Practical Deployment of MACsec in Automotive Networks: Real-World Challenges and Insights

Jessica Mann, PE

John Simon, Intrepid Control Systems

IEEE SA STANDARDS ASSOCIATION

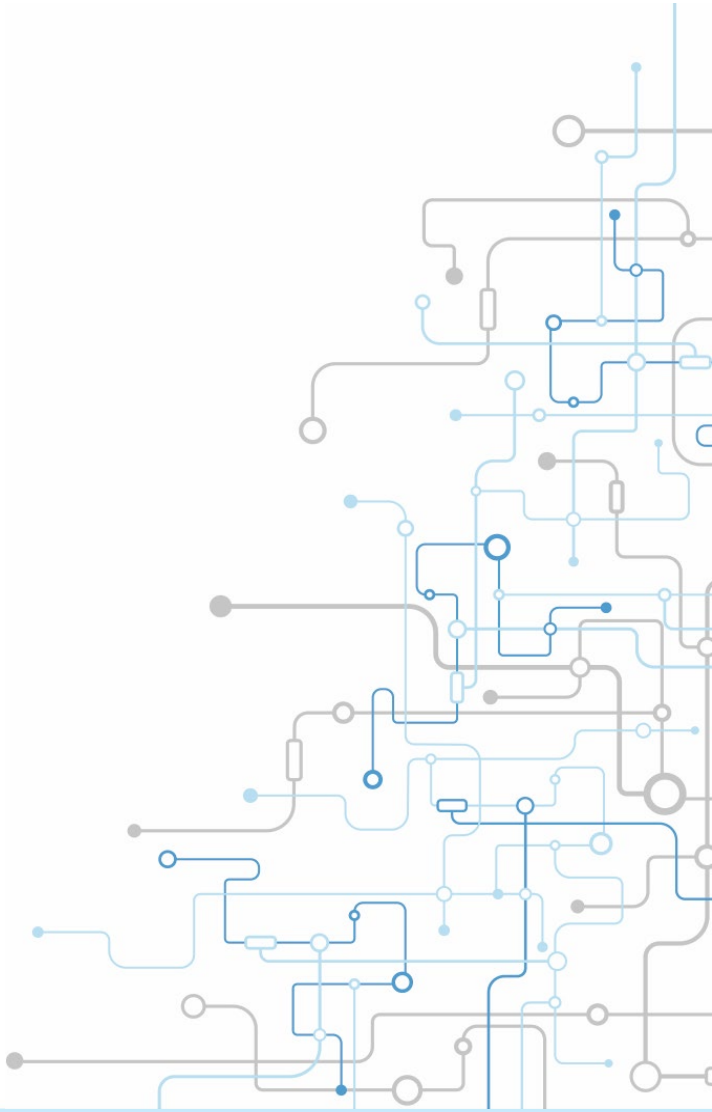
2024 ETHERNET & IP @ AUTOMOTIVE TECHNOLOGY DAY

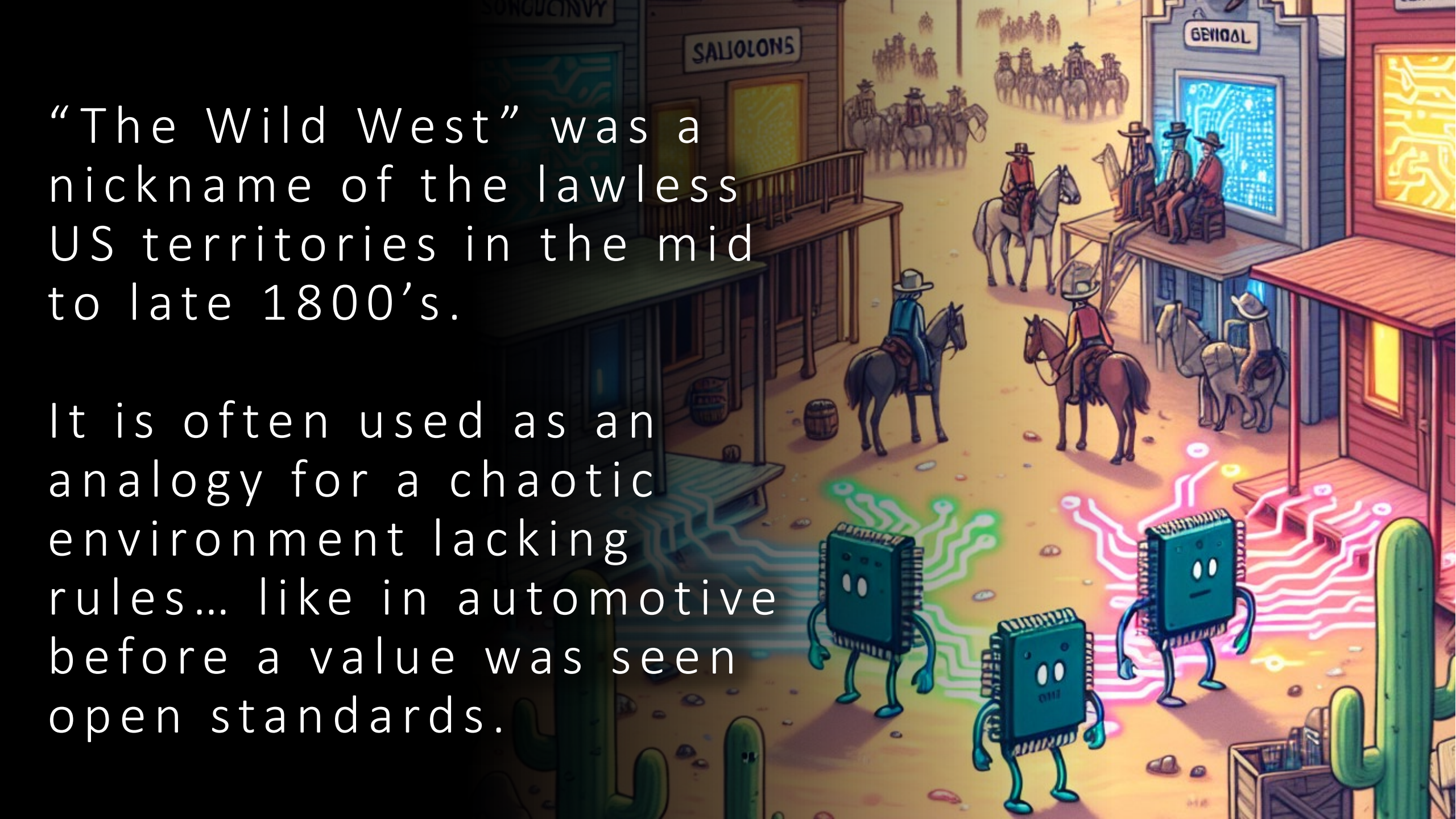
16-17 October 2024 | Detroit, Michigan USA

INTREPID CONTROL SYSTEMS
www.intrepidcs.com

Agenda

- Introduction
- Objectives of TC17
- MACsec/MKA Deployment
- Practical Test Scenarios
- Takeaways and Discussion





"The Wild West" was a nickname of the lawless US territories in the mid to late 1800's.

It is often used as an analogy for a chaotic environment lacking rules… like in automotive before a value was seen open standards.

Standards impose rules, but do not necessarily bring order to chaos.

Successfully deploying MACsec in Automotive networks goes well beyond IEEE 802.1AE and IEEE 802.1X.

OPEN TC17 is determining how IEEE 802.1AE and 802.1X can be applied to meet automotive requirements.

But in the meantime…

Product Developers Grow Anxious

As time passes, questions mount

- Implementation
  - How are MACsec and MKA sourced?
  - How do I integrate MKA software to the MACsec hardware?
  - Is there a standard API?
- Secret Keys
  - How do we store keys securely?
  - How can keys be updated?
  - At what point should keys be considered secret?
  - Best practices for key distribution?
- Are there legal requirements for vehicle service or right to repair?
- Integration/Testing
  - How is startup time validated?
  - Can I test without MKA?
  - How do I test MKA?
  - What selectable configurations do we need evaluate?

So many questions…

- ***Are the all valid?***
- ***Which concern me?***
- ***Is TC17 going to answer them all?***


"What does TC17 offer, and how do we implement it effectively?"

What are the Open Alliance's TC17 objectives?

- The industry desires interoperable Ethernet security.
- TC17 established to create an automotive profile for MACsec that could be adopted by all OEMs.
- Aims to align IEEE 802.1AE (MACsec) and IEEE 802.1X (MKA) with Automotive requirements
- Activity in three TC17 subgroups
  - TC17 802.1AE Automotive Profile
  - MKA Key Management
  - 10BASE-T1S
- Automotive MKA proposal released by October 2024!

Current planned TC17 validation test specifications

Group 1	Group 2	Group 3	Group 4	Group 5	Group 6
Packet Level	Protocol Level	Interoperability Level	Performance Level	Security Level	Diagnostic Session Level

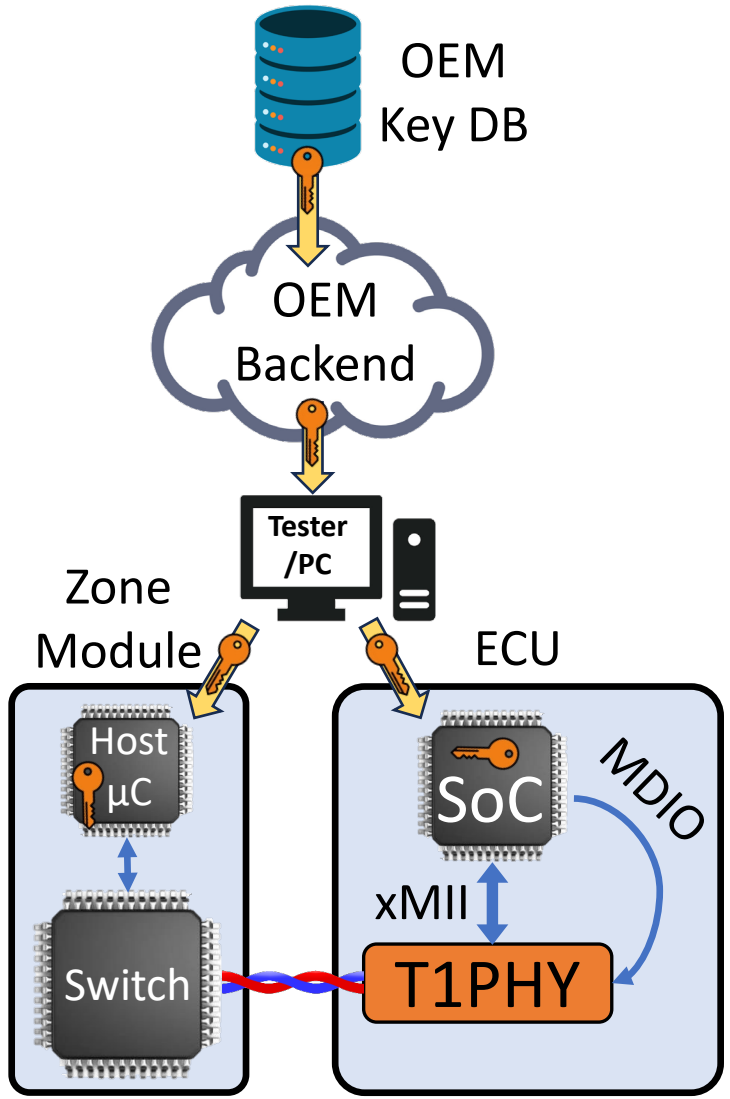
- TC17 planning for six groups of test categories which are being developed as part of the test specification.
- Create a realization of converting a test specification into practical test use cases.
- Addresses interoperability and conformance.
- Does not tell OEMs how to test their systems over car lifetime.

Out of Scope for TC17

TC17 does not specify

- How to distribute keys to ECUs.
  - OEMs have different ways to distribute keys within the Vehicle ECUs from their secure key servers (e.g., SecOC CAN ECUs).
  - Part of key distribution can be done at Tier 1 and part at Vehicle manufacturing facility.
- Testing of Secret Key distribution or installation
- How to integrate MACsec into the product development process
- Service Considerations

Once the Keys have been installed into ECUs, it is from that point TC17's MKA proposal applies with a fixed CAK at a MKA server and client.

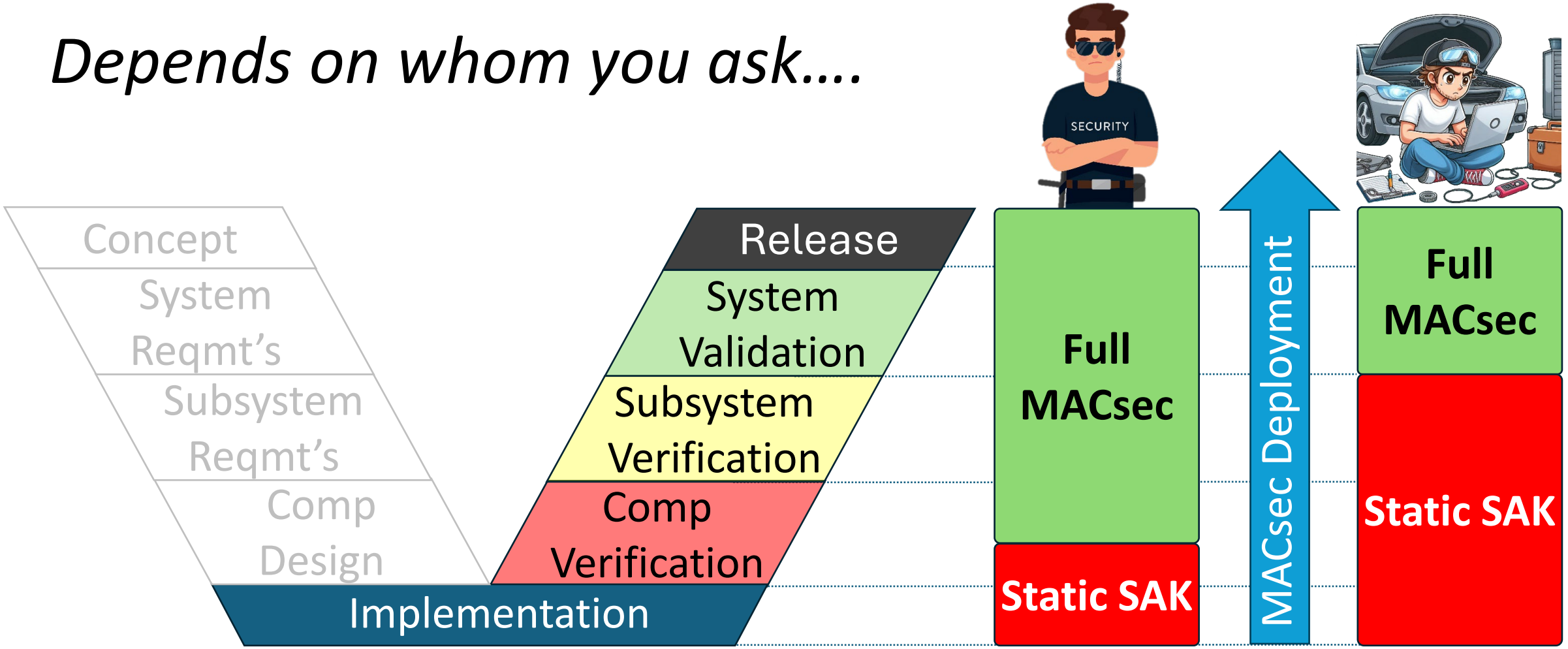


MACsec/MKA Ecosystem in a Vehicle

Deployment Strategy

Ideal MACsec deployment strategy?

Depends on whom you ask….

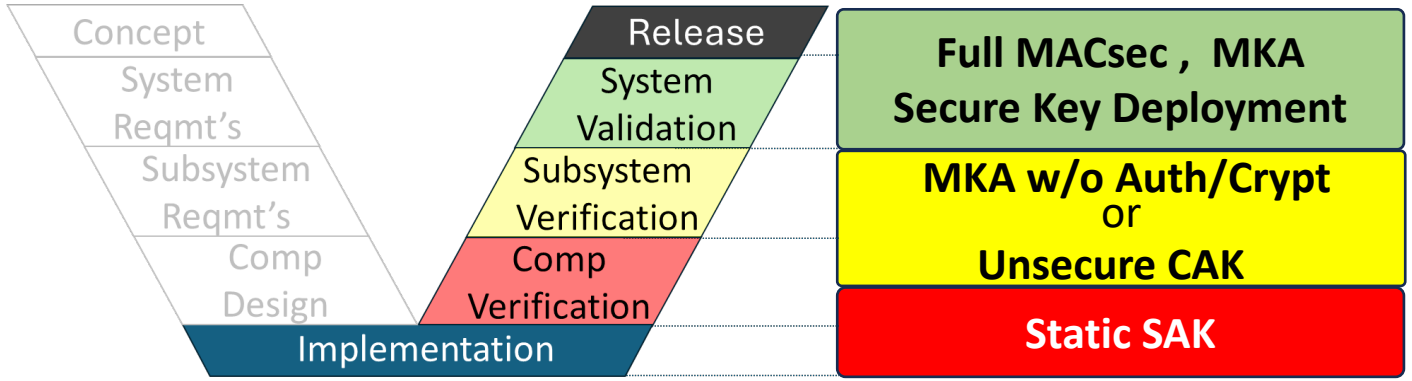


Full MACsec = MACsec + MKA + Production Intent Deployment of Secure CAK

“Big Bang” is rarely a plan for success

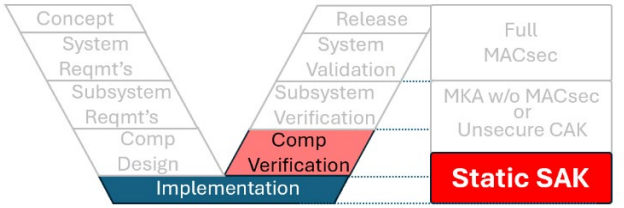
Incremental deployment

- Static SAK
- MACsec/MKA w/o Auth/Crypt
- MACsec/MKA
  - Unsecure CAK
  - Secured CAK
  - Secured deployment

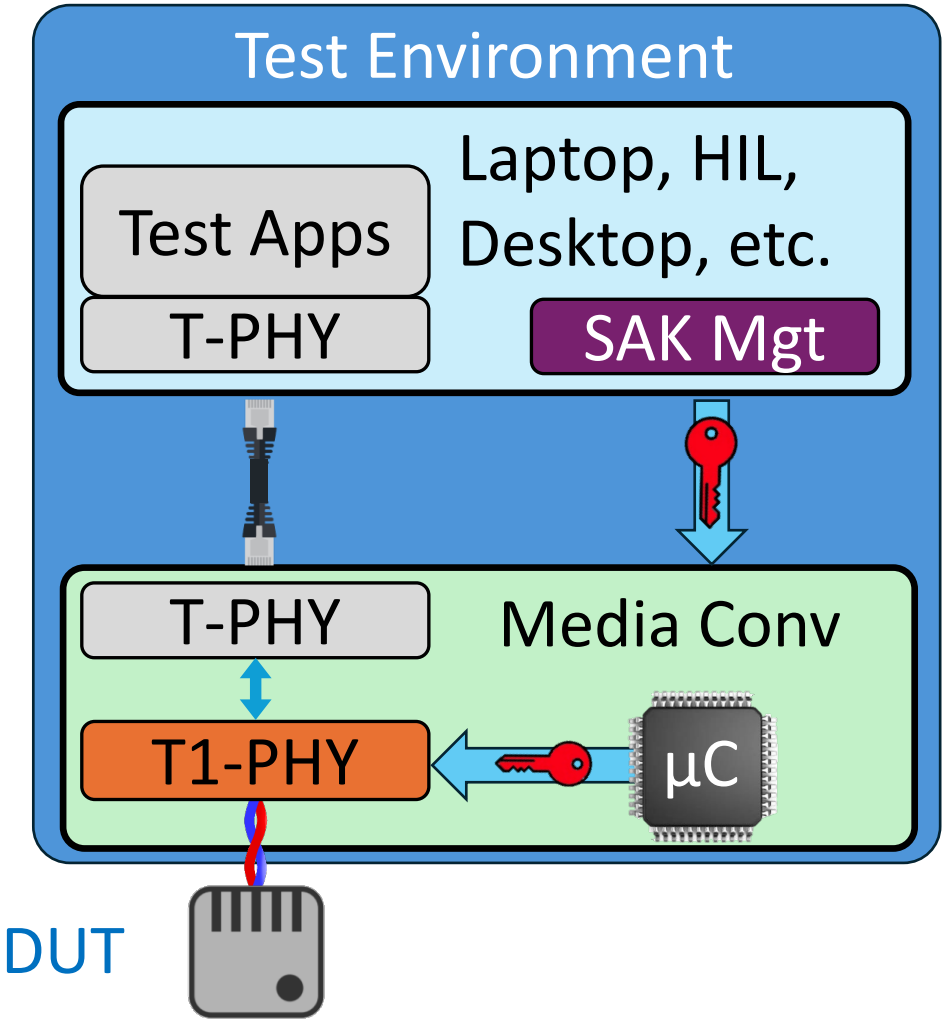


Different tool requirements at each stage

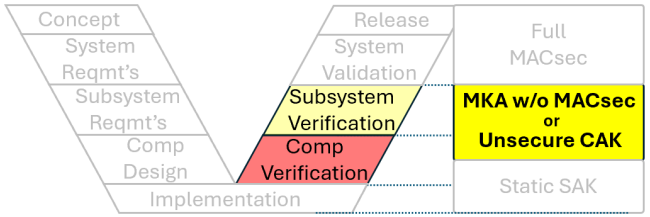
Early Development



- Insert projected MACsec/MKA startup time
  - Interoperability
  - PHY configuration interface
  - Test PHY configurations
- Tool options
  - MACsec in PHY
  - MACsec in software
    - Introduced to Linux in 2016
    - Use older media converters
    - Performance limited



MKA/MACsec without Authentication/Crypt

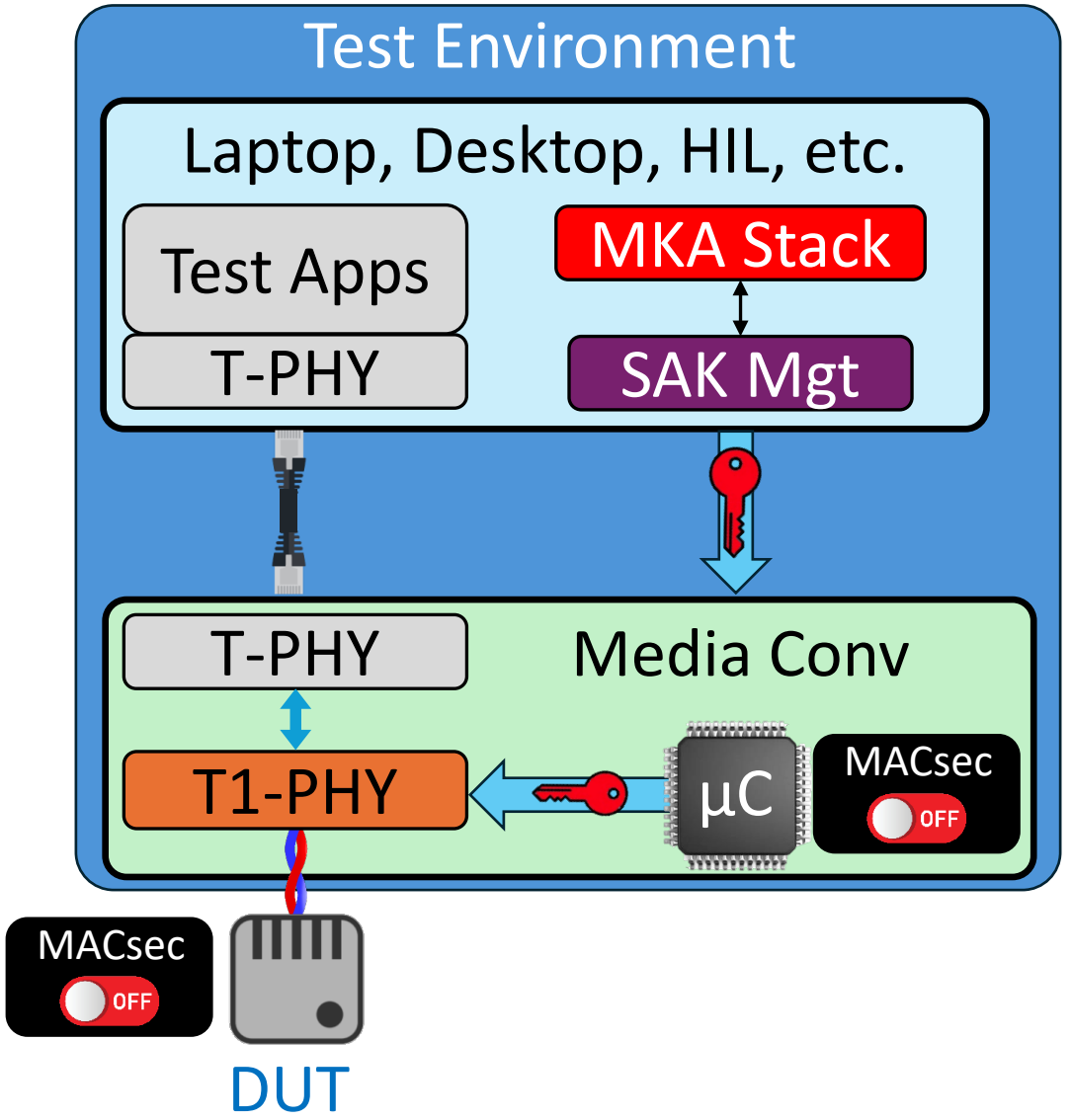


Pros

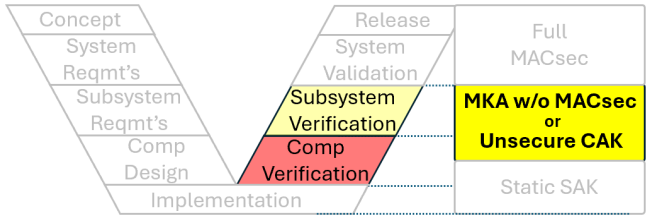
- MKA exchange latencies present
- Widespread MKA testing
- Minimal impact to product dev

Cons

- Not testing full implementation
  - Key installation/rotation
  - Replay Attack mechanism
  - PHY MACsec IP
- Potential attack surface?



Default (Unsecure) CAKs



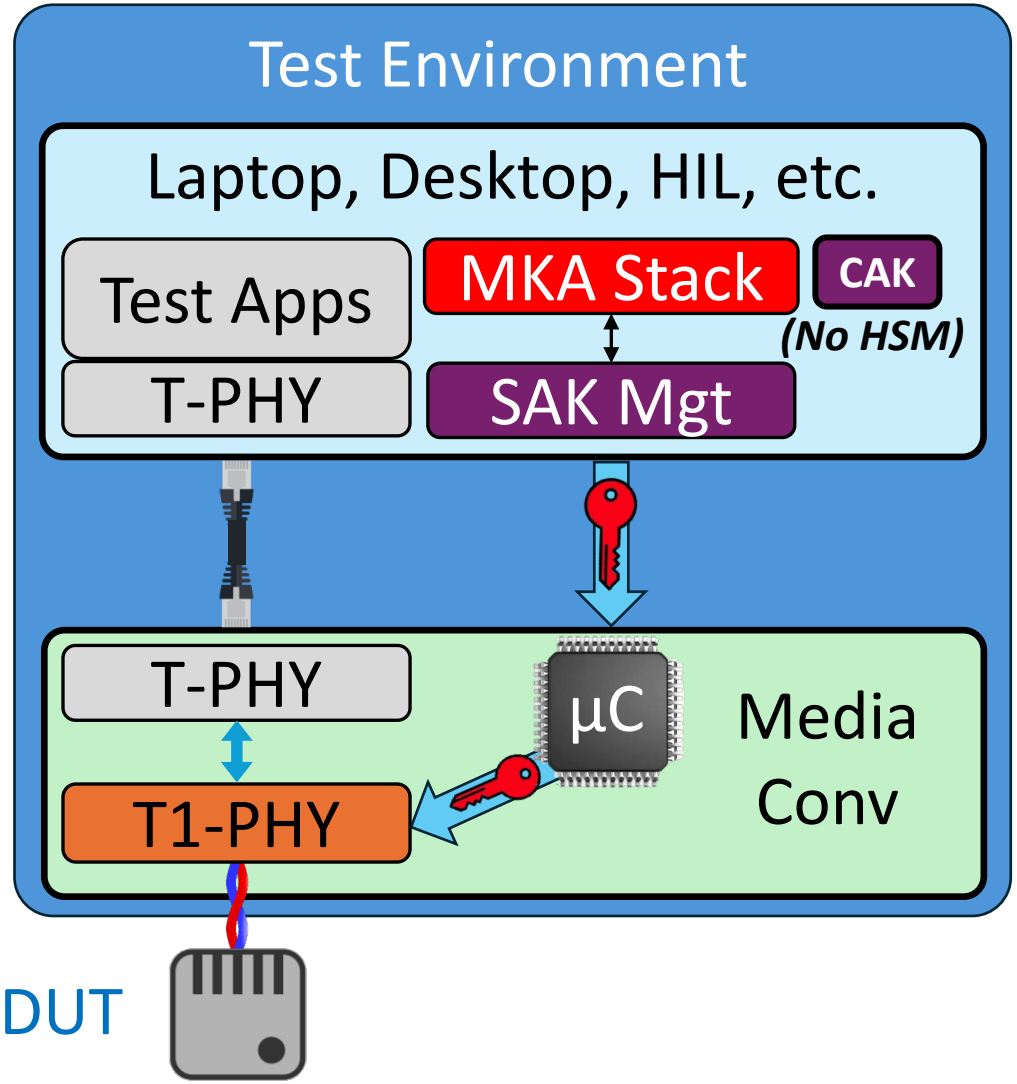
Pros

- CAK deployment is not complicated
- Minimal impact to development
- MKA latencies present

Cons

- Does not exercise secure deployment of keys
- Does not test secure key installation
- Unencrypted SAK exposed

(Dramatic Foreshadowing)



INTREPID CONTROL SYSTEMS

Tools after CAKs are locked down?

- Secure CAK deployment and installation
- Tool needs for secure CAK?
  - Pre-production
  - Post-production
  - In the field
  - Right to repair
- Managing Vulnerabilities?
  - Disable MACsec
  - Deploy new CAK
  - Securely retrieve CAKs
  - Tools with secured CAKs

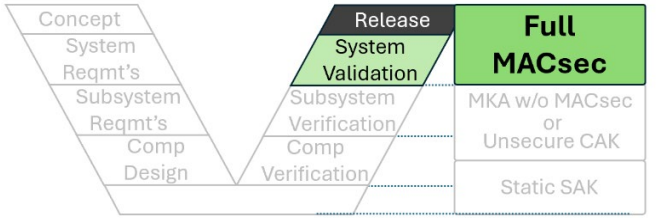
Impact to tool requirements?

Unacceptable Risk

Unacceptable Complexity

Acceptable Costs?

Tool CAK Deployment via Secure Server

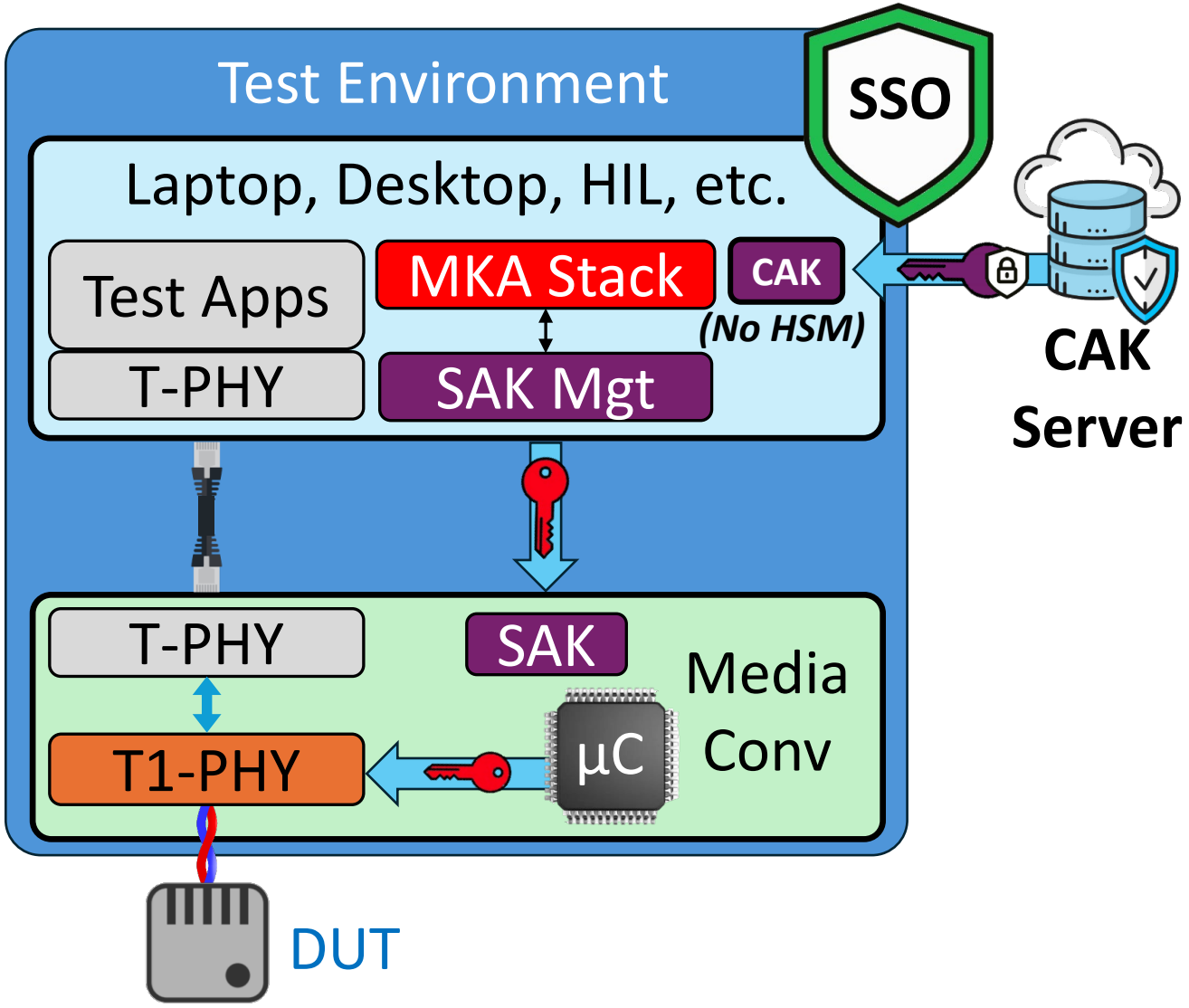


Pros

- SSO managed access
- Existing infrastructure?

Cons

- Vulnerable in RAM
- Cannot be stored locally between uses
- Persistent network connection
- Requires IT integration with each series of tools



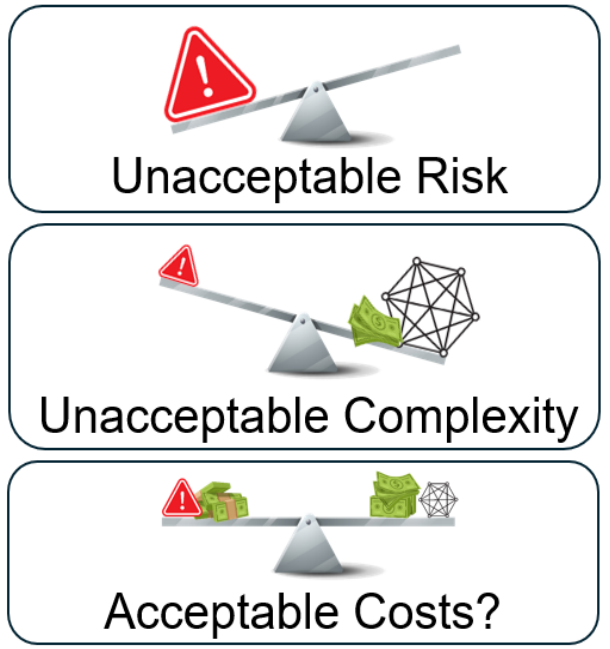
Alternatives to a CAK server?

Goals

- Secure/Persistent Key(s)
- No persistent network connection
- Common key deployment

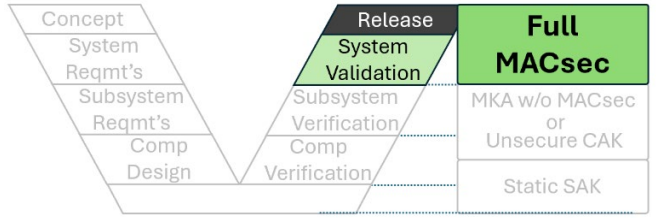
Requirement

- Prevent unauthorized use of CAK

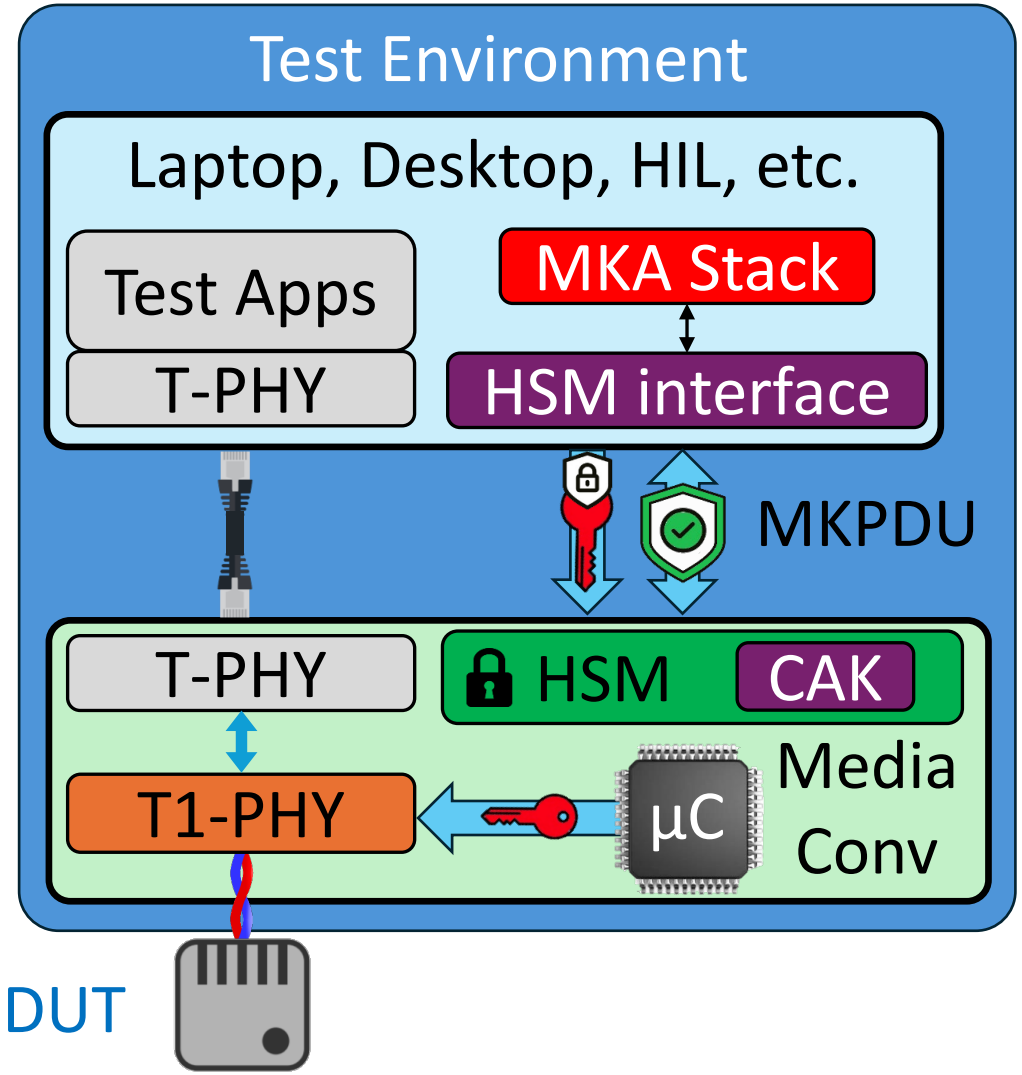


Ideas worth consideration?

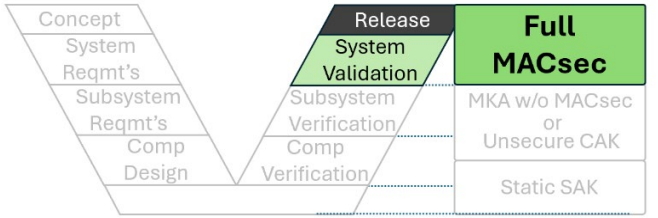
Media Conv / Offboard HSM



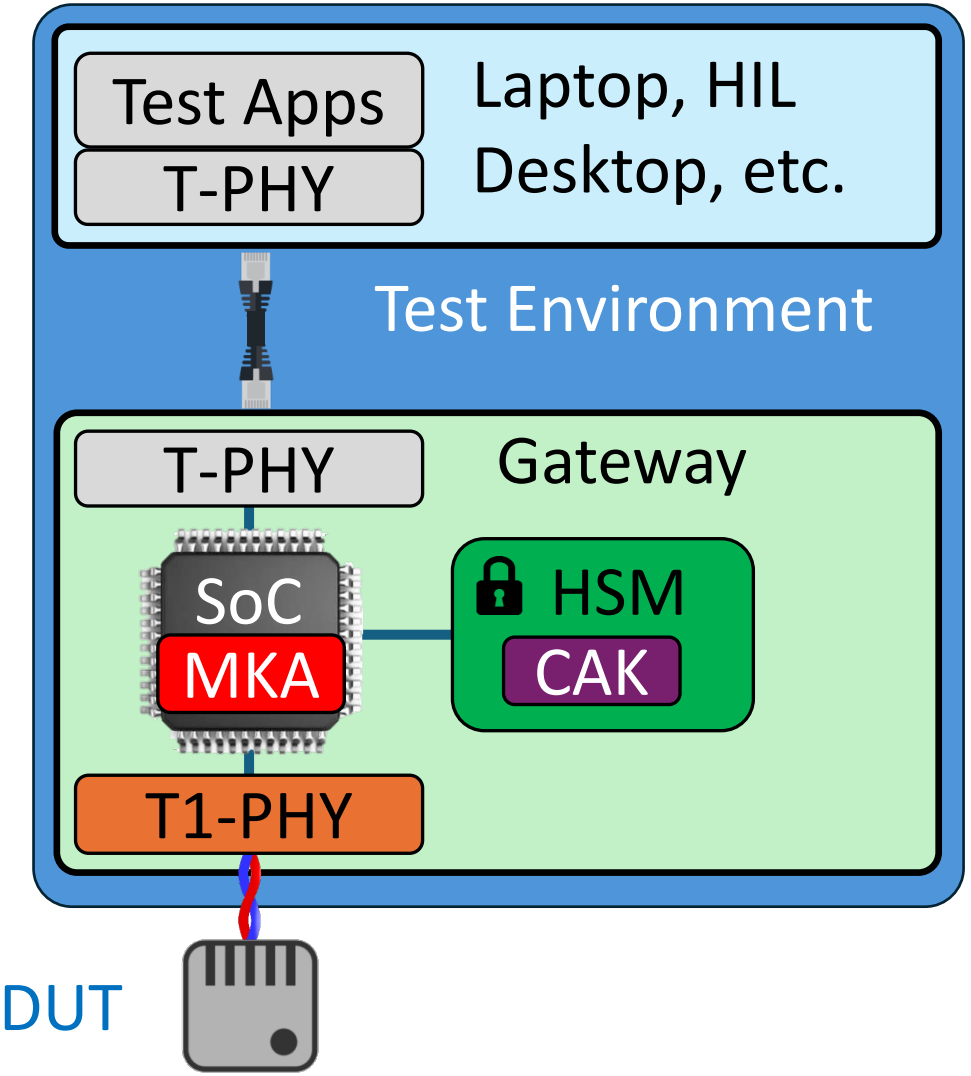
- Secure CAK storage
  - USB Device?
  - Integral to media converter?
- HSM Interface to MKA
  - Authenticate MKA frames
  - Pass encrypted SAK
  - CAK protected in HSM Hardware
  - CAK not available in RAM
- User/PC authentication prevents unauthorized use

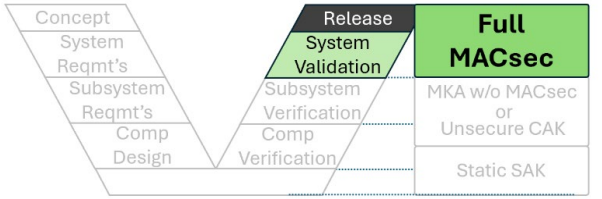


Gateway w/ embedded MKA



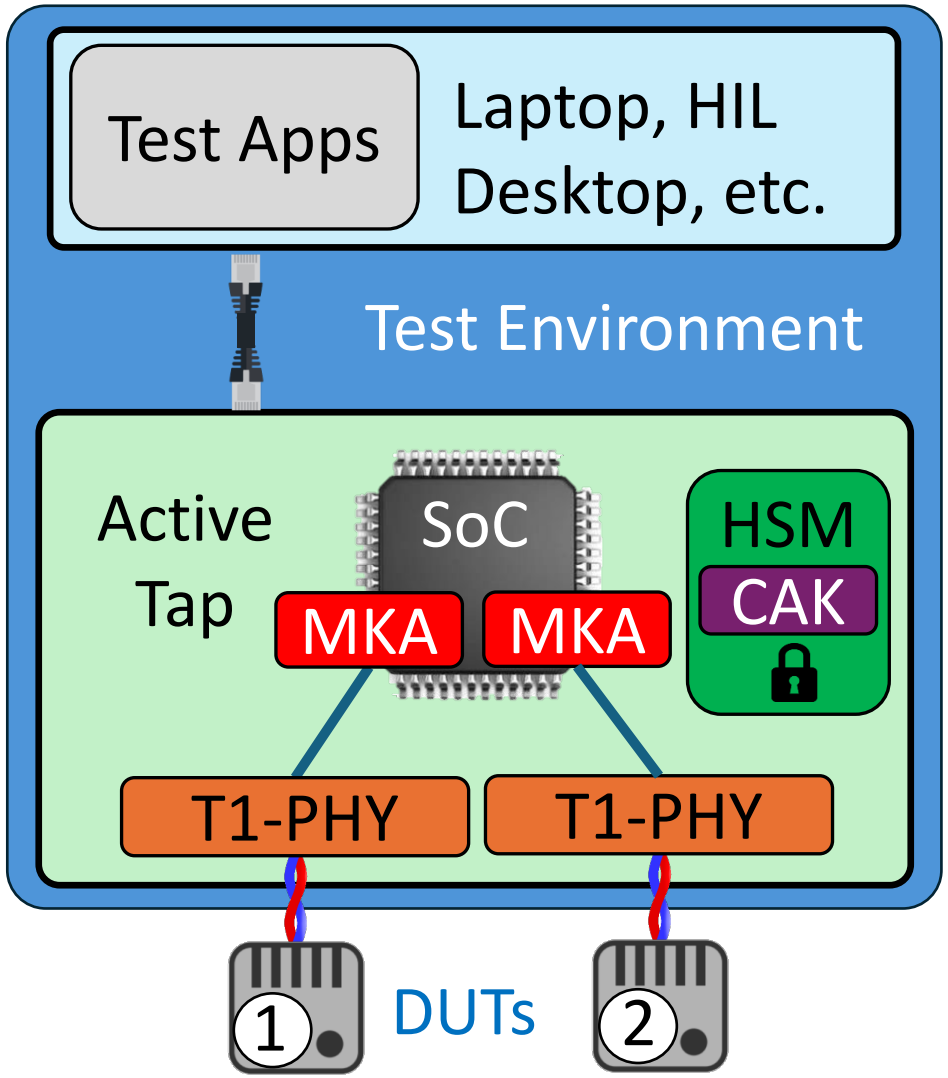
- For use with legacy hardware w/o MACsec or MKA stack
- BASE-T PHY link disabled until successful MKA key exchange
- Tool authentication with PC can prevent unauthorized use
- Possible Variants
  - Switch vs. SoC
  - No HSM





Active Tap with MKA

- *Taps don't necessarily need MACsec (let alone MKA)*
  - Encryption is not used
  - No TX requirements
  - Authentication not important
- Use cases requiring MKA
  - Man-in-the-middle
    - Fault testing / Inject traffic
    - Debugging MACsec
  - Parallel DUT testing



INTREPID CONTROL SYSTEMS

Takeaways and Discussion

Does <a tool> "Support TC17"?

If the engineers working with MACsec cannot define "Support", can we do it for them?

- Tool purpose?
  - Transparent MACSEC
  - Test/Debug MACSEC and MKA startup
- Standard PHY Interface? (SecY, SAK, rules, etc.)
- MKA – Embedded stack?
- Key storage
  - Secure Storage?
  - How many?

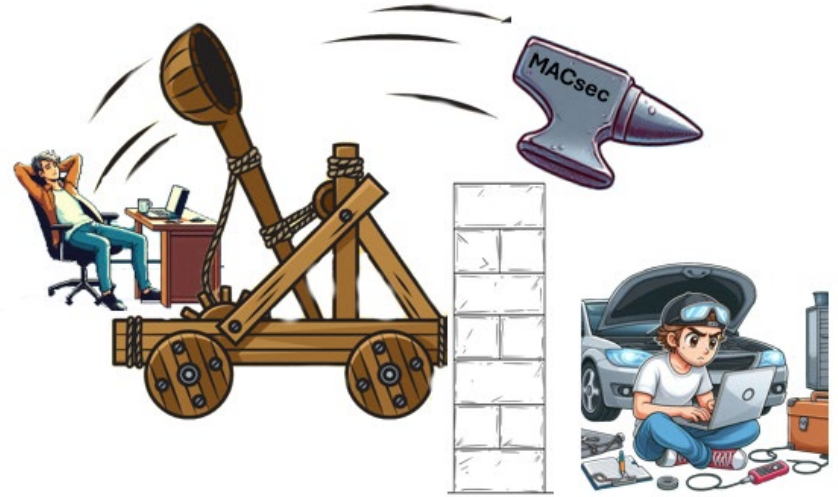
Is there a need for tool profiles or standardized interfaces?

INTREPID CONTROL SYSTEMS

For the Benefit of Product Developers

Close the knowledge gap between the spec authors and product developers.

- MACsec Training? *(Top down for the masses)*
- Understand the deliverables of TC17
  - Standard configs, APIs, Test
- Comprehend ***what is not specified*** by TC17
- Plan for MACsec and MKA deployment
  - Phased Deployment
  - Training / Best Practices
  - Tools Development



Ease of Service?

"Replace an ECU as easily as replacing a tire?"

- Is this a realistic goal?
- Significant Motivation
  - Cost
  - Car culture / Right to repair
  - Historical vehicles
- But what about…
  - Safety
  - Security

Uniformity in service might help

- Retrieve/Install Keys?
- Replace Keys?
- Rebuilding connectivity associations? (pairing)

If the risk universally shared, why not share the cost to balance risk/complexity?

Questions?

Jessica Mann
Professional Engineer
https://www.linkedin.com/in/jessicalmannpe/

John Simon
Product & Applications Manager
Intrepid Control Systems
jsimon@intrepidcs.com

IEEE SA STANDARDS ASSOCIATION

2024 ETHERNET & IP @ AUTOMOTIVE TECHNOLOGY DAY

16-17 October 2024 | Detroit, Michigan USA