



Security for the Autonomous Vehicle – Identifying the Challenges

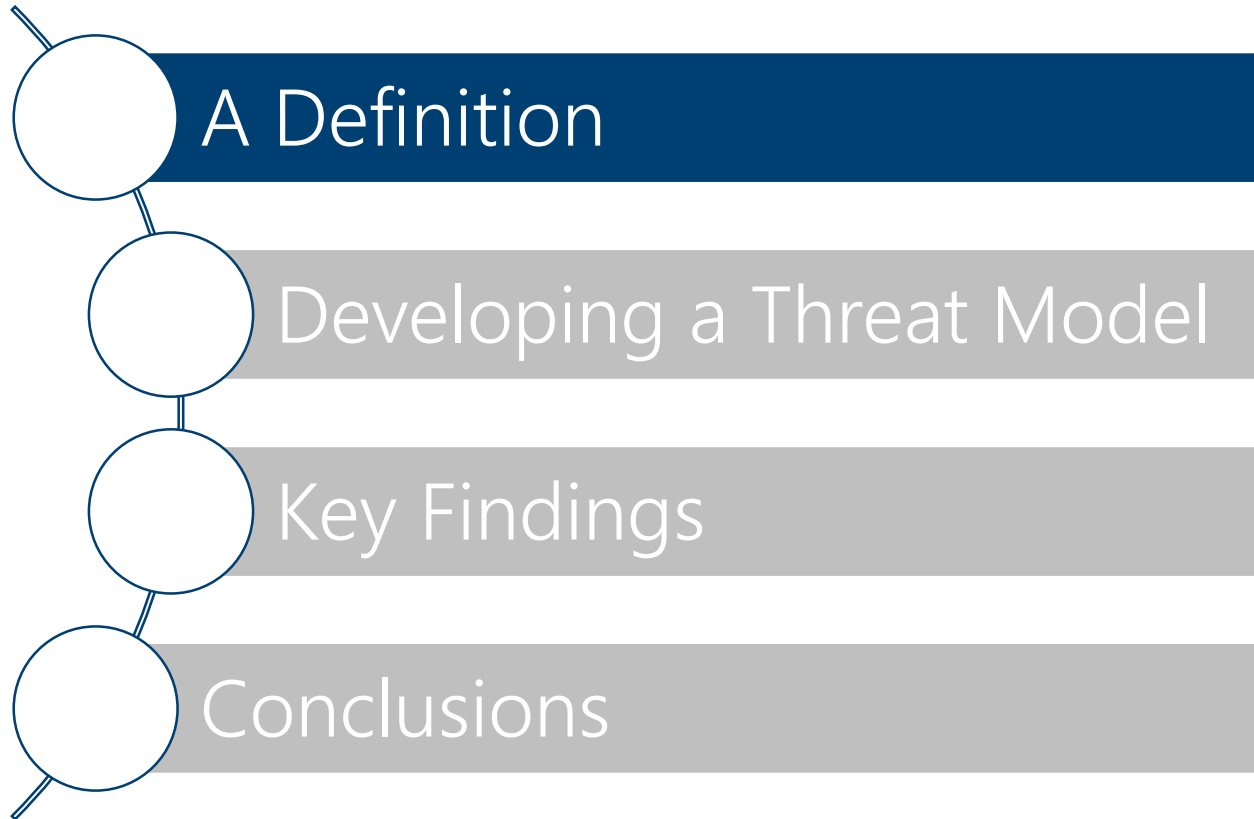
Mike Parris – Head of Secure Car Division

November 2016



Today's agenda

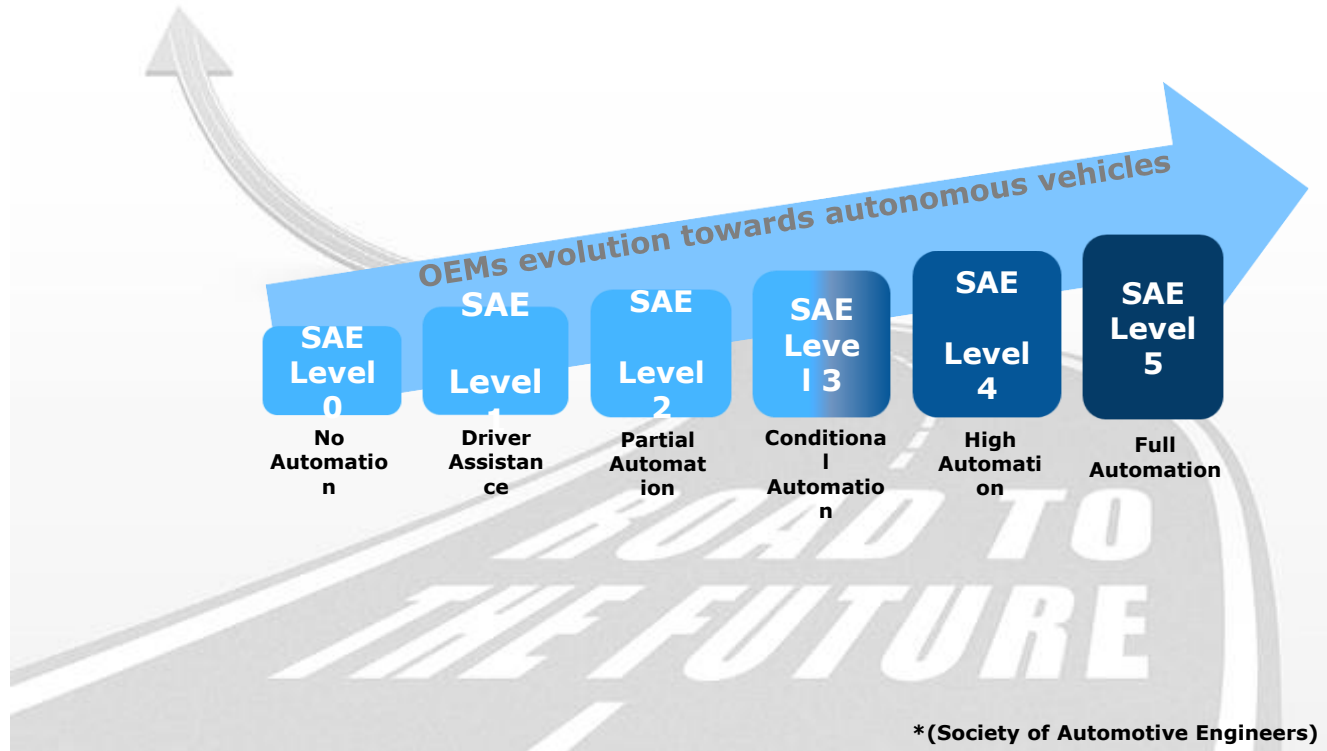




SAE levels of vehicle autonomy



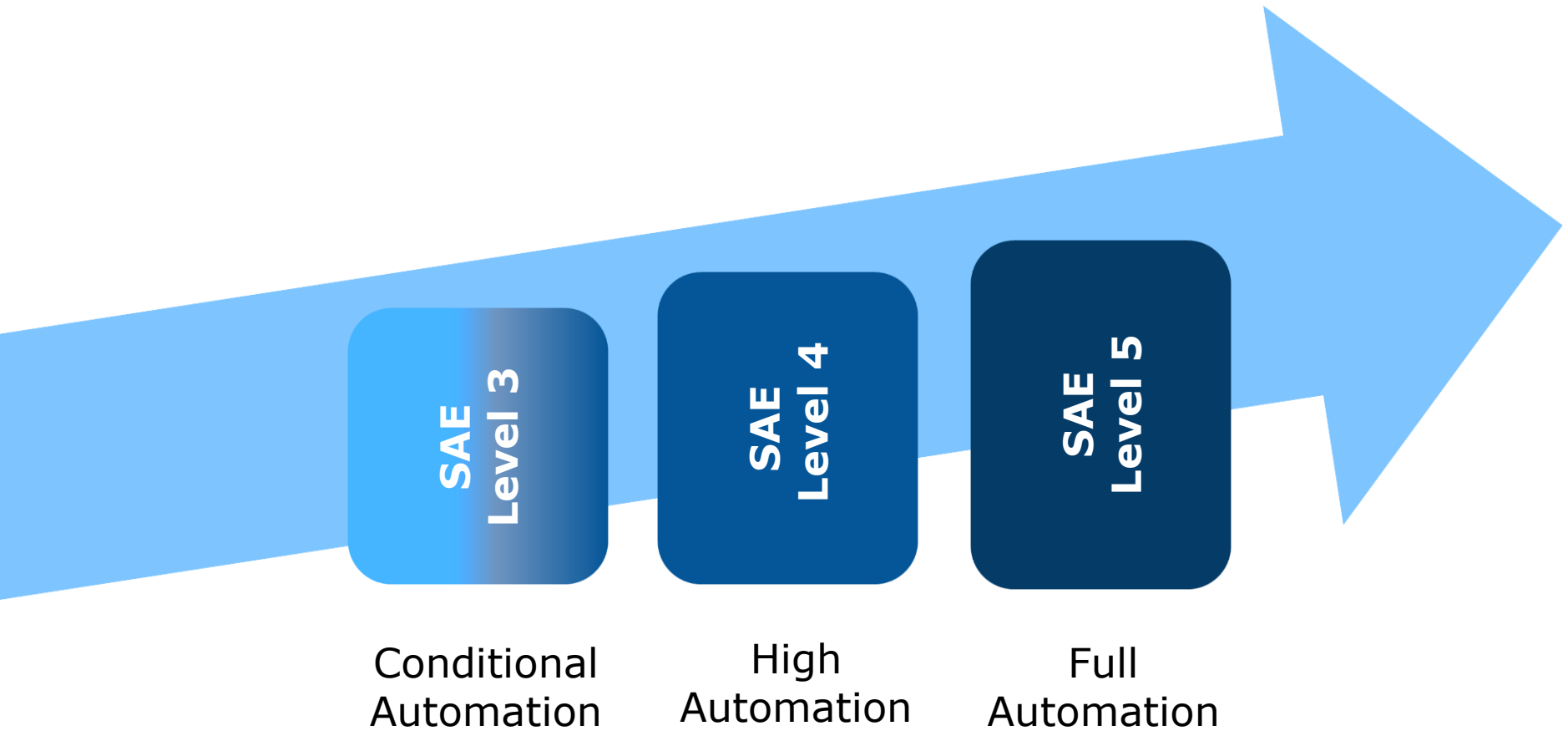
Car manufacturers are working towards deploying systems corresponding to **Level 3**.



SAE levels of vehicle autonomy

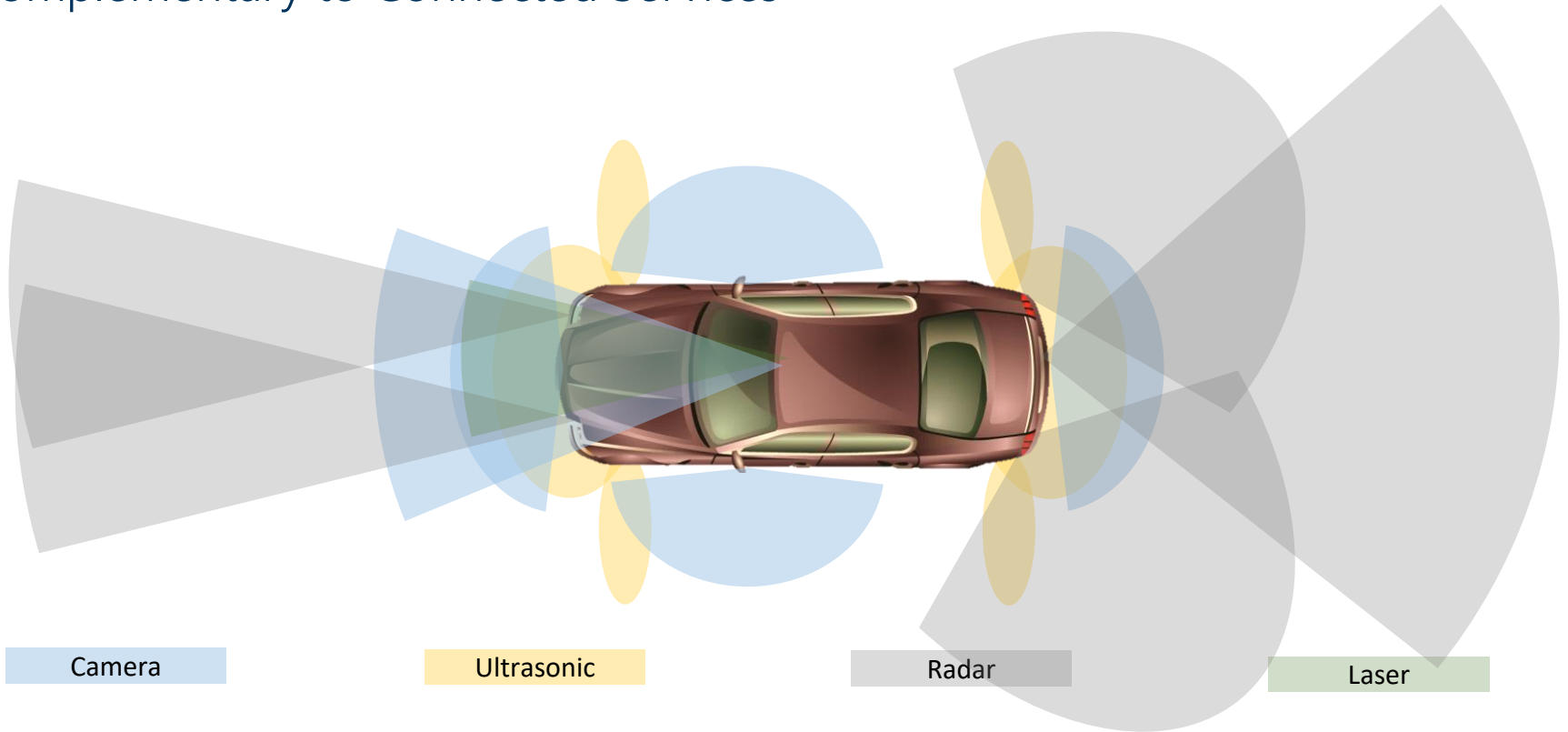


We're going to focus from **Level 3** onwards.



Autonomous Technologies

Complementary to Connected Services



Sensing needs

The sensors all have different characteristics and therefore can't replace each-other but rather complement each-over, leading to complex sensor fusion schemes.

ADAS Partitioning



Piecemeal ADAS development over the years - 3 main groups

Forward Facing	Rear Facing	All Around
Adaptive Cruise Control	Blind Spot Information	360 degree view
Automatic Emergency Braking	Side Collision Mitigation	Fully Autonomous
Lane Keeping Assistance		



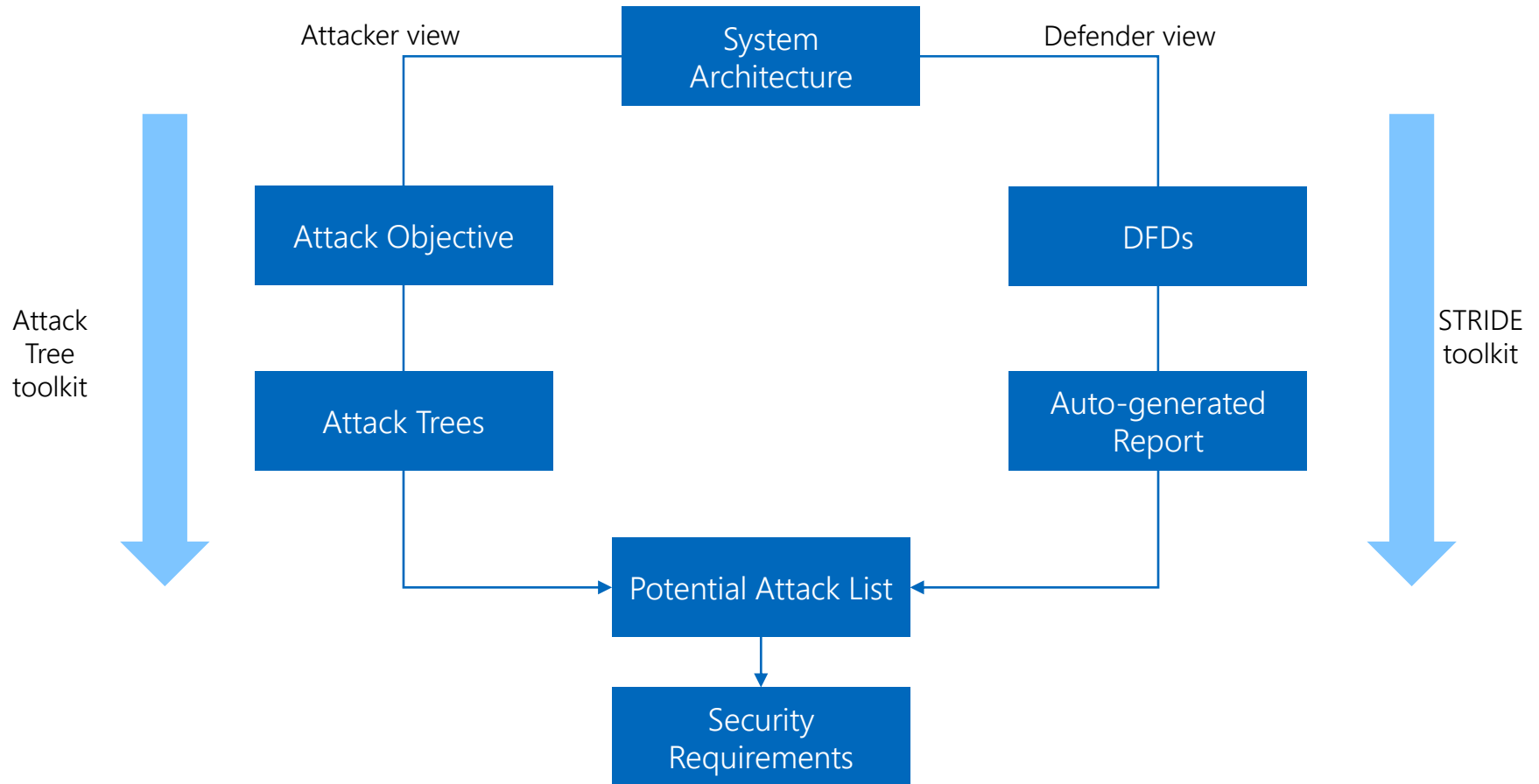
SAE Level 3 systems fuses forward facing and rear facing sensors (hybrid approach between hardwired and networked topology)



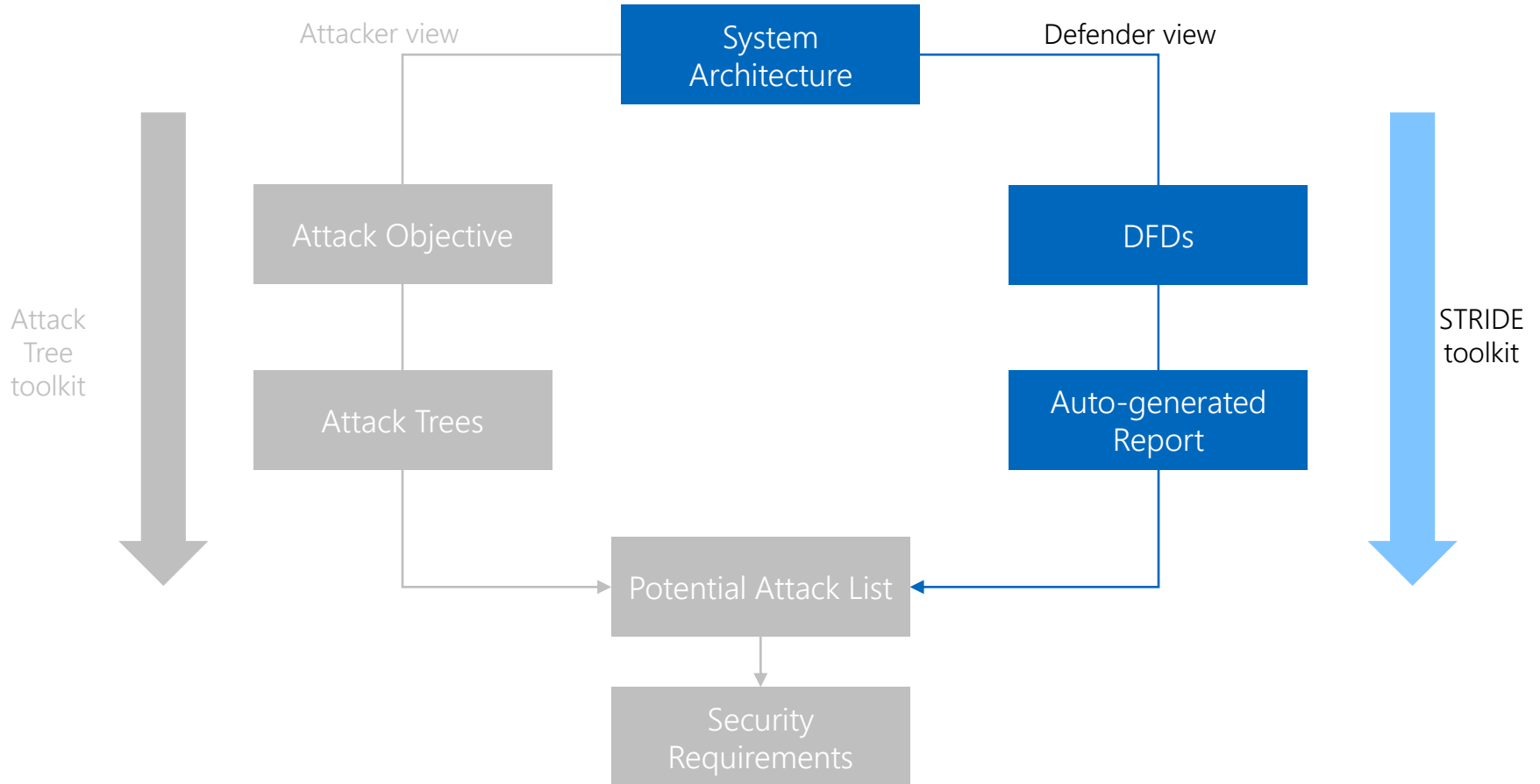
SAE Level 4 will fuse all sensors in a centralised unit



Threat Modelling



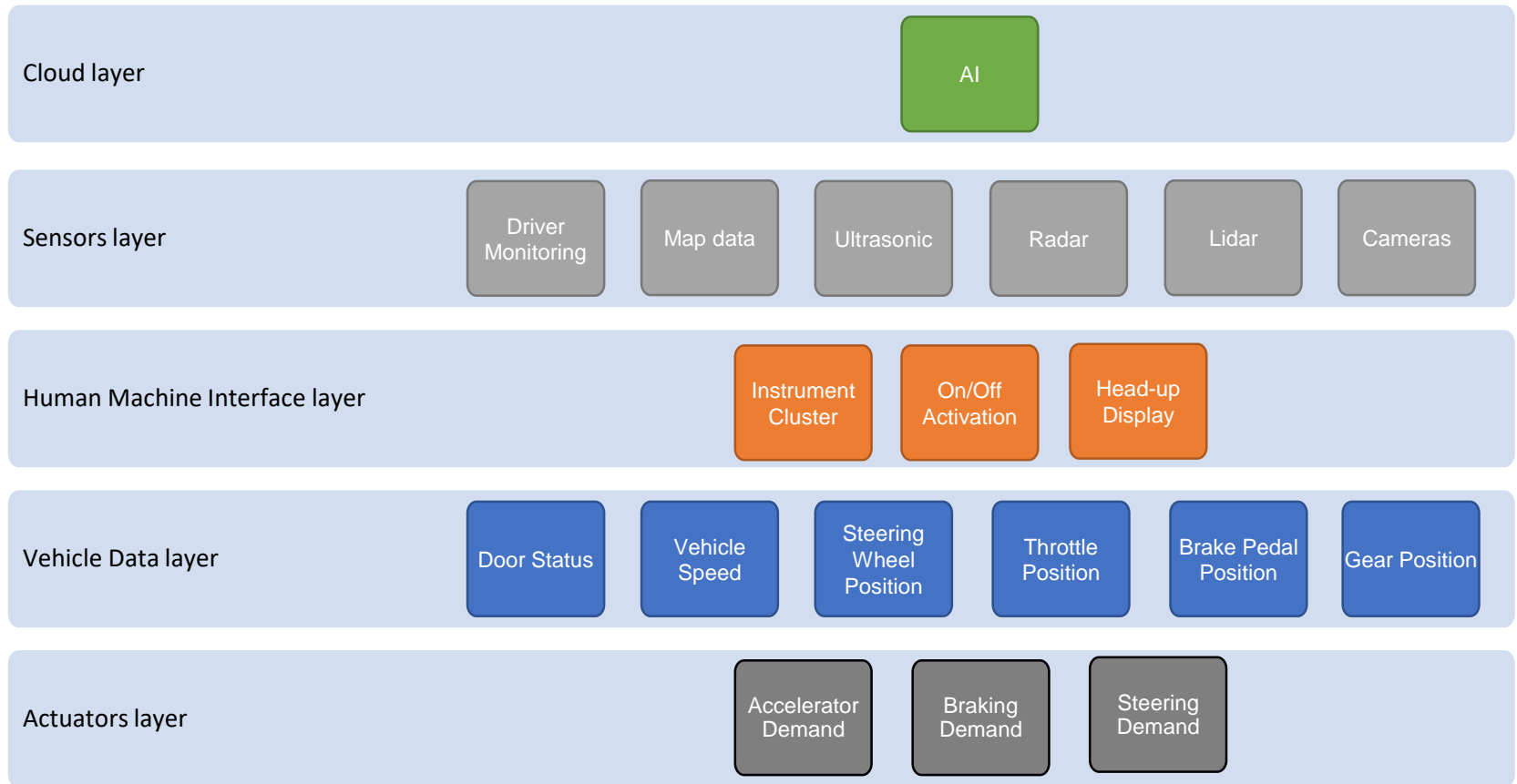
Threat Modelling



Developing a Threat Model

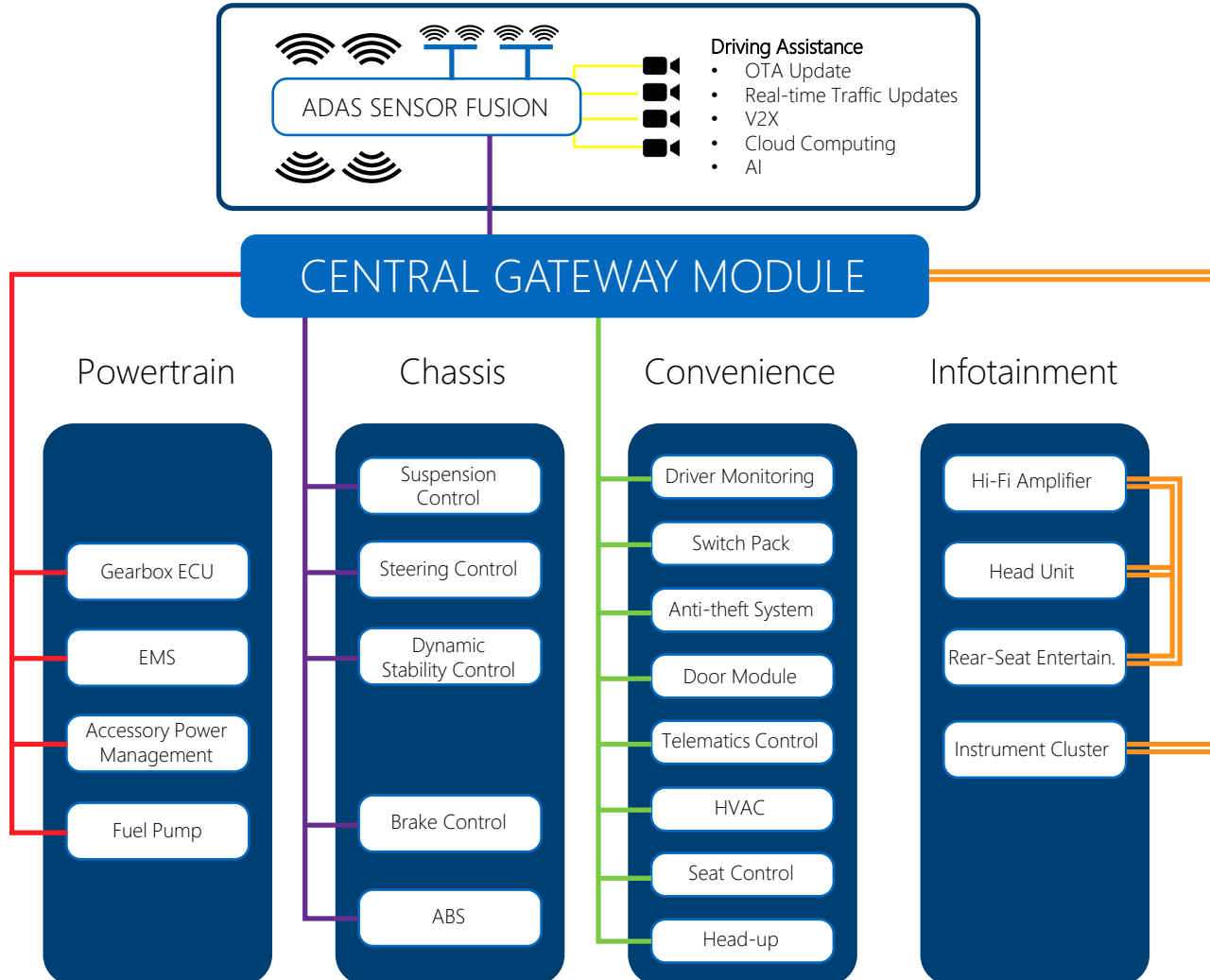


Identify generic layers and entities



Developing a Threat Model

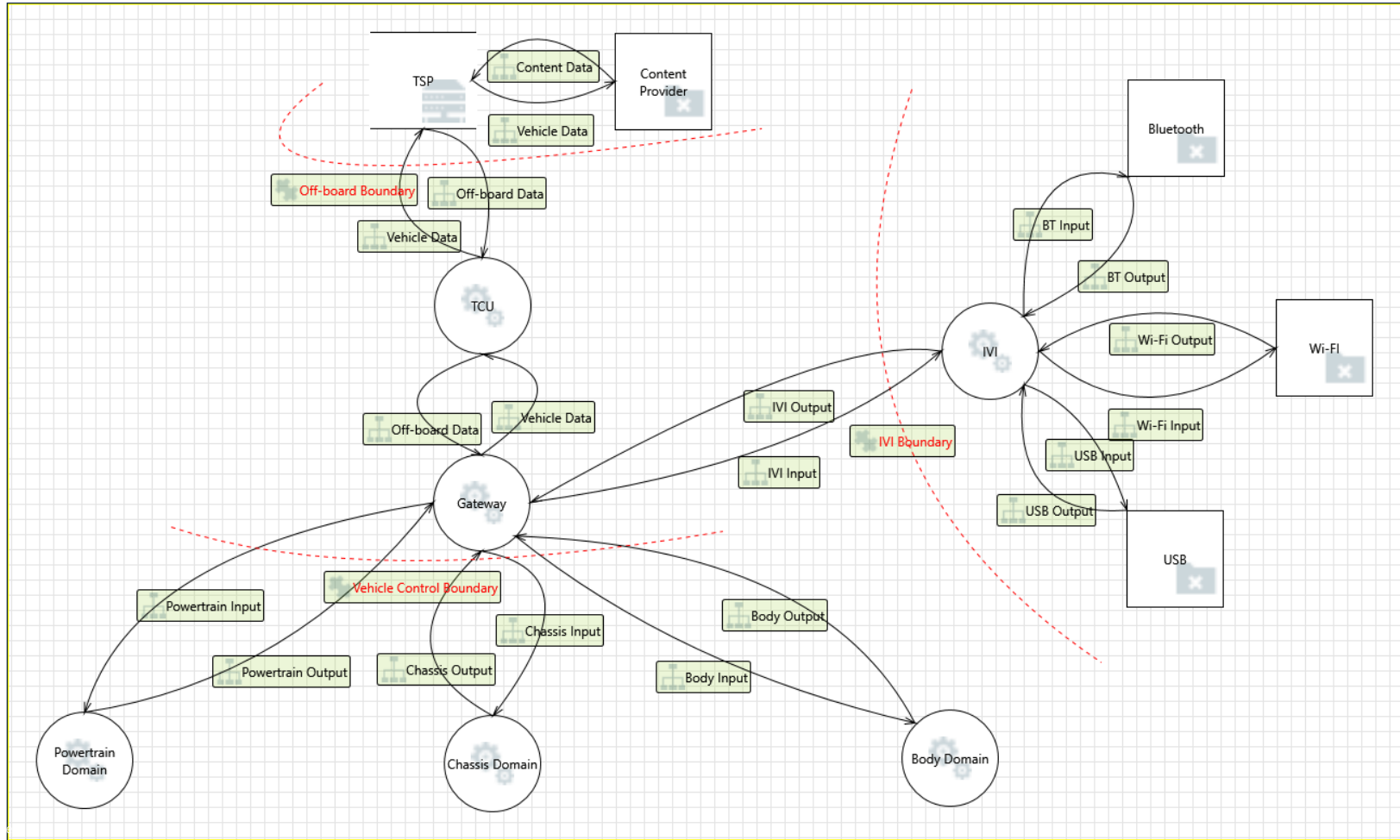
Create a system architecture



Developing a Threat Model



Create a data flow diagram (DFD)



Developing a Threat Model

Auto-generate DFD threat report

2. Spoofing the Gateway Process [State: Not Started] [Priority: High]

Category: Spoofing

Description: Gateway may be spoofed by an attacker and this may lead to unauthorized access to Body Domain. Consider using a standard authentication mechanism to identify the source process.

Justification: <no mitigation provided>

3. Spoofing the Body Domain Process [State: Not Started] [Priority: High]

Category: Spoofing

Description: Body Domain may be spoofed by an attacker and this may lead to information disclosure by Gateway. Consider using a standard authentication mechanism to identify the destination process.

Justification: <no mitigation provided>

4. Potential Lack of Input Validation for Body Domain [State: Not Started] [Priority: High]

Category: Tampering

Description: Data flowing across Body Input may be tampered with by an attacker. This may lead to a denial of service attack against Body Domain or an elevation of privilege attack against Body Domain or an information disclosure by Body Domain. Failure to verify that input is as expected is a root cause of a very large number of exploitable issues. Consider all paths and the way they handle data. Verify that all input is verified for correctness using an approved list input validation approach.



Justification: <no mitigation provided>

5. Potential Data Repudiation by Body Domain [State: Not Started] [Priority: High]

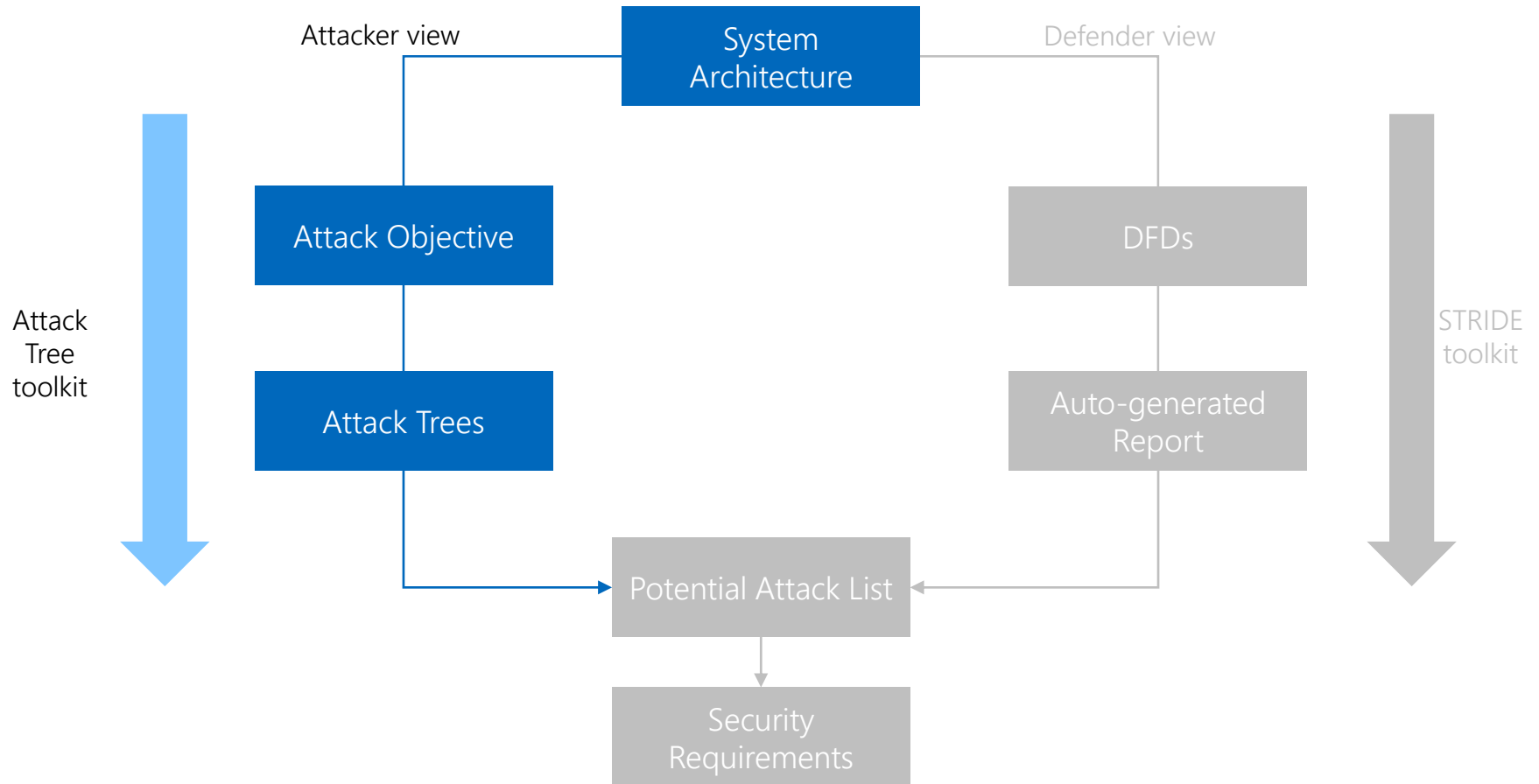
Category: Repudiation

Description: Body Domain claims that it did not receive data from a source outside the trust boundary. Consider using logging or auditing to record the source, time, and summary of the received data.

Justification: <no mitigation provided>

-  Identifies all possible threats from system architecture perspective
-  Not all threats are relevant and there may be considerable duplication

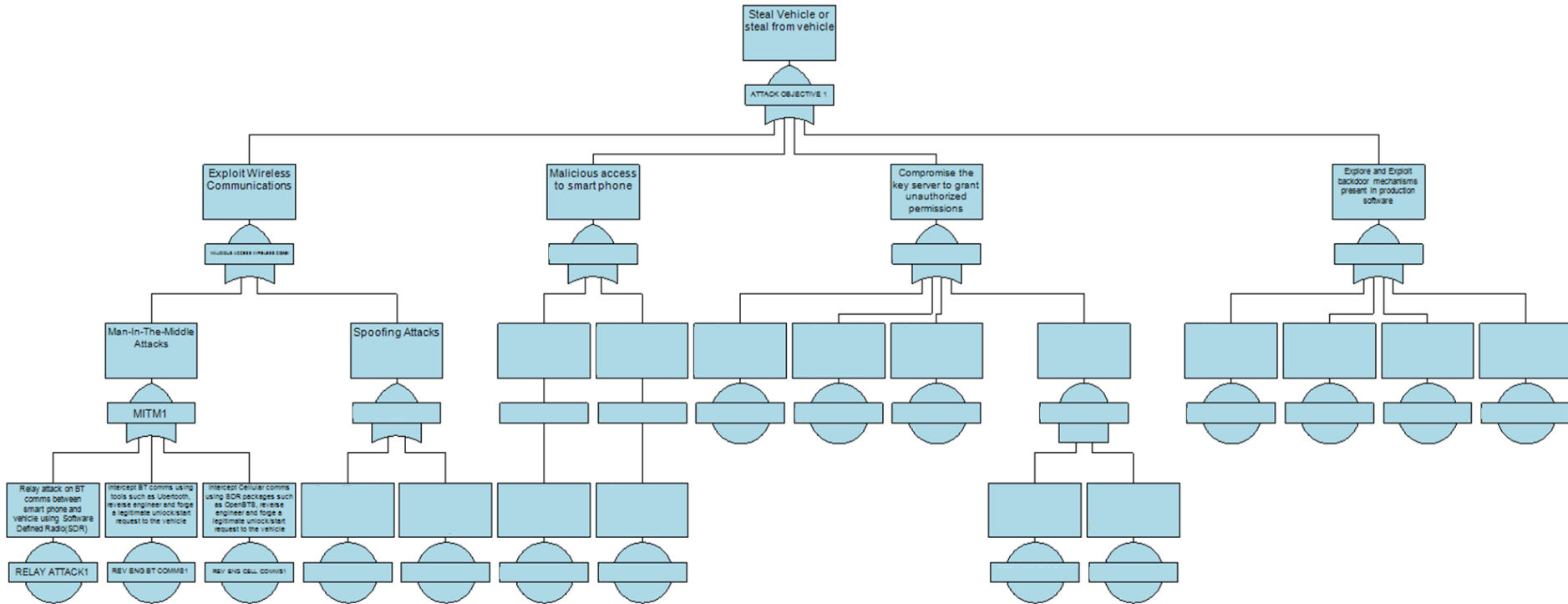
Threat Modelling



Developing a Threat Model



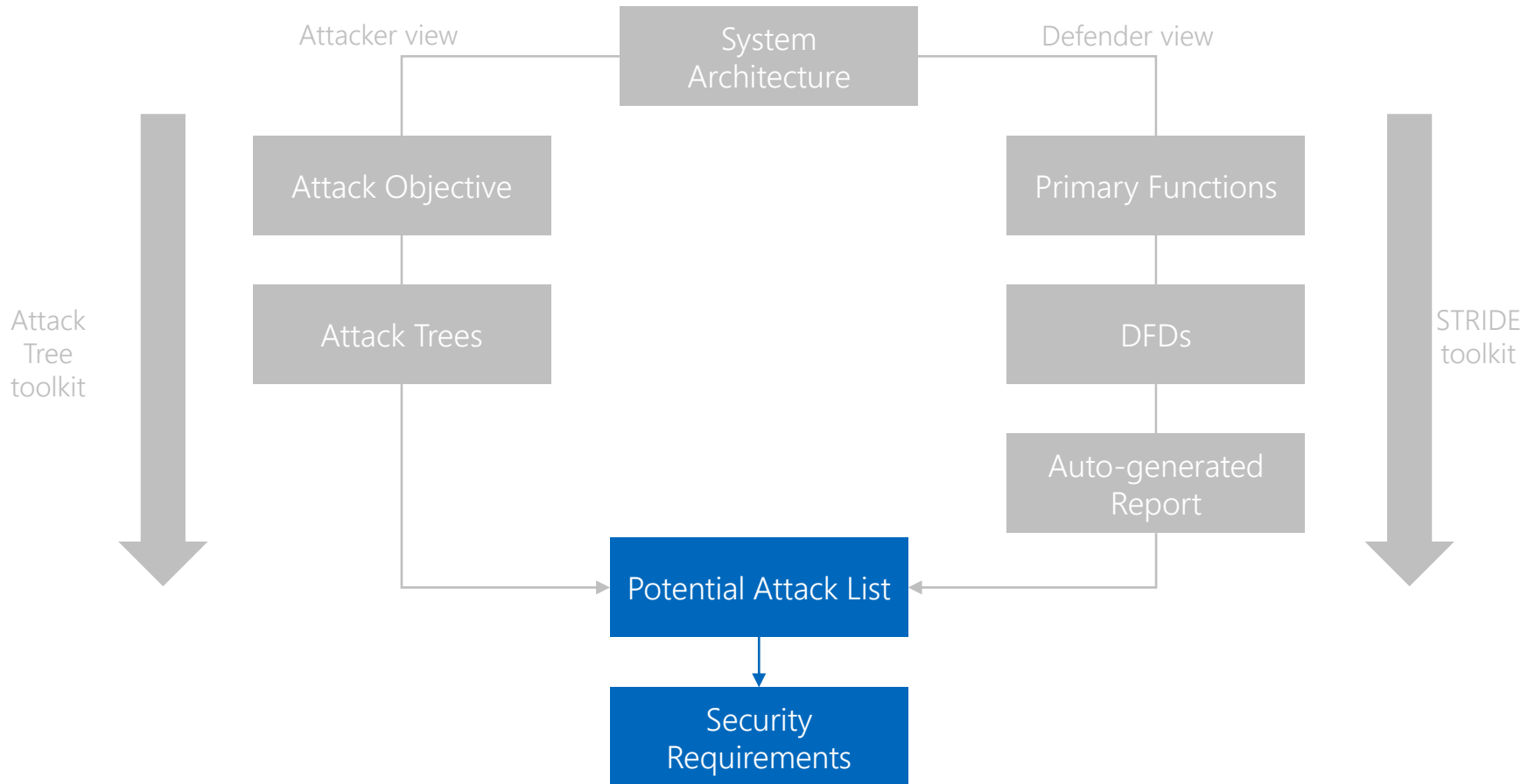
Identify attack objectives and create attack trees



+ All threats are relevant

- Difficult to demonstrate completeness of attack tree

Threat Modelling



- + All Potential Attacks and Security Requirements are relevant with full 2-way traceability
- + Completeness demonstrated by reference to DFD Auto-generated report



A large, dark blue circle containing the text 'Some obvious...'.

Some
obvious...

Forced crash – direct control

Complete Denial of Service:

- fail to start/engage
- operational failure –
SAE L4&L5 - no driver fall-back

**Leakage (theft) of Personally
Identifiable Information (PII)**

- real-time
- historical

A large blue circle containing the text 'Some less obvious...'.

Some less
obvious...

Partial system failure – driver unaware

- including calibration errors

Leakage (theft) of Personally Identifiable Information (PII)

- predictive

Breach of an Autonomous vehicle geo-fence (SAE L4)

Pedestrian provoked injury

Congestion management

Findings – Vehicle level threats



Key Mitigations

Resilience to Sensor interference

- Need for duplicate/redundant sensors
- Multiple verification – special case of fusion:
 - Like sensors (duplicate/redundant)
 - Unlike sensors (e.g. correlate wheel speed with GPS speed)

Security validation at point of manufacture

Security validation during operational service:

- Calibration
 - Roadside/Service Facility
(windscreen mounted sensors/accident repair)
- OEM parts vs After-market parts

Supply Chain Integrity

- Supplier-OEM-Distributor / Dealer – Customer / Driver – Service - Repair

Vehicle Behaviour:

- Monitoring of one vehicle (use – misuse – abuse)
- Standard operations of systems between vehicles
- Fail-safe / Limp-home modes

AI Integrity:

- Digital Forensics/Data Recorder/PII Privacy

Failure – Misuse – Abuse is a spectrum of resilience



Conclusions

Are all Industry Stakeholders Being Sufficiently Proactive?



More about SBD



Since 1995 we live, eat and breath automotive

We enable data-driven decisions

We are here to help!

Our Mission



To be the world-leading knowledge partner for the automotive industry

Our Intelligence & Insight Services



Model-level databases

Technology forecasts

Supplier intelligence

Market regulations

News analysis

Our Approach



We are committed to adapting to our client's needs and always strive for the highest quality of service

Our Expertise



The largest team of in-car technology specialists recruited from over 10 OEMs & suppliers

Our Evaluation Services



Expert UX testing

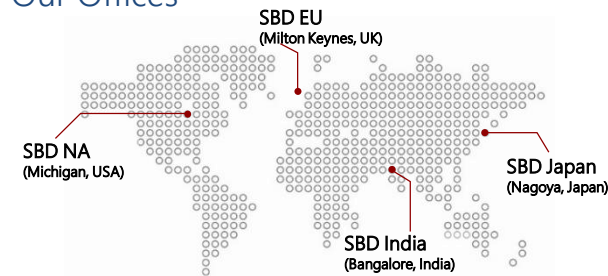
Consumer UX testing

Iterative prototype evaluation

KPI setting

Cyber security testing

Our Offices



Our Customers



95% of OEMs

65% of Tier-1s

60% of Service Providers

Our Strategy Services



New market entry support

RFP/RFO management

M&A due diligence

Strategic workshops

Supplier positioning support

Your Contact Person



Mike Parris

✉ MikeParris@sbdautomotive.com



+44 (0)1908-305105