SYNOPSYS®
Silicon to Software™

Security 101 for Artificial Intelligence SoCs

D&R IP SoC Virtual Event

Dana Neustadter, Senior Manager of Product Marketing for Security IP

April 2020

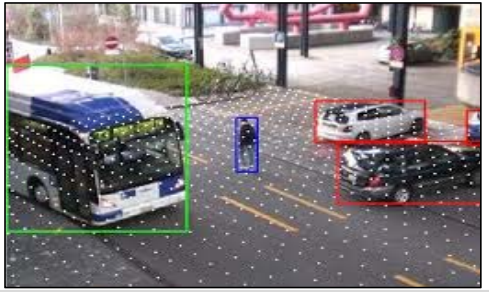
AI Applications are Exploding

From Data Center to Edge

Data Center

Automotive

Vision Systems

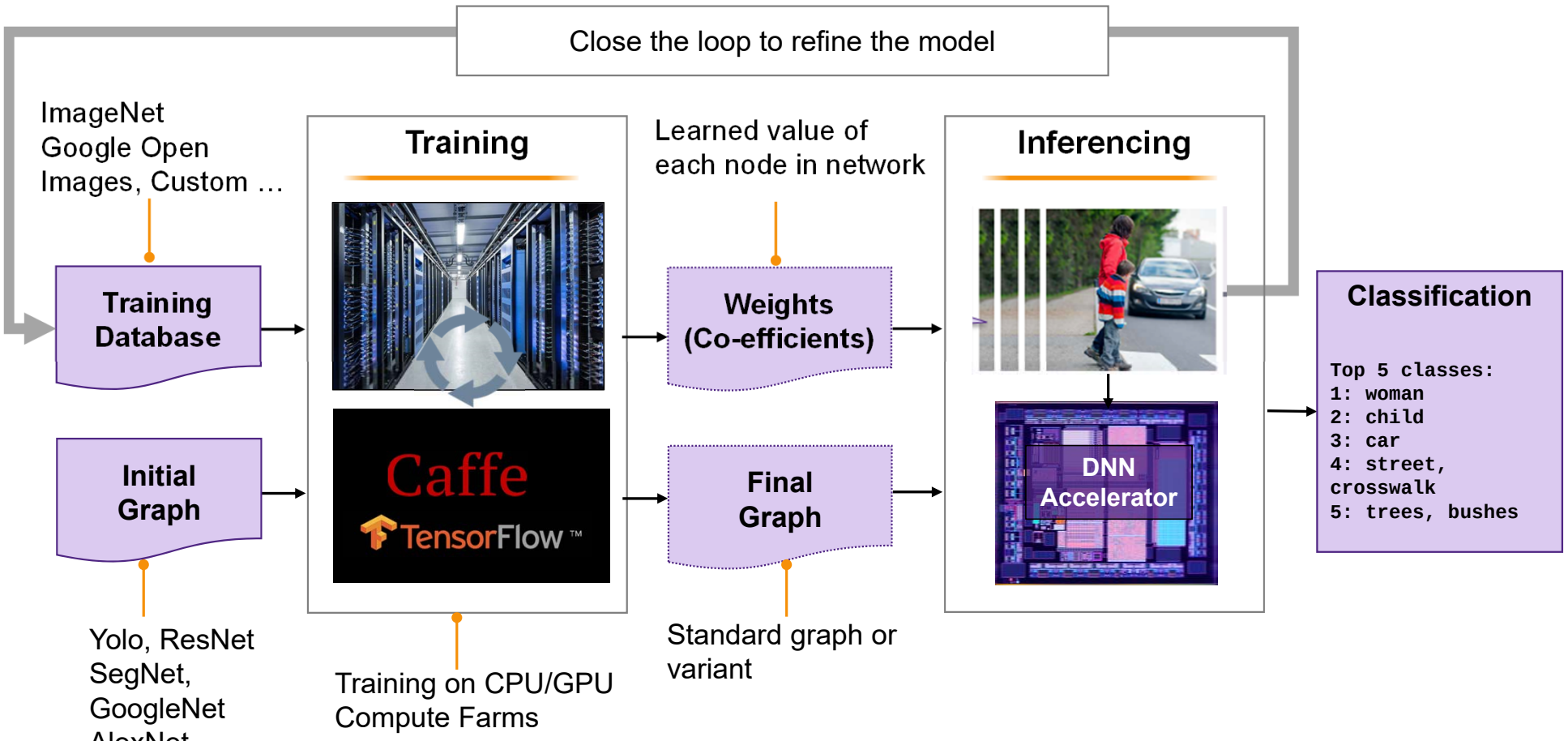


Natural Language Understanding

Context Awareness

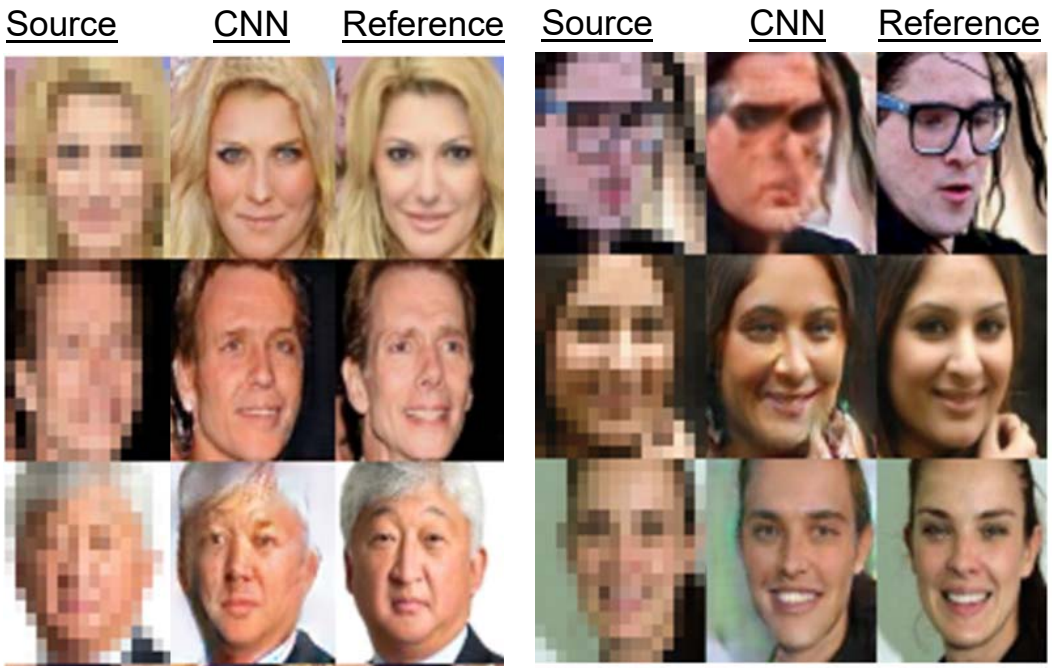
5G Self Optimization

Complex Models: From Training to Inferencing



Valuable Assets in AI

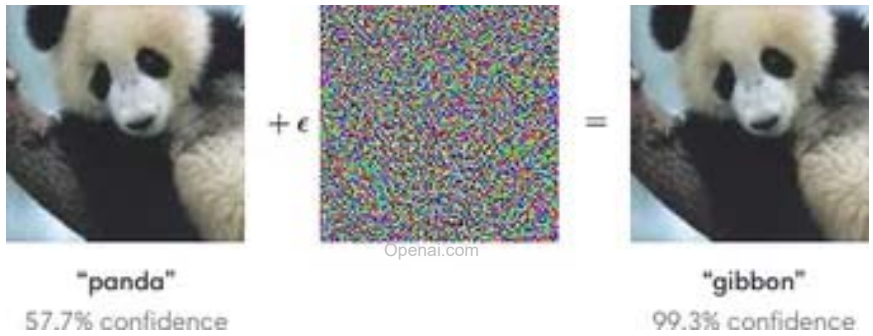
- Embedded AI inference engines built on neural networks (NN) implemented in Silicon
  - Continue to be an active area of research
- Models are expensive to compute and are a valuable intellectual property investment
- Many embedded AI applications focus on user biometrics such as voice, face and fingerprint identification and recognition
  - User privacy concerns
  - Integrity of the model: a corrupted model behaves poorly and leads to mistakes
- Training of NNs to extract the model (weights) takes place off-line
  - Usually in the cloud
  - Training requires large amounts of compute and huge high quality datasets

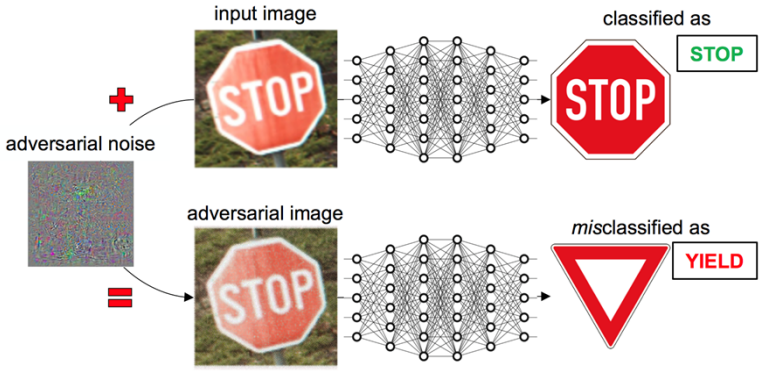


"Image Super-Resolution Using Deep Convolutional Networks (2016), C. Dong et al."
http://i2.cdn.turner.com/cnn/dam/assets/140411160038-faces-brain-study-story-top.jpg

Who are the Adversaries? What can they do?

- Most known attacks on AI systems today are still academic or by “white-hat” researchers
  - Attacks in the wild: big AI engines for network threat detection (e.g. Gmail spam detector)
- Adversaries: hacktivists, criminals and criminal organizations, cyber terrorists, nation states
  - Add to that: insiders (accidental or malicious), the curious and mischievous, researchers
- Adversarial Inputs: craft the input to produce a desired outcome

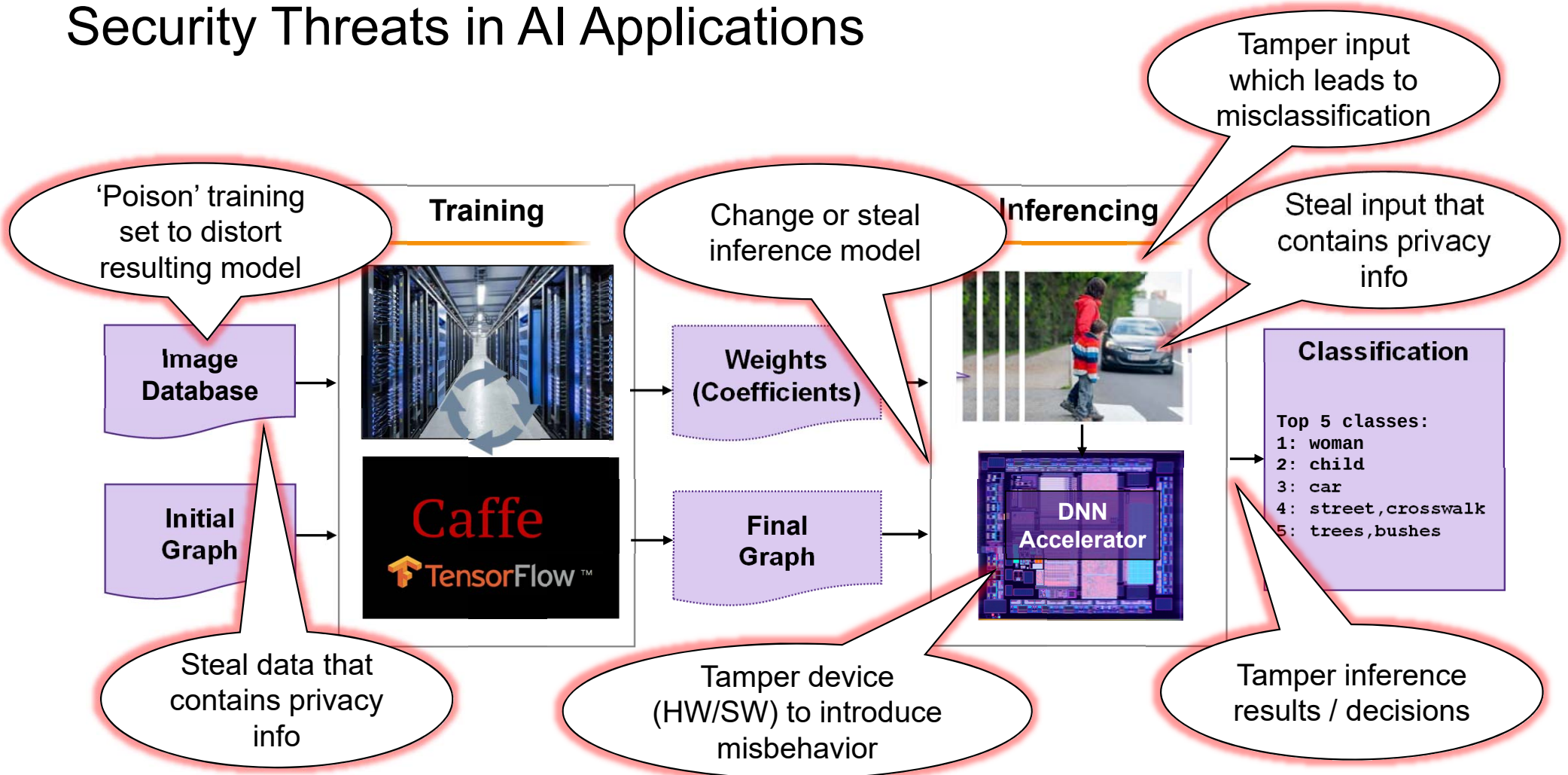




https://www.pluribus-one.it/research/sec-ml/wild-patterns

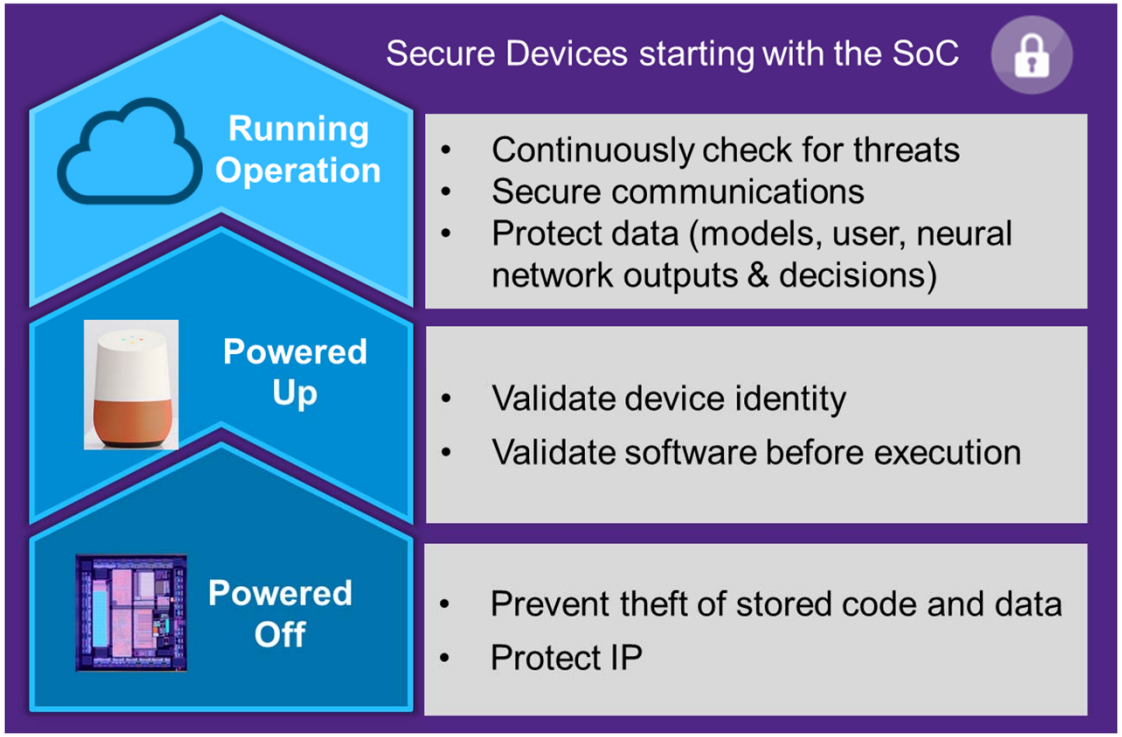
- “Data Poisoning”: manipulate the training data
  - Trojan insertion – a special case of data poisoning
- Model theft: let someone else do the hard work

Security Threats in AI Applications

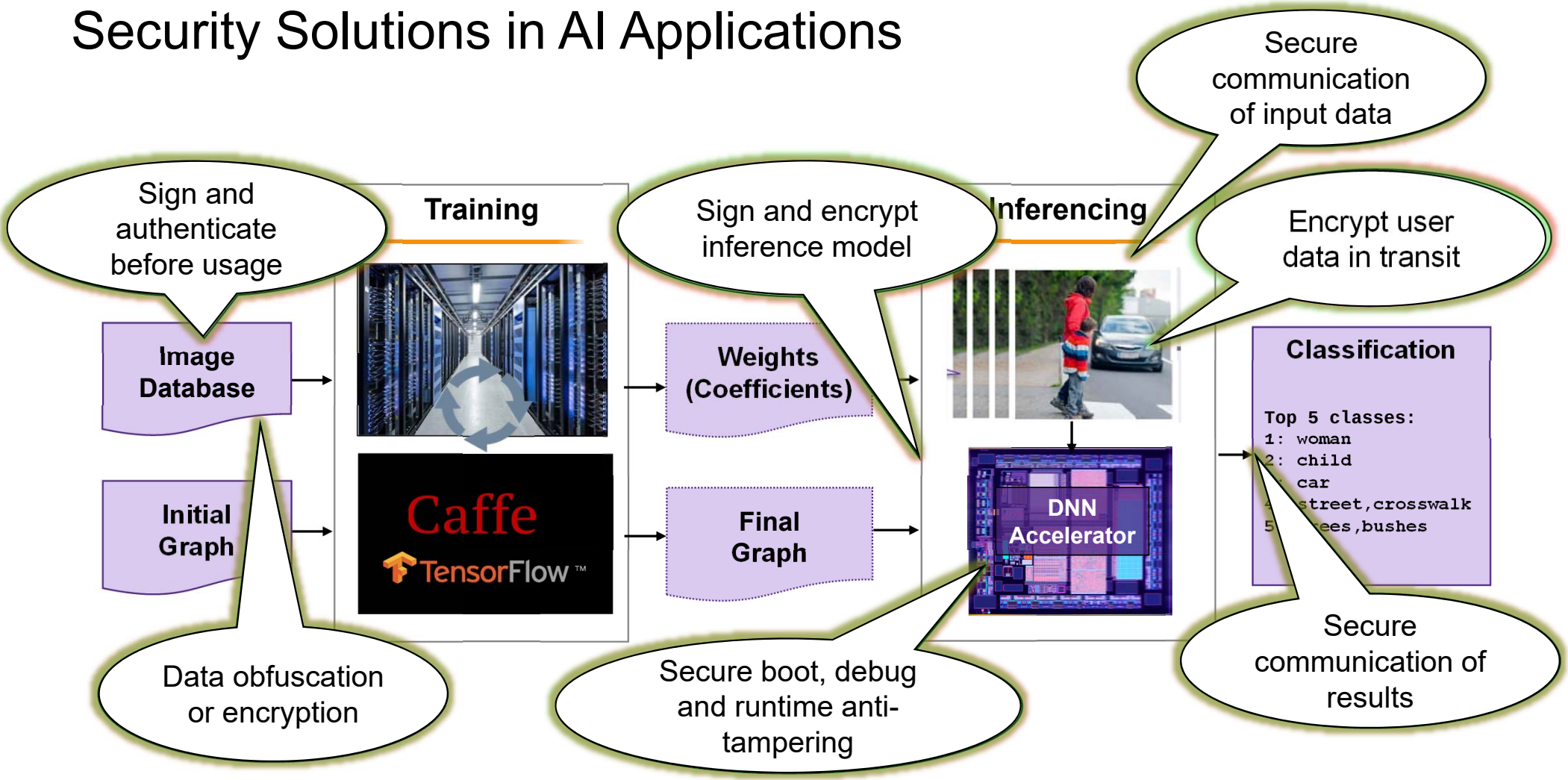


Approaches to Dealing With Threats

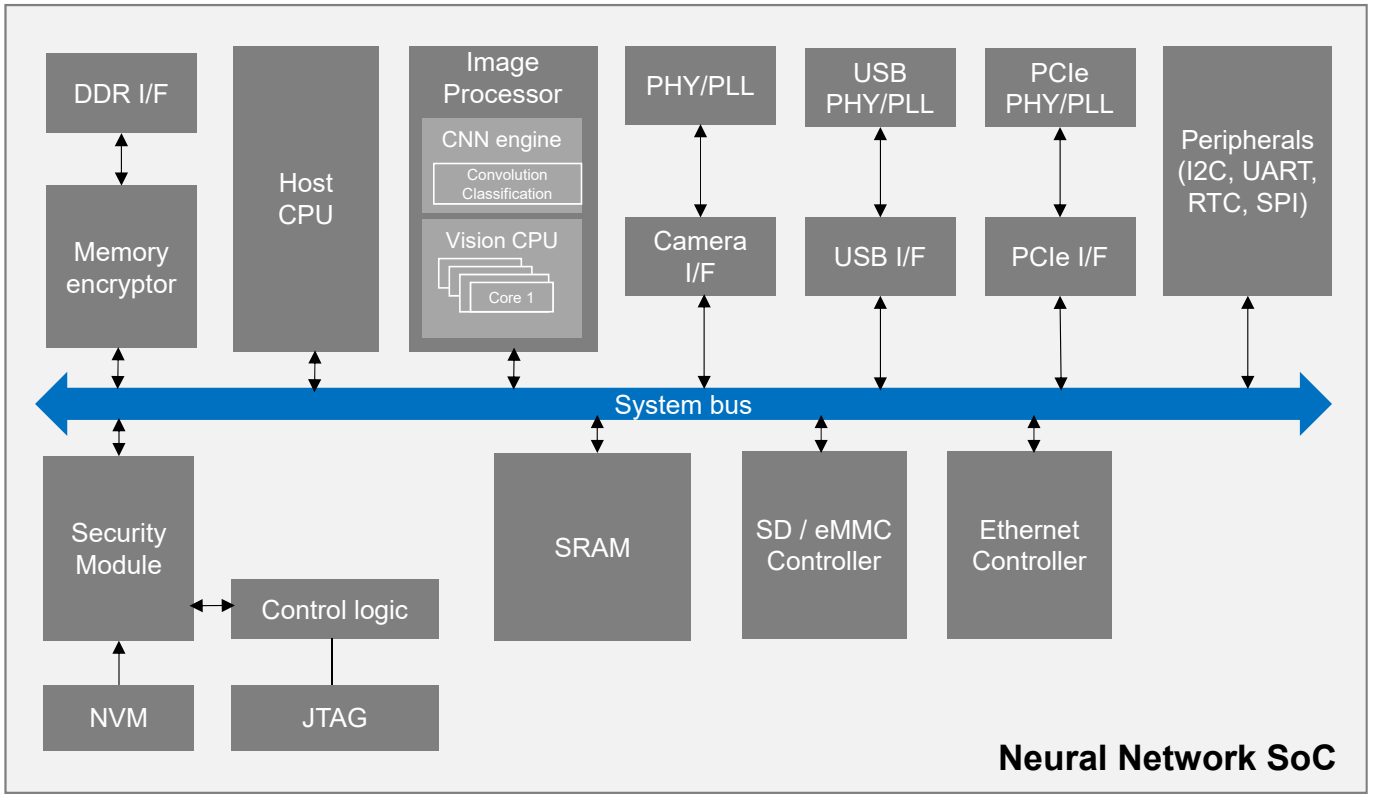
Actively Secure Your SoC



Security Solutions in AI Applications



Automotive Vision with NN SoC Example



Vision Processing SoC

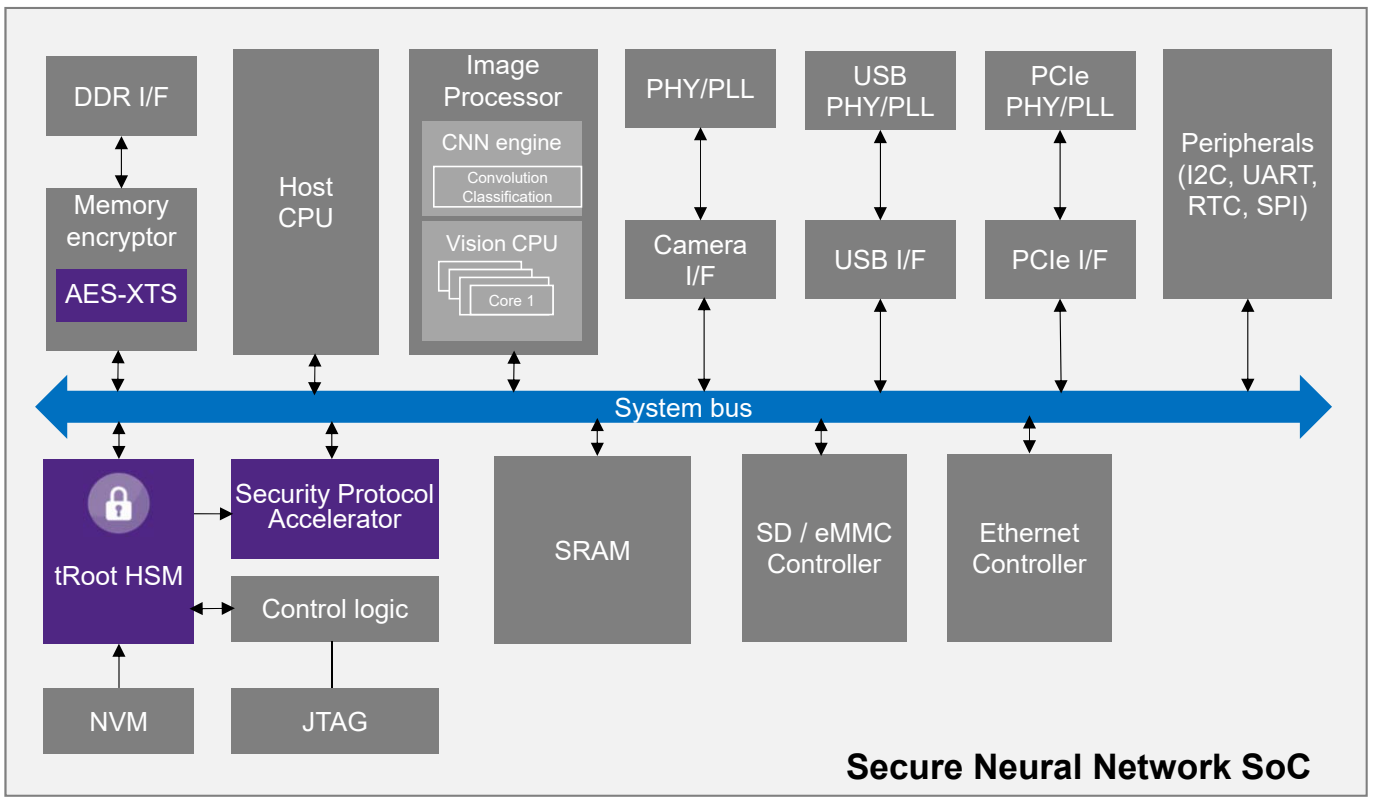
- Operates standalone or via multiple interface options as offload engine to host application processor

Security Needs

- Overall SoC protection functions (secure bootstrap, key management, secure updates, secure debug/JTAG access, …)
- Secure data-at-rest: memory encryption/decryption
- Encryption and authentication for model updates, secure communication and inputs from peripherals (e.g. camera)

Automotive Vision with NN SoC Example

Example with Synopsys Security IP



tRoot HSM provides a secure enclave in which to process sensitive data and operations for the SoC

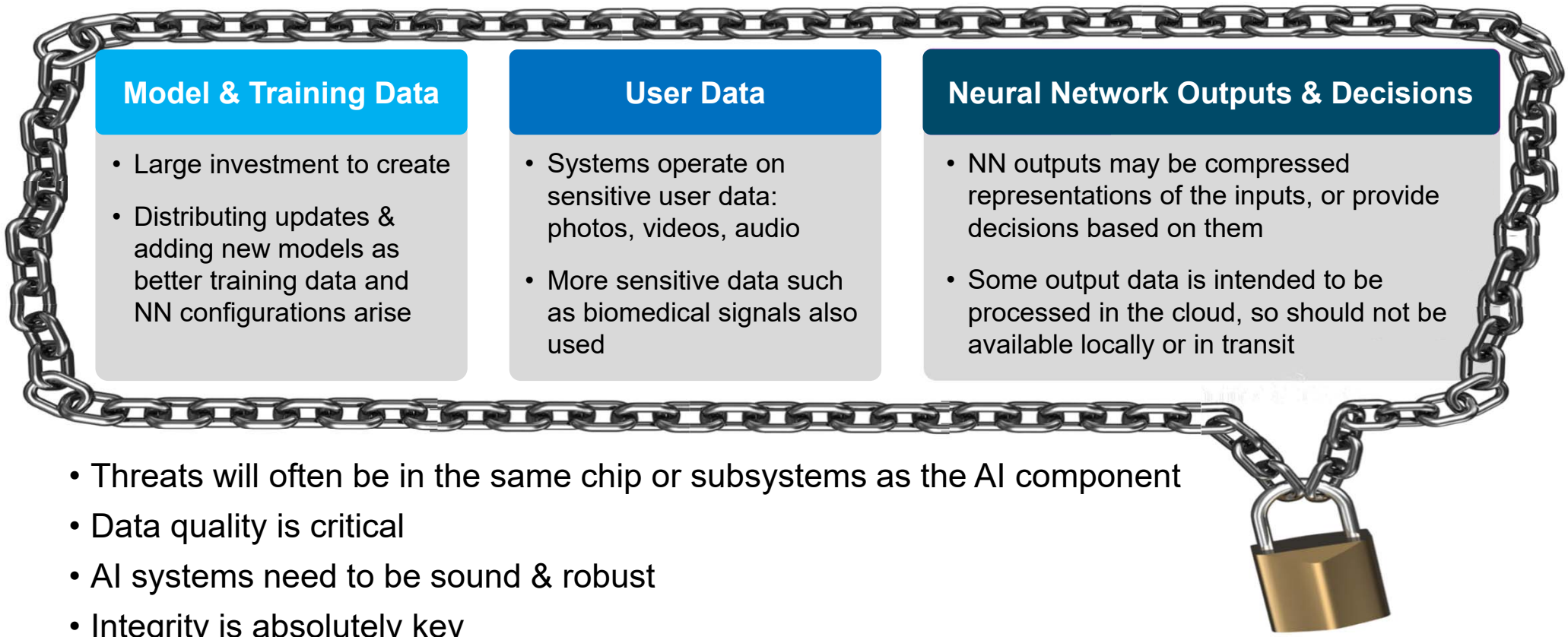
- Secure boot
- Key management
- Secure updates
- Secure debug and JTAG access

Security Protocol Accelerator (SPAcc) supports encryption and authentication for

- Model updates
- Secure communication
- Optional encrypted input from camera and other peripherals

High Performance AES-XTS for External memory encryption / decryption

Some Observations on Security Design



Model & Training Data	User Data	Neural Network Outputs & Decisions
• Large investment to create • Distributing updates & adding new models as better training data and NN configurations arise	• Systems operate on sensitive user data: photos, videos, audio • More sensitive data such as biomedical signals also used	• NN outputs may be compressed representations of the inputs, or provide decisions based on them • Some output data is intended to be processed in the cloud, so should not be available locally or in transit

- Threats will often be in the same chip or subsystems as the AI component
- Data quality is critical
- AI systems need to be sound & robust
- Integrity is absolutely key
- Confidentiality is very important for privacy and legal reasons

Summing Up

AI is revolutionizing the world

- Many new applications are driving growth in SoC designs with vision processing and neural network capabilities

Embedded AI has a number of assets to protect

- AI model
- User's private data
- Neural Network output

Security is integral to the design process, starting with the SoC

Synopsys has solutions to these challenges

Let Synopsys help protect your valuable AI assets

SYNOPSYS®
Silicon to Software™

Thank You