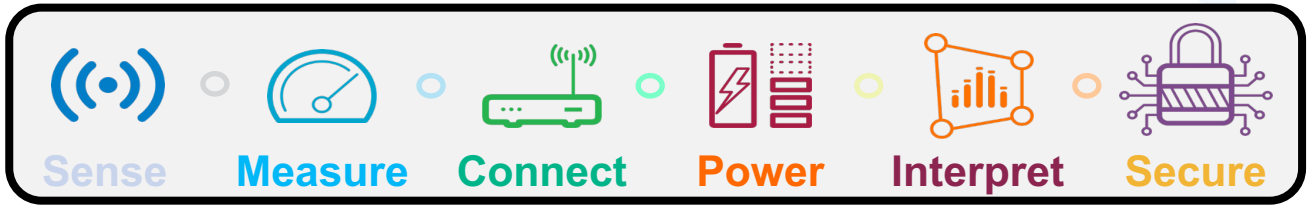
Security and Data at the Intelligent Edge: First Principles and a Few Case Studies

David Robertson (david.Robertson@analog.com)
Doug Gardner
John Wallrabenstein

AHEAD OF WHAT'S POSSIBLE™

Analog Devices – Brief Introduction



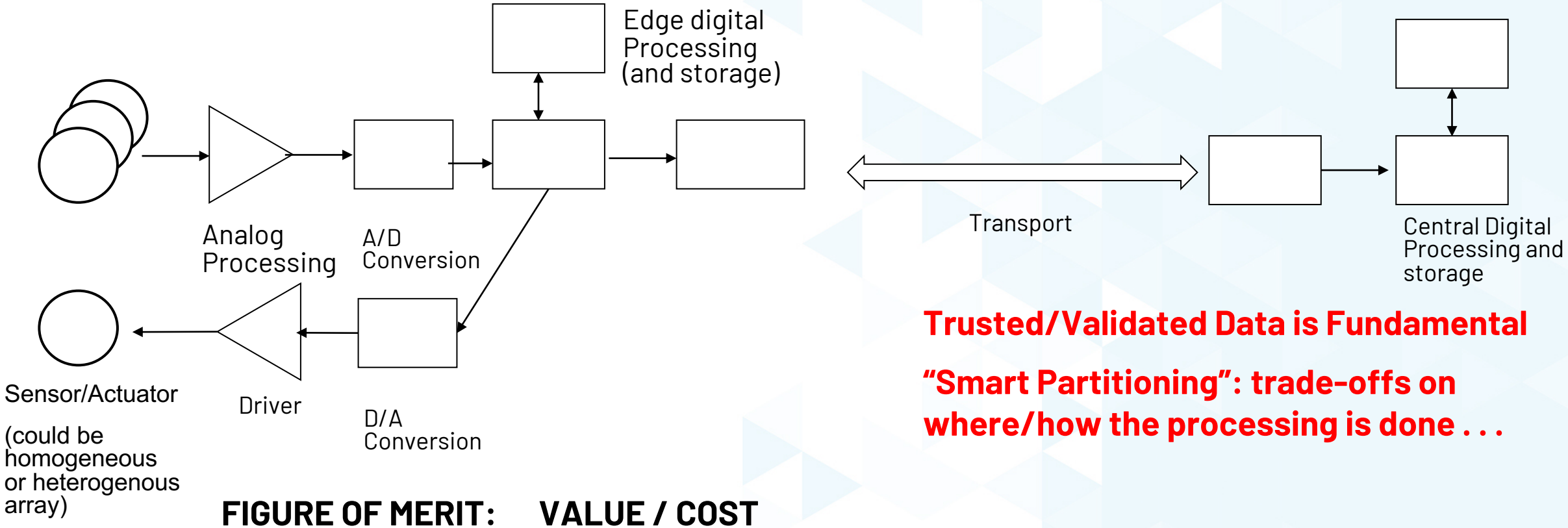
- The Intelligent Edge:
  - Where the real world meets the digital world
- World Leader in Semiconductors
  - Analog
  - Mixed-signal
  - Sensors
  - Digital signal processing
  - Algorithms

Outline

- Intro: the Intelligent Edge
  - Key Elements
  - Performance Trade Space
- Security at the Edge
  - Diverse Threats/multiple attack surfaces (in addition to normal “faults”)
  - Concerns: Disruption/interference, interception, spoofing, weaponizing
  - Possible Solutions/Mitigation (including analytics)
- Trust
  - Security Trust and Reliability Trust
  - What “zero trust” means at the edge
  - Root of trust/authentication chain
  - Notion of “watermarking” or other mechanisms of authenticity tracking
- Case Study 1: Wireless Infrastructure (including 5G and Open RAN)
- Case Study 2: Remote Sensor Nodes

Edge Processing “Chain”

(note– depending on situation requiring action, this may be a “round trip” journey back to an actuator . . .)



Trusted/Validated Data is Fundamental

“Smart Partitioning”: trade-offs on where/how the processing is done . . .

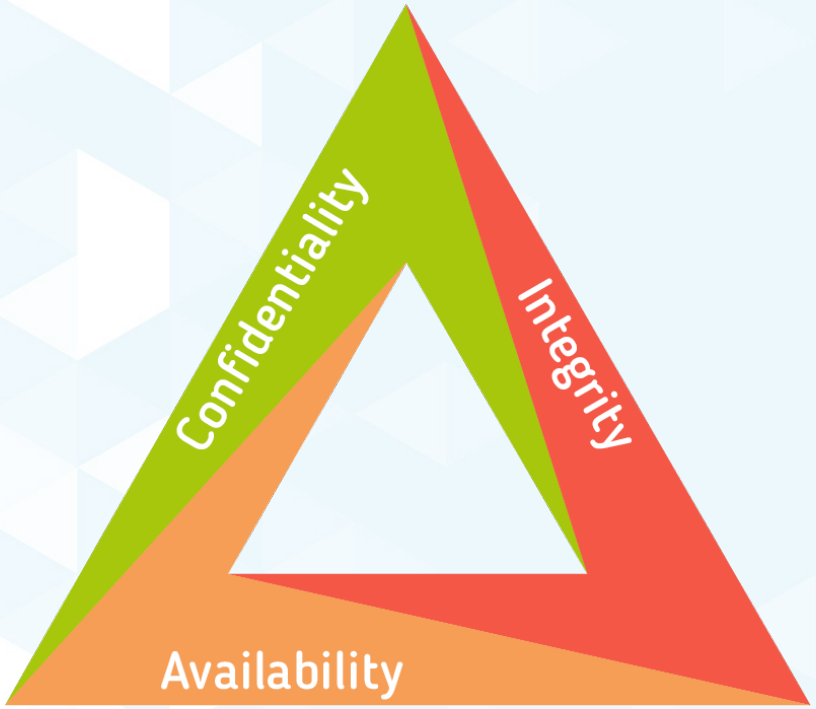
FIGURE OF MERIT: VALUE / COST

Value: Data → Information → INSIGHT (modifiers: location, latency, confidence: accuracy, security: trust)

Cost: Power (as a convenient proxy)

What does “Security” Mean?

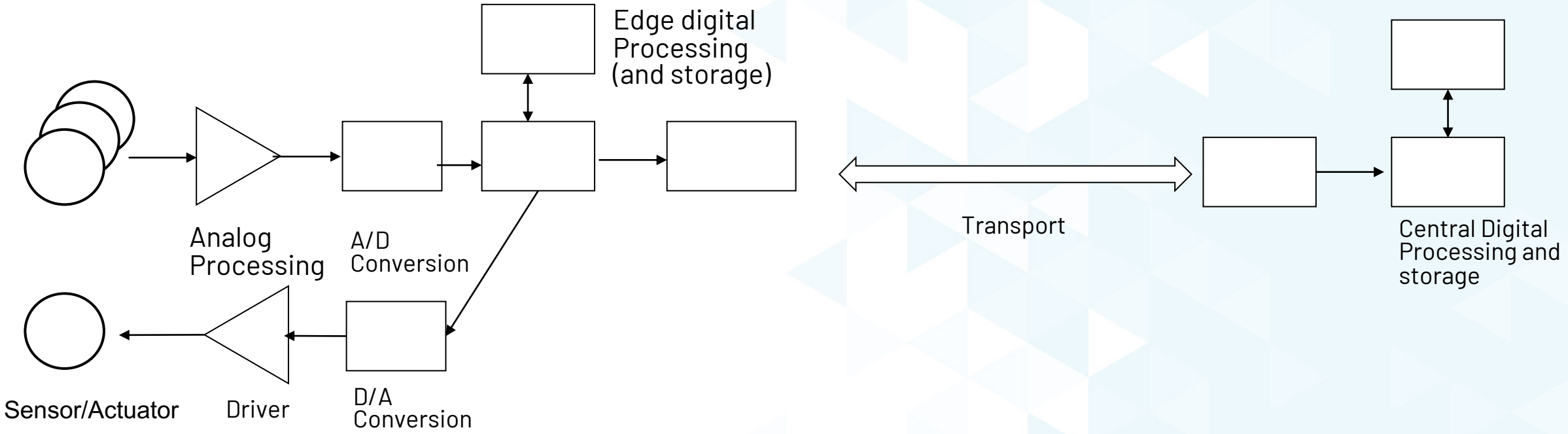
- Candidate Answers
  - The adversary can’t read my messages
    - What if they can change them?
  - The adversary can’t compromise my system
    - What if no one can access the system at all?
  - Important to define **security goals**
  - **Reliability** related, but a different kind of “trust” . . .



- Core Properties of Security
  - **Confidentiality**
    - Protecting data from unauthorized views
  - **Integrity**
    - Protecting data from unauthorized modifications
  - **Availability**
    - Protecting authorized users from service disruptions

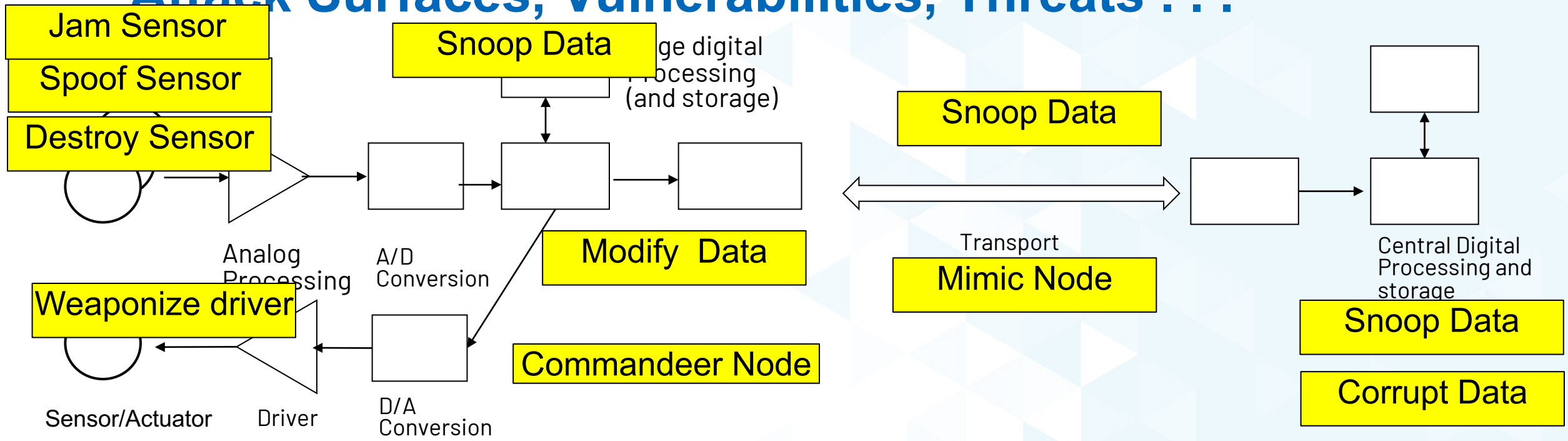
- **Authentication**
  - Are you who you claim to be?
- **Authorization**
  - Do you have permission to perform this operation?
- **Accountability**
  - What happened, when, and by whom?

Security at Edge - Processing "Chain": Attack Surfaces, Vulnerabilities, Threats . . .



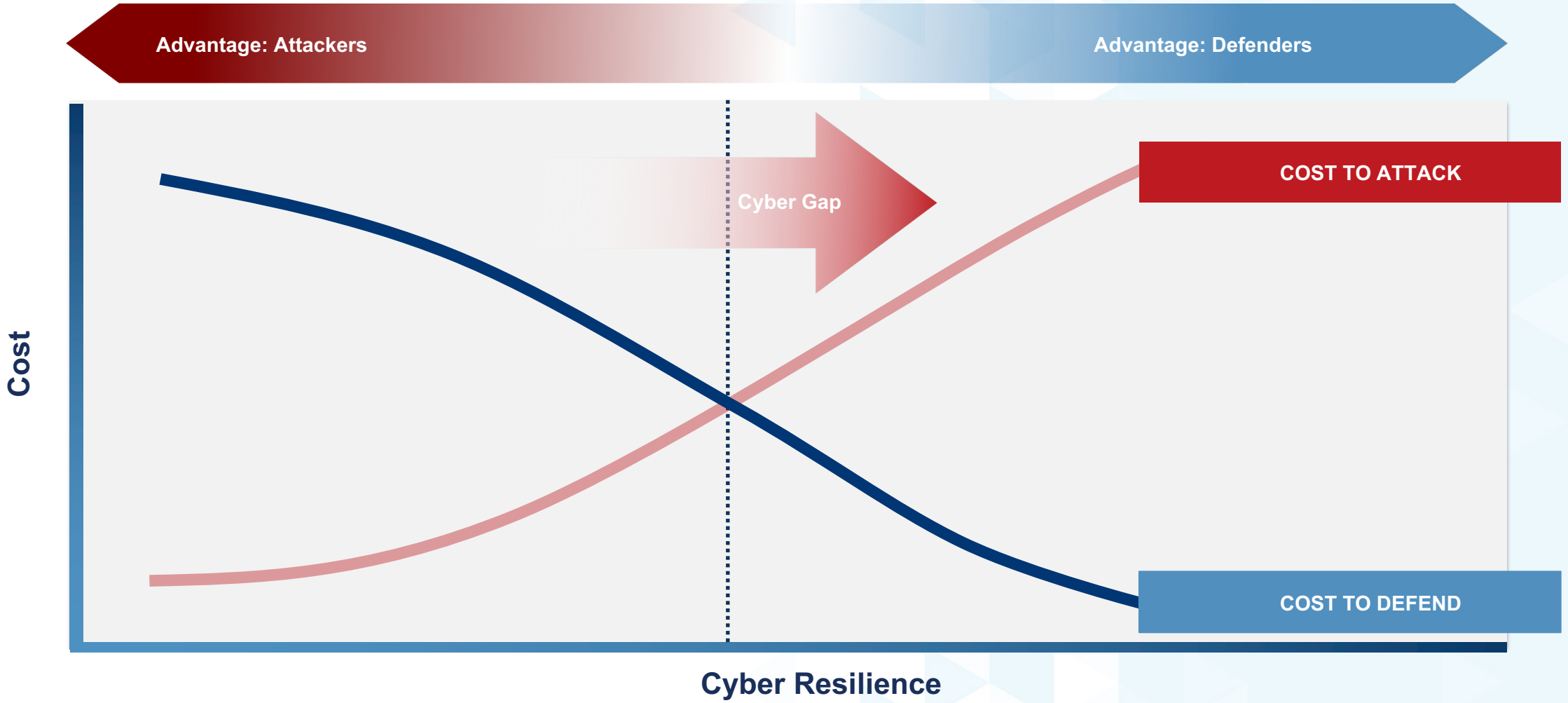
Assets:	Images	Configuration	Identity	Data		
Services:	Secure Boot	Cryptographic Services Encryption, Signing	Policy Controls	Mutual Authentication	Trusted Data Source Identity & Integrity	Functional Safety

Security at Edge - Processing "Chain": Attack Surfaces, Vulnerabilities, Threats . . .

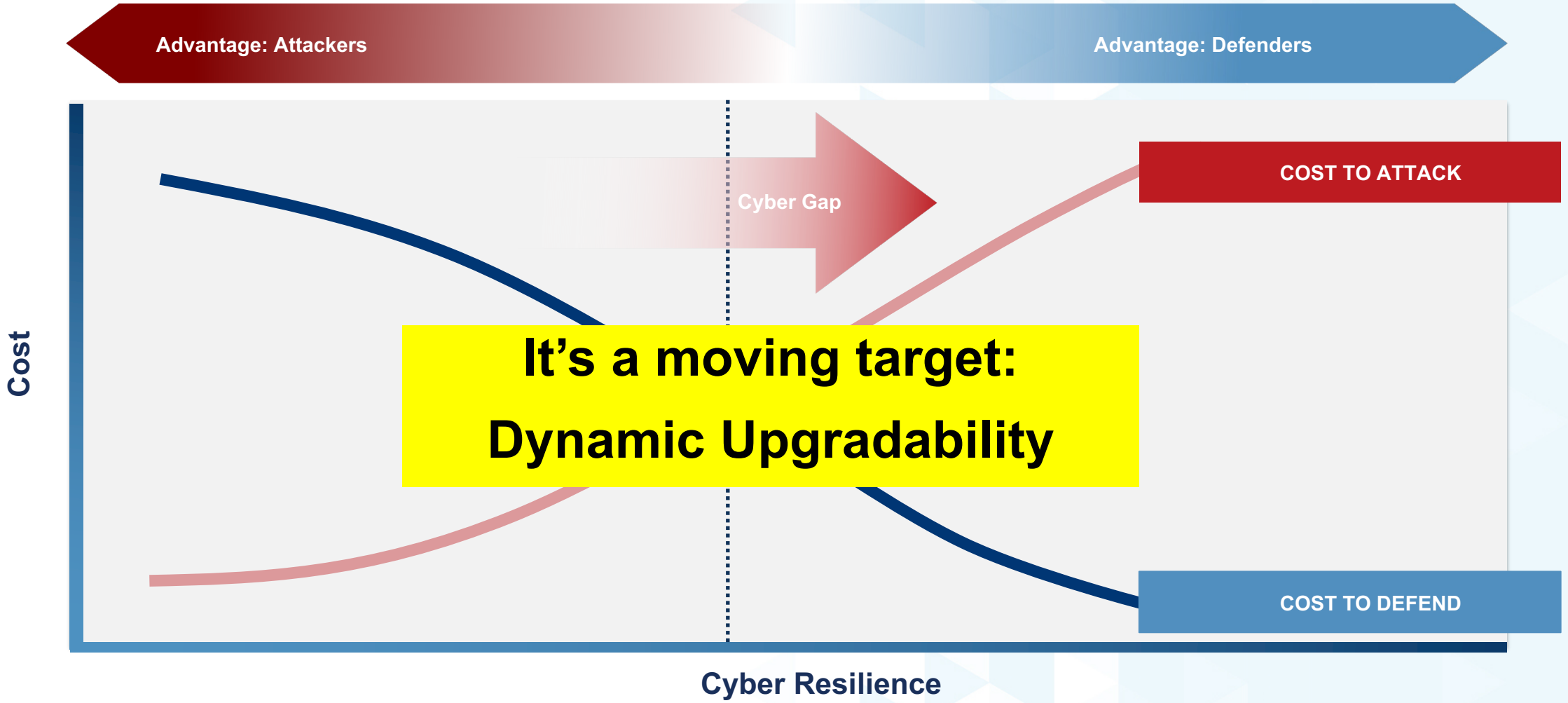


Assets:	Images	Configuration	Identity	Data		
Services:	Secure Boot	Cryptographic Services Encryption, Signing	Policy Controls	Mutual Authentication	Trusted Data Source Identity & Integrity	Functional Safety

Core Goal of Security: Deter, Detect, Derail . . .



Core Goal of Security: Deter, Detect, Derail . . .



Security at the Edge Chaining Trust Up

Secure Data Where it is Born

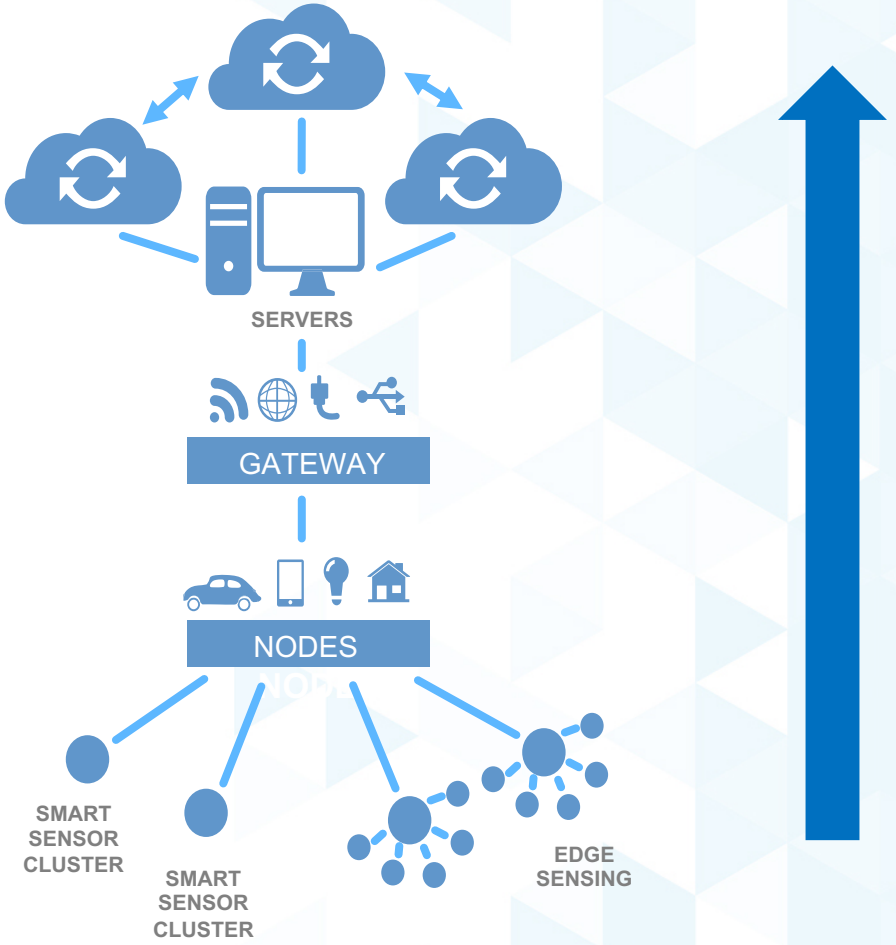
- Analog to Digital

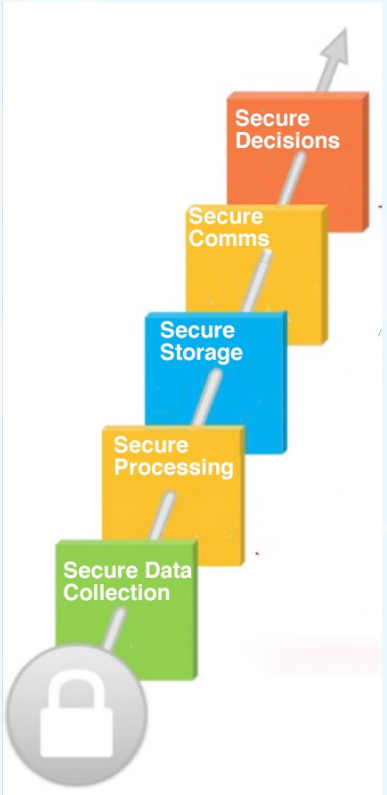
Create Trusted Data with

- Data Source Identity
- Data Integrity Checks

Enhance System Awareness

- Sensing and analytics . . .

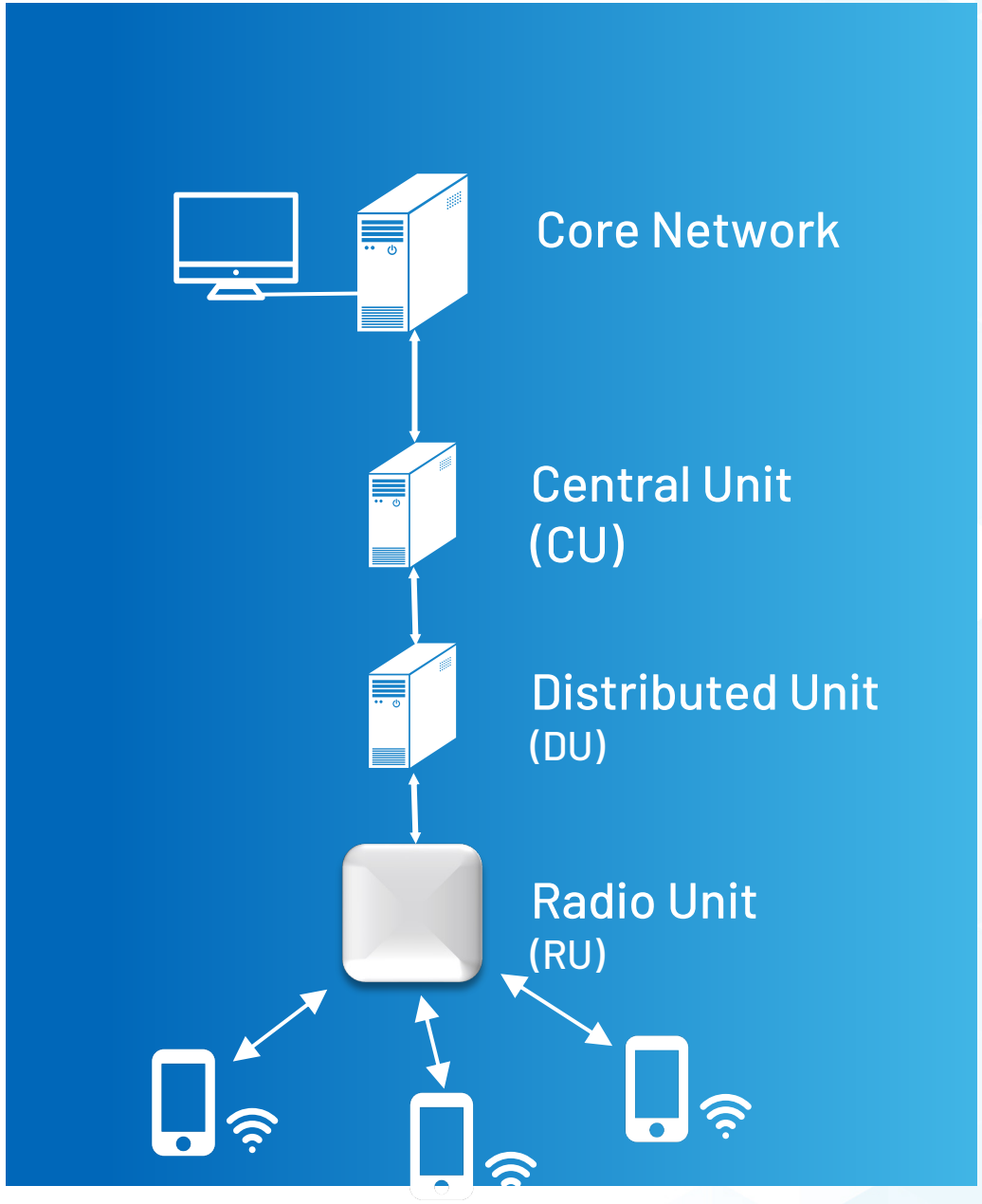




Create Chain of Trust

Case Studies

Open RAN Network Architecture



Case Study 1: Wireless Infrastructure (5G & Open RAN)

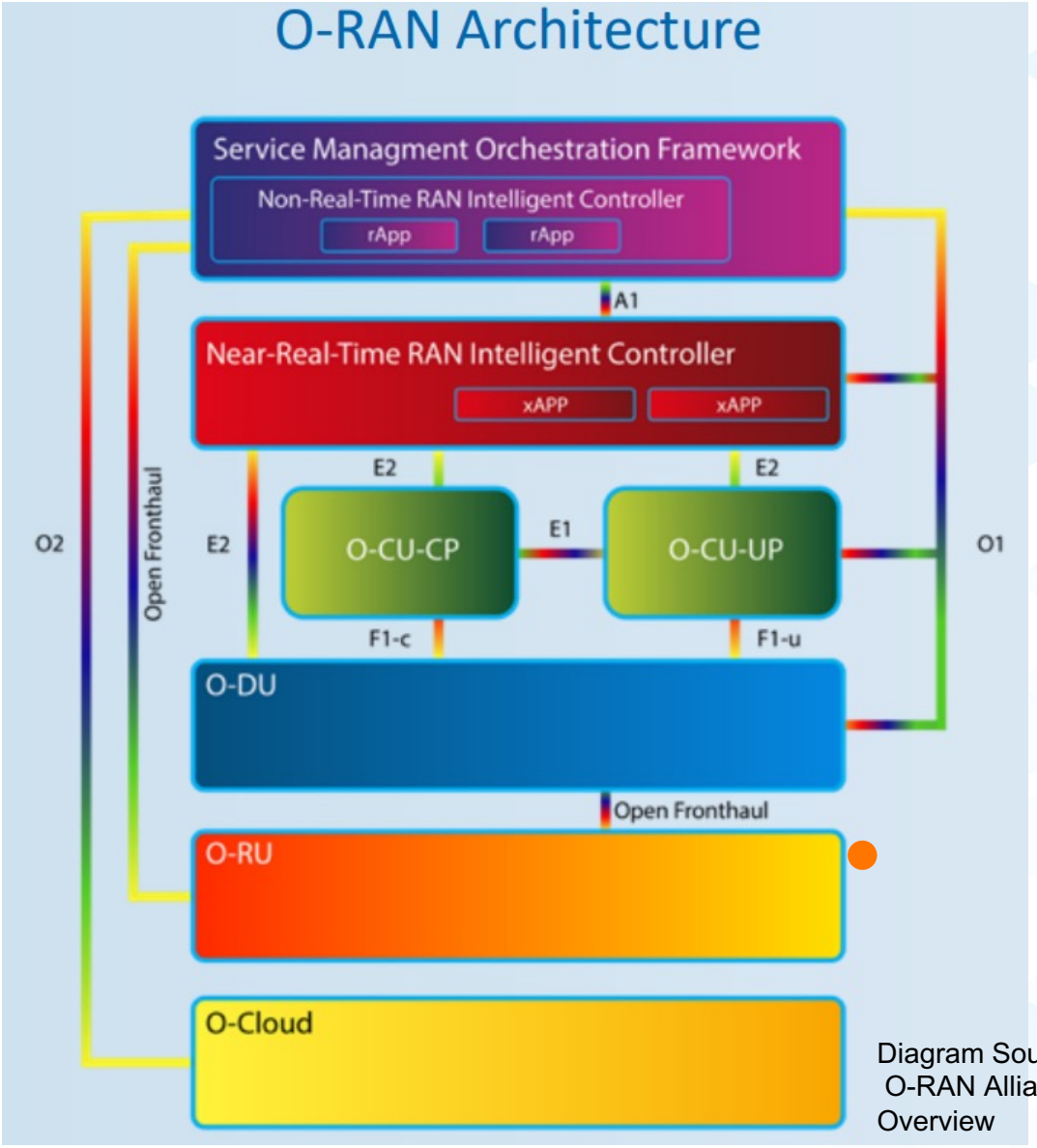
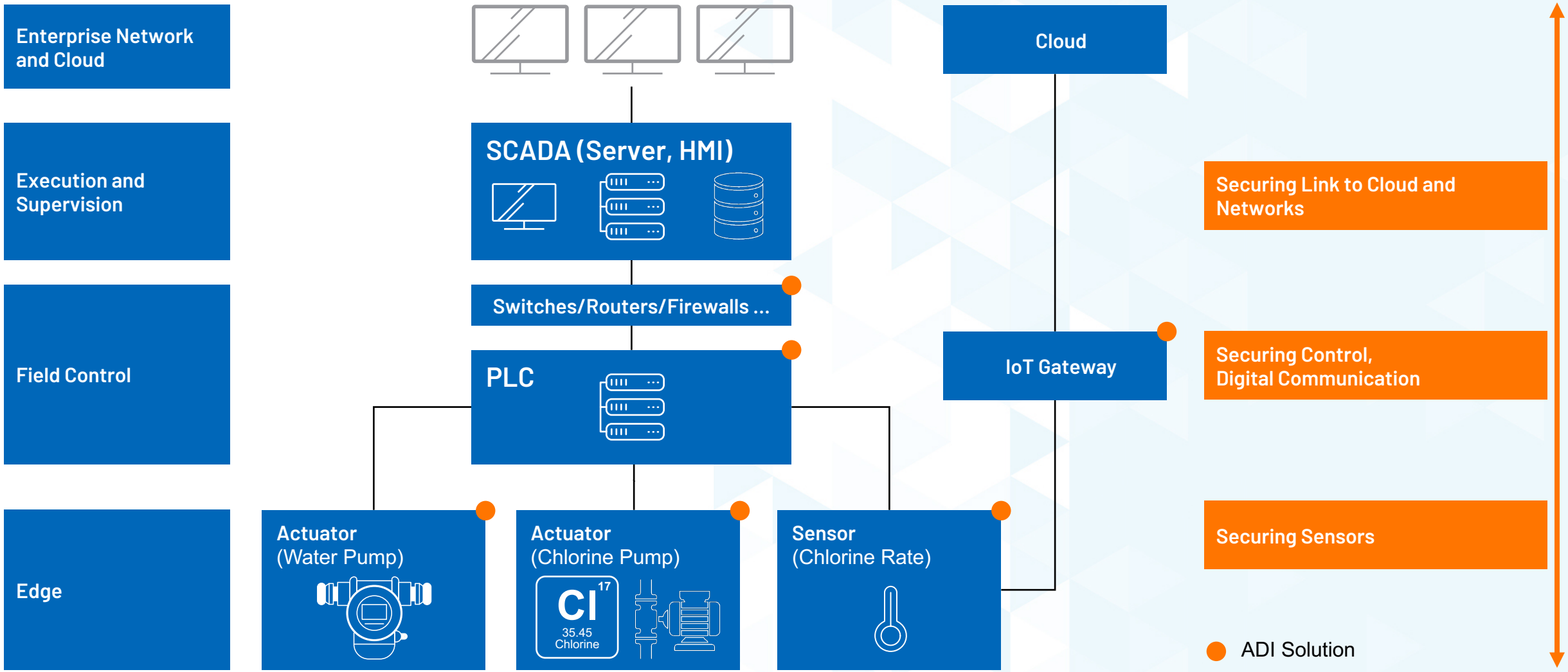


Diagram Source: O-RAN Alliance Overview

- Securing Link to Cloud and Networks
- Securing Ethernet Communications Links to O-RU
- Securing Digital Processing
- Securing Analog RF Tx/Rx

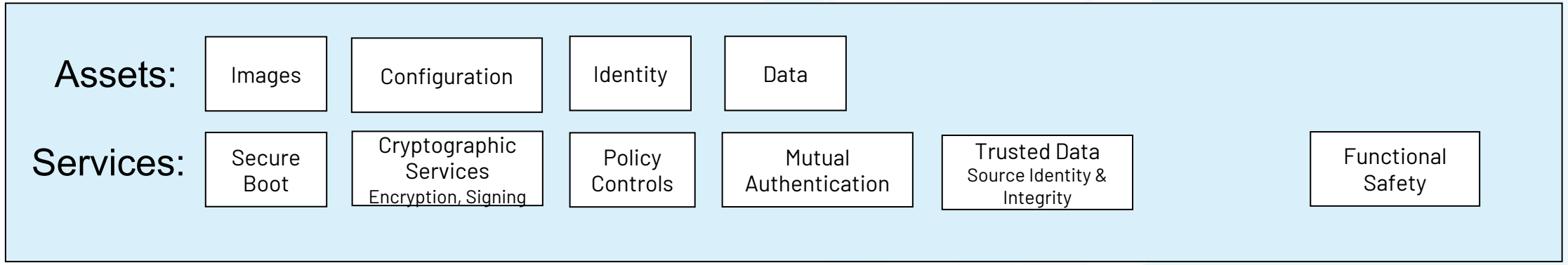
● ADI Solution

Case Study 2: Industrial Automation and Control System Nodes



Tool Box for “Securing the Edge”

- **Power efficient edge processors (including security functional like secure boot)**
- **Secure identity engines (PUF .. .)**
- **Multiple sensor modalities (and sensor fusion processing)**
  - **Consider Functional Safety mindset: early/active fault/tamper detection**
- **Network management functionality**



Conclusion

- The EDGE (sensor interface to the “real world”) is the origin of much of data we are gathering and presents a diverse set of security challenges
- Interception of data is not the only threat: spoofing can corrupt data sets, and Edge nodes can be weaponized
- As a principle of “root of trust” and “chain of trust”: establish trust/identity at the origin of the data
- Provide intelligence in the edge device: “All-knowing cloud, dumb edge devices” is a dangerous model . . . SWAP-C a particular challenge at the edge
- There are opportunities to use analytic techniques to detect/counter a number of potential threats, these include “side channel defenses”

Security to support the analytics . . . Analytics to support security