

An HMI Personalization Concept for Increasing Safety of the Intended Functionality



Sahoo Swagat Sukumar, **Barbara Gallina**, Soheila Sheikh-Bahaei
barbara.gallina@mdu.se

Supported by: **Software Center** | **Continuous Digitalization**

#49-∞COMPASS – **Continuous** Regulatory **Compliance** and **Assurance** of Socio-technical Systems
#60-TSF-Towards a Sustainable Future

- **Context and motivation**
- **Background**
- **HMI Personalization Concept**
- **Related work**
- **Conclusion and Future work**



SAE J3016™ LEVELS OF DRIVING AUTOMATION™

Learn more here: [sae.org/standards/content/j3016_202104](https://www.sae.org/standards/content/j3016_202104)

Adapted from https://brx-content.fullsight.org/site/binaries/content/assets/sae-org/content/news/blog/sae-j3016-visual-chart_5.3.21.pdf

Copyright © 2021 SAE International. The summary table may be freely copied and distributed AS-IS provided that SAE International is acknowledged as the source of the content.



Driver in the loop...

Technical Context: Software-defined vehicles are taking shape

- continuous value creation model
- consumer value realized in software
- preventive maintenance
- personalization
 - personalised measure of driving risk

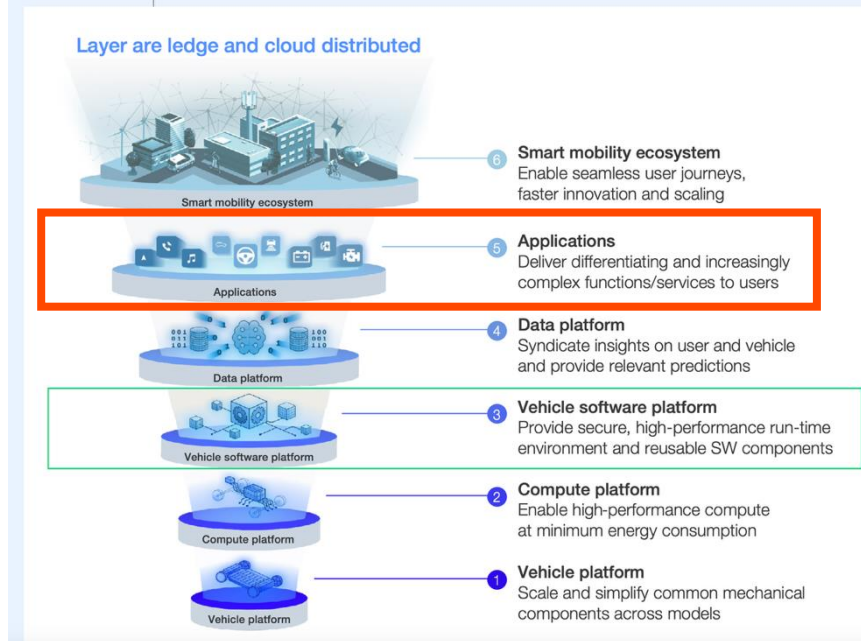
ADAS -Advanced Driver Assistance System

Several ADAS are mandatory

The driver must constantly supervise these systems and must be ready to steer, brake or accelerate as needed to maintain safety, at any moment during the drive



FIGURE 1 | Six layers of the software-defined vehicle



Taken from: https://www3.weforum.org/docs/WEF_Unlocking_Safety_and_Innovation_in_Vehicle_Software_2023.pdf



- **Moving Off Information System (MOIS)**
- **Blind Spot Information System (BSIS)**
- **Reversing Detection System (REV)**
- **Intelligent Speed Assist (ISA)**
- **Driver Drowsiness and Alertness Warning (DDAW)**
- **Tire Pressure Monitoring System (TPMS)**
- **Emergency Stop Signal (ESS)**
- **Alcohol Interlock Installation Facilitation (ALC)**

Since July 2024, mandatory for trucks and buses

In-vehicle Operational Context



Information signals
Collision signals



An ADAS may function as intended...
Functional Safety (ISO 26262) demonstrated!

Adapted from <https://www.wikihow.com/Drive-a-Stick-Shift-Truck#/media:Drive-a-Stick-Shift-Truck-Step-16.jpg>



Information signals

Collision signals

->intrusivness matters!



Perception matters!

Cognition matters!

Motorics matters!

Human variability matters!

if the functionality is underspecified
from a **foreseeable misuse** perspective →

misunderstanding

delayed response

nuisance-driven mistrust



Safety Of The Intended Functionality is undermined

Background

- **Moving Off Information System (MOIS)**
- **Human Machine Interface (HMI) and Interaction**
- **Safety Of The Intended Functionality (SOTIF)**
- **Human variability**

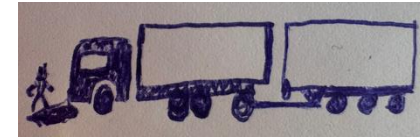


UN Regulation No. 159

Uniform provisions concerning the approval of motor vehicles with regard to the Moving Off Information System for the Detection of Pedestrians and Cyclists

MOIS - detects and informs the driver of the presence of VRU in the close-proximity forward blind-spot of the vehicle and, if deemed necessary based on manufacturer strategy, warn the driver of a potential collision.

→ timely and correct driver response



**VRU- Vulnerable Road User
pedestrians and cyclists
Children/Adults**

N2	Vehicles used for the carriage of goods and having a maximum mass exceeding 3.5 tonnes but not exceeding 12 tonnes.
N3	Vehicles used for the carriage of goods and having a maximum mass exceeding 12 tonnes.
M2	Vehicles used for the carriage of passengers, comprising more than eight seats in addition to the driver's seat, and having a maximum mass not exceeding 5 tonnes.
M3	Vehicles used for the carriage of passengers, comprising more than eight seats in addition to the driver's seat, and having a maximum mass exceeding 5 tonnes.



UN Regulation No. 159

Uniform provisions concerning the approval of motor vehicles with regard to the Moving Off Information System for the Detection of Pedestrians and Cyclists



Information signal (low intrusion), optical signal only

Collision signal (high intrusion), at least two signal modes selected from an optical signal, acoustic signal or haptic signal (optical signal shall be different from information signal)

Underspecified HMI behavior and Interaction can lead to

- *misunderstanding,*
- *delayed response, or*
- *nuisance-driven mistrust → disuse*

H. Eom and S. H. Lee, “Mode confusion of human–machine interfaces for automated vehicles,” *Journal of Computational Design and Engineering*, vol. 9, no. 5, pp. 1995–2009, 2022.

J. Li, Y. He, S. Yin, and L. Liu, “Effects of automation transparency on trust: Evaluating HMI in the context of fully autonomous driving,” in *Proceedings of the 15th International Conference on Automotive User Interfaces and Interactive Vehicular Applications (AutomotiveUI '23)*, pp. 1–16, ACM, 2023.

HMI and Interaction: lightining, icon, sound, etc., design

...how the light source interacts with the observer

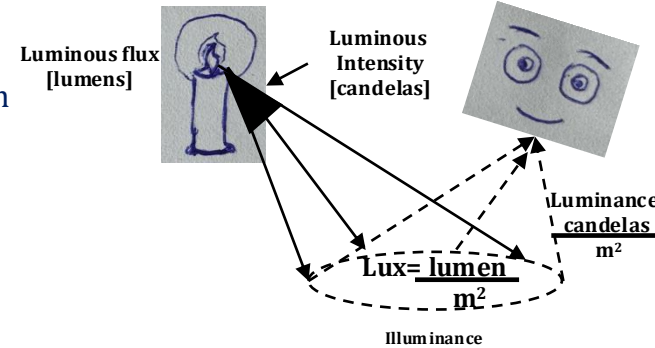
Luminance, i.e., power of light radiation emitted by a light source in a specific direction

...as the **icon size** increases, perception time decreases...

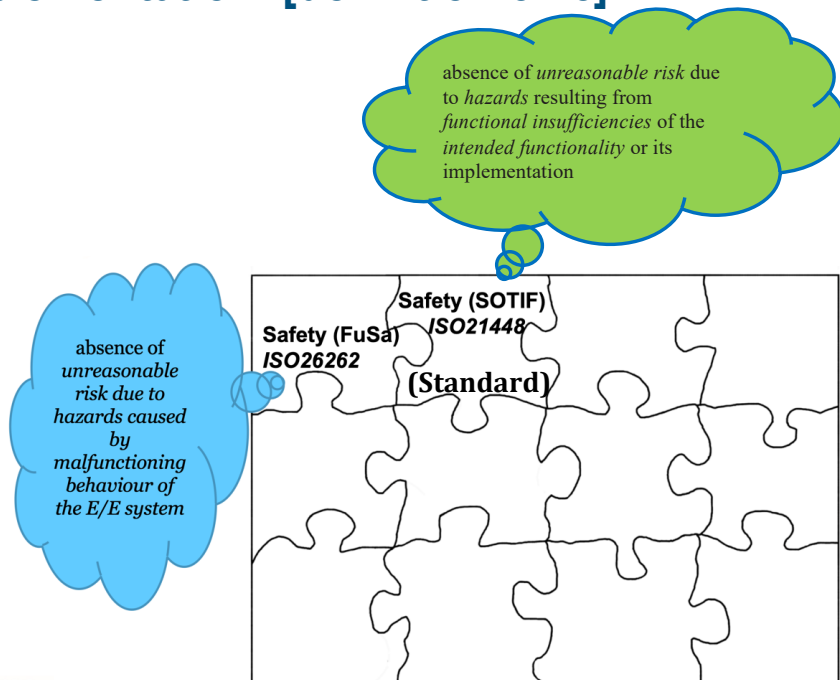
...**acoustic-based warning** may reduce response time

Startle reflex i.e., neuromuscular body reaction to intense stimuli

...different cues can be considered



Absence of unreasonable **risk** due to hazards resulting from **functional insufficiencies** of the intended functionality or its implementation. [definition 3.25]



Digression: ASIL-Palette for Functional Safety (FuSa) ISO 26262:2018

Risk = combination of the probability of occurrence of harm and the severity of that harm. [definition 3.23]

Harm “Physical injury or damage to the health of persons”

Probability of occurrence is a function of E and C →

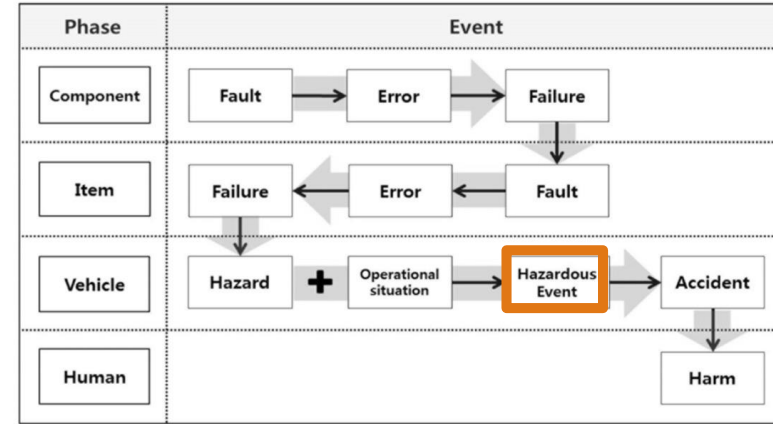
$$R=f(S, E, C)$$



S= severity – the potential severity of the resulting harm

E=probability of exposure considers how frequent and for how long the vehicle is in an operational situation that can be hazardous if coincident with the failure mode under analysis

C= controllability – the ability to avoid harm by the driver



[Source: Jang, Hyeon Ae et al. “A Study on Situation Analysis for ASIL Determination.” (2014)]

FuSa : focus on malfunctions

Driving factors and scenarios	Class of controllability (see Table 3)			
	C0	C1	C2	C3
	Controllable in general	99 % or more of all drivers or other traffic participants are usually able to avoid harm	90 % or more of all drivers or other traffic participants are usually able to avoid harm	Less than 90 % of all drivers or other traffic participants are usually able, or barely able, to avoid harm

	Class of severity (see Table 1)			
	S0	S1	S2	S3
Reference for single injuries (from AIS scale)	AIS 0 and less than 10 % probability of AIS 1-6	More than 10 % probability of AIS 1-6 (and not S2 or S3)	More than 10 % probability of AIS 3-6 (and not S3)	More than 10 % probability of AIS 5-6
Damage that cannot be classified safety-related				

functional insufficiency *insufficiency of specification or performance insufficiency*

insufficiency of specification

specification, possibly incomplete, contributing to either a hazardous behaviour or an inability to prevent or detect and mitigate a reasonably foreseeable indirect *misuse* when activated by one or more *triggering conditions*

performance insufficiency

limitation of the technical capability contributing to a hazardous behaviour or inability to prevent or detect and mitigate reasonably foreseeable indirect *misuse* when activated by one or more *triggering conditions*

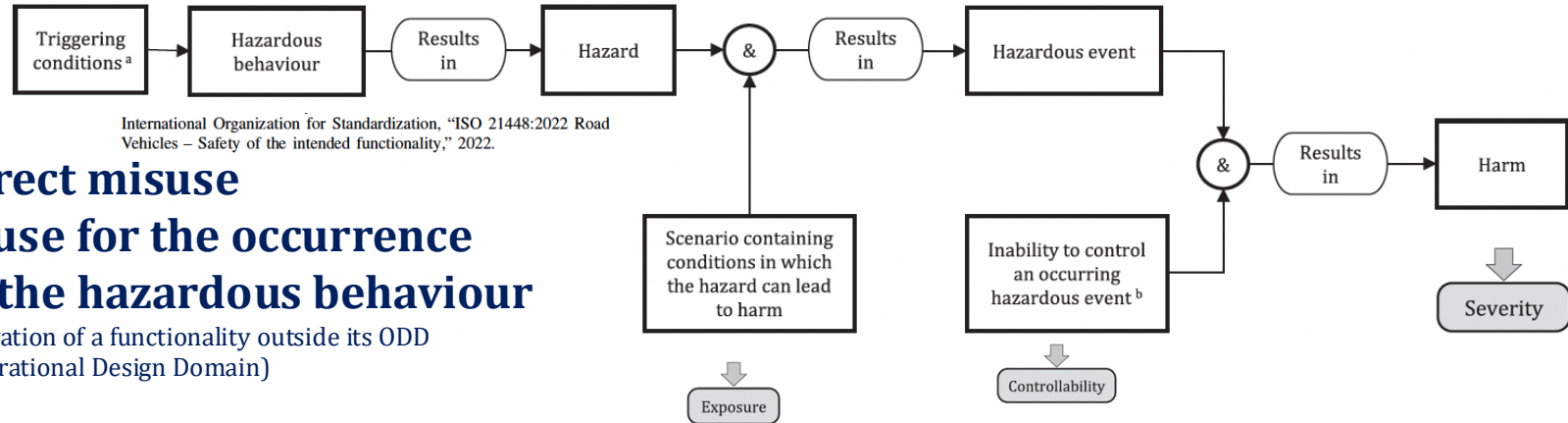
triggering condition

specific condition of a *scenario* that serves as an **initiator for a subsequent system reaction** contributing to either a hazardous behaviour or an inability to prevent or detect and mitigate a **reasonably foreseeable indirect misuse**

misuse

usage in a way not intended by the manufacturer or the service provider

Depending on the causal relationship to the hazardous behaviour, there are two kinds of misuse: **direct** and **indirect**



Direct misuse cause for the occurrence of the hazardous behaviour

Activation of a functionality outside its ODD
(Operational Design Domain)

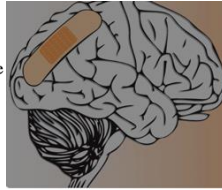
Indirect misuse ..leads to reduced controllability or increased severity

Inattentive driver
Driver misunderstanding
(confusion mode)
Complacency
Physical / Mental conditions



Safety of the Intended Functionality: What about Mental Harm?

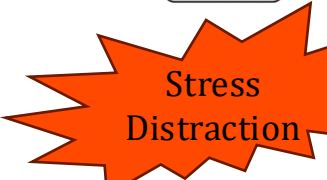
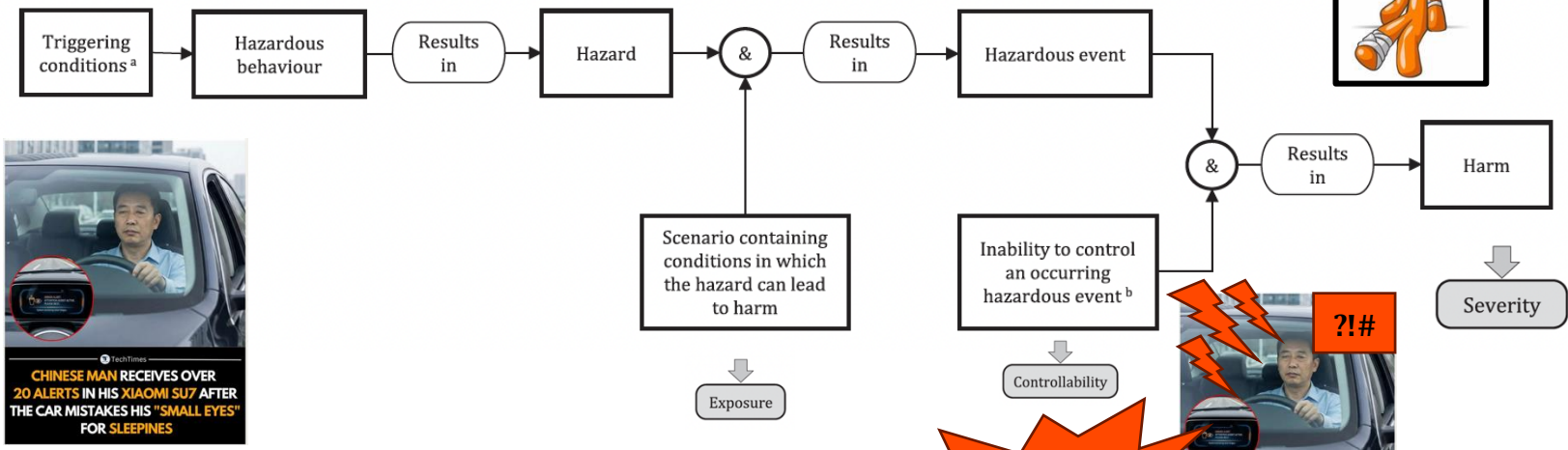
Barbara Gallina
Mälardalen University, Västerås, Sweden, Email: barbara.gallina@mdu.se



<https://www.youtube.com/watch?v=ojvwQp3n0>

A Physiology-based Driver Readiness Estimation Model for Tuning ISO 26262 Controllability

Moses Mariageoph¹, Barbara Gallina¹, Marco Carli² and Daniele Bibbo³
¹Department of Engineering, Roma Tre University, Rome, Italy,
moses.mariageoph@uniroma3.it, marco.carli@uniroma3.it, daniele.bibbo@uniroma3.it
³School of Innovation, Design and Engineering, Mälardalen University, Västerås, Sweden, barbara.gallina@mdu.se



Source https://www.linkedin.com/posts/avad-a-99448179_a-chinese-man-reportedly-received-over-20-activity-7426512382195048448-QVsj/

Driver capabilities may vary and change over time

- **sensory variability**
- **temporary cognitive conditions affecting attention**
- **workload**
- **...**

This variability may lead to foreseeable misuse!

Solution Proposal

The concept is structured around

- **fixed regulatory guardrails,**
- **a banded personalisation policy, and**
- **measurable verification hooks that link SOTIF relevant claims to evidence without processing personal data**

- **Activation and Operational Design Domain**
 - moving-off from rest/straight-ahead at very low speed
 - speed limit (10 km/h)
 - illuminance gate (>15 lx)
- **Detection zone**
 - close-proximity zone geometry
 - target classes
- **Availability and fail-safe behaviour:**
 - self-check
 - contamination/failure handling
 - unavailability indication
- **Telltale semantics**
 - information warning,
 - collision warning (if present), and
 - unavailable/failure states

- Use of only **coarse, non-identifying bands** (optionally enabled) and always supports a safe default
 - sensory band (default/vision-reduced/hearing-reduced/unknown),
 - workload band (low/normal/high based on an OEM proxy or test condition),
 - seat-to-display distance band (short/medium/long for legibility scaling)
 - optional cabin noise band (low/high to avoid ineffective modalities)outputs restricted to presentation tuning, e.g., icon size within legibility limits

- Practical engineering targets that make the HMI testable
 - **contrast ratio** $\geq 4.5 : 1$ (day) and $\geq 7 : 1$ (night/glare)
 - **luminance bounded** to avoid
 - being too dim to miss or
 - too bright to distract
 - **legibility geometry** based on minimum visual angle at typical viewing distances
 - stroke 7 arc-min
 - icon height 20 arc-min at 60–90 cm
 - **temporal behaviour** consistent with information signalling
 - steady icon
 - controlled dwell 150–350 ms
 - no flashing
 - no urgent cues on the central information display

- **Glance behaviour metrics to**
 - limit long off-road glances
 - ensure total off-road time does not increase beyond an acceptable margin
 - example gate: total off-road time within +5 percentage of baseline, and no single off-road glance exceeding a predefined limit
- **Startle & confusion checks to avoid abrupt warning escalation & misinterpretation**
 - example: avoid sudden audio level jumps (if warning audio exists)
- **Tone/icon confusion below a defined threshold across cohorts**
 - example gate: less than 5% confusion rate

- **SOTIF claim is linked to:**
 - **a measurable evaluation hook**
 - **a concrete evidence artifact**

SOTIF claim	What we measure	Acceptance gate (example)	Evidence source
Information is noticed without distraction	Eye glance behavior	No single off-road glance exceeds limit; total off-road time non-inferior to baseline	Eye-tracking report
Information is understood	Interpretation / confusion	Confusion rate below threshold across cohorts	HF comprehension study
Information is non-intrusive	Startle/annoyance + subjective workload	Startle score below threshold; workload not increased	HF startle + workload report
No false trust when unavailable	Unavailable indicator behavior	Unavailable is visible and consistent when operation is not guaranteed	Test report + HMI log
Timing supports meaningful reaction	End-to-end latency distribution	Latency meets defined percentile targets	Latency histogram report
Personalisation does not change function	Guardrail compliance check	Zone/speed/availability behavior unchanged across modes	Requirements + test evidence
Privacy preserved	Data handling	Only banded profiles; no identifiers stored	Privacy design note

- **Evaluation combines:**
 - **simulator studies** (e.g., age-stratified cohorts and dual-task conditions)
 - **vehicle tests** addressing zone coverage, illumination boundary conditions, and contamination triggered unavailability
- **Measurements include**
 - **photometric and geometry checks** for non-intrusiveness and **attention metrics** via eye-tracking or equivalent instrumentation
- **Evidence artifacts are kept lightweight and auditable**

- **coarse banding is simple and cannot represent all individual differences**
--> conservative defaults, stability rules, and fallbacks
are needed when band information is missing or contradictory
- **simulator evidence may not fully transfer to on road operation**, where workload, stress, and risk perception differ
--> controlled field validation (e.g., track trials or limited fleet pilots) is needed
- **personalization can unintentionally create nuisance or inconsistency**; repeated nonhelpful cues may reduce trust and increase delayed reactions or manual deactivation
→ the evidence strategy shall include attention-related metrics and acceptance indicators, not only technical compliance checks

- **Generalisability** – potentially generalisable to other driver-in-the-loop-items
 - Key reusable element: separation of what is tunable from what is not
 - Evidence-based verification that the presentation remains
 - non-intrusive,
 - understandable
 - attention-compatible
 - timely
- **Initial drivers' feedback:**
 - HMI effectiveness depends not only on correct function, but also on how information is presented under real workload

- **Exploration of evolution of HMIs, effects of proper HMIs design on user experience and functional safety and security..SOTIF is not in focus**

I. Grobelna, D. Mailland, and M. Horwat, "Design of Automotive HMI: New Challenges in Enhancing User Experience, Safety, and Security," Applied Sciences, vol. 15, no. 10, p. 5572, 2025.

- **Review of adaptive HMIs →personalisation →safety, user experience, inclusiveness**

L. Wirtz, E. Sever, and L. Eckstein, "Adaptive Human-Machine Interfaces and Inclusivity in the Automotive Field: A Review," Accessibility, Assistive Technology and Digital Environments, vol. 121, 2024.

- **Comparative study on HMIs →personalisation →right amount at the right time**

F. Hartwich, C. Hollander, D. Johannmeyer, and J. F. Krems, "Improving Passenger Experience and Trust in Automated Vehicles Through User-Adaptive HMIs: "The More the Better" Does Not Apply to Everyone," Frontiers in Human Dynamics, vol. 3, 2021.

- **A practical, auditable, privacy-preserving, SOTIF-oriented, regulatory-guardrailed HMI personalisation concept for MOIS**
 - **presentation-focused parameters only**
 - **ISO 26262:2018 and ISO 21448:2022 compliance**
- **Refinement and validation of the evidence**
 - **provision of detailed ISO 21448:2022-compliant artifacts**
 - **structured experimental studies and practical demonstrations.**
 - **confirmation of the proposed presentation bounds and attention safeguards with representative driver cohorts**
 - **complementary simulator-based results with limited field validation to assess transferability under real operating conditions**
- **Ontology-based approach for assurance and compliance demonstration**
- **Deeper personalisation**

Hope it was interesting!
Thank you very much for your attention!

#49-∞COMPASS – Continuous Regulatory Compliance and Assurance of Socio-technical Systems
#60-TSF-Towards a Sustainable Future



e-mail: barbara.gallina@mdu.se