How to assure In service Safety for Autonomous Vehicles?

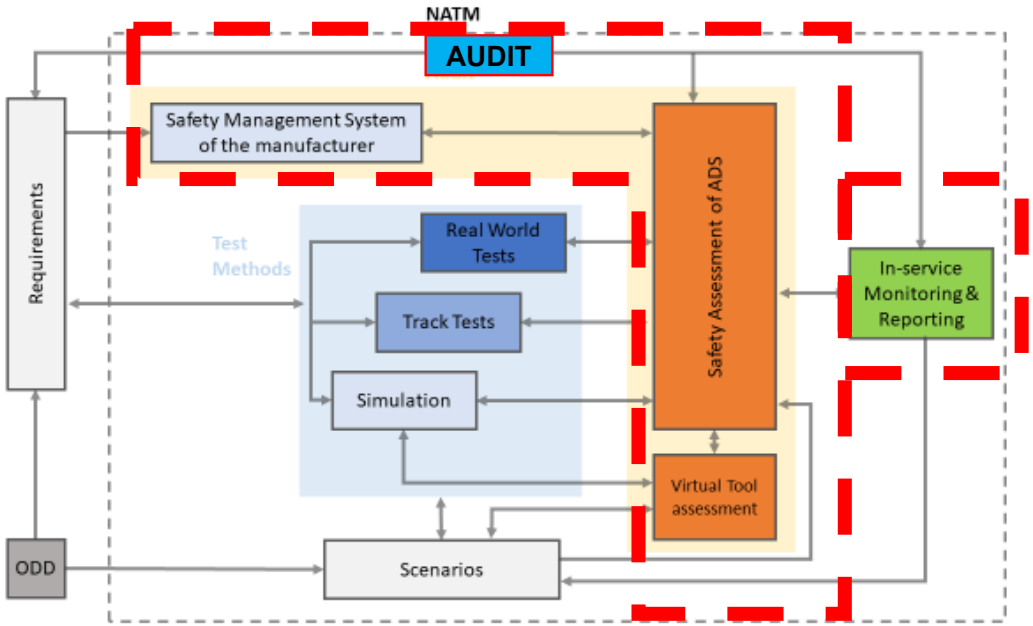
An In-Service Monitoring and Reporting (ISMR) Journey from VMAD SG3

Espedito Rusciano, RDW
VMAD SG3

16/05/2022

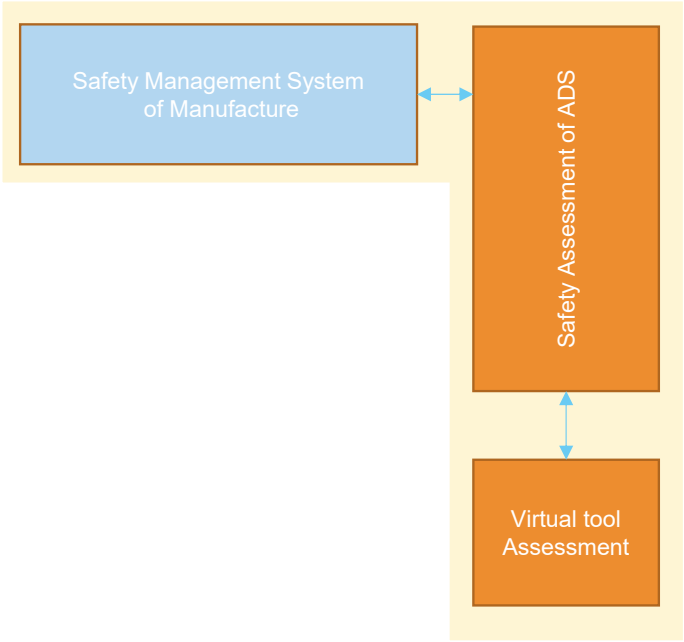
VMAD SG3

- SG3 is a subgroup of VMAD IWG that provides a contribution for the development of the New Assessment/Test Method for automated driving (NATM)
- SG3 activities are focused on two areas: **Audit** and **In-Service Monitoring and Reporting**.



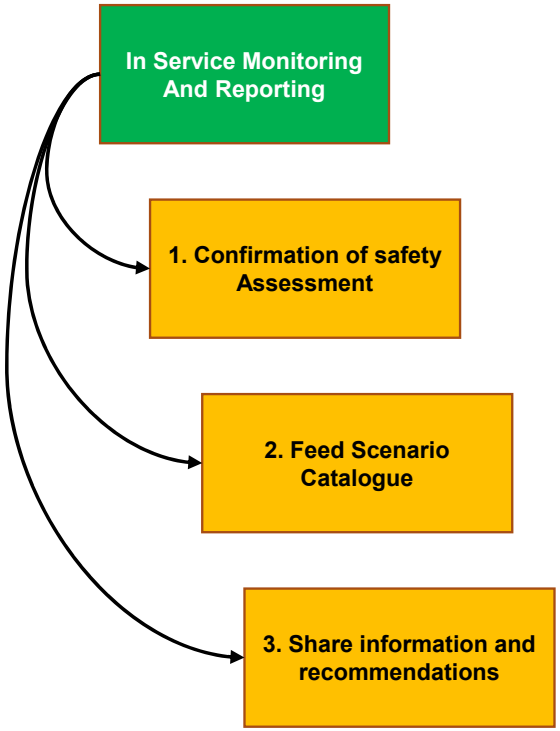
SG3-Audit, Objectives and Deliverables

- To develop ***Audit procedures*** to verify that ADS manufactures have robust processes/mechanisms/strategies (i.e., ***safety management system***) that are in place to ensure the ADS meets the relevant functional requirements throughout the vehicle lifecycle.
- To develop ***Audit/Assessment procedures*** to validate that ADS's hazards and risks have been identified and that a consistent ***safety-by-design concept*** has been put in place
- To develop ***Audit/Assessment procedures*** which establish how manufacturers will be required **to demonstrate** to safety authorities using documentation, their simulation, test-track, and/or real-world testing of **the capabilities of an ADS**.
- To Assure the **complementarity between the different pillars** of the assessment and the overall scenario coverage.

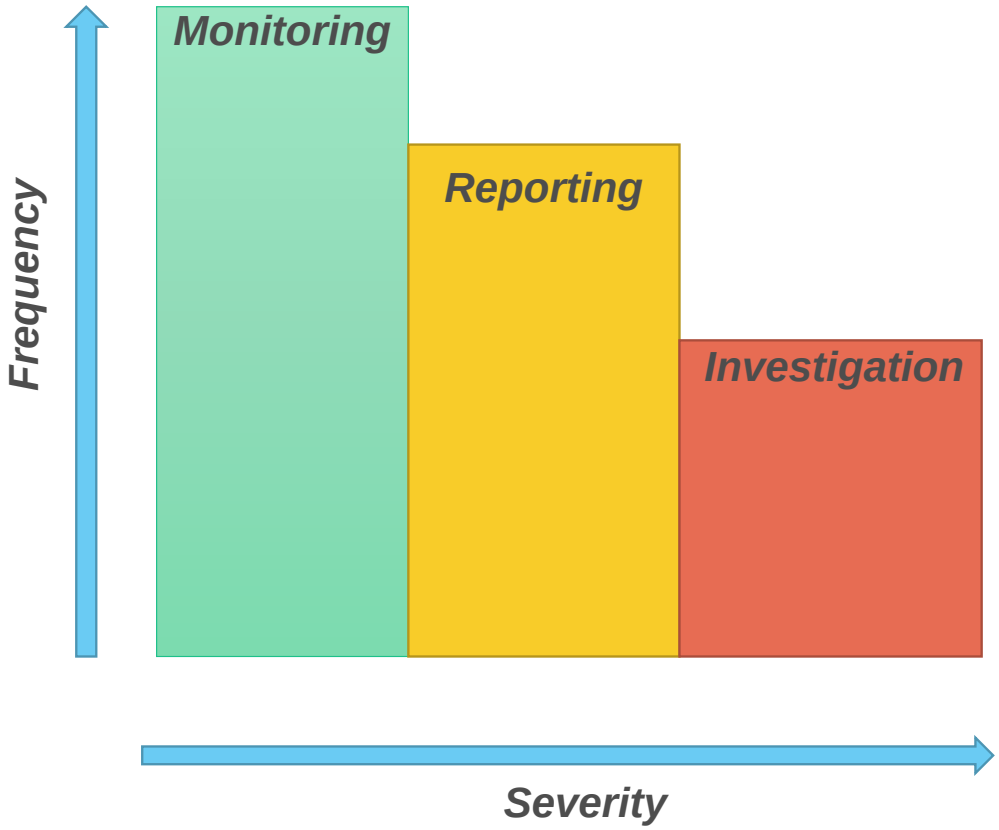


The In-Service Monitoring and Reporting (ISMR)

- In-Service Monitoring and Reporting (ISMR) addresses the ***in-service safety*** of the Autonomous Driving System after its placing on the market (***operational experience feedback loop***)
- It relies on the collection of in-service data(***fleet monitoring***) **to assess** whether the **Autonomous Driving System continues to be safe** when operated on the road and to identify safety risks.
- This data collection can be used for the **identifying new scenarios** not tested during the type approval.
- The data collection can also be used to **improve the testing** methodologies **and interaction** between human and vehicle.
- ISMR allows the whole Autonomous Driving System community to **learn from** major Autonomous Driving System **accidents/incidents** through information sharing, but also to spread the **safety benefit of ADS** on the road.

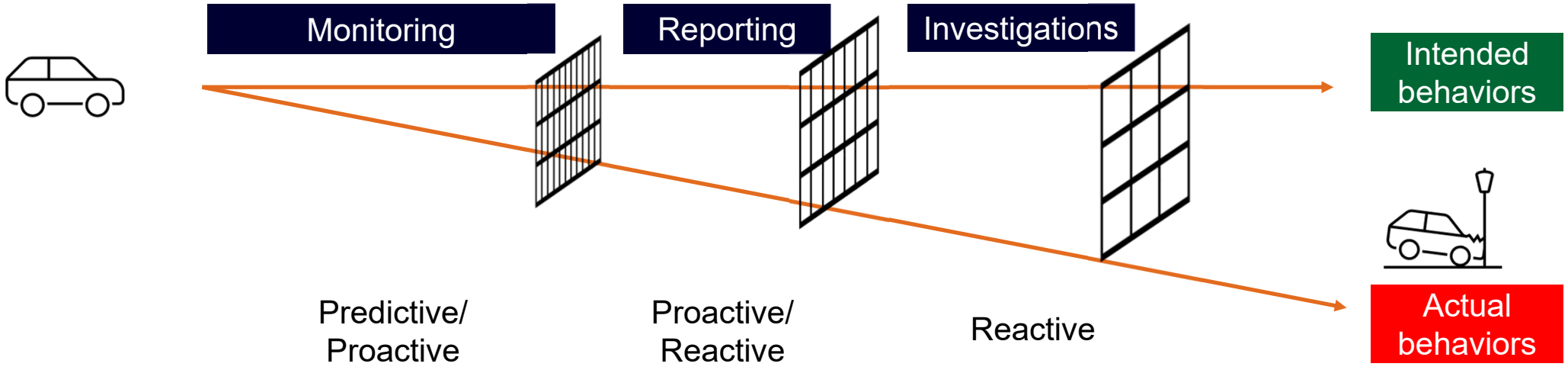


The 3 legs of ISMR



Process	Focus
Monitoring	Overall Data collection and analysis
Reporting	Critical and not critical occurrences
Investigation	Critical occurrences

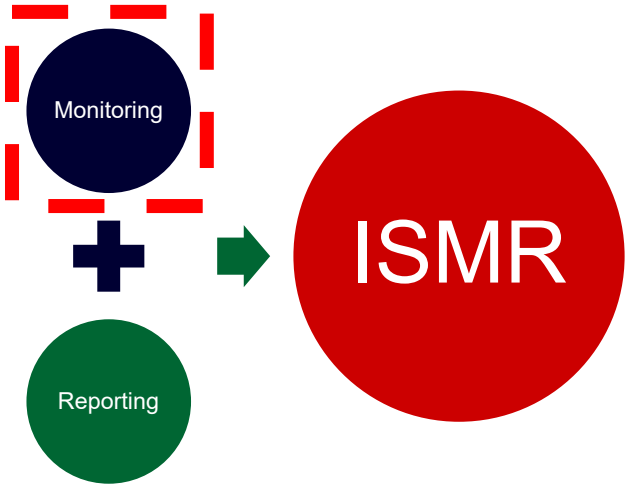
Understanding the 3 legs: Safety management levels



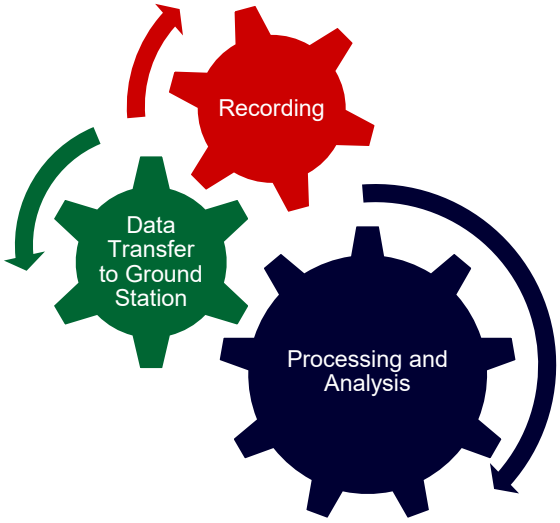
In Service Monitoring

Monitoring*(Link with the AUDIT Pillar):*

- Manufacturers should set up a monitoring program according to the Safety Management System Requirements
- Vehicle data collection and analysis by the manufactures for reporting under ISMR, besides EDR/DSSAD
- Manufacturers are expected to collect data also from other accessible sources of data (e.g., customer reports)

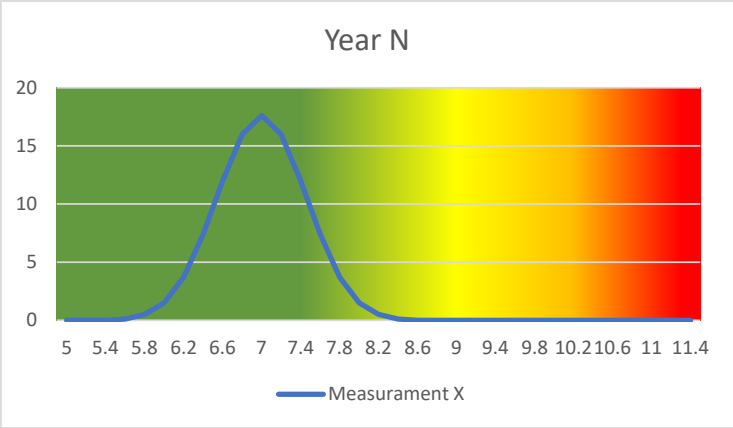


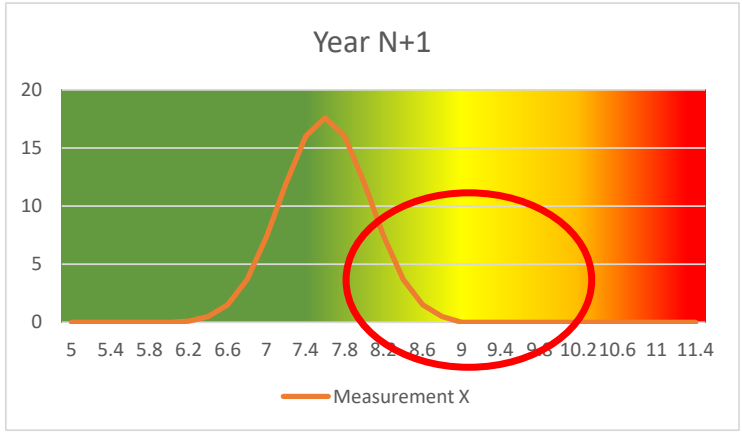
- Predictive and Proactive approach for Safety which shall be integrated in the Safety Management System
- Beyond the scope of the occurrences reporting.
- Increase safety by identifying trends and unusual or unsafe circumstances.



Possible benefit from monitoring

Monitor drifting of safety performance (reduction of margins)





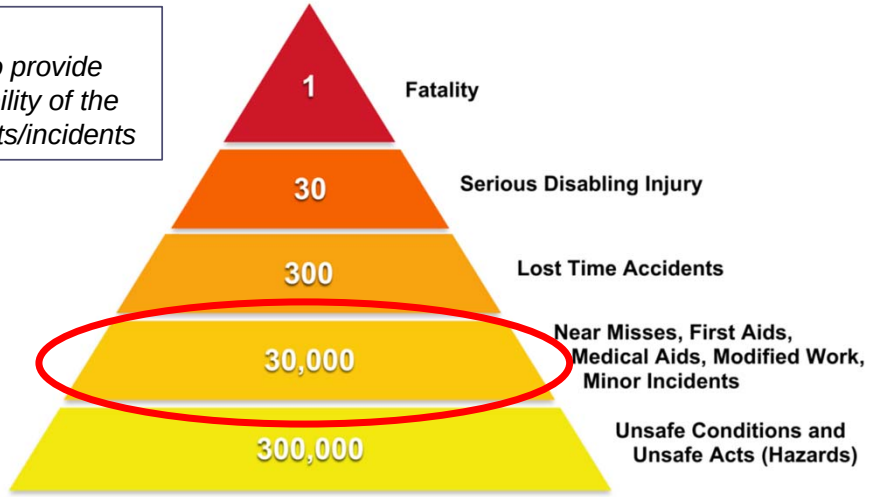
Collection and analysis of Near Misses

"An unplanned event that did not result in injury, illness or damage – but had the potential to do so".

SAFETY PYRAMID

It is far better to be reporting and learning from Near Misses, Minor Incidents and Hazards, where there is little or no loss, than to be reporting actual serious losses.

Note:
Near misses can also provide evidence on the capability of the ADS to prevent accidents/incidents

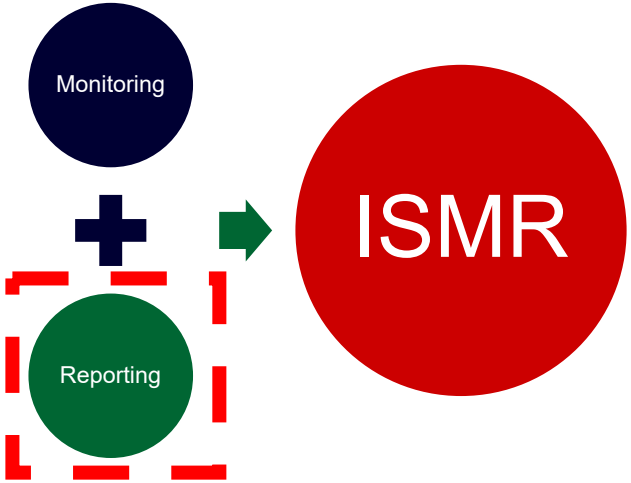


Retrieved from Industrial Accident Prevention, A Scientific Approach, Herbert W. Heinrich 1931.

In Service Reporting

Occurrence Reporting:

- Occurrence refers to any safety-related event involving a vehicle equipped with an Autonomous Driving System.
- Two different categories of occurrences are identified for reporting: critical and not critical occurrences.
- The manufacturer should report, as required by the Authority, on both critical and non-critical occurrences.



The main purpose of in-service reporting is the prevention of accidents and incidents and not to attribute blame or liability. (Just culture)

Types of Reporting

- **Short-term reporting** – occurrences that require the manufacturer to take remedial action when data provides evidence of the Autonomous Driving System posing an unacceptable in-service risk.
  - due within 1 month
  - examples of short-term reporting:
    a. indications of failure to meet safety requirements
    b. critical occurrence where the Autonomous Driving System was involved

- **Periodic reporting** - reporting in the form of aggregated data (per hour of operation or driven km) for Autonomous Driving System-vehicle type and related to Autonomous Driving System operation
  - due at least once a year
  - examples of periodic reporting:
    - no inconsistencies have been detected compared to the safety performance assessed prior to market introduction;
    - the Autonomous Driving System respects the performance requirements set by Regulation
    - all new ADS safety performance issues are addressed

Occurrences list

OCCURRENCE	SHORT-TERM REPORTING [1 Month]	PERIODIC REPORTING [6 Month/1 Year]
1.a. Safety critical occurrences known to the Autonomous Driving System manufacturer or OEM	X	X
1.b. Occurrences related to Autonomous Driving System operation outside its ODD	X	X
1.c. Autonomous Driving System failure to achieve a minimal risk condition when necessary	X	X
1.d. Communication-related occurrences		X
1.e. Cybersecurity-related occurrences		X
1.f. Interaction with remote operator if applicable		X
2.a. Driver unavailability (where applicable) and other user-related occurrences		X
2.b. Occurrences related to Transfer of Control failure		X
2.c. Prevention of takeover under unsafe conditions		X
3.a. Occurrences related Autonomous Driving System failure		X
3.b. Maintenance and repair problems		X
3.c. Occurrences related to unauthorized modifications		X
3.d. Modifications made by the Autonomous Driving System manufacturer or OEM to address an identified and significant Autonomous Driving System safety issue		X
4. Occurrences related to the identification of new safety-relevant scenarios	X	X

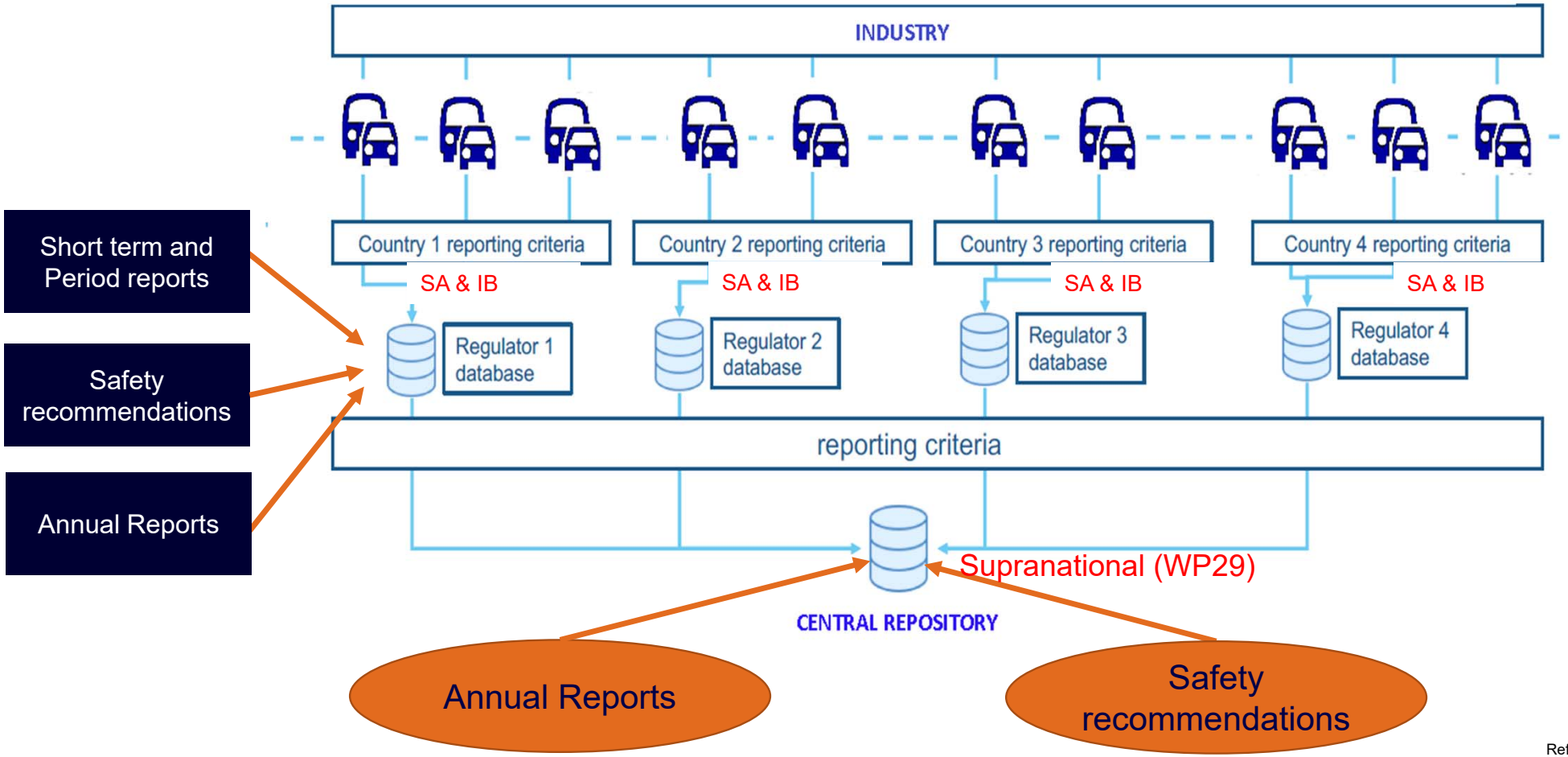
Investigation

Occurrence Investigations

- ***Focus on critical occurrences***, but it can include also other occurrences
- It is expected an immediate notification to the authority on occurrences which can pose an immediate risk to public safety.
- An ***Independent body*** conducts investigations according to its mandate
- The ***investigation report***, containing where appropriate ***safety recommendations***, should be made available to all parties involved in the shortest possible time.

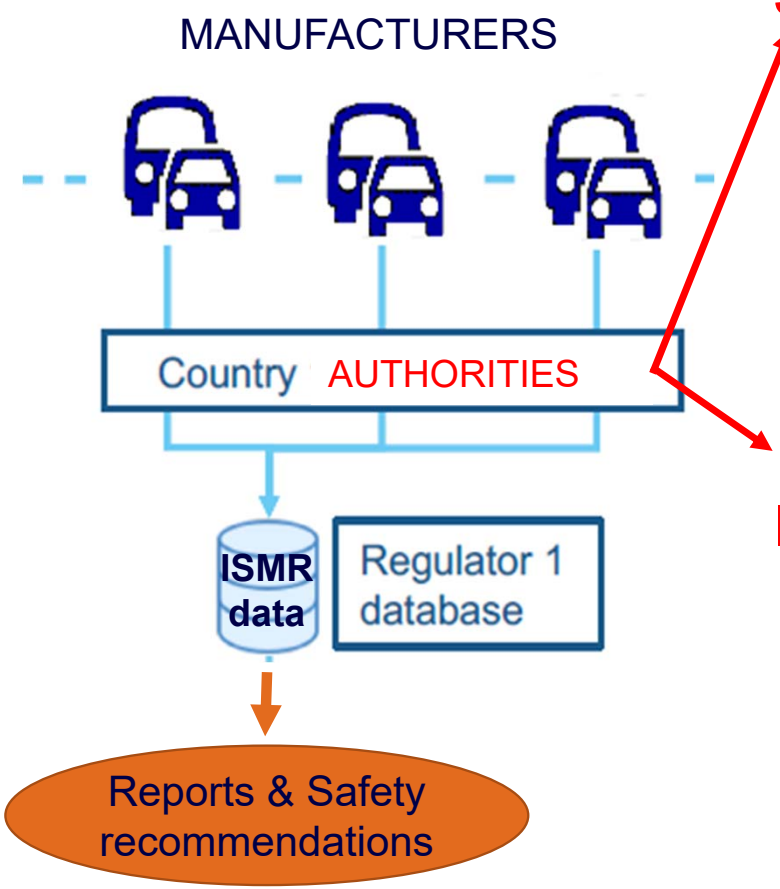
The main purpose is the safety investigations of accidents and serious incidents to prevent future occurrences

ISMR Framework



Ref: Validation Methods for Automated Driving Systems (UNECE/WP29/GRVA/VMAD)

ISMR Roles and responsibilities



Safety Authority (SA)

- Can be the (Approval) Authority or not; if not, it gives recommendations to the (Approval) Authority
- Responsible for ISMR data management at national level
- Derives safety recommendations and shares them at higher level
- Publish annual report summarizing the level of Autonomous Driving System safety.

Investigation Body (IB)

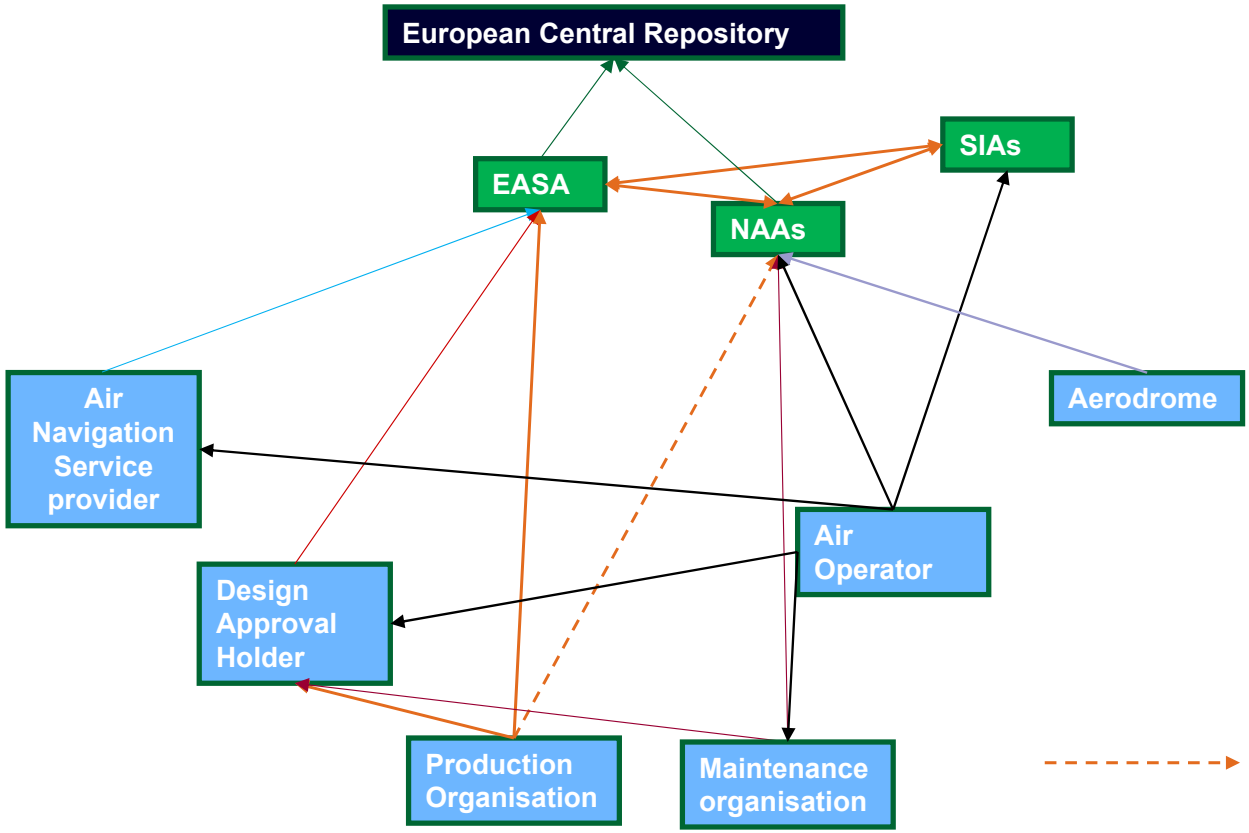
- Independent/impartial body, investigates occurrences
- Issue an investigation report including (where applicable) safety recommendations
- Provides an Annual report with evidence of investigations

Ref: Validation Methods for Automated Driving Systems (UNECE/WP29/GRVA/VMAD)

Reporting from other sources

- Limiting the reporting requirements to manufacturers will also limit the amount and type of information covered by ISMR, with a strong impact on the achievable safety improvement.
- E.g. identification of traffic rules infringement is not possible through data collected on-board the vehicle, and reporting by local authorities and Autonomous Driving System vehicle users is needed.
- Other transport sectors extend the operational reporting mechanism also to drivers, operators, users, traffic managers, and any other person connected to the vehicle operation.

A more comprehensive approach to ISMR is needed
(example from aviation sector)



A "Total System Approach" increase the overall level of Safety

Simplified version (not all actors are included) of the European approach to ISMR, adapted from EASA

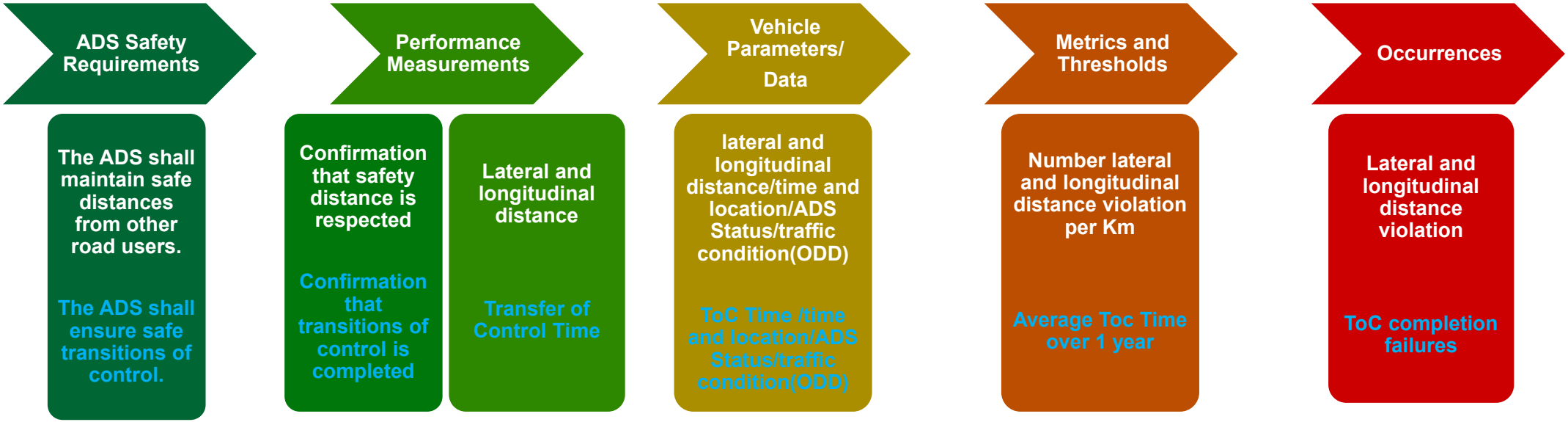
Information Sharing & Protection

- The final aim of ISMR is to improve Autonomous Driving System safety through dissemination of lessons learned
- A broader exchange of information and the dissemination of safety recommendations should be ensured among the Contracting Parties/Authorities, at international level
- Data collection should ensure confidentiality, the protection of its source
- Sensitive safety information should be protected by preventing its use for purposes other than safety.

Guiding principles

- Safety Authorities must set up a confidential reporting scheme and to ensure that no personal details are ever recorded in the databases both at national/international level.
- Access to the database for the authorities
- Safety Recommendations publicly accessible

Next Steps: Performance, Occurrence and Data



Thanks for your Attentions