

Collaborative Defense: OEM and Researcher Perspectives on Truck Cybersecurity



Robert Zimmerman
Manager of Autonomous
Vehicle Cybersecurity,
Daimler



Jaime Lightfoot
Cybersecurity Researcher,
Lightfoot Labs



Ben Gardiner
Senior Cybersecurity
Research Engineer, NMFTA

What is ATG?

Autonomous Technology Group



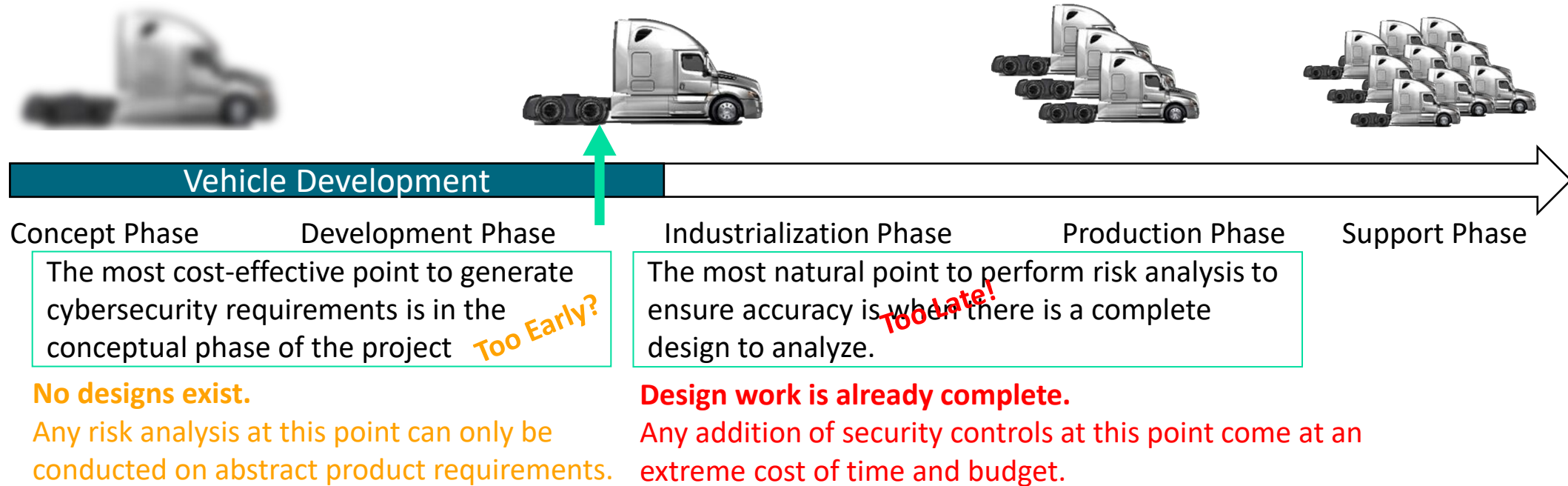
ATG is a specialized team within Daimler Truck singularly focused on bringing an SAE Level 4, class 8 truck to full scale production.

Our Core Product: Autonomous-driver agnostic, redundant vehicle platform

Our Imperative: The vehicle platform sets the bar for industry safety and security standards

Secure Design to Build

Goal: Produce the most secure truck possible within the time/budget available



No, it's not too early! We conduct abstract functional risk analysis to realize secure by design

Collaborative Defense: OEM and Researcher Perspectives on Truck Cybersecurity



Robert Zimmerman
Manager of Autonomous
Vehicle Cybersecurity,
Daimler



Jaime Lightfoot
Cybersecurity Researcher,
Lightfoot Labs



Ben Gardiner
Senior Cybersecurity
Research Engineer, NMFTA

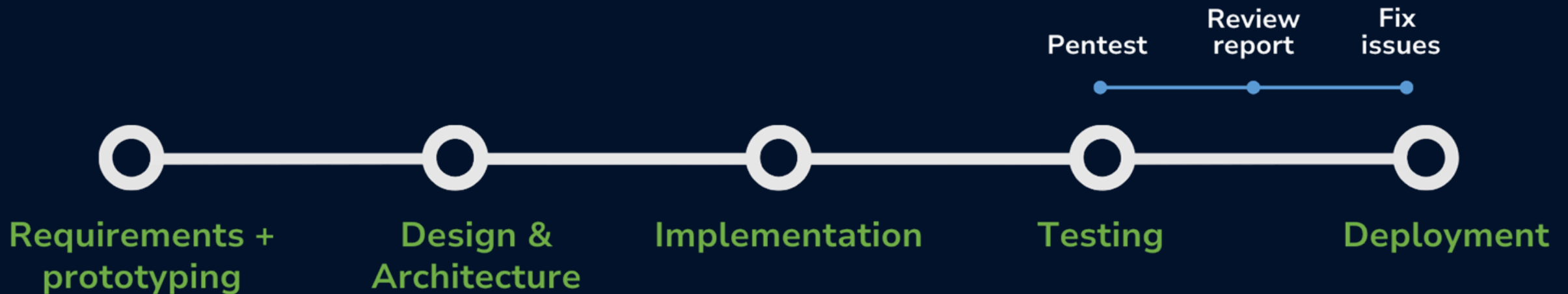
How Security Testing Fits into Product Design



- **Penetration testing** AKA pentesting for short

Pentesting Overview

1. **Test the device**: try to hack into it, gain access/information as though you're a (malicious) hacker
2. **Report the issues**: Write up all issues with mitigations
3. **Fix the gaps**: work with engineers to fix the discovered issues



Pentesting: “Who”

- **Parties involved:**

- Manufacturer or vendor with a product or service to secure
- Pentester or pentesting company

- **Legal agreement granting pentester permission to test**

- Scope and timeframe decided in advance
- *Not* a random tester you’ve never met before (that’s bug bounty)
- *Not* someone extorting the company (that’s a crime)

Pentesting: “What”

- **Device under test**

- ELD, telematics unit, ECU, website, cloud, API backend

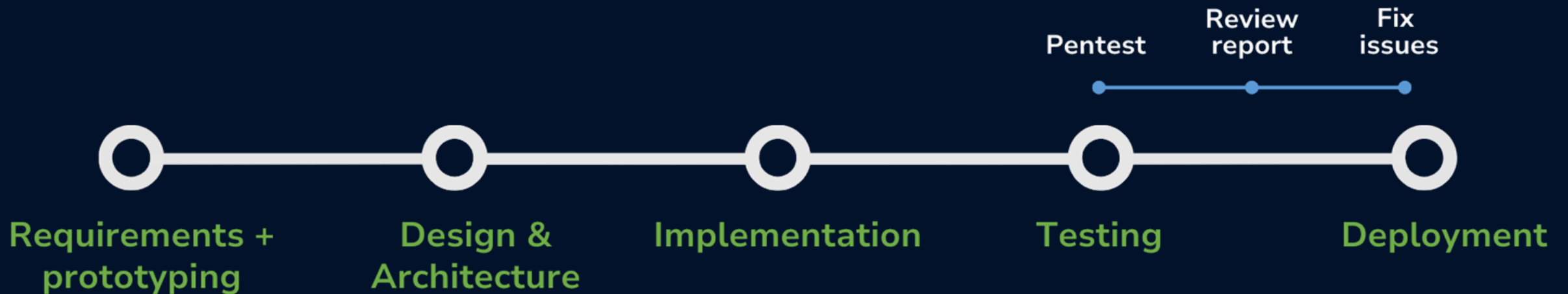
- **Report**

- Discovered issues
- Proof-of-concepts
- Technical + business impact
- Mitigations



Pentesting: “When”

- **Before launch** (but after feature freeze)
- **Retest after launch** if additional features are added
- **Length of testing** depends on product



Pentesting: “Where”

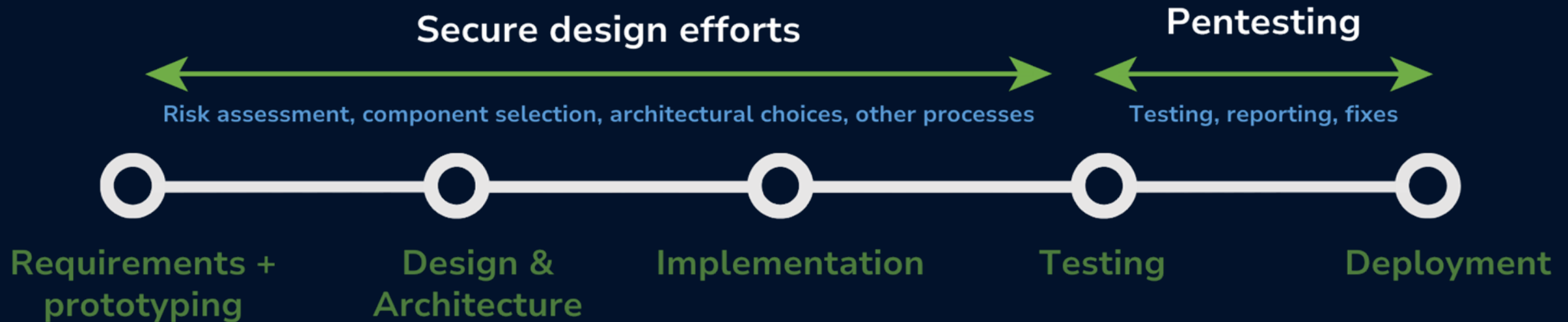
- Often remote, not tested as part of entire truck

Pentesting: “Why”

- **Independent security check** on engineering efforts
- **Protect against risks** as identified by manufacturer
 - **Safety:** ELDs/telematics putting messages on vehicle bus
 - **Integrity:** protecting firmware on ECUs
 - **Confidentiality:** of manufacturer IP, customer data, truck locations
 - **Availability:** denial-of-service attacks

Security Before Pentesting

- **“Shift left”**: starting security efforts earlier helps avoid big last-minute problems found in pentesting



Collaborative Defense: OEM and Researcher Perspectives on Truck Cybersecurity



Robert Zimmerman
Manager of Autonomous
Vehicle Cybersecurity,
Daimler



Jaime Lightfoot
Cybersecurity Researcher,
Lightfoot Labs



Ben Gardiner
Senior Cybersecurity
Research Engineer, NMFTA