Continental
The Future in Motion

Data & Safety

An introduction through a concrete example with connected vehicles

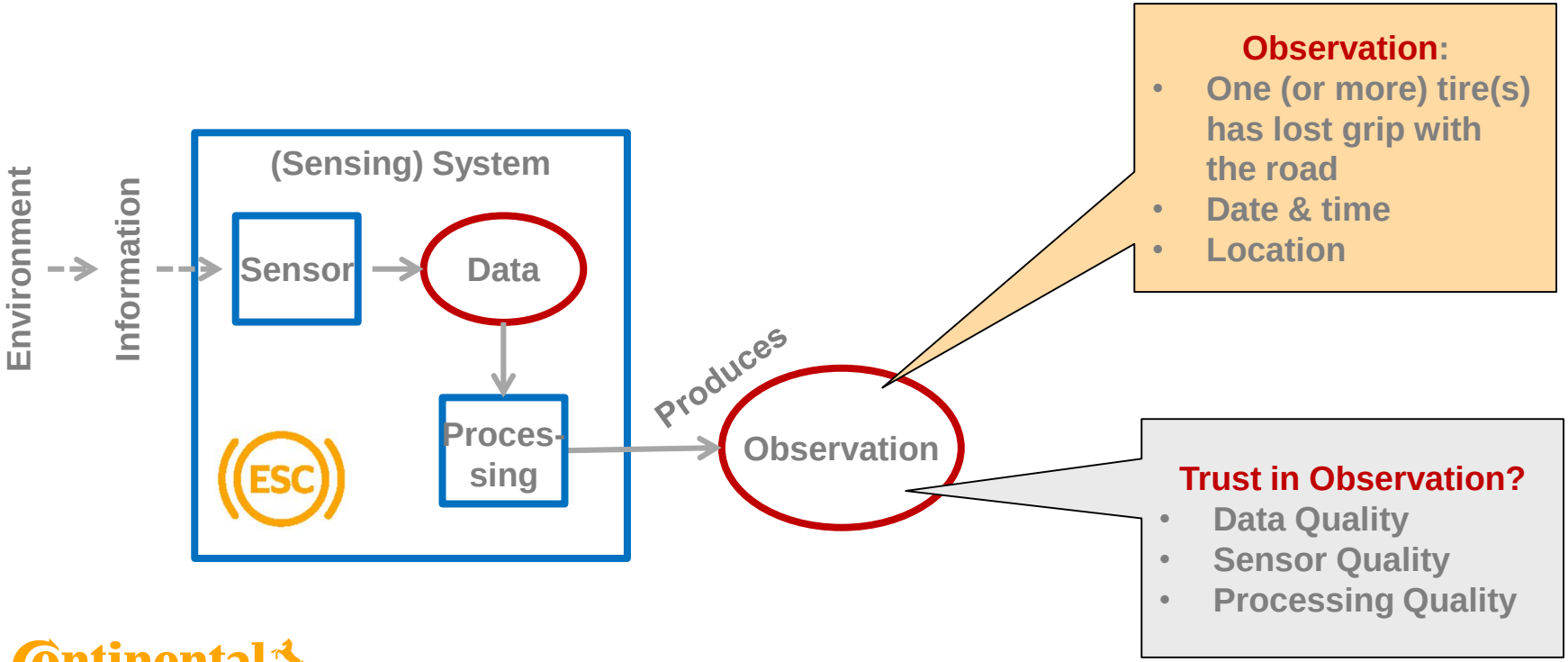
Hugues "*Safety*" Bonnin, Olivier "*Data*" Flebus

10th EDITION EUROPEAN CONGRESS
ERTS 2020
FROM 29th TO 31st JANUARY / TOULOUSE, FRANCE
PIERRE BAUDIS CONGRESS CENTER

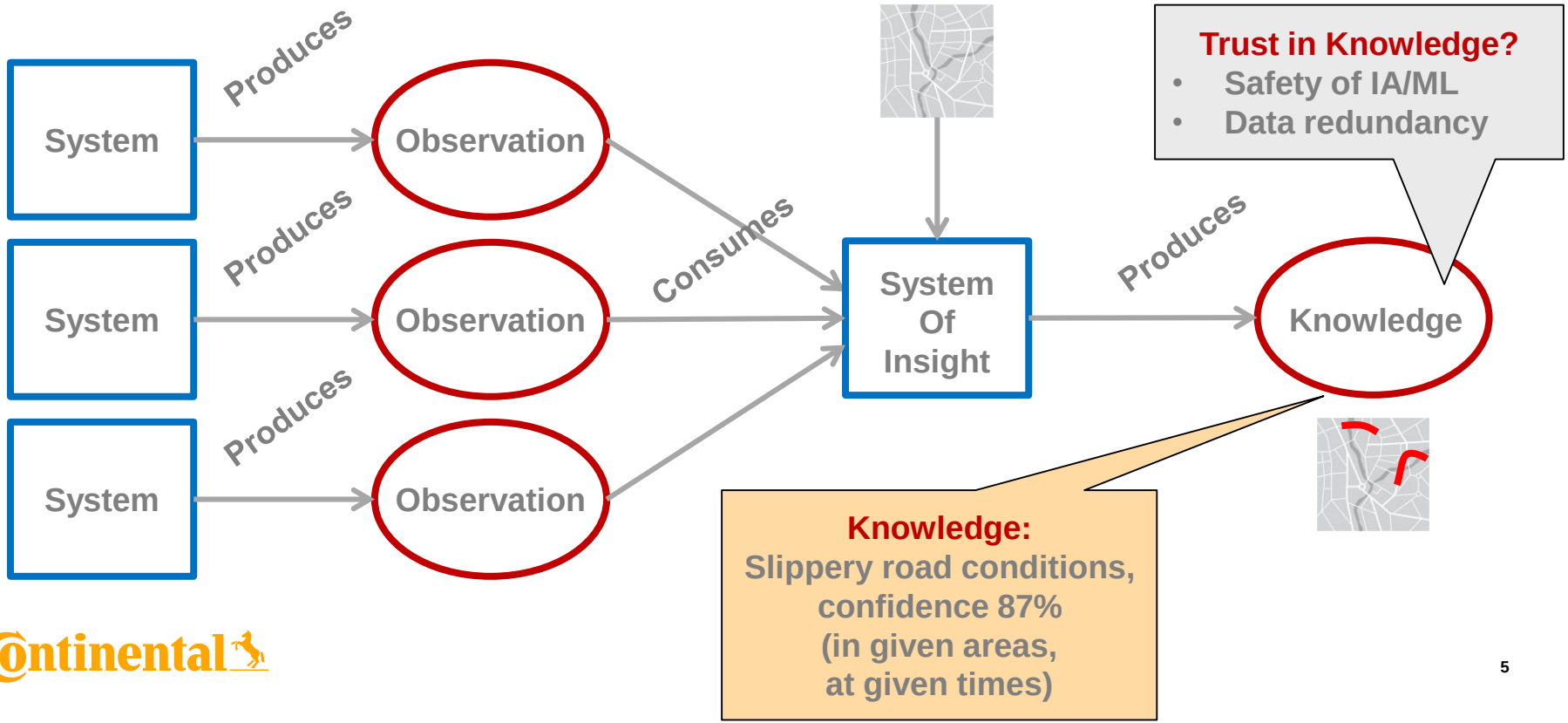
Safety Risk Balance with Data?


A (dynamic) “map” that could warn drivers and/or vehicles of dangers ahead (eg: slippery road conditions)?
Slippery road ahead

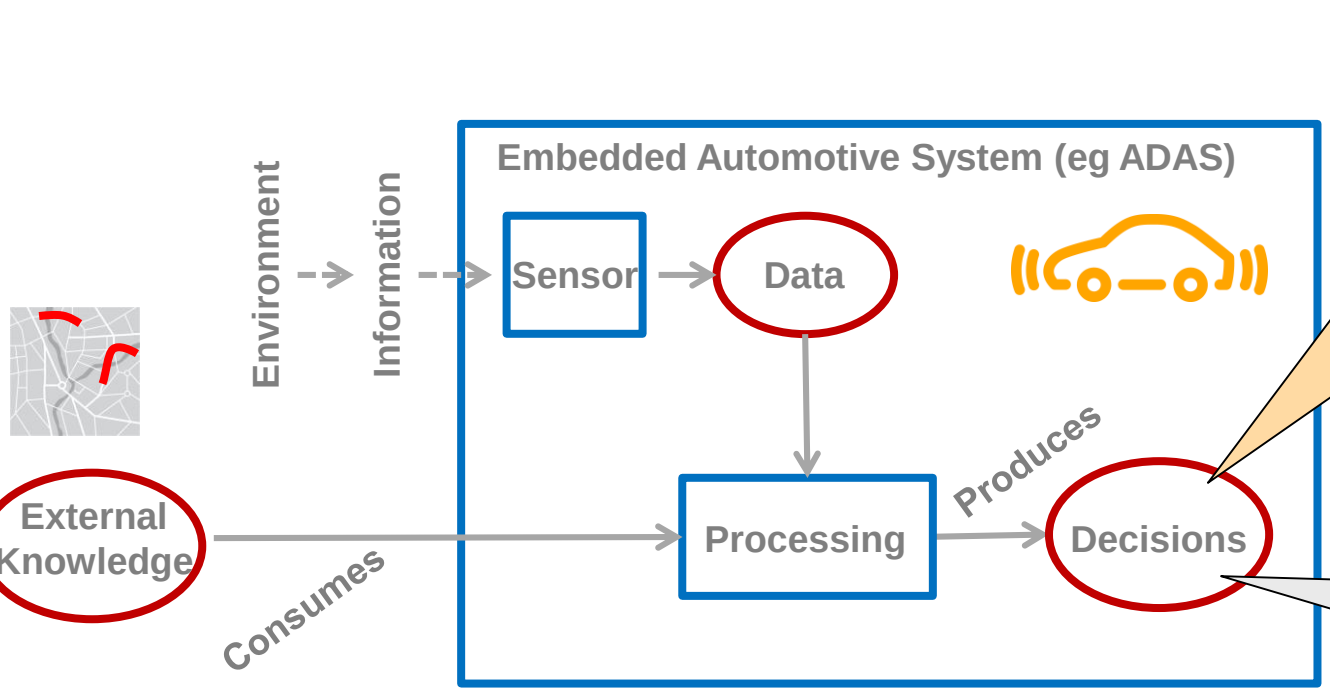
Stage 1 – Use existing systems (ESC, ESP) to sense when tires lose grip with the road



Stage 2 – Connect vehicles and then combine multiple observations into Knowledge



Stage 3 – Leverage external knowledge in the context of every vehicle (when relevant)



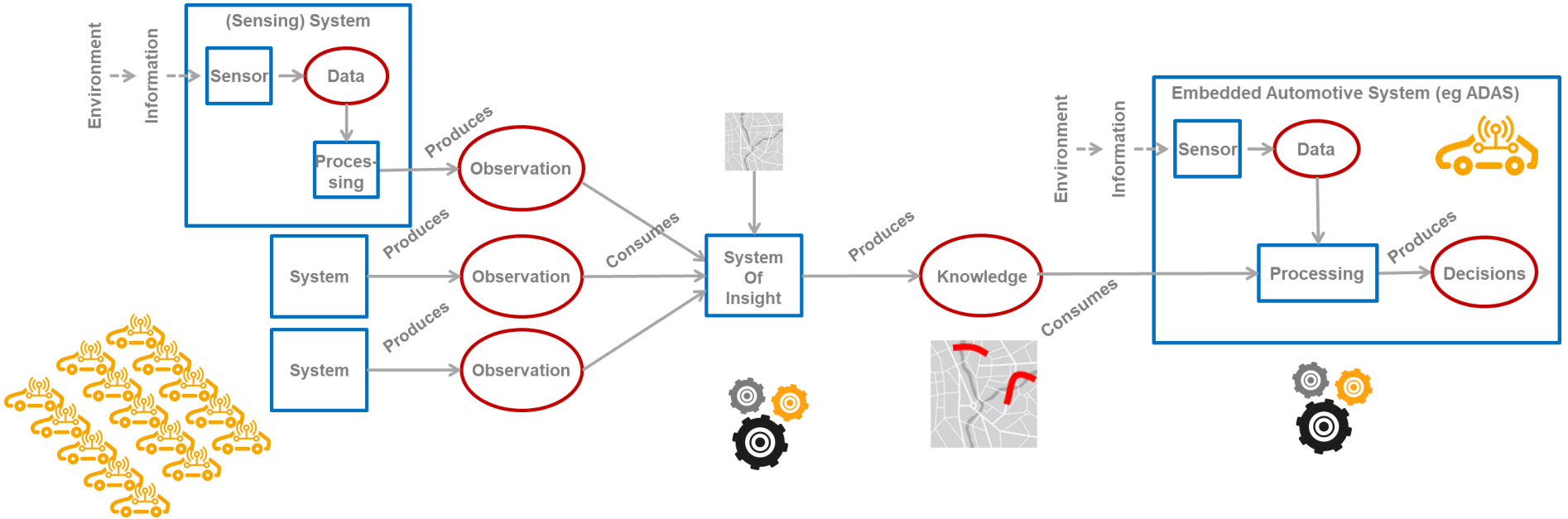
Anticipation:

- Warning to Driver
- Speed Assist : decrease speed
- Action (SAE L3): Handover to driver
- Action (SAE L4): Brake and/or Decelerate

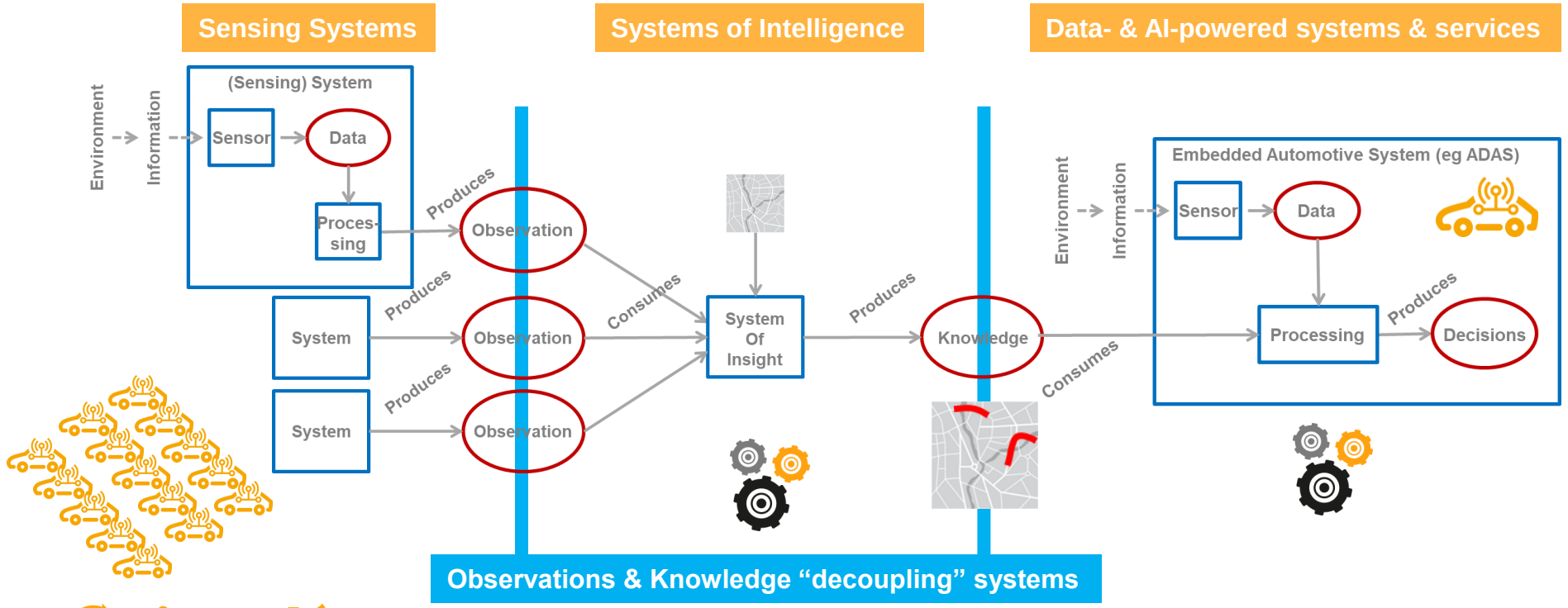
Safety of Decisions?

- Trust in Knowledge
- New interface?

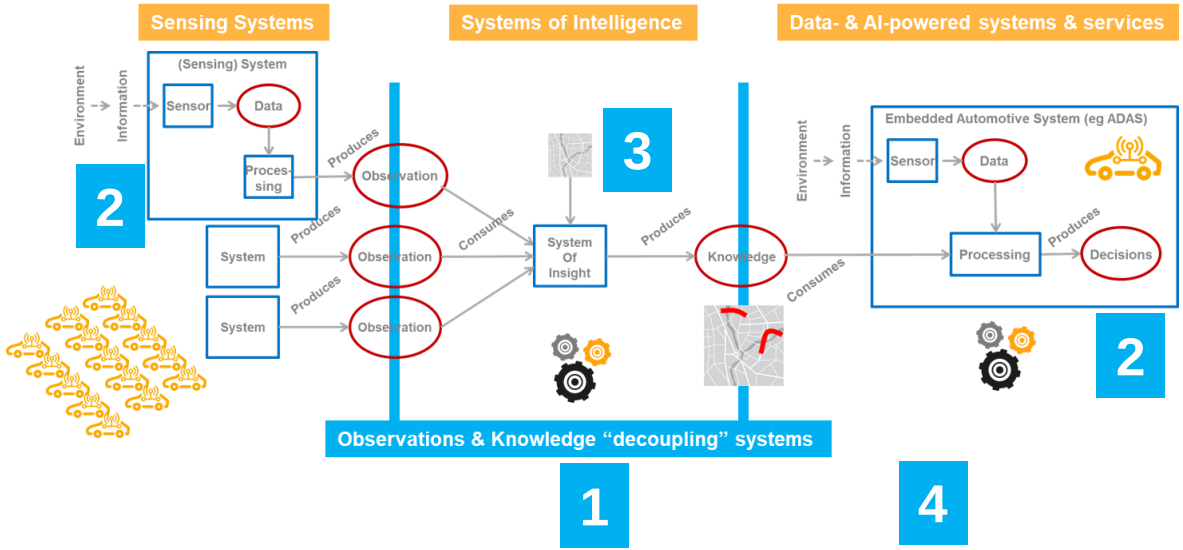
All stages in one – A very complex *chain of trust* mixing multiple System- and Data-driven lifecycles



(External) data to decouple systems



What do we need to do?



1. Build the confidence in data (means, level, methods)
2. Adjust (or not) the existing standards to integrate the "Safe Data" ones
3. Define Safety for systems of intelligence
4. Don't forget the data transmisson integrity!


We are convinced that data can improve safety
We have the intuition that a data centric approach for safety can bring more opportunities than risks
Join us!
hugues.bonnin@continental.com
olivier.flebus@continental.com

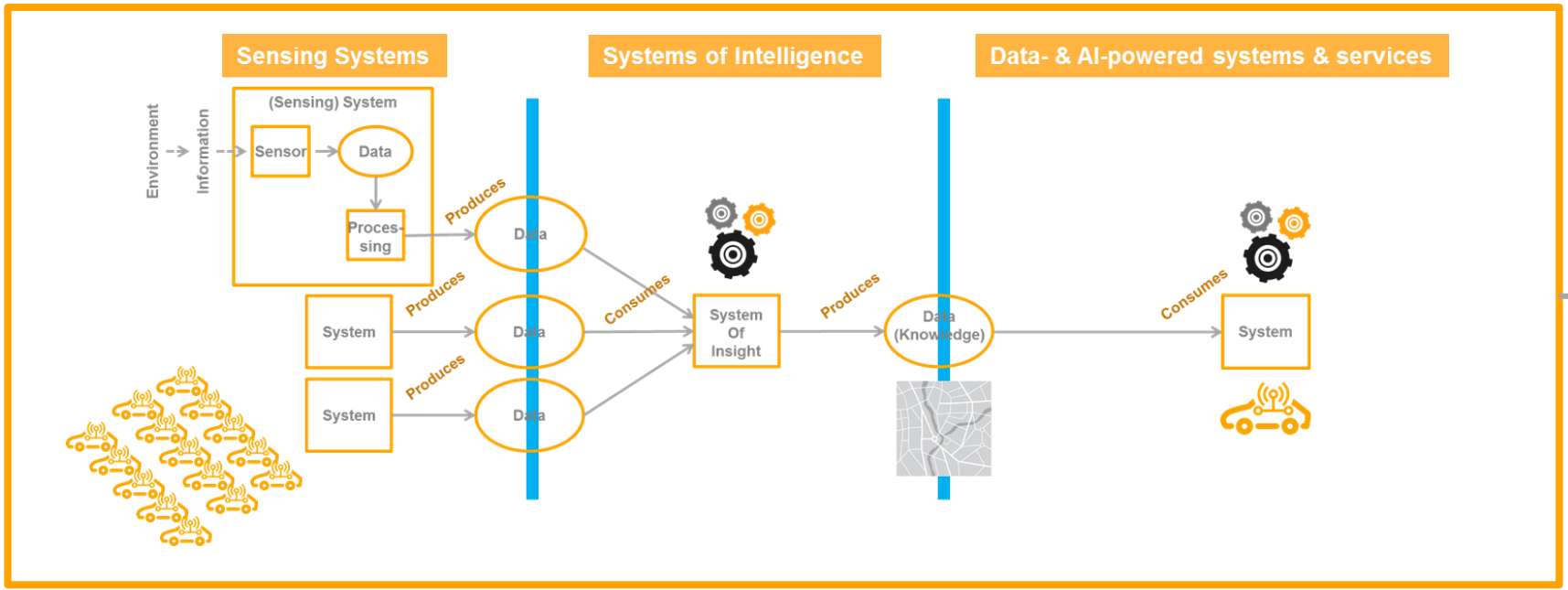
Backup

7 reasons why data matters to safety

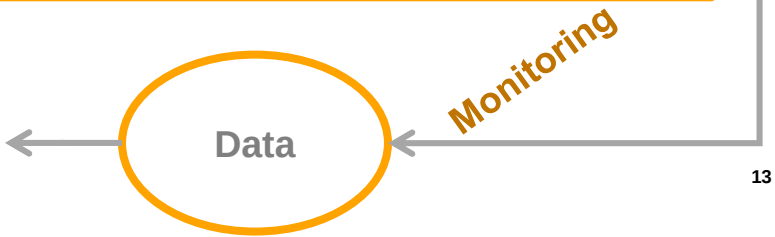
1. Connected vehicles and fleets introduce **Road Traffic Safety** challenges & opportunities
2. Data flows can provide key knowledge to help vehicle **anticipate hazards** – especially for autonomous driving
3. Vehicle **connectivity** brings more **complexity** – data connects together a larger number of vehicles and systems
4. Data can **harm** systems – especially when it comes from the “outside”
5. Ensure that the **Safety Risk Balance** is positive (SaFAD)
6. Data engineering relies on **lifecycles** and practices that are very different from software engineering
7. Data plays a key role in the **AI/ML** systems that will power autonomous driving in future vehicles

Continental

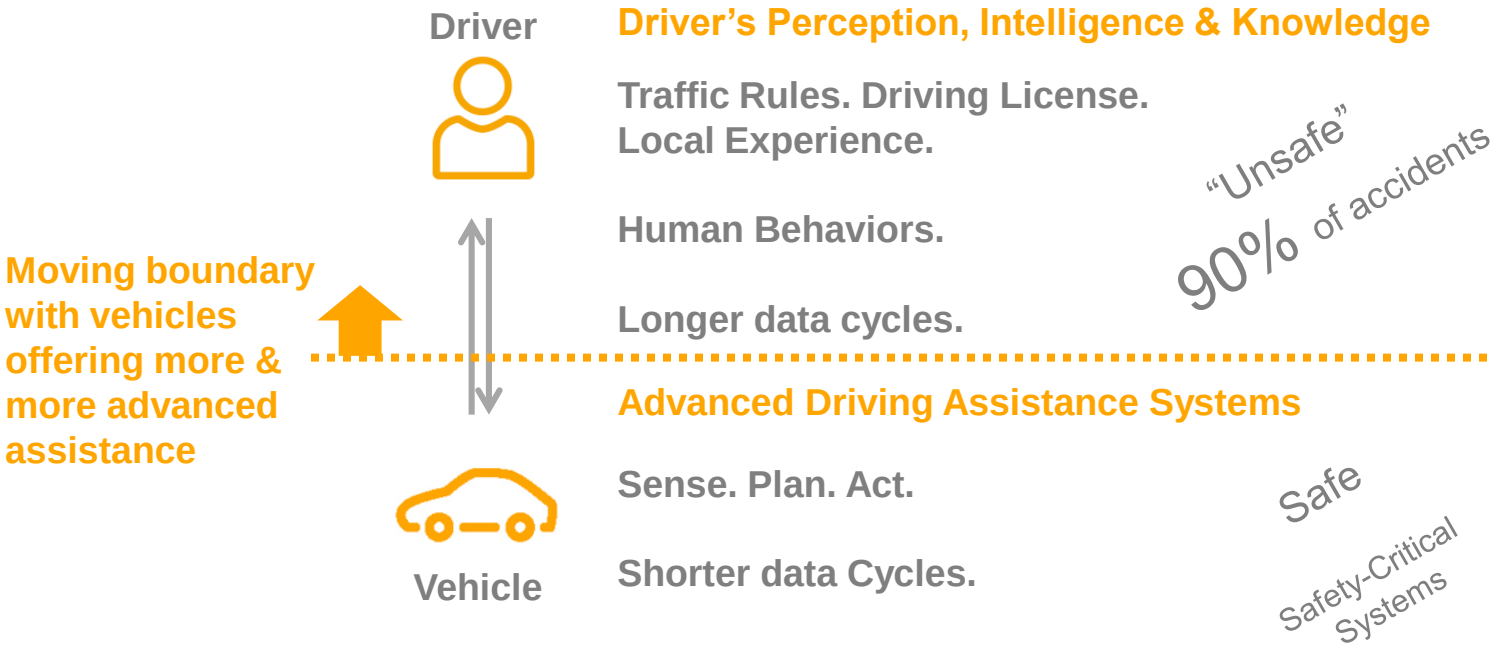
Additional (data-driven) feedback loop



Better Design for next systems.
Improved Governance.



Driving a vehicle involves multiple different information / data lifecycles



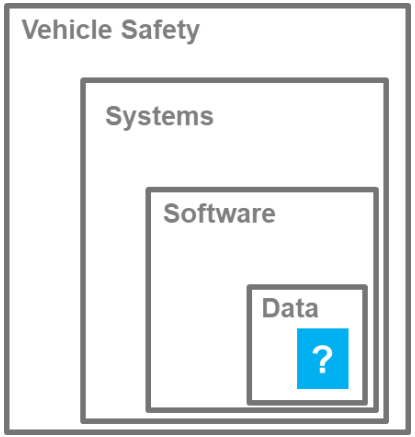
Lifecycles matter!
The “chain of trust” for “Systems Safety”

BUILD

RUN

Development → Tests – Verification – Qualification → Integration → (Certification) → Operations

The System is (certified) Safe



Safety Case at System Level

Software Safety as a part of the System

Data as part of the Software?

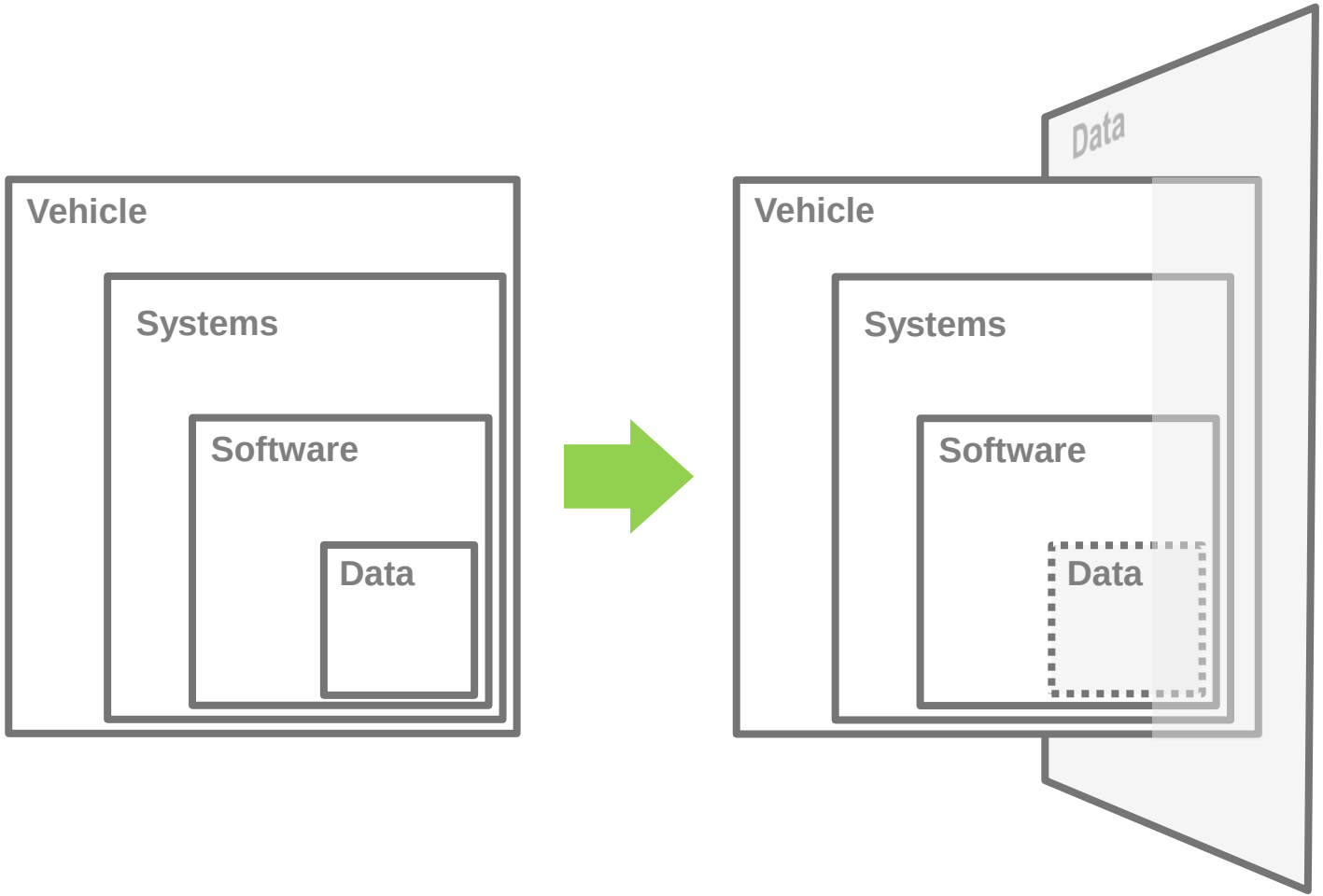
Risks
Faults
Incidents

Continuous Improvement

Data

Data lives here!

Continental


Vehicle
Systems
Software
Data
Data
Vehicle
Systems
Software
Data