IFIP WG 10.4 IVDS Workshop

How to defend connected intelligent vehicles

Transferring established Information Security best practices to the vehicular world

We transform automotive mobility

CARIAD
A VOLKSWAGEN GROUP COMPANY

Agenda

// Who we are
// Our Motivation
// Detecting attacks against vehicles
// Responding to attacks
// Looking forward

0x00

Who we are

We are the newest member of Volkswagen Group.

We love cars.
We love digitalization.

That's why we're combining these two fields in one company.

CARIAD has a clear vision paving the way to achieve our purpose

mobility made easy. for everyone. software driven.

Seamless, convenient, and digital mobility experience enabled through our automotive ecosystem and flagship experiences …

… available to all users and developers in our digital mobility ecosystem …

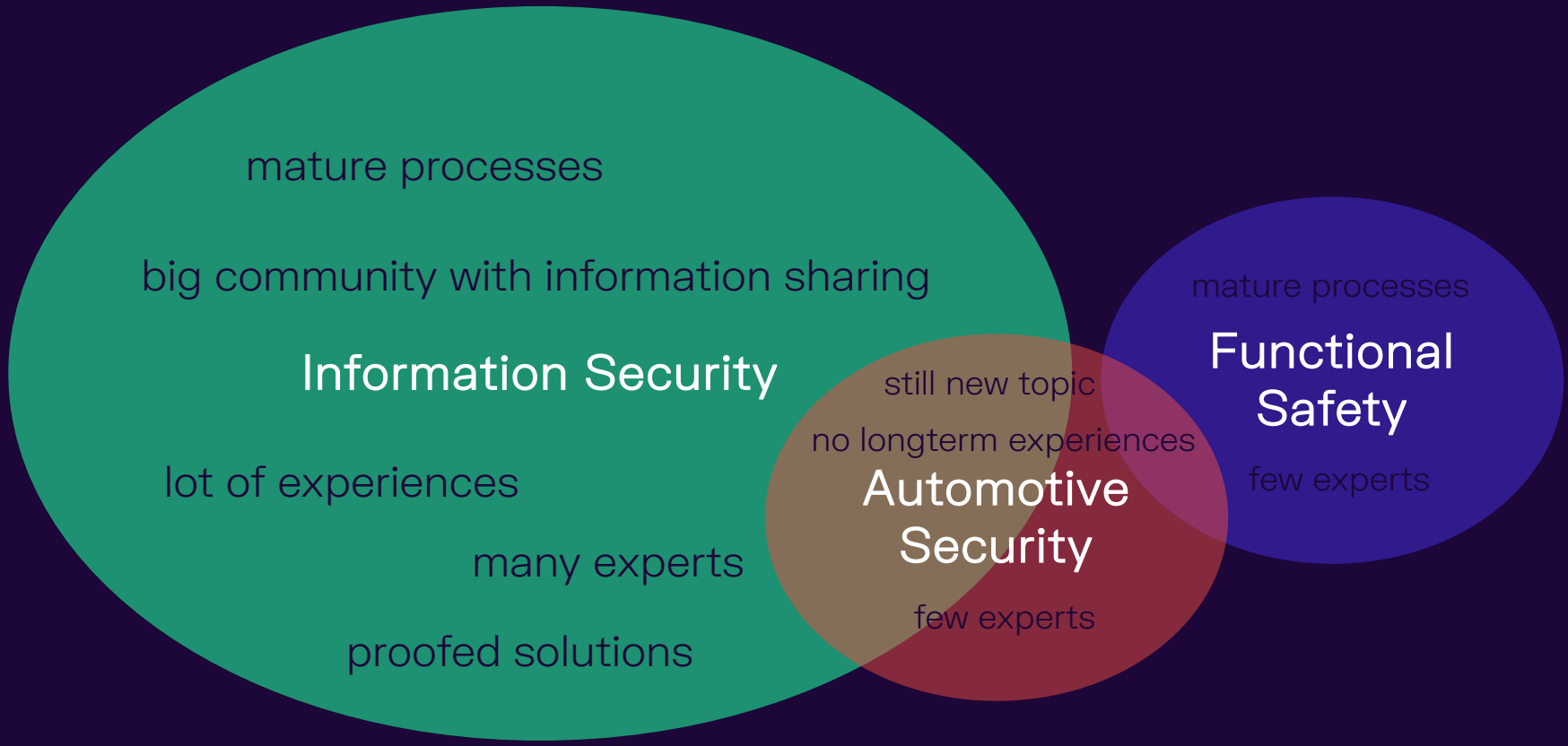
… achieved via one scalable tech platform and game-changing in-house tech & team – always sustainable

0x01

Motivation

Collision of two worlds – Automotive and IT

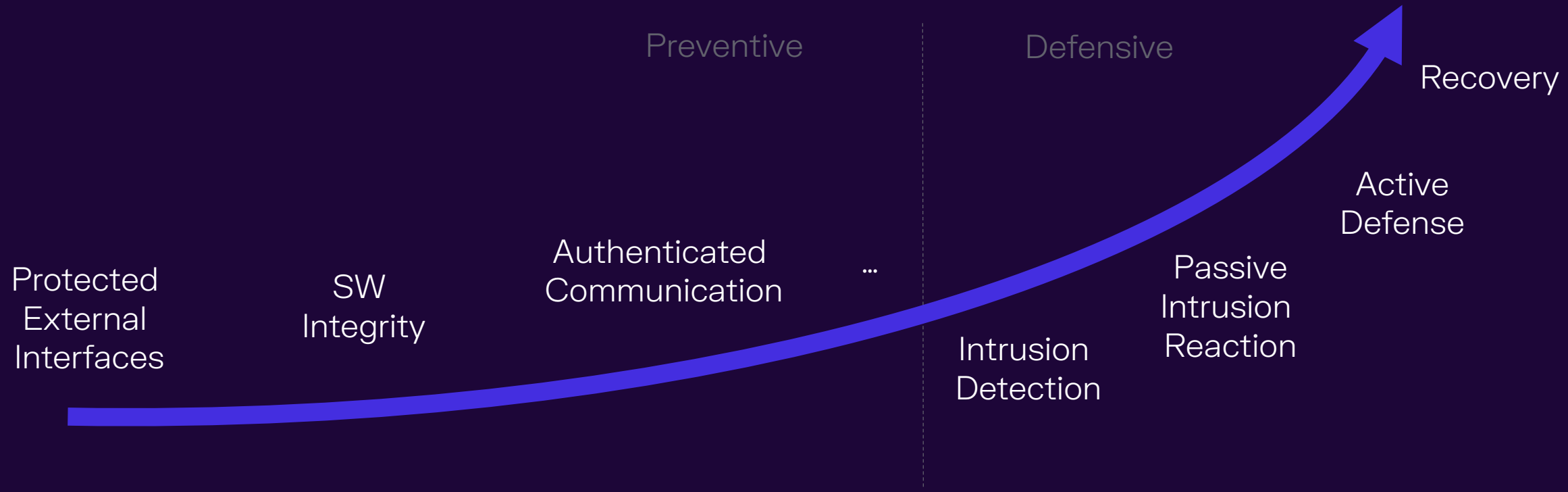
Comparison of both worlds – Why automotive can profit from information security?



But you can‘t just lift & shift enterprise IT procedures into an automotive environment.

From Prevention to Active Defense

Looking on information security: What is next after introducing processes and technical control measures?



First steps into passive defense are made, but there is a long way until real active defense!

0x02

Detecting active attacks

How is an attack detected?

collect system data

+ apply anomaly detection rules

= detect possible ongoing attack

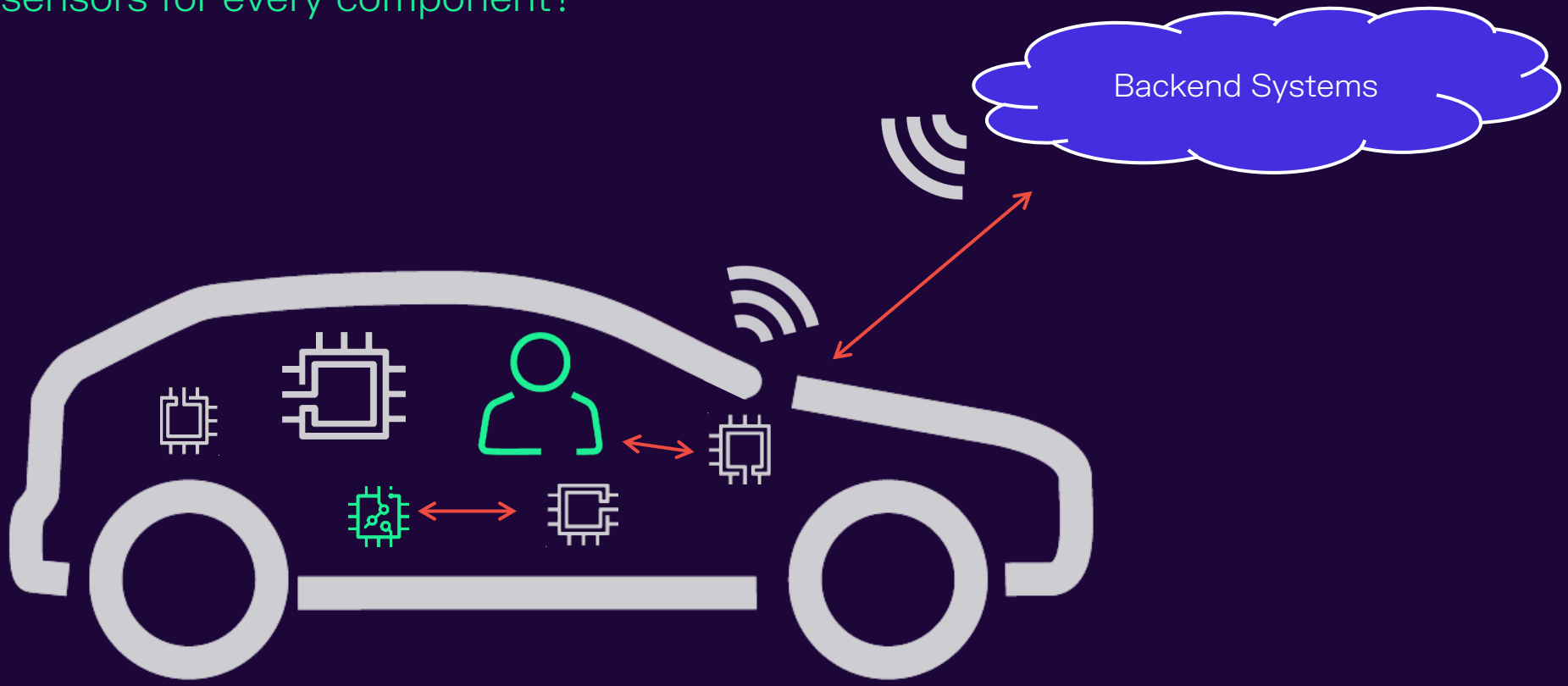
What data can we gather from which source in what format?

How can we collect it?

How can we store it?

Let's take a look at interesting interfaces.

Implement sensors for every component?



...and how much data do we want to collect?

Collecting too much or irrelevant data only makes our job harder.

*(analyse the attack **and** reverse engineer your own infrastructure?)*

Sorry: there is no blanket solution for any given specific vehicle.

But there are some general steps we can follow:

1. Create and maintain an asset register *(so you know where your data is from).*
2. Base data collection configuration on use cases provided by the asset.
3. Keep service owners (and other stakeholders) in the loop and review regularly.

Most importantly:

These are process issues, not tooling issues.

which does not mean you don't need tools ;)

Utilizing the power of the backend.

+ more processing power and storage space than vehicles

+ allow for up-to-date centralized fleet-wide anomaly detection

+ are not safety-critical systems

? introduce more complexity into the infrastructure (connectivity requirements)

Utilizing the power of the backend.

Goal: Bring together vehicle and backend to detect anomalies.

1. Acquire data in vehicle
2. Perform first detection in vehicle
3. Aggregate data in backend
4. Follow-up with more thorough detection in backend

Okay, we've detected an attack.

What now?

0x03

Response

Goal of response measures

1. Contain or mitigate the attack

2. Completely stop the incident

3. Recover your systems

(4. Do Lessons Learned)

Sorry, there is no step-by-step guide handle every attack.

Every incident is unique and attackers will always be more creative than you.

But let's share and discuss our thoughts.

Safety First!

Considering safety aspects when defining responses.

- Check safety context!
- Develop for usage in safety-critical context
- Establish freedom of interference
- Trigger fallback to safe state as response

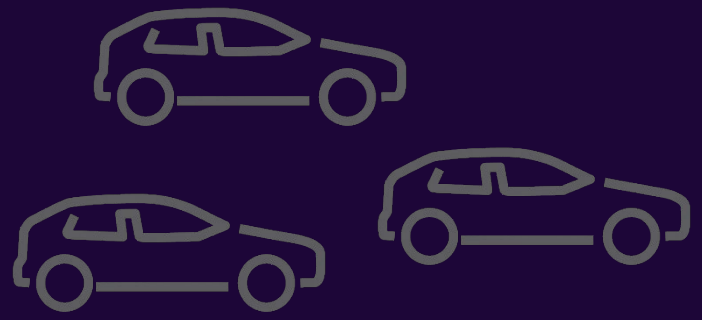
The Power of Automation

Or: What do when scaling up?

Scale of modern automotive fleets: massive

Is it viable to manually verify autonomous responses before implementation?

...it depends!

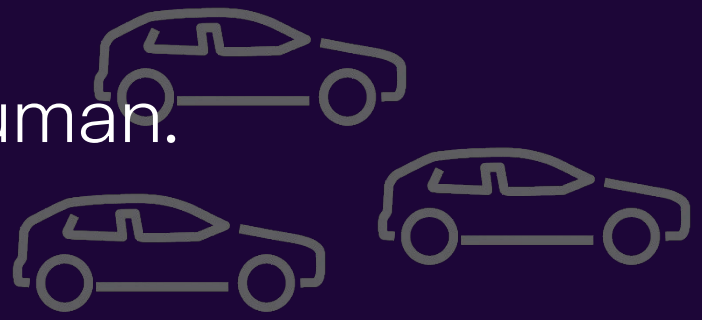


Scaling and the power of automation

Always consider how probable a given situation is.

High likelihood, little severity: autonomous response plausible.

Low likelihood, high severity: better include a human.

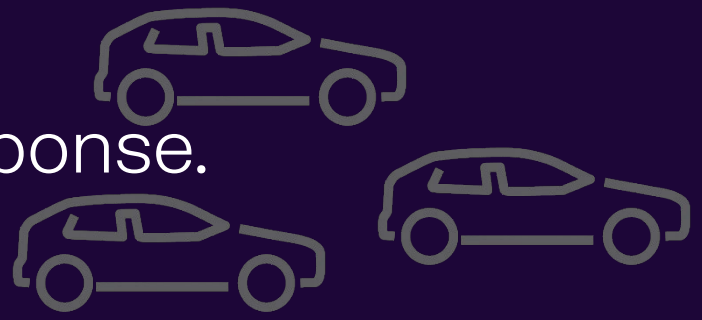


Let's talk AI.

Whenever scaling and automation are involved, AI is considered as a solution.

AI-based Vehicle Defense =

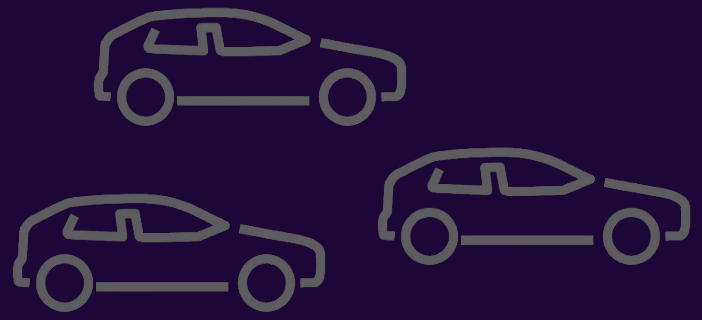
AI-based detection + AI-based response.



A word about AI-based approaches.

For us, AI-based response is currently too risky.

Interfering with safety-critical systems requires absolute certainty and there are just not enough real-world incidents to train an AI on, yet.



0x04

Looking Forward

Where to start?

Question your mindset.

Learn from experiences

Do Lessons Learned

Continuous exchange of ideas and visions

Discuss openly within technical community

Learn from real-world attacks

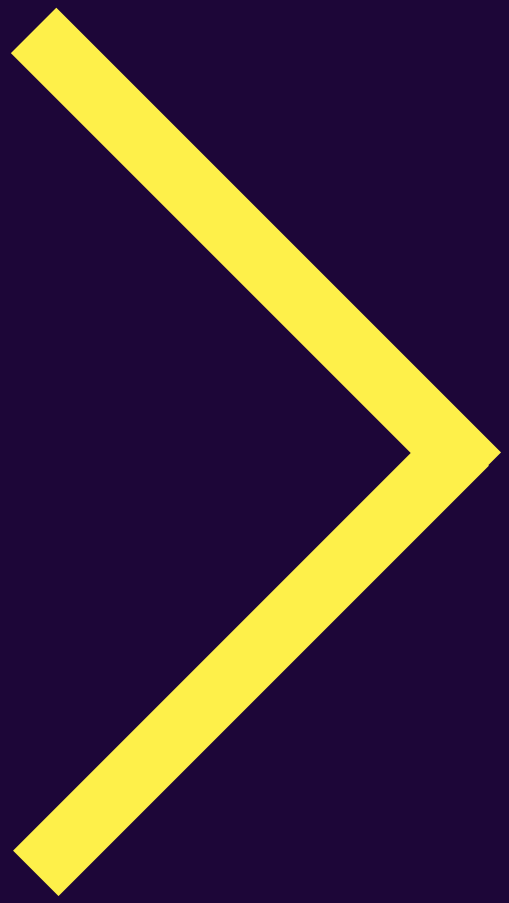
Don‘t stop refining your procedures

Successful defense works because of preparation and introspection.

Nobody knows how the future of Automotive Information Security will look like...

...but let's build it together.

Thank you!



miriam.gruber@cariad.technology

jan.lange@cariad.technology