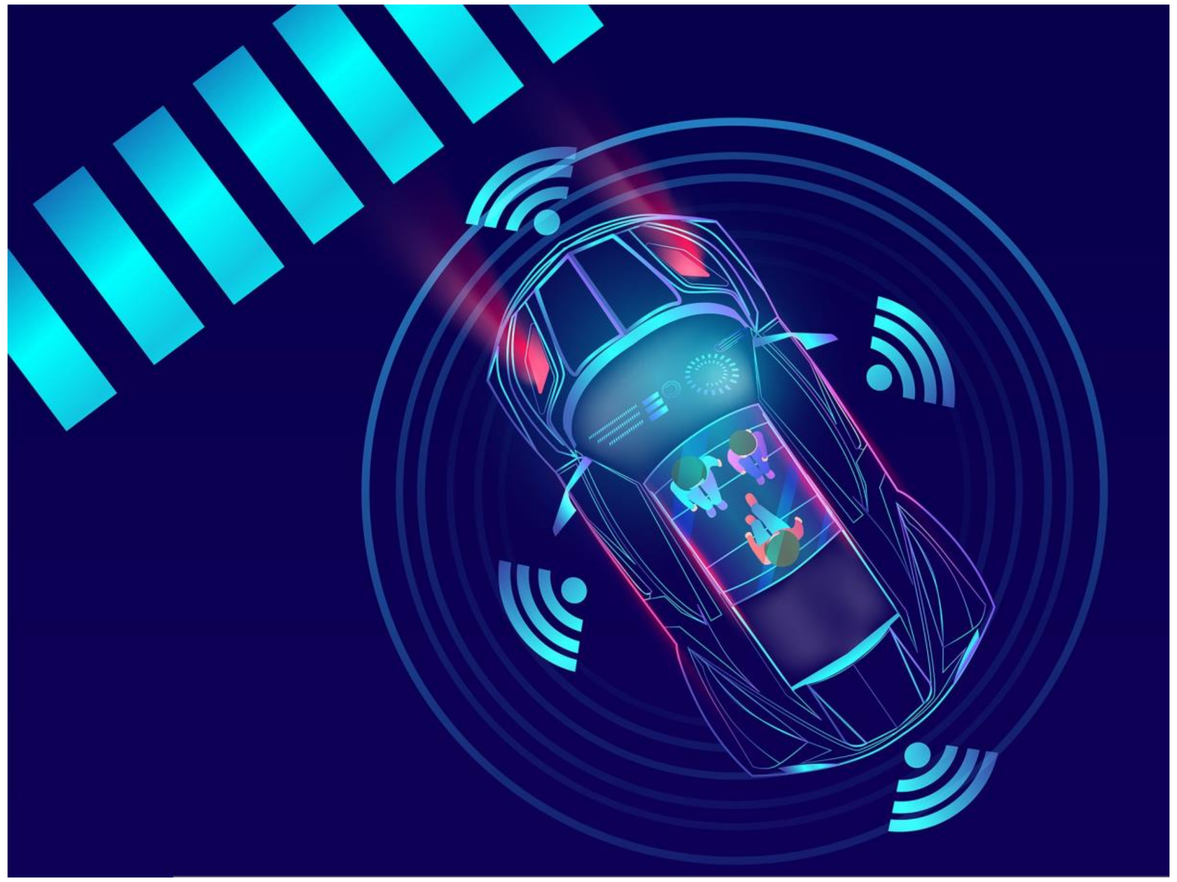
November 20th, 2025

MaxiMals: A Low-cost Hardening Technique for Large Vision Transformers

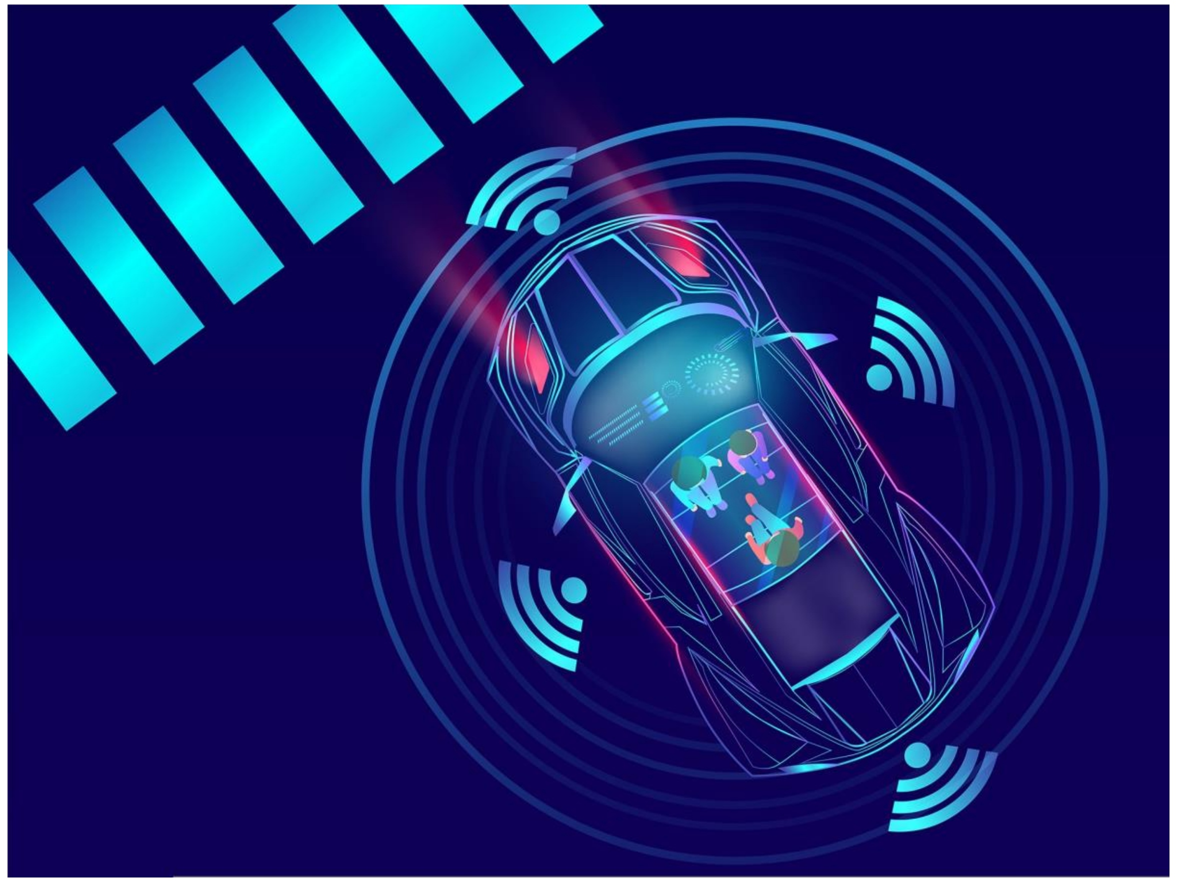
Lucas Roquet, Fernando Fernandes dos Santos, Paolo Rech, Marcello Traiola, Olivier Sentieys, and Angeliki Kritikakou

Machine Learning (ML) is Everywhere



- ML models are very **complex** and very **accurate**
- They can be applied to a wide range of applications

Machine Learning (ML) is Everywhere



ML models are included in Safety-critical Applications

Transformer Models

Transformer Models

- Transformers, state-of-the-art of ML

Transformer Models

- Transformers, state-of-the-art of ML
  - Highly accurate

Transformer Models

- Transformers, state-of-the-art of ML
  - Highly accurate
  - Various tasks : language processing, radar processing or…

Transformer Models

- Transformers, state-of-the-art of ML
  - Highly accurate
  - Various tasks : language processing, radar processing or…
  - … computer vision (ViTs)

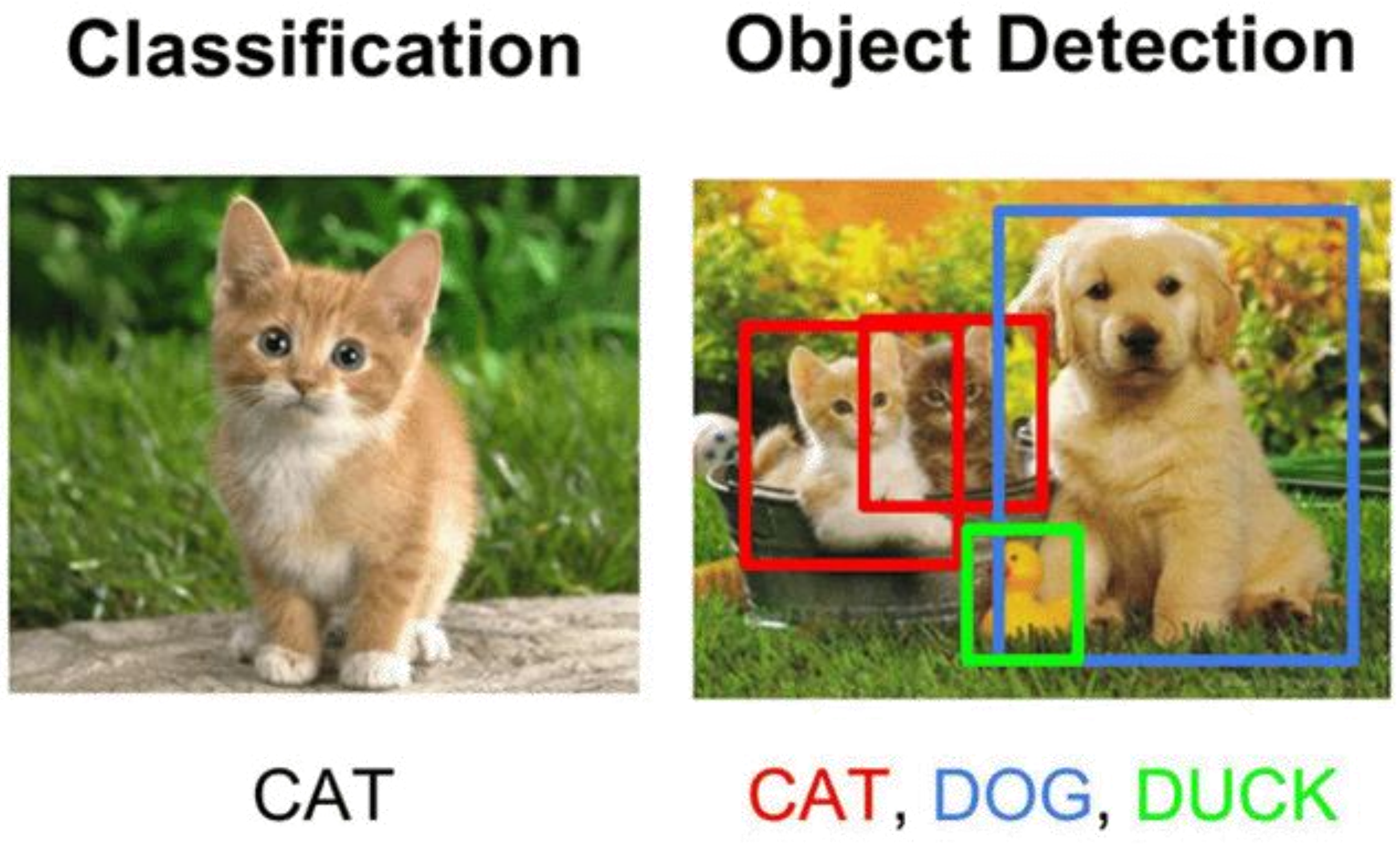
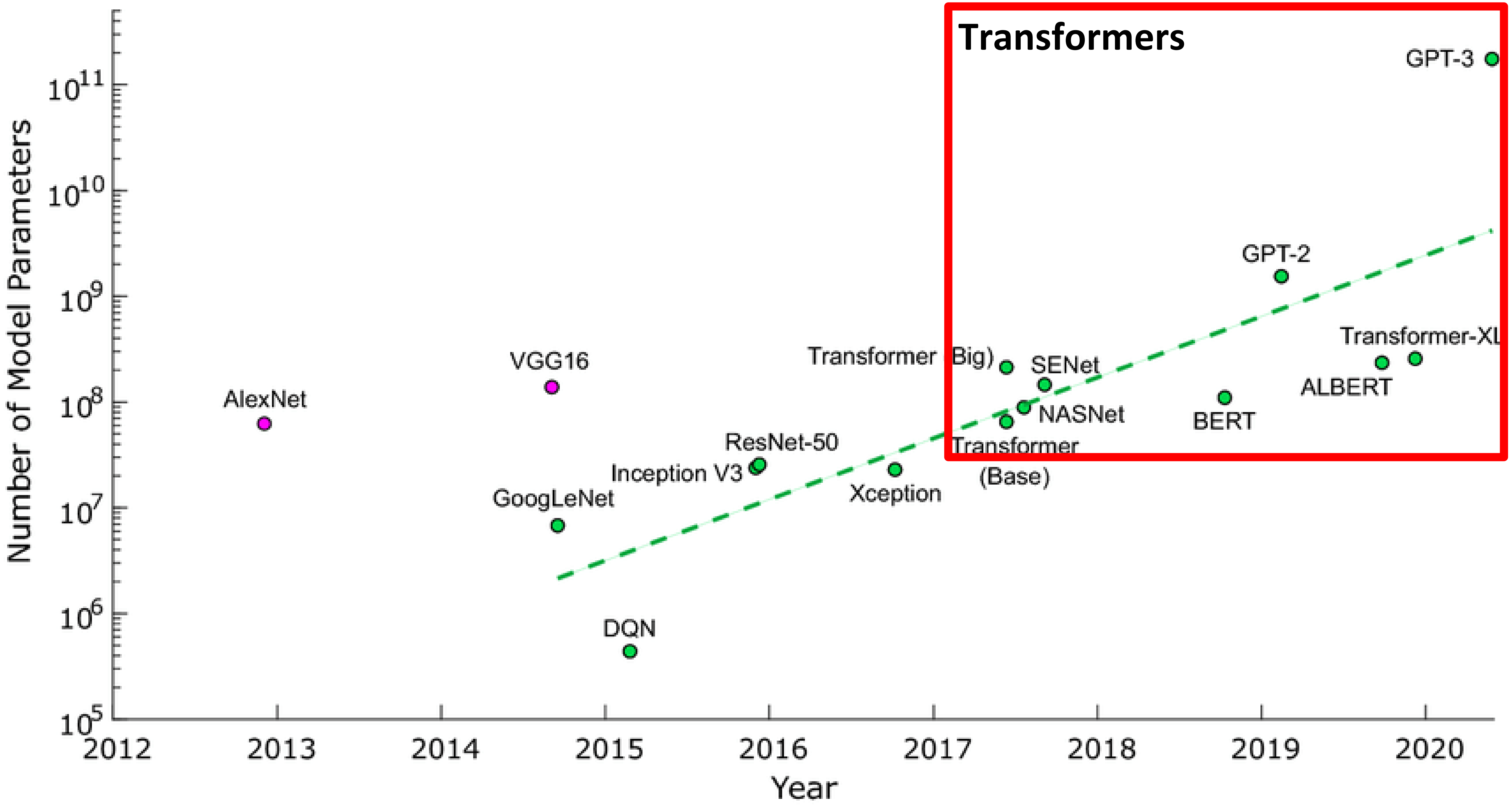


Image Segmentation

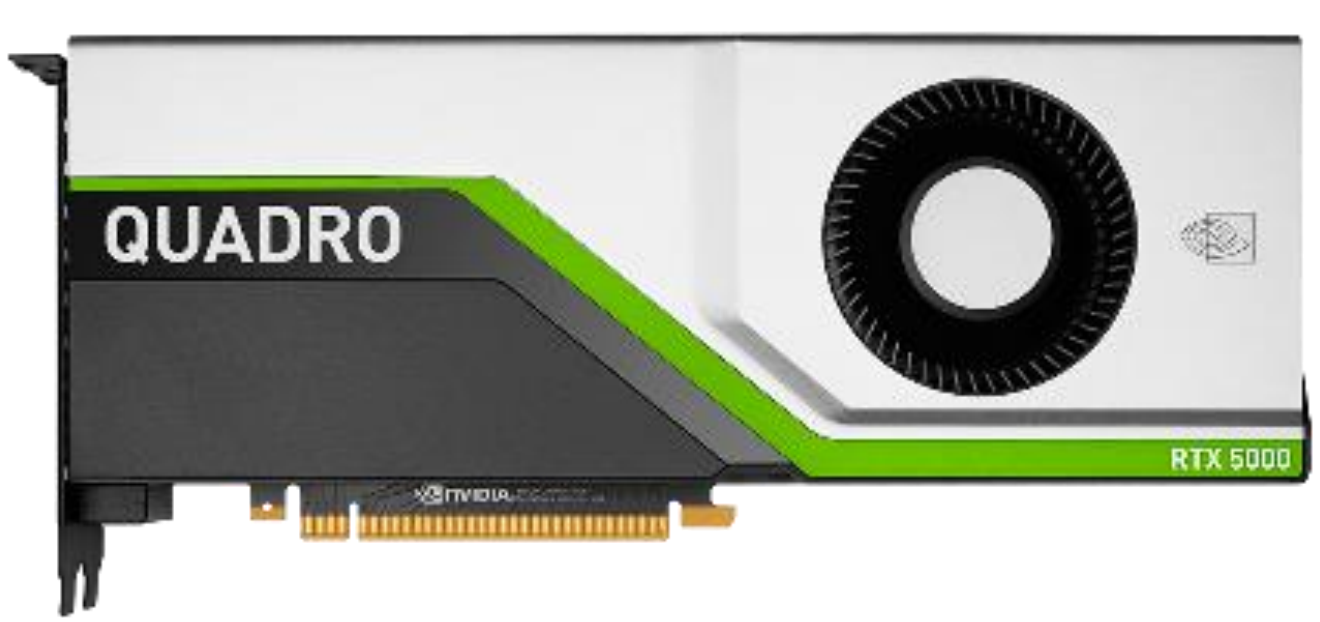
Transformer Models

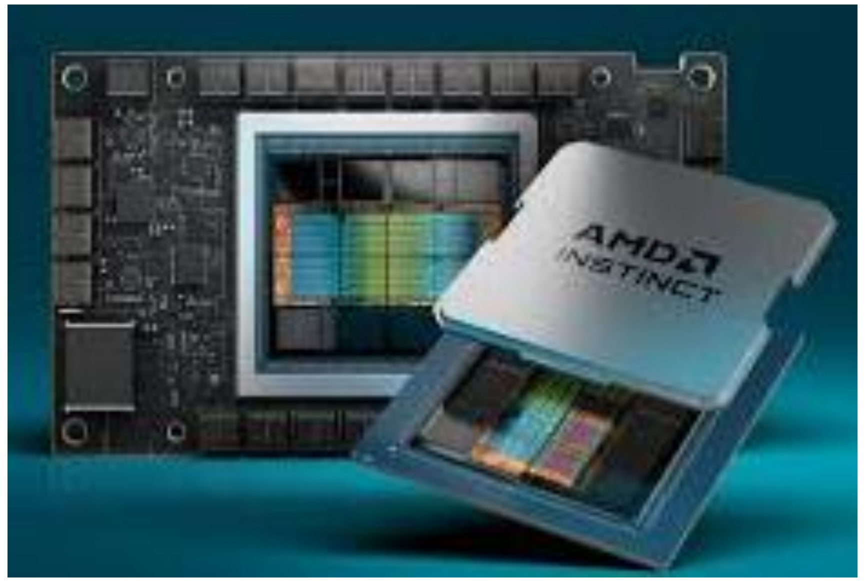


Evolution of the number of parameters of ML models[1]

[1] L. Bernstein *et al.* – Nature 2021

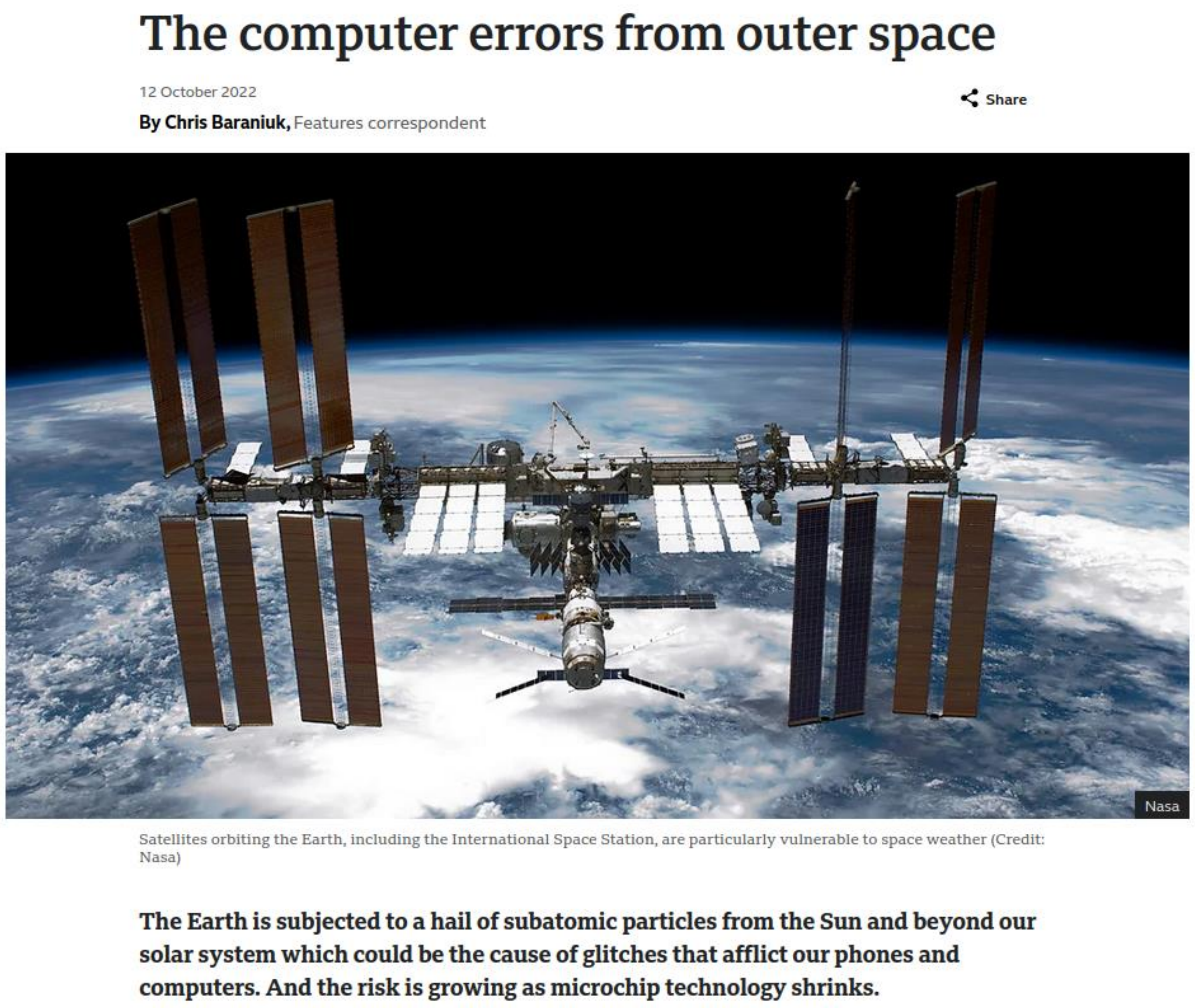
Transformer Models





They need large hardware accelerators

Vulnerability Sources



The computer errors from outer space

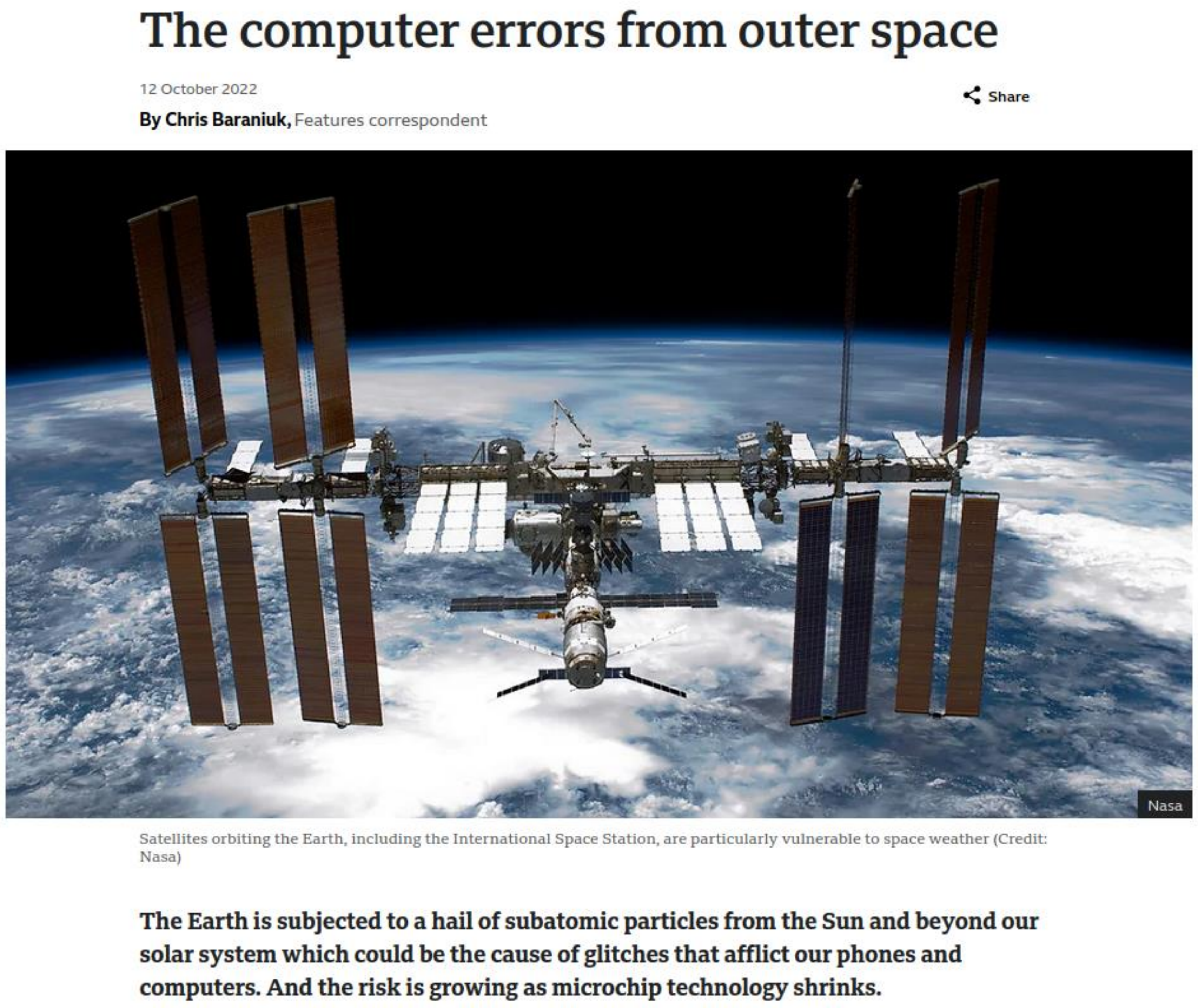
12 October 2022

By Chris Baraniuk, Features correspondent

Satellites orbiting the Earth, including the International Space Station, are particularly vulnerable to space weather (Credit: Nasa)

The Earth is subjected to a hail of subatomic particles from the Sun and beyond our solar system which could be the cause of glitches that afflict our phones and computers. And the risk is growing as microchip technology shrinks.

Vulnerability Sources



The computer errors from outer space

12 October 2022

Share

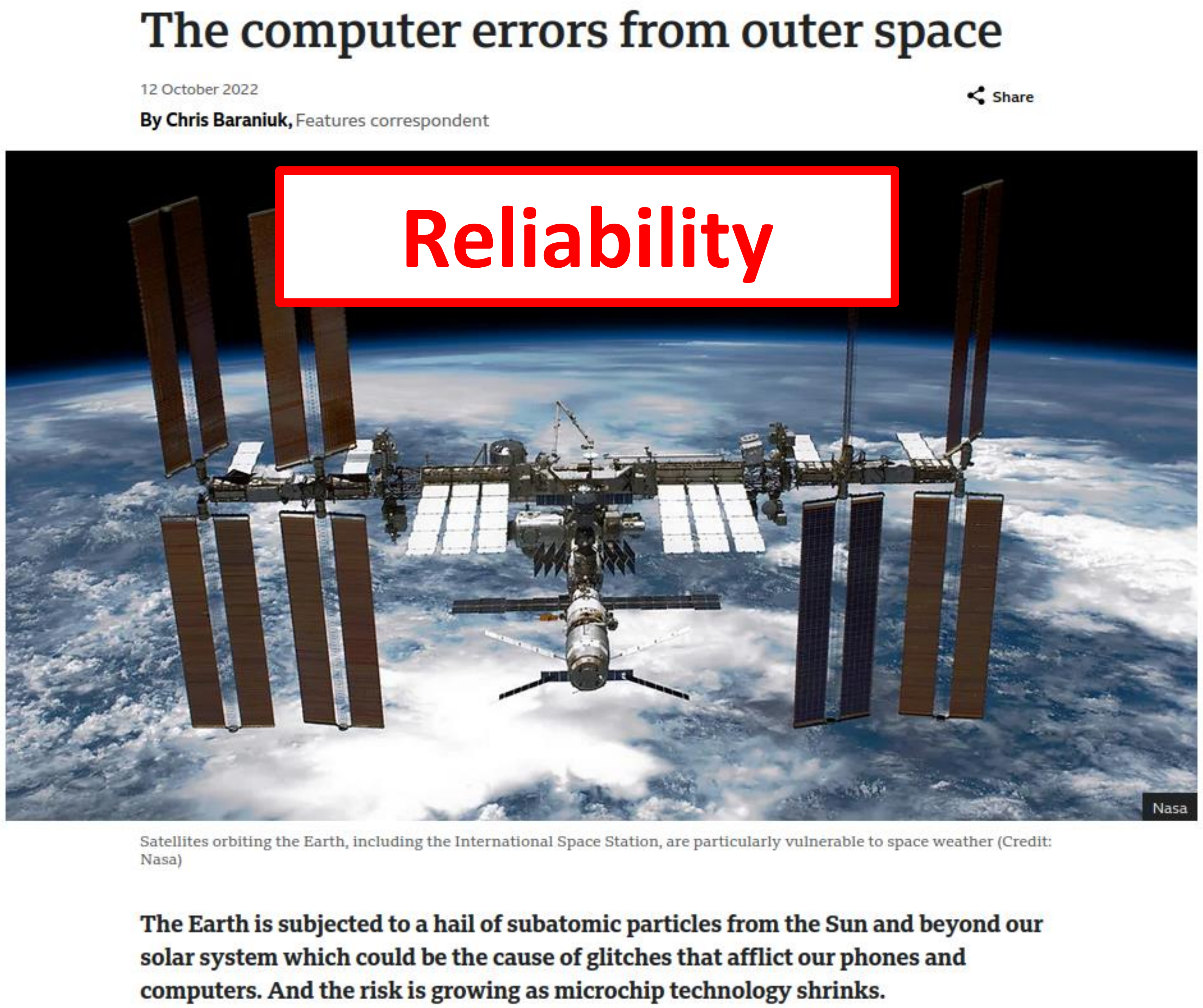
By Chris Baraniuk, Features correspondent

Satellites orbiting the Earth, including the International Space Station, are particularly vulnerable to space weather (Credit: Nasa)

The Earth is subjected to a hail of subatomic particles from the Sun and beyond our solar system which could be the cause of glitches that afflict our phones and computers. And the risk is growing as microchip technology shrinks.

☢ Neutrons, Protons, Heavy-ions, etc.

Vulnerability Sources



The computer errors from outer space

12 October 2022

Share

By Chris Baraniuk, Features correspondent

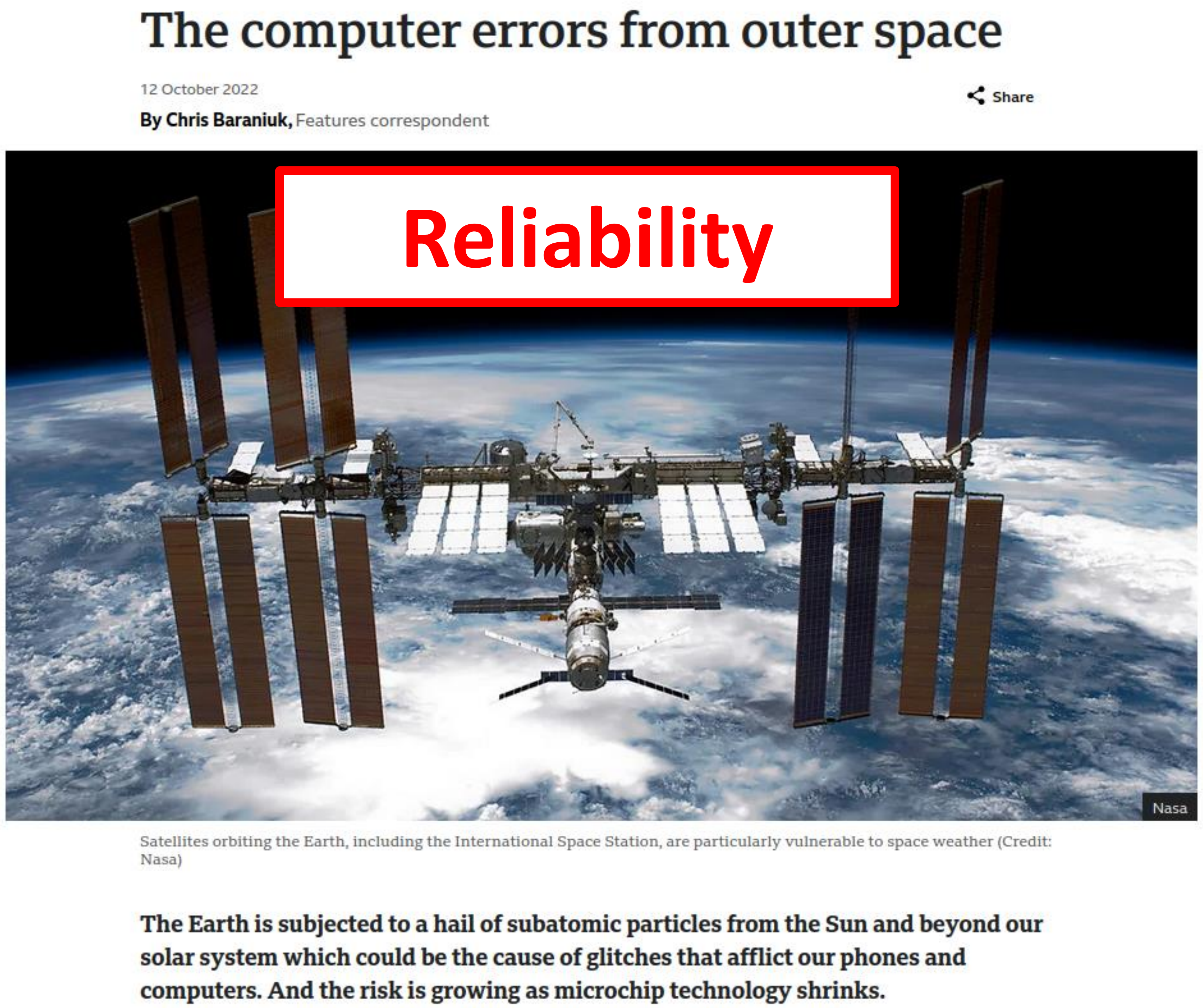
Reliability

Satellites orbiting the Earth, including the International Space Station, are particularly vulnerable to space weather (Credit: Nasa)

The Earth is subjected to a hail of subatomic particles from the Sun and beyond our solar system which could be the cause of glitches that afflict our phones and computers. And the risk is growing as microchip technology shrinks.

Neutrons, Protons, Heavy-ions, etc.

Vulnerability Sources



The computer errors from outer space

12 October 2022

Share

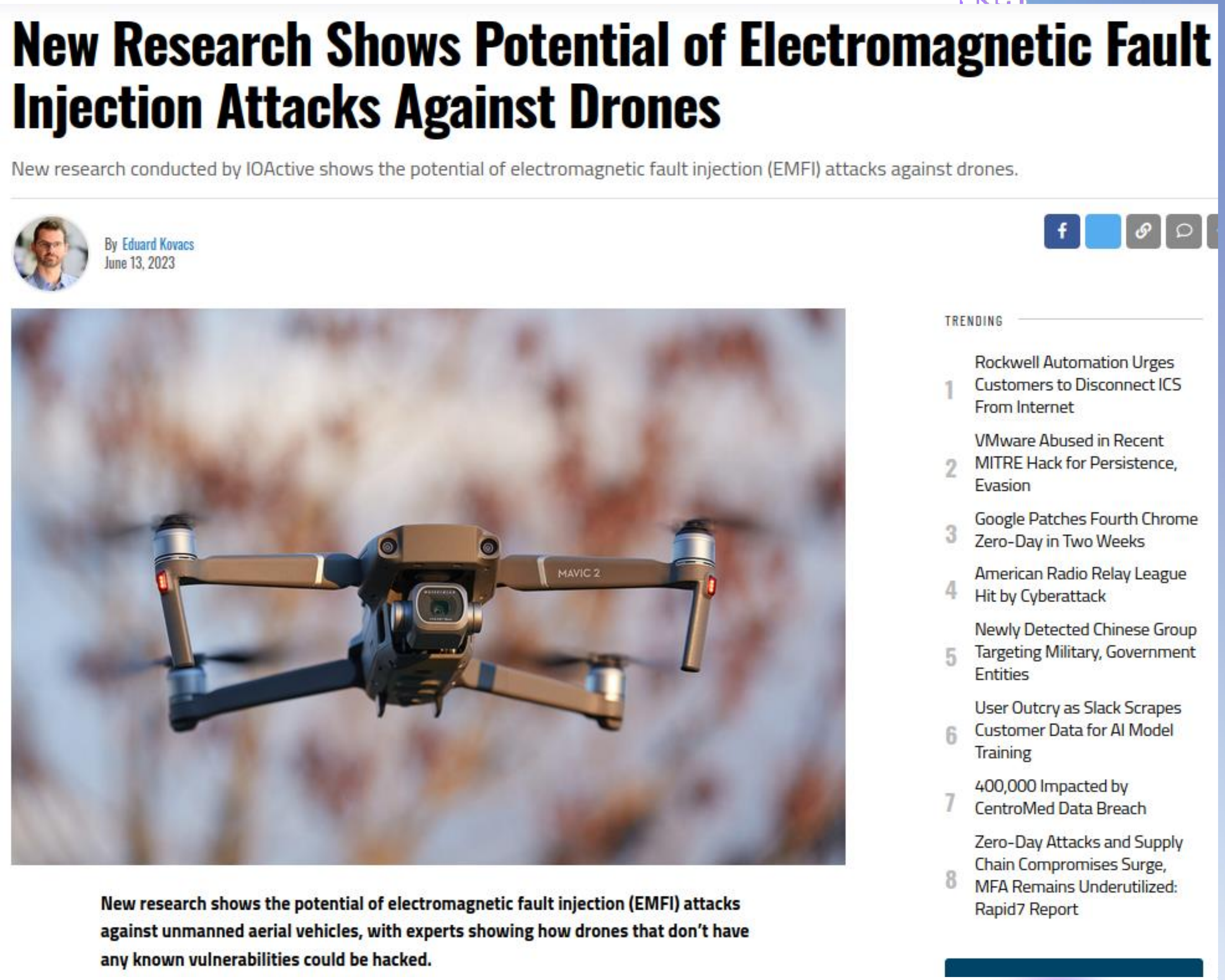
By Chris Baraniuk, Features correspondent

Reliability

Satellites orbiting the Earth, including the International Space Station, are particularly vulnerable to space weather (Credit: Nasa)

The Earth is subjected to a hail of subatomic particles from the Sun and beyond our solar system which could be the cause of glitches that afflict our phones and computers. And the risk is growing as microchip technology shrinks.

Neutrons, Protons, Heavy-ions, etc.



New Research Shows Potential of Electromagnetic Fault Injection Attacks Against Drones

New research conducted by IOActive shows the potential of electromagnetic fault injection (EMFI) attacks against drones.

By Eduard Kovacs
June 13, 2023

New research shows the potential of electromagnetic fault injection (EMFI) attacks against unmanned aerial vehicles, with experts showing how drones that don't have any known vulnerabilities could be hacked.

TRENDING

1 Rockwell Automation Urges Customers to Disconnect ICS From Internet

2 VMware Abused in Recent MITRE Hack for Persistence, Evasion

3 Google Patches Fourth Chrome Zero-Day in Two Weeks

4 American Radio Relay League Hit by Cyberattack

5 Newly Detected Chinese Group Targeting Military, Government Entities

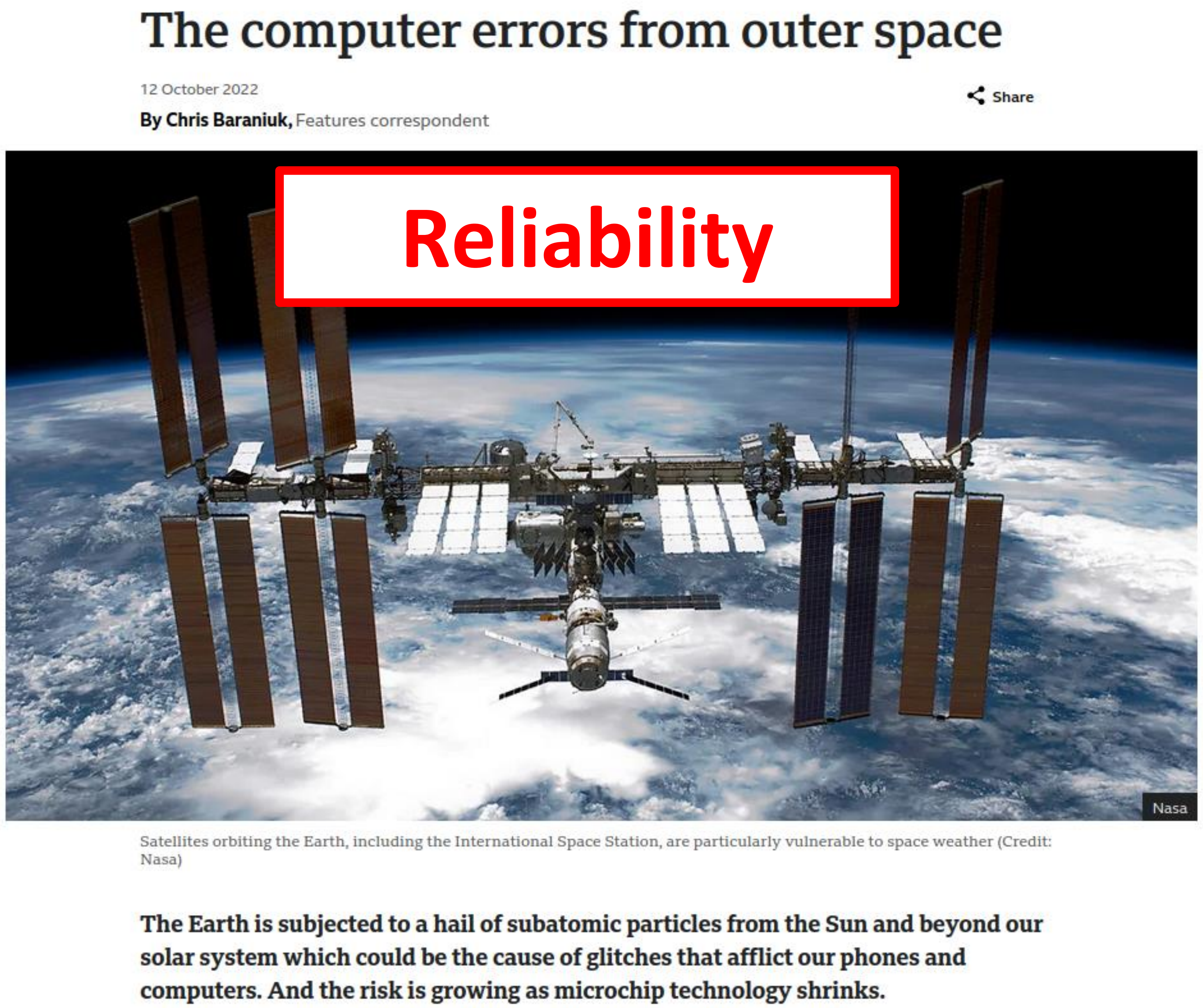
6 User Outcry as Slack Scrapes Customer Data for AI Model Training

7 400,000 Impacted by CentroMed Data Breach

8 Zero-Day Attacks and Supply Chain Compromises Surge, MFA Remains Underutilized: Rapid7 Report

European Cyber Week

Vulnerability Sources



The computer errors from outer space

12 October 2022

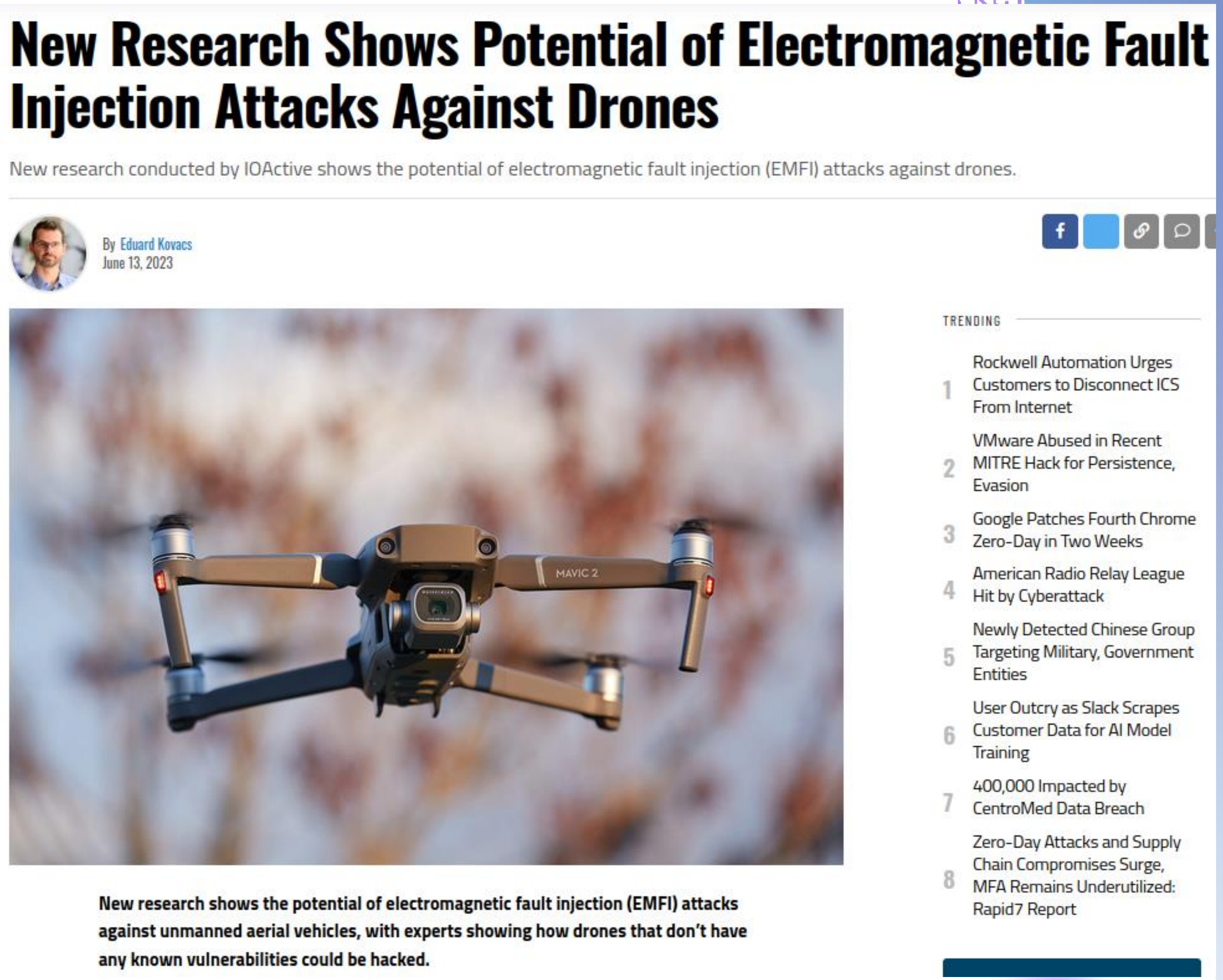
Share

By Chris Baraniuk, Features correspondent

Reliability

Satellites orbiting the Earth, including the International Space Station, are particularly vulnerable to space weather (Credit: Nasa)

The Earth is subjected to a hail of subatomic particles from the Sun and beyond our solar system which could be the cause of glitches that afflict our phones and computers. And the risk is growing as microchip technology shrinks.



New Research Shows Potential of Electromagnetic Fault Injection Attacks Against Drones

New research conducted by IOActive shows the potential of electromagnetic fault injection (EMFI) attacks against drones.

By Eduard Kovacs
June 13, 2023

New research shows the potential of electromagnetic fault injection (EMFI) attacks against unmanned aerial vehicles, with experts showing how drones that don't have any known vulnerabilities could be hacked.

TRENDING

1 Rockwell Automation Urges Customers to Disconnect ICS From Internet

2 VMware Abused in Recent MITRE Hack for Persistence, Evasion

3 Google Patches Fourth Chrome Zero-Day in Two Weeks

4 American Radio Relay League Hit by Cyberattack

5 Newly Detected Chinese Group Targeting Military, Government Entities

6 User Outcry as Slack Scrapes Customer Data for AI Model Training

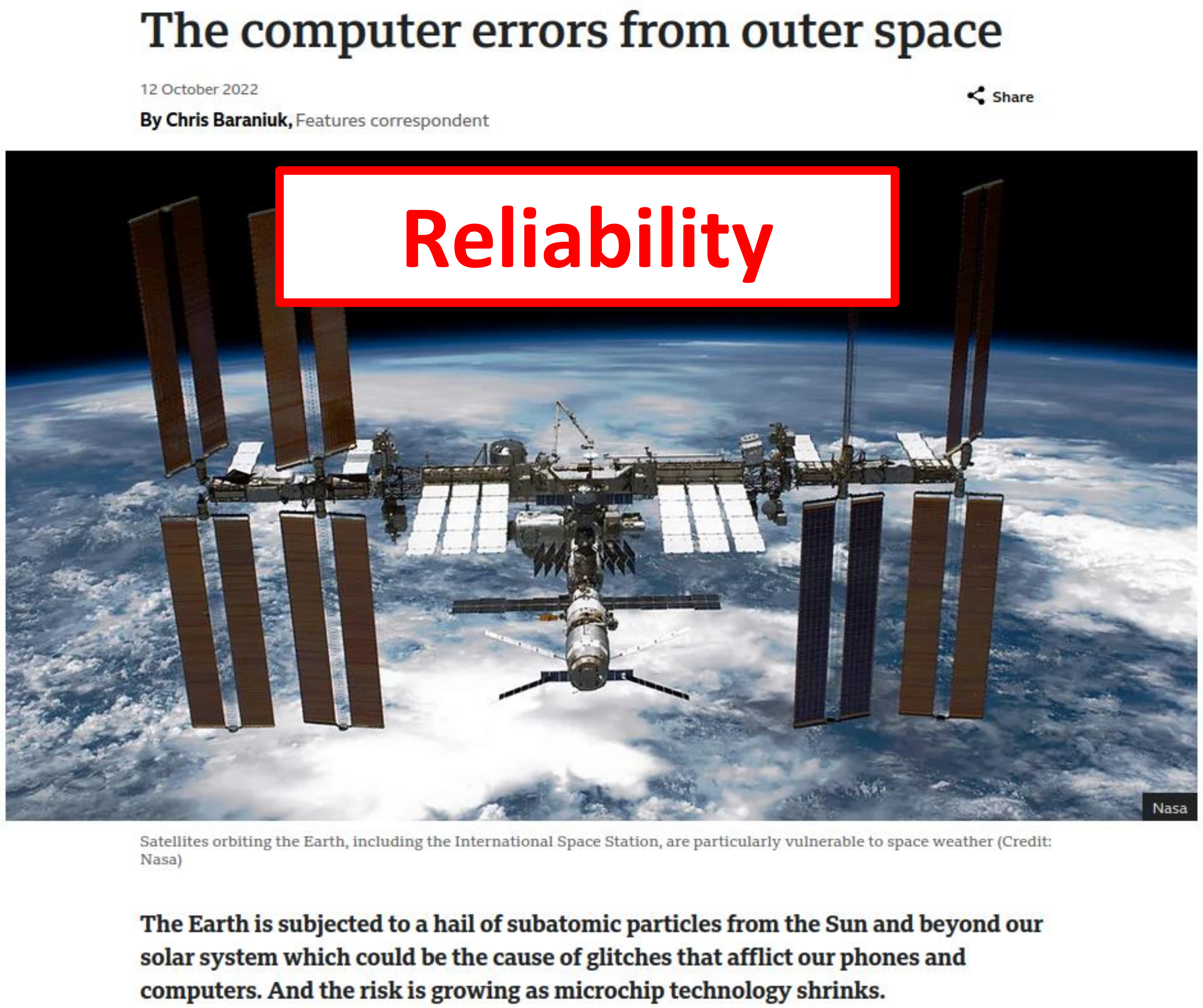
7 400,000 Impacted by CentroMed Data Breach

8 Zero-Day Attacks and Supply Chain Compromises Surge, MFA Remains Underutilized: Rapid7 Report

☢ Neutrons, Protons, Heavy-ions, etc.

Electromagnetic FI, laser FI, SCAs, etc.

Vulnerability Sources



The computer errors from outer space

12 October 2022

Share

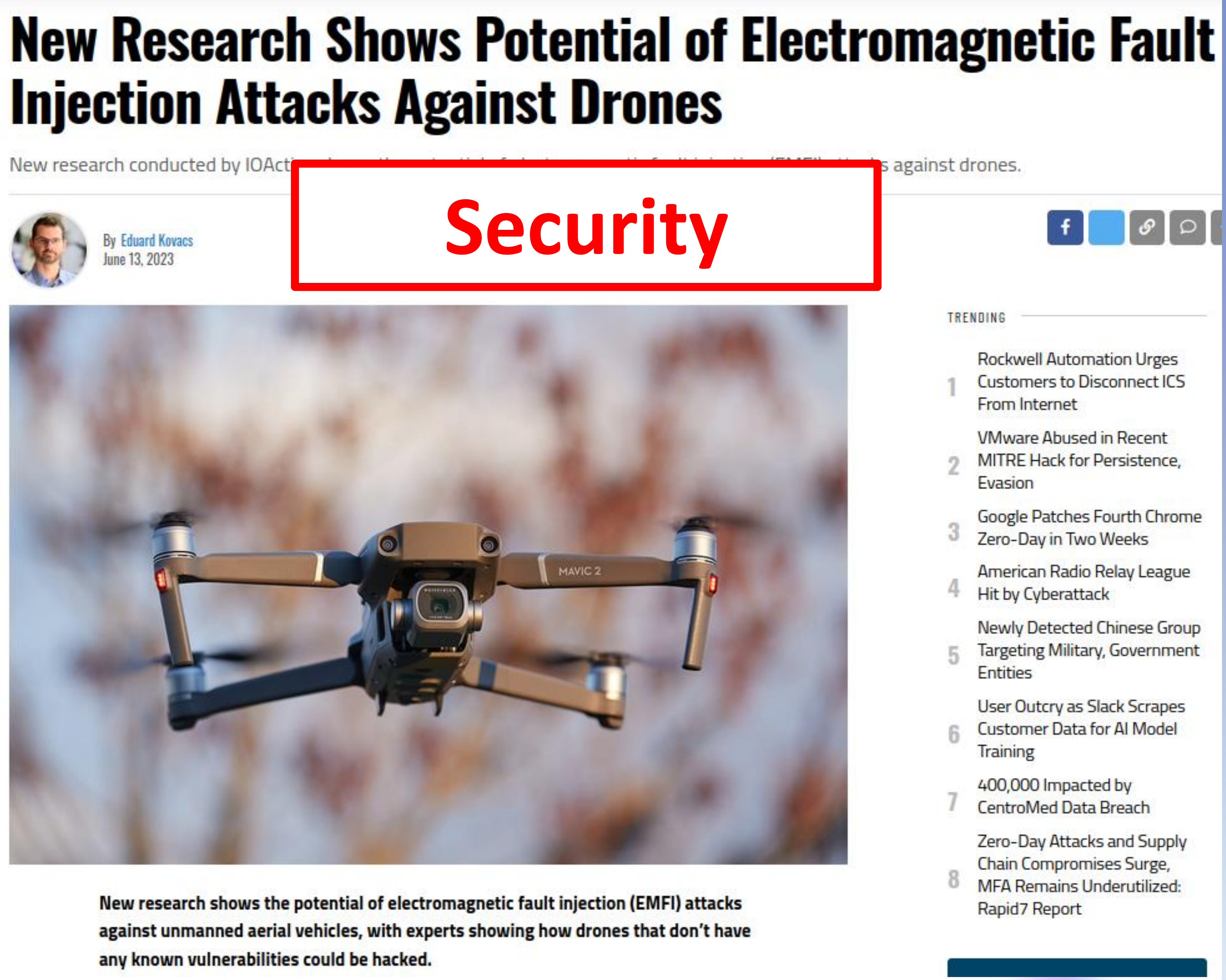
By Chris Baraniuk, Features correspondent

Reliability

Satellites orbiting the Earth, including the International Space Station, are particularly vulnerable to space weather (Credit: Nasa)

The Earth is subjected to a hail of subatomic particles from the Sun and beyond our solar system which could be the cause of glitches that afflict our phones and computers. And the risk is growing as microchip technology shrinks.

☢ Neutrons, Protons, Heavy-ions, etc.



New Research Shows Potential of Electromagnetic Fault Injection Attacks Against Drones

New research conducted by IOActi s against drones.

Security

By Eduard Kovacs
June 13, 2023

New research shows the potential of electromagnetic fault injection (EMFI) attacks against unmanned aerial vehicles, with experts showing how drones that don't have any known vulnerabilities could be hacked.

TRENDING

1 Rockwell Automation Urges Customers to Disconnect ICS From Internet

2 VMware Abused in Recent MITRE Hack for Persistence, Evasion

3 Google Patches Fourth Chrome Zero-Day in Two Weeks

4 American Radio Relay League Hit by Cyberattack

5 Newly Detected Chinese Group Targeting Military, Government Entities

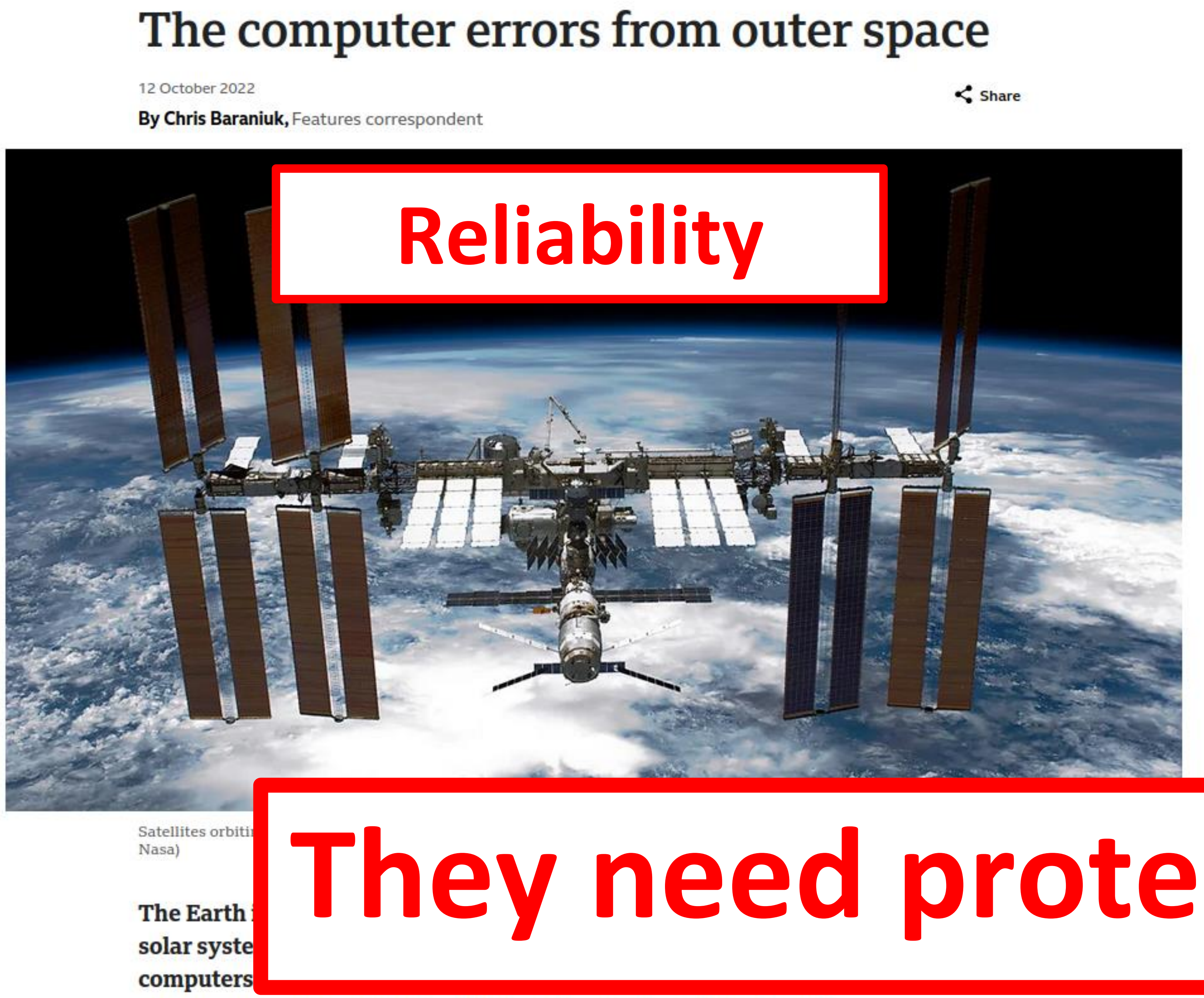
6 User Outcry as Slack Scrapes Customer Data for AI Model Training

7 400,000 Impacted by CentroMed Data Breach

8 Zero-Day Attacks and Supply Chain Compromises Surge, MFA Remains Underutilized: Rapid7 Report

Electromagnetic FI, laser FI, SCAs, etc.

Vulnerability Sources



The computer errors from outer space

12 October 2022

Share

By Chris Baraniuk, Features correspondent

Satellites orbiti
Nasa)

The Earth i
solar syste
computers

Reliability

New Research Shows Potential of Electromagnetic Fault Injection Attacks Against Drones

New research conducted by IOActi s against drones.

By Eduard Kovacs
June 13, 2023

TRENDING

1 Rockwell Automation Urges Customers to Disconnect ICS From Internet

2 VMware Abused in Recent MITRE Hack for Persistence, Evasion

3 Google Patches Fourth Chrome Zero-Day in Two Weeks

4 American Radio Relay League Hit by Cyberattack

5 Newly Detected Chinese Group Targeting Military, Government Entities

6 User Outcry as Slack Scrapes Customer Data for AI Model Training

7 400,000 Impacted by CentroMed Data Breach

8 Zero-Day Attacks and Supply Chain Compromises Surge, MFA Remains Underutilized: Rapid7 Report

any known vulnerabilities could be hacked.

Security

They need protection mechanisms

Neutrons, Protons, Heavy-ions, etc.

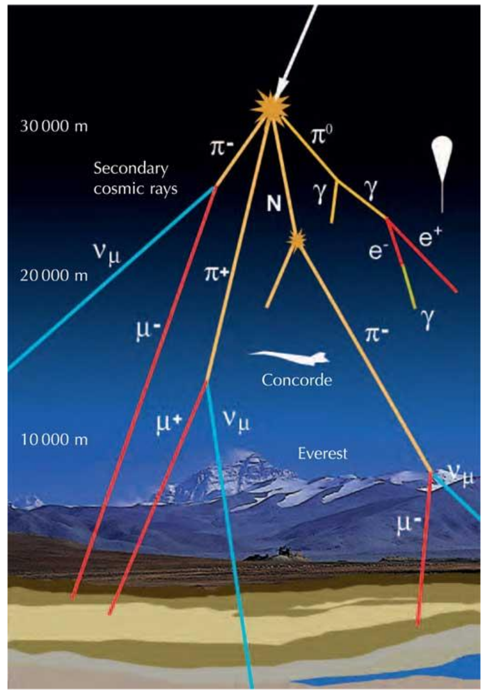
Electromagnetic FI, laser FI, SCAs, etc.

Agenda

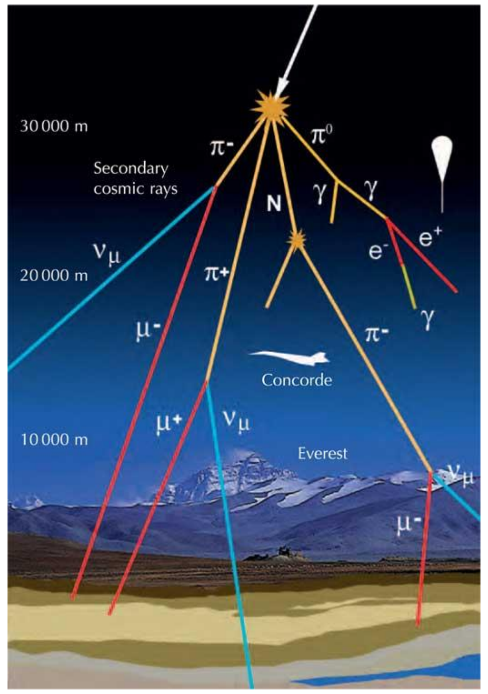
- Radiation Effects on ML
- ViT Reliability Characterization
- Efficient Fault Tolerance
- Conclusions and Future Directions

Radiation Effects on ML

Radiation Impact on GPUs



Radiation Impact on GPUs

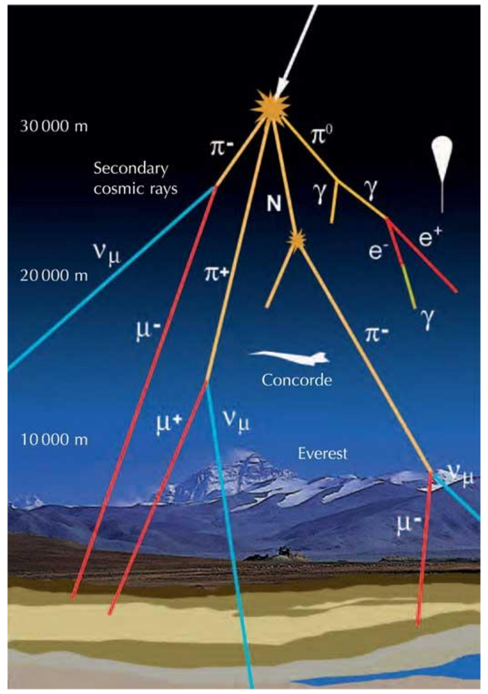


Ionizing particle

Memories

0 1 0 0 0 1 0 0 1 0 1 0 0 0 1 1
0 1 1 1 0 1 0 0 1 0 1 0 1 0 0 0
1 0 0 1 1 0 1 0 1 0 1 0 0 0 1 1
0 1 0 1 0 1 0 1 1 0 1 0 0 1 0 0

Radiation Impact on GPUs



Ionizing particle

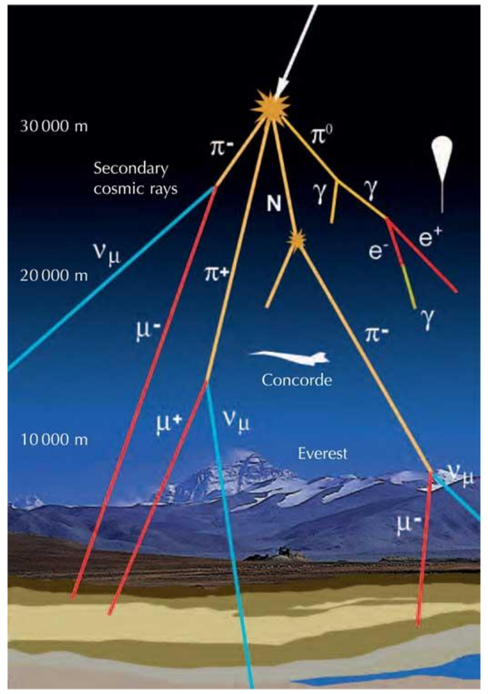
Memories

0 1 0 0 0 1 0 0 1 0 1 0 0 0 1 1
0 1 1 1 0 1 0 0 1 0 1 0 1 0 0 0
1 0 0 1 1 0 1 0 1 0 1 0 0 0 1 1
0 1 0 1 0 1 0 1 1 0 1 0 0 1 0 0

Logic

1 + 1 = 3

Radiation Impact on GPUs



Ionizing particle

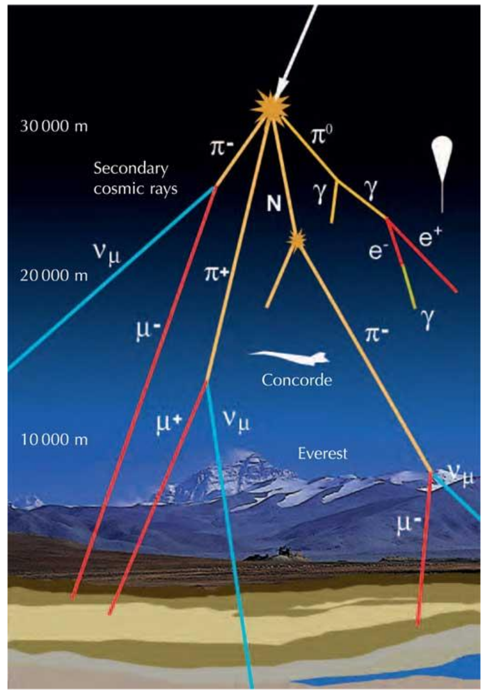
Memories

0 1 0 0 0 1 0 0 1 0 1 0 0 0 1 1
0 1 1 1 0 1 0 0 1 0 1 0 1 0 0 0
1 0 0 1 1 0 1 0 1 0 1 0 0 0 1 1
0 1 0 1 0 1 0 1 1 0 1 0 0 1 0 0

Logic

1 + 1 = 3

Radiation Impact on GPUs



Ionizing particle

Memories

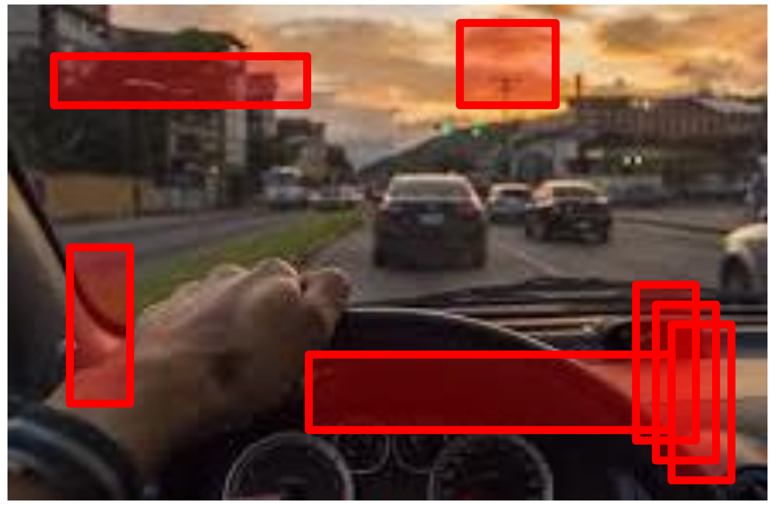
0 1 0 0 0 1 0 0 1 0 1 0 0 0 1 1
0 1 1 1 0 1 0 0 1 0 1 0 1 0 0 0
1 0 0 1 1 0 1 0 1 0 1 0 0 0 1 1
0 1 0 1 0 1 0 1 1 0 1 0 0 1 0 0

Logic

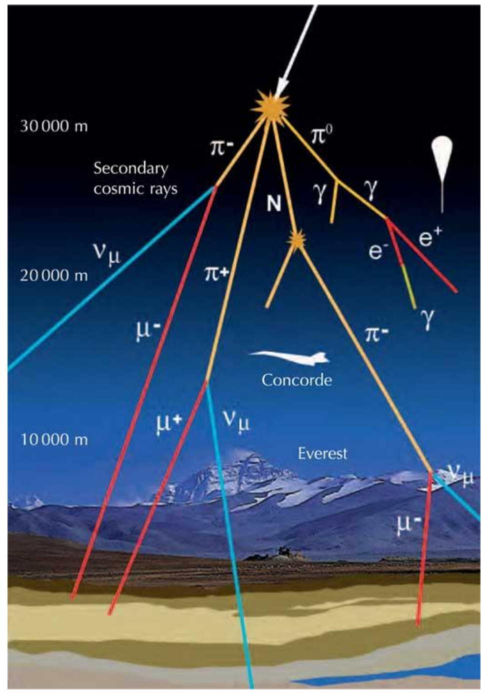
1 + 1 = 3

Silent Data Corruption (SDC)

- Computation is done but result is altered



Radiation Impact on GPUs



Ionizing particle

Memories

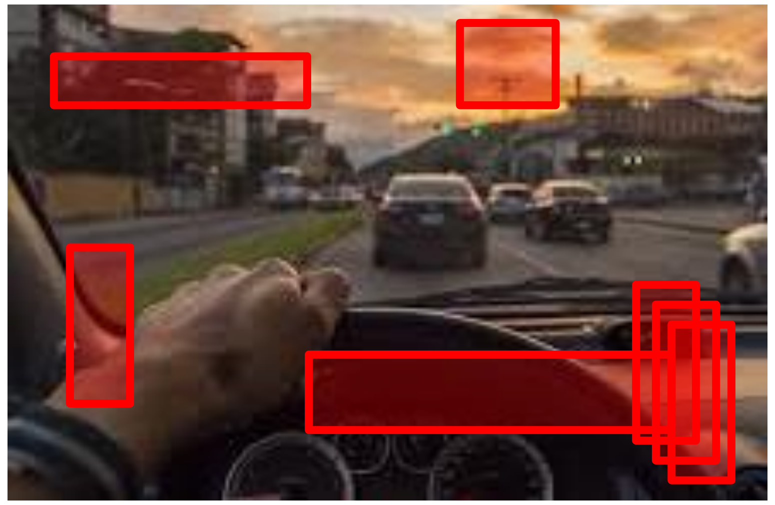
0 1 0 0 0 1 0 0 1 0 1 0 0 0 1 1
0 1 1 1 0 1 0 0 1 0 1 0 1 0 0 0
1 0 0 1 1 0 1 0 1 0 1 0 0 0 1 1
0 1 0 1 0 1 0 1 1 0 1 0 0 1 0 0

Logic

1 + 1 = 3

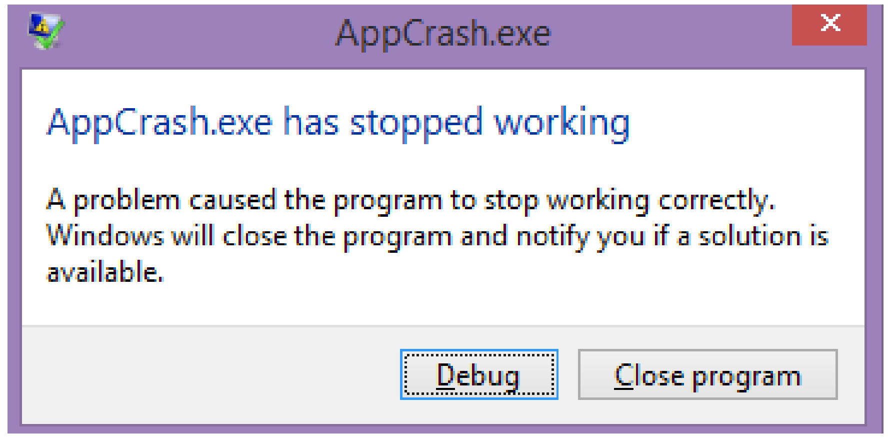
Silent Data Corruption (SDC)

- Computation is done but result is altered



Data Unrecoverable Error (DUE)

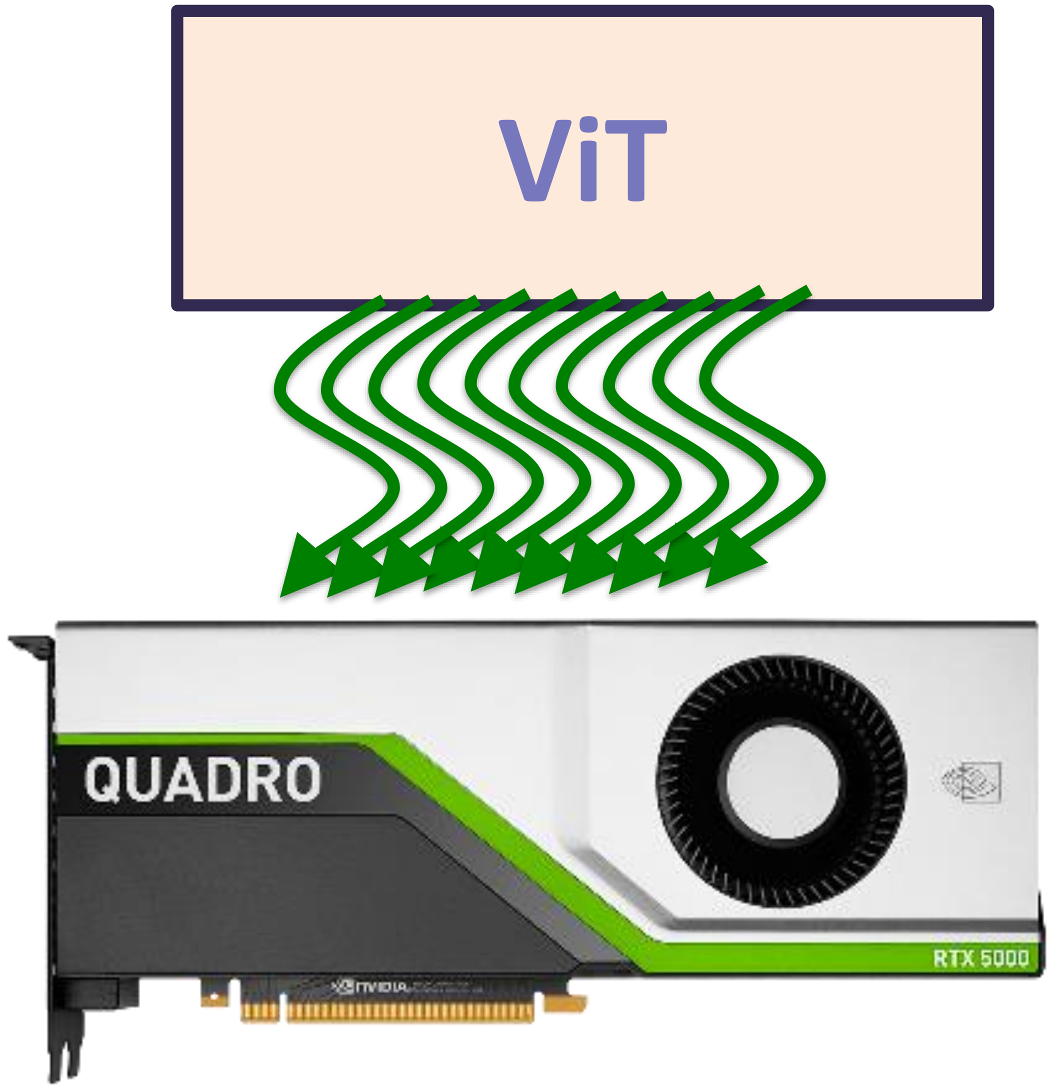
- Crash and OS hangs



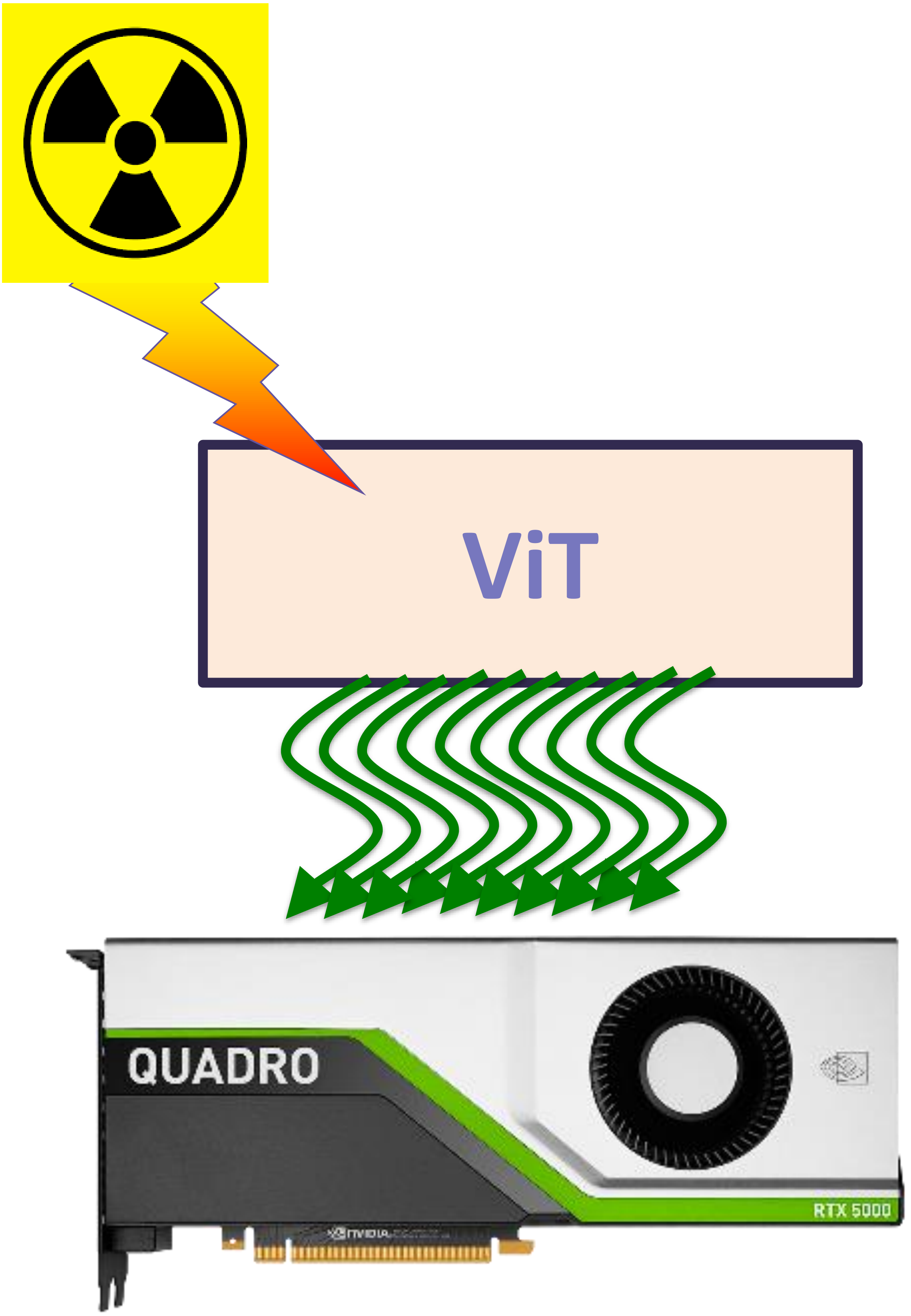
AppCrash.exe has stopped working

A problem caused the program to stop working correctly. Windows will close the program and notify you if a solution is available.

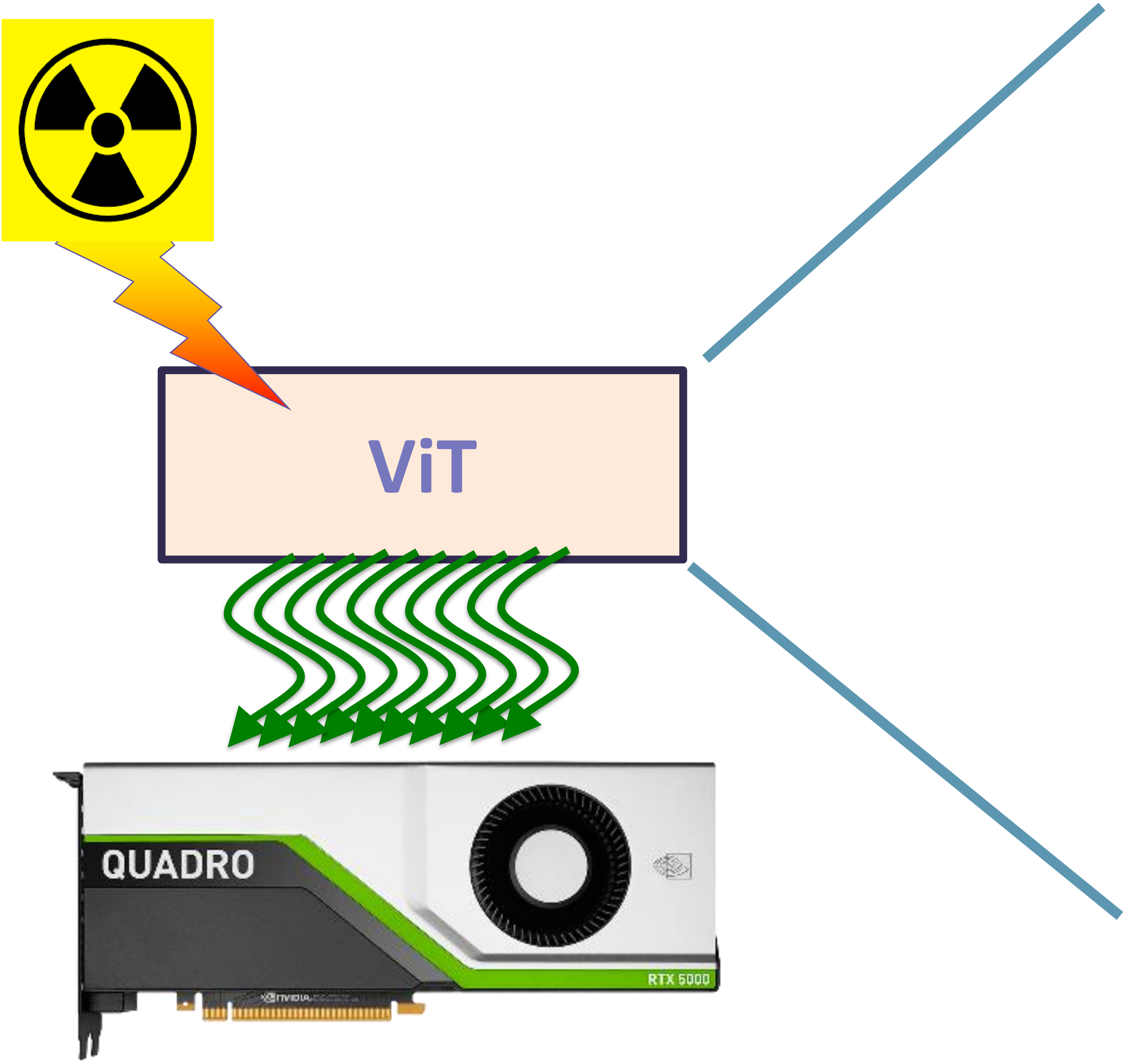
ViT SDC Types



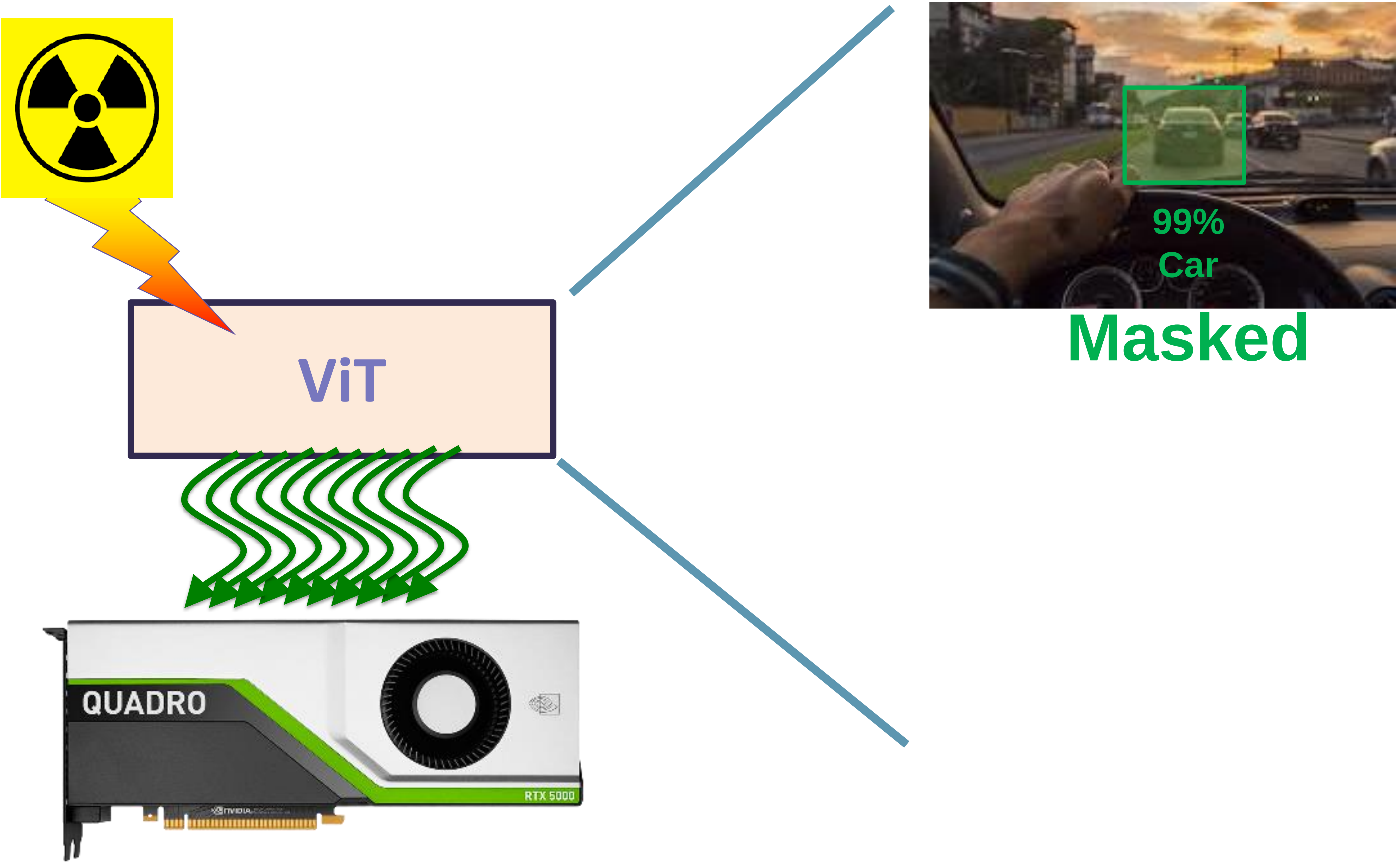
ViT SDC Types



ViT SDC Types



ViT SDC Types

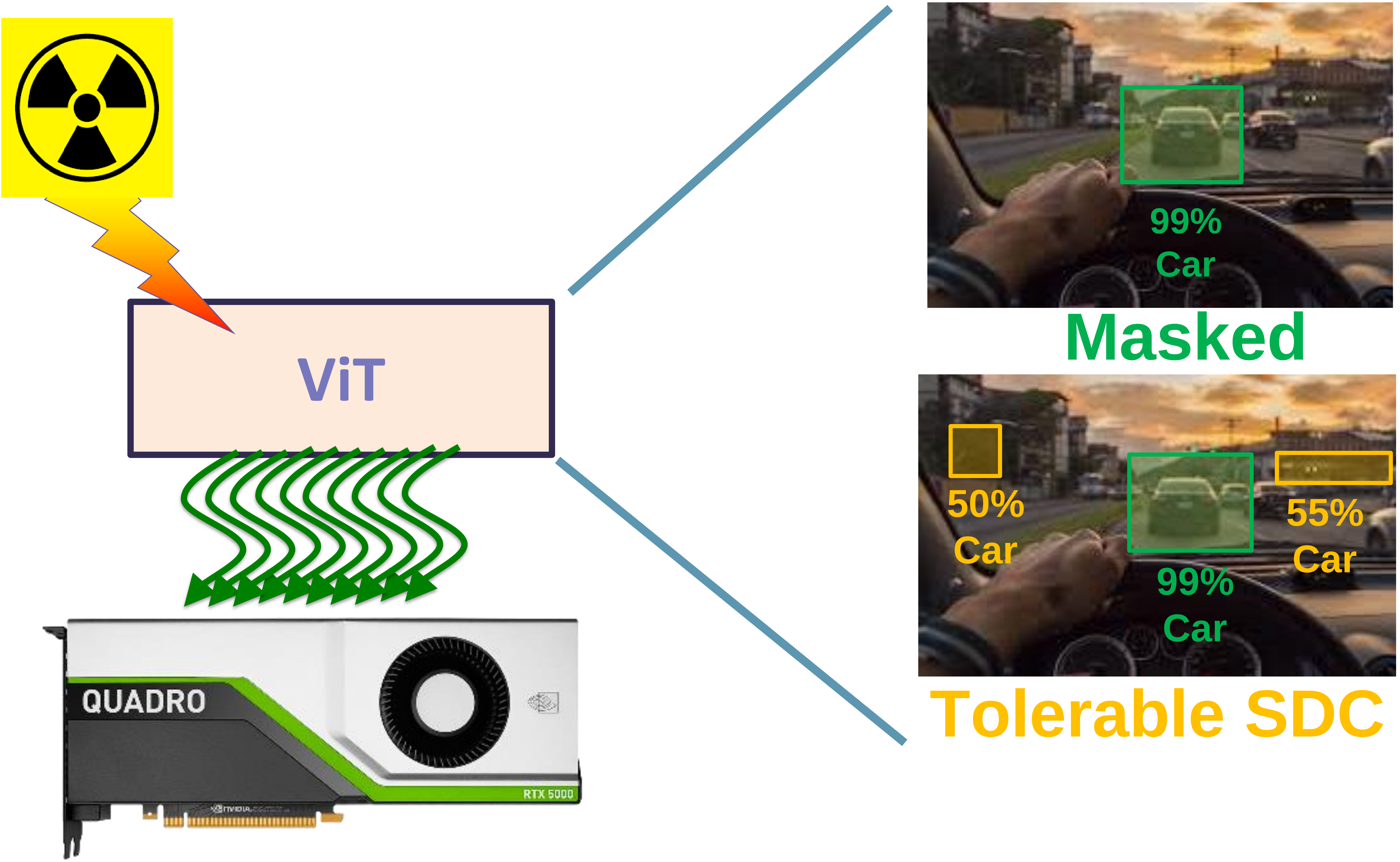


ViT

99%
Car

Masked

ViT SDC Types

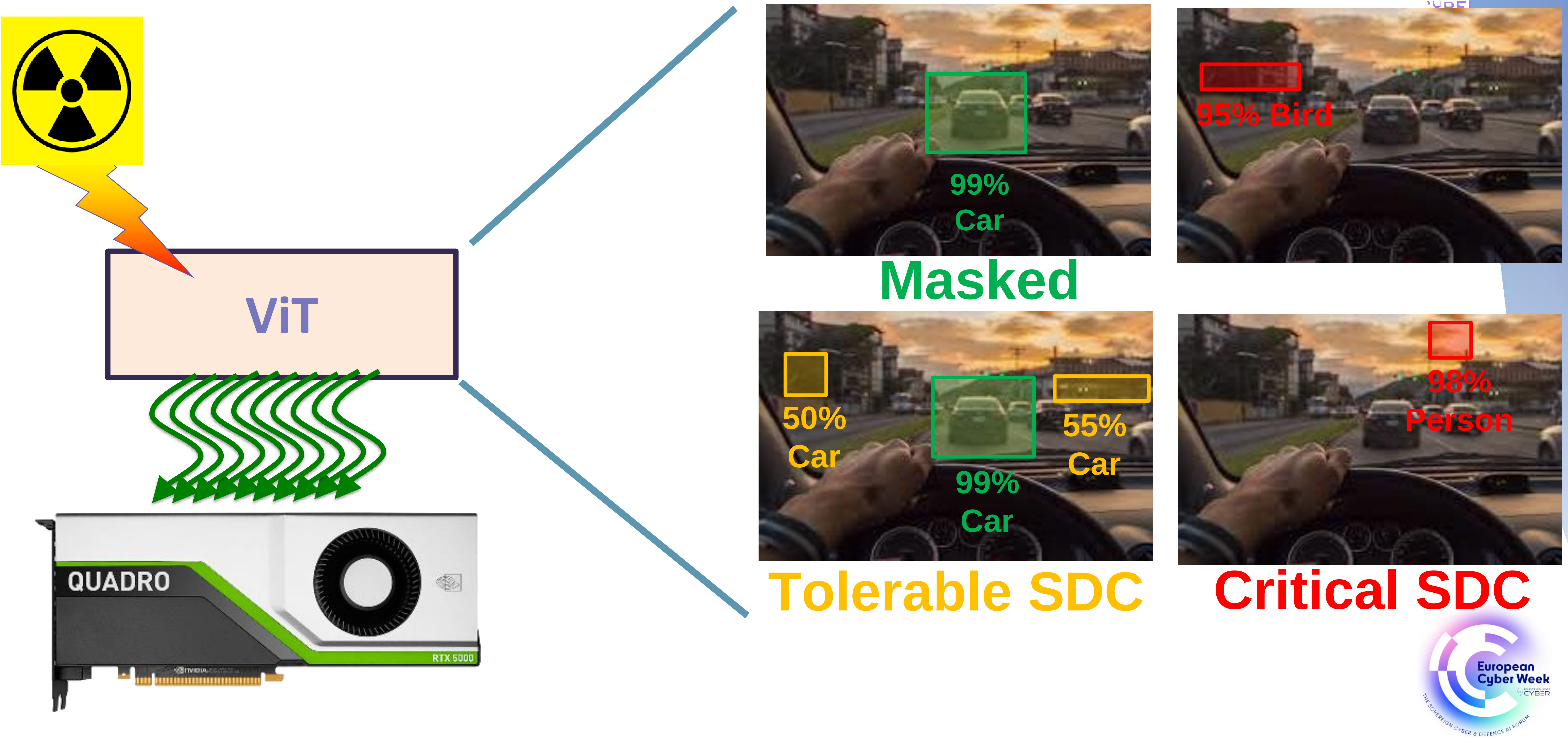


ViT

Masked

Tolerable SDC

ViT SDC Types



ViT

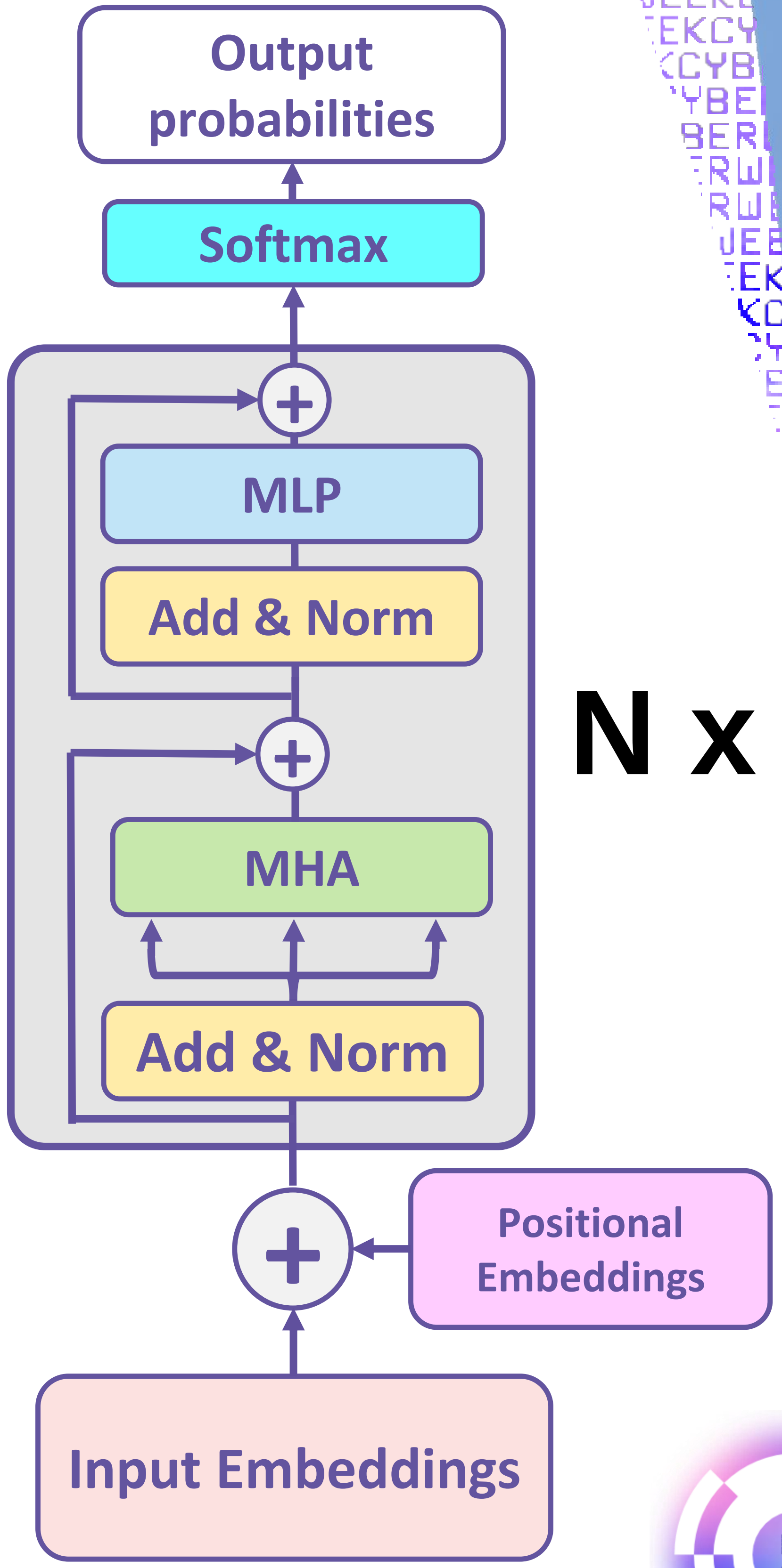
Masked

Tolerable SDC

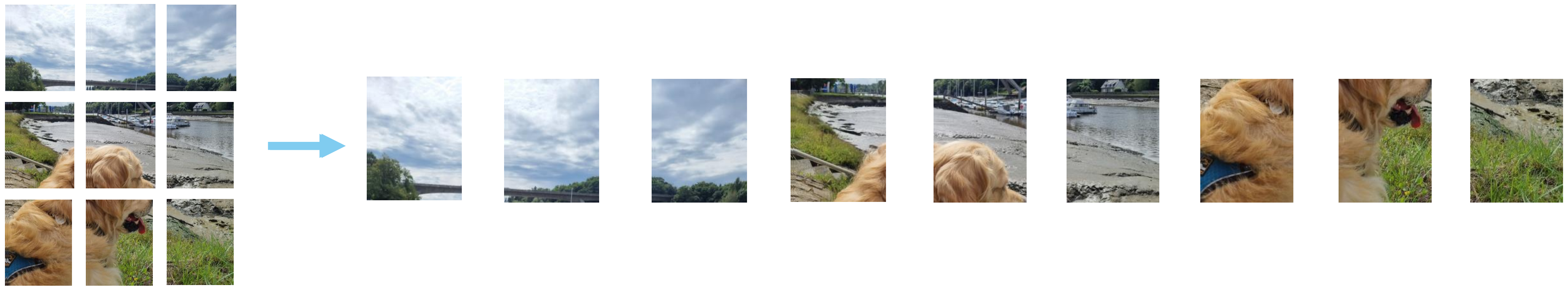
Critical SDC

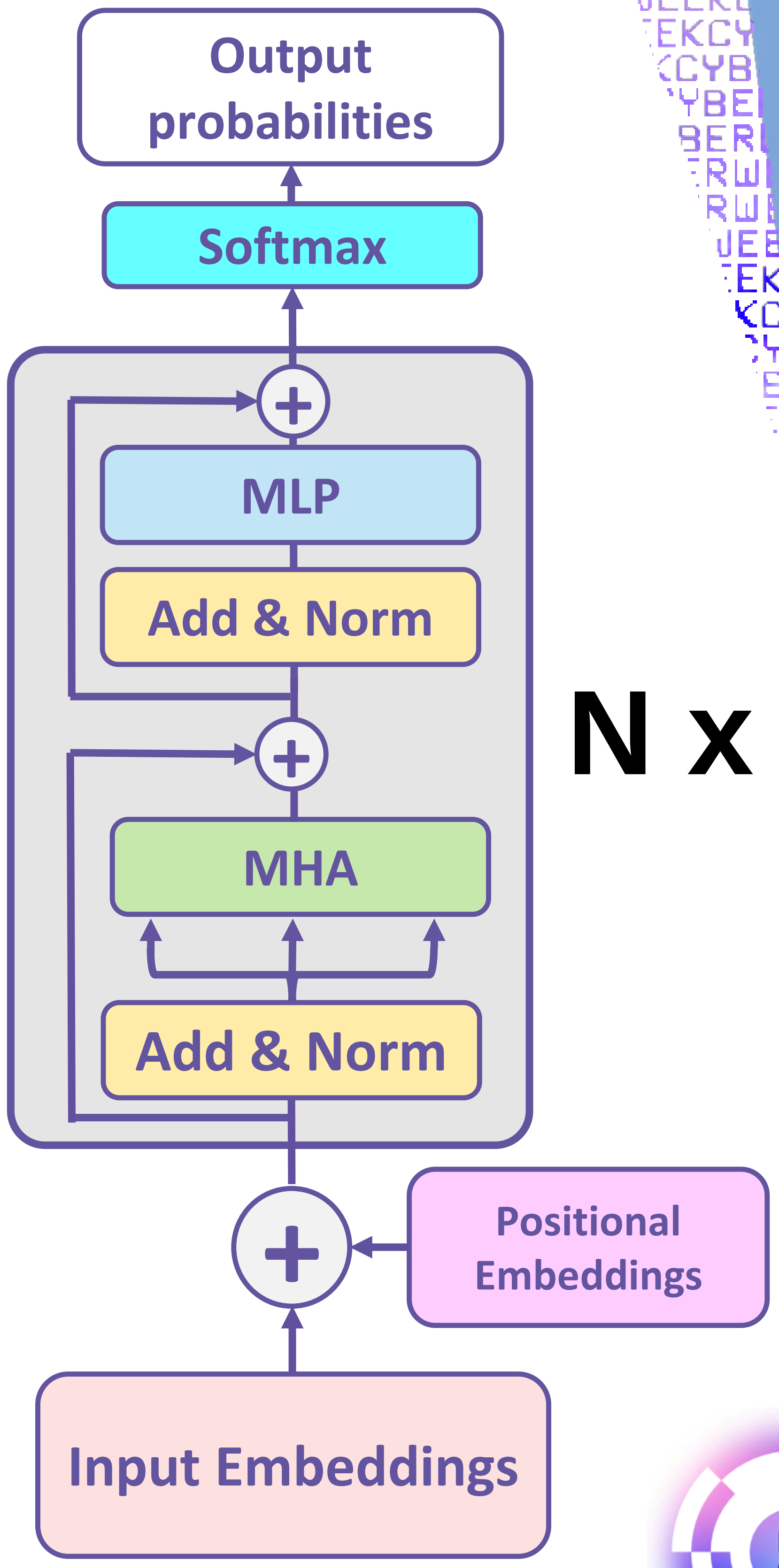
ViT Relibility Characterization

ViT Architecture



ViT Architecture





Output probabilities

Softmax

MLP

Add & Norm

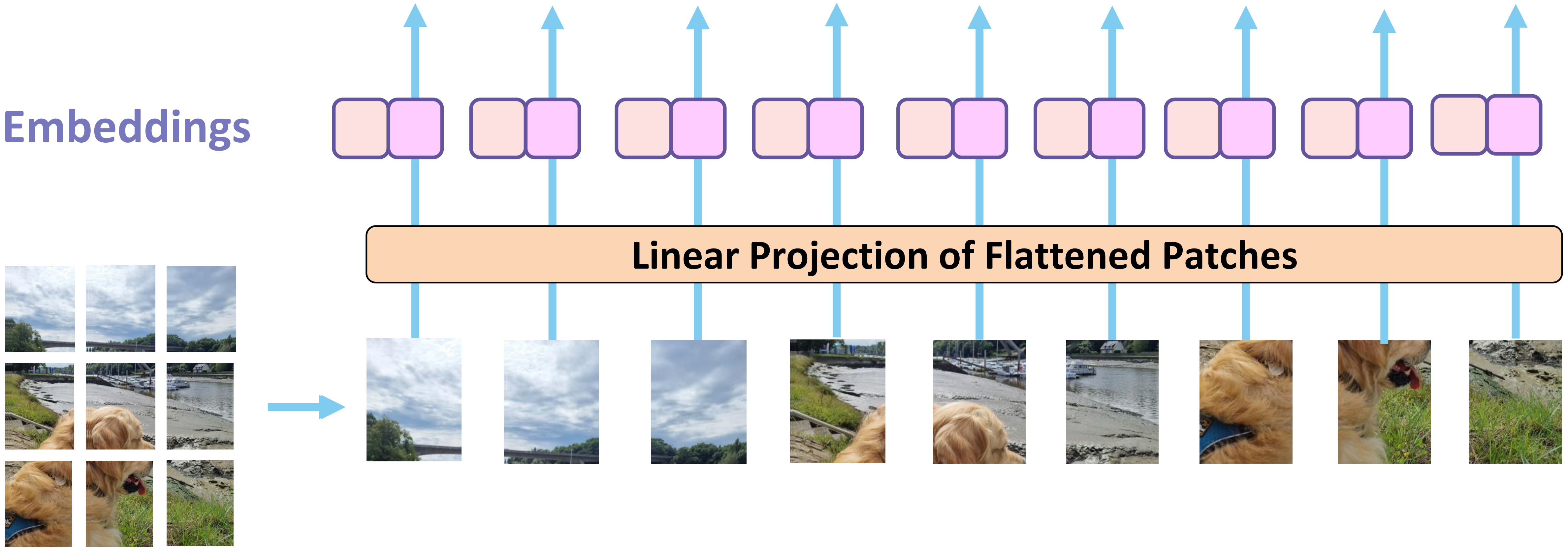
MHA

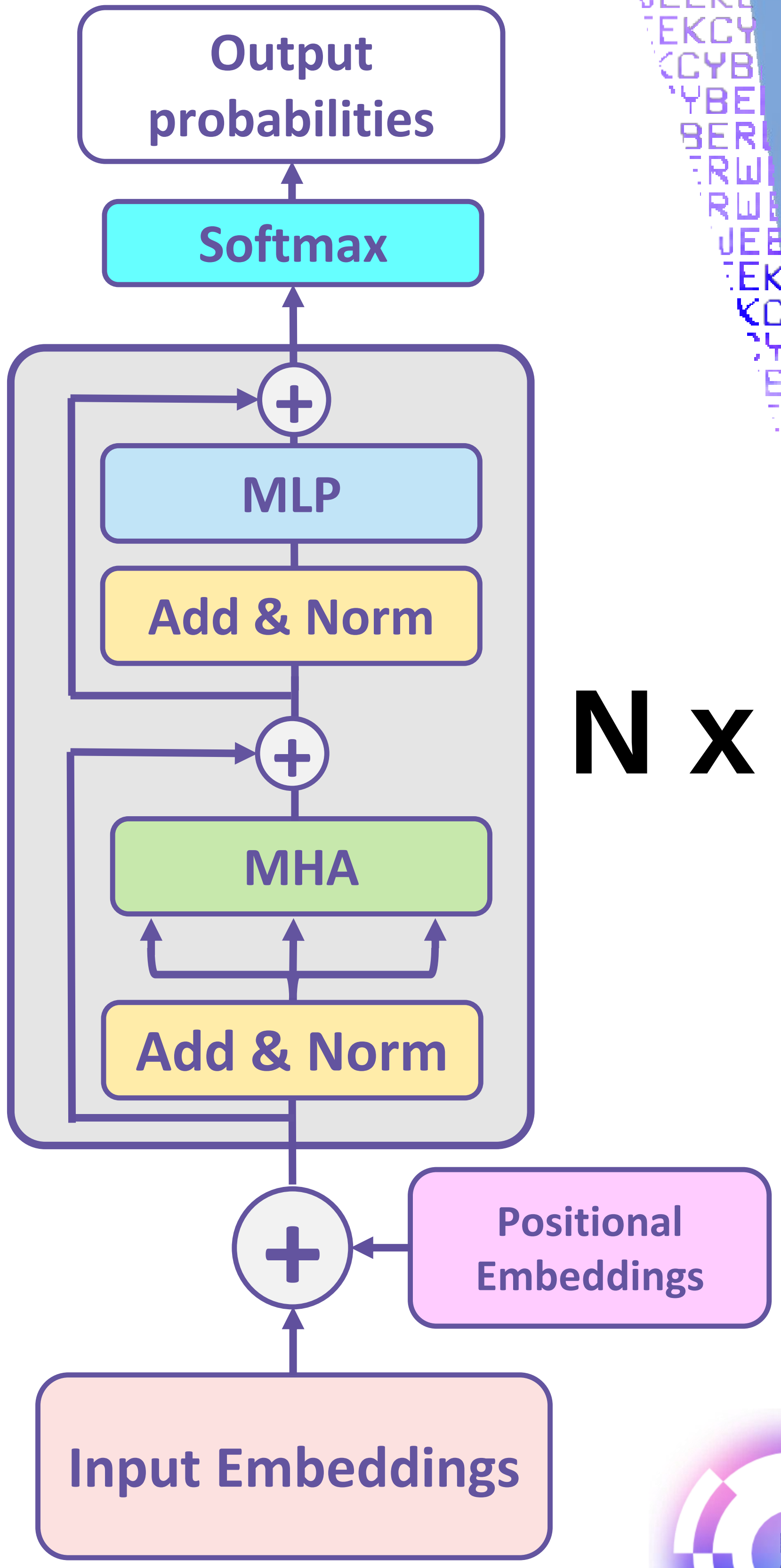
Add & Norm

Positional Embeddings

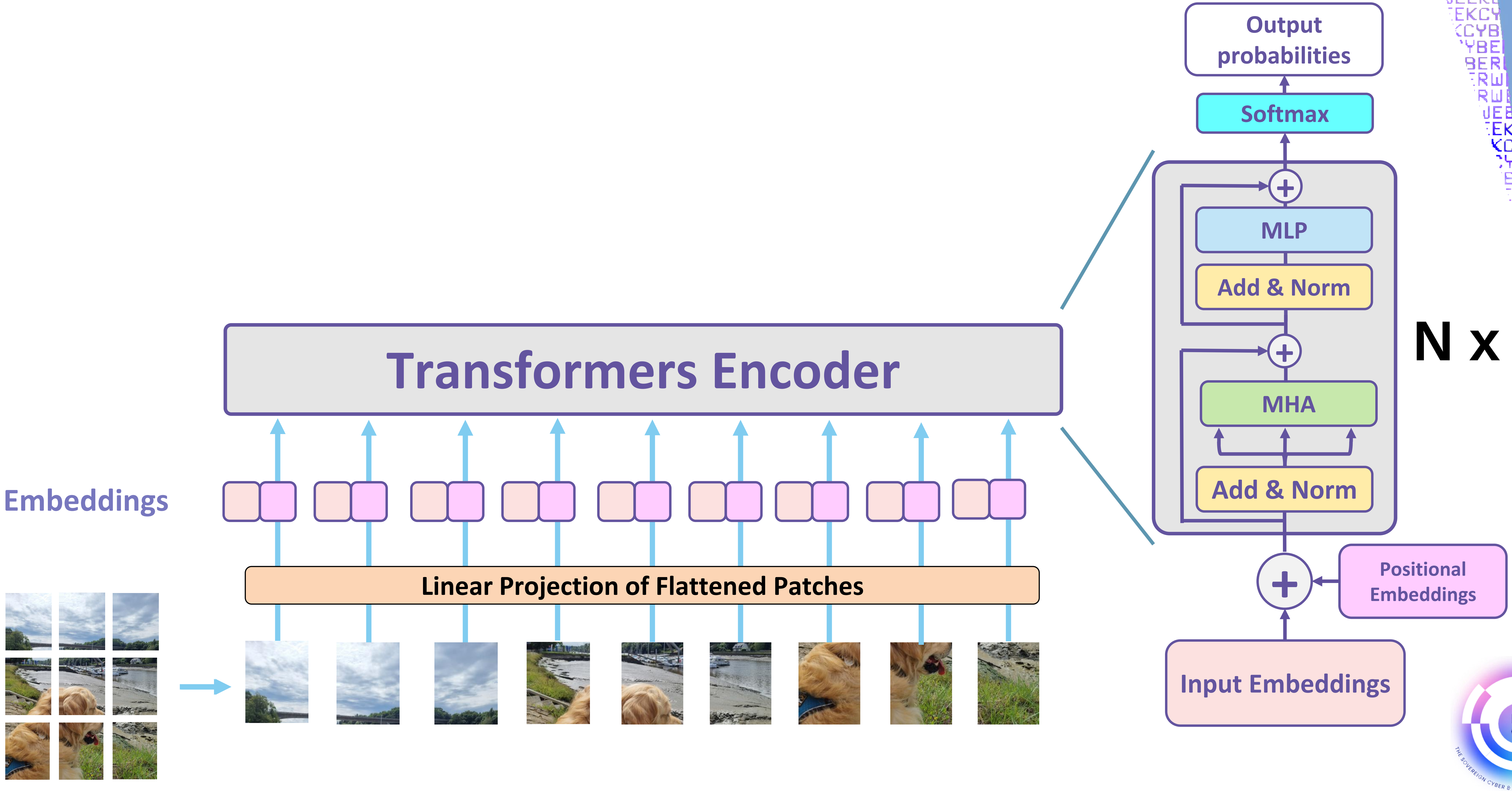
Input Embeddings

ViT Architecture

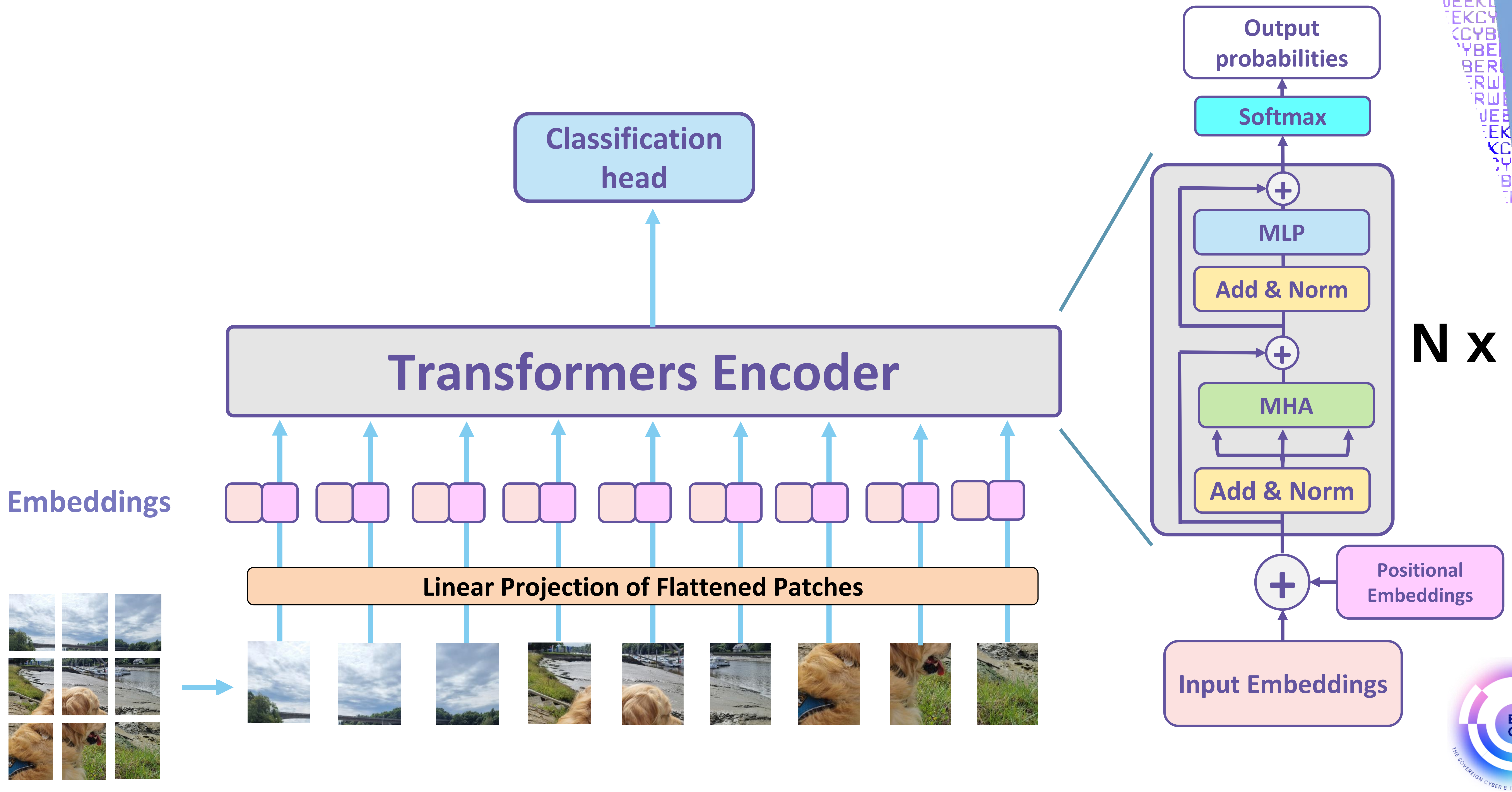




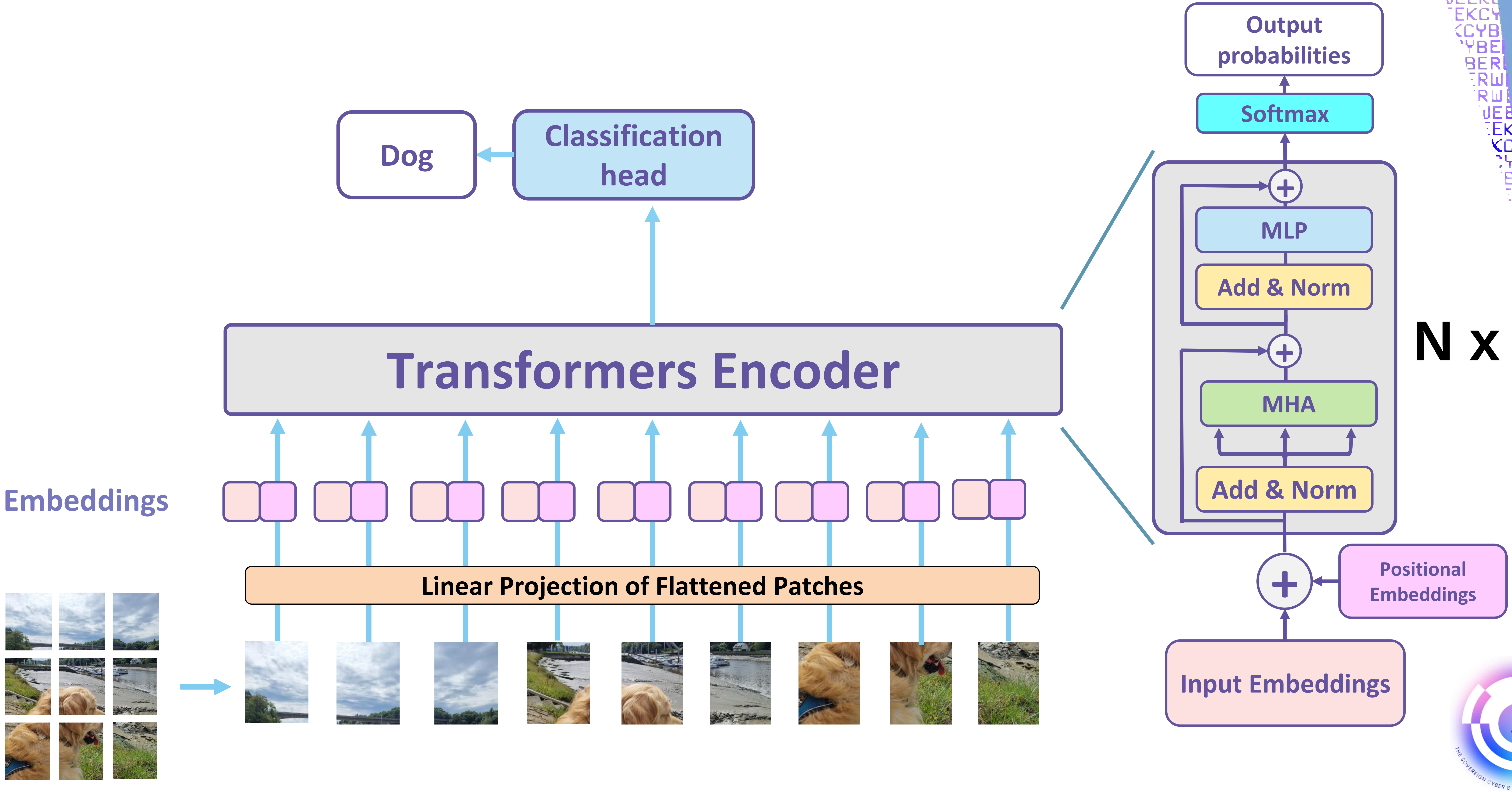
ViT Architecture



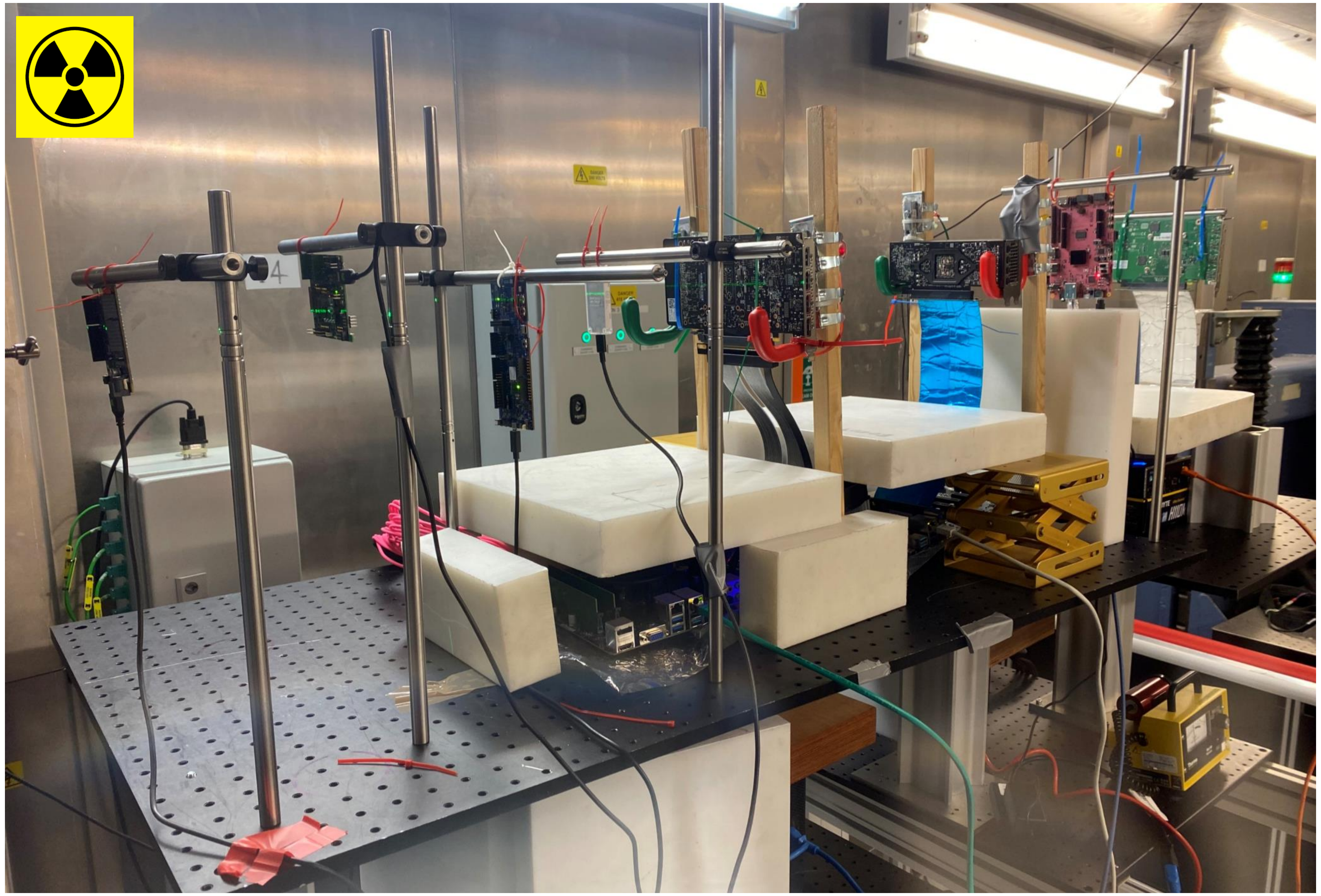
ViT Architecture



ViT Architecture

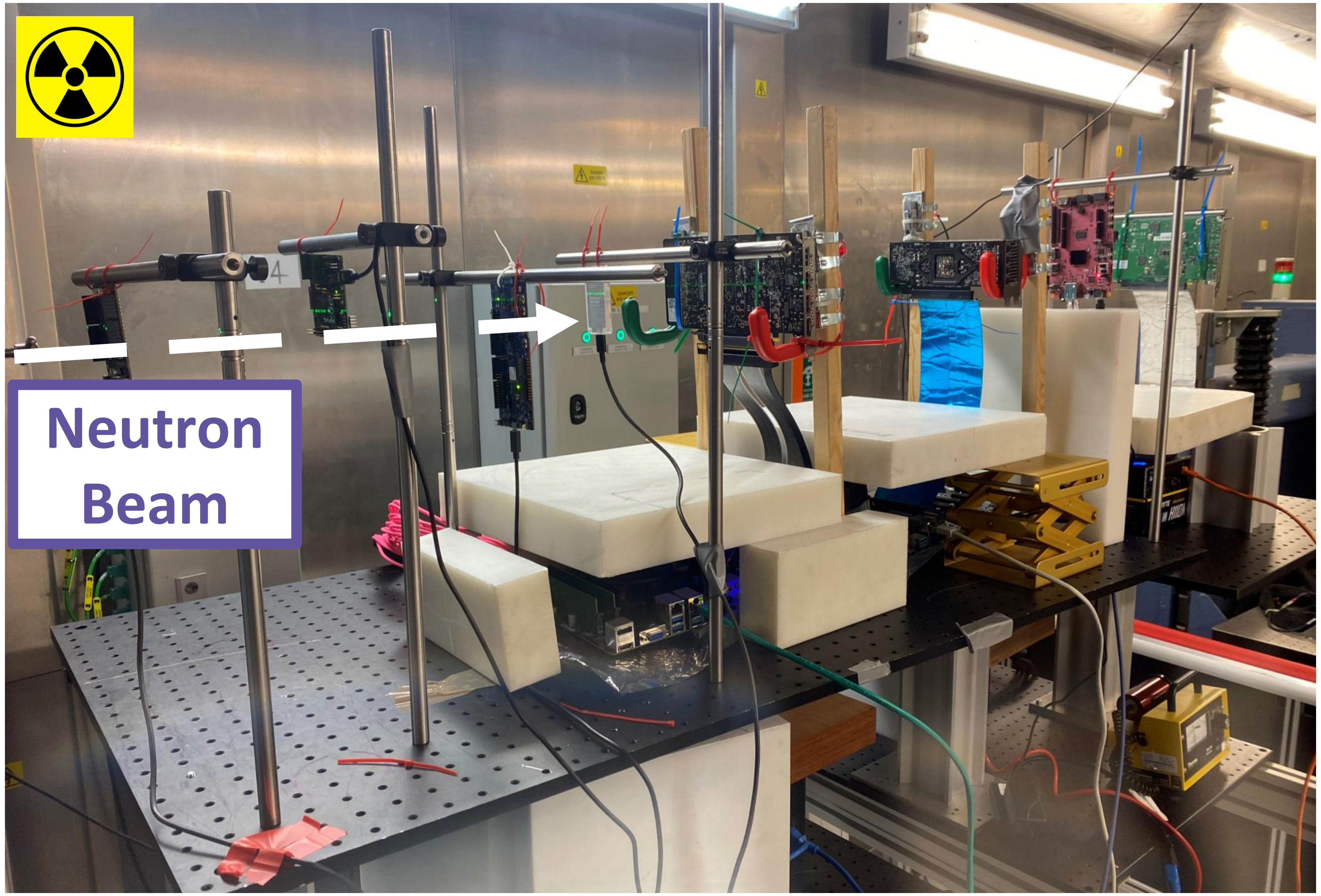


Neutron Beam Setup



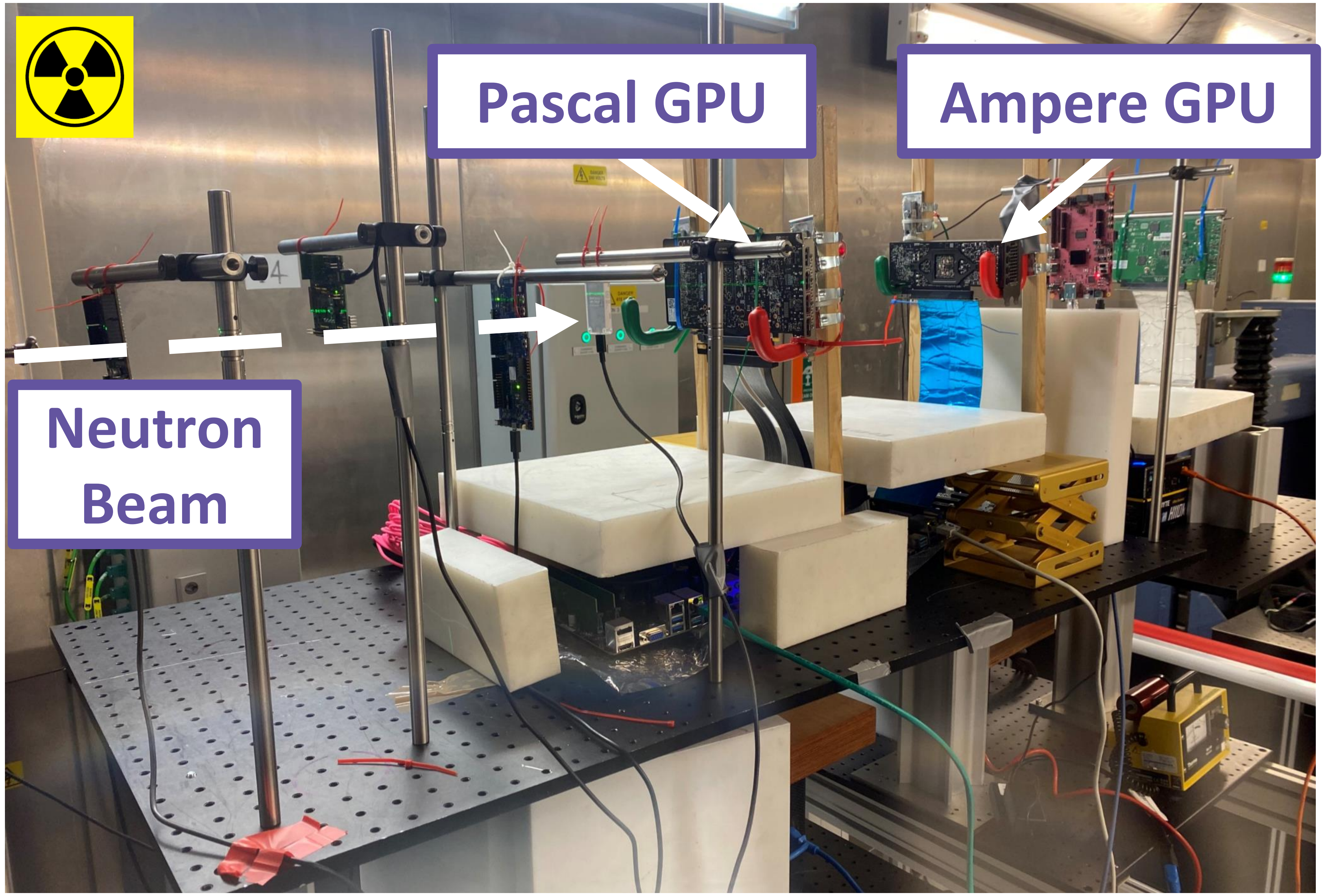
Setup at ChipIR Facility, RAL, UK

Neutron Beam Setup



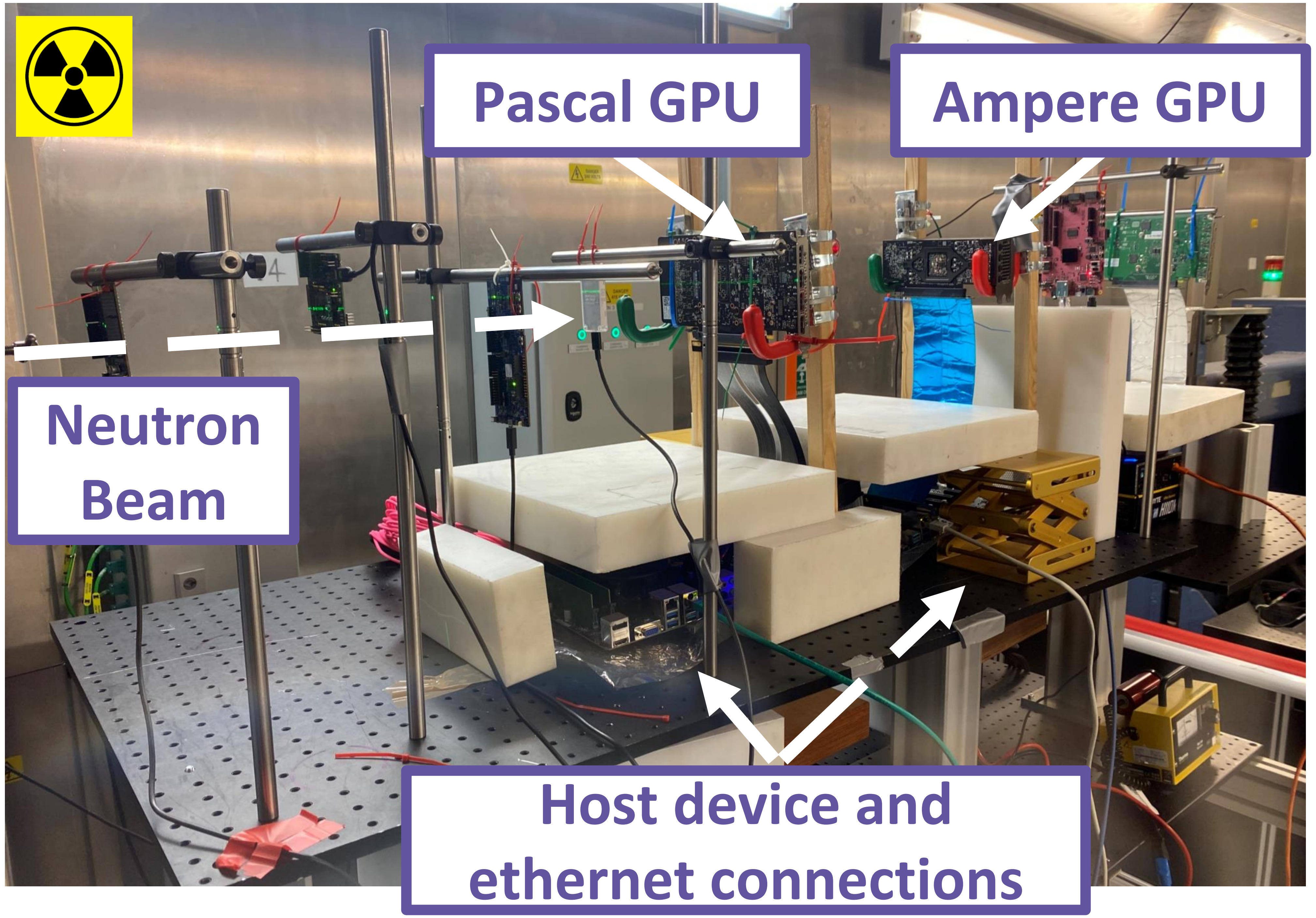
Setup at ChipIR Facility, RAL, UK

Neutron Beam Setup



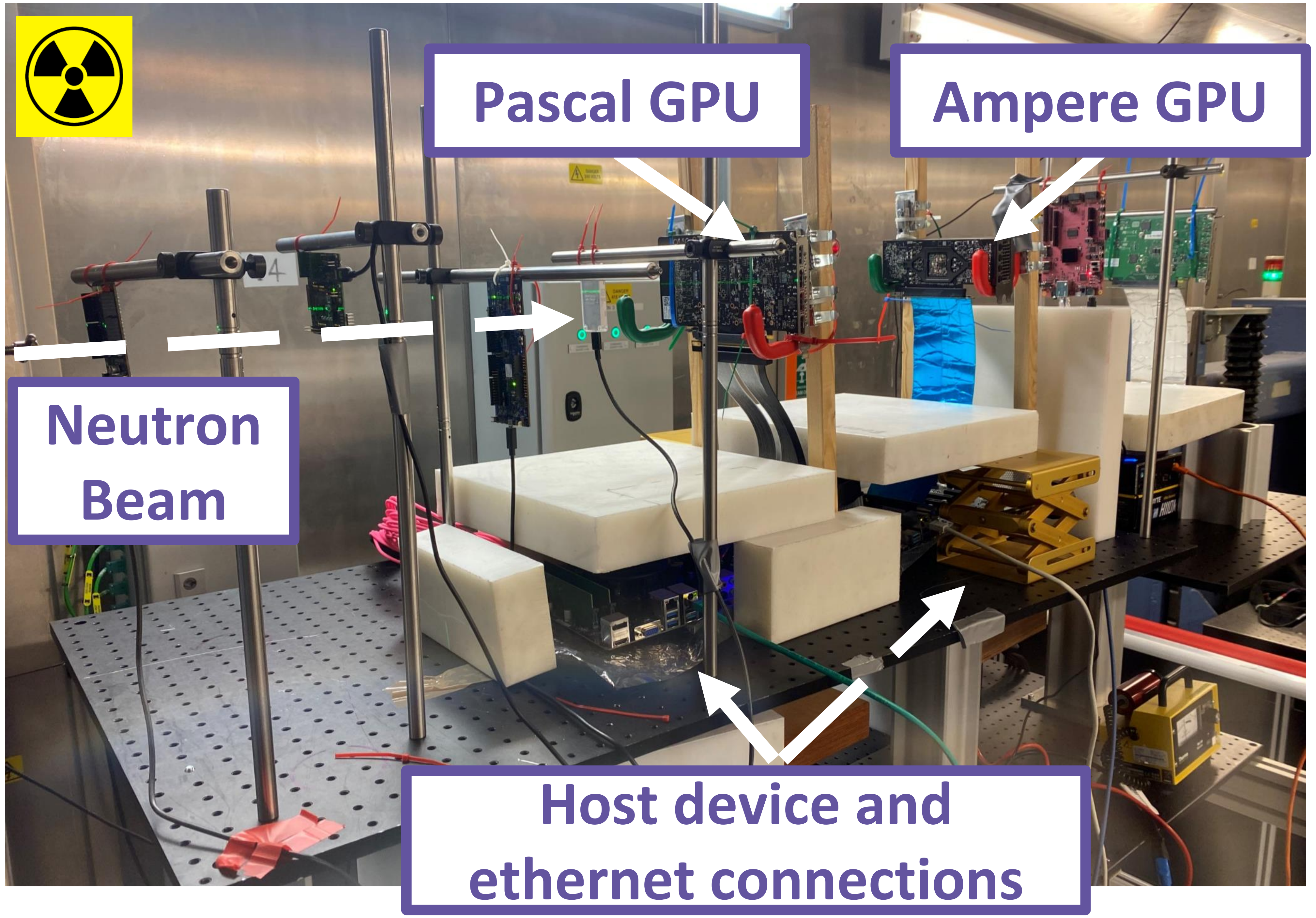
Setup at ChipIR Facility, RAL, UK

Neutron Beam Setup



Setup at ChipIR Facility, RAL, UK

Neutron Beam Setup



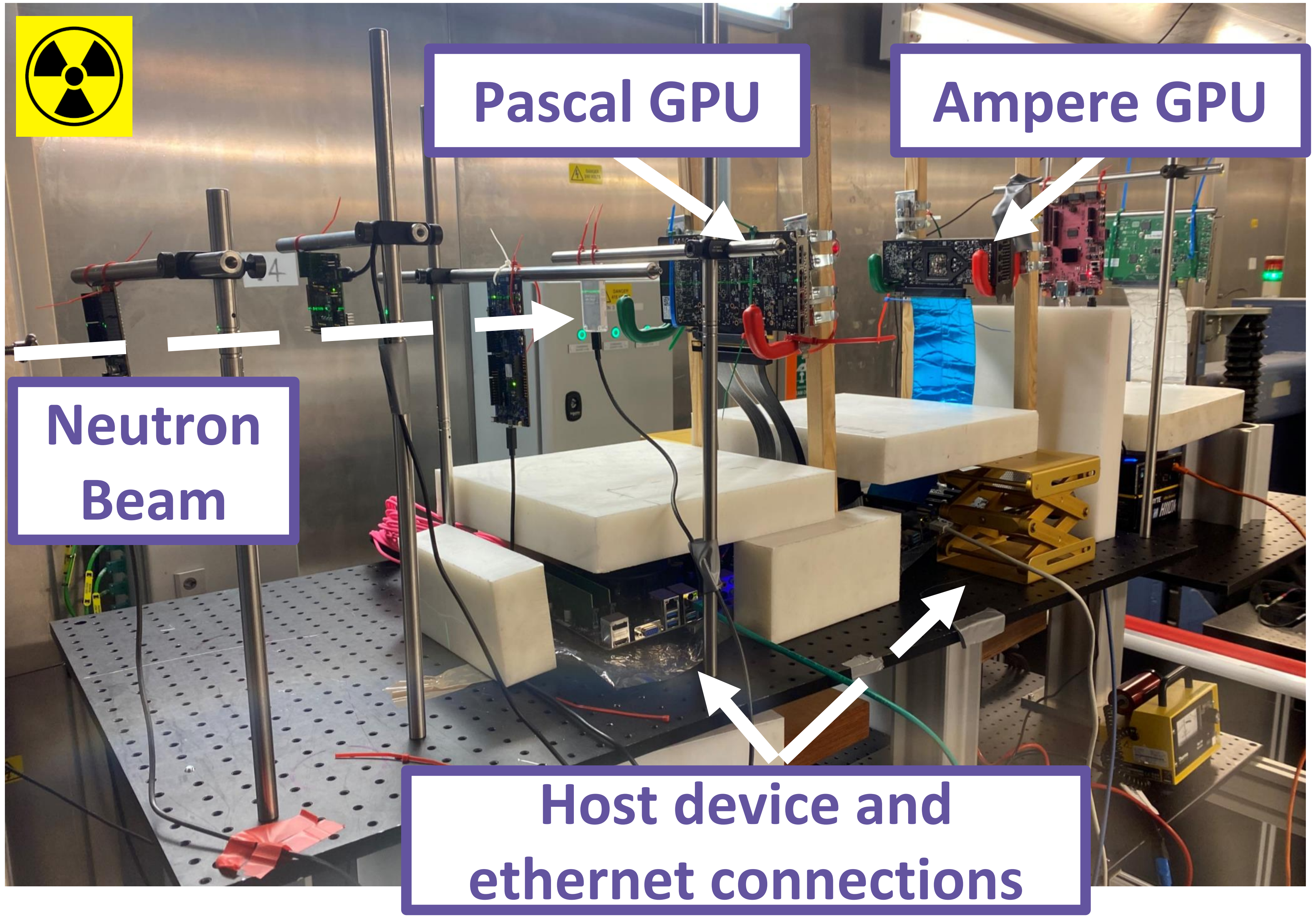
Setup at ChipIR Facility, RAL, UK

Failure Classification

- SDC: Tolerable and Critical
- DUE: ViT crashes, OS hangs

A server outside controls the experiments

Neutron Beam Setup



Setup at ChipIR Facility, RAL, UK

Failure Classification

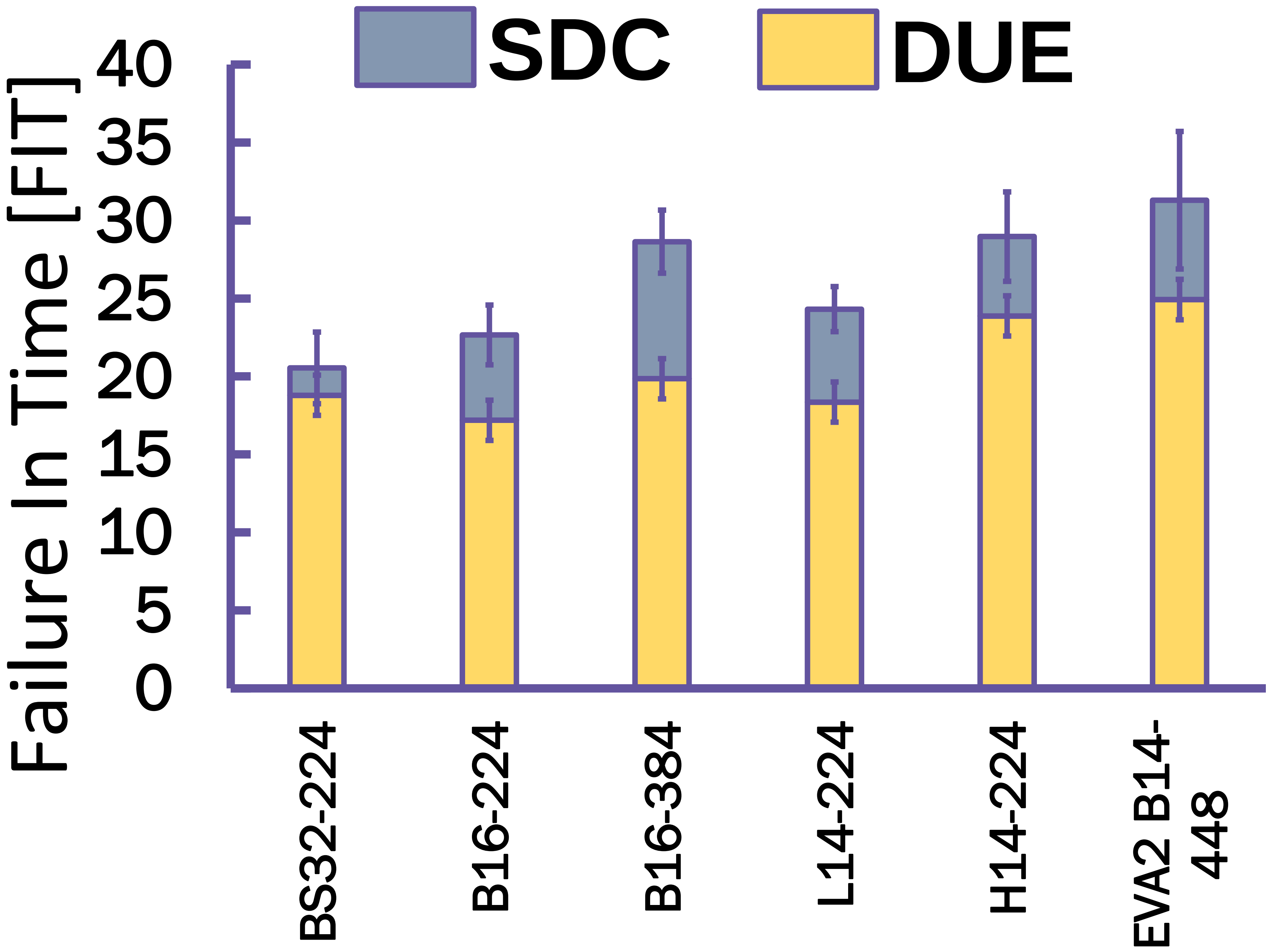
- SDC: Tolerable and Critical
- DUE: ViT crashes, OS hangs

A server outside controls the experiments

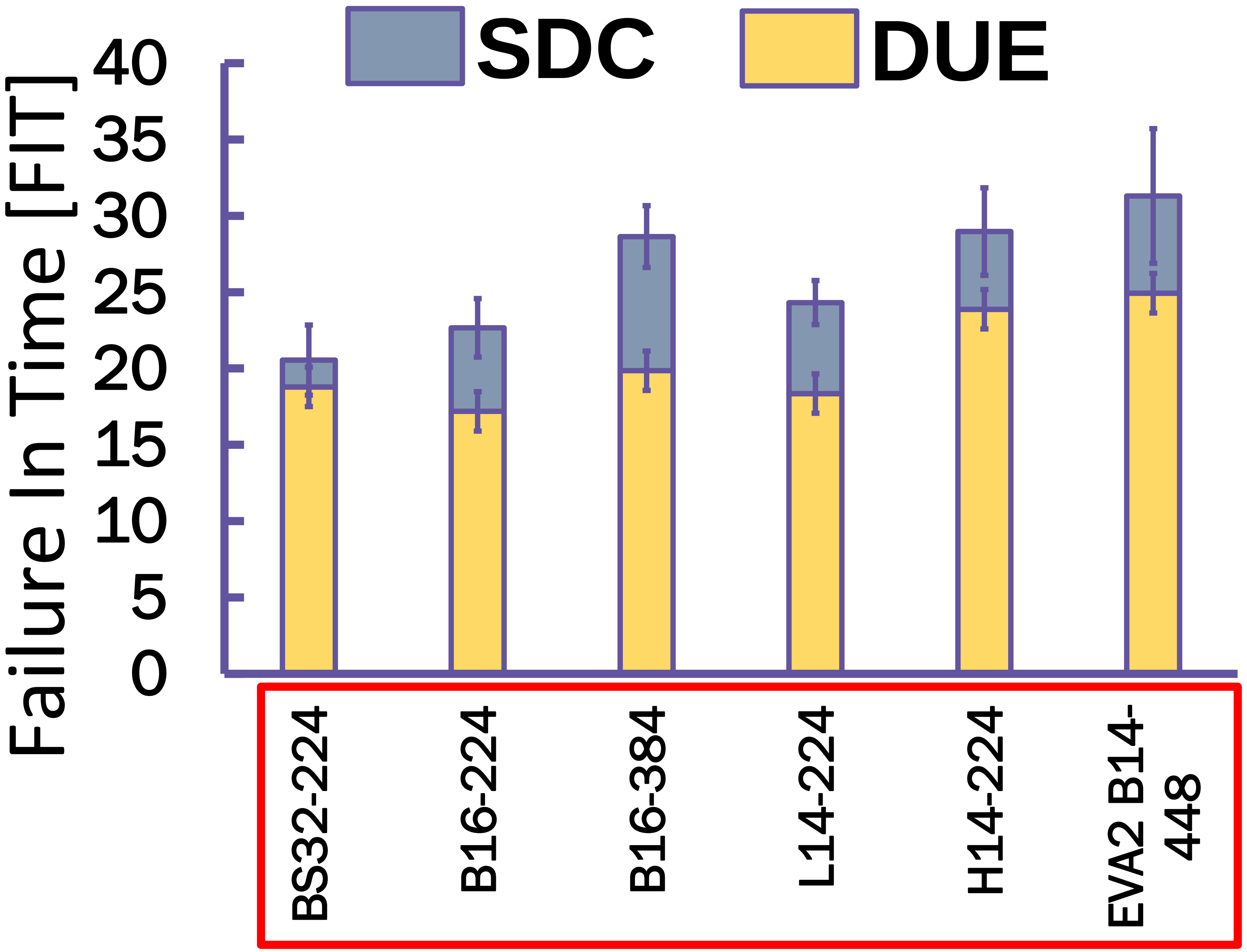
Configurations

- Dataset: ImageNet (classification)
- 12 ViTs, 4 families: ViT, EVA2, SwinV2 and MaxViT
- 2 NVIDIA GPUs: Quadro P2000 (Pascal) and RTX A2000 (Ampere)

ViT’s Failure in Time (FIT)

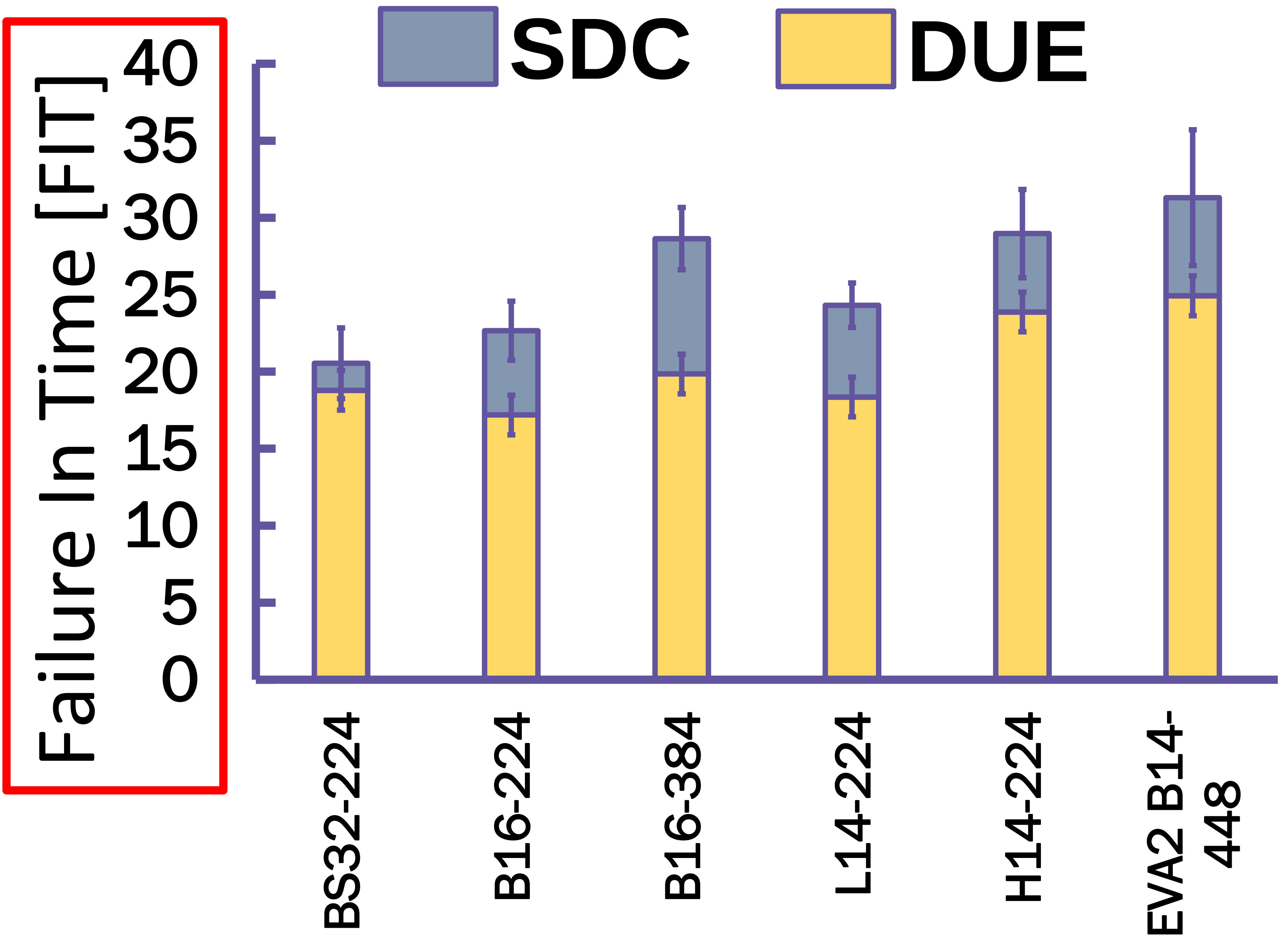


ViT’s Failure in Time (FIT)

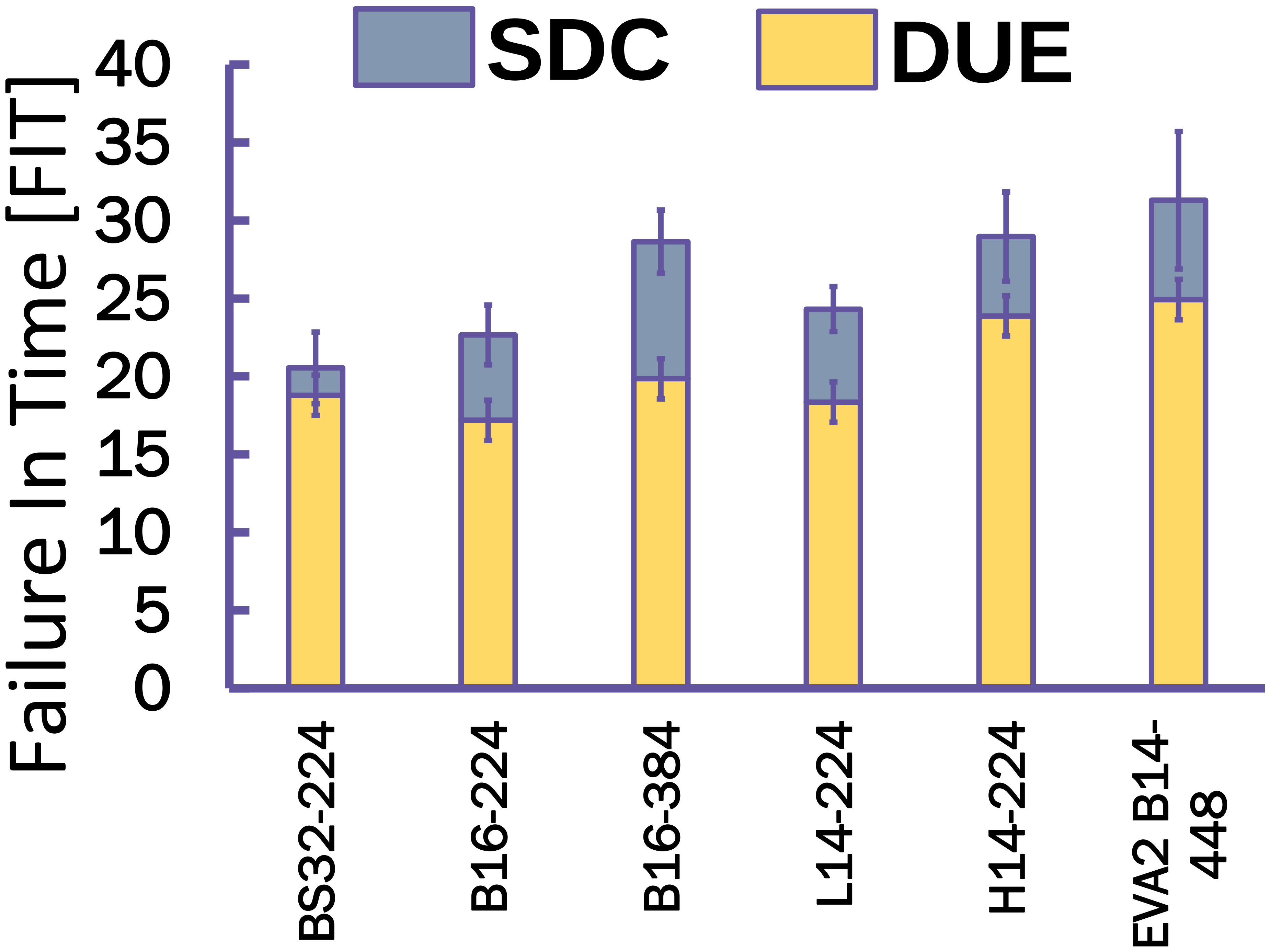


Configuration for Pascal GPU

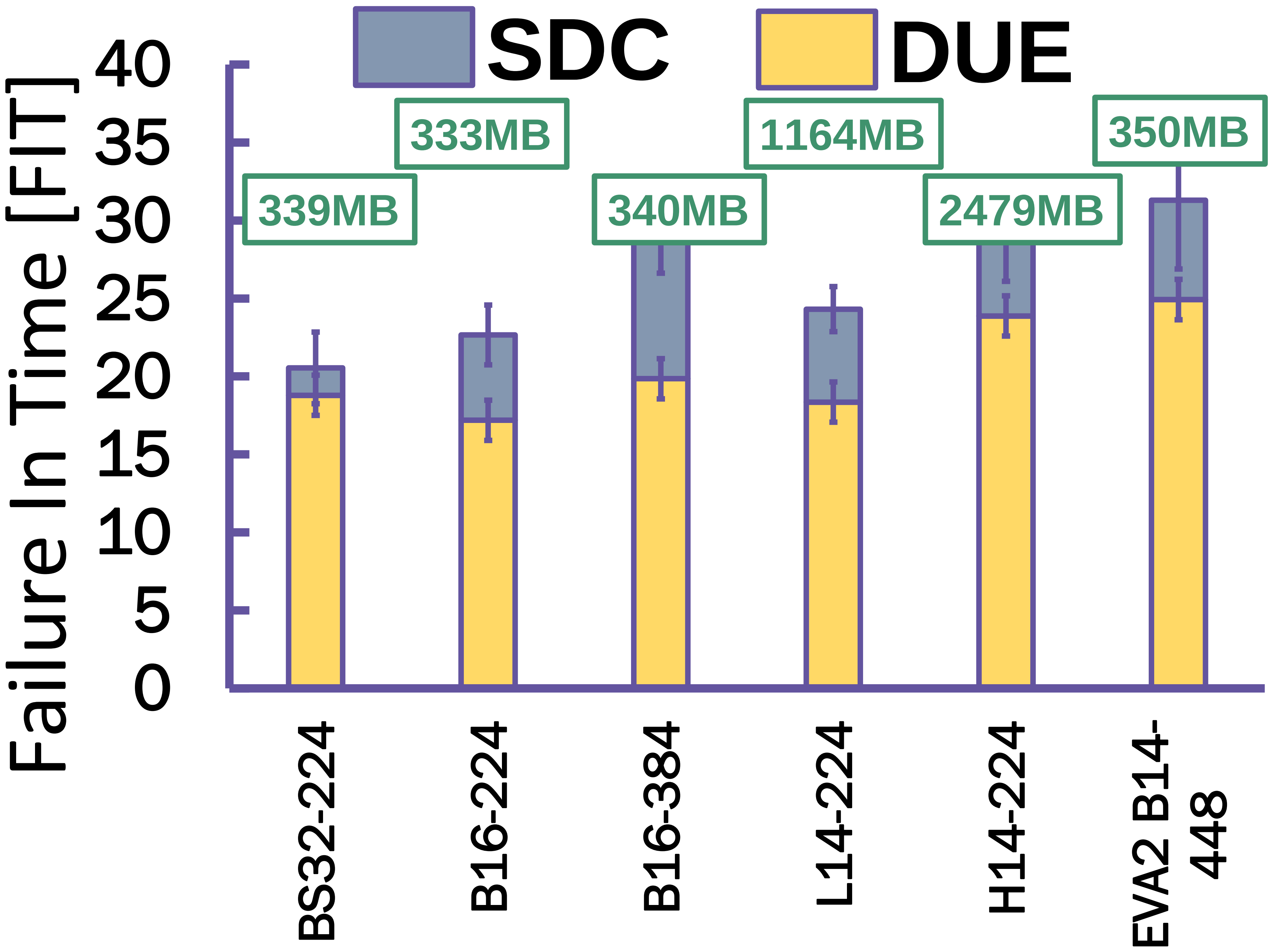
ViT’s Failure in Time (FIT)



ViT's Failure in Time (FIT)

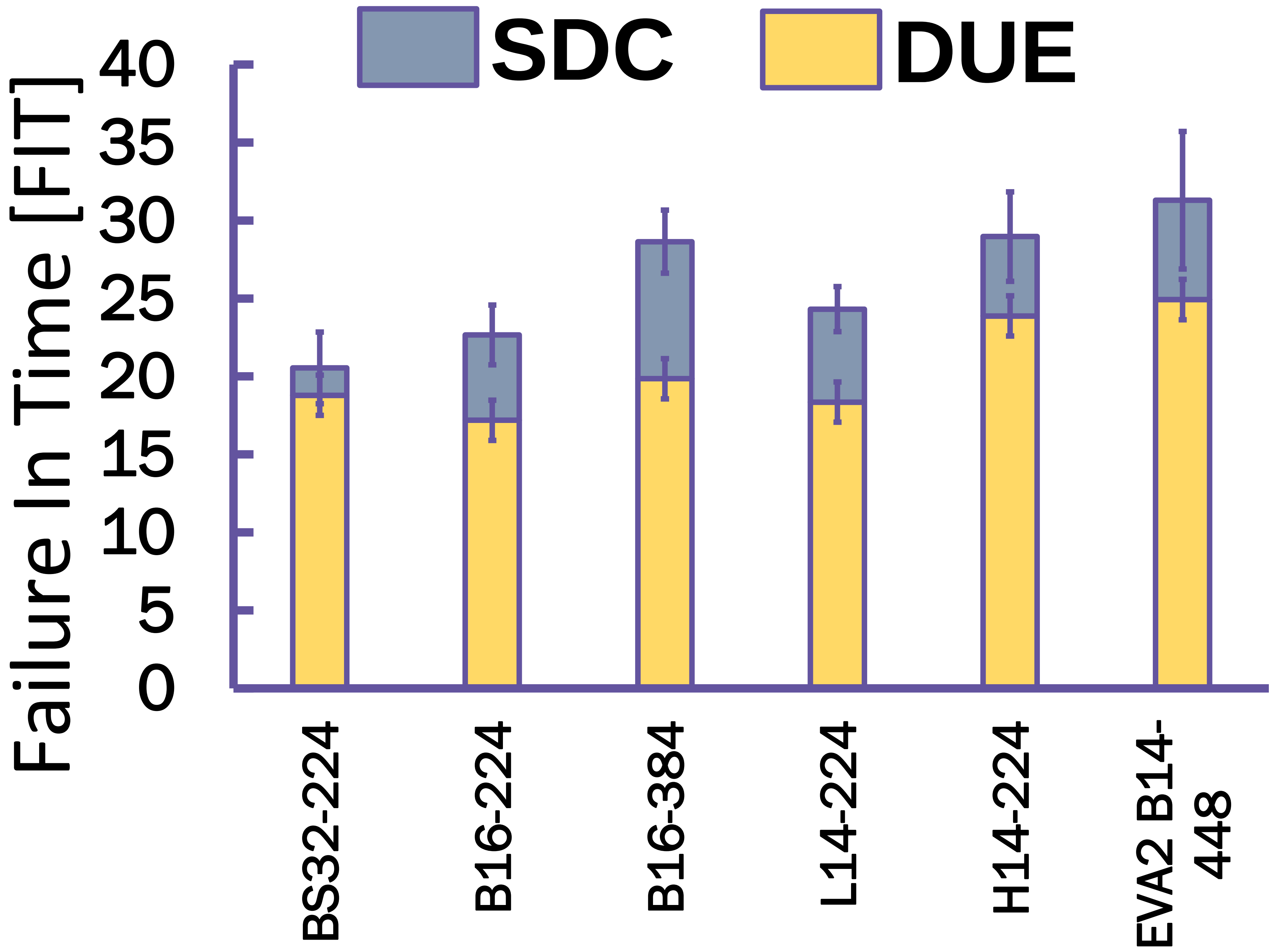


ViT’s Failure in Time (FIT)



- The ViT FIT grows along its resource usage and family

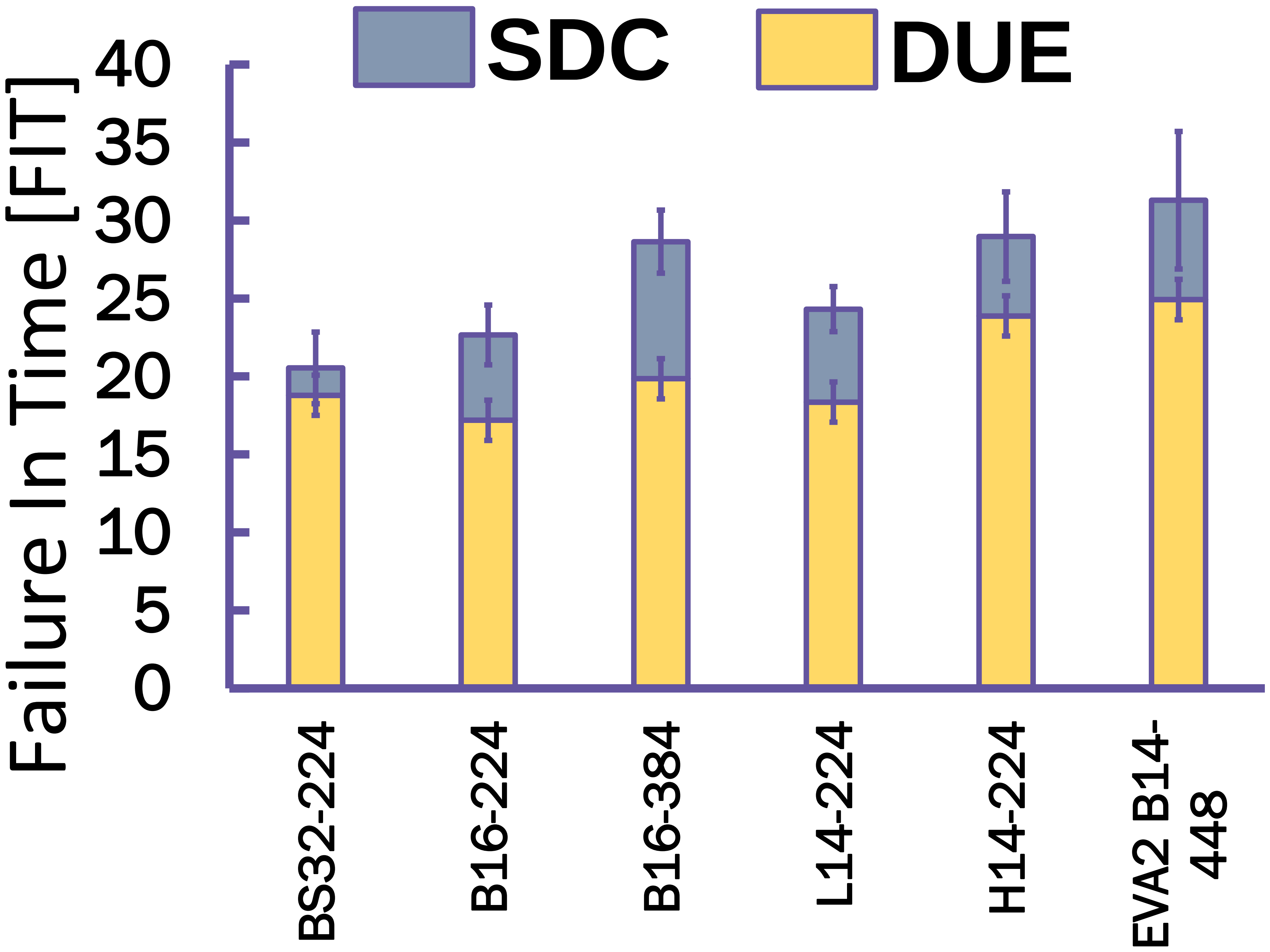
ViT’s Failure in Time (FIT)



- On average, 14.7% of Critical SDCs (max. 33.3%)

- The ViT FIT grows along its resource usage and family

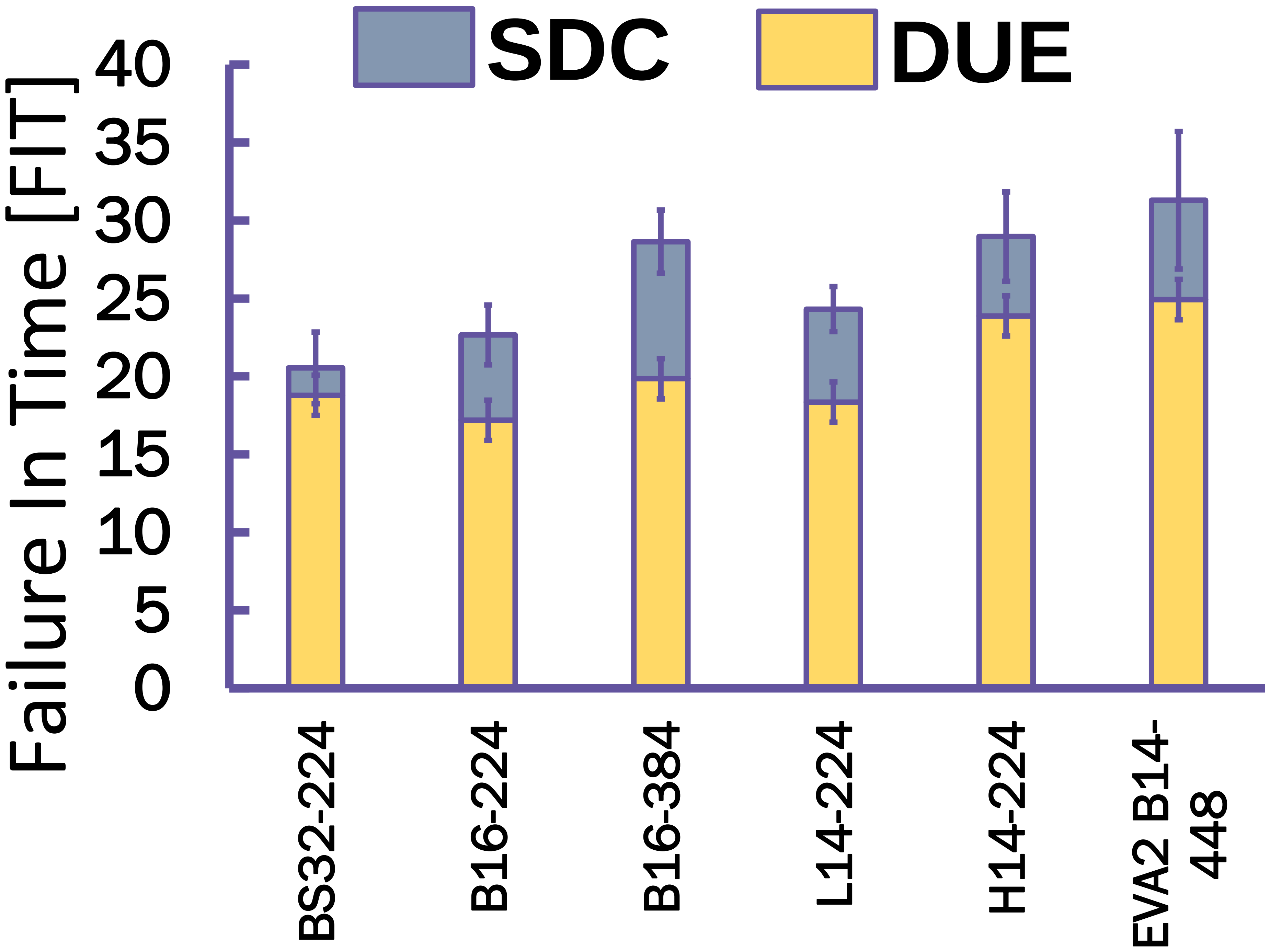
ViT’s Failure in Time (FIT)



- On average, 14.7% of Critical SDCs (max. 33.3%)
- Same observations for Ampere GPU

- The ViT FIT grows along its resource usage and family

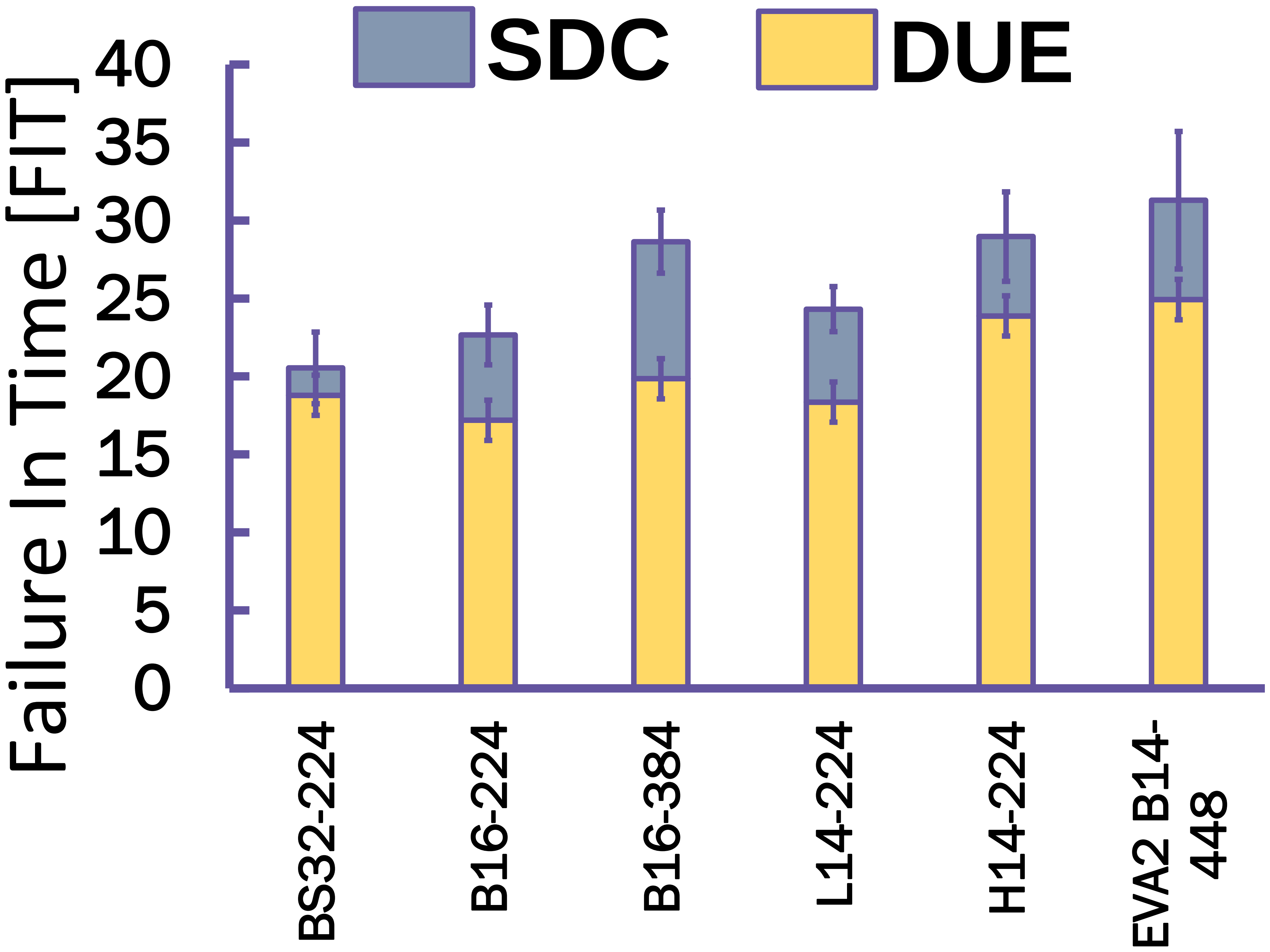
ViT's Failure in Time (FIT)



- On average, 14.7% of Critical SDCs (max. 33.3%)
- Same observations for Ampere GPU
  - 16.3% of Critical SDCs on average (max. 37.3%)

- The ViT FIT grows along its resource usage and family

ViT’s Failure in Time (FIT)

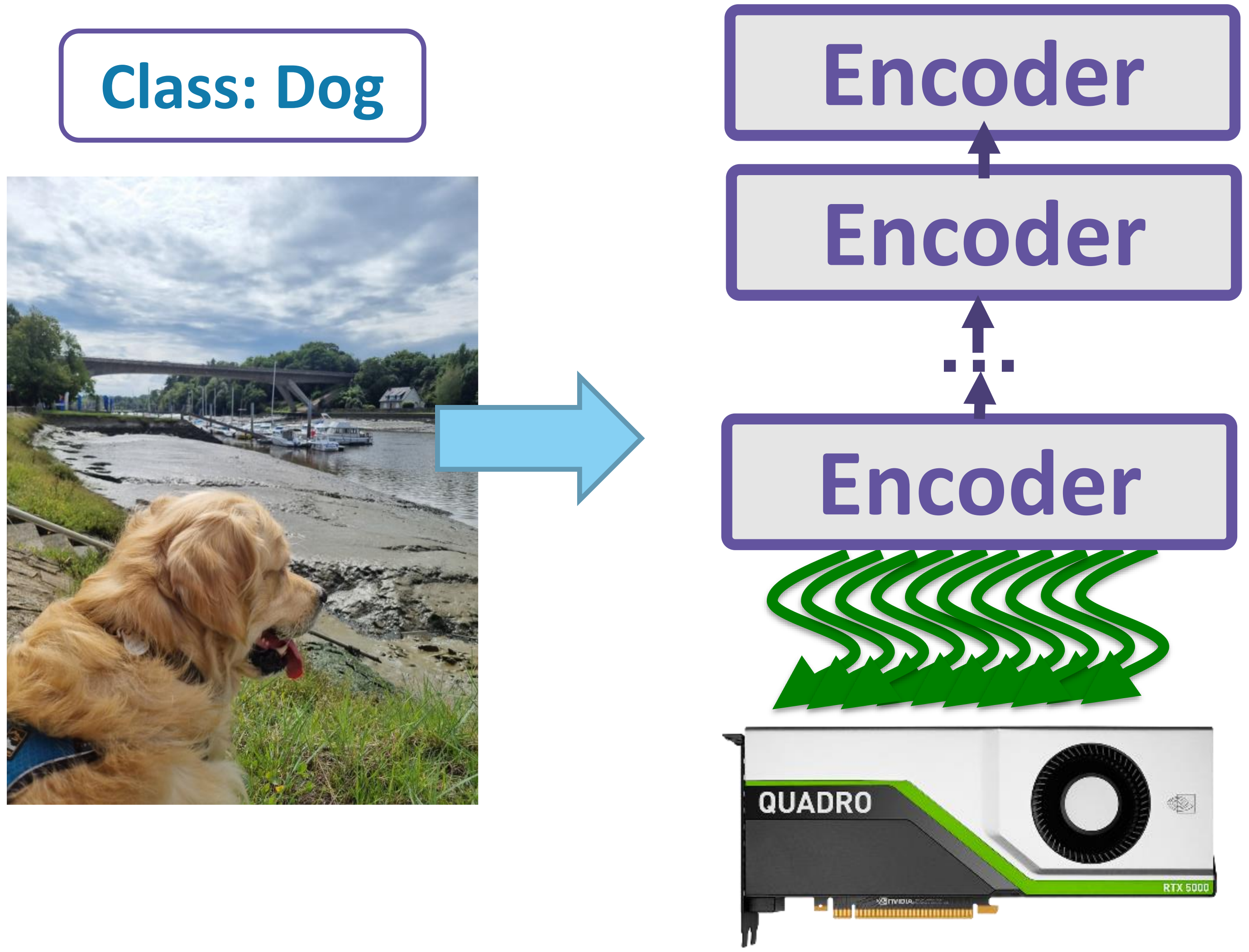


- On average, 14.7% of Critical SDCs (max. 33.3%)
- Same observations for Ampere GPU
  - 16.3% of Critical SDCs on average (max. 37.3%)
  - with ECC ON: up to 10.0% of Crititical SDCs

- The ViT FIT grows along its resource usage and family

Efficient Fault Tolerance

Fault Impact on ViTs



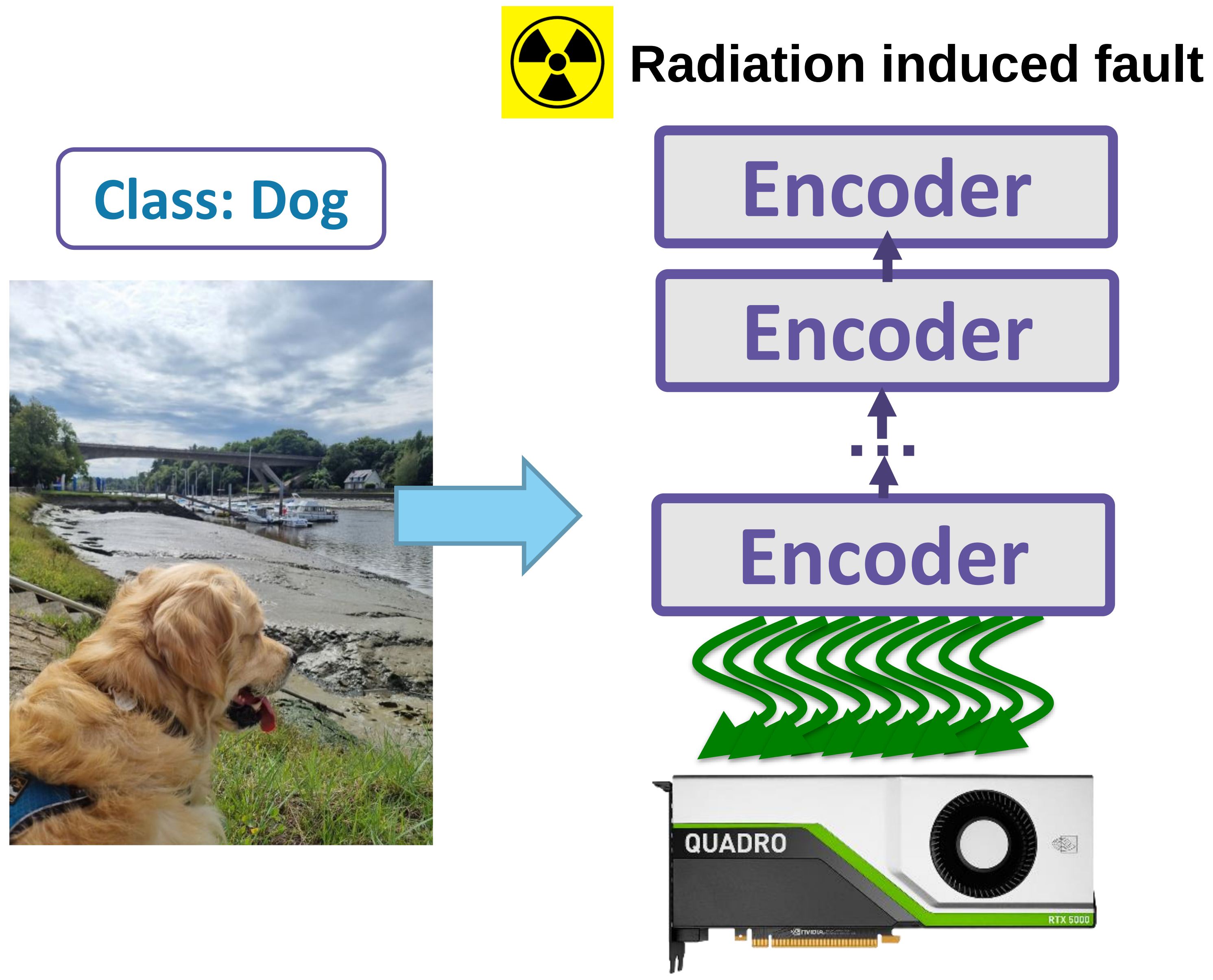
Class: Dog

Encoder

Encoder

Encoder

Fault Impact on ViTs



Radiation induced fault

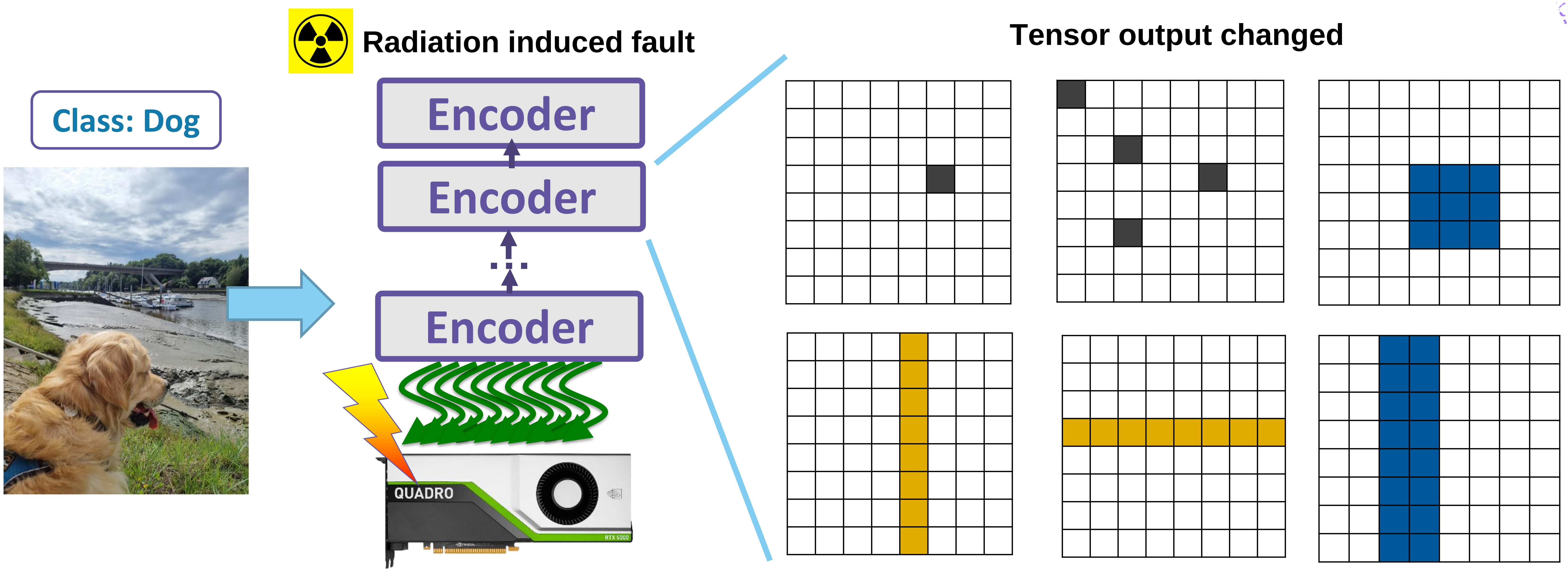
Class: Dog

Encoder

Encoder

Encoder

Fault Impact on ViTs



Radiation induced fault

Tensor output changed

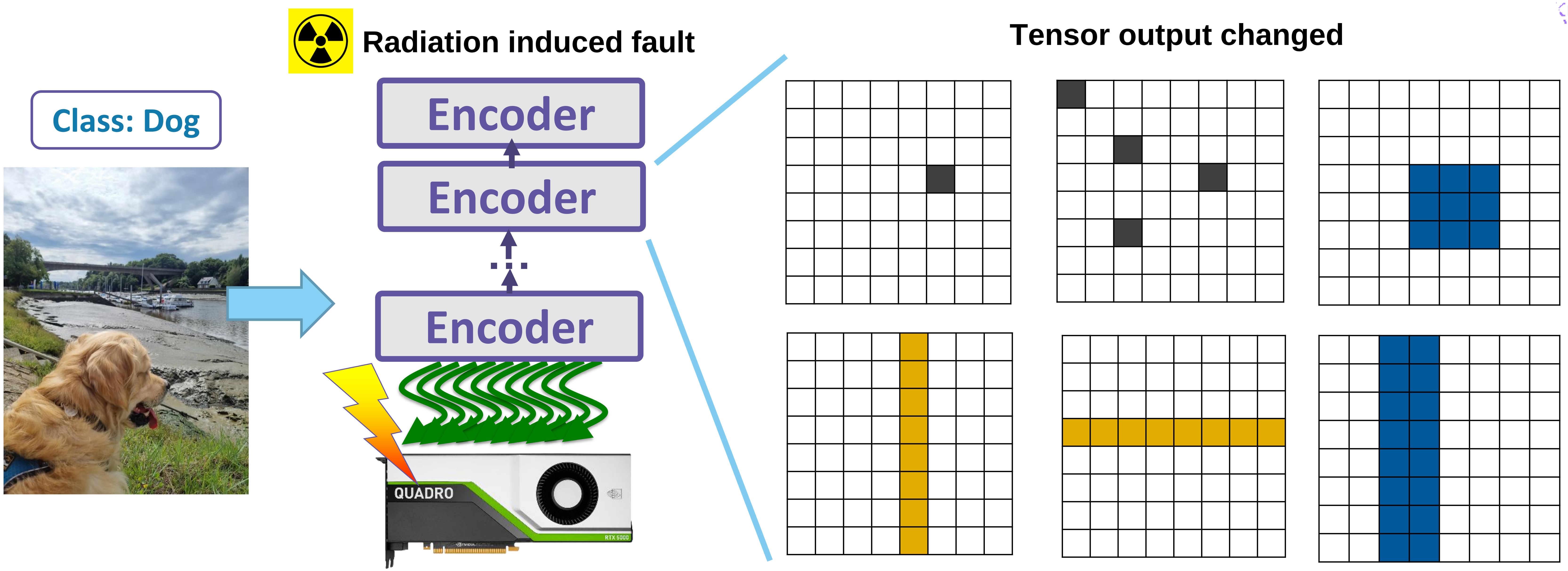
Class: Dog

Encoder

Encoder

Encoder

Fault Impact on ViTs



Fault assessement

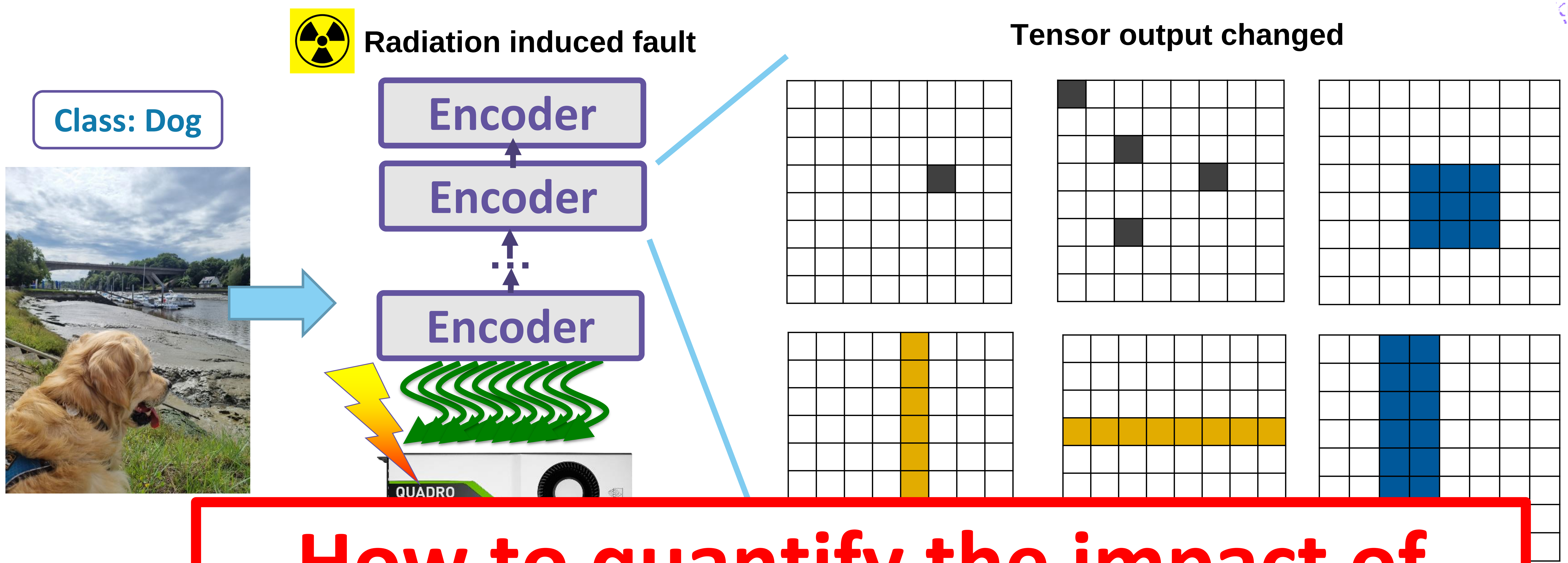
- Physical fault injection
- Software fault simulation

NVIDIA.

```
int foo(S,P){
  int r;
  if (S==P)
    r=1;
  else
    r=0;
  return r;
}
```

European Cyber Week

Fault Impact on ViTs



How to quantify the impact of faults ?

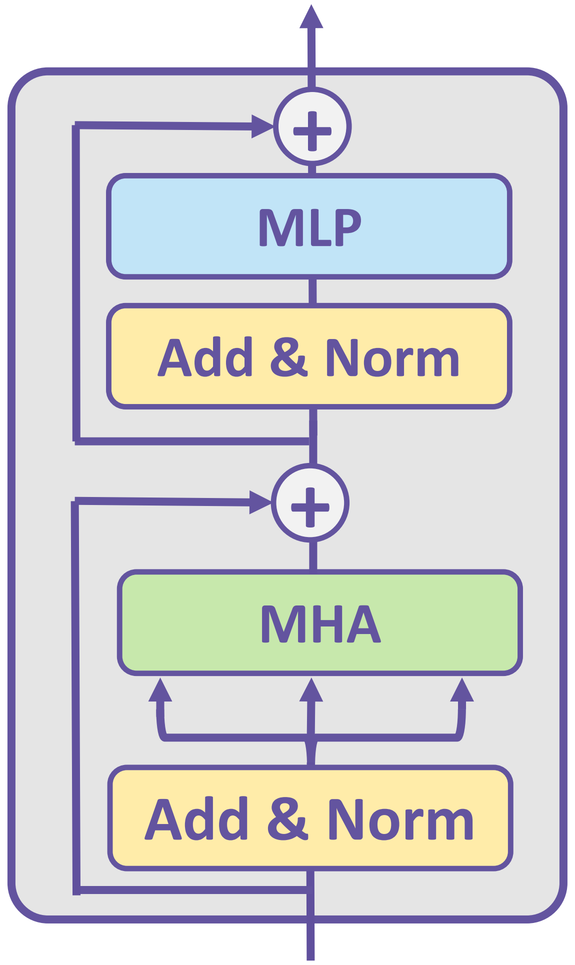
Fault

- Phys
- Software fault simulation

```
int foo(S,P){
  int r;
  if (S==P)
    r=1;
  else
    r=0;
  return r;
}
```

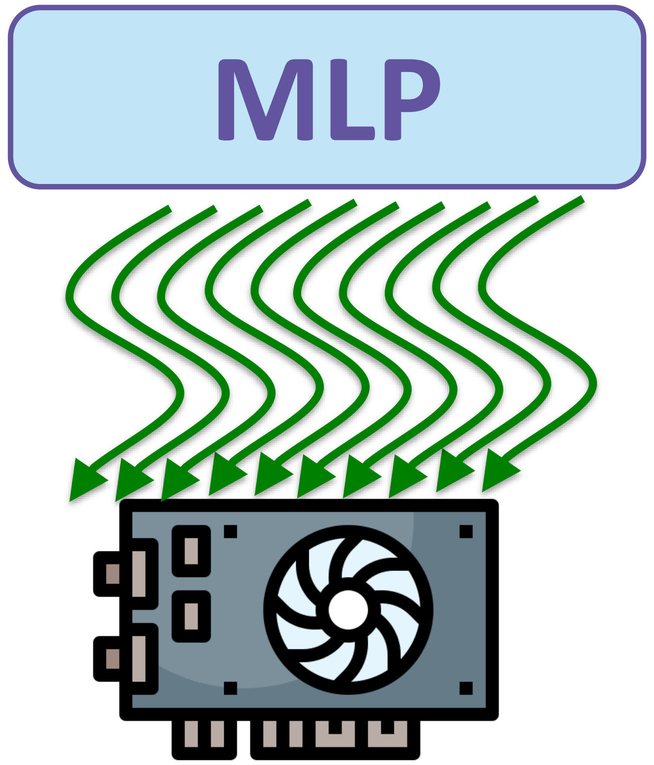
Fault Impact on ViT Operations

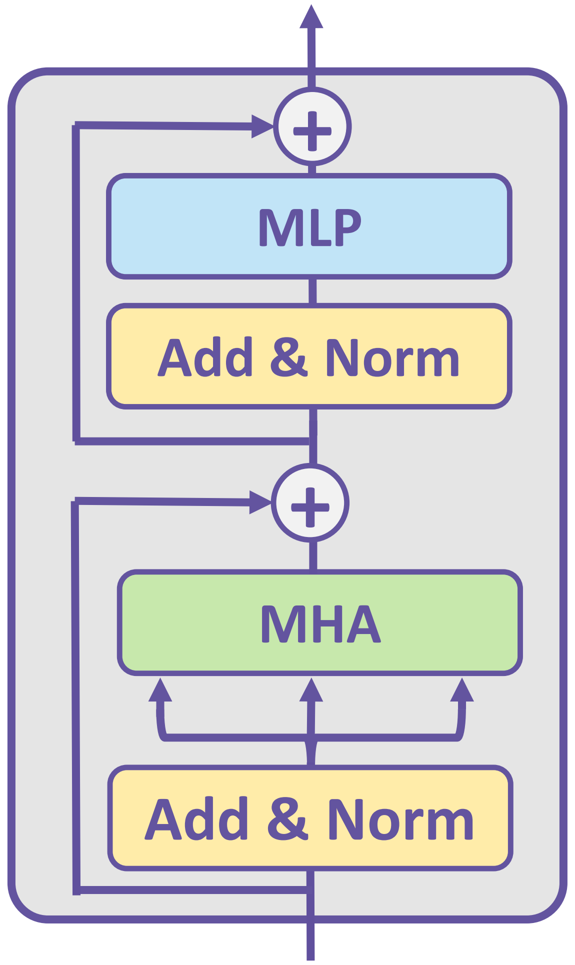
- We split the ViT into its essential operations
- We measure the FIT rate of each operation



Fault Impact on ViT Operations

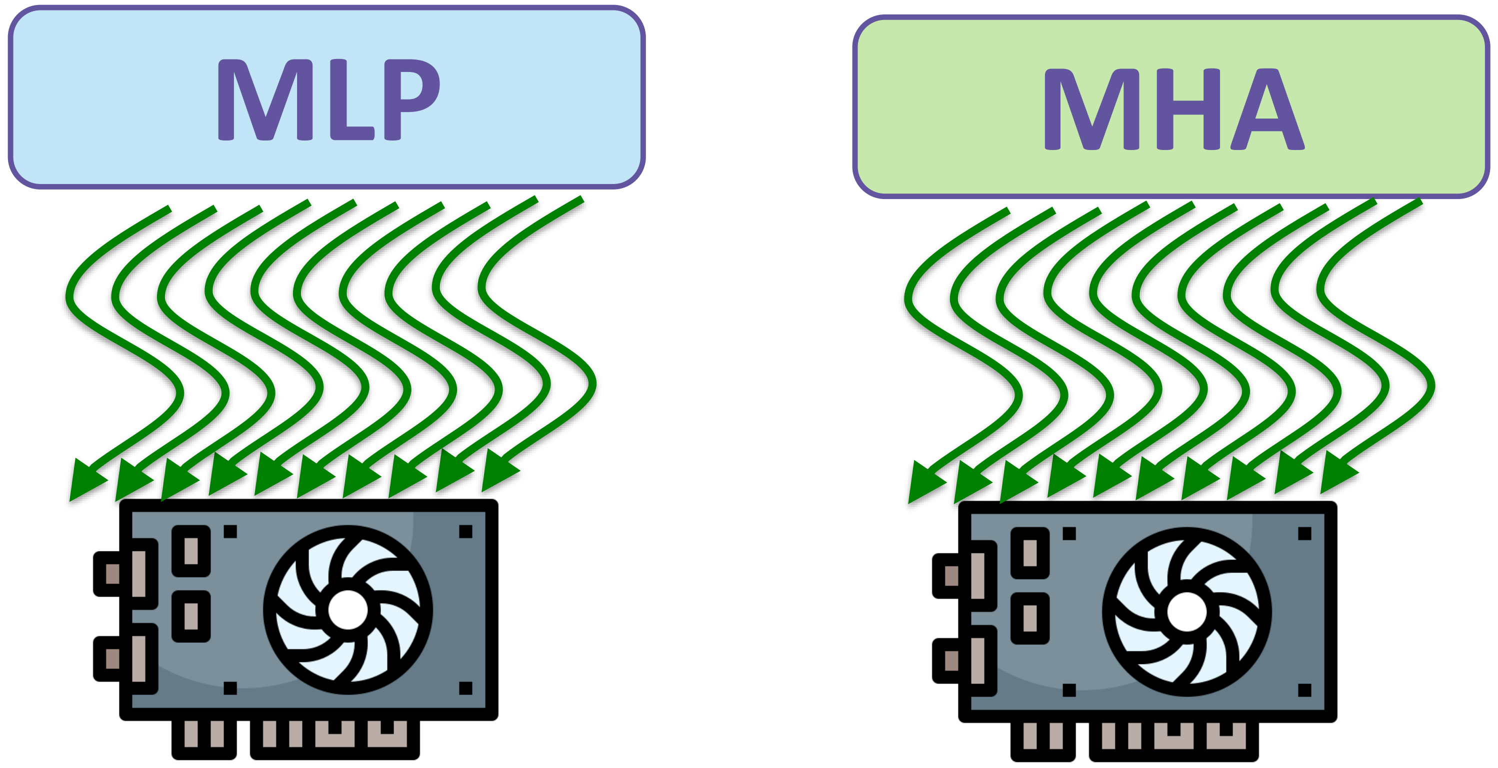
- We split the ViT into its essential operations
- We measure the FIT rate of each operation

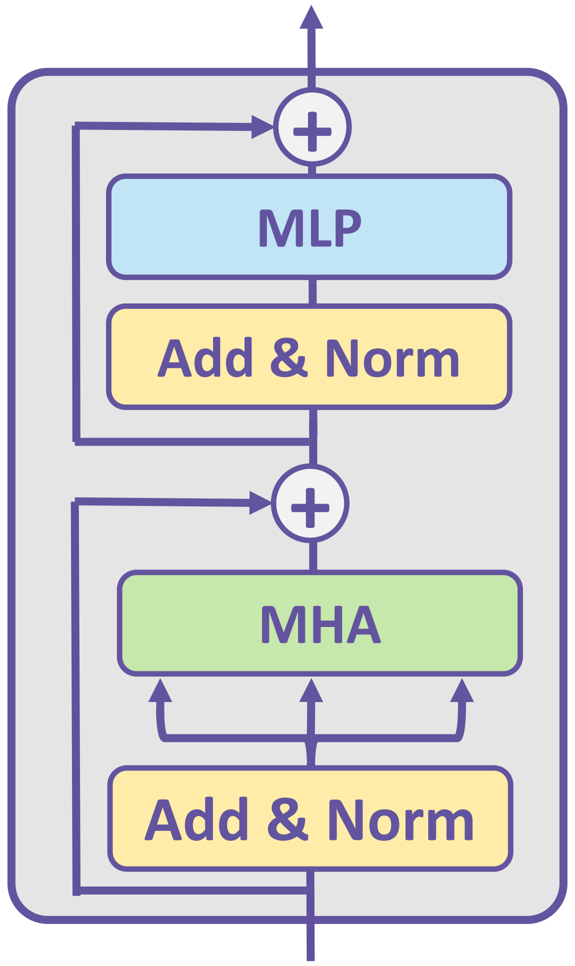




Fault Impact on ViT Operations

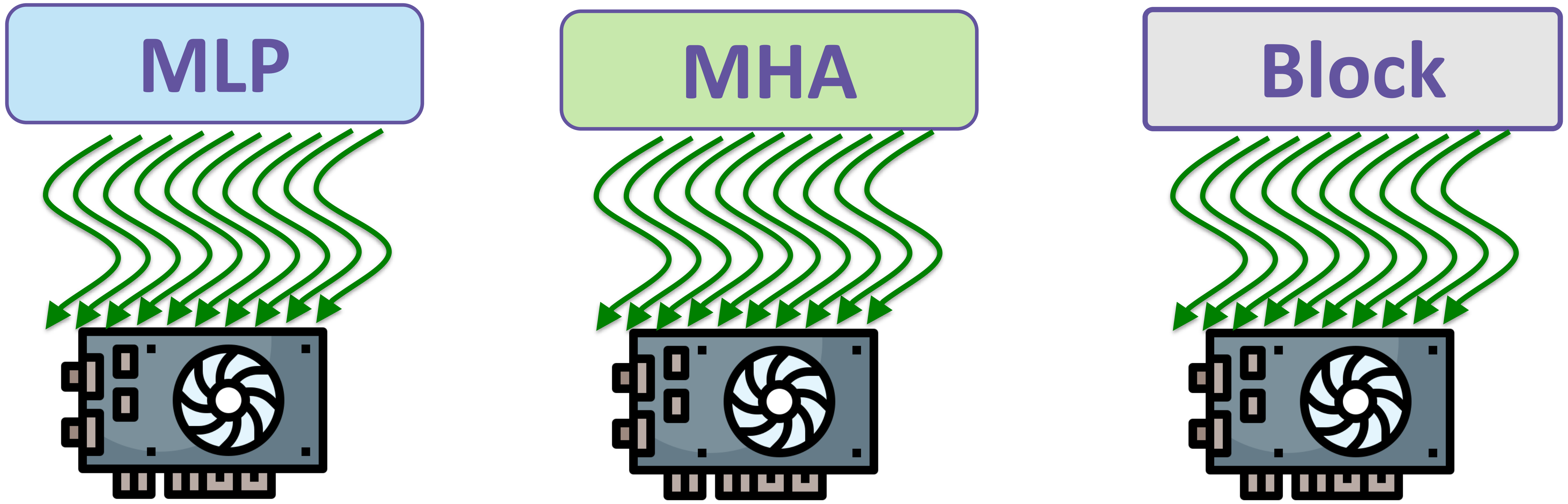
- We split the ViT into its essential operations
- We measure the FIT rate of each operation

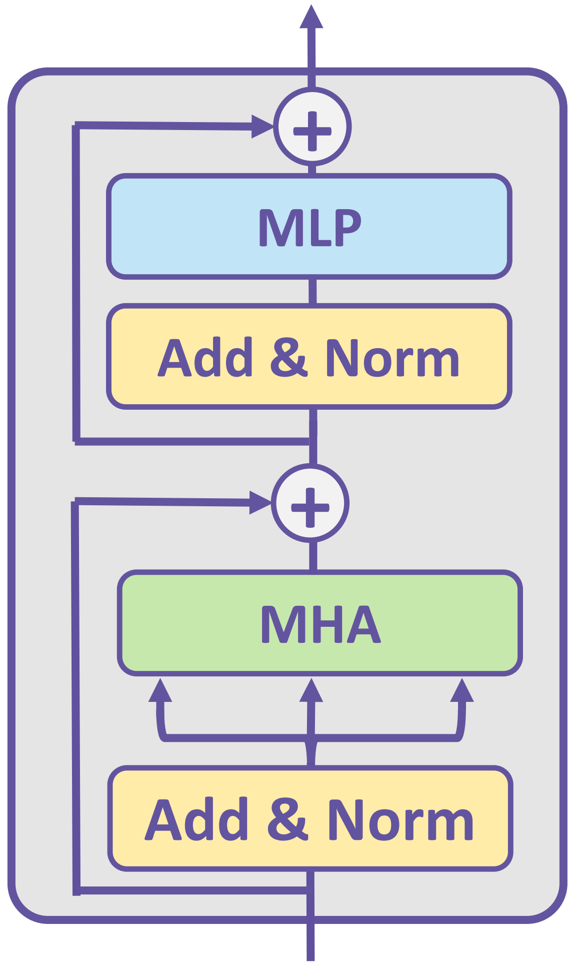




Fault Impact on ViT Operations

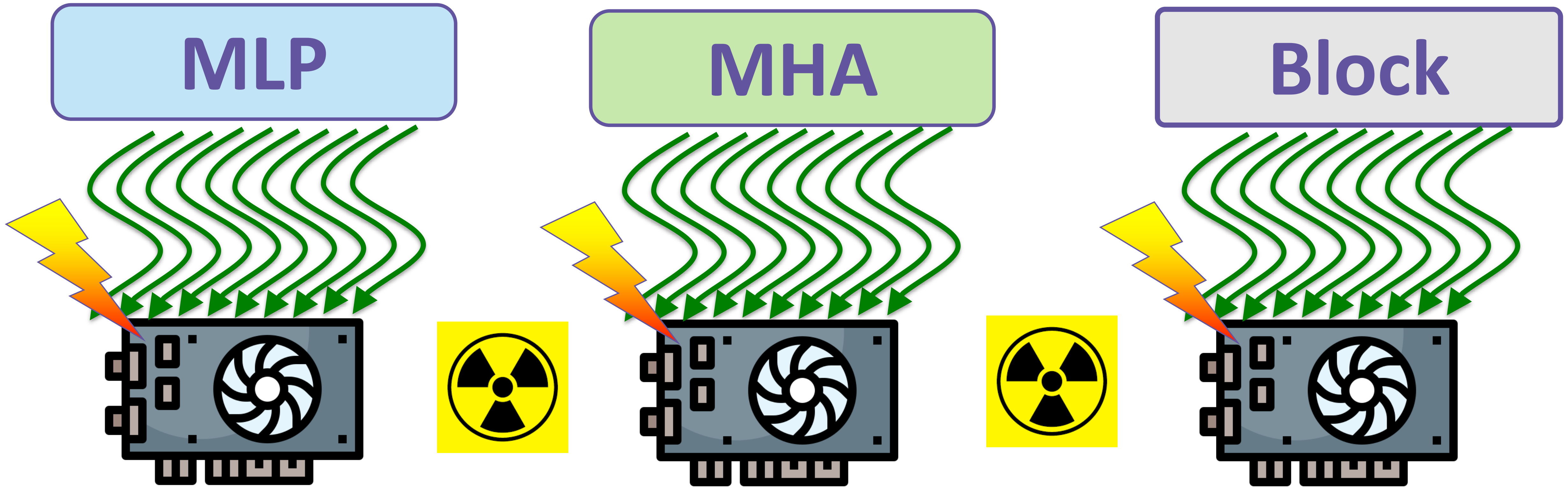
- We split the ViT into its essential operations
- We measure the FIT rate of each operation

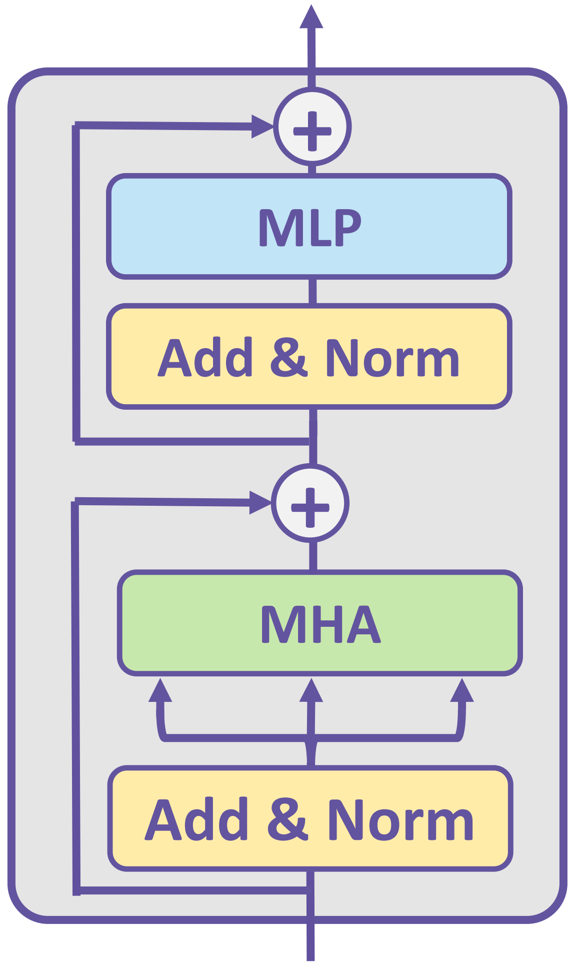




Fault Impact on ViT Operations

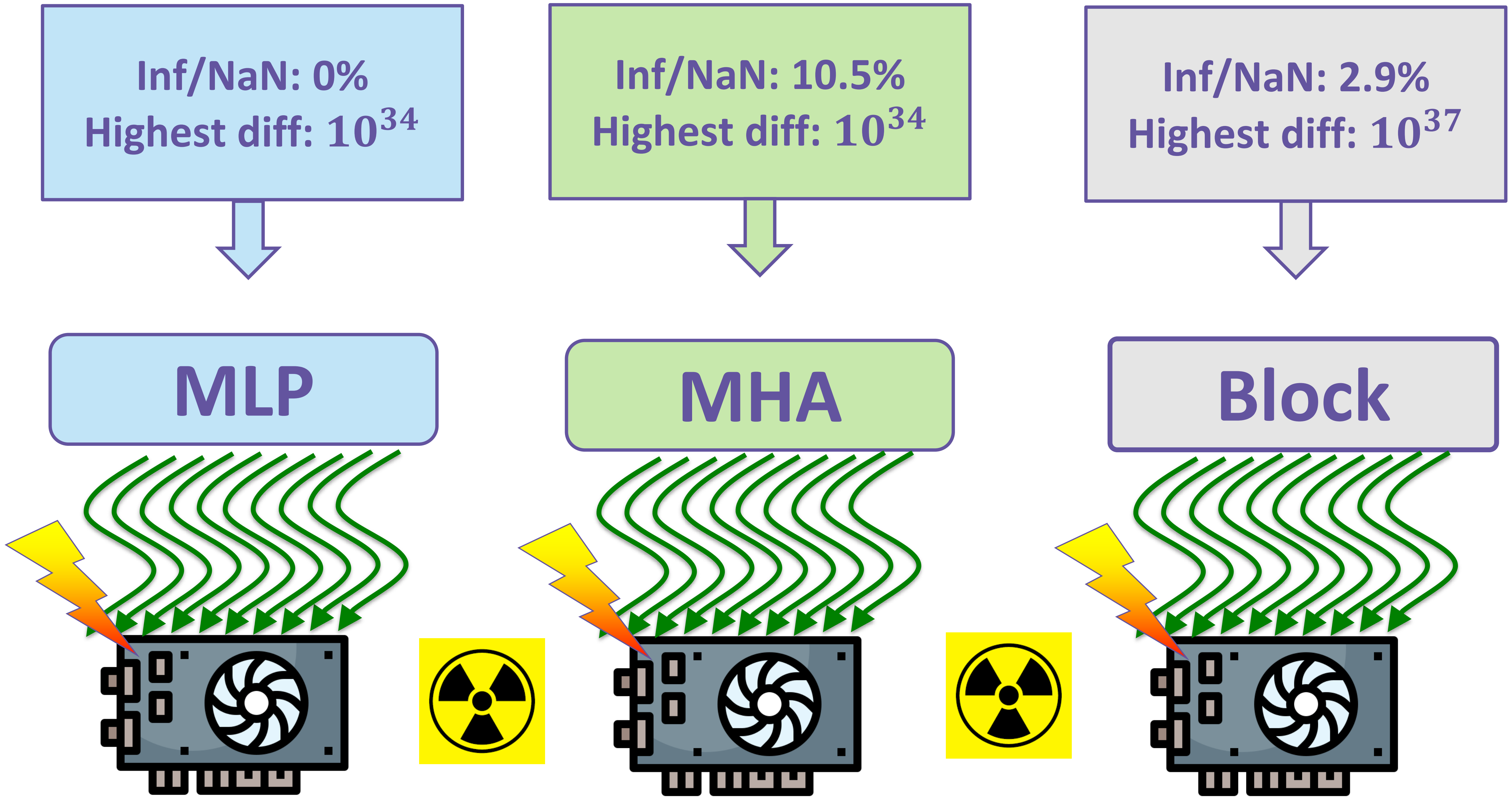
- We split the ViT into its essential operations
- We measure the FIT rate of each operation

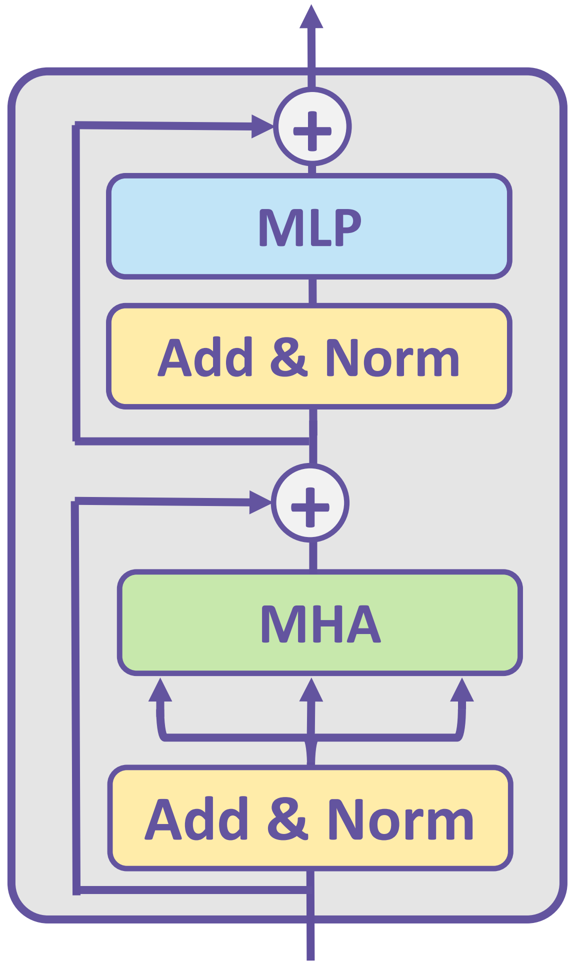




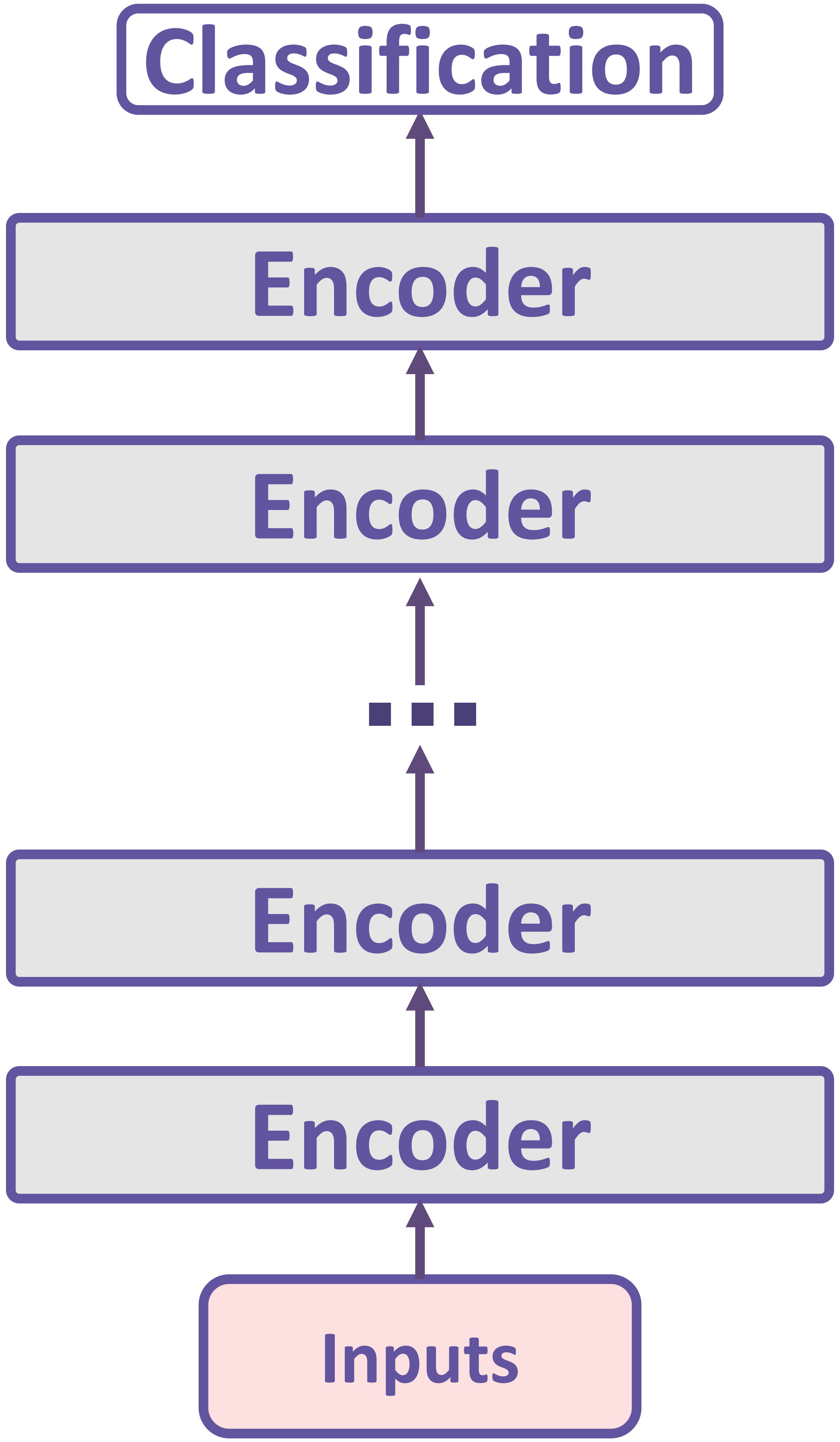
Fault Impact on ViT Operations

- We split the ViT into its essential operations
- We measure the FIT rate of each operation

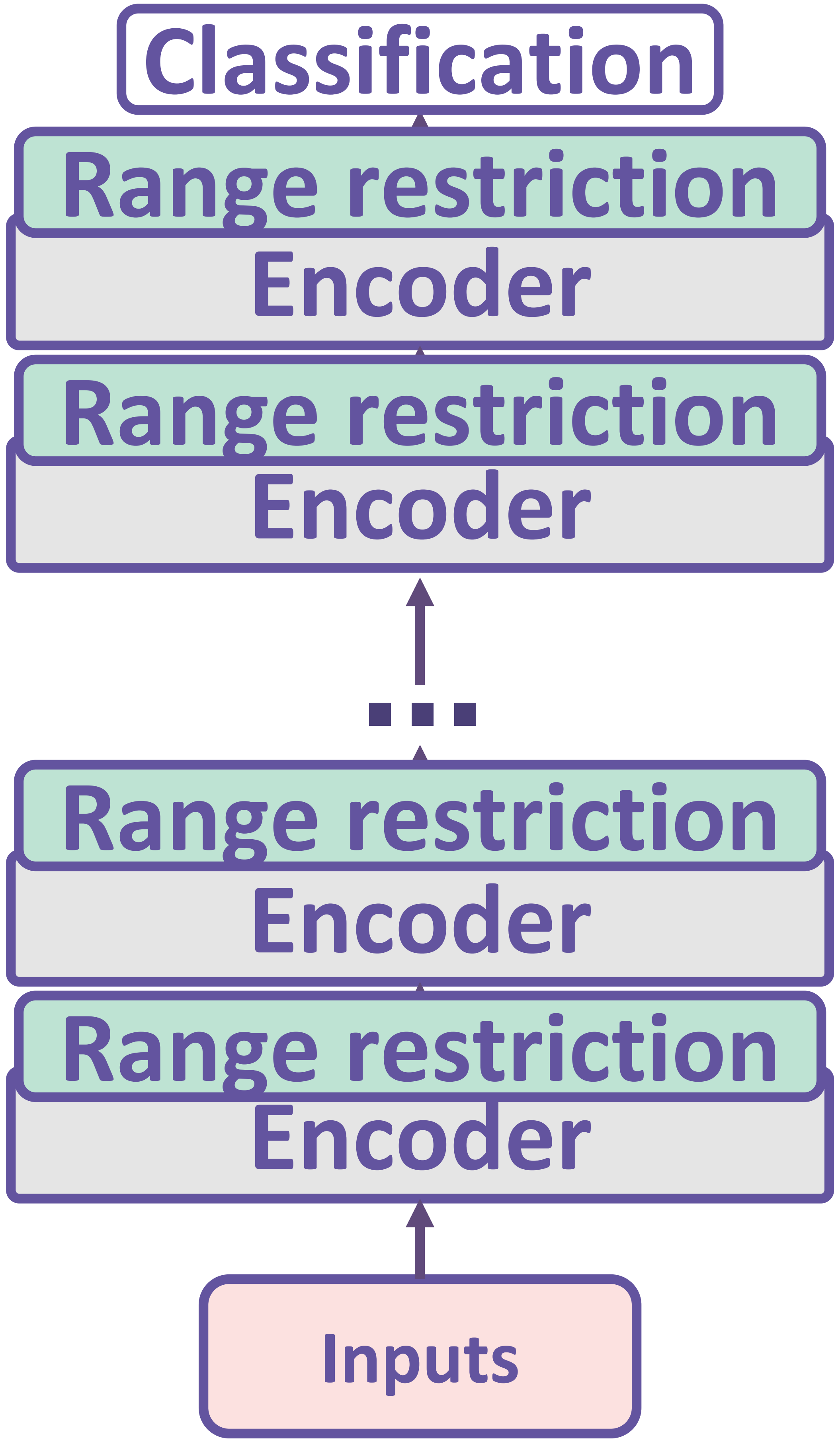




MaxiMals Idea



MaxiMals Idea


Classification

Range restriction

Encoder

Range restriction

Encoder

...

Range restriction

Encoder

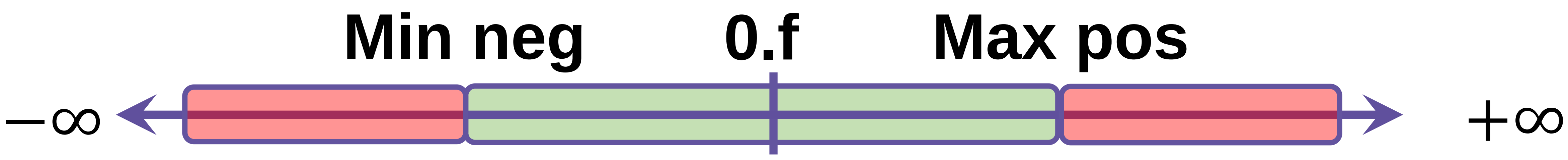
Range restriction

Encoder

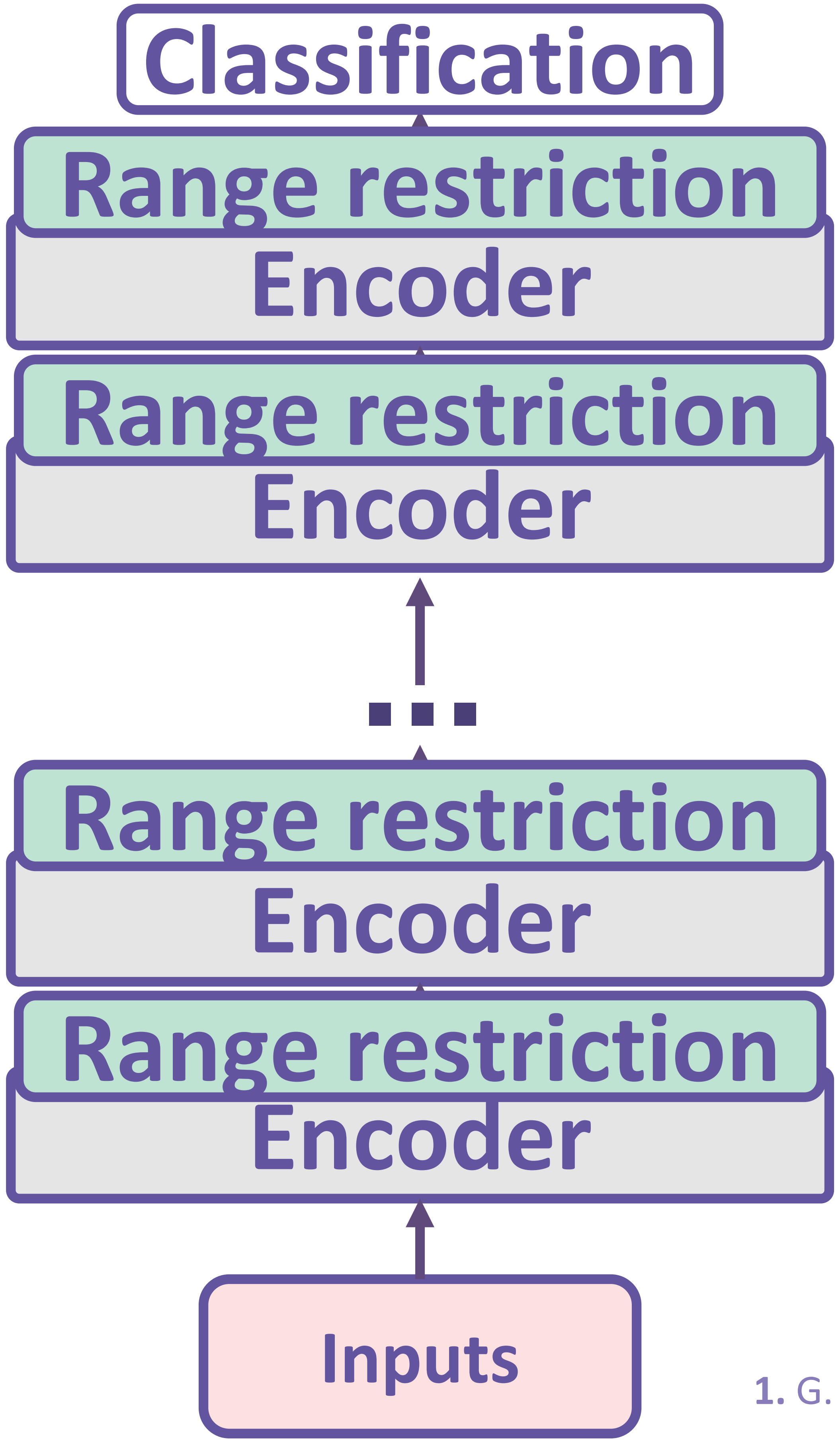
Inputs

Range Restriction is a common hardening technique

🟩 Safe values 🟥 Values that may change the classification

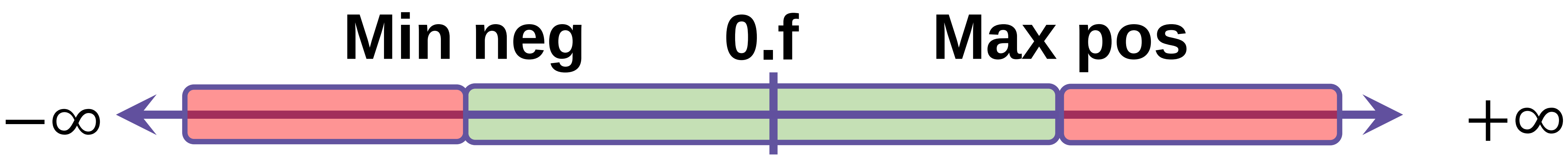


MaxiMals Idea



Range Restriction is a common hardening technique

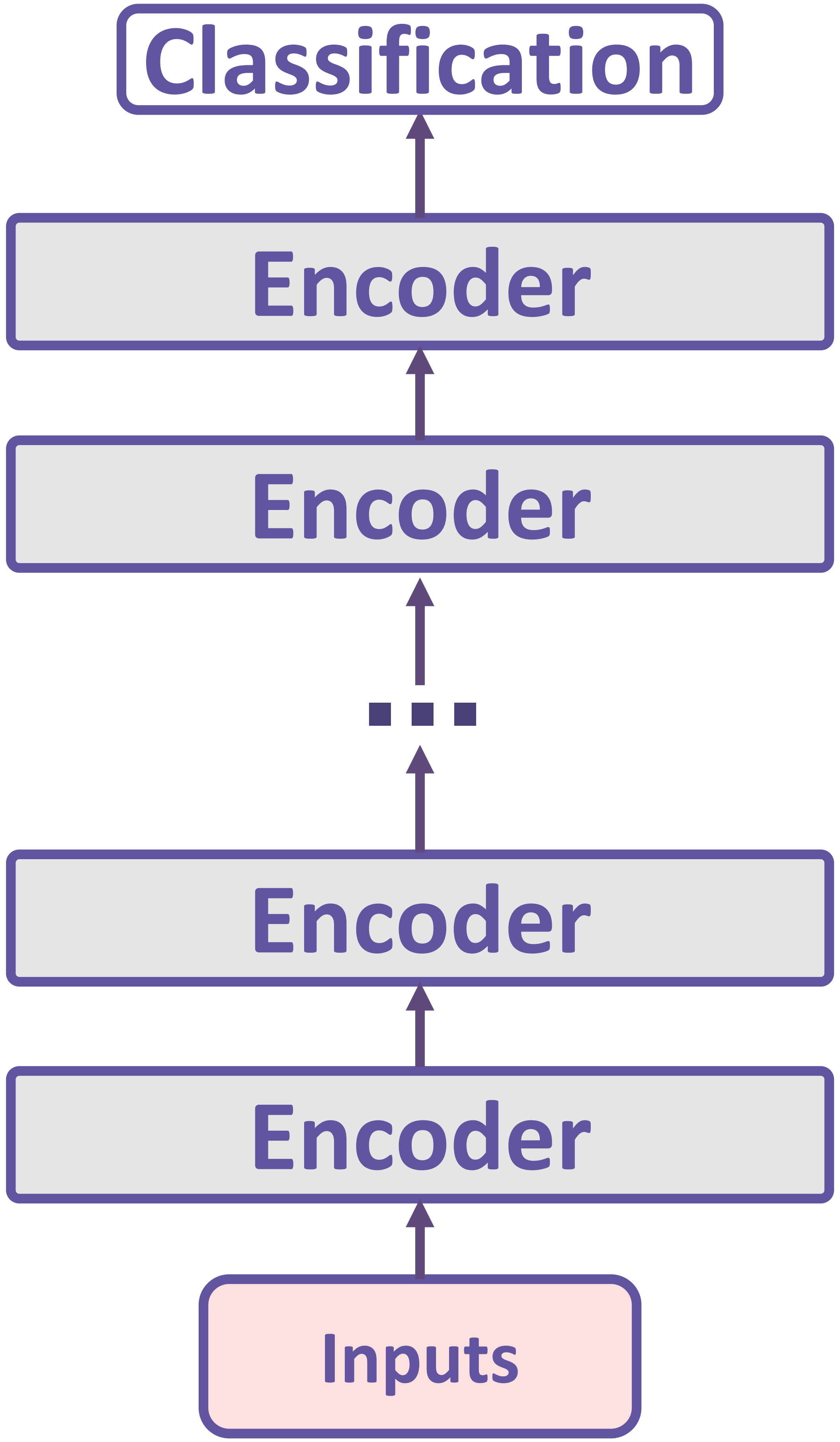
🟩 Safe values 🟥 Values that may change the classification



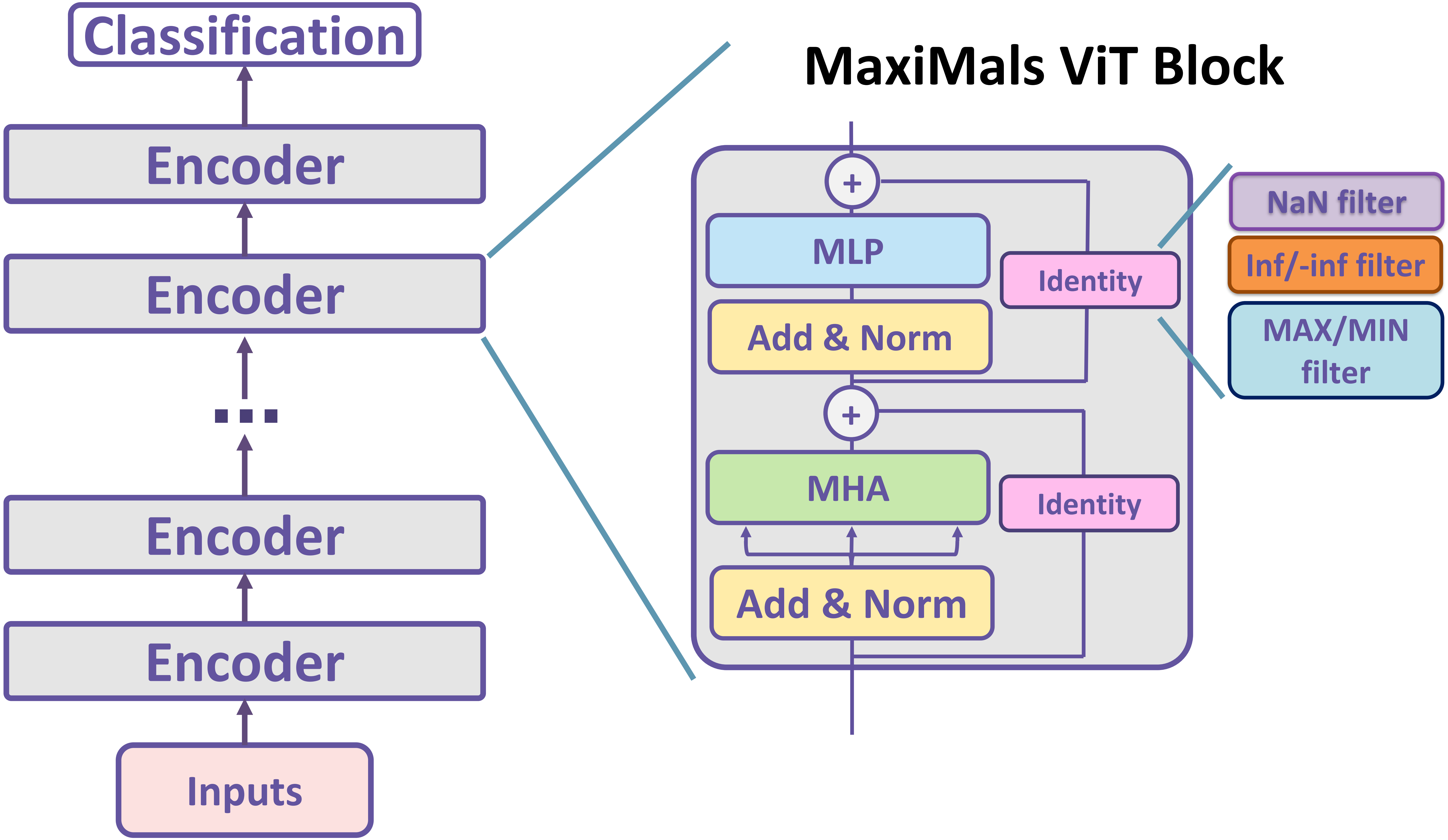
68% time overhead if applied on every block of a ViT[1]

[1] G. Gavarini *et al.* "**Evaluation and mitigation of faults affecting swin transformers**" – IEEE IOLTS 2023

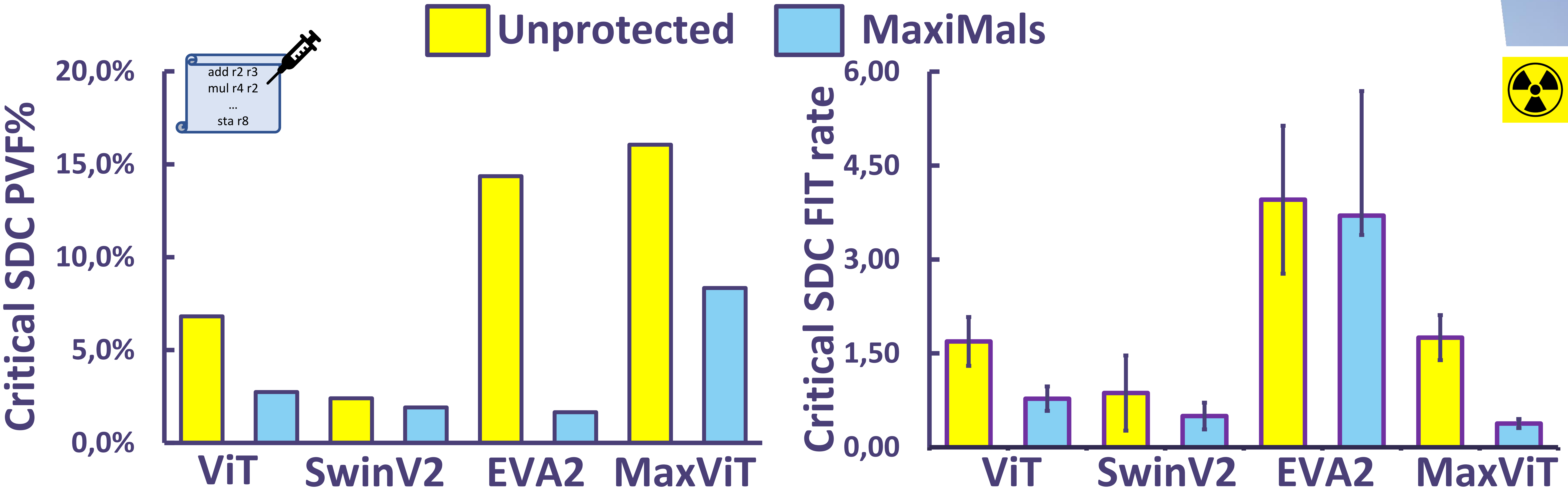
MaxiMals Idea



MaxiMals Idea

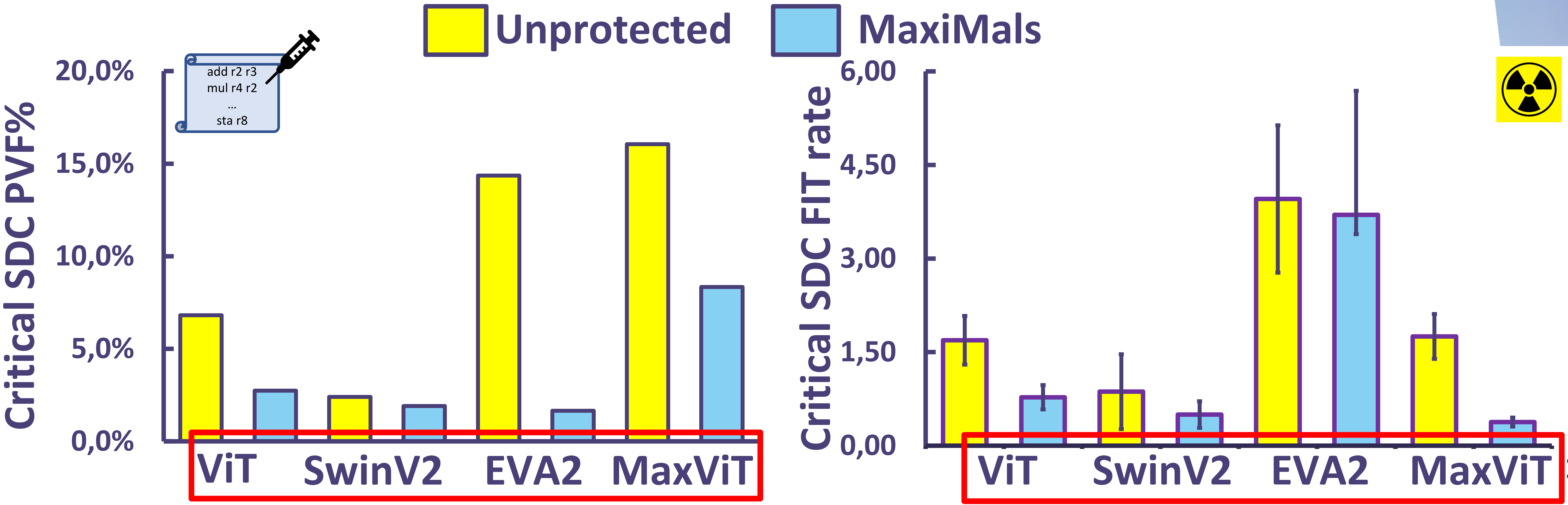


MaxiMals Efficiency



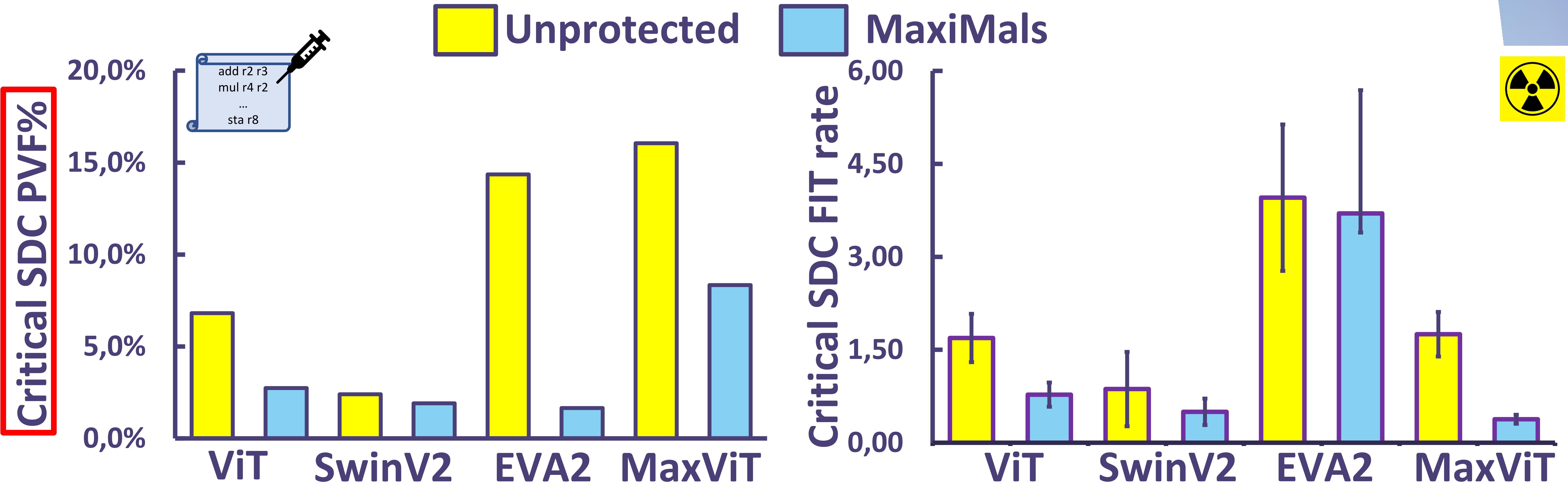
```
add r2 r3
mul r4 r2
...
sta r8
```

MaxiMals Efficiency

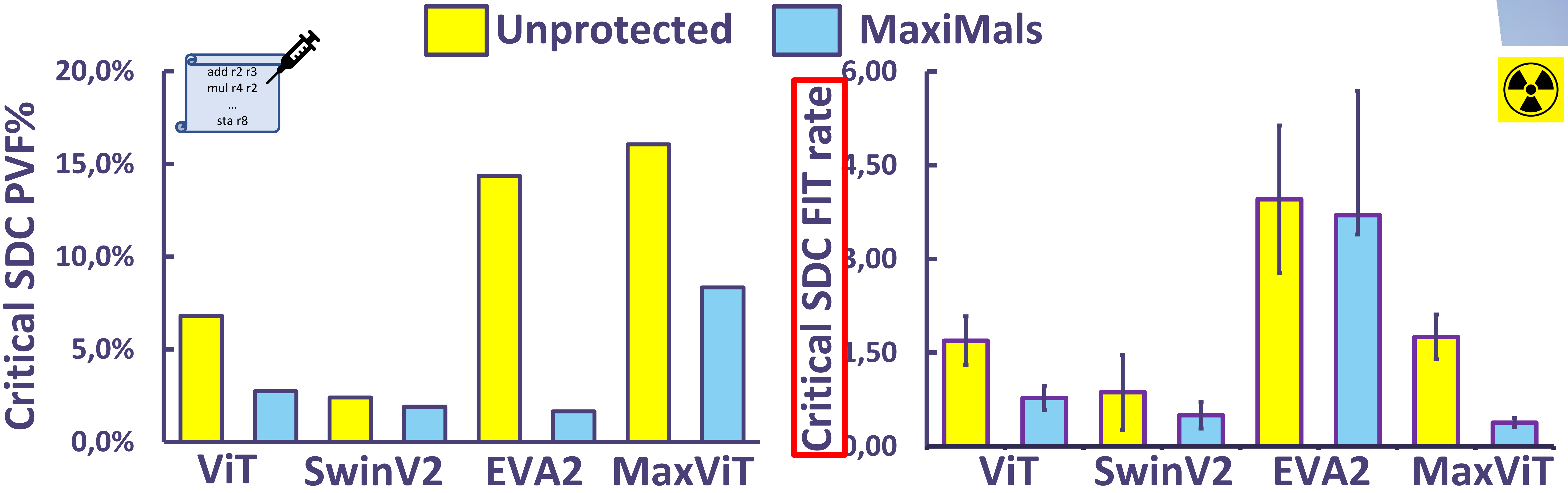


```
add r2 r3
mul r4 r2
...
sta r8
```

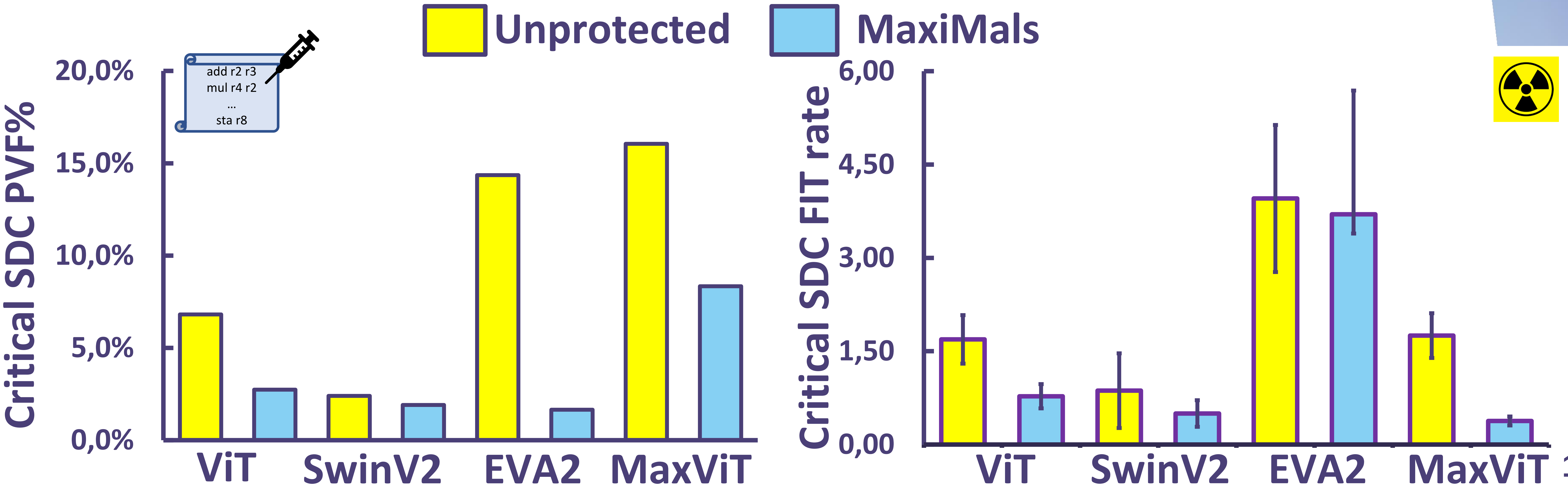
MaxiMals Efficiency



MaxiMals Efficiency



MaxiMals Efficiency

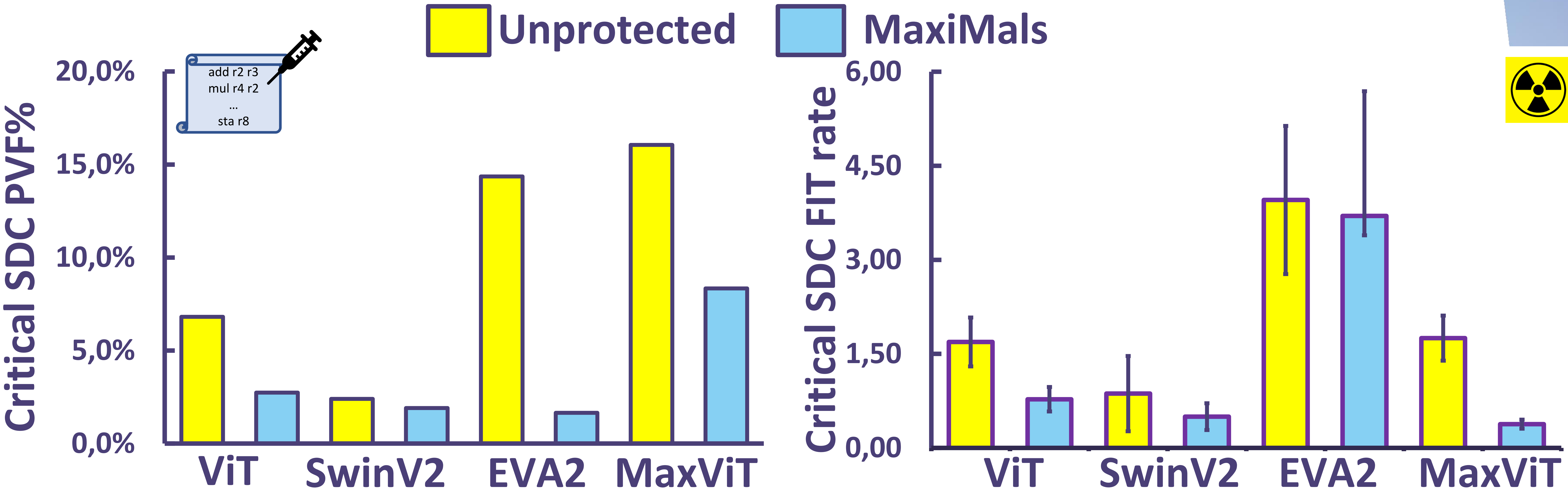


```
add r2 r3
mul r4 r2
...
sta r8
```

MaxiMals Efficiency

Fault Simulation:

- Injections with NVBitFI
- Critical SDCs are reduces by half on average



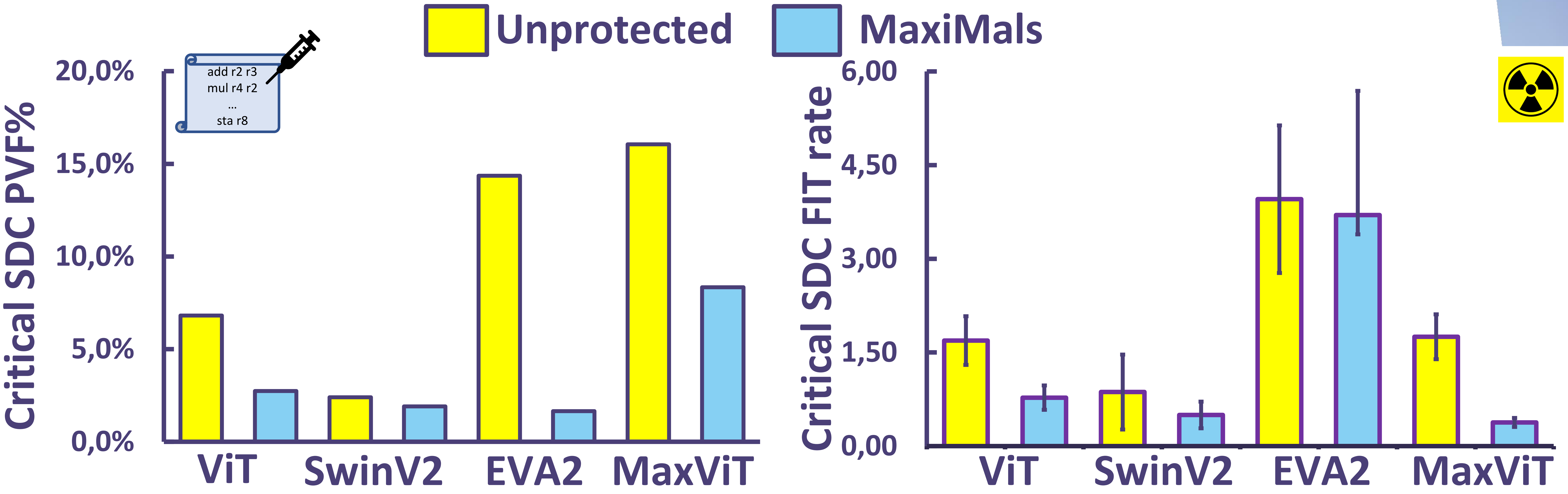
MaxiMals Efficiency

Fault Simulation:

- Injections with NVBitFI
- Critical SDCs are reduces by half on average

Beam injection:

- Similar reduction for beam
- Similar trend on FP16

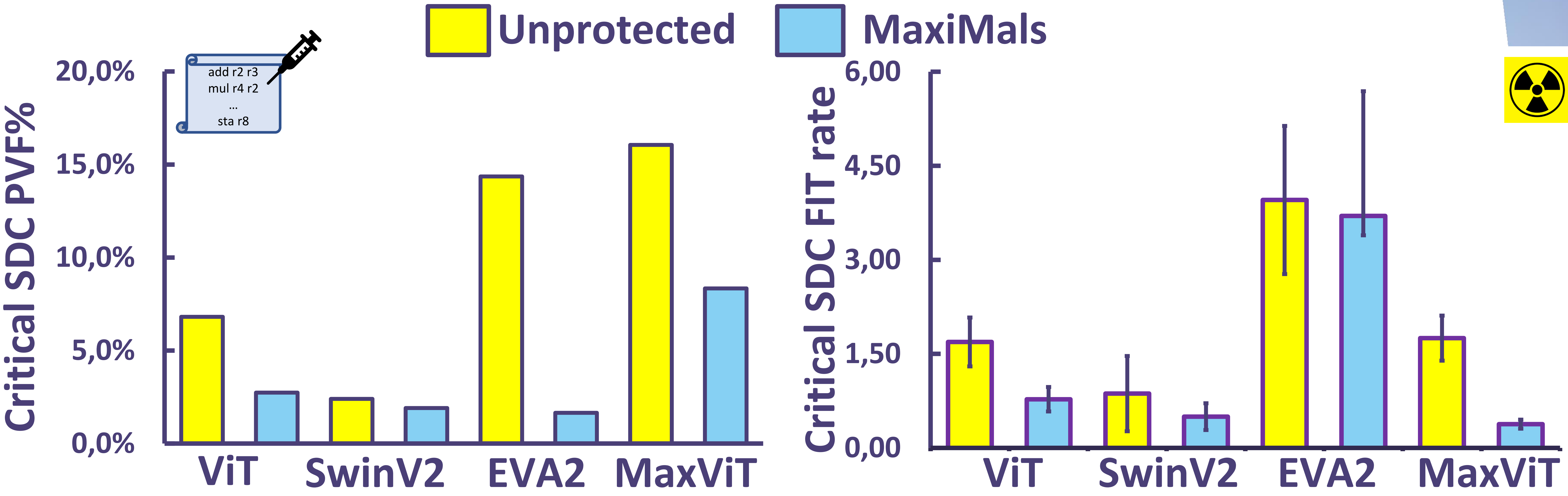


```
add r2 r3
mul r4 r2
...
sta r8
```

MaxiMals Efficiency

Average overhead:

- **Time: 7.1% (max. 16.1%)**
- **1.6% of additionnal instructions**



Conclusions and Future Directions

Conclusions and Future Directions

Conclusions and Future Directions

ViT FIT Rate

- FIT rate is high and grows according to model’s complexity
- ViT are vulnerable even if ECC is enabled (up to 10%)

Conclusions and Future Directions

ViT FIT Rate

- FIT rate is high and grows according to model's complexity
- ViT are vulnerable even if ECC is enabled (up to 10%)

MaxiMals

- A simple range restriction method for ViT
- Low overhead compared to similar techniques (max. 16%)

Conclusions and Future Directions

ViT FIT Rate

- FIT rate is high and grows according to model’s complexity
- ViT are vulnerable even if ECC is enabled (up to 10%)

MaxiMals

- A simple range restriction method for ViT
- Low overhead compared to similar techniques (max. 16%)

Future works

- Impact on INT8 precision
- Dependency between inputs and Critical SDC rates
- Other fault models:
  - different particles
  - HW attacks (RowHammer)

Supporters

Science & Technology
Facilities Council

anr
agence nationale
de la recherche

FASY

RAD
NEXT

Avec le soutien de

Région
BRETAGNE

Thank you ！

Questions ?

Contact: lucas.roquet@inria.fr