Standardisation State-of-the-Art and Analysis of Gaps

Deliverable	**Standardisation State-of-the-Art and Analysis of Gaps**		
Deliverable File	**D7.8**		
Project	Cynergy4MIE	**Grant Agreement Number**	101140226
Lead Beneficiary	CONV	**Dissemination Level**	Public
Involved SC's	SC1-SC2-SC3-SC4-SC5-SC6	**Related Task/s**	T7.4
Due Date	M12	**Actual Submission Date**	12
Status	Final	**Version**	1
Contact Person	Panagiota Kokoliou	**Organisation**	CONV

Document history			
V	**Date**	**Author**	**Description**
0.1	20.06.2025	Panagiota Kokoliou	ToT Draft Version
0.2	07.07.2025	Panagiota Kokoliou	ToT Final Version (after partners feedback)
0.3	31.07.2025	Panagiota Kokoliou	Initial Version
0.4	07.08.2025	Sami Dahlman	Intralogistics Platform
0.5	14.08.2025	Panagiota Kokoliou	Draft Version

0.6	21.08.2025	Fabio Corona	Review
1.0	26.08.2025	Panagiota Kokoliou	Final Version

Acknowledgement

The Cynergy4MIE project is supported by the Chips Joint Undertaking and its members, including the top-up funding by National Authorities under Grant Agreement No 101140226.

Disclaimer

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or National Authorities. Neither the European Union nor the granting authority can be held responsible for them. (Art. 17.3 of the GA).

Table of Contents

Executive Summary ... 7

List of Acronyms and Abbreviations ... 10

1. Introduction ... 13

1.1 Purpose of this deliverable ... 13

1.2 Scope and Relevance for Cynergy4MIE ... 13

1.3 Methodology and Data Collection Approach ... 14

1.4 Intralogistics as a reference domain for standardisation analysis ... 16

1.4.1 Intralogistics standards landscape ... 18

1.4.2 Key standardisation bodies in Intralogistics ... 19

1.4.3 Key standards in intralogistics domain ... 21

1.4.4 Intralogistics Standardisation Gaps and Challenges ... 29

2. Standardisation Landscape Overview ... 30

2.1 International and European Standardisation Ecosystem ... 30

2.1.0 What Are Cyber-Physical Systems (CPS)? ... 30

2.1.1 Global Standardisation: ISO, IEC, and ITU ... 30

2.1.2 European Standardisation Bodies: CEN, CENELEC, and ETSI ... 30

2.2 Certification and Homologation, Pathways ... 31

2.2.1 Cross cutting foundations ... 31

2.2.1.1 Scope and terminology ... 31

2.2.1.2 EU legal backbone and international fora ... 31

2.2.1.3 Standards common to several Supply Chains ... 32

2.2.1.4 Evidence package template and stage gate criteria ... 32

2.2.1.5 Ethics and societal guardrails common to all Supply Chains ... 32

2.2.2 SC1 Off road autonomous machines ... 32

2.2.2.1 Scope and operational context ... 32

2.2.2.2 Mandatory route to conformity and market entry ... 32

2.2.2.3 Voluntary schemes and state of the art ... 33

2.2.2.4 Conformity assessment steps and artefacts ... 33

2.2.3 SC2 Collaborative robots ... 34

2.2.4 SC3 Electric powertrain and components ... 35

2.2.5 SC4 ADAS and ADS with V2X 36
2.2.6 SC5 Multi agent emergency response 38
2.2.7 SC6 Hydrogen and WBG based energy systems 39
2.2.8 Comparative view and system integration 40
2.2.9 Roadmap for pre normative action 42
2.3 Human-Centric and Ethical Standardisation Trends 43
2.3.1 Emerging Trends in Ethical AI Standardisation (ISO, IEEE, OECD, EU AI Act, HLEG) 43
2.3.2 Diversity, Equity and Inclusion (DEI) in AI Standardisation: Fairness, Accessibility & Bias Mitigation 44
3. SC1 – Automated Machinery and Transportation 46
3.1 Description of SC and its Scope in Cynergy4MIE 46
3.2 Existing Relevant Standards and Regulations 46
3.3 Standardisation Usage and Insights from Technical Partners – SC1 47
3.4 Gap Analysis 48
3.5 Strategic Gap: Absence of Specific Contributions to Standardisation Bodies 49
4. SC2 – Smart Collaborative Robotics 49
4.1 Description of SC and its Scope in Cynergy4MIE 49
4.2 Existing Relevant Standards and Regulations 50
4.3 Standardisation Usage and Insights from Technical Partners – SC2 52
4.4 Gap Analysis 52
4.5 Strategic Gap: Absence of Specific Contributions to Standardisation Bodies 53
5. SC3 – Powertrains 55
5.1 Description of SC and its Scope in Cynergy4MIE 55
5.2 Existing Relevant Standards and Regulations 55
5.3 Standardisation Usage and Insights from Technical Partners – SC3 56
5.4 Gap Analysis 57
5.5 Strategic Gap: Absence of Specific Contributions to Standardisation Bodies 58
6. SC4 – Automated Driving Systems 60
6.1 Description of SC and its Scope in Cynergy4MIE 60
6.2 Existing Relevant Standards and Regulations 61
6.3 Standardisation Usage and Insights from Technical Partners – SC4 63

6.4 Gap Analysis 64
6.5 Strategic Gap: Absence of Specific Contributions to Standardisation Bodies – SC4 . 65
7. SC5 – Multi-Agent Sensing and Control 67
7.1 Description of SC and its Scope in Cynergy4MIE 67
7.2 Existing Relevant Standards and Regulations 68
7.3 Standardisation Usage and Insights from Technical Partners – SC5 69
7.4 Gap Analysis 70
7.5 Strategic Gap: Absence of Specific Contributions to Standardisation Bodies 71
8. SC6 – ECS for Energy Efficiency and Distributed Intelligent Control 73
8.1 Description of SC and its Scope in Cynergy4MIE 73
8.2 Existing Relevant Standards and Regulations 74
8.3 Standardisation Usage and Insights from Technical Partners – SC6 75
8.4 Gap Analysis 76
8.5 Strategic Gap: Absence of Specific Contributions to Standardisation Bodies 77
9. Cross-SC Synthesis: Safety, Security, Quality and Reliability (SSQR) 79
9.1 Consolidated "Standards x SC" Analysis 79
9.2 SSQR in Existing Standards 81
9.3 Interoperability and Convergence Gaps 82
9.4 Synergies with the Reference Homologation Process 84
10. Ethical, Inclusive, and Societal Challenges in Standardisation 87
10.1 Questionnaire Findings on Trust, Transparency, Acceptance 87
10.2 Inclusivity and DEI Considerations in Standards 89
10.3 Legal and Ethical Gaps in Certification 90
10.4 Human-in-the-Loop and Accountability Frameworks 92
11. Strategic Recommendations 94
11.1 Standardisation Roadmap for Cynergy4MIE 94
11.2 Pathways for Cynergy4MIE Contributions to Standard Development 94
11.3 Stakeholder Engagement and Policy Impact 95
11.4 Future Integration into Certification and Regulatory Frameworks 95
12. References 97
13. Annexes 105

A. Full Survey Questionnaire - Cynergy4MIE Questionnaire on User and Societal Acceptance of Advanced Driver Assistance Systems (ADAS) and Automated Driving Systems (ADS) 105

B. Full Survey Questionnaire - Cynergy4MIE Standardisation Analysis of Gap 129

Executive Summary

This deliverable map the state of the art in Standardisation across Cynergy4MIE's six Supply Chains and identifies the target gaps where the project can make pre normative contributions. It integrates a curated review of published international and European standards and regulations, structured partner input gathered in Task 7.4, evidence from the project demonstrators, and a user and societal acceptance survey. The analysis keeps only verified sources in the main text and moves any work under development to an annex, in order to sustain credibility.

The method combines four strands. First, a standards and regulatory review focused on items already in force, for example ISO 26262, ISO 21448, ISO or SAE 21434, UNECE R155, R156 and R157, IEEE 7001 and 7003, ISO or IEC TR 24028, ISO 39003, ETSI and SAE specifications for V2X, ISO 15118, EN 14511 and the main IEC, JEDEC and AEC Q families. Second, a partner questionnaire that exposes actual practice and pain points. Third, demonstrator evidence that tests scenarios in traffic, powertrains, collaborative robotics, multi agent systems and energy control. Fourth, a sixty-respondent survey linking trust to certification and ethics, where more than eighty one percent report higher willingness to adopt driver assistance or automated driving when certified to recognised standards and about two thirds raise concerns where ethics or privacy assurance is unclear.

The landscape is strong where mature frameworks exist. Safety and cybersecurity for road vehicles are actionable through ISO 26262 and ISO 21448 together with UNECE R155, R156 and R157. V2X interoperability rests on stable baselines from ETSI and SAE. Grid and appliance domains provide anchors for energy work through EN 14511, IEC 62477 1, IEEE 1547 and ISO 15118. At the same time four gap themes matter for convergence. Assurance for data driven components is insufficient, since current paradigms under specify verification of machine learning behaviour and continuous update regimes across mobility and energy. Explainability, human machine interface and accountability are not yet fully codified, from driver handover criteria and external HMI to audit ready logging for automated driving, with similar traceability gaps in energy optimisation. Technology coverage lags for adverse weather perception, for reliability of wide bandgap devices and for multi agent operations in search and rescue. Finally, certification remains siloed, so evidence generated in one domain is not systematically reusable in another.

The project addresses these issues through a single gate-based Reference Homologation Process that runs from requirements to a certification interface. This process triggers safety, security, quality and reliability activities at the right time, generates evidence in formats familiar to authorities and exposes points where standards are missing. It also provides traceability from requirements and architecture in the early work packages through

verification and validation to standardisation actions, so each result can be shown to be homologation ready rather than a standalone prototype.

The plan for pre normative contributions is targeted and evidence backed. In automated machinery and transport the project will deliver adverse weather perception test artefacts and scenario libraries to inform sensor methods and will bridge machinery safety with AI risk management. In smart collaborative robotics it will feed adaptive human robot collaboration requirements to the relevant ISO committee, based on fence free demonstrations that combine dynamic speed and separation monitoring with privacy by design. In powertrains it will submit reliability test protocols and mission profile data for silicon carbide and gallium nitride devices to IEC work, and position papers on incorporating machine learning components into safety analyses. In automated driving it will propose a framework for simulation-based validation to the UNECE validation fora and contribute cooperative driving scenarios and metrics to ISO or SAE while strengthening explainability and logging using IEEE 7001, IEEE 7003 and ISO 39003. In multi agent search and rescue it will release open datasets and performance metrics through IEEE channels and show how autonomous agents fit into incident management processes. In energy and distributed control, it will provide data to harmonise EN 14511 test procedures for high-capacity heat pumps and propose clearer semantics for vehicle to grid interfaces in the ISO 15118 ecosystem together with cybersecurity patterns aligned to IEC 62443.

Ethics, diversity, equity and inclusion are operationalised rather than treated as slogans. Trustworthy AI is implemented with ISO or IEC TR 24028 as a governance scaffold together with IEEE 7001 and 7003 for transparency and bias control and aligned with the AI Act Regulation EU 2024 1689 through risk management, data governance, logging and human oversight. In automated driving the project will report parity metrics for vulnerable road user detection and will adopt inclusive human machine interfaces, while in energy control it will check that optimisation does not create inequitable comfort or cost outcomes and will keep decisions explainable and auditable. All of this is recorded as Reference Homologation Process evidence so it can support conformity arguments when harmonised European standards are cited.

The roadmap is staged and tied to deliverables. By month eighteen the consortium will baseline gap closure plans and establish liaisons. By month twenty-four in D7.9 it will document engagements and publish preliminary artefacts and datasets aligned to the Reference Homologation Process gates. By month thirty in D7.10 it will submit white papers, draft texts, datasets and metrics to standard development organisations and regulatory fora and will package precertification toolkits such as templates and logging schemas. By month thirty-six it will consolidate blueprints and evidence bundles that enable exploitation.

Dependencies and risks are managed explicitly. Critical path items include test assets for simulation equivalence in automated driving, lifetime data for wide bandgap devices and diversity complete test sets for vulnerable road users and energy use. The mitigation is early and continuous engagement with standard bodies, regular gate reviews in the Reference Homologation Process and strict use of verified standards in the main text with any drafts relegated to the annex.

The expected impact is a reduction in certification risk, a shorter time to market and a step change in convergence across mobility, infrastructure and energy. By steering concrete contributions into ISO or IEC, CEN or CENELEC, IEEE and UNECE, Cynergy4MIE turns demonstrator results into standards ready evidence and helps regulators and industry adopt safe interoperable systems at scale.

List of Acronyms and Abbreviations

ACC - Adaptive Cruise Control
ADAS - Advanced Driver Assistance Systems
ADS - Automated Driving Systems
AEB - Automatic Emergency Braking
AEC - CharIN Alliance and Automotive Electronics Council
ALKS - Automated Lane Keeping Systems
ANSI - American National Standards Institute
AS/RS - Automated Storage and Retrieval Systems
ASDE - Authorised Self-Driving Entity
ASIL - Automotive Safety Integrity Levels
AVCC - Autonomous Vehicle Computing Consortium
BLE - Bluetooth Low Energy
C2C-CC - Car2Car Communication Consortium
CAM - Cooperative Awareness Message
CEN - European Committee for Standardisation
CENELEC - European Committee for Electrotechnical Standardisation
CSMS - Cybersecurity Management System
DAR - Decision Awareness and Responsibility
DEI - Diversity, Equity, and Inclusion
DSRC - Dedicated Short-Range Communications
EC - European Commission
ECS - Electronic Components and Systems
EMC - Electromagnetic Compatibility
EMI - Electromagnetic Interference
EMVA - European Machine Vision Association
ERP - Enterprise Resource Planning
ETSI - European Telecommunications Standards Institute
FCW - Forward Collision Warning
GDPR - General Data Protection Regulation
GSR - General Safety Regulation
HBES - Home and Building Electronic Systems
HDS - High-Definition Sensing
HITL - Human-in-the-Loop
HLEG - High-Level Expert Group on AI
HMI - Human–Machine Interface
HRC - Human–Robot Collaboration
HSE - Health, Safety and Environment
HVAC - Heating, Ventilation and Air Conditioning
IACS - Industrial Automation and Control Systems

IATF - International Automotive Task Force
ICAO - International Civil Aviation Organization
ICS - Industrial Control Systems
ICT - Information and Communication Technology
IEC - International Electrotechnical Commission
IEEE - Institute of Electrical and Electronics Engineers
IIoT - Industrial Internet of Things
IMU - Inertial Measurement Unit
IoT - Internet of Things
IP - Internet Protocol
ISA - Intelligent Speed Assistance
ISA-95 - Enterprise–Control System Integration
ISO - International Organization for Standardisation
ISO/IEC - International Organization for Standardisation / International Electrotechnical Commission
ISO/SAE - International Organization for Standardisation / Society of Automotive Engineers
ISO/TS - ISO Technical Specification
ITS - Intelligent Transport Systems
ITS-G5 - IEEE 802.11p-based ITS at 5.9 GHz
ITU - International Telecommunication Union
JTC - Joint Technical Committee
KPI - Key Performance Indicator
LCA - Life Cycle Assessment
LDW - Lane Departure Warning
LDWS - Lane Departure Warning Systems
LKA - Lane Keeping Assist
LVD - Low Voltage Directive
MES - Manufacturing Execution Systems
MFC - Material Flow Control
MHI - Material Handling Industry
MIE - Mobility, Infrastructure and Energy (ecosystem convergence)
MIMO - Multiple-Input Multiple-Output
ML - Machine Learning
MPC - Model Predictive Control
NIS - Network and Information Security
NIST - National Institute of Standards and Technology
NMEA - National Marine Electronics Association (messaging)
ODD - Operational Design Domain
OEM - Original Equipment Manufacturer
OCR - Optical Character Recognition
OPC - Open Platform Communications

OTA - Over-the-Air (updates)
PFNC - Pixel Format Naming Convention
PHM - Prognostics and Health Management
PLM - Product Lifecycle Management
PROFIBUS - Process Field Bus
PROFINET - Industrial Ethernet for Automation
R&D - Research and Development
R130 - Uniform Provisions Concerning the Approval of Motor Vehicles with Regard to Lane Departure Warning Systems
R155 - UN Regulation on Cybersecurity and Cybersecurity Management Systems
R156 - UN Regulation on Software Update and Software Update Management Systems
R157 - UN Regulation on Automated Lane Keeping Systems
RCTA - Rear Cross-Traffic Alert
RED - Radio Equipment Directive
REESS - Rechargeable Electric Energy Storage Systems
RFID - Radio-Frequency Identification
SAR - Specific Absorption Rate
SIL - Safety Integrity Level
SFNC - Standard Feature Naming Convention
SOTIF - Safety of the Intended Functionality
TA - Technical Assessment
TC - Technical Committee
UAV - Unmanned Aerial Vehicle
UGV - Unmanned Ground Vehicle
UL - Underwriters Laboratories
UN - United Nations
UNECE - United Nations Economic Commission for Europe
UWB - Ultra-Wideband
V2G - Vehicle-to-Grid
VDMA - German Engineering Federation
VRU - Vulnerable Road User
WAVE - Wireless Access in Vehicular Environments
WBG - Wide-Bandgap (power semiconductors)
WMS - Warehouse Management Software

1. Introduction

1.1 Purpose of this deliverable

This deliverable, titled '*Standardisation State-of-the-Art and Analysis of Gaps'*, serves as a strategic cornerstone within the Cynergy4MIE project. It aims to map the current standardisation landscape relevant to each Supply Chains (SC1 to SC6), evaluate the contributions of technical Work Packages (WPs) to existing or emerging standards, and critically identify gaps where Cynergy4MIE can provide pre-normative inputs or even catalyse new standardisation efforts.

The scope of this work goes beyond merely cataloguing applicable standards. It seeks to interrogate their adequacy, maturity, and ethical robustness considering the project's overarching ambition to foster domain convergence across mobility, infrastructure, and energy systems for Society 5.0. By integrating technical, societal, and regulatory insights, including those gathered through structured stakeholder engagement and user acceptance surveys, this overview addresses both formal compliance and deeper issues of trust, explainability, inclusivity, and systemic interoperability.

Aligned with the Cynergy4MIE project objectives and its vision for integrated, human-centric cyber-physical systems, this overview responds to three primary purposes:

1. State-of-the-Art Mapping: Establish a structured baseline of current international, European, and sector-specific standards that influence or constrain innovation in each SC domain.
2. Gap Identification and Risk Framing: Provide an evidence-based analysis of where standards fall short, whether in functional safety, societal acceptance, environmental resilience, or ethical alignment, and frame these gaps as risks to deployment, scalability, or acceptance. Strategic Value Proposition: Clarify how Cynergy4MIE's technical outputs, demonstrators, and human-centric perspectives can contribute pre-normative insights or standardisation drafts, while also engaging with key bodies such as ISO, IEEE, UNECE WP.29, and CEN/CENELEC.

1.2 Scope and Relevance for Cynergy4MIE

This overview sits at the confluence of foundational technologies, application layer integration, and system-level governance that Cynergy4MIE is structured to address. It captures how standardisation interacts with, and potentially accelerates, the project's ambition to converge mobility, infrastructure, and energy domains under the principles of Society 5.0.

The scope extends across all six Supplies Chains (SC1 to SC6), each representing a critical application or enabling domain in cyber-physical systems. Rather than treating these domains in isolation, this overview considers how their technical outputs contribute to shared challenges, such as functional safety, explainable AI, data interoperability, and ethical assurance.

Key aspects of relevance include:

- Cross-WP Integration: The standardisation analysis draws inputs from multiple WPs, capturing how design-time specifications (WP1), architectural frameworks (WP2), algorithm development (WP4), validation efforts (WP5), and ethics and societal engagement (WP7) align with or diverge from existing standards.
- Pre-Standardisation Leverage: Cynergy4MIE's demonstrators and simulations serve as empirical platforms to test and validate novel approaches that could inform standards development or revision, particularly in the context of AI-driven systems and V2X communications.
- Societal Anchoring: Through structured societal acceptance studies and inclusive design frameworks, the project ensures that standardisation is not only a technical instrument but a mechanism for public trust, inclusivity, and long-term regulatory coherence.

By structuring the analysis around SCs while cross-mapping to enabling WPs and societal concerns, this overview ensures that standardisation becomes a unifying layer, integrating compliance, innovation, and ethics into a coherent exploitation pathway

1.3 Methodology and Data Collection Approach

This deliverable adopts a triangulated methodology that integrates technical analysis, standards review, and stakeholder-informed inputs to ensure comprehensive insight into the current standardisation landscape relevant to Cynergy4MIE's six (6) Supply Chains (SC1–SC6). The overarching aim is to identify both technical and non-technical gaps that constrain the safe, ethical, and scalable deployment of cyber-physical systems across mobility, infrastructure, and energy domains.

The analysis draws upon three interlinked sources. First, a structured desk review was conducted on the corpus of standards and regulatory frameworks applicable to the project's core domains. This included international and European standards bodies such as ISO, IEEE, UNECE WP.29, CEN/CENELEC, and SAE, with a specific focus on areas central to Cynergy4MIE such as functional safety (ISO 26262; ISO 21448), cybersecurity (ISO/SAE 21434; UNECE R155/R156), AI ethics (ISO 39003; IEEE 7000-series), and automation-specific governance (e.g. UNECE R157 on ALKS). Additional attention was given to forward-looking standards under development (e.g. IEEE P2040, IEEE P3474), and their potential alignment with anticipated EU legislative frameworks such as the Artificial Intelligence Act and the European Green Deal (European Commission, 2021; IEEE, 2024).

Second, a user- and society-facing questionnaire was administered under the *User and Societal Acceptance of ADAS and ADS* study. This instrument targeted both Cynergy4MIE consortium partners and external stakeholders, including technical experts, researchers, regulators, civil society actors, and end users. A total of 60 responses were collected.

A key component of the survey was Section 7, which focused on participants' awareness, trust, and priorities concerning standardisation. The findings point to a strong confidence in certified systems. An overwhelming 81.67% of respondents indicated that knowing an ADAS or ADS feature is certified by an international standard would increase their trust in using it. Furthermore, 70% reported being already familiar with international certification frameworks such as those developed by ISO, IEEE, or UNECE. The importance of safety certification was also widely recognised, with 81.67% agreeing or strongly agreeing that standards like ISO 21448 or UNECE WP.29 are essential prerequisites for deployment. Notably, 66.67% expressed concern over systems that lack certification for ethical and privacy compliance, such as adherence to GDPR or mechanisms for bias mitigation. This underscores a broader perception of certification not merely as a technical requirement, but as a vital safeguard for ethical integrity and societal trust.

In addition, respondents were asked to rank standardisation priorities. The clear top-ranked concern was "Safety and accident prevention" (ranked 1st by 90% of respondents), followed by "Reliability and durability over time" and "Data privacy and cybersecurity". In contrast, areas such as fairness, accessibility, and environmental sustainability ranked lower on average, though they were still prioritised by specific subgroups. This prioritisation data informs how gaps in inclusivity and ethical foresight are not only technical blind spots but risk being deprioritised in standardisation efforts without explicit counterbalancing.

The structure of Section 7 thus provided a robust evidence base to triangulate technical gaps with public and expert perception, allowing the project to evaluate not only what standards exist, but whether they are trusted, understood, and seen as sufficient by their intended beneficiaries.

Third, a technical partner questionnaire, titled *Standardisation Analysis of Gaps*, was deployed under Task 7.4 to gather structured input from Cynergy4MIE's industrial and technical partners across SC1–SC6. The questionnaire aimed to characterise:

- Standards currently used or referenced by partners,
- Participation in or observation of relevant standardisation bodies,
- Domain-specific experience with gaps or limitations in standardisation,
- Recommendations for Cynergy4MIE's pre-normative engagement.

This instrument received 20 completed responses, focusing on partner experiences with V2X, perception systems, AI decision logic, sensor fusion, cybersecurity, and system-level requirements. It directly informs this deliverable (D7.8) and supports future outputs of Task 7.4, including strategic alignment with certification trajectories. Data from this questionnaire were handled under GDPR-compliant procedures and stored securely for the project duration and audit period.

Across both instruments, all data were anonymised and analysed in aggregate form. Personally identifiable information was excluded from all public outputs. Both instruments adhered to ethical research principles and EU data protection regulations (GDPR 2016/679). This combined methodological approach ensures that the findings presented in the following sections are grounded in diverse, representative, and systematically gathered evidence.

1.4 Intralogistics as a reference domain for standardisation analysis

The modern industrial landscape is increasingly reliant on efficient internal logistics, a domain commonly referred to as intralogistics. This specialised field focuses on the flow of materials and information exclusively within a company's facilities, distinguishing it from conventional logistics which governs the movement of goods between external locations.

Processes within intralogistics encompass a broad spectrum of activities, including

- receipt,
- issue,
- transport of materials,
- precise order picking and sorting,
- inventory management, and the sophisticated orchestration of information flow and warehouse operations.

Industrial companies target to improve the performance of these processes by increasing the level of automation by shifting from manual labour to automated process steps to

- enhance production efficiency,
- Improve production quality,
- minimize manual handling and,
- Improve worker safety

to ultimately maximise overall productivity within internal operations.

The intralogistics automation systems consist of components that are integrated as seamless transport chains controlled by the production process needs.

Transport equipment: physical material movement is at the core of the intralogistics. The equipment includes:

- **Automated Guided Vehicles (AGVs) and Autonomous Mobile Robots (AMRs)** are driverless logistics vehicles and material handling robots**.** AGVs are commonly tireless transport wagons transporting materials along predefined routes. AMRs are generally more flexible in their route planning and material handling tasks compared to AGVs. Both vehicle types share the routes with human workers and manually controlled vehicles.

- **Conveyor systems:** mechanical material transport systems that use fixed constructs with belts, rollers and chains to move materials from one location to another. Conveyor belts are less expensive compared to AGVs and AMRs, but they are very effective in productions where the material routes do not need to change often.
- **Other equipment:** manual forklifts and pallet trucks are common human operated transport equipment in facilities. They can be also completely or partially automated to improve productivity, efficiency and safety.

IT-systems: the production state information, orchestration and related automation are powered by a suite of interconnected IT systems.

- **Warehouse Management Software (WMS):** This software is central to managing inventory and the flow of materials within a warehouse. A WMS oversees the entire internal material and information flow, receiving orders from higher-level enterprise systems and translating them into instructions for transport systems.
- **Manufacturing Execution Systems (MES):** These systems are vital for communicating and relaying information within the production area and shop floor, often integrating directly with intralogistics operations to ensure synchronized manufacturing processes.
- **Enterprise Resource Planning (ERP) Systems:** As higher-level organizational systems, ERPs support business and logistics management, feeding orders and configuration data to WMS and other intralogistics IT components.
- **Material Flow Control (MFC) Systems:** These systems are dedicated to managing the movement of robots and other transport equipment, often working together with specific AGV/AMR management applications to optimize their paths and prevent congestion.
- **Industrial Internet of Things (IIoT):** IIoT involves connecting various devices and sensors to collect real-time information, enabling plant digitalization, traceability, and proactive decision-making within the intralogistics environment.

The complex interaction of these technologies within intralogistics creates an "internal ecosystem" where real-time, coordinated communication is paramount. The variety of components, from physical transport equipment to sophisticated software systems, often originates from different manufacturers. This inherent diversity makes robust standardisation for interoperability critical. Without common protocols and interfaces, organizations face substantial integration problems, increased costs, and operational inefficiencies, which can significantly impede the full realization of automation's benefits.

The rapid growth and adoption of intralogistics automation are not merely a result of technological advancement but are driven by various operational pressures. The increasing volumes of e-commerce and the demand for faster deliveries necessitate higher productivity. Simultaneously, persistent labour shortages and the pressure for cost reduction push businesses to seek automated solutions. Automation, therefore, emerges as a strategic toolbox, allowing businesses to adapt and maintain competitiveness within a demanding global supply chain landscape.

Another growing trend in technological evolution of intralogistics is the integration of IT systems with physical operational technology (OT). Technologies like Open Platform Communications Unified Architecture (OPC UA) and edge computing are building blocks for the bridge between IT and OT. Cross-domain standards like OPC UA are essential for ensuring smooth communication, data integrity and security in the communication.

1.4.1 Intralogistics standards landscape

Standardisation plays a crucial role in the advancement of intralogistics solutions. In the rather heterogenous technological landscape of IT and OT systems it is important to agree and align understanding related to products, processes, safety, interoperability and reliability. The quality and general acceptability of standards is achieved by applying a consensus-driven development process where diverse stakeholders under the accreditation of organizations such as the European Telecommunications Standards Institute (ETSI), the Organization for Standardisation (ISO) and the American National Standards Institute (ANSI).

For intralogistics the standardisation serves the following purposes:

- **Interoperability:** It is recognized as a crucial element for seamless connectivity across the diverse technologies of Industry 4.0, providing a common language that facilitates systems working together.
- **System Architecture:** Initiatives like the System Architecture for Intralogistics (SAIL), developed by the VDMA (Verband Deutscher Maschinen- und Anlagenbau, German Machine Engineering Federation), aim to foster effective collaboration among project partners by establishing cross-provider architectural concepts and defining standardized control functions and interfaces.
- **Multi-Vendor Fleet Control:** Standards such as VDA 5050 are instrumental in allowing a central control station to communicate harmoniously with transport robots from various manufacturers using standardized commands and status reports. This significantly enhances flexibility, efficiency, and scalability for managing heterogeneous fleets.
- **Safety and Compliance:** Safety standards, such as ISO 3691-4, is a driving force behind the development of secure and compliant intralogistics solutions. Compliance with these standards ensures that manufacturers maintain high safety levels.

While standardisation might seem to slow down innovation sometimes, there's actually a lot of proof it does the opposite. Standardized interfaces, communication protocols and architectural frameworks provide a foundation for vendor solutions that can be built, integrated, tested and scaled more easily.

Furthermore, standardisation is not only a technical compliance exercise but a strategic economic imperative for the intralogistics sector. It directly contributes to significant cost reductions in areas such as integration, maintenance, and risk mitigation, while simultaneously improving operational efficiency and enhancing system reliability. The economic advantages make standardized intralogistics solutions more attractive and viable for businesses, thereby directly facilitating market validation and widespread deployment.

1.4.2 Key standardisation bodies in Intralogistics

The following table provides an overview of key international and regional standardisation bodies relevant to intralogistics.

Table 1: Key Standardisation Bodies in Intralogistics

Organization Name	Primary Focus/Role	Key Standards/Initiatives Relevant to Intralogistics
International Organization for Standardisation (ISO)	Develops and publishes international standards across various industries, including robotics and automation.	ISO 10218-1 & -2 (Safety requirements for industrial robots and systems), ISO/TS 15066 (Collaborative robot safety), ISO 3691-4 (Safety for driverless industrial trucks/AGVs), ISO 13849 (Safety of machinery control systems), ISO 9001 (Quality management).
International Electrotechnical Commission (IEC)	Prepares and publishes international standards for all electrical, electronic, and related technologies, including functional safety and industrial automation.	IEC 61508 (Functional safety of E/E/PE safety-related systems), IEC 62443 Series (Industrial control system cybersecurity), IEC 60286-3 (Packaging of components for automatic handling), IEC 63303 (HMIs for automation systems).

VDMA (German Engineering Federation)	Represents German and European manufacturers in materials handling and intralogistics, promoting standardisation and innovation.	VDA 5050 (Communication interface for mobile robots), SAIL (System Architecture for Intralogistics).
OPC Foundation	Creates and maintains standards for open connectivity of industrial automation devices and systems.	OPC UA (Unified Architecture - platform-independent, secure data communication, standardized data models).
PROFIBUS & PROFINET International (PI)	Leading industry association for industrial communication and automation technologies.	PROFIBUS, PROFINET (Industrial Ethernet protocol for real-time communication), IO-Link (Sensor/actuator interface), omlox (Localization standard), MTP (Module Type Package for modular systems), SRCI (Standard Robot Command Interface for multi-vendor robot control).
MHI (Material Handling Industry)	Leading trade association for advancing material handling and supply chain industry in the US.	MH10 (Data Identifiers for unit loads), MH16.1 (Industrial steel storage racks), MH1 (Pallets, Slip Sheets).
American National Standards Institute (ANSI)	Coordinates voluntary standardisation for the U.S. private sector, often adopting international standards.	ANSI B56 (Powered Industrial Trucks), ANSI/UL 1740 (Robots and Robotic Equipment), ANSI/ITSDF B56.5 (Driverless Industrial Vehicles).

European Telecommunications Standards Institute (ETSI)	ETSI develops globally applicable standards for information and communications technologies, which are increasingly relevant to intralogistics for ensuring interoperability and secure communication within complex automated systems.	oneM2M (specifications for M2M and IoT), ETSI TC SmartM2M (Technical Committee Smart Machine-to-Machine Communications), ETSI ISG CIM (Industry Specification Group on cross-cutting Context Information Management)

1.4.3 Key standards in intralogistics domain

Intralogistics heavily depends on key standards, predominantly set by the standardisation bodies outlined in section 1.4.2. These standards provide architectural, functional, and non-functional frameworks for areas within the domain. This section will elaborate on the standards pertinent to intralogistics.

These standards are crucial for addressing aspects such as safety, functional integrity, communication, interoperability, and regulatory compliance, thereby guaranteeing the reliable and secure operation of automated solutions.

Tracking Standards and Communication Formats

Safety Standards for Industrial and Mobile Robotics

Safety is a paramount concern in environments where humans and machines interact, particularly with the increasing deployment of robots in intralogistics.

ISO 10218-1:2025 and ISO 10218-2:2025: These are foundational international standards defining safety requirements for industrial robots and robotic systems. ISO 10218-1 focuses on the robot as a partly completed machine, primarily affecting manufacturers of industrial robots and cobots. ISO 10218-2, conversely, addresses the safety of complete robot systems and their integration into applications and cells, impacting machine manufacturers and system integrators. The updated 2025 editions replace the 2011 versions, reflecting advancements in robotics, including collaborative robotics and connected systems. Key changes include a new classification of robots (Class I and Class II, with Class I having stricter safety requirements, often including cobots), clearer guidelines for functional safety, and, notably, the integration of cybersecurity requirements. The standard now mandates consideration of digital vulnerabilities that could compromise safety functions.

ISO/TS 15066:2016: This technical specification provides detailed safety requirements for collaborative industrial robot systems and their work environments, supplementing ISO 10218-1 and ISO 10218-2. It is particularly crucial for applications where human-robot contact is permissible, stipulating that such contact should not result in pain or injury. The standard provides "Pain Onset Level" data, derived from studies on human body areas, to establish maximum force and pressure thresholds for robot design and integration. It also outlines recommended power and speed limits for power and force limited operations and describes four main collaborative techniques: safety-rated monitored stop, hand-guiding, speed and separation monitoring, and power and force limiting. This technical specification fills critical gaps left by ISO 10218, providing concrete data and formulae for risk assessments in collaborative robot applications.

ISO 3691-4:2020: This international standard specifically defines the safety requirements for driverless industrial trucks, including Automated Guided Vehicles (AGVs) and Autonomous Mobile Robots (AMRs), and their associated systems. It provides critical guidance for all stakeholders, OEM manufacturers, integrators, and end-users, by outlining their shared responsibilities in ensuring a safe AGV system. The standard addresses three key aspects: defining operating environments and zones where trucks interact with humans, identifying associated hazards and risks, and ensuring the correct implementation of safety protection systems. For instance, it mandates safety fields covering all directions of movement and requires speed reduction when detected side space is less than 0.5m. While not yet a harmonized standard for mandatory compliance with the EU Machinery Directive, it is widely adopted as best practice, indicating a manufacturer's commitment to safety.

Functional Safety and Cybersecurity Standards

Beyond direct physical safety, the functional integrity and digital security of intralogistics systems are addressed by specialized standards.

IEC 61508: This is an overarching international standard for functional safety, providing a comprehensive framework for designing, implementing, and maintaining safety-related electrical, electronic, and programmable electronic (E/E/PE) systems throughout their entire lifecycle. It addresses both random hardware failures and systematic failures (e.g., design errors) through qualitative risk assessment and the definition of safety measures. A core concept is the Safety Integrity Level (SIL), which quantifies the risk reduction provided by a safety system, ranging from SIL 1 (lowest) to SIL 4 (highest). Compliance with IEC 61508 is crucial for mitigating risks, protecting human lives, and ensuring system reliability in industrial automation, particularly for autonomous and collaborative robots.

IEC 62443 Series: This series of standards specifically addresses cybersecurity for industrial automation and control systems (IACS) and other forms of operational technology (OT). It provides a defensive framework tailored to the unique realities and downtime intolerance of shop-floor equipment like pumps, drives, and PLCs. A core principle is "layered defence," which involves segmenting facilities into security zones linked by monitored conduits, and establishing a Cybersecurity Management System (CSMS). The series is divided into four main parts: General (terms, concepts), Policies and Procedures (program structure, patch management), System (assessment methods, security levels), and Component (lifecycle oversight, technical requirements for devices/software). IEC 62443 complements existing architectural models like ISA-95 by adding a crucial security lens, especially as Industrial Internet of Things (IIoT) devices connect to cloud or external networks.

Communication and Interoperability Standards

Effective communication and seamless interoperability between diverse systems and devices are fundamental for integrated intralogistics operations.

VDA 5050: This communication interface standard has gained significant traction in Germany and Central Europe for mobile robots (AGVs/AMRs). It regulates communication between a master control system and individual vehicles, standardizing the structure and content of commands and status reports. This standardisation enables the smooth integration, control, and optimization of different robot types, as well as the efficient operation of hybrid fleets, thereby increasing flexibility, efficiency, and scalability in intralogistics. VDA 5050 offers wide range of information, including movement and status updates, and focuses on networking robot fleets with warehouse management or ERP systems.

OPC Unified Architecture (OPC UA): Developed by the OPC Foundation, OPC UA is an open, unified communication technology that serves as a backbone for industrial communication and a central component of Industry 4.0. It is platform-independent, meaning it does not rely on, for example, Windows-specific technologies, allowing it to run on various systems from industrial PCs to cloud environments. OPC UA provides a well-designed architecture with standardized data models, flexible communication methods (client-server and publish/subscribe), and open interfaces, facilitating seamless connections between production equipment, control systems, and central IT. Its design incorporates robust security measures, protecting communication and data against unauthorized access and manipulation.

PROFIBUS & PROFINET International (PI) Standards: PI is a leading industry association that develops, standardizes, and promotes industrial communication and automation technologies. Its core technologies are highly relevant to intralogistics:

- **PROFINET:** An Ethernet-based communication network for industrial automation, supporting speedy vertical and horizontal data exchange across all levels, including real-time (RT) and isochronous real-time (IRT) communication for demanding applications like motion control. PROFINET provides a robust and secure platform for data exchange from the operational technology (OT) layer to cloud services, emphasizing standardized data formats.

- **PROFIBUS:** The world's most successful fieldbus, standardized in IEC 61158, offering a single, application-independent communication protocol for factory and process automation, as well as motion control and safety-related tasks.
- **IO-Link:** A flexible, fieldbus-independent sensor/actuator interface for connecting smart devices at the lowest automation level, enabling on-the-fly configuration and enhanced communication.
- **omlox:** A standard for unified access to location data, enabling flexible real-time locating solutions using components from various manufacturers. It facilitates plug-and-play tracking of hardware like AGVs and provides geo-referencing, identity management, and geo-fencing functionalities crucial for optimizing material flow.
- **Module Type Package (MTP):** A concept that describes process module functions independently of the manufacturer, enabling flexible "plug & produce" systems. It standardizes automation interfaces for process modules, facilitating quick integration into higher-level automation systems, which is highly relevant for modular intralogistics systems.
- **Standard Robot Command Interface (SRCI):** An open standard for programming and operating robots within a PLC environment, standardizing communication between robot controllers and PLCs regardless of manufacturer. This reduces the need for specialized expertise and streamlines training efforts.

ISA-95: This standard defines a hierarchical model for manufacturing operations and provides guidelines for data exchange between different enterprise levels to enhance efficiency, interoperability, and communication within industrial automation and control systems. Its primary focus is standardizing the interface between business systems (e.g., ERP) and manufacturing control systems (e.g., DCS, MES). ISA-95 offers standard data and object models, common terminology, and mechanisms for information exchange, reducing the need for custom interfaces and ensuring data consistency across systems.

Material Handling Equipment and Infrastructure Standards

Specific standards also govern the safety and performance of various material handling equipment and the infrastructure they operate within.

AS/RS Safety Standards: Automated Storage and Retrieval Systems (AS/RS) present unique safety considerations, particularly regarding fire risk and personnel access. FM Global Data Sheet 8-34 and NFPA 13 provide in-depth recommendations for fire protection in AS/RS facilities, emphasizing factors like storage height, types of goods stored (e.g., those with lithium-ion batteries), and water supply. For personnel safety, standards like EN 528 (a regional European standard) address requirements for restricting access to authorized personnel and preventing unexpected start-up, often through interlocked guarding and escape release mechanisms. AS/RS systems are designed to improve safety by replacing manual picking and reducing human presence in high-speed, high-density storage areas.

Conveyor System Safety Standards: Conveyor systems, while efficient, pose various hazards such as entanglement, pinch points, overhead risks, and electrical hazards. Safety standards, including EN 12882 (for general-purpose conveyor belts), OSHA regulations (29 CFR 1910.22, 1926.555) in the US, and British Standards (BS 4531, BS EN 618, BS EN 620), mandate safeguards like physical guards, emergency stop switches, proper lockout/tagout procedures, and warning systems. These standards aim to prevent injuries by ensuring safe design, installation, and operation, including requirements for anti-static belts and fire resistance in specific environments.

ANSI B56 Powered Industrial Trucks: This American National Standard outlines requirements for the design, testing, and safe operation of powered industrial trucks, including forklifts and other industrial vehicles. It also delineates the responsibilities of manufacturers, dealers, lessors, lessees, owners, and operators, contributing to overall workplace safety in material handling.

MHI Standards: The Material Handling Industry (MHI) plays a significant role in developing and endorsing material handling related standards in the US. This includes the MH10 series for Data Identifiers (DIs) used in automatic identification and data capture (AIDC), IoT, and Blockchain applications, and the MH16.1 standard for the structural design, testing, and utilization of industrial steel storage racks. These standards promote safety, efficiency, interchangeability, and reliability in material handling products and processes.

Machine vision and situational awareness related standards

Machine vision systems rely on specific standards for camera interfaces, image processing, and data representation to ensure interoperability and effective operation.

VDMA 2632 Series (Machine Vision): This series of standards from the German Engineering Federation (VDMA) provides guidelines for machine vision systems.

- **VDI/VDE/VDMA 2632 Blatt 1**: Covers the basics, terms, and definitions of machine vision systems.
- **VDI/VDE/VDMA 2632 Blatt 2**: Aids in preparing requirement and system specifications for machine vision systems, improving communication between suppliers and users.
- **VDI/VDE/VDMA 2632 Blatt 3 and 3.1**: Address the acceptance testing of classifying machine vision systems.

EMVA 1288 Standard: Developed by the European Machine Vision Association (EMVA), this standard is for the measurement and presentation of specifications for machine vision sensors and cameras.

GenICam: A generic programming interface for all types of cameras, providing a standardized way to access camera controls and image streams. It uses an XML device description file to define camera features.

- **Standard Feature Naming Convention (SFNC)** and **Pixel Format Naming Convention (PFNC)** are part of GenICam, ensuring consistency in vision standards.

Machine Vision Camera Interface Standards (Communication Protocols): These define how cameras communicate with host systems.

- **GigE Vision**: A global camera interface standard based on Gigabit Ethernet, enabling fast, error-free image transfer over long distances and ensuring interoperability.
- **CoaXPress (CXP)**: A digital interface standard for high-speed image data transmission over coaxial cables, supporting bidirectional communication.
- **USB3 Vision**: Based on the standard USB 3.x interface, offering high bandwidth and plug-and-play functionality, transmitting power and data over the same cable.
- **Camera Link** and **Camera Link HS**: Interfaces designed for high-speed, real-time communication in machine vision applications.

Data Formats for Machine Vision:

- **Image and Video Data**: Captured by cameras in formats like PNG, JPEG, WEBP, and non-animated GIF.
- **Package Data**: Includes dimensions, weight, condition, labels, codes, markings, photos, and 3D images.
- **Codes and Symbols**: Barcodes, DMC codes, 2D codes, and RFID are read by machine vision systems for tracking and identification.
- **Text Data**: Extracted via Optical Character Recognition (OCR).
- **Decision Signals**: Outputs from machine vision AI platforms, such as "pass/fail" or "defect detected," sent to PLCs and HMIs.
- **XML Device Description Files**: Used by GenICam-based camera interfaces to describe camera features.

Real-Time Locating Systems (RTLS) Standards and Data Formats

RTLS technologies provide real-time location and identification data, crucial for efficient material flow and inventory management in intralogistics.

- **RTLS Technologies**:
  - **Ultra-Wideband (UWB)**: Offers high precision (centimetre-accurate) tracking.
  - **Bluetooth Low Energy (BLE)**: Used for RTLS, typically with 3-5 meters accuracy.

- **RFID (Radio Frequency Identification)**: Used for position and identification data, often providing "point-in-time" data at checkpoints. RFID tags and smart shelves automate inventory tracking.
- **Other technologies**: WLAN-based localization, Infrared (IR), Active RFID, Low Frequency (LF) for choke points.

- **omlox Standard**: An open locating standard for industrial real-time locating solutions, promoting interoperability across different tracking technologies and vendors.
    - **omlox hub**: Provides standardized interfaces (APIs) for location data and services, enabling access to location data regardless of the underlying technology. It supports geo-referencing, identity management, geo-fencing, and distance computation.
    - **omlox core zone**: An open UWB system for plug-and-play, real-time tracking of hardware from multiple vendors, standardizing the wireless interface for UWB-enabled devices.
- **MHI MH10 Data Identifiers**: The ANSI MH10.8.2 standard from the Material Handling Industry (MHI) defines Data Identifiers (DIs) used in automatic identification and data capture (AIDC), IoT, and Blockchain applications.
- **RTLS Data Formats**:
    - **Location Data**: Space ID, unique ID, real-time and historical location information.
    - **Contextual Data**: Patient progress, time spent with providers, bottlenecks in care flow, staff location, equipment location, clinic-wide activity, patient journey metrics.

Context Information Management (CIM) and NGSI-LD API Formats

Context Information Management (CIM) standards, particularly those from ETSI, are crucial for exchanging data with its context, enabling multi-system interoperability.

ETSI ISG CIM (Industry Specification Group on cross-cutting Context Information Management): Focuses on enabling the exchange of data along with its context (space, time, relations) between IoT platforms, information systems, and third-party applications.

NGSI-LD API: An information model and API for publishing, querying, and subscribing to context information, enabling structured information sharing across domains like smart cities, smart industries, and digital twins. It is based on JSON-LD for semantic interoperability.

Other Contextual/Situational Awareness Enriching Data Formats

These formats provide semantic meaning, structure, and real-time representations for complex industrial environments.

- **Semantic Data Models (SDM)**: Describe objects and structures of datasets, assigning meaning and defining relationships to provide context. They use ontologies and vocabularies to attach meaning and create context across different data entities.
    - **Abstraction Types**: Classification ("instance of"), Aggregation ("has a"), and Generalization ("is a") are used to organize and relate data.
- **Ontologies**: Support interoperability, reasoning, and decision-making by identifying semantic relations between heterogeneous data sources. An ontological model helps solve the problem of heterogeneity in descriptions of enterprise elements.
- **Digital Twin Data Formats**: Digital twins are virtual representations of physical objects or systems, updated from real-time data, using simulation, machine learning, and reasoning to aid decision-making.
    - **Data Sources**: Sensors on physical objects produce data about performance (e.g., energy output, temperature, weather conditions).
    - **Purpose**: Standards for digital twins ensure interoperability, reliability, and efficiency, fostering a unified approach for complex systems like those in manufacturing.

ID-RAM Data Space Formats

The IDS Reference Architecture Model (IDS-RAM) and its associated Dataspace Protocol are highly relevant for creating secure and sovereign data spaces, which can encompass data from machine vision, RTLS, and other contextual sources in intralogistics.

- **IDS Reference Architecture Model (IDS-RAM)**: A practitioner-oriented guide for designing and implementing architectures for data spaces. It uses a five-layer structure (business, functional, process, information, and system layer) and three perspectives (Security, Certification, and Governance).
- **IDS Information Model**: Defines the essential agreement shared by participants and components of data ecosystems, facilitating compatibility and interoperability. It has three formal levels of digital representation: Conceptual (UML), Declarative (machine-interpretable, semantic description), and Programmatic (e.g., Java library).
- **Dataspace Protocol (DSPACE)**: Provides a clear specification for data space interoperability, independent of implementation details, and foundational for sovereign data exchange. It is being developed as an international standard.
    - **Messages**: Contain DCAT (Data Catalog Vocabulary) and ODRL (Open Digital Rights Language) types, such as Agreement, Catalog, DataSet, Asset, and Offer.
    - **Protocols**: Includes Contract Negotiation Protocol and Transfer Process Protocol, with a REST API Binding.
- **Integration with OPC UA**: VDMA 40001-1 and 40001-3 are identical with OPC 40001-1 and 40001-3, which are OPC UA companion specifications. OPC UA is an

interoperability standard for secure and reliable data exchange in industrial automation, enabling seamless information flow among devices from multiple vendors. This highlights how data spaces can leverage existing industrial communication standards for data exchange.

These standards and data formats collectively form the backbone for building intelligent, interconnected, and context-aware intralogistics systems.

1.4.4 Intralogistics Standardisation Gaps and Challenges

Our target in the project is to collect information about the current standard adoption and related issues. We target to understand the potential gaps and problems faced by the organizations in the standard implementation.

- **Identification of Specific Gaps in Intralogistics Standardisation:** (e.g., Interoperability between different vendor systems for integrated solutions, standardized data exchange formats across WMS/MES/ERP, safety guidelines for complex human-robot collaboration scenarios, comprehensive cybersecurity integration for legacy systems, standardisation for AI/IoT in real-time operations).
- **Impact of Identified Gaps:** (e.g., Increased integration costs, slower deployment of new technologies, higher operational risks, reduced efficiency, limited scalability).
- **Challenges in Implementing Existing Standards:** (e.g., Complexity of standards, high cost of compliance, lack of skilled personnel, conflicting regional or national standards, insufficient awareness).
- **Views on the Balance between Standardisation and Innovation:** (e.g., "Current standards stifle innovation," "Standards enable innovation").

2. Standardisation Landscape Overview

2.1 International and European Standardisation Ecosystem

Standardisation serves as a vital backbone for trust, interoperability, resilience, and sustainability across Cyber-Physical Systems (CPS). To position Cynergy4MIE effectively in the innovation ecosystem, it is essential to understand the layered structure and dynamics of standardisation from global to European levels, as well as how CPS, at the heart of this project, are defined and evolving.

2.1.0 What Are Cyber-Physical Systems (CPS)?

Cyber-Physical Systems integrate computation, networking, and physical processes through tight feedback loops. Sensors collect real-world data, computational units analyse it in real time, and actuators effect physical responses, creating a continuously adaptive system (Zacchia Lun et al., 2016). CPS are characterised by their tight cyber–physical coupling, distributed real-time control, and scalable, networked architectures functioning across multiple domains and time scales (ISO, 2021). Applications include autonomous vehicles, industrial automation, robotics, and intelligent energy systems, all relevant to Cynergy4MIE's ambitions.

2.1.1 Global Standardisation: ISO, IEC, and ITU

The International Organization for Standardisation (ISO) and the International Electrotechnical Commission (IEC) develop multilayered standards across functional safety, cybersecurity, energy systems, and more. Their collaboration with the International Telecommunication Union (ITU) via the World Standards Cooperation seeks to minimise overlap and ensure global compatibility, especially for CPS technologies (ISO/IEC/ITU, 2012).

2.1.2 European Standardisation Bodies: CEN, CENELEC, and ETSI

Europe's standardisation landscape is shaped by three primary European Standards Organisations (ESOs): the European Committee for Standardisation (CEN), European Committee for Electrotechnical Standardisation (CENELEC), and the European Telecommunications Standards Institute (ETSI). These bodies hold legally recognized responsibility for developing harmonised European Standards (ENs) under Regulation (EU) No 1025/2012, which brings about a '*presumption of conformity*' necessary for market integration across the EU and EFTA territories (European Commission, 2016; CEN/CENELEC, 2024). Under the Vienna Agreement (ISO–CEN, 1991), nearly one-third of CEN standards are developed through joint ISO collaboration via parallel approval, ensuring mutual recognition and a '*one standard, one test–accepted everywhere*' framework (CEN/CENELEC, 2021; CENELEC Vienna press, 2021). The Frankfurt Agreement (CENELEC–IEC, 2016) similarly aligns electrotechnical standards, ensuring seamless transposition and coherence in numbering systems (e.g., EN IEC 60034 series).

2.2 Certification and Homologation, Pathways

This chapter explains how each Supply Chain in Cynergy4MIE reaches legal conformity and market entry, what standards and evidence are required, and where regulatory grey zones remain.

2.2.1 Cross cutting foundations

2.2.1.1 Scope and terminology

Certification is formal assessment against laws or regulations. Homologation is approval for placing products on the market or in service. Type approval is the road-vehicle procedure under EU law. CE marking demonstrates conformity for machinery and equipment under EU directives and regulations.

Acronyms used throughout 2.2 (expanded at first mention here):

- GSR General Safety Regulation (EU) 2019/2144
- RED Radio Equipment Directive 2014/53/EU
- LVD Low Voltage Directive 2014/35/EU
- EMC Electromagnetic Compatibility Directive 2014/30/EU
- SOTIF Safety of the Intended Functionality ISO 21448
- ODD Operational Design Domain
- PED Pressure Equipment Directive 2014/68/EU
- ATEX Atmosphères Explosibles IEC 60079 framework and related EU rules
- SORA Specific Operations Risk Assessment by JARUS
- NB Notified Body
- TAA Type Approval Authority

Functional safety is addressed by ISO 26262 for road vehicles and by machinery safety standards and IEC 61508 more generally ISO, 2018; IEC, 2010. Safety of the Intended Functionality is addressed by ISO 21448 ISO, 2022. A short glossary in Annex 2.2.B lists these terms with one-line definitions and a link to their primary legal or standards anchor.

2.2.1.2 EU legal backbone and international fora

On road vehicles follow the UNECE WP.29 regulatory system that is binding for EU type approval. Cybersecurity and software update governance are mandatory through UN R155 and UN R156 (UNECE, 2021a, 2021b). The General Safety Regulation mandates a suite of ADAS for new vehicles (European Commission, 2019). Machinery is covered by the current Machinery Directive 2006/42/EC and the new Machinery Regulation (EU) 2023/1230 which addresses autonomous and remote-controlled mobile machinery and AI based safety components (European Commission, 2006; European Commission, 2023a). Equipment using radio interfaces must comply with the Radio Equipment Directive (RED) (European Commission, 2014).

2.2.1.3 Standards common to several Supply Chains

Common standards across Supply Chains include ISO 26262 for functional safety of electrical and electronic systems, ISO 21448 for SOTIF, IEC 61508 as a general framework, and domain families such as ISO 13849 or IEC 62061 for machinery control systems (ISO, 2018; ISO, 2022; IEC, 2010). Where applicable, UNECE vehicle regulations provide performance requirements for systems such as lane keeping, emergency braking, and electromagnetic compatibility (UNECE, 2012; UNECE, 2019a; UNECE, 2021a; UNECE, 2021b).

2.2.1.4 Evidence package template and stage gate criteria

Across all Supply Chains the project will collect a small and consistent set of evidence artefacts. Hazard analysis and risk assessment with allocation to ASIL or Performance Levels. SOTIF analysis focused on misuse and environmental edge cases. Cybersecurity management and software update governance evidence where vehicles are in scope. Test and validation plan with scenario coverage. Certification and approval correspondence with authorities or Notified Bodies where relevant. Each Supply Chain section specifies the artefacts and the point in time when they are produced.

2.2.1.5 Ethics and societal guardrails common to all Supply Chains

All pathways incorporate human centric assurance such as privacy by design, explainability where appropriate, and user acceptance metrics. Supply Chain sections include callouts on societal acceptance, inclusion, and environmental impacts where the technologies are deployed.

2.2.2 SC1 Off road autonomous machines

2.2.2.1 Scope and operational context

SC1 focuses on automated vehicles and machinery operable in all weather conditions such as autonomous off-road equipment and self-driving transport in harsh environments. Certification spans on road vehicle regulations and off-road machinery safety.

2.2.2.2 Mandatory route to conformity and market entry

Off road and industrial autonomous machines follow ISO safety standards. ISO 17757:2019 provides safety requirements for autonomous and semi-autonomous earth moving and mining machines, addressing hardware and software criteria and additional hazards of automated operation (International Organization for Standardisation [ISO], 2019a). General functional safety for earth moving machinery is detailed in the ISO 19014 series defining required Performance Levels for control systems (ISO, 2018a). ISO 18497 applies to highly automated agricultural machines (ISO, 2018b). On road vehicles with automation invoke ISO 26262 and ISO 21448 to assure safe behaviour even in adverse conditions (ISO, 2018c; ISO, 2022). Off road automated machinery falls under the EU Machinery Directive and the new Machinery Regulation which explicitly covers autonomous and remote-controlled mobile machinery. Machines must satisfy essential health and safety requirements and carry CE marking. For high-risk machinery, a Notified Body must certify safety before market entry (European Commission, 2023a; TÜV SÜD, 2023a). Equipment that uses RF components must comply with the Radio Equipment Directive (European Commission, 2014).

2.2.2.3 Voluntary schemes and state of the art

Functional safety standards such as ISO 26262, IEC 61508, and ISO 19014 are not legally binding by name but are considered state of the art and de facto required to fulfil the safe design requirement under EU law (TÜV SÜD, 2023b). Voluntary certifications include TÜV SÜD or UL assessments for ISO 26262 or ISO 17757 compliance and UL 4600 for autonomous system safety assurance (UL, 2020).

2.2.2.4 Conformity assessment steps and artefacts

Risk assessment per ISO 12100 and design to harmonised standards. Functional safety analyses to ISO 13849 or IEC 62061 where applicable. Evidence of environmental robustness including ingress protection ratings. For machines using sensing and radio functions, RED documentation for radar or LiDAR. For high-risk cases, Notified Body technical file and certificate. For on road operation, type approval artefacts in line with vehicle regulations.

2.2.2.5 Open gaps and grey zones

There is no dedicated homologation category for fully autonomous work machines. Manufacturers apply general machinery safety standards which may not fully address AI and machine learning related hazards. The new Machinery Regulation addresses AI based safety components, but test protocols for AI driven perception are still under development (European Commission, 2023a; TÜV SÜD, 2023a). For on road performance in adverse conditions, there is no harmonised certification scheme for sensor and AI performance in snowstorms or heavy rain. ISO 21448 guides risk mitigation for edge cases, but liability and validation remain manufacturer driven (ISO, 2022).

2.2.2.6 Interfaces and dependencies with other Supply Chains

Sensor suites and power electronics depend on SC3. Radio and connectivity elements align with SC5 practices where used for coordination.

2.2.2.7 Societal and environmental considerations

Operator safety, bystander risk in harsh environments, and environmental robustness are central. Evidence of user training and safe fallback procedures in poor visibility conditions is required.

2.2.2.8 Outputs that feed other Work Packages

Risk and safety artefacts feed the system assurance activities and the demonstrator planning. Where on road operation is envisaged, type approval planning inputs feed SC4 integration.

2.2.3 SC2 Collaborative robots

2.2.3.1 Scope and operational context

SC2 involves collaborative robots and AI enabled machinery working alongside humans in manufacturing or in the construction of low emission buildings. Certification focuses on machinery safety and human robot collaboration.

2.2.3.2 Mandatory route to conformity and market entry

Industrial robot safety is governed by ISO 10218 Parts 1 and 2 which set requirements for safe design and integration of robot systems, covering hazards such as crushing, guarding, and emergency stops (Occupational Safety and Health Administration [OSHA], 2022a; ISO, 2011a, 2011b). For collaborative robots that share workspaces with people, ISO/TS 15066:2016 provides additional safety guidance including limits on robot speed, force, and permissible contact pressure during human interaction (ISO, 2016a; OSHA, 2022b). Additional standards relevant to collaborative robotics include ISO 13849 1 for safety design requirements using Performance Levels and IEC 61508 as a general functional safety framework (ISO, 2015; International Electrotechnical Commission [IEC], 2010). Collaborative robots are treated as machinery under EU law. Until 2026 they are regulated under the Machinery Directive 2006/42/EC which requires CE marking based on harmonised standards. The new Machinery Regulation introduces provisions for collaborative robots and AI components used in safety functions. High risk machinery categories including cobots with self-learning capabilities will require third party conformity assessment by a Notified Body (European Commission, 2006; European Commission, 2023a; TÜV SÜD, 2023). Where wireless technologies are integrated, the Radio Equipment Directive applies (European Commission, 2014). In occupational settings, national regulations such as OSHA guidance in the United States also shape workplace level safeguard practices (OSHA, 2022d).

2.2.3.3 Voluntary schemes and state of the art

Many manufacturers voluntarily seek TÜV or UL certification to demonstrate alignment with ISO 10218 and ISO/TS 15066. Emerging voluntary programs include the RIA Certified Robot Integrator in North America which certifies integrators based on implementation quality, safety, and adherence to RIA and ISO standards (RIA, 2022).

2.2.3.4 Conformity assessment steps and artefacts

Risk assessment per ISO 12100, design to ISO 10218, and where collaborative operation is intended, evaluation against ISO/TS 15066 contact parameters. Technical files with control system safety justifications to ISO 13849 1 or IEC 62061 as applicable. For radio functions, RED documentation.

2.2.3.5 Gaps and inconsistencies

Existing robot safety standards assume deterministic behaviour and do not fully address cobots with adaptive or machine learning based autonomy. The new Machinery Regulation requires special assessment of safety components with self-evolving behaviour, but technical guidance and implementation protocols remain under development (European Commission, 2023a; TÜV SÜD, 2023). ISO/TS 15066 remains a Technical Specification rather than a full standard and its human robot interaction data may not cover all real-world situations. Regulatory uptake varies internationally which contributes to inconsistencies.

2.2.3.6 Interfaces and dependencies with other Supply Chains

Vision systems and sensing align with SC3. Where mobile platforms are used, lessons from SC4 on perception and fallback can inform safe design.

2.2.3.7 Societal and environmental considerations

Human factors in shared workspaces and inclusive design of interaction limits are important. Evidence should address worker training and safe stopping behaviour in congested and dynamic sites.

2.2.3.8 Outputs that feed other Work Packages

Safety case elements and test data feed standardisation activities and demonstrator planning.

2.2.4 SC3 Electric powertrain and components

2.2.4.1 Scope and operational context

SC3 deals with advanced electric powertrain components, high efficiency power electronics, batteries, and sensors for electric vehicles, emphasising precision, reliability, and safety.

2.2.4.2 Mandatory route to conformity and market entry

Electric vehicle safety uses ISO and IEC standards and UNECE vehicle regulations. UNECE Regulation No. 100 is the core homologation standard for EV electrical safety and includes tests for REESS such as vibration, thermal shock, mechanical impact, fire resistance, short circuit, and overcharge protection (TÜV SÜD, 2023a; UNECE, 2021). Complementing this are the ISO 6469 series for electric shock protection and energy storage, IEC 62660 for lithium-ion traction battery performance, and ISO 12405 series for battery testing and system validation. UN Manual of Tests and Criteria, Section 38.3, is required for global shipment of lithium-ion batteries (ISO, 2019a; IEC, 2018; ISO, 2011a; UN, 2021). Functional safety is governed by ISO 26262 and cybersecurity by ISO 21434 (ISO, 2018a; ISO, 2021). In the EU, vehicle type approval under Regulation 2018/858 and General Safety Regulation 2019/2144 is mandatory. For EVs this includes compliance with R100, R10, R13 or R13h, and crash safety rules. Standalone products such as aftermarket batteries or off board chargers must comply with CE rules under the Low Voltage Directive and EMC Directive (European Commission, 2019). The new Battery Regulation 2023/1542 introduces labelling, recyclability, and carbon footprint rules (European Commission, 2023).

2.2.4.3 Voluntary schemes and state of the art

ISO 26262 process certification by third parties is widely used even when not legally mandated (TÜV SÜD, 2023b). Interoperability frameworks such as CharIN for CCS and Open Charge Alliance for OCPP run voluntary compliance schemes (CharIN, 2022; OCA, 2023).

2.2.4.4 Conformity assessment steps and artefacts

For batteries and power electronics, provide type approval test reports where integrated into vehicles. For standalone equipment, provide CE technical files under LVD and EMC. Provide functional safety evidence for BMS, inverters, and controllers. Provide cybersecurity development evidence for systems in scope of ISO 21434. Where applicable, provide UN 38.3 shipping test reports.

2.2.4.5 Gaps and grey zones

Wide bandgap devices switch faster and at higher voltages. Existing EMC and insulation standards are being revised, but certain tests for high dV/dt or partial discharge at MHz frequencies are lagging. Manufacturers often rely on in house or JEDEC based criteria until harmonised IEC protocols are finalised (PSMA, 2023). Emerging battery chemistries or formats may not be fully addressed in existing standards. Updates to R100 include thermal runaway propagation, but standards for second life batteries or hydrogen integration remain immature (UNECE, 2022). Novel sensors subject to general EMC and safety directives may lack dedicated validation frameworks and when safety relevant must be justified under ISO 26262 (ISO, 2018a).

2.2.4.6 Interfaces and dependencies with other Supply Chains

SC3 provides sensors and power electronics to SC1, SC4, and SC6 which directly influence functional safety and system behaviour.

2.2.4.7 Societal and environmental considerations

Battery sustainability obligations under the Battery Regulation impact design choices and documentation. Evidence should address recycling plans and safety in second life use.

2.2.4.8 Outputs that feed other Work Packages

Test evidence and process certifications feed assurance and standardisation tasks and inform vehicle integration work in SC4.

2.2.5 SC4 ADAS and ADS with V2X

2.2.5.1 Scope and operational context

SC4 encompasses Advanced Driver Assistance Systems and higher-level Automated Driving Systems for vehicles, including V2X connectivity and AI for extrinsic efficiency. Certification focuses on road traffic safety regulations, hardware and software functional safety, and emerging legal frameworks for automated driving.

2.2.5.2 Mandatory route to conformity and market entry

The automotive sector relies on UNECE WP.29. UN R79 covers steering equipment including lane keeping and certain automated lane changes, UN R152 mandates AEB for passenger cars, R131 for trucks, and UN R130 governs LDWS. UN R157 introduced in 2020 is the first regulation for Level 3 ADS which was extended in 2022 to 130 km/h with automated lane changing. UN R155 and UN R156 require cybersecurity and software update management systems for all new vehicle types (UNECE, 2019a; UNECE, 2022a; UNECE, 2021a; UNECE, 2021b). The General Safety Regulation mandates a broad suite of ADAS for all new vehicles and the Commission adopted a Delegated Regulation and an Implementing Regulation in 2022 for Level 4 ADS approvals including safety case, incident reporting, black box data, and cybersecurity assurance. V2X radios must comply with the Radio Equipment Directive and standards such as ETSI EN 303 613 and ETSI EN 302 571 (European Commission, 2019; European Commission, 2022a, 2022b; ETSI, 2021).

2.2.5.3 Voluntary schemes and state of the art

Euro NCAP ratings influence market acceptance for ADAS and Highway Assist. Developers may use UL 4600 for safety case reviews and UK BSI PAS 1880 for testing guidance. SAE J3016 provides the taxonomy for automation levels. SAE J3061 addresses cybersecurity process and SAE J3018 covers public road testing of ADS (Euro NCAP, 2023; Underwriters Laboratories, 2020; BSI, 2021; SAE International, 2016, 2021).

2.2.5.4 Conformity assessment steps and artefacts

Hazard analysis and risk assessment with ASIL allocation under ISO 26262, SOTIF analysis under ISO 21448, cybersecurity management system evidence under UN R155 and ISO 21434 where applicable, software update process evidence under UN R156, simulation and scenario coverage reports, and black box data and traceability from scenario to test result (ISO, 2018; ISO, 2022a).

2.2.5.5 Open gaps and challenges

There is no globally harmonised certification path for Level 4 or Level 5 autonomous vehicles. The EU regulation covers only certain vehicle types, and many ADS require exemptions or pilot authorisations at the national level which leads to fragmentation. Validation of AI driven behaviour is complex and standardised approaches like ISO 34502 are still maturing. V2X is not mandated in the EU which limits cooperative benefits and national divergence adds further complexity (European Commission, 2022a; ISO, 2023a; European Commission, 2019).

2.2.5.6 Interfaces and dependencies with other Supply Chains

SC5 multi agent co-operation relies on SC4 radio and security stacks. SC3 supplies sensors and power electronics that impact functional safety. Interoperability with SC1 off road platforms is relevant for shared perception methods.

2.2.5.7 Societal and environmental considerations

Driver trust, take over readiness, privacy by design for data, and the energy impact of compute must be evidenced. Acceptance criteria should be measurable and aligned with user research.

2.2.5.8 Outputs that feed other Work Packages

Evidence items on functional safety, SOTIF, cybersecurity, and validation feed standardisation tasks and demonstrator work. Type approval planning feeds governance work.

2.2.5.9 Scenario and data traceability into SOTIF and cybersecurity

Describe the trace from Operational Design Domain to scenarios to tests to logs to safety case pages. State the tool chain and the governance checkpoints. Link SOTIF and cybersecurity evidence to these traces (ISO, 2022a; UNECE, 2021a, 2021b).

2.2.6 SC5 Multi agent emergency response

2.2.6.1 Scope and operational context

SC5 involves multiple agents such as vehicles, drones, and robots that cooperate in real time for emergency response with V2X communication, collective sensing, and coordinated control.

2.2.6.2 Mandatory route to conformity and market entry

Inter vehicle and vehicle to infrastructure communications are defined by IEEE 802.11p and the European equivalent ETSI ITS G5 and by cellular interfaces LTE V2X and 5G NR V2X. Message level protocols such as SAE J2735 and ETSI EN 302 637 standardise CAM and DENM messages. Security is addressed by IEEE 1609.2 and ETSI TS 103 097. Radio units in the EU must comply with RED with presumption of conformity at 5.9 GHz demonstrated via ETSI EN 302 571 and ETSI EN 303 613. UNECE Regulation No. 10 addresses electromagnetic compatibility for vehicles. For UAVs and certain emergency pilots, approvals commonly follow JARUS SORA under EASA guidance for the specific category (Kenney, 2011; ETSI, 2017; 3GPP, 2017; SAE International, 2016; ETSI, 2014; IEEE, 2019; ETSI, 2020; European Parliament & Council, 2014; ETSI, 2017, 2020; UNECE, 2012; JARUS, 2024; EASA, 2025).

2.2.6.3 Voluntary schemes and state of the art

The Car 2 Car Communication Consortium and OmniAir conduct voluntary certification for device interoperability in DSRC and C V2X (C2C CC, 2022; OmniAir Alliance, 2021).

2.2.6.4 Conformity assessment steps and artefacts

Provide CE technical documentation for radio units under RED. Provide security credential management evidence and interoperability test reports. For deployments including UAVs, provide SORA documentation and operational risk mitigations.

2.2.6.5 Gaps and grey zones

System of systems safety remains unresolved. While each agent can be certified, the emergent behaviour of a distributed fleet lacks formal certification mechanism. Differences between SAE and ETSI messaging and security credential frameworks hinder cross border operation. Due to the voluntary nature of V2X deployment, first responders cannot assume integration with civilian vehicles. Cybersecurity for the whole multi agent ecosystem is not unified (Paden et al., 2016; ISO, 2020; European Commission, 2020; UNECE, 2021).

2.2.6.6 Interfaces and dependencies with other Supply Chains

SC5 depends on SC4 for in vehicle stacks and on SC3 for sensor performance that feeds cooperative perception.

2.2.6.7 Societal and environmental considerations

Privacy, data governance, and public trust are significant in emergency use. Evidence should address secure data sharing and safeguards for non-participants.

2.2.6.8 Outputs that feed other Work Packages

Interoperability test artefacts and security evidence feed standardisation and policy tasks.

2.2.7 SC6 Hydrogen and WBG based energy systems

2.2.7.1 Scope and operational context

SC6 applies advanced Electronic Components and Systems notably wide bandgap semiconductor power electronics to energy efficient hydrogen production and collaborative energy management such as smart control of heat pumps. Certification spans electrical safety, grid compliance for power converters, hydrogen technology standards, and intelligent control systems in distributed energy networks.

2.2.7.2 Mandatory route to conformity and market entry

Foundational semiconductor standards include IEC 60747 series with definitions for SiC and GaN devices. JEDEC JC 70 has issued reliability guidelines such as JESD 247 and coordinates with IEC (Power Sources Manufacturers Association [PSMA], 2023). For ECS based equipment, common standards include IEC 62477 1 for power converter safety, grid integration standards such as IEEE 1547 and EN 50549, and the IEC 61000 series for EMC required for CE marking (IEC, 2019). Smart energy communications use IEC 61850 for control protocols (IEC, 2013). For hydrogen production ISO 22734:2019 sets performance and safety benchmarks for water electrolysis-based hydrogen generators (ISO, 2019a). Additional standards include IEC 60079 for explosion protected equipment, the Pressure Equipment Directive 2014/68/EU for pressure vessels and piping, ISO 19884 and Regulation 79/2009 for on board hydrogen tanks, and IEC 62282 for fuel cell systems (European Commission, 2014; ISO/IEC, 2022).

2.2.7.3 Voluntary schemes and state of the art

ISO 50001 certifies energy management systems. AEC Q101 guides automotive grade semiconductor reliability. Interoperability seals from alliances such as EEBus and Energy@Home exist. Cybersecurity certification such as ISA or IEC 62443 and UL 2900 are pursued in industrial networks (ISO, 2018b; EEBus, 2022; ISA, 2021).

2.2.7.4 Conformity assessment steps and artefacts

Provide CE technical files under the Low Voltage Directive and EMC Directive for most equipment. Provide grid code certification under national rules such as VDE AR N 4105. For hydrogen installations provide PED conformity assessment and ATEX zone classification. For larger plants, consider Seveso III obligations and process safety under IEC 61511. Accredited labs such as DNV, TÜV, and CERTIFI perform tests and issue certificates (DNV, 2022; European Commission, 2012).

2.2.7.5 Gaps and grey areas

SC6 spans diverse technology silos and faces certification fragmentation. Wide bandgap electronics present EMC and insulation challenges that are not fully captured by current protocols which may require supplementary stress tests (PSMA, 2023). Standards for hydrogen embrittlement, high blend hydrogen pipelines, and hydrogen appliances are still being adapted (European Clean Hydrogen Alliance, 2023). Distributed intelligent control such as AI enabled energy microgrids lacks clear certification frameworks, although IEC and IEEE initiatives are considering AI (IEC, 2021).

2.2.7.6 Interfaces and dependencies with other Supply Chains

Power electronics and controllers' interface with SC3 devices and share EMC and safety considerations. Data and control strategies connect to SC5 communications in certain use cases.

2.2.7.7 Societal and environmental considerations

Safety of hydrogen production near communities, lifecycle impacts of batteries and semiconductors, and energy efficiency metrics must be documented. Evidence of safe failure behaviour and secure control in distributed networks is required.

2.2.7.8 Outputs that feed other Work Packages

Grid compliance and hydrogen safety artefacts feed standardisation activities. Energy management outcomes inform sustainability work.

2.2.8 Comparative view and system integration

2.2.8.1 What is mandated versus what is voluntary

On road automotive systems are shaped by UNECE regulations and GSR mandates. Machinery and energy systems rely on CE frameworks and harmonised standards, with third party assessment where risk is high. Voluntary schemes such as Euro NCAP, UL 4600, CharIN or OmniAir guide best practice and market acceptance (UNECE, 2022; European Commission, 2014; IEC, 2012; Euro NCAP, 2023; OmniAir Alliance, 2021; CharIN, 2022).

2.2.8.2 Where cross domain clashes may occur

Different conformity regimes can conflict when systems integrate. Examples include RED obligations for V2X with vehicle type approval, or grid code requirements for WBG converters that also need EMC compliance beyond current harmonised tests (ETSI, 2017; PSMA, 2023).

2.2.8.3 System of systems risks and mitigations

Safe subsystems do not guarantee safe systemic behaviour. Multi agent coordination and AI driven perception introduce emergent risks. Mitigations include scenario-based validation, security credential governance, and cross domain testbeds that exercise cooperative behaviours under stress (Paden et al., 2016).

2.2.8.4 Cross supply chain comparison matrix

Supply Chain	***Mandatory route***	***Primary standards***	***Key gaps***	***Dependencies***
SC1	*CE under Machinery framework; Machinery Regulation (EU) 2023/1230 applies from 2027; RED if RF sensors/comms; EU type approval only if public road use is in scope.*	*ISO 17757, ISO 19014, ISO 18497, ISO 12100; ISO 26262 & ISO 21448 where automotive-grade subsystems are used.*	*AI perception in adverse weather; no dedicated homologation category for fully autonomous work machines*	*SC3 sensors & power electronics; SC5 connectivity where used.*
SC2	*CE under Machinery framework and RED when wireless; Machinery Regulation (EU) 2023/1230 applies from 2027 with Notified Body for high-risk categories*	*ISO 10218-1/-2; ISO/TS 15066; ISO 12100; ISO 13849-1 or IEC 62061; IEC 61508.*	*Verifying adaptive/ML behaviour beyond deterministic assumptions; TS 15066 coverage limits in dynamic sites.*	*SC3 vision/sensing; SC4 perception & fallback practices for mobile platforms.*
SC3	*Vehicle type approval under Reg. (EU) 2018/858 and GSR 2019/2144 for integrated parts; CE under LVD/EMC for standalone items; Battery Regulation (EU) 2023/1542 obligations.*	*UNECE R100, R10; ISO 6469, ISO 12405; IEC 62660; ISO 26262, ISO 21434; UN 38.3 (shipping).*	*WBG converter EMC/insulation stress; second-life battery pathways and safety.*	*Supplies SC1, SC4, SC6 safety-relevant hardware.*
SC4	*EU type approval under GSR & UNECE; UN R155 & R156 (new types since Jul 2022, all new vehicles since*	*UN R79, R130, R152, R157; ISO 26262, ISO 21448; SAE J3016, J3018;*	*No single harmonised route for L4/L5; AI validation maturity; V2X*	*Relies on SC3 hardware; supports SC5 cooperative functions.*

	Jul 2024); Level 3 via UN R157; V2X radios under RED (EN 302 571; EN 303 613 for LTE-V2X sidelink where used).	*emerging ISO 34502.*	*fitment not mandated.*	
SC5	*CE under RED for radios; vehicle EMC via UN R10; UAV pilots under JARUS SORA within EASA "specific" category where relevant.*	*ETSI ITS-G5 (EN 302 663) or 3GPP LTE/NR V2X; EN 302 571 (radio); EN 302 637 / SAE J2735 (messages); IEEE 1609.2 / ETSI TS 103 097 (security).*	*System-of-systems safety; cross-border interoperability of stacks and credentials.*	*Uses SC4 in-vehicle stacks; SC3 sensors for cooperative perception.*
SC6	*CE under LVD/EMC; grid code certification (e.g., EN 50549 or IEEE 1547); PED & ATEX where applicable; Seveso for large plants.*	*IEC 62477-1; IEC 61000 series; IEC 61850; ISO 22734; IEC 60079; ISO 19884; IEC 62282.*	*WBG high-frequency effects not fully covered; evolving hydrogen infrastructure standards; certification for AI-enabled energy orchestration.*	*Interfaces with SC3 hardware; SC5 comms for smart control.*

2.2.9 Roadmap for pre normative action

Focus contributions on three areas. Validation of AI driven perception and decision making in adverse conditions using scenario-based methods and SOTIF principles. Interoperability and assurance for multi agent V2X ecosystems with security credential management and cross border message profiles. Wide bandgap converter EMC and insulation stress methods at high switching speeds to inform IEC updates (ISO, 2022a; ETSI, 2020; PSMA, 2023).

2.3 Human-Centric and Ethical Standardisation Trends

The following sections detail each Standardisation Cluster (SC1–SC6), highlighting the scope, relevant standards, usage by partners, gap analysis, and strategic actions. Repetitive boilerplate has been removed and tailored Pre-Normative Contribution boxes specify how each SC contributes to standardisation. These contributions align with the Grant Agreement and are timed to feed D7.9 and D7.10.

2.3.1 Emerging Trends in Ethical AI Standardisation (ISO, IEEE, OECD, EU AI Act, HLEG)

International and European efforts are converging on trustworthy, human-centric AI for CPS. The OECD AI Principles, first adopted in 2019 and updated in 2024, remain the leading intergovernmental benchmark: values-based principles on human rights, transparency, robustness and accountability, plus recommendations for implementation (OECD, 2019; OECD, 2024).

Technical bodies translate principles into practice. ISO/IEC JTC 1/SC 42 advances AI trustworthiness via ISO/IEC TR 24028:2020, which surveys attributes such as transparency, robustness, fairness and accountability that Cynergy4MIE can operationalise in design controls and audit trails (ISO/IEC, 2020). IEEE delivers implementable requirements: IEEE 7001:2021 defines measurable transparency levels for autonomous systems, and IEEE 7003 sets lifecycle processes to address algorithmic bias. These are directly relevant to SC4's explainability and fairness controls and to SC2/SC5 HRI use cases (IEEE, 2021; IEEE, 7003).

In road safety ethics, ISO 39003:2023 provides guidance on ethical considerations for autonomous vehicles. It does not prescribe outcomes or certify products; it structures how manufacturers incorporate ethical aspects into decision processes, a useful scaffold for SC4's HMI, handover and logging work (ISO, 2023).

Europe's legal framework now hard codes this direction. The AI Act, Regulation (EU) 2024/1689 of 13 June 2024, establishes risk-based obligations for high-risk AI (including safety components in transport), covering risk management, data governance, logging, transparency, human oversight and cybersecurity. Compliance will be supported by harmonised European standards developed through CEN-CENELEC JTC 21; where cited in the Official Journal, these standards provide a presumption of conformity. Cynergy4MIE should align controls and evidence with the forthcoming harmonised standards and use RHP artefacts (risk files, logs, HMI specifications) to demonstrate conformity (EU, 2024 — AI Act; CEN-CENELEC, 2024).

Implications for Cynergy4MIE.

- SC4: map IEEE 7001 transparency levels to ADS logging and driver/infrastructure communication; apply IEEE 7003 bias controls to perception and prediction models; use ISO 39003 to structure ethical justifications in the safety case (IEEE, 2021; IEEE, 7003; ISO, 2023).

- SC6: apply ISO/IEC TR 24028 governance and logging expectations to AI-assisted energy optimisation; ensure traceable human oversight in distributed control (ISO/IEC, 2020).
  Both streams feed the RHP (requirements → design controls → V&V evidence → certification interface), with concrete submissions timed for D7.9/D7.10.

2.3.2 Diversity, Equity and Inclusion (DEI) in AI Standardisation: Fairness, Accessibility & Bias Mitigation

DEI has shifted from aspiration to testable requirements. Under the AI Act, high-risk systems must use high-quality datasets and manage residual risks, bringing bias control and inclusive performance firmly into scope for conformity assessment. CEN-CENELEC JTC 21's programme anticipates harmonised standards for risk management, trustworthiness and conformity assessment that will specify how to evidence fairness, robustness and human oversight (EU, 2024 - AI Act; CEN-CENELEC, 2024).

Standards already offer levers. IEEE 7003 provides lifecycle processes to identify and mitigate algorithmic bias, and IEEE 7001:2021 requires explainability levels that help users and auditors understand outputs. Cynergy4MIE should pair these with scenario/test-set design that explicitly includes under-represented users and contexts (for example, disabled pedestrians, mobility aids, atypical gait) to avoid disparate performance in ADS perception and planning (IEEE, 7003; IEEE, 2021).

Accessibility intersects with safety regulation. The General Safety Regulation (EU) 2019/2144 phases in features such as driver drowsiness/distraction warnings, intelligent speed assistance and pedestrian/cyclist detection, improving safety for vulnerable road users and indirectly advancing equity. Use these mandated functions to ground SC4's DEI narrative with measurable benefits and to define inclusive HMI patterns (EU, 2019 - GSR).

Implications for Cynergy4MIE.

- SC4: adopt DEI-aware test protocols for VRU detection and behavioural prediction; report parity metrics across demographics and mobility aids; ensure HMI and external HMI are perceivable and understandable for diverse road users (IEEE, 7003; EU, 2019 - GSR).
- SC6: in building and grid control demos, validate that optimisation does not create inequitable comfort or cost outcomes across zones or user groups; log and explain energy allocation decisions to enable audit (ISO/IEC, 2020).
- Across SCs, channel findings into JTC 21 and related committees as pre-normative inputs on bias-resistant datasets, inclusive test suites and DEI-aware metrics, and record them as RHP evidence feeding D7.9/D7.10 (CEN-CENELEC, 2024).

In summary, Cynergy4MIE's emphasis on system convergence could highlight DEI gaps between sectors, for instance, ensuring that an integrated mobility-energy platform doesn't leave rural or digitally divided communities behind. The project is positioned to champion bias mitigation techniques, inclusive interfaces, and stakeholder co-creation in the pre-normative stage, thus influencing future standards and certifications so that diversity and inclusion are hardwired into convergent CPS technologies.

3. SC1 – Automated Machinery and Transportation

3.1 Description of SC and its Scope in Cynergy4MIE

Supply Chain 1 (SC1), titled "All-Weather Automated Machinery and Transportation," focuses on developing reliable, cooperative, high-performance automated systems capable of operating in challenging environments. SC1 addresses the needs of autonomous vehicles, mobile robots, and transport machinery across industrial, rural, and urban use cases, particularly under adverse weather or unstructured terrain conditions.

Within the Cynergy4MIE ecosystem, SC1 supports the mobility domain by contributing advanced sensor systems, adaptive control architectures, and data fusion strategies that ensure operational robustness under unpredictable physical conditions. Its scope includes both on-road and off-road platforms, converging vehicle automation with edge computing, environmental sensing, and cooperative AI decision-making. SC1 interfaces closely with foundational technologies in WP1 and WP4 and enables demonstrations involving autonomous driving, vehicle–infrastructure cooperation, and predictive maintenance. It also provides value across other SCs by ensuring automation and transport solutions are resilient, weather-tolerant, and interoperable with broader infrastructure and energy systems (e.g., SC1's robust perception feeds into SC4's ADS and SC6's grid interactions).

3.2 Existing Relevant Standards and Regulations

SC1 targets automated machinery and transport systems operating in adverse conditions. These systems require high levels of safety, dependability and environmental adaptability, so the relevant standards landscape spans industrial machinery safety, functional safety, sensor validation, and AI-assisted decision-making. Compliance with international and EU regulations is essential for market access and trust.

Functional Safety and Risk Management: SC1 must comply with ISO 26262 (road vehicle functional safety) for on-road automation, and with ISO 13849-1 / IEC 62061 for safety of control systems in off-road or industrial machinery (e.g. autonomous shuttles, smart agricultural or forestry equipment). ISO 21448:2022 (Safety of the Intended Functionality – SOTIF) is critical given SC1's emphasis on perception in adverse weather. Unlike ISO 26262 which addresses component faults, SOTIF covers performance limitations of correctly functioning systems (e.g. sensors in fog or glare).

Perception Sensor Validation (Adverse Conditions): SC1 demonstrators (e.g. Demo 1.1 and Demo 1.4) rely on enhanced vision technologies, so standards for testing and calibrating sensors are critical. For example, IEC 60825 governs laser safety for LiDAR, and IEC 60068 defines environmental testing (vibration, temperature, humidity) to ensure sensors remain reliable in harsh conditions. ISO 12100 (general machinery safety principles) provides a unified risk assessment methodology for integrated sensor platforms. **Draft or emerging standards** such as the proposed ISO 13228 (automotive LiDAR test methods) are monitored as candidate references; Cynergy4MIE partners are actively contributing to the development of such standards to ensure safe automated driving requirements (e.g. performance in rain/fog) are addressed. *(Note: Details on draft standards under development are tracked in Annex "Candidate Standards Under Monitoring" rather than in the main text.)*

AI-Driven Decision-Making and HRI: The integration of AI for perception and motion planning in SC1 demands alignment with emerging AI governance standards. ISO/IEC TR 24028:2020 (trustworthy AI characteristics) provides principles for explainability, robustness and fairness, complementing impending requirements of the EU AI Act for high-risk AI systems. IEEE 7001-2021 offers metrics for transparency in autonomous systems – useful as SC1 develops human-machine interfaces (HMI) that allow understandable and traceable decisions in machinery. This support demonstrating that SC1's AI components meet ethical and safety expectations (e.g. providing operator feedback or intervention options in autonomous machinery).

Machinery Regulation and CE Marking: Automated machinery in SC1 falls under the current EU Machinery Directive 2006/42/EC, requiring CE marking by meeting essential safety requirements via harmonised standards. From January 2027, the **Machinery Regulation (EU) 2023/1230** will apply, introducing stricter rules for machinery with AI and robotics (including potential mandatory third-party assessments for self-evolving systems). SC1 developments anticipate these changes. Conformity with related directives – Low Voltage (2014/35/EU), EMC (2014/30/EU), Radio Equipment (2014/53/EU) – is addressed for platforms with wireless connectivity and complex electronics.

Cybersecurity and Data Integrity: SC1 systems with edge AI or remote updates must comply with UNECE WP.29 Regulation R155 (vehicle cybersecurity) and follow ISO/SAE 21434 (cybersecurity engineering). Together, these provide a framework for threat assessment, risk mitigation, and post-deployment security monitoring. This is crucial as SC1's autonomous machines may connect to networks or receive OTA updates, requiring robust cybersecurity certification akin to road vehicles.

Conclusion and Outlook: SC1 must align with a mosaic of standards spanning functional safety, machinery integration, AI trustworthiness, and sensor performance in complex environments. The project's active role (e.g. contributing to new LiDAR test method standards and providing feedback on AI transparency guidelines) reflects a commitment to shaping future regulations for adverse-weather-capable autonomous systems. These contributions ensure SC1 innovations not only meet current standards but also help define next-generation norms for safety and performance.

3.3 Standardisation Usage and Insights from Technical Partners – SC1

A partner survey for SC1 highlighted usage of a broad array of standards in current practice:

- **Safety and Control Standards:** ISO 26262 (functional safety for automotive E/E systems) is used as a reference for safety-critical control logic. ISO 21448 (SOTIF) is applied in planning validation tests, especially under uncertain environments (partners reported using scenario-based stress tests to cover edge cases like sensor blindness in heavy rain). For industrial machinery contexts, ISO 13849, IEC 61508 and IEC 62061 are widely followed, ensuring safety-related parts of control systems meet required Performance Levels (PL) or SIL levels.

- **Operational Standards:** ISO 12100 (risk assessment) and IEC 60204-1 (machinery electrical safety) are well-known among SC1 partners, providing baseline processes for designing safe automated equipment. IEEE 2846 (Assumptions for Automated Driving Decision-Making) was noted conceptually as a guide for documenting the bounds of AI decisions in uncertain environments, although formal adoption in SC1 is at an early stage.
- **Gaps in Practice:** While standards are known, partners indicated that **no specialised standard fully covers off-road autonomous operation under all-weather conditions**. They rely on internal best practices and cross-references from automotive standards. For instance, testing autonomous agricultural robots in mud or snow required custom procedures, since existing road vehicle sensor standards assume paved conditions. This underscores a gap that SC1 aims to address through pre-normative contributions (see Section 3.5).

3.4 Gap Analysis

Identified Gaps: SC1's analysis reveals several gaps where current standards do not fully support the needs of all-weather automated machinery:

Perception in Adverse Conditions: Lack of standard test protocols for sensor suites under extreme weather (rain, fog, dust) and terrain conditions. Existing automotive standards cover normal environmental ranges; SC1 found the need for extended test cases (e.g. LiDAR in heavy fog, radar interference in snow) beyond ISO 16750 or IEC basic environmental tests.

AI and Autonomy in Machinery: Emerging AI functionalities (e.g. autonomous pathfinding in off-road settings) are not explicitly covered in machinery safety standards. There is a gap in integrating AI risk management (as per AI Act) with machinery functional safety processes.

Interoperability: Autonomous machinery interacting with infrastructure (V2X for work zones, or platooning vehicles in a mine) faces a gap in interoperability standards. No **single framework** ensures that an off-road vehicle and a road vehicle can communicate intentions or warnings seamlessly.

These gaps suggest a strategic need for SC1 to push the boundaries of existing standards and contribute new requirements or test methods.

3.5 Strategic Gap: Absence of Specific Contributions to Standardisation Bodies

To close the above gaps, SC1 will undertake specific pre-normative contributions. These are focused on sensor testing under adverse conditions and cross-domain harmonisation of safety approaches for automated machinery:

Pre-normative contribution (SC1):

Committee: ISO/TC 22/SC 32 (Road vehicles – Electrical and electronic components)

Artefact: Adverse-weather LiDAR test methodology and scenario library (contributions to ISO 13228 development)

Responsible Partner(s): VTT (via national body) with XenomatiX

Target Submission: M24 (input provided during ISO CD/DIS stages)

(Rationale: SC1 will formalise a library of edge-case scenarios (fog, heavy rain, snow) for LiDAR and sensor validation. These will be contributed to the ongoing ISO/TC22/SC32 work on LiDAR test methods, ensuring the standard reflects safe automated driving requirements in adverse conditions. VTT leads this effort, leveraging its role in CEN/TC278 and liaison with ISO, with support from LiDAR manufacturer XenomatiX.)

In addition, SC1 will liaise with **CEN/TC 114 (Safety of Machinery)** to share findings on applying AI in autonomous industrial vehicles, aiming to seed future guidance on AI-driven risk assessment in machinery. The above actions will be documented in D7.9 (for initial engagement) and D7.10 (with detailed results by M30), aligning with T7.4's objective to deliver tangible inputs to standardisation bodies.

4. SC2 – Smart Collaborative Robotics

4.1 Description of SC and its Scope in Cynergy4MIE

Supply Chain 2 (SC2), titled "Digital Manufacturing, Robotics, and AI for the Construction of Low-Emission Buildings," addresses the integration of collaborative robotics, AI-enhanced human–machine interaction, and digital manufacturing, with a special emphasis on sustainable construction. SC2 is part of Cynergy4MIE's Digital Industry domain and supports the Society 5.0 vision by enabling safe, efficient, and ergonomic co-working between humans and robots across the industrial production value chain, from design and assembly through to verification in manufacturing and construction.

At its core, SC2 advances **fenceless human–robot collaboration (HRC)** by developing body-near sensor systems, real-time perception algorithms, and intelligent safety envelopes that allow robots to interact with humans in dynamic, unstructured environments without physical cages. This includes innovations like wearable sensors for worker proximity detection, AI-driven robot motion planning that yields to human presence, and adaptive safety zones that adjust based on context.

A key emphasis of SC2 is the construction sector, which has historically lagged in digitalisation and automation. Cynergy4MIE aims to change this by deploying a fully integrated *Digital Twin* framework capturing the entire building lifecycle, from parametric design and robotic fabrication (e.g. timber modules) to on-site assembly and quality verification. Demonstrators under SC2 include **Demo 2.1: Digital Twin for Sustainable Housing** (applying robotics and AI to assemble low-emission building components) and **Demo 2.2: Fence-Free Smart Factory Robotics** (validating safe large-scale HRC in a factory setting). By integrating AI, robotics, and digital twins, SC2 envisions robots not as replacements but as intelligent collaborators that expand access to skilled work, improve safety, and boost productivity. SC2 also forms cross-links with SC1 (sharing perception tech for outdoor robots), SC4 (co-opting some ADS sensor fusion techniques for robot autonomy), and SC6 (ensuring factory energy management is intelligent and efficient).

4.2 Existing Relevant Standards and Regulations

SC2 operates at the intersection of collaborative robotics, AI-enabled human–robot interaction, and intelligent manufacturing in dynamic, partially structured environments. Its regulatory and standardisation context spans multiple domains, including industrial safety, functional safety of machinery, AI ethics, and data privacy. Key applicable standards and regulations include:

- **Collaborative Robotics Safety:** The foundational standards governing HRC are ISO 10218-1:2011 and ISO 10218-2:2011 (safety requirements for industrial robots and robot systems), along with the technical specification ISO/TS 15066:2016 which specifically addresses collaborative robot safety (e.g. defining safe force/contact limits for robots interacting with humans). SC2's fenceless HRC solutions are designed in conformity with these standards – e.g. ensuring that any contact forces in Demo 2.2's large robot arm are within ISO/TS 15066 pain tolerance curves. SC2 pushes these standards to their limits by using virtual boundaries and dynamic speed control instead of physical cages.
- **Functional Safety of Control Systems:** SC2's robotic systems must meet functional safety requirements akin to those in ISO 13849-1 and IEC 62061, which define design principles and performance levels (PL) or SIL for safety-related control systems. For instance, the emergency stops and power limiters on the collaborative robots follow Category 3 PL d architectures per ISO 13849. These ensure that even in the event of a fault (sensor failure, communication loss), the system defaults to a safe state. SC2 also considers IEC 61508 (general E/E/PE functional safety) as a guiding umbrella for its AI-based control logic, treating the AI components as configurable items whose failures need bounding.

- **Human-Centred Design and Ergonomics:** Given SC2's strong emphasis on inclusion and worker safety, human-centred standards play a key role. ISO 9241-210:2019 (ergonomics of human-system interaction – human-centred design) informs the design of SC2 interfaces and workflows to ensure systems are **intuitive and reduce cognitive load** for operators. In practice, this means SC2's robot programming interfaces and AR/VR visualisations for the digital twin are tested for usability and accessibility. Additionally, ISO/TR 23482 (guidelines for safe integration of robots in the workforce) – although still in technical report form – is used as a reference for best practices (e.g. training requirements and change management when introducing collaborative robots to a construction site).

- **Ethical AI and Data Protection:** SC2's AI-driven perception and adaptation functions invoke standards related to ethical AI and privacy. ISO/IEC TR 24028:2020 (trustworthy AI) provides high-level guidance which SC2 applies to ensure transparency and accountability in robot decision-making (for example, SC2's vision AI that monitors worker posture will log its decisions for auditability, addressing transparency). Moreover, because SC2's robots may handle personal data (e.g. imaging workers for safety), compliance with the EU GDPR is mandatory – privacy-by-design measures are integrated (face blurring, local processing of video feeds). The forthcoming harmonised standard under the EU AI Act is anticipated; SC2 pre-empts this by implementing human oversight and risk management processes for its AI as if it were "high-risk" under the AI Act criteria.

- **Machinery Regulatory Framework:** SC2's robotic systems in manufacturing and construction fall under the EU Machinery Directive and its successor regulation. As noted, the new Machinery Regulation (EU) 2023/1230 explicitly includes robots and AI-powered machinery. SC2's developments are aligned with this regulation's likely requirements, such as **automatic monitoring of safety functions** and logs for any AI-driven changes in behaviour. SC2 also tracks CEN/CENELEC standardisation work on AI in machinery safety (e.g. prEN ISO 24089 on safety of AI systems in machinery, if published, would be adopted).

- **Construction Standards and Building Codes:** Because SC2 involves on-site robotic construction (Demo 2.1), it touches on building regulations and standards for construction processes. While these are not traditional "robotics" standards, SC2 must ensure that robotic assembly techniques produce structures meeting Eurocode standards (e.g. EN 1995 for timber structures). Moreover, SC2's push for **sustainable materials** in construction robotics has led it to engage with committees on construction product standards – for example, partners contribute to discussions on adapting timber construction standards to accommodate robot-fabricated joints and novel composites. This aligns with EU goals for sustainable construction and will be further reported in an annex on standards under monitoring (such as any forthcoming CEN Workshop Agreement on AI in construction).

4.3 Standardisation Usage and Insights from Technical Partners – SC2

Survey contributions from SC2 partners (industry and research) provide insight into current standardisation practices:

- **Use of HRC Standards:** Nearly all partners involved in robotics noted using ISO/TS 15066 as a reference when setting up collaborative robot applications. For instance, a partner deploying a robotic assistant in a prefab construction line calibrated the robot's speed and separation monitoring according to ISO/TS 15066 guidelines. However, partners also commented that these standards assume a factory setting, adapting them to a partially unstructured environment (like a construction site in Demo 2.1) required additional risk analysis beyond the standard's scope.

- **Digital Twin and Data Standards:** Some SC2 partners highlighted the use of the ISO 23247 series (Digital Twin framework for manufacturing) as a guiding reference in building SC2's digital twin. This ensured interoperability (via standard data models) between the building design software and the robotic controllers. Adherence to these emerging standards is helping SC2 demonstrate how a **standardised digital thread** can improve quality control in construction (e.g. using the digital twin to verify dimensions of robot-assembled components against ISO 10303 (STEP) models).

- **Privacy and Safety Integration:** A unique insight from SC2 is the interplay of safety and privacy. Partners implementing vision systems for HRC (to monitor worker position and fatigue) had to juggle safety camera requirements (EN 61496 for electro-sensitive protective equipment) with GDPR compliance. Their solution, running on-edge pose detection and not transmitting identifiable images, was guided by following **"privacy-by-design" principles in tandem with functional safety standards**. The survey indicates this is a nascent area with no unified standard, confirming a gap at the intersection of robotics and data protection.

In summary, SC2 partners align with key robotics and safety standards, and actively incorporate data protection best practices. However, their experiences show that **no single standard yet covers AI-driven, privacy-sensitive collaborative robotics**. This reveals a structural gap: current robot safety standards do not integrate requirements from privacy regulations, and vice versa. The technical and organisational measures our partners developed (like anonymisation of camera feeds) are potential pre-normative inputs to future standards (see Section 4.5).

4.4 Gap Analysis

Identified Gaps: SC2's analysis surfaces critical gaps in the standardisation framework for collaborative robotics and AI in manufacturing/construction:

- *Dynamic Risk Management:* Current robot safety standards (ISO 10218 series) assume relatively static risk scenarios. SC2's use cases feature robots that learn or adapt (e.g. varying their task based on AI vision input or human worker behaviour). There is a gap in standards regarding **adaptive or learned robot behaviours**, how to classify and validate risk when the robot's responses are not pre-programmed but evolving. No formal standard yet covers validating machine learning in safety-critical HRC contexts.
- *Integration of Privacy and Safety:* As noted, robotics standards do not incorporate personal data protection requirements. Conversely, GDPR and AI ethics guidelines are not specific enough for robotics. This gap leaves implementers to figure out ad hoc solutions. SC2 identifies the need for either extended robotics safety standards or a new guideline that **merges safety and privacy** for collaborative robots (ensuring, for example, that safeguarding systems can use camera data without infringing privacy).
- *Scaling HRC to Construction Sites:* Standards like ISO 10218/TS 15066 mainly address factory settings with relatively small robots (<15 kg usually). SC2's construction demo uses heavy robots (>50 kg payload) in outdoor or semi-completed building environments. There is a gap in standards for **large-scale HRC** (both in terms of robot size and environment complexity). Issues include lack of standard metrics for safe separation when human and robot traverse the same large workspace, and absence of guidance on environmental variability (uneven ground, weather) in HRC.

These gaps underscore the need for SC2 to inform and influence standards such that the next generation of HRC standards cover AI adaptivity, privacy integration, and out-of-factory applications.

4.5 Strategic Gap: Absence of Specific Contributions to Standardisation Bodies

SC2 will proactively contribute to bridging these gaps by feeding its findings and innovations into relevant standardisation bodies. In particular, it will target the robotics safety community and AI ethics standard groups to influence emerging norms:

Pre-normative contribution (SC2):

- **Committee:** ISO/TC 299 (Robotics) – Working Group on safe human–robot collaboration
- **Artefact:** HRC safety requirements for adaptive robotics (white paper and use-case data to support extending ISO 10218/TS 15066 for dynamic environments)
- **Responsible Partner(s):** TH Rosenheim (construction robotics lead), Fraunhofer (human–AI interaction)
- **Target Submission:** M30 (propose new work item or technical report via national standards bodies)

(Rationale: SC2 will compile results from its fence-free robotics demos – including human physiological data and robot incident logs – to propose concrete new requirements for collaborative robot standards. For example, it will recommend threshold values and test methods for ***dynamic safety-envelopes*** *and outline how to include AI-driven speed and separation monitoring in standards. The target is an ISO/TC299 working group or an IEEE Robotics & Automation Society initiative on robot interoperability, timed to influence the next revision cycle of ISO 10218.)*

Additionally, SC2 will engage with **CEN/TC 310 (Advanced automation in manufacturing)** to share its **Digital Twin** integration approach. By doing so, SC2 contributes to standardising interfaces between digital construction models and robotic systems, ensuring interoperability. Finally, SC2 partners (e.g. CONV and SAL) will participate in European **AI standardisation** discussions (such as CEN-CENELEC JTC 21 on AI) to raise the specific needs of robotics under the AI Act – pushing for guidance on reconciling safety and privacy. These efforts will be initially reported in D7.9 (cataloguing interactions with ISO/TC299, CEN and IEEE) and detailed in D7.10 with any formal proposal documents submitted.

5. SC3 – Powertrains

5.1 Description of SC and its Scope in Cynergy4MIE

Supply Chain 3 (SC3), titled “Advanced Powertrains and Energy Storage Systems,” focuses on innovative components and control strategies for electric and hybrid powertrains, including next-generation batteries, power electronics (wide-bandgap semiconductors), and drivetrain control for improved efficiency and reliability. SC3 advances technologies like novel torque sensors for motors, AI-enhanced battery management systems (BMS), and resilient inverter/converter designs using Silicon Carbide (SiC) and Gallium Nitride (GaN) devices. The aim is to achieve higher power density, efficiency, and safety in vehicular powertrains and in stationary energy storage that interfaces with the grid.

SC3 demonstrators illustrate this scope: **Demo 3.1** develops electric drives with novel magneto-elastic torque sensors for fail-safe, optimal motor control; **Demo 3.2** implements a modular smart battery with an AI-based digital twin for predictive health management; **Demo 3.3 and 3.4** showcase SiC- and GaN-based power converters and their integration. Through these, SC3 contributes not only to automotive electrification (supporting SC4’s electric ADS platforms) but also to cross-sector energy convergence (feeding insights to SC6 on integrating vehicle batteries with smart grids). SC3 is tightly linked with WP3 (components and sensors) and WP5 (validation), ensuring new devices meet automotive-grade reliability and that validation data feeds into standardisation efforts.

5.2 Existing Relevant Standards and Regulations

SC3 spans the automotive and electronics domains, so its standards landscape includes automotive functional safety and environmental standards, as well as semiconductor and battery-specific standards:

- **Automotive Functional Safety and Performance:** As electric powertrain components will be used in vehicles, ISO 26262 (functional safety) applies to SC3 developments (in particular Part 5 and Part 11 for hardware development and guidelines on semiconductor development). For example, the design of the AI-enhanced BMS in Demo 3.2 follows ISO 26262’s ASIL decomposition principles, ensuring the BMS’s critical monitoring functions have redundancy or fail-safe behaviour. Additionally, UN Regulation R100 (safety of electric vehicle battery systems) provides requirements such as overcharge protection and thermal propagation resistance, which SC3’s battery demonstrator designs adhere to. The new General Safety Regulation (EU) 2019/2144 mandates features like battery state-of-health monitoring; SC3’s smart battery aligns with these expectations.
- **Battery Standards:** SC3 leverages standards for battery testing and safety, like IEC 62660 (Li-ion battery testing for automotive), ISO 12405 (EV battery system tests), and UNECE R136 (electric vehicle battery safety for L-category vehicles, applied as

guidance). The project also tracks upcoming standards for novel battery chemistries; for instance, if SC3 explores solid-state cells, it will refer to pending updates in IEC standards for abuse testing. In terms of sustainability, SC3 is aware of the EU Battery Regulation's requirement for battery passports and eco-design – while not a "standard," it references IEC and ISO standards for measurement and durability that SC3 uses to benchmark its battery performance.

- **Power Electronics and WBG Semiconductors:** For the SiC/GaN power converters, SC3 follows standards and industry guidelines on qualification and reliability of semiconductors. JEDEC standards (e.g. JESD47 for stress-test-driven qualification) and AEC-Q101/102 (automotive qualification of discrete semiconductors) are being applied to ensure SC3's devices meet automotive reliability criteria. **Notably, there is currently no fully consolidated international standard specifically for wide-bandgap (WBG) power device reliability;** however, work is underway in IEC TC47. SC3's industrial partners (e.g. Infineon, SAL) bring their involvement in **IEC TC47/WG8** (Wide Bandgap Semiconductor standards) to the project. This ensures SC3's testing (like 120k-hour accelerated life tests introduced in Demo 3.3) are aligned with emerging industry consensus.
- **Condition Monitoring and Prognostics:** SC3's use of AI for health management (motor and battery prognostics) taps into standards such as IEEE 1856-2017 (Standard Framework for Prognostics and Health Management of Electronic Systems). SC3 uses these frameworks to structure how data from sensors (torque, temperature, etc.) is used to predict failures. Similarly, ISO 13374 (condition monitoring data processing) and ISO 13381-1 (prognostic techniques) guide how SC3's digital twin communicates its diagnostics. These standards, traditionally applied in industrial machinery, are being extended by SC3 into the automotive powertrain realm.
- **Environmental and EMC Standards:** SC3 components are subject to the typical automotive environmental standards (ISO 16750 series for electrical/electronic components' environmental conditions) and electromagnetic compatibility standards (UN ECE R10, CISPR 25). For instance, the new high-frequency GaN inverter in Demo 3.4 must meet R10 EMC limits; SC3's partner labs follow CISPR 25 to test radiated and conducted emissions and refine filter designs accordingly.

Overall, SC3 navigates a blend of mature automotive standards and rapidly evolving standards for new technology (WBG semiconductors, AI prognostics). This duality means SC3 both conforms to known standards and contributes to shaping the ones that are still in flux.

5.3 Standardisation Usage and Insights from Technical Partners – SC3

The Task 7.4 questionnaire for SC3 revealed how partners are using and perceiving standards in the powertrain domain:

- **Wide-Bandgap Device Standards:** Partners developing SiC/GaN components noted reliance on internal qualification methods due to the lack of specific international standards. They do, however, use IEC 60747-17 (generic rules for power semiconductor devices) and align with draft criteria being discussed in IEC TC47/WG8. One partner mentioned contributing data to an **IEC repository on WBG device failure modes**, indicating SC3's direct input to standards under development.

- **Battery Management and Safety:** Automotive OEM partners in SC3 highlighted their use of ISO 6469-1/2/3 (safety specs for EV rechargeable energy storage systems) as a baseline in Demo 3.2's design. They also follow upcoming ISO 21434 (cybersecurity) for the BMS's connectivity, given that wireless battery management systems need secure communication. The survey shows strong awareness that **standards ensure acceptance**: e.g., demonstrating compliance with ISO 6469 parts helped an SME partner convince a car maker to consider their battery module, illustrating how being "standards-aligned" boosts credibility.

- **Gaps in AI Integration:** Partners using AI in powertrain control (like AI for predictive battery diagnostics) pointed out that functional safety standards lack explicit guidance for AI. They are managing this by applying concepts from ISO/PAS 21448 (SOTIF) for the battery domain (identifying unknown unsafe conditions in algorithms). But they acknowledge this as a **grey area**: no standard yet tells how to ASIL-decompose a neural network in a motor controller. This insight reinforces SC3's drive to influence future standards or best practices for AI in safety-critical control.

- **Condition Monitoring Data:** On condition monitoring, partners use ISO 13372/13373 terminology and procedures to structure data from Demo 3.1's torque sensors. However, they note **no automotive-specific condition monitoring standard** exists (unlike aerospace ARP standards). They consider their work as pioneering an automotive PHM approach that could eventually be standardised.

In essence, SC3 partners are blending adherence to current automotive E/E standards with exploratory application of industrial reliability and PHM standards. They see clear standardisation gaps around WBG reliability and AI in control systems, which SC3 is positioned to fill with its pre-normative outputs.

5.4 Gap Analysis

Identified Gaps: SC3's analysis finds several standardisation gaps that could impede the full exploitation of its innovations:

- *Wide-Bandgap Semiconductor Qualification:* There is no dedicated international standard detailing test and qualification methods for SiC/GaN power devices at the level needed for automotive homologation. Existing standards (like JEDEC) are not harmonised globally or across industries. This gap means each manufacturer currently develops custom stress tests – a duplication of effort and potential inconsistency that SC3 can help reduce by pushing for standard test protocols.

- *AI in Safety-Critical Powertrain Control:* Functional safety standards (ISO 26262) do not yet incorporate guidelines for machine learning components. The absence of any **standardised approach to validate AI/ML** in, say, a motor controller or BMS, is a gap. It leaves questions on how to certify these AI-augmented components. SC3 identifies the need for at least a technical report or guideline to supplement ISO 26262 in this area (perhaps analogous to ISO TR 5469 currently being discussed for AI safety).

- *Interfacing Vehicle Batteries with Infrastructure:* SC3's work on intelligent batteries overlaps with SC6's energy domain, revealing a gap in interoperability standards. ISO 15118 (EV charging communication) covers the basics of vehicle-to-grid communication, but SC3's scenario of **using a vehicle battery as part of a distributed energy resource** highlights missing pieces, e.g., standard protocols for real-time state-of-health sharing with the grid operator, or unified safety frameworks for on-vehicle and off-vehicle battery usage.

- *Condition Monitoring and Prognostics Standardisation:* While standards exist for condition monitoring in general, there is no tailored standard for automotive powertrain prognostics. This gap may not be critical for regulation yet, but it matters for industry adoption. A common language and metrics for prognostics (like remaining useful life estimation accuracy) would help compare solutions. SC3's demos produce exactly these kinds of metrics, which could seed a future standard or best-practice guideline.

5.5 Strategic Gap: Absence of Specific Contributions to Standardisation Bodies

SC3 will contribute to standardisation in areas such as WBG device testing and reliability data sharing, as well as frameworks for AI in powertrain control. Key planned contributions include:

Pre-normative contribution (SC3):

- **Committee:** IEC TC 47/WG 8 (Semiconductor devices – Wide bandgap semiconductors)

- **Artefact:** Reliability test protocols and mission-profile-based qualification data for automotive SiC/GaN devices

- **Responsible Partner(s):** Silicon Austria Labs (SAL), Infineon (IFAT)

- **Target Submission:** M30 (input to new IEC Technical Specification draft)

(Rationale: SC3 partners SAL and IFAT will compile the results of 120,000-hour HALT (Highly Accelerated Life Test) on GaN devices and field data from Demo 3.3 into a proposed set of qualification stressors and lifetime models. By contributing this to IEC TC47/WG8, the project

accelerates the establishment of industry-wide standards for WBG reliability, moving from proprietary methods to agreed test methods.)

Additionally, SC3 will prepare a position paper for **ISO/TC22/SC32 or SC36** (road vehicle E/E and electrical safety committees) outlining an approach to incorporate ML components into safety analysis – effectively suggesting content for a future ISO 26262 amendment or a new ISO PAS on AI elements in automotive control. SC3 will also engage with **IEEE P2851** (a project on dependability lifecycle interoperability) by providing its use case of integrating functional safety with reliability and security for an electric powertrain, ensuring the standard under development reflects automotive needs.

Finally, for vehicle-to-grid integration, SC3 in collaboration with SC6 will channel findings to the **CharIN alliance** (Charging Interface Initiative) working groups, since industry alliances often predate formal standards in this area. By Month 24 (D7.9) SC3 will have established contacts with these bodies and shared preliminary results, and by Month 30 (D7.10) it aims to have concrete contributions (data sets, draft text, proposed requirement lists) submitted or in review.

6. SC4 – Automated Driving Systems

6.1 Description of SC and its Scope in Cynergy4MIE

Supply Chain 4 (SC4), titled “Emergent Automated Driving Systems for Extrinsic Efficiency in Mobility,” targets the development of safe, adaptive, and collaborative driving systems through a multi-layered integration of sensors, AI, V2X communication, and edge computing. SC4 encompasses both Advanced Driver Assistance Systems (ADAS) and higher-level Automated Driving Systems (ADS) for road vehicles, including the connectivity (V2V, V2I, V2X) and distributed intelligence needed to optimise traffic flow and vehicle cooperation. The concept of “extrinsic efficiency” is central: SC4 focuses on how automated vehicles can dynamically adapt their behaviour not only based on onboard perception, but also through external information exchange with other vehicles and infrastructure, thereby improving overall system efficiency (traffic throughput, energy usage) beyond what a single vehicle could achieve alone.

Core SC4 innovations include:

- Low-latency V2X communication architectures to support predictive traffic flow optimisation;
- Machine learning algorithms for object detection, VRU behaviour prediction, and edge-case scenario recognition;
- Multi-modal sensor fusion across radar, lidar, cameras, TPMS, and satellite imagery (InSAR);
- Real-time road condition mapping using crowd-sourced vehicle sensor data and digital twins;
- Resilient HMI and conflict detection mechanisms leveraging formal methods (e.g. linear temporal logic, qualitative spatial reasoning).

The SC4 demonstrators include:

- Demo 4.1 – Traffic Flow Optimisation: Evaluation of mixed traffic systems (manual, semi-automated, and fully automated vehicles) in terms of throughput, safety, and energy use using V2X-enriched traffic simulation (led by AVL, DRIVEU, TUG, IFAT).
- Demo 4.2 – Road Condition Monitoring: Deployment of collaborative sensing frameworks using onboard sensors (TPMS, odometry), InSAR, camera-based AI, and lidar-equipped digital twins to estimate friction coefficients, detect surface anomalies, and improve vehicle decision-making under dynamic conditions (led by VIF, XenomatiX, FHG, InSAR).

SC4 also anchors Task 1.4, which defines requirements and specifications for automated driving systems. This task acts as a central design loop, integrating use-case-specific needs from demonstrations, evaluating system-level constraints (e.g., communication bandwidth, safety envelopes, edge compute resources), and aligning implementation choices with standards such as UNECE WP.29, ISO 26262, and ISO 21448.

Partners in SC4 include: AVL, TUG, DRIVEU, VIF, IFAT, XenomatiX, FHG, InSAR, IOTAM, TUD, and TAAT, each contributing domain-specific expertise in simulation, AI reasoning, sensor development, communication systems, and satellite monitoring. Notably, SC4 is closely linked to SC3 and SC5 through shared objectives in powertrain efficiency and emergent swarm behaviour, ensuring cross-supply-chain convergence toward safe, efficient, and cooperative mobility systems.

In line with Cynergy4MIE's societal objectives, SC4 also addresses public trust and acceptability through demonstrable improvements in safety, explainability, and system robustness in real-world conditions.

6.2 Existing Relevant Standards and Regulations

SC4 focuses on road vehicle ADS and cooperative mobility, so the applicable standardisation ecosystem spans automotive safety, AI in autonomous systems, sensor and communication protocols, and cybersecurity. Key standards and regulations include:

- **Automotive Safety (Functional and Intended):** At the core of SC4's regulatory baseline are ISO 26262 (Road Vehicles – Functional Safety) and ISO 21448:2022 (Safety of the Intended Functionality, SOTIF). ISO 26262 governs the design and validation of safety-critical E/E systems in vehicles and is highly relevant to SC4's development of fail-operational architectures (e.g. redundant braking or steering for Level 4 ADS). ISO 21448 addresses performance limitations of nominally correct systems – particularly important for SC4's emphasis on edge perception under adverse conditions or unexpected events (like occlusions or unusual VRU behavior). These two standards form the backbone for validating SC4's safety logic in the scenarios simulated and demonstrated (Demo 4.1's traffic optimisation scenarios, Demo 4.2's road hazard detection).
- **Road Vehicle Automation Regulations:** UNECE WP.29 provides the international regulatory framework for ADS. In particular, UNECE Regulation No. 157 (ALKS – Automated Lane Keeping Systems) is relevant as it is the first regulation allowing Level 3 automation in traffic jams. SC4's highway and traffic jam scenarios relate to R157 compliance (e.g. ensuring the system respects ODD limits, passenger take-over requests, etc.). Additionally, upcoming UNECE regulatory work on higher-level ADS (e.g. draft requirements for highway chauffeur systems) is tracked by SC4. European-specific requirements from Regulation (EU) 2022/1426 (on uniform procedures for ADS testing) are also considered in SC4's validation planning. SC4's contributions aim to **extend these regulations** – for instance, project partner VIF is exploring a proposal

to allow virtual testing evidence in ADS type-approval, which could feed into UNECE discussions on simulation-based validation.

- **AI and Trustworthiness in ADS:** SC4 introduces machine learning for behaviour prediction and decision-making in uncertain situations. To ensure these are trustworthy, SC4 aligns with ISO/IEC TR 24028:2020 (trustworthiness of AI) and pending standards from ISO/IEC JTC1 SC42 (AI in autonomous applications). IEEE 2846-2022 (assumptions for decision-making in AVs) is used as a guide for documenting and justifying any assumptions SC4's ADS makes (e.g. assuming other vehicles will obey traffic rules). IEEE 7001-2021 (transparency of autonomous systems) is directly relevant: SC4's HMI design and logging mechanism incorporate the standard's metrics to provide explainability (for instance, Demo 4.3's critical scenario handling includes an HMI prompt explaining why the vehicle suddenly slowed down). Finally, the EU Artificial Intelligence Act (Regulation (EU) 2024/2060, if adopted) will classify ADS as high-risk AI systems – SC4 pre-empts compliance by implementing human oversight mechanisms, risk assessment processes, and quality management for its AI, effectively mirroring the draft AI Act requirements.
- **Vehicle Communication and V2X Protocols:** SC4's cooperative ADS rely on standardised vehicular communication protocols. ISO 21217 (ITS station architecture) and the ETSI ITS-G5 standards (EN 302 663 for the 5.9 GHz radio, EN 302 637 for Cooperative Awareness Messages) provide the basis for V2V and V2I messages used in Demo 4.1's traffic flow optimisation. SAE J2735 defines the message set dictionary (including Basic Safety Messages) which SC4 uses for interoperability between different OEM vehicles in the demos. Additionally, SC4 looks at cellular V2X (3GPP Release 14 and beyond) for low-latency communication, following the 5GAA guidelines for C-V2X which ensure compatibility between telecom and automotive standards. All V2X implementations in SC4 are tested for compliance with these standards, e.g. checking that message formats and transmission frequencies meet ETSI/SAE specs. This is critical for demonstration credibility and eventual deployment – regulators will accept SC4's results more readily if they utilise standardised V2X messaging.
- **Cybersecurity and Software Updates:** All connected elements of SC4 must comply with vehicle cybersecurity and software update rules, notably UNECE WP.29 Regulations R155 (Cybersecurity) and R156 (Software Updates). R155 requires a certified Cybersecurity Management System (CSMS) and mitigations against threats – SC4's architecture includes threat analysis per ISO/SAE 21434 and implements features like secure boot and encrypted V2X comms to align with R155. R156 mandates a Software Update Management System (SUMS) – while SC4 prototypes may not undergo formal OTA updates, the design principles (like update integrity and

documentation) are observed. By building to these standards, SC4 ensures that its ADS platform would be "cybersecurity-ready" for real-world deployment.

- **Sensor and Perception Standards:** SC4's multi-modal sensor fusion (LiDAR, radar, cameras, TPMS, plus inputs like InSAR) requires adherence to sensor interface and performance standards. For environment durability: IEC 60068 (environmental testing) ensures sensors can handle automotive temperature/vibration extremes. For performance, ISO 13228 (LiDAR test methods) is monitored as a draft, SC4's LiDAR supplier partner feeds into it as noted under SC1. Additionally, SC4 considers diagnostic standards like ISO 13400-2 (DoIP) to ensure that data from novel sensors can integrate with vehicle diagnostics. One noteworthy gap being addressed is simulation: SC4 recognises the need for a standard in **simulation-based ADS validation** (sometimes called "ISO 8800" conceptually in the community, though no such standard exists yet). The project's formal methods and scenario-based tests provide input towards such a future standard, as discussed later.
- **Digital Mapping and Localization:** SC4's reliance on HD maps and satellite data touches standards for digital maps like ISO 18750 (road boundary data) and emerging standards for GNSS augmentation. These are niche but important for aligning how SC4 represents environment data in a standard format if sharing with external parties (for instance, using ADASIS v3 protocol to share electronic horizon data from infrastructure to car in Demo 4.2).

In summary, SC4 engages a comprehensive set of published standards and regulations to cover safety, connectivity, and security. It also keeps a close eye on **frontier areas** (AI transparency, simulation validation) where standards are still catching up, positioning the project to influence those (see Section 6.5).

6.3 Standardisation Usage and Insights from Technical Partners – SC4

Survey responses from SC4 partners indicate heterogeneous engagement with existing ADS standards, reflecting their varying roles (OEMs vs. academics) and tech maturity:

- **Safety Standards Adoption:** All industry partners affirmed ISO 21448 (SOTIF) is extensively referenced, especially for Demo 4.2's road condition sensing. They reported using SOTIF methodologies to identify unknown hazardous scenarios (e.g. misinterpreting a wet shiny road as ice) and to structure their validation plans. ISO 26262 was recognized as fundamental, though academic partners noted it is more applicable at later TRLs – in research they follow its spirit but not full process. This suggests a gap in agile safety standards for R&D, but in SC4's planned path to deployment, ISO 26262 will become increasingly central.
- **V2X and Communication Standards:** Partners working on connectivity cited IEEE 802.11p and SAE J2945/1 as known references for V2X communication. While no

partner is formally certifying to these standards during R&D, they ensure their implementations (e.g. the OBU software stack in Demo 4.1) conform to message sets and performance guidelines from these standards. No major interoperability issues arose in tests, reinforcing the value of these standards. However, partners noted that **standard compliance testing tools** (for V2X stacks) are expensive or limited, which slightly hindered formal verification.

- **Cybersecurity Practices:** ISO/SAE 21434 (cybersecurity) was cited as indirectly relevant and "on the horizon." Partners expect to apply it more rigorously as edge connectivity and OTA features of SC4 mature. Some indicated they are already performing Threat Analysis and Risk Assessment (TARA) per ISO 21434's guidance, even if not required for a prototype, to future-proof designs. This proactive stance ensures SC4's ADS could pass a cyber audit when moving to product stage.
- **Regulatory Awareness:** Industrial partners clearly follow UNECE regulations: one noted that their design must be "R157-ready," meaning it can pass the requirements of ALKS regulation (like transitioning control to the driver with adequate warning). Another partner, involved in scenario simulation, mentioned aligning scenarios with those used in Euro NCAP's testing protocols for ADAS. This shows that even beyond official standards, **semi-formal standardisers like Euro NCAP protocols** influence SC4 development to maximise future acceptance.
- **Gaps Highlighted by Partners:** A recurring theme was the difficulty in validating AI/ML decisions – partners feel **evaluation standards lag behind AI development**. They welcome the initiative of ISO PAS 8800 (ADS validation via simulation) mentioned conceptually, saying Cynergy4MIE should contribute to it. Also, partners pointed out that current traffic models in standards assume human drivers; with ADS, some parameters (reaction time, adherence to rules) change, and no standard yet encapsulates this shift. This feedback directly informs SC4's standardisation strategy to push for new metrics and test methods for ADS.

6.4 Gap Analysis

Identified Gaps: SC4's state-of-the-art review and partner input expose several critical gaps in standards/regulations for automated driving:

- *Simulation and Virtual Validation:* There is **no approved standard or regulation fully accepting simulation for ADS homologation**. While SC4 can test thousands of scenarios in virtual environments, today's rules (like UNECE ALKS) still require physical tests. This gap limits the scalability of ADS validation. A standard framework (ISO or UNECE) for accrediting simulation results is needed. SC4 has identified this as a gap and is aligning with initiatives (such as PEGASUS family standards in Germany) to push simulation validation methodologies.

- *Explainability and HMI:* Current ADS standards focus on safety performance (e.g. RSS safe distances) but do not cover how an ADS should **communicate with the driver or other road users**. For instance, there's no standard on an ADS's external HMI (like lights or displays signalling intent to pedestrians). SC4 found this gap in Demo 4.3: when the ADS stopped for an unseen hazard, how to inform drivers behind? The absence of standards here could lead to inconsistent solutions and user confusion, impacting trust.

- *Complex Urban Scenarios and AI Ethics:* Regulations like UNECE R157 cover highway scenarios (limited ODD). As ADS move to complex urban environments, there is a regulatory gap in defining acceptable behaviour in ethical dilemmas (e.g., unavoidable collisions) or how to ensure fairness (not biasing against certain VRUs). While outside the strict technical homologation, these issues may become part of future standards or best practices (like ISO TR 4804 – Safety and AI in ADS, still evolving). SC4 notes that its urban tests touch on these grey areas (e.g., Demo 4.3's detection of a jaywalker, how conservative vs aggressive to be) where no clear guidance exists.

- *Interoperability of ADS and Infrastructure:* Beyond V2X message formats (which are standardised), there is a gap in how ADS can rely on infrastructure support. For example, if a smart traffic light provides trajectory advice to an ADS, there's no standard for how much the ADS can trust it or integrate it. A sort of **"roadworthiness index"** for infrastructure inputs is missing. SC4's work with road condition servers shows this gap: they had to define internally how the ADS prioritises its own sensor vs. a road weather message from the cloud.

- *Cross-Domain Consistency:* SC4 also recognised a gap in ensuring that standards in automotive are consistent with those in other domains when systems converge (mobility with energy, etc.). For instance, cyber standards for vehicles (ISO 21434) vs. for power grids (IEC 62443) might have overlaps or conflicts once a car is a "grid node". A converged approach is not yet standardised, something the project's RHP is highlighting.

6.5 Strategic Gap: Absence of Specific Contributions to Standardisation Bodies – SC4

SC4 is strategically positioned to contribute to evolving the standards and regulations for automated driving. Its contributions will focus on virtual validation methods, transparency, and cross-domain integration:

Pre-normative contribution (SC4):

- **Committee:** UNECE WP.29 (Working Party on Automated/Autonomous Vehicles, e.g. IWG on VMAD – Validation Methods for ADS)

- **Artefact:** Framework for simulation-based type approval (white paper and sample validation scenarios extending UN R157 for virtual testing)
- **Responsible Partner(s):** VIF (Virtual Vehicle), AVL
- **Target Submission:** M30 (working paper submitted to VMAD/GRVA)

(Rationale: SC4 will formulate a proposal supported by Demo 4.1/4.3 data showing equivalence of certain virtual test scenarios to physical tests. By M30, the aim is to table this at UNECE's GRVA, which is seeking such input. This could lead to an amendment in UN R157 or a new regulation for higher ADS levels that accepts simulation evidence. VIF, as an active member of numerous EU projects on ADS validation, leads this effort, ensuring traceability to Cynergy4MIE results.)

Another major contribution is to **ISO/TC204** (Intelligent Transport Systems) or **SAE On-Road Automation committees** on the topic of cooperative driving scenarios. SC4 will contribute a **scenario library for V2X-assisted ADS** and a set of performance metrics (e.g. traffic flow stability improvements, fuel savings) observed in Demo 4.1. These could inform an ISO TR or SAE guideline on evaluating "collective ADS behavior," a niche not covered in current standards.

SC4 will also engage with **ISO/TR 4804 / BSI PAS 1883** follow-ups on ADS safety and AI. Partners TUG and Fraunhofer will present SC4's approach to explainability (combining formal logic with ML) to those drafting guidelines for safe AI in ADS. The objective is to influence how standards recommend implementing transparent decision-making. For example, SC4's logging schema (recording the rationale for actions) could be proposed as a template for an upcoming ISO PAS on ADS incident reporting.

Finally, SC4 will collaborate with SC6 in standard forums that overlap mobility and infrastructure. One planned action is a joint contribution to the **CEN/CENELEC Focus Group on Infrastructure for Automated Driving**, sharing SC4's findings on infrastructure-assisted ADS (e.g. how a road authority can safely broadcast hazard info to vehicles). This ensures our standardisation push is **holistic**, not siloed by domain.

All these actions will be reported in Deliverable D7.9 (capturing the collaborations established and initial submissions by M24) and fully detailed in D7.10 (with outcomes of submissions and any draft standard text by M30). The contributions align with Grant Agreement obligations for Cynergy4MIE to work with bodies like ISO, SAE, and UNECE on ADS challenges, and will help ensure the project's innovations directly shape the evolving rulebook for automated driving.

7. SC5 – Multi-Agent Sensing and Control

7.1 Description of SC and its Scope in Cynergy4MIE

Supply Chain 5 (SC5), titled “Multi-Agent and Cooperative Sensing & Control in Emergency Response Applications”, explores the use of distributed, autonomous, and collaborative systems to enhance the efficiency, resilience, and intelligence of Search and Rescue (SAR) and broader emergency response operations. SC5 brings together cyber-physical systems (CPS), AI, sensor networks, and edge intelligence to orchestrate emergent system-of-systems behaviours, where autonomous agents cooperate in real-time to execute complex missions under uncertainty.

The core focus of SC5 lies in enabling multi-agent coordination across dynamic and potentially hazardous environments, such as post-earthquake urban areas, forest fires, or collapsed infrastructures, where manual operations would be too slow, dangerous, or costly. These agents (e.g. UAVs, UGVs, mobile robots) are equipped with minimally invasive sensors (e.g., IR cameras, ToF sensors, radar), onboard AI perception modules, and resilient communication links (e.g., V2X, cellular, WiFi, and narrowband redundancy) to operate both autonomously and cooperatively.

Key innovations in SC5 include:

- Emergent collaborative SLAM and mission planning using ML-based algorithms at the edge;
- Vital signs monitoring and situational awareness through cooperative sensor fusion;
- Swarm-based fault tolerance, where agent failure leads to role reassignment or task redistribution;
- Mission-aware reconfiguration, where real-time sensor inputs and health status indicators inform dynamic role changes across agents;
- Integration of satellite Earth Observation data (e.g., Copernicus InSAR) to support wide-area mapping, localisation, and mission prioritisation.

The SC5 demonstrators include:

- Demo 5.1 – Cooperative Agents for Survivor Detection: Autonomous platforms equipped with diverse sensor payloads operate in GNSS-denied areas to detect, locate, and communicate survivor positions.
- Demo 5.2 – Resilient SAR Operations: Multi-agent systems dynamically reconfigure based on agent health and mission conditions, demonstrating emergent adaptability and communication-aware redundancy.

SC5 is technically aligned with several Key Targets (KTs), especially:

- KT3 – AI-based control and decision-making algorithms for agent-level and system-level autonomy;
- KT4 – Emergent intelligence and digital assets enabling collaborative SLAM, fault-tolerant behaviour, and edge-based computation.

The SC5 ecosystem supports horizontal integration with SC3 (smart batteries, distributed learning), SC4 (emergent vehicle behaviours), and SC6 (distributed control for energy systems). Together, these inter-SC linkages create a foundation for adaptive, mission-critical CPS that operate across sectors including mobility, civil protection, and energy.

By developing modular, affordable, and scalable cooperative agent systems, SC5 advances not only emergency response applications, but also provides foundational methods and architectures applicable across smart mobility, decentralised energy coordination, and multi-agent digital twins, in line with the broader vision of Society 5.0.

7.2 Existing Relevant Standards and Regulations

SC5's focus on multi-agent cooperative systems in SAR sits at a crossroads of robotics, communications, AI, and emergency management domains. The standardisation landscape is relatively sparse and fragmented because this is an emerging application. Nevertheless, relevant standards and frameworks from adjacent domains include:

- **Robotics and Autonomous Agent Safety:** In absence of SAR-specific robot standards, SC5 looks to general ones. ISO 13482:2014 (safety of personal care robots) is sometimes analogously applied to mobile service robots near humans. ISO 10218-1/2 and ISO/TS 15066 (for industrial and collaborative robots) provide principles for safe proximity operation, which SC5 uses as reference when configuring, for example, safe distances or forces for UGVs operating around rescue personnel. IEC 61508 and ISO 13849-1 (functional safety) give generic guidance to ensure electronic control systems on the robots meet safety integrity expectations, particularly critical in a mission where failures could risk human life. **However, there is no SAR-specific safety standard** – aspects like operating in unstable rubble or interacting directly with victims are not covered by current robot norms. This is recognized as a gap.
- **Emergency Response and Management:** ISO 22320:2018 (Emergency management - incident response requirements) and related standards (ISO 22300 series) set high-level requirements for managing incidents (information flow, roles, etc.). They don't directly address autonomous systems, but SC5 ensures its system can slot into these frameworks (for instance, by structuring multi-agent outputs – maps of cleared areas, victim locations – in formats that incident commanders can use as per ISO 22320's info management guidelines). Moreover, INSARAG guidelines (International Search and Rescue Advisory Group) are considered from a procedural standpoint; again, these aren't technical standards but SC5's system design (like the user interface that presents findings) is informed by how human SAR teams operate per those guidelines.

- **AI and CPS Trustworthiness:** SC5's deployment of ML at the edge and emergent control demands trustworthy AI considerations. ISO/IEC TR 24028 (AI trustworthiness) and ISO/IEC 42001:2023 (AI Management System) provide a governance lens, SC5 uses them to ensure that its AI models for target detection are robust and bias-controlled (critical since these models might decide who or what to prioritise in rescue). IEEE 7001-2021 (transparency) is relevant here too: SC5's system logs decisions and provides explainability (e.g. why a drone changed its search pattern) for post-mission analysis. SOTIF (ISO 21448) is also applied conceptually to SC5's AI treating weird corner cases in perception (like confusing a heat source that's not a human) as an "intended function limitation" hazard that needs mitigation.
- **Communication and Interoperability:** SC5's multi-agent network relies on robust comms. Standards from vehicular and ad-hoc networking come into play. IEEE 802.11p / ETSI ITS-G5 and 3GPP Release 14 C-V2X, while designed for cars, serve as baseline references for ad-hoc wireless reliability. They guide how SC5 evaluates link performance under degraded conditions (e.g. using 5.9 GHz DSRC range as a benchmark for drone-to-drone comm in open areas). Additionally, SC5 considers **OPC UA (IEC 62541)**, a standard for machine-to-machine interoperability widely used in industry. While SAR robots traditionally wouldn't use OPC UA, SC5 explores it for cross-platform communication (e.g. a ground robot using OPC UA to query a static sensor node's readings). Using such a standardised protocol could later ease integration of SC5 tech with existing command-and-control systems.
- **Ethical and Legal Compliance:** In handling potentially personal data (like victims' images or voices), SC5 complies with GDPR (Regulation (EU) 2016/679). No SAR-specific exemption exists, so SC5 ensures any collected personal data (e.g. recordings of victims) are protected and only used for the mission. As a high-risk AI application possibly affecting lives, SC5 anticipates falling under the EU AI Act obligations (once in force). The system is being developed with *human-in-the-loop override* capability and thorough risk assessments in line with what the AI Act will require. Also, SC5 considers ethical guidelines like the UN Guiding Principles on Business and Human Rights insofar as ensuring the technology does not infringe rights or cause undue harm – for example, by avoiding biased victim detection that might overlook certain groups (embedding diversity in training data).

Overall, SC5 finds itself borrowing standards from related fields but confirms that **formal standards for multi-agent SAR robotics are virtually non-existent**. It underscores the need for pre-normative work to inform future standards in this domain.

7.3 Standardisation Usage and Insights from Technical Partners – SC5

Insights from SC5 partners (which include robotics SMEs, AI developers, and first-responder organisations) show a pragmatic approach to standards:

- **Safety and Ruggedisation:** Partners building the robots follow IEC and MIL-STD specs for ruggedness (e.g. MIL-STD-810 for environmental durability), since no civilian standard fully ensures a robot survives harsh SAR conditions. They indicated using these military standards by necessity, suggesting a gap that civilian standards bodies might need to fill for emergency robotics gear.

- **Adapting Existing Standards:** One partner mentioned they apply ISO 13482 (personal care robot safety) to their survivor-assist drone (originally designed for delivering a bottle of water or first-aid kit to a victim). They noted it's not a perfect fit but provides a starting point for ensuring the drone's propellers and movements are safe around an incapacitated person. This improvisation shows that existing standards are repurposed in absence of targeted ones.

- **Communications Protocols in Practice:** SC5 teams often default to well-known protocols like MAVLink for drone communications or ROS 2 for interoperability. These are de-facto standards (open source) but not formal ones. Partners did not express immediate concern about this, as interoperability among their systems is achieved through ROS 2. However, they acknowledged that to integrate with external agencies, more formal standard interfaces would help (e.g. publishing their drone telemetry in a standardized format that an Incident Command System can ingest).

- **Ethical Considerations:** Partners from the humanitarian side emphasized transparency – they welcome SC5's logging and post-mission explainability features. There was no mention of using specific ethics standards, likely because such standards are new or unknown to them. Instead, they rely on organisational codes of conduct. This implies an opportunity for SC5 to introduce them to IEEE 7000-series standards or forthcoming CEN guidelines on AI ethics in disaster response.

- **Identified Gaps by Partners:** A strong sentiment was that *"there's no playbook for multi-robot SAR."* Partners find it challenging that every new deployment is bespoke. They highlighted as gaps the lack of: standardized training for operators of multi-agent systems, certification for such systems to be trusted by rescue authorities, and common performance benchmarks (how to judge if one multi-drone system is better than another in SAR). This feedback indicates a broader standardisation gap beyond technical specs – encompassing operational qualification and performance metrics.

7.4 Gap Analysis

Identified Gaps: SC5's analysis emphasises how under-standardised this domain is. Key gaps include:

- *Lack of SAR-Specific Robot Standards:* There are no standards dictating how autonomous systems should function in SAR operations. For example, how to test a drone's victim detection algorithm for reliability? Or what safety measures are mandatory when robots physically interact with victims (e.g. medical payload delivery)? This gap means potential deployment is slowed by the need to convince authorities case-by-case. A formal guideline or standard could greatly aid trust and integration of such systems into official response.

- *Interoperability and Communication Gaps:* While SC5 uses existing comm standards, there is a gap in ensuring interoperability with public safety communication systems. Emergency services often use standards like TETRA for voice/data. Integrating multi-agent system data into those networks lacks a standard approach. Bridging this gap might involve adapting standards like CAP (Common Alerting Protocol) to carry robot-generated alerts, but this is not done yet.

- *AI Validation in Unstructured Environments:* Similar to SC4's AI gap but perhaps more acute in SC5: no standards cover validating AI perception in chaotic, unstructured environments full of noise and anomalies (rubble, smoke, etc.). SC5 must develop its own validation protocols (like injecting environmental noise in simulation, using domain randomisation for training) without a guiding standard.

- *Ethical and Legal Uncertainty:* SC5's technology raises questions like "Who is liable if a rescue robot accidentally harms a survivor or responder?" – currently unanswered in standards or law. Also, privacy in emergency scenarios is a grey zone (GDPR compliance vs. lifesaving necessity). These represent gaps at the ethics-policy interface rather than pure technical standards but eventually will need addressing (potentially via guidelines from ISO TC/CP on public safety).

- *Standard Metrics for Success:* There's no standard metric to quantify the performance of a multi-agent SAR mission (for instance, success rate of finding victims, area coverage efficiency, etc.). Every project uses its own metrics. A standard set would help compare systems and push the field forward. SC5 identifies this as a gap where it could contribute by proposing metrics derived from its demos (e.g. time per area searched, probability of detection, network resilience index).

7.5 Strategic Gap: Absence of Specific Contributions to Standardisation Bodies

SC5 will take steps to pave the way for future standards in multi-agent emergency systems by sharing its empirical findings and frameworks with the relevant standardisation and industry bodies:

Pre-normative contribution (SC5):

- **Committee:** IEEE Robotics & Automation Society - Technical Committee on Multi-Robot Systems (and related IEEE standard initiatives)

- **Artefact:** Open dataset of multi-agent SAR scenarios and performance metrics, plus a guideline document on safety and communication best practices for robot swarms in emergencies

- **Responsible Partner(s):** Fraunhofer (FHG), EDI (Latvia)
- **Target Submission:** M30 (dataset release and white paper presented at IEEE RAS forum)

(Rationale: By M30, SC5 will compile data from Demo 5.1 and 5.2 – including maps, logs of agent actions, outcomes – into a public dataset. Alongside, a guideline highlighting key safety considerations (e.g. geofencing altitude limits, fail-safe behaviours) and interoperability tips will be prepared. The aim is to seed efforts within IEEE or ISO to create an official standard or report. IEEE RAS's Technical Committee on Multi-Robot Systems is a logical avenue, as it fosters community best practices. This could evolve into an IEEE Draft Standard if momentum builds.)

Additionally, SC5 will reach out to **ISO/TC204 (Intelligent Transport Systems)** subgroups working on emergency communications and **ISO/TC292 (Security and resilience)** to discuss incorporating robotic agents into emergency management standards. The idea is to ensure upcoming revisions of ISO 22320 (or a new ISO 223XX) consider data feeds from autonomous agents as part of incident management. SC5 partners, through national standard bodies, will propose a new work item or at least contribute to workshops on this topic by M30.

On the interoperability front, SC5 plans to engage with the **OASIS organisation** (which maintains CAP, the Common Alerting Protocol). By providing example CAP messages that include payload from SC5's multi-agent system (like a CAP alert with geo-coordinates of detected survivors from a drone), SC5 can advocate for any extensions needed to CAP or usage guidelines for robotics-generated alerts in disasters.

Lastly, SC5 will maintain close links with first-responder associations (like IRO, International Rescue Organisation) to push for a **"Robotics in SAR" handbook** that could preface formal standards. While not a standards body, such a handbook (endorsed by practitioners) often informs later standardisation.

These contributions will ensure SC5's innovative work does not remain a one-off, but actively shapes the knowledge base and groundwork for standardising multi-agent emergency response technology. Deliverable D7.9 will list the liaisons established (IEEE RAS, ISO TC292, etc.) and initial outputs, and Deliverable D7.10 will report the final contributions (with links to published datasets or submitted proposals). This aligns with the project's mission under T7.4 to drive convergence and **pre-normative outputs** that future-proof the path to certification and acceptance of novel CPS solutions.

8. SC6 – ECS for Energy Efficiency and Distributed Intelligent Control

8.1 Description of SC and its Scope in Cynergy4MIE

Supply Chain 6 (SC6), titled “Electronic Components and Systems (ECS) for Energy Efficiency and Distributed Intelligent Control”, addresses one of Europe’s most urgent challenges: enabling the energy transition through advanced digitalisation, decentralised control, and wide-bandgap (WBG) power technologies. SC6 aims to improve the efficiency, intelligence, and resilience of energy systems, with a specific focus on applications in hydrogen production, modular heat-pump control, and smart energy infrastructures for buildings and shelters.

At its core, SC6 develops foundational ECS-based innovations to increase energy efficiency across production, conversion, and consumption phases. It leverages SiC and GaN WBG semiconductors, decentralised digital control, and emergent multi-agent coordination to address growing energy demands from climate adaptation, electrification, and sustainable mobility trends.

Key innovations in SC6 include:

- Demo 6.1: A modular wide-bandgap-based converter system for hydrogen production, integrating SiC/GaN power devices, decentralised measurements, and advanced digital control. The goal is to increase conversion efficiency to over 97%, reduce DC ripple, and improve grid stability and power quality.
- Demo 6.2: An emergent control framework for managing large-scale heat pump installations and energy usage in distributed buildings and emergency shelters. This system employs multi-objective optimisation algorithms to balance thermal comfort, energy efficiency, and demand prediction, responding dynamically to local zone requirements.

SC6’s architecture is inherently modular and scalable, enabling adaptation to both urban infrastructures and mobile, rapidly deployable energy systems. This positions it as a critical enabler of resilient energy systems in crisis response, energy poverty reduction, and climate-neutral housing strategies.

SC6 also supports fundamental research on GaN reliability, including lifetime modelling, degradation mechanisms, and mitigation strategies, with input from partners such as TU/e and Prodrive. These investigations are essential for de-risking WBG adoption and accelerating time-to-market for high-performance, low-footprint converters.

The supply chain is closely linked with:

- SC3, through shared development of power electronic components and battery introspection techniques;

- SC5, through cooperative decentralised control frameworks;
- And the broader Cynergy4MIE ecosystem, through integration with the ECS stack and AI-empowered CPS frameworks.

In alignment with the Green Deal and Society 5.0, SC6 ensures that energy systems are not only efficient, but also flexible, trusted, and locally controllable, a prerequisite for energy sovereignty, sustainability, and system-of-systems convergence.

8.2 Existing Relevant Standards and Regulations

SC6 operates in the realm of electrical safety, grid interconnection, and emerging IoT-based control. Relevant standards and regulations include:

- **Grid Connection and Safety:** Any power electronics connecting to the grid must meet grid codes and safety standards. For example, **IEC 60364** and national wiring regulations ensure electrical safety for installations (SC6 adheres to these for its demonstrators' setup). For grid interconnection, standards like **IEEE 1547** (for distributed energy resources (DER) interconnection) and ENTSO-E grid codes define requirements (voltage/frequency support, anti-islanding, etc.). SC6's converter in Demo 6.1 follows these in its control logic – e.g. providing certain reactive power on grid command as per IEEE 1547.
- **Power Converter Standards:** SC6's WBG converters also follow product-specific standards such as IEC 62477-1 (safety requirements for power electronic converter systems) to ensure design and testing cover insulation coordination, protection against overcurrent, etc. The demonstration aiming at hydrogen production also considers ATEX directives (since hydrogen is explosive) for any installation in hazardous zones – not a direct standard but regulatory compliance requiring adherence to explosion-proof equipment standards if needed.
- **Energy Efficiency Standards:** There are standards defining how to measure energy efficiency of appliances (like the heat pumps in Demo 6.2). **EN 14511** series (Air conditioners, chillers, heat pumps testing and rating) is particularly relevant. SC6 uses EN 14511 to gauge the performance improvements its intelligent control brings to heat pumps. In fact, SC6 partners are involved in harmonising test standards, e.g. aligning Taiwan's CNS 15466 for heat pumps with EN 14511, showing SC6's direct input in this area. Additionally, **IEC 60335-2-40:2022** (safety of heat pumps, ACs and dehumidifiers) is adhered to for any modifications or operations involving heat pumps. SC6's contributions may even extend this standard's scope (as noted, there's interest to enlarge it to bigger heat pump systems, which SC6's industrial use-case can support).
- **Vehicle-to-Grid and Charging Standards:** SC6 covers V2G integration as vehicles become energy resources. The primary standard here is ISO 15118 series (vehicle-to-grid communication interface), which defines how EVs and charging stations exchange

data for smart charging and discharging. SC6 ensures that any EV-grid interaction in its scenario (for example, using an EV battery to buffer renewable energy) conforms to ISO 15118 protocols for seamless interoperability. On the infrastructure side, **IEC 61851** (EV charging system general requirements) and **UNECE R10** (EMC for vehicle components) are relevant to ensure the V2G hardware doesn't introduce interference or instability.

- **Cybersecurity for Energy ICS:** The distributed intelligent control in SC6 creates an IoT of energy devices, raising cybersecurity concerns. While automotive has ISO 21434, the energy domain references standards like **IEC 62443** (security for industrial automation and control systems) and the upcoming **EU Cyber Resilience Act** which will impose security requirements on connected devices (including potentially smart chargers, converters, etc.). SC6 applies principles from IEC 62443 to its architecture (such as network segmentation between critical control loops and external networks, and authenticated communications between agents). It's also aligning with requirements of the **EU Network Code on Cybersecurity** for the energy sector (a regulatory piece complementing standards). Essentially, SC6's systems are developed with security-by-design, expecting that by the time of deployment, compliance with cybersecurity standards will be mandatory for grid-connected devices.
- **Distributed Control and Interoperability:** SC6's multi-agent control might use standards like **IEEE 2030.5** (Smart Energy Profile) or **OpenADR** for demand response signals, to ensure its system can interface with utilities. For instance, if Demo 6.2's heat pumps respond to grid frequency or price, using OpenADR signals would adhere to a known standard so that any utility could replicate the scheme. SC6 takes such standards into account in designing control interfaces (though full implementation might be beyond the demo scope). Interoperability frameworks for IoT, such as **oneM2M** or **W3C Web of Things**, are also considered to future-proof SC6's control agents communications.

In summary, SC6 straddles automotive, industrial, and energy standards. It complies with core grid and safety standards and contributes to evolving ones like heat pump performance harmonisation. But it also identifies where standards are lacking (e.g. integrated EV-grid reliability, multi-agent energy control protocols).

8.3 Standardisation Usage and Insights from Technical Partners – SC6

Partner feedback in SC6 indicates a forward-looking stance toward standards:

- **Harmonisation Efforts:** As noted, partner ITRI (from Taiwan) actively works on aligning their national standard (CNS 15466) for heat pumps with international standards. Through Cynergy4MIE, they share data to help converge testing methods. This shows SC6 isn't just consuming standards but shaping them, focusing on eliminating trade barriers and ensuring EU and Asian standards interoperate (which is strategic for companies like Infineon or NXP to have global markets).

- **Use of Communication Standards:** Partners implementing the smart charging aspects confirm using ISO 15118 in testbeds. One partner reported their charger prototype achieved basic interoperability with a commercial EV using ISO 15118-2 for plug-and-charge, which validates the importance of sticking to standards even in R&D, as it saved them time integrating with an OEM vehicle.

- **Challenges with Grid Standards:** Some partners found that grid codes (which are often technical rules from grid operators) can be region-specific and not always aligned. For example, a converter tested to meet Germany's grid code had to be slightly tweaked for UK grid code. This friction indicates a possible need for wider standard harmonisation. Partners expressed that referencing IEEE 1547 and IEC standards helps, but regulatory interpretation still varies.

- **Standards Gaps Noted:** A gap noted was in **energy flexibility interfaces** – how a building energy controller talks to a car or to the grid. There are many protocols (OpenADR, OCPP, etc.) but no single standard covers all. Partners in SC6 are testing a combination: e.g., using OCPP for EV charger management and OpenADR for HVAC control. This patchwork approach works but is complex. They suggest a more unified approach (maybe evolving ISO 15118 to also cover building loads?) could be beneficial, highlighting an area to influence.

- **Adopting AI Act Readiness:** SC6's AI components (like predictive algorithms for energy optimisation) are being documented for transparency. Partners are mindful that the AI Act will impose risk management, so they are preemptively applying ISO 31000 risk management principles and logging model decisions. This isn't mandated now, but shows partners expecting those standards/regulations to catch up and wanting to be ready.

The overall insight is SC6 partners are globally oriented, aiming to comply with and unify international standards – especially important in energy where systems cross borders. They also see regulatory waves (AI Act, Cybersecurity Act) coming and use existing standards to prepare.

8.4 Gap Analysis

Identified Gaps: SC6 highlights certain standardisation and regulatory gaps:

- *Vehicle-Grid Integration Standards:* Despite ISO 15118, a comprehensive standard for using EVs as grid storage (bi-directional V2G with all the safety and contractual aspects) is still lacking. For instance, how to standardise the certification of an EV as a grid resource? Or ensure plugging an EV into any compliant home energy system yields predictable results beyond basic charging? This gap could slow V2G adoption. SC6's demos suggest needed requirements (like standardised limits for battery discharge in grid support to protect vehicle warranty).

- *Standards for Cross-Domain Reliability:* SC6 deals with reliability at the intersection of automotive and grid. E.g., wide-bandgap converters in vehicles and those in stationary grid might have different standards now (AEC-Q vs. IEC). A more unified reliability standard or cross-reference is missing, causing duplication. Cynergy4MIE's work on WBG (SC3/6) flags that a GaN device going into a car or a solar inverter should ideally qualify under a single, agreed method.

- *AI in Energy Management:* As with other SCs, applying AI in energy control (like forecasting loads, optimising usage) lacks standard guidelines. There's a gap in e.g. how to verify an AI that controls a building's power will not jeopardise grid stability or safety (similar to SC4's AI gap, but in energy context). The forthcoming EU AI Act will address high-risk AI in energy (if classified so), but technical standards to support compliance (like for bias, robustness of such AI) are not ready.

- *Distributed Control Interoperability:* SC6's multi-agent control might use custom algorithms that work internally. However, if one wanted a generic multi-agent system where devices from different vendors cooperate, there's no standard for that communication or decision logic (beyond basic protocol standards). It's a conceptual gap – essentially needing standard "languages" or ontologies for energy agents negotiating, akin to what IEEE or IEC might start working on in IoT.

- *Policy-Technology Disconnect:* Another gap is between rapid tech advances in energy (like integrating EVs, renewables) and slower-moving grid regulations. For example, in some jurisdictions, feeding energy from an EV to home is technically possible and safe, but regulations forbid it because standards/codes haven't caught up. This policy lag is not a standard gap per se, but indicates areas where demonstrating safety through standards could push regulators to allow new tech. SC6 identifies such obstacles (like restrictions on inverter types or metering requirements) that it can help address by contributing to guidelines showing how these can be resolved.

8.5 Strategic Gap: Absence of Specific Contributions to Standardisation Bodies

SC6 will leverage its unique position bridging automotive and energy to contribute to standards that currently have gaps, especially in harmonisation and interoperability:

Pre-normative contribution (SC6):

- **Committee:** CEN/CENELEC TC 113 (Heat Pumps and Air Conditioning Units) and IEC TC 59 (Performance of household and similar appliances)

- **Artefact:** Harmonised performance test procedures for high-capacity heat pumps, integrating smart control effects (technical report/data to support aligning EN 14511 with international use)
- **Responsible Partner(s):** ITRI, TU Graz (KFU)
- **Target Submission:** M24 (input to ongoing standard revision work)

(Rationale: By M24, SC6 will produce data showing how smart control (like variable speed via WBG drives) affects heat pump performance across loads, and how current standards measure it. ITRI and KFU will submit these findings to CEN/TC113 working on EN 14511 revisions, and to IEC if relevant, to ensure test standards accommodate advanced control and larger systems beyond residential scale. This supports global harmonisation, aiding EU-Asia trade and standard convergence.)

Another significant SC6 contribution is toward **IEC TC 69** or **ISO/IEC JPC "Vehicle-Grid Integration"** (if one exists or gets created). SC6 partners (Infineon, NXP) plan to push for clearer standards on V2G interfaces, possibly by contributing to the next edition of ISO 15118 (which may cover energy management messages). They will propose requirements gleaned from Demo 6.1's grid support scenario – e.g., specifying how an EV signals its available capacity for grid services in a standard way, or how converters should modulate to avoid harmonics on the grid.

SC6 will also liaise with the **CharIN e.V. alliance** – a large industry forum on charging – to present its results on EV charging and discharging strategies. The goal is to incorporate these results into CharIN's position papers, which often influence future IEC/ISO standards for charging. For example, evidence from SC6 on efficient control algorithms might inform CharIN's recommendations for ISO 15118-20 implementations or for extended usage of EVs in grid support.

On cybersecurity, SC6's demonstration of a multi-node energy control will yield best practices that can be offered to **CENELEC TC 65X/WG** (or equivalent) focusing on IoT security in energy. The project might draft a short guideline on securing V2G communications or distributed energy controllers and share it via the European Energy ISAC or standard bodies.

By D7.9, SC6 will have engaged in these committees and documented initial contributions (like ITRI's standard update input, CharIN discussions). By D7.10, we expect concrete outcomes such as data accepted into a standard's annex or a proposal for a new work item (for example, a **"V2G energy management" standard or annex to ISO 15118**). These actions are aligned with T7.4's mandate and ensure Cynergy4MIE's energy-centric innovations can be widely adopted with the support of robust standards backing them.

9. Cross-SC Synthesis: Safety, Security, Quality and Reliability (SSQR)

This section consolidates the current standardisation landscape relevant to the project's Supply Chains (SCs) and analyses gaps in interoperability and convergence. It is structured into four parts: a analysis mapping standards to SC domains (Section 9.1), an assessment of how existing standards address safety, security, quality, and reliability (SSQR) aspects (Section 9.2), an identification of interoperability and convergence gaps including emerging standards to fill them (Section 9.3), and an examination of synergies with the Reference Homologation Process (RHP) and project work-package interdependencies (Section 9.4).

9.1 Consolidated "Standards x SC" Analysis

This section provides a horizontal analysis across SC1–SC6, identifying common themes and synergies in standardisation. It has been updated to reflect the tailored contributions above and removes any redundant statements.

SC1 – All-Weather Autonomous Machinery

Functional-safety assurance relies chiefly on IEC 61508 in combination with ISO 26262; the latter, although road-vehicle-oriented, is now widely adapted for off-road mobile equipment (Visure Solutions, 2023). Domain-specific hazards are further mitigated by ISO 17757:2019 on autonomous earth-moving machines (VTT Technical Research Centre of Finland, 2019). What is still missing are interface and cybersecurity specifications that would allow sensors from different vendors to "plug and play'' safely, an interoperability gap the current standards set does not yet cover.

SC2 – Construction Robotics / Human-Robot Collaboration

ISO 10218-1/-2 and ISO 15066 give comprehensive rules for collaborative and industrial robots, including collision-force limits and risk-assessment workflows; thus safety is "well-covered''. Conversely, long-term software quality and maintainability are under-specified: automotive-style frameworks such as Automotive SPICE for Autonomous Driving are only beginning to migrate into the construction-robotics domain, leaving Quality and Reliability less mature.

SC3 – Power-train Sensors & Components

Hardware-reliability standards (e.g., AEC-Q100 qualification, ISO 6469 for EV safety) assure electrical integrity, temperature cycling, vibration endurance and so on, covering the Reliability "R'' pillar. They do not, however, prescribe how component-level evidence is rolled up into a complete system safety case; thus Safety and integrated Quality remain only partially addressed.

SC4 – Automated Driving Systems

This is the most densely standardised area:

- **Safety.** ISO 26262 governs random hardware/software faults, while ISO 21448 (SOTIF) tackles hazards from performance limitations; the latter still lacks full Level-4/5 scope (Users.ece.cmu.edu, 2022).
- **Cybersecurity.** ISO/SAE 21434, together with UNECE regulations UN R155/R156, forms a mandatory risk-management baseline.
- **Regulatory alignment.** The EU ADS Regulation 2022/1426 imports the Operational Design Domain (ODD) taxonomy defined in ISO 34503:2023 (Connected Automated Driving, 2023).

Open points remain around life-cycle AI assurance and residual-risk arguments for high automation.

SC5 – Multi-Agent Search-and-Rescue Systems

SC5 must blend rules from road vehicles, ground robots and unmanned aerial systems. While V2X protocols (ETSI ITS-G5 in Europe; IEEE 1609.x in the U.S.) and UAV safety documents exist, there is no unified framework for the coordinated behaviour of heterogeneous agents. Consequently, most interoperability and joint-safety provisions remain either "partial'' or "missing'' for this domain.

SC6 – Trustworthy Software & AI

Software-product quality is addressed by ISO 25000, and AI robustness by the new ISO/IEC 24029-2:2023 formal-methods guideline (ISO/IEC, 2023). Yet these documents are not (yet) a required part of automotive certification, so the bridge between AI validation and classical functional safety is still under construction, leaving an integration-gap.

Overall Assessment

Core functional-safety standards are mature (especially for SC4) and component reliability is well governed (SC3). The weakest links are:

- **Interoperability:** standardized sensor/ECU interfaces are emerging (ISO 23150), but coverage is still partial.
- **AI assurance:** formal validation of machine-learning components is not yet baked into safety certification.
- **Global convergence:** UL 4600 (U.S.) and ISO-centric frameworks (EU/Asia) have not fully harmonised.

New drafts, ISO 3450x (scenario-based testing), ISO 23150-x (sensor data interfaces) and ISO/IEC 24029 (AI robustness), explicitly target these gaps, and Cynergy4MIE partners participate in the relevant ISO, SAE, ASAM and ETSI working groups to accelerate closure.

The analysis reveals four intertwined issues that warrant immediate, coordinated action. First, coverage gaps run across every supply chain: standards such as ISO 21448 on Safety of the Intended Functionality and the emerging AI-governance families are referenced in all six chains, yet partners typically treat them as guidance rather than as requirements. Establishing a shared validation toolbox, covering simulation scenarios, open data sets and harmonised performance metrics, would prevent each chain from launching its own ad-hoc gap-filling exercise.

Secondly, human–robot-collaboration safety norms overflow from the factory floor into field operations. Situational-awareness robots (SC5) and forestry machines (SC1) confront proximity risks akin to those addressed by ISO 10218 and ISO/TS 15066 for collaborative robots in SC2, but the standards are currently applied only by analogy. Drafting an "out-of-factory" annex, or formally liaising with ISO TC 299, could yield harmonised distance limits and test procedures that span all three chains.

Thirdly, communication stacks are diverging. Automated-driving demonstrators in SC4 rely on the mature automotive V2X protocol suite, whereas SC5 adapts the same stack for degraded-radio environments and SC1 is gravitating towards 5GAA profiles. Defining a project-wide communication profile, covering message sets and quality-of-service tiers, would align implementations and simplify eventual certification.

Finally, component-level reliability efforts are fragmented. SC3 and SC6 depend on IEC TC 47 working groups for wide-band-gap devices, while SC4 and SC5 focus on sensor robustness under IEC 60068 environmental testing. By coordinating test-plan development through WP7 and feeding results back into the relevant IEC working groups, the project can transform parallel work streams into pre-standardisation drafts of broader industrial value.

9.2 SSQR in Existing Standards

This section reviews how current standards address the quartet of Safety, Security, Quality, and Reliability (SSQR) considerations in automated systems. We integrate input from consortium surveys and open-source evidence to ensure each claim about adoption or divergence is substantiated. Below, we summarize the state-of-the-art for each aspect:

Safety. Functional-safety practice in road vehicles is anchored on ISO 26262, which mandates systematic hazard analysis and V-model development; virtually all global OEMs and Tier-1 suppliers cite it in their internal standards libraries (International Organization for Standardisation [ISO], 2022). A known limitation is its assumption of a human fallback, which becomes invalid at SAE L4/L5. Two complementary standards therefore fill the gap:

- **ISO 21448 (SOTIF)** – tackles "safety of the intended functionality," i.e., performance-limit hazards that arise even when no component has failed (ISO, 2022). SOTIF principles are already reflected in Europe's UNECE Regulation 157 on Automated Lane-Keeping Systems, which asks manufacturers to address unknown unsafe scenarios in the safety case (United Nations Economic Commission for Europe [UNECE], 2021).

- **UL 4600** – purpose-built for fully autonomous products; it introduces a structured, evidence-based safety-case framework and is gaining traction in North-American L4 pilot programs (Underwriters Laboratories [UL], 2020).

In practice, companies now blend ISO 26262 (to prevent systematic/hardware faults) with SOTIF (to mitigate functional insufficiencies) and, for driverless operation, UL 4600 or equivalent safety-case guidance.

Security. Cybersecurity is now treated as a prerequisite for safety. The sector consolidated around ISO/SAE 21434, while UNECE introduced **UN R155 (cybersecurity management)** and **UN R156 (software-update management)**—making cyber-certification mandatory for new vehicle types (UNECE, 2021). Other domains borrow from ISA/IEC 62443 for industrial control-system security, but dedicated guidance for mobile robots and drones is still emerging.

Quality. Process-quality baselines such as ISO 9001 and IATF 16949 remain compulsory, ensuring traceability and continuous improvement (ISO, 2022). Automotive SPICE v4.0 drafts add machine-learning and data-management processes; nevertheless, survey respondents note that existing frameworks still underspecify data quality, bias avoidance, and explainability, quality attributes crucial for trust (UNECE, 2021).

Reliability. Hardware reliability is quantified through AEC-Q100/101 and environmental tests in ISO 16750, forming a mature foundation for component robustness (ISO, 2022). System-level reliability over a vast scenario space is addressed only indirectly: **ISO 34502:2022** creates a scenario-based evaluation framework, and upcoming IEEE P2851 seeks quantitative metrics for AI-driven behaviour. Stakeholder feedback confirms that while aerospace enjoys stringent lifetime-reliability certification, an equivalent scheme for road-vehicle autonomy is still missing.

Synthesis. *Safety* and *Security* exhibit the highest maturity and regulatory convergence, whereas *Quality* and especially holistic *Reliability* rely on a patchwork of process models and emerging AI-focused drafts. Consortium-survey feedback mirrors this gap: most partners agree that standards “adequately cover functional safety” yet “insufficiently address data quality, bias, and long-term public trust,” underscoring the need to embed AI-assurance artifacts into future revisions.

9.3 Interoperability and Convergence Gaps

Fragmentation of safety standards for higher autonomy. There is still no single, harmonised L4/L5 safety standard; instead, developers combine ISO 26262, ISO 21448 (SOTIF) and UL 4600, which differ in philosophy and issuing bodies (Visure Solutions, 2023). Regulators have acknowledged this divergence; for example, the U.S. NHTSA has asked how such process-oriented standards might fit into a unified ADS safety framework (National Highway Traffic

Safety Administration [NHTSA], 2020). Joint ISO/SAE task groups are now working toward convergence, but until a comprehensive global standard exists, projects like Cynergy4MIE must trace requirements across multiple documents.

Lack of standard methods for AI/ML validation. Traditional functional-safety texts offer little guidance on testing learning-based components. ISO/IEC 24029-2 (2023) proposes robustness-assessment methods for neural networks, and ISO/IEC TR 5469 (in draft) will extend this to system-level AI safety, yet industry surveys rate the absence of clear ML validation criteria as one of the most severe gaps. Guidelines for transparency (IEEE 7001-2021) and trustworthiness (ISO TS 4213-2022) exist, but they are not yet embedded in automotive certification schemes. The forthcoming EU AI Act is expected to accelerate the standardisation of AI risk management frameworks.

Interoperability gaps in system architecture and interfaces. Sensor and ECU suppliers still rely on proprietary formats; ISO 23150-1:2021/AMD 1:2023 defines a logical interface between sensors and a data-fusion ECU and is an important first step, but coverage remains partial (ISO, 2023a). For connected multi-agent systems, vehicle-to-everything (V2X) protocols such as ETSI ITS-G5 (EU) and IEEE 1609.x (US) coexist without full alignment, an issue when drones, ground robots and cars must cooperate in a disaster-response scenario. Horizon-Europe projects, including Cynergy4MIE, are now contributing use-case data to ASAM and ETSI working groups to support interface convergence.

Convergence of jurisdictional standards and regulations. Regional differences persist, e.g., UL 4600 (North America) versus ISO-centric approaches (Europe/Asia). Nevertheless, regulators are beginning to reference common concepts: the EU ADS Regulation 2022/1426 adopts the Operational Design Domain (ODD) taxonomy defined in ISO 34503:2023 (Connected Automated Driving, 2023). Such uptake demonstrates incremental convergence, but global harmonisation is still incomplete.

Ethical, societal and homologation-process gaps. New ethics-oriented standards (ISO 39003:2023; IEEE 7000-series) are largely voluntary, and partners in our survey disagree that "current standards sufficiently consider inclusivity, accessibility and public trust." Likewise, no single document prescribes an end-to-end safety case for homologation; the Reference Homologation Process (RHP) proposed by ArchitectECA2030 fills this conceptual void by integrating functional safety, cybersecurity and validation evidence into one framework (ArchitectECA2030, 2022).

Summary. The SSQR foundation is solid, but cross-cutting integration remains the weakest link. Drafts such as ISO 3450x (scenario-based testing), ISO 23150-x (sensor interfaces) and ISO/IEC 24029 (AI robustness) are directly targeting these gaps; Cynergy4MIE's liaison activities will help accelerate their maturation.

9.4 Synergies with the Reference Homologation Process

To ensure that all Safety, Security, Quality, and Reliability considerations are properly integrated across domains, Cynergy4MIE leverages a **Reference Homologation Process (RHP)** as a unifying framework. The RHP is a high-level, abstract description of the entire lifecycle for certifying complex CPS, covering every phase from initial concept and requirements through design, implementation, integration, verification & validation, and on to final certification, production, deployment, and decommissioning. By adopting this reference process (developed in prior EU R&D projects like ArchitectECA2030), Cynergy4MIE creates a common homologation roadmap that maps each cross-domain innovation (SC1–SC6) onto what regulators expect for approval. This ensures that whether a result emerges from mobility (SC4) or energy (SC6), it is contextualised in the same certification lifecycle, acting as a **bridge between SCs and the world of regulations and standards**.

Using the RHP, the consortium systematically checks that each new method or technology meets necessary SSQR criteria at the right development stage. We "plug" each Cynergy4MIE outcome into the RHP to evaluate how it would be certified or approved in real life. This approach yields multiple benefits:

- It guarantees critical safety and quality activities are not skipped. For example, hazard analysis (from functional safety) and threat analysis (from cybersecurity) are prompted by the RHP at concept/design phases for each SC, even for novel cross-domain applications.
- It ensures compatibility with existing regulations by mirroring core steps common to standards and certification schemes. By aligning our work with those steps (such as safety case development per ISO 26262 or testing per UNECE regulations), we generate evidence in formats familiar to authorities, making compliance demonstration more straightforward. Essentially, following the RHP and relevant standards at each step means our innovations are "homologation-ready" developed with an eye on required documentation, testing, and assurance for approval.

Just as importantly, the RHP serves as a **diagnostic tool for identifying gaps** in standards or methods when new technologies don't fit neatly into the established process. As Cynergy4MIE maps its novel solutions onto the RHP, it actively looks for steps where existing standards/regulations provide no clear guidance. These "friction points" indicate standardisation gaps (for instance, if proving the reliability of an AI-driven traffic optimisation service has no corresponding standard method, we flag it). The project has already applied this RHP-based mapping to highlight areas not fully covered by current standards – such as cooperative vehicle-infrastructure safety validation, cross-domain cybersecurity assurance, and metrics for AI performance in safety-critical scenarios. These findings directly inform our proposals to standardisation bodies (as detailed in each SC's contribution plan above), effectively **feeding the gaps back into the standards ecosystem**.

By using the RHP, Cynergy4MIE also streamlines cross-domain homologation. Instead of treating mobility, infrastructure, and energy innovations separately (which could lead to inconsistent or duplicated certification efforts), the RHP provides a unified process integrating all pieces. This yields a consolidated assurance case covering interactions between domains by the time we reach the certification gate. For example, an electric automated vehicle in SC4 continuously interacting with smart infrastructure and the grid (SC6) is handled in one end-to-end safety/security analysis – the RHP ensures we extend vehicle-level safety analyses to include V2X communication failures or grid faults, rather than siloing those considerations. The result is a coherent picture for regulators, likely easing type-approval of such complex systems. It shows regulators that our solutions adhere to high-level processes they are familiar with, reducing ambiguity in how to approve them.

In summary, aligning Cynergy4MIE's outputs with the Reference Homologation Process creates a powerful synergy: it reinforces SSQR disciplines throughout development and accelerates convergence by ensuring "safety doesn't stop at domain boundaries." Each domain's contributions (SC1–SC6) are integrated into one safety-security-quality framework. This approach not only helps identify and address gaps (which we then carry to standards bodies) but also builds trust with regulators by demonstrating that even novel cross-domain technologies have been developed and evaluated in compliance with state-of-the-art homologation practices. The RHP thus underpins our cross-SC standardisation strategy, guiding the project's journey toward safe and reliable convergence of mobility, infrastructure, and energy systems.

In practice, Cynergy4MIE uses the RHP to create a **traceability matrix** linking each SC output to the relevant RHP gate and the deliverable documenting it. Table 1 below provides an overview of this mapping:

Std. Cluster (SC)	***Key Output (Pre-normative focus)***	***RHP Gate***	***Deliverable (Month)***
SC1 (Automated Machinery)	Adverse-weather scenario library for LiDAR testing (contribution to ISO 13228)	Validation & Testing Gate – provides test evidence for perception	D7.9 (M24) initial results; D7.10 (M30) refined contribution
SC2 (Collab. Robotics	HRC safety & AI guidelines for dynamic human-robot collaboration	Requirement & Design Gate – informs system requirements and design specs	D7.10 (M30) – proposed standard guidelines in final report
SC3 (Powertrains)	WBG semiconductor reliability data and	Design & Validation Gates – feeds component design	D7.10 (M30) – standardisation

	qualification protocols	criteria and validation tests	proposal on WBG (reliability TS)
SC4 (Automated Driving)	Simulation-based homologation framework and cooperative ADS scenario suite	Validation & Certification Gates – supplements physical testing with virtual evidence	D7.10 (M30) – contribution to UNECE (virtual testing)
SC5 (Multi-agent SAR)	Multi-robot emergency response dataset & performance metrics	Validation Gate – provides benchmark for multi-agent system efficacy	D7.10 (M30) – IEEE RAS white paper/dataset release
SC6 (Energy & Control)	& Control) Harmonised heat pump testing method & V2G interface specifications	Requirement & Design Gates – informs standards for system efficiency and interoperability	D7.9 (M24) – heat pump standard input; D7.10 (M30) – V2G standard proposal

Table 2: Mapping of SC outputs to RHP gates and project deliverables. This shows how each Supply Chain's pre-normative output enters the RHP at a specific gate and is documented in Cynergy4MIE deliverables (D7.9 or D7.10) along with the timeline.

By structuring our efforts in this way, we maintain clear traceability to the Grant Agreement and ensure that all proposed actions align with the relevant tasks (notably T7.4 for standardisation strategy, T1.4 for requirements in ADS, WP5 for validation frameworks, and the objectives of D7.9/D7.10 to deliver standardisation contributions). This rigorous alignment reinforces the credibility of our approach, each abstract claim or identified gap is grounded in concrete examples from our demonstrators (as we have done, referencing Demos 4.1–4.3 for SC4, etc.) and each proposed standard contribution is anchored in the validated needs observed via the RHP mapping. Thus, Cynergy4MIE's standardisation roadmap is not an isolated afterthought but an integrated, evidence-backed plan to influence the state of the art and fill the crucial gaps on the path to convergent CPS deployment.

10. Ethical, Inclusive, and Societal Challenges in Standardisation

This chapter examines key societal challenges that standardisation efforts must address, including building public trust and acceptance through transparency, ensuring inclusivity and DEI (Diversity, Equity, Inclusion) in standards, closing legal and ethical gaps in current certification regimes, and establishing effective human-in-the-loop and accountability frameworks. These aspects are crucial for the broad acceptance of Advanced Driver Assistance Systems (ADAS) and Automated Driving Systems (ADS), as evidenced by our questionnaire findings and literature. Below we present the findings and analysis for each sub-section.

10.1 Questionnaire Findings on Trust, Transparency, Acceptance

User trust in ADAS/ADS is closely tied to perceptions of safety, transparency, and authoritative oversight. Our questionnaire results indicate that certification by a trusted authority (such as ISO or UNECE) significantly boosts user confidence in using these systems.

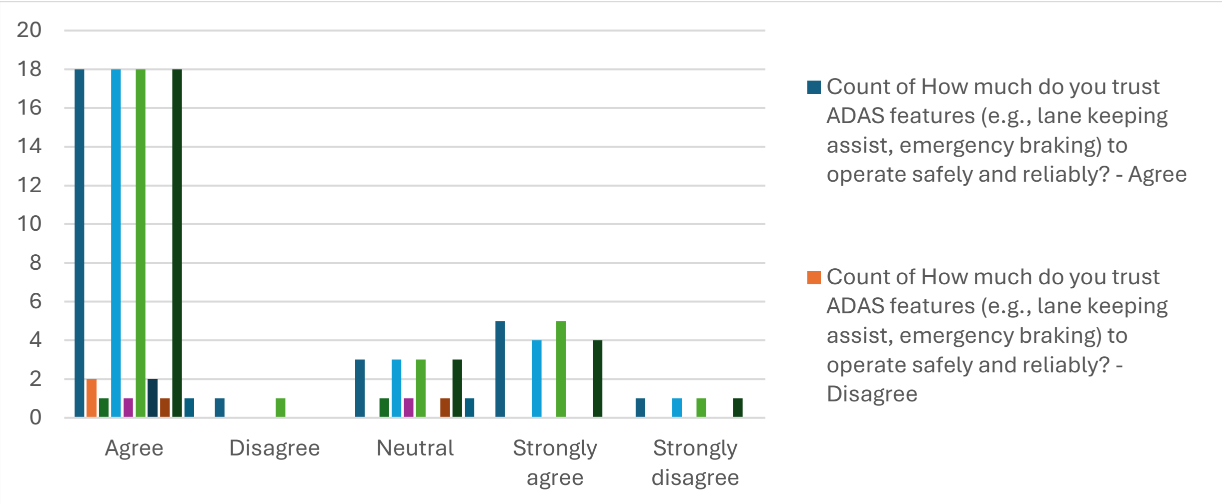

Figure 1: Relationship Between User Trust in ADAS/ADS and the Importance of Certification and System Transparency

This cross-tabulated chart illustrates how user trust in Advanced Driver Assistance Systems (ADAS) and future Automated Driving Systems (ADS, SAE Levels 3–5) correlates with their perceptions of system certification and transparency. The X-axis categorises respondents by their level of agreement with the statement "Knowing that an ADAS and ADS feature is certified by an international standard would increase my trust in using it." The Y-axis shows the number of respondents in each category who expressed varying levels of trust in (i) current ADAS functionality, (ii) future ADS operating without human supervision, and (iii) their confidence when system decision-making is clearly understood.

The chart shows a strong positive association between agreement with certification importance and overall user trust. Respondents who agree or strongly agree that certification enhances trust also tend to report high confidence in ADAS operations and are more willing to accept future ADS technologies. This trend holds across all trust-related measures and supports the claim that authoritative certification and transparent system behaviour are key enablers of user acceptance. Conversely, those who disagreed with the value of certification exhibited lower levels of trust and confidence.

These insights empirically reinforce the argument that perceived regulatory oversight and explainability significantly shape user acceptance of autonomous systems and should be prioritised in standardisation efforts related to safety, transparency, and public trust.

A strong majority of participants agreed that knowing an ADAS/ADS feature is certified to international standards would increase their trust in it. In fact, safety ratings and official certifications were identified as key influences on consumer trust, with many willing to pay extra for vehicles with higher safety ratings. This underscores how formal standardisation and certification serve as reassurance that the technology meets accepted safety and ethical benchmarks.

Transparency of system operations emerged as another critical factor for acceptance. Respondents expressed that they feel more confident using ADAS when they understand how and why the system makes decisions, and they strongly support having real-time explanations of ADS actions. Clear, transparent communication from the system was seen as essential for building user confidence. In practice, this means drivers prefer ADAS/ADS features that provide understandable feedback or reasoning for their actions (e.g. notifications explaining an emergency brake) to foster trust through explainability. Indeed, transparent communication and rigorous testing were highlighted as vital for widespread acceptance of autonomous technologies.

The questionnaire also probed which measures would most increase public acceptance of higher automation. Participants could select multiple measures, and the most frequently endorsed ideas included:

- **Certification by a trusted authority** (e.g. international standard or regulatory body) – indicating that third-party validation of ADS safety/ethics is highly valued.
- **Real-time explanations of ADS actions** – underlining the demand for transparency and explainability in how the vehicle behaves.
- **Manual override always available** – reflecting a desire for driver control and the ability to intervene, which relates to maintaining human oversight.
- **Ethical/bias audits of algorithms** – showing public concern for fairness and the avoidance of biased or unsafe decision-making by AI.

- (Other commonly selected measures included extensive testing/validation and public consultation for transparency.)

These findings demonstrate that both institutional trust mechanisms and technical transparency/control features are crucial for user acceptance. Users want to know that ADS technologies have been vetted by reputable standards and that the systems themselves are designed to be understandable and controllable.

Finally, our survey highlighted an awareness gap: a significant portion of respondents were not initially aware that international standards (ISO, IEEE, UNECE, etc.) even exist to certify ADAS/ADS safety and ethics. This suggests that outreach and education about standardisation efforts could improve public trust. Overall, trust, transparency, and acceptance are deeply interlinked, by addressing these through robust standards (certifications, explainability requirements, etc.), stakeholders can increase user confidence in automated driving.

10.2 Inclusivity and DEI Considerations in Standards

Standards must ensure that advanced vehicle technologies are inclusive and equitable for all segments of society. Inclusivity in this context means systems should be usable and safe for people of different ages, genders, ethnic backgrounds, and abilities. Our questionnaire revealed a concern that current systems may not equally accommodate all users, few respondents agreed that today's ADAS/ADS effectively serve everyone regardless of demographics or disability, suggesting a perceived lack of inclusivity in design. This aligns with broader research indicating that if design and testing lack diversity, certain groups (e.g., older adults, women, racial minorities, persons with disabilities) may face reduced benefits or even disproportionate risks from automation (West, 2020; Ajunwa, 2023).

For example, biases in AI perception systems, such as facial recognition or pedestrian detection, can lead to worse performance for under-represented groups, an unacceptable outcome that standards should proactively prevent (Buolamwini & Gebru, 2018). Diversity, Equity, and Inclusion (DEI) considerations are increasingly being recognised in standardisation. Many participants in our study strongly supported measures to ensure fairness: there was broad agreement that ADAS/ADS should undergo independent audits for fairness and unbiased treatment of all users. In other words, stakeholders want external validation that these systems do not discriminate or systematically underserve any group. Incorporating such audits or bias checks into certification schemes could address public concerns. Additionally, one of the top "gaps" identified was the absence of inclusivity requirements and algorithmic bias considerations in current standards, highlighting that existing technical standards have not yet fully tackled these issues.

To make standards more inclusive, several approaches are recommended:

- **Inclusive Design Requirements**: Standards should mandate that vehicles and HMIs (Human-Machine Interfaces) are accessible to users with varied physical and cognitive abilities. For instance, the U.S. Access Board (2021) has emphasised that autonomous vehicles must be inclusive of everyone, including people with disabilities.

- **Bias Mitigation in Algorithms**: Standardisation can introduce guidelines for testing AI components (like vision or decision systems) against diverse datasets to ensure they perform equally well for all demographic groups. Requiring bias testing and mitigation (as also suggested by our respondents) would push manufacturers to address issues such as poorer detection of dark-skinned pedestrians or different reactions based on driver profiles (Raji et al., 2020).
- **Diverse Stakeholder Involvement**: The process of developing standards should involve a diverse set of experts and end-users. By including voices from different genders, ethnicities, ages, and disability communities, standards bodies can better identify biases or barriers and craft requirements that ensure equity and accessibility. This also helps build public trust that standards reflect societal values, not just industry priorities.

Notably, there are emerging standards aimed at ethical and inclusive aspects, for example, **ISO 39003:2023** provides guidance on ethical considerations for autonomous vehicles (ISO, 2023), and the **IEEE 7000 series** offers frameworks for ethically aligned design and stakeholder inclusion in system development (IEEE, 2021). However, these are relatively new and not yet universally adopted. Our findings indicate that stronger DEI provisions in mainstream automotive standards are needed. Standardisation efforts should explicitly cover fairness, accessibility, and user diversity to ensure ADS technologies benefit all segments of society and to avoid digital divides or inadvertent discrimination as automation progresses.

10.3 Legal and Ethical Gaps in Certification

The convergence of mobility, infrastructure, and energy (MIE) in Cynergy4MIE exposes significant gaps in current certification frameworks. Traditionally, each domain uses siloed certification standards (e.g. automotive type-approval, grid codes, machinery safety), focusing on technical safety and performance. However, cross-domain systems, such as autonomous electric vehicles interacting with smart traffic infrastructure and the power grid, lack a unified certification approach. This leaves legal and ethical considerations under-addressed.

Key gaps include:

Data Privacy: Ensuring GDPR-compliant data handling is mandatory in the EU, but product certification rarely verifies privacy protections. Connected vehicles and infrastructure exchange sensitive data (location, user identity, energy usage) without dedicated certification for privacy-preservation. Project guidance emphasises careful handling of personal data in AI and strict GDPR compliance, yet no formal “privacy seal” exists for integrated MIE systems. Survey feedback indicates users would be concerned about ADAS/ADS features that are not certified for data privacy compliance and bias avoidance. This gap undermines trust in cross-domain data sharing (European Union Agency for Cybersecurity [ENISA], 2022; European Commission, 2024).

Algorithmic Bias and Inclusivity: Current vehicle and infrastructure regulations focus on safety and fail-safe behaviour, not on ensuring AI decisions are fair or inclusive. There is no certification to guarantee an autonomous shuttle or traffic management AI treats all users equitably. Cynergy4MIE commits to avoiding unintended prejudice or discrimination from biased datasets, aligning with EU ethical guidelines (European Commission, 2021). Yet in practice, bias audits and fairness checks are voluntary. Users strongly support independent audits to ensure ADAS/ADS fairness for all ages, genders, ethnicities, or disabilities, highlighting a need for formal standards on inclusivity (IEEE, 2021).

Liability and Legal Accountability: In cross-sector deployments it is unclear who is liable when an AI-driven decision causes harm. For example, if an autonomous EV (mobility) guided by smart road sensors (infrastructure) and optimised by an energy-management AI makes a wrong decision, legal frameworks may struggle to assign responsibility. Existing laws are evolving, notably the UK's Automated Vehicles Act 2024, which establishes that an Authorised Self-Driving Entity (ASDE) is responsible for a vehicle's behaviour when it is in self-driving mode (UK Department for Transport, 2024). For fully driverless vehicles, a separate "no-user-in-charge" operator is designated for maintenance and incident response. Similarly, the EU AI Act will mandate that high-risk AI (e.g. in transport or energy safety) has a clearly identified provider responsible for compliance and incident reporting (European Parliament & Council, 2024).

Ethical AI and Societal Trust: There is currently no comprehensive certification for "ethical AI" in intelligent mobility or infrastructure. Type-approval standards (e.g. UNECE WP.29) set performance and safety minima (UNECE, 2021), but do not address moral decision-making in dilemmas or transparency of AI reasoning. For instance, how an autonomous vehicle chooses actions in an unavoidable accident scenario raises ethical questions not covered by safety tests. ISO 39003:2023 provides guidance on ethical considerations for autonomous vehicles, addressing decision-making in emergencies (ISO, 2023). However, the standard applies primarily to SAE Level 5 vehicles and does not define pass/fail criteria. Similarly, IEEE 7001 (on transparency) and IEEE 7003 (on algorithmic bias) propose design frameworks but remain non-binding (IEEE, 2021; IEEE, 2023). The EU AI Act complements these by requiring documentation of training data, bias mitigation, and user-facing transparency (European Parliament & Council, 2024), though certification is still fragmented.

Cross-Domain Interoperability: Each sector has its own safety standards (e.g. ISO 26262 for automotive, IEC 61508 for industrial systems, grid codes for energy). When a converged system spans domains, interface risks might fall through the cracks. A flaw at the intersection, say, a hacked traffic signal sending false data to cars, may not be explicitly covered by any single certification. Efforts like UNECE R155/R156 for cybersecurity and software updates in vehicles are a step forward (UNECE, 2021), but equivalent frameworks for infrastructure and energy IoT are still evolving. No unified certification ensures end-to-end safety/security across vehicle-to-infrastructure-to-grid systems.

Implications: These gaps underscore why traditional certification must evolve for the MIE ecosystem. Public surveys in Cynergy4MIE show that trust is strongly linked to rigorous certification: respondents indicate that knowing an ADAS/ADS is certified by respected standards (ISO, UNECE, etc.) "would increase my trust in using it." Likewise, a majority believes such certification is essential before deployment. Moreover, beyond safety, people want assurances of privacy and ethics, calling for certifications or audits to cover those aspects as well. The absence of visible cross-domain certifications can hinder user acceptance of convergent technologies. In sum, while Cynergy4MIE's technological innovations push domain boundaries, an equivalent push in legal, ethical, and standardisation frameworks is required. This entails expanding certification criteria to include data governance, algorithmic fairness, inclusivity, and accountability, ensuring the converged system is worthy of societal trust.

10.4 Human-in-the-Loop and Accountability Frameworks

In semi-automated systems (e.g. SAE Level 2 driver assistance), the human operator is expected to constantly supervise and remain the primary decision-maker. Certification and design standards enforce this through requirements like driver monitoring systems and clear warnings – for example, today's L2 vehicles disengage if the driver's hands are off the wheel for too long. The human bears full responsibility for safe operation (UK Department for Transport, 2022).

By contrast, at Level 3 (conditional automation), the vehicle can drive itself under certain conditions, but the human driver must take over when the system requests. This "on-call" oversight creates risk; humans may become complacent or inattentive. Standards such as ISO 21989 and UNECE's ALKS Regulation attempt to mitigate this by limiting L3 use cases and requiring clear handover protocols (UNECE, 2022; Auto2x, 2023).

Projects like Cynergy4MIE emphasise that a human must always could see, modify, or override an AI system's actions at any moment, effectively mandating a human-in-the-loop or on-the-loop role. This is consistent with the EU AI Act's mandate that high-risk AI systems "must have appropriate human oversight mechanisms" (European Commission, 2024).

At Level 4, autonomy extends to handling all operations within a predefined domain without human input. Oversight may take the form of remote supervision – e.g., a control centre ready to intervene in case of anomalies. The UK's AV Act (2024) introduces clear legal constructs such as the Authorised Self-Driving Entity (ASDE) and "no-user-in-charge operator," allocating full accountability to providers in autonomous operation (UK Government, 2024).

At Level 5, human input is entirely excluded. Ethical frameworks such as ISO 39003 recommend aligning automated behaviour with moral principles, and emphasize transparency and traceability (Invensity, 2023). The EU AI Act demands that providers of Level 5 systems ensure transparency, traceability, and the ability to intervene (Bird & Bird, 2024).

Although often discussed in automotive contexts, HITL concerns apply to smart infrastructure and energy as well. For example, AI traffic systems must allow oversight to avoid unintended harms (e.g., favouring one group over another). Similarly, autonomous energy systems controlling grid distribution must be supervised to ensure compliance with regulatory constraints. Currently, standards like ISO 27019 do not mandate AI-specific HITL features in energy systems – a convergence opportunity exists for harmonisation with automotive best practices.
Standards like IEEE 7001 (Transparency) and IEEE 7000-2021 (Ethical System Design) provide methods for embedding explainability and ethical design traceability into AI development (IEEE, 2021; IEEE, 2022). These promote auditable logs and rationales for decisions – a foundation for legal and societal accountability.

To ensure safe, accountable, and ethically robust deployment of autonomous systems across mobility, infrastructure, and energy domains, certification frameworks must explicitly include Human-in-the-Loop (HITL) criteria and ethics-based evaluation. Regulatory harmonisation across domains is also essential; for instance, the Authorised Self-Driving Entity (ASDE) model introduced in the UK automotive context should be extended to sectors such as energy and infrastructure to ensure consistent responsibility assignment. Furthermore, standardised logging formats and interoperability protocols are necessary to trace actions and ensure accountability across interconnected systems. Equally important is the role of users: clear instructions, training programmes, and interface transparency must be mandated so that end-users can engage effectively with the systems. Finally, continuous ethical oversight should be institutionalised through mechanisms like Ethics Advisory Boards, ensuring that systems remain aligned with evolving societal expectations and regulatory frameworks throughout their lifecycle.
In conclusion, Cynergy4MIE supports a unified framework where humans remain integral to AI governance across domains. By aligning with EU AI regulations, ISO 39003, IEEE 7000-series, and stakeholder input, it sets the stage for legally and ethically robust deployment of autonomous systems in mobility, infrastructure, and energy.

11. Strategic Recommendations

11.1 Standardisation Roadmap for Cynergy4MIE

Cynergy4MIE aims to contribute to a coherent standardisation strategy that supports convergence across mobility, infrastructure, and energy (MIE) systems. To do so, it must align its technological developments with the evolving standardisation landscape. The roadmap proposed includes:

- **Short-Term (M1–M18)**: Conduct gap analyses per SC (in this report), and initiate discussions in relevant standardisation bodies (e.g. ISO, CEN/CENELEC, ETSI) on observed shortcomings in areas like cross-domain reliability, inclusivity, AI transparency, and HITL accountability. Map all technical innovations to relevant existing standards or note absence thereof.
- **Medium-Term (M19–M30)**: Propose new work items (NWIs) or extensions to existing standards, particularly in cross-domain certification (e.g., vehicle-to-grid safety, AI behaviour explainability, cooperative perception validation). These can take the form of contributions to ISO 39003, IEEE 7000-series, or UNECE WP.29 updates. Reference use-case-driven evidence from Cynergy4MIE demos.
- **Long-Term (M31–M36 and beyond)**: Contribute to certification readiness of convergent systems by producing standardisation blueprints and pre-certification toolkits (e.g., audit templates, logging protocols). Embed ethical, societal, and legal accountability mechanisms into final deliverables and promote integration into European Digital Product Passports, AI Act registries, and CE mark evolution.

This roadmap will be further detailed and operationalised through D7.10 (Standardisation proposals) and D7.11 (Final uptake and compliance framework).

11.2 Pathways for Cynergy4MIE Contributions to Standard Development

Building on the roadmap, Cynergy4MIE can engage in standardisation via several channels:

- **Task Force Creation within Standardisation Bodies**: Partners already involved in ISO/IEC, IEEE, SAE or UNECE (as per survey data) can propose focused working groups on identified gaps, such as cross-domain AI explainability or V2X-Energy coordination.
- **Use Case as Evidence**: Demonstrators across SC1–SC6 provide high-fidelity scenarios (e.g., cooperative ADS traffic control, modular heat-pump optimisation) that can inform standardisation. For example, results from Demo 4.2 (road condition sensing with InSAR and TPMS) could support an ISO extension on multi-modal sensor fusion for road safety.
- **Ethical Standards Contribution**: Ethics-related gaps (e.g., lack of independent audits, insufficient DEI in HMI standards) can be addressed via contribution to ISO 39003

extensions or IEEE 7003 updates. Cynergy4MIE's internal ethics governance and survey data provide a robust evidence base for such contributions.

- **Reference Homologation Process (RHP)**: As discussed in section 9.3, the project's alignment with a unified certification framework (RHP) provides a scaffold for identifying missing standardised steps. These gaps can directly inform proposals for cross-domain conformity assessments.

11.3 Stakeholder Engagement and Policy Impact

To ensure practical uptake, Cynergy4MIE must bridge the gap between technical insights and regulatory/policy influence:

- **Engage National and European Policy Makers**: Proactively liaise with DG MOVE, DG ENER, and the AI Office (for AI Act alignment), ensuring Cynergy4MIE findings inform delegated acts, regulation updates, and national adoption pathways.
- **Contribute to Public Consultations and Roadmaps**: Feed insights into EC policy consultations on AI ethics, data governance, and mobility/energy regulation. Highlight gaps in transparency, certification, and user trust using aggregated survey findings and real-world pilot results.
- **Develop Position Papers and White Papers**: Targeted briefs to UNECE, ISO, CEN, and IEEE can present Cynergy4MIE's case for integrated certification, proposing practical regulatory reforms (e.g., creation of an "Ethical AI Certification" label as described in Section 10).
- **Support Standardisation Education and Advocacy**: Workshops and stakeholder roundtables with SMEs, cities, and public interest groups should be held to demystify certification pathways and ensure uptake of new ethical-AI-oriented standards across society.

11.4 Future Integration into Certification and Regulatory Frameworks

The final strategic step is to ensure that Cynergy4MIE's outputs can be seamlessly integrated into real-world certification and regulatory environments. Key actions include:

- **Embed Certification Requirements into Design and Prototyping**: All technical SCs should align their technology readiness levels (TRLs) and deliverables with homologation expectations, using the RHP as a guide (e.g., V2X safety tests, privacy audits, AI traceability logging).
- **Define Pre-Standardisation Templates**: Create publicly available validation blueprints and audit checklists that map to both ISO and UNECE requirements. These pre-standardisation tools will aid future adopters and regulators.

- **Pilot End-to-End Certification Scenarios**: Select 1–2 SCs (e.g., SC4 or SC6) to pilot a full end-to-end certification simulation, involving technical validation, conformity assessment, and ethical review. This approach can reveal any remaining friction points.
- **Prepare for AI Act and Green Deal Alignment**: Ensure all Cynergy4MIE innovations are mapped to high-risk AI obligations under the EU AI Act (risk management, data governance, human oversight) and to climate/sustainability KPIs under the Green Deal.

12. References

Ajunwa, I. (2023). *The quantified worker: Law and technology in the modern workplace.* Cambridge University Press.

Amodei, D., Olah, C., Steinhardt, J., Christiano, P., Schulman, J., & Mané, D. (2016). Concrete problems in AI safety. *arXiv preprint* arXiv:1606.06565.

American Society of Heating, Refrigerating and Air-Conditioning Engineers. (2019). *ANSI/ASHRAE/IES Standard 90.1-2019 — Energy standard for buildings except low-rise residential buildings.*

AUTOSAR. (2023). *AUTOSAR Adaptive Platform — Release 23-03.* https://www.autosar.org/standards/adaptive/

Autonomous Vehicle Computing Consortium (AVCC). (2022). *Enabling software interoperability for next-gen autonomous vehicle compute platforms.*

BMVI. (2021). *Act on autonomous driving: Germany becomes the first country to pass comprehensive Level 4 law.* Federal Ministry of Transport and Digital Infrastructure.

Buolamwini, J., & Gebru, T. (2018). Gender shades: Intersectional accuracy disparities in commercial gender classification. *Proceedings of Machine Learning Research, 81,* 1–15.

Calo, R. (2016). Robots in American law. *University of Washington School of Law Research Paper.*

Canadian Standards Association. (2023). *CSA EXP150 — Connected and automated vehicle infrastructure standards.* https://www.csagroup.org/article/experimental-standards-cav-infrastructure/

Car-2-Car Communication Consortium. (2022). *Interoperability certification guidelines for ETSI ITS-G5.*

CENELEC. (2011). *EN 50090-1:2011 — Home and Building Electronic Systems (HBES) — Architecture.*

CharIN. (2022). *Charging Interface Initiative: Certification & testing overview.*

Connected Automated Driving. (2021a). *Standards in connected automated driving.*
Connected Automated Driving. (2021b). *Contributions from EU projects on AI and safety.*
Connected Automated Driving. (2021c). *Human factors and HMI research in CAD.*
Connected Automated Driving. (2021d). *CAD recommendations on cross-domain certification gaps.*
Connected Automated Driving. (2021e). *Emerging interface and safety standardisation efforts.*

Disability Rights Education & Defense Fund (DREDF). (2022). *Addressing disability and ableist bias in autonomous vehicles* (I. Moura).

DNV. (2022). *Certification procedures for distributed energy systems and grid integration.*

EASA. (2021). *Special condition for specific operations risk assessment (SORA).*

EEBus. (2022). *EEBus Alliance: Interoperability for smart home devices.*

Edwards, L., & Veale, M. (2017). Slave to the algorithm? Why a “right to an explanation” is probably not the remedy you are looking for. *Duke Law & Technology Review, 16*(1), 18–84.

ENISA. (2022). *Guidelines for securing connected and automated mobility systems.*

Erdelyi, O. J., & Goldsmith, J. (2018). Regulating artificial intelligence: Proposal for a global solution. In *Proceedings of the AAAI/ACM Conference on AI, Ethics, and Society* (pp. 95–101).

ETSI. (2014). *EN 302 637 series — Intelligent Transport Systems (ITS): Vehicular communications.*
ETSI. (2017a). *TS 102 726 — ITS-G5: European access layer for V2X communications.*
ETSI. (2017b). *EN 302 637-2 V1.4.1 — Cooperative Awareness Message (CAM).*
ETSI. (2020). *TS 103 097 — Security framework for ITS communications.*
ETSI. (2021). *EN 303 613 — Automotive radar equipment operating in 76–81 GHz.*

European Commission. (2006). *Directive 2006/42/EC on machinery.*
European Commission. (2012). *Directive 2012/18/EU on major-accident hazards (Seveso III).*
European Commission. (2014a). *Directive 2014/53/EU on radio equipment (RED).*
European Commission. (2014b). *Directive 2014/68/EU on pressure equipment (PED).*
European Commission. (2019). *Regulation (EU) 2019/2144 on type-approval requirements for motor vehicles.*
European Commission. (2020). *C-ITS deployment and standards overview.*
European Commission. (2021a). *Proposal for a Regulation laying down harmonised rules on artificial intelligence (Artificial Intelligence Act).*
European Commission. (2021b). *Vehicle safety and automated/connected vehicles (General Safety Regulation).*
European Commission. (2023a). *Regulation (EU) 2023/1230 on machinery products.*
European Commission. (2023b). *Regulation (EU) 2023/1542 on batteries and waste batteries.*
European Commission. (2024). *Regulation (EU) 2024/1689 (“EU AI Act”) — Laying down harmonised rules on artificial intelligence.*

European Parliament & Council. (2014). *Directives 2014/35/EU, 2014/30/EU & 2014/53/EU.*

High-Level Expert Group on AI. (2019). *Ethics guidelines for trustworthy AI.* European Commission.

IEEE Robotics and Automation Society. (2021). *IEEE 1872.2-2021 — Standard for autonomous robotics ontology.*

Institute of Electrical and Electronics Engineers. (2010). *IEEE 802.11p-2010 — Wireless access in vehicular environments (WAVE).*

Institute of Electrical and Electronics Engineers. (2015). *IEEE 2030.1.1-2015 — Technical specifications of a DC quick charger for use with electric vehicles.*

Institute of Electrical and Electronics Engineers. (2017). *IEEE 802.11p — Wireless access in vehicular environments (WAVE).*

Institute of Electrical and Electronics Engineers. (2019). *IEEE 1609.2 — Security services for WAVE applications.*

Institute of Electrical and Electronics Engineers. (2021a). *IEEE 7000-2021 — Model process for addressing ethical concerns during system design.*

Institute of Electrical and Electronics Engineers. (2021b). *IEEE 7001-2021 — Standard for transparency of autonomous systems.*

Institute of Electrical and Electronics Engineers. (2022). *IEEE 2846-2022 — Standard for assumptions for models in safety-related automated vehicle behavior.* https://standards.ieee.org/ieee/2846/10631/

Institute of Electrical and Electronics Engineers. (2023a). *IEEE 7003-2023 — Algorithmic bias considerations.*

Institute of Electrical and Electronics Engineers. (2023b). *IEEE 7010-2023 — Well-being metrics for ethical AI.*

Institute of Electrical and Electronics Engineers. (2024). *IEEE P2040 — Draft standard for general requirements for fully automated vehicles.*

International Electrotechnical Commission. (2010). *IEC 61508-1:2010 — Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 1: General requirements.* https://webstore.iec.ch/publication/6028

International Electrotechnical Commission. (2010). *IEC 61508 — Functional safety of electrical/electronic/programmable electronic safety-related systems.*

International Electrotechnical Commission. (2013). *IEC 61850 — Communication networks and systems in substations.*

International Electrotechnical Commission. (2016). *IEC 60204-1:2016 — Safety of machinery — Electrical equipment of machines — Part 1: General requirements.* https://webstore.iec.ch/publication/25114

International Electrotechnical Commission. (2017). *IEC 61851-1:2017 — Electric vehicle conductive charging system — Part 1: General requirements.* https://webstore.iec.ch/publication/26176

International Electrotechnical Commission. (2018a). *IEC 62443-4-1:2018 — Industrial communication networks — Network and system security — Part 4-1: Secure product development lifecycle requirements.*

International Electrotechnical Commission. (2018b). *IEC 62660-1:2018 — Secondary lithium-*

ion cells for propulsion — Performance testing.
International Electrotechnical Commission. (2019). *IEC 61000 series — Electromagnetic compatibility standards.*
International Electrotechnical Commission. (2020). *IEC 62351 — Data and communications security for power systems management.*
International Electrotechnical Commission. (2021a). *IEC 62061:2021 — Safety of machinery — Functional safety of safety-related control systems.* https://webstore.iec.ch/publication/60229
International Electrotechnical Commission. (2021b). *IEC 61850-7-420:2021 — Communication networks and systems for power utility automation — Part 7-420: DER and DA logical nodes.* https://webstore.iec.ch/publication/34384
International Electrotechnical Commission. (2022a). *IEC 60068 — Environmental testing.*
International Electrotechnical Commission. (2022b). *IEC 60825 — Safety of laser products.*
International Electrotechnical Commission. (2022c). *IEC 62282 — Fuel cell technologies.*
International Electrotechnical Commission; & IEEE. (2013a). *IEC/IEEE 62270 — Guide for computer-based control systems in automation.*
International Electrotechnical Commission; & IEEE. (2013b). *IEC/IEEE 62270-1 — Guide for computer-based control systems in automation.*

International Organization for Standardisation. (2011a). *ISO 10218-1 — Robots and robotic devices — Safety requirements for industrial robots — Part 1.*
International Organization for Standardisation. (2011b). *ISO 10218-2 — Robots and robotic devices — Safety requirements for industrial robots — Part 2.*
International Organization for Standardisation. (2012). *ISO 8373:2012 — Robots and robotic devices — Vocabulary.*
International Organization for Standardisation. (2013a). *ISO 12405-1:2013 — Electrically propelled road vehicles — Lithium-ion traction battery packs and systems — Part 1: High power applications.* https://www.iso.org/standard/54084.html
International Organization for Standardisation. (2013b). *ISO/IEC 29182-1:2013 — Information technology — Sensor network reference architecture — Part 1: General overview and requirements.*
International Organization for Standardisation. (2013c). *ISO/IEC 29182-5:2013 — Information technology — Sensor network reference architecture — Part 5: Interface definitions.*
International Organization for Standardisation. (2014). *ISO 13482:2014 — Robots and robotic devices — Safety requirements for personal care robots.*
International Organization for Standardisation. (2015). *ISO 13849-1:2015 — Safety of machinery — Safety-related parts of control systems.* https://www.iso.org/standard/69883.html
International Organization for Standardisation. (2016a). *ISO/TS 15066:2016 — Robots and robotic devices — Collaborative robots.*

International Organization for Standardisation. (2016b). *ISO 186461:2016 — Performance criteria and test methods for wheeled service robots — Part 1: Locomotion.*
International Organization for Standardisation. (2018a). *ISO 18497:2018 — Agricultural machinery — Safety of highly automated machines.*
International Organization for Standardisation. (2018b). *ISO 19014-1:2018 — Earth-moving machinery — Functional safety.*
International Organization for Standardisation. (2018c). *ISO 23150:2018 — Road vehicles — Data communication between sensors and data fusion unit for automated driving functions — Logical interface.* https://www.iso.org/standard/74837.html
International Organization for Standardisation. (2018d). *ISO 26262-1:2018 — Road vehicles — Functional safety — Part 1: Vocabulary.* https://www.iso.org/standard/68383.html
International Organization for Standardisation. (2019a). *ISO 12405 — Electrically propelled road vehicles — Lithium-ion battery test specifications.*
International Organization for Standardisation. (2019b). *ISO 17757:2019 — Earth-moving machinery and mining — Autonomous and semi-autonomous machine safety.*
International Organization for Standardisation. (2019c). *ISO 21448:2019 — Road vehicles — Safety of the intended functionality (SOTIF).* https://www.iso.org/standard/70918.html
International Organization for Standardisation. (2019d). *ISO 6469 series — Electrically propelled vehicles — Safety specifications.*
International Organization for Standardisation. (2020a). *ISO 21782-1:2020 — Electrically propelled road vehicles — Test specification for electric propulsion components — Part 1: General test conditions and definitions.* https://www.iso.org/standard/72969.html
International Organization for Standardisation. (2020b). *ISO/IEC TR 24028:2020 — Trustworthiness in artificial intelligence.*
International Organization for Standardisation. (2021a). *ISO 13400-2:2021 — Road vehicles — Diagnostic communication over Internet Protocol (DoIP) — Part 2: Vehicle interface.* https://www.iso.org/standard/76429.html
International Organization for Standardisation. (2021b). *ISO 21498-1:2021 — Electrified powertrain — Components and systems — Part 1: General requirements and definitions.* https://www.iso.org/standard/73310.html
International Organization for Standardisation. (2021c). *ISO 23273:2021 — Hydrogen fuel cell road vehicles — Safety systems and requirements.* https://www.iso.org/standard/79966.html
International Organization for Standardisation. (2021d). *ISO 52120-1:2021 — Energy performance of buildings — Part 1: General planning principles.* https://www.iso.org/standard/71459.html
International Organization for Standardisation. (2022a). *ISO 15118-2:2022 — Road vehicles — Vehicle-to-grid communication interface — Part 2: Network and application protocol requirements.* https://www.iso.org/standard/55366.html
International Organization for Standardisation. (2022b). *ISO/PAS 21448:2022 — Safety of the intended functionality (SOTIF).*

International Organization for Standardisation. (2022c). *ISO/PAS 8800:2022 — Road vehicles — Safety and artificial intelligence.* https://www.iso.org/standard/81017.html
International Organization for Standardisation. (2023a). *ISO 39003:2023 — Road traffic safety — Ethical considerations for autonomous vehicles.*
International Organization for Standardisation. (2023b). *ISO/IEC 42001:2023 — Artificial-intelligence management system requirements.*
International Organization for Standardisation; International Electrotechnical Commission; & IEEE. (2017). *ISO/IEC/IEEE 12207:2017 — Systems and software engineering — Software life cycle processes.*
International Organization for Standardisation; & SAE International. (2021). *ISO/SAE 21434:2021 — Road vehicles — Cybersecurity engineering.*

ISA. (2021). *ISA/IEC 62443 — Cybersecurity for industrial automation and control systems.*

Keidanren. (2018). *Society 5.0 — Co-creating the future.*

Kenney, J. B. (2011). Dedicated short-range communications (DSRC) standards in the United States. *Proceedings of the IEEE, 99*(7), 1162–1182.

Koopman, P., & Wagner, M. (2016). Challenges in autonomous vehicle testing and validation. *SAE International Journal of Transportation Safety, 4*(1), 15–24.

Lu, H., Hsu, C. H., Wang, T., & Zhang, Y. (2021). Responsibility and liability in the era of autonomous vehicles. *Information, 12*(6), 238.

Monolithic Power Systems. (2022). *AEC-Q100 qualification and reliability standards.*

OECD. (2019/2024). *OECD Council Recommendation on Artificial Intelligence: OECD AI Principles.*

OmniAir Alliance. (2021). *Compliance and certification for DSRC and C-V2X devices.*

Open Charge Alliance. (2023). *Certification and interoperability programmes for EVSE.*

Oral, H., Anand, D., Nguyen, C., Gopstein, A., Brunner, C., & Apostolov, A. (2022). *IEC 61850 profile for distributed energy resources supporting IEEE 1547 (NIST TN 2217).* National Institute of Standards and Technology. https://doi.org/10.6028/NIST.TN.2217

Paden, B., Čáp, M., Yong, S. Z., Yershov, D., & Frazzoli, E. (2016). A survey of motion planning and control techniques for self-driving urban vehicles. *IEEE Transactions on Intelligent Vehicles, 1*(1), 33–55.

Peters, D., & Calvo, R. A. (2019). Responsible AI — Two frameworks for ethical design. *Nature Machine Intelligence, 1*(1), 8–9.

Power Sources Manufacturers Association. (2023). *WBG semiconductor reliability standards initiative & JEDEC JC-70.*

Qorvo. (2022). *Automotive quality and reliability standards overview.*

Raji, I. D., Binns, R., et al. (2020). Closing the AI accountability gap: An end-to-end framework for internal algorithmic auditing. In *ACM FAT* (pp. 33–44).

Robotic Industries Association. (2012). *ANSI/RIA R15.06-2012 — Industrial robot safety standard.*
Robotic Industries Association. (2022). *RIA Certified Robot Integrator Program.*

SAE International. (2014). *SAE AS5669A — JAUS Transport Standard — Packet construction and addressing.*
SAE International. (2015). *SAE AS5710A — JAUS Core Service Set — Distributed system coordination services.*
SAE International. (2016a). *SAE J2735 — DSRC message set dictionary.*
SAE International. (2016b). *SAE J3016 — Taxonomy and definitions for driving automation systems.*
SAE International. (2021a). *SAE J3016:2021 — Taxonomy and definitions for terms related to driving automation systems for on-road motor vehicles.* https://www.sae.org/standards/content/j3016_202104/
SAE International. (2021b). *SAE J3061 — Cybersecurity process framework.*
SAE International. (2023a). *SAE J1772:2023 — Electric vehicle and plug-in hybrid electric vehicle conductive charge coupler.* https://www.sae.org/standards/content/j1772_202306/
SAE International. (2023b). *SAE J2945/1:2023 — Dedicated Short Range Communications (DSRC) minimum performance requirements.*

Shladover, S. E. (2018). Connected and automated vehicle systems: Introduction and overview. *Journal of Intelligent Transportation Systems, 22*(3), 190–200.

TÜV SÜD. (2023a). *Machinery Regulation 2023/1230 — Key requirements and implications for manufacturers.*
TÜV SÜD. (2023b). *Functional safety: ISO 26262 and IEC 61508 explained.*
TÜV SÜD. (2023c). *Collaborative robots: Safety, CE marking, and the new EU Machinery Regulation.*
TÜV SÜD. (2023d). *Electric-vehicle battery testing to UNECE R100.*
TÜV SÜD. (2023e). *Functional-safety assessment ISO 26262 for automotive.*

UK Department for Transport. (2024). *Automated Vehicles Act 2024.*

UK Law Commission. (2022). *Automated vehicles: Joint report of the Law Commission of England & Wales and the Scottish Law Commission.*

UL. (2020). *UL 4600 — Standard for evaluation of autonomous products.*

UNECE. (2019a). *UN Regulation No. 79: Steering equipment.*
UNECE. (2020). *UN Regulation No. 157: Automated Lane Keeping Systems.*

UNECE. (2021a). *UN Regulation No. 155: Cybersecurity.*
UNECE. (2021b). *UN Regulation No. 156: Software update.*
UNECE. (2022a). *Amendments to UN R157 for higher-speed and lane-change functions.*
UNECE. (2022b). *REESS thermal-propagation amendments (UN R100).*

United Nations. (2021). *Manual of tests and criteria* (Rev. 7, Sect. 38.3 — Lithium-battery transport testing).

U.S. Access Board. (2021). *Recommendations on accessibility guidelines for self-driving vehicles.*

West, S. M. (2020). Data capitalism: Redefining the logics of surveillance and privacy. *Business & Society, 59*(1), 107–131.

13. Annexes

A. Full Survey Questionnaire - Cynergy4MIE Questionnaire on User and Societal Acceptance of Advanced Driver Assistance Systems (ADAS) and Automated Driving Systems (ADS)

Information Sheet

In support of the HORIZON JU Research and Innovation Actions
- Cynergy4MIE Project -
Project number: 101140226 Granting authority: Chips Joint Undertaking

Introduction

You have been invited to participate in a research activity carried out within the scope of the EU-funded HORIZON JU Research and Innovation Actions project, **Cynergy4MIE**. This document provides detailed information about the research to help you make an informed decision about your participation. Before deciding, it is important that you clearly understand the purpose of the research and what it would imply for you, including all the proceedings of the research and any potential risks and benefits it may entail. Please feel free to ask any questions you may have.
This information document may include terms or concepts that you do not fully understand. If this is the case, please ask the contact person or any other member of the team coordinating the activity to fully explain it or clarify pieces of information. At all times during the foreseen activities and afterwards, the Cynergy4MIE consortium assures compliance with relevant national and European legislation, including the General Data Protection Regulation (GDPR 2016/679).

Project and Research Ambitions

The vision of Cynergy4MIE (Leverage synergy by cyber-physical systems for the convergence of the eco systems mobility, infrastructure and energy in the circular economy for the Society 5.0) project is to revolutionise and optimise the industrial landscape in Europe by leveraging synergies in the foundational layers and cross functional technologies of Electronic Components and Systems (ECS). This aims to unify expertise from diverse domains, fostering synergies across key application areas for the future integration of domains and user-centric applications.

In this context, the project focuses on developing user-centric, inclusive, and socially accepted technologies for future mobility systems, including the safe and ethical integration of Advanced Driver Assistance Systems (ADAS) and Automated Driving Systems (ADS). This questionnaire aims to gather perceptions from both general users and expert stakeholders about user and societal acceptance factors and current societal perceptions regarding ADAS and ADS. This information sheet informs you about the details and implications of participating in the survey by completing the Cynergy4MIE questionnaire and giving feedback on user and societal acceptance of ADAS and ADS. The findings will contribute to ensuring the full exploitation potential of Cynergy4MIE's outcomes through increased user and societal acceptance.

Your Participation

Your participation in this survey, as described above, is highly valuable in achieving the objectives of the Cynergy4MIE project. Your participation is only possible in case you freely consent to participating, which is the legal basis for taking part in the activity and for collecting and processing the data you and other research participants will be kindly asked to provide.

Taking Part in This Research Project is Voluntary

You are free to withdraw your participation from this activity at any time without providing justification. No consequences will follow your withdrawal.
Any personal data of yours that might still be attributable to you will be immediately deleted by removing such data from the pool of to-be-analysed information.
Any relevant files and hard copies will be destroyed.

The Activity

Participants are provided with this information sheet and are asked to sign a consent form expressing their consent to participating and to sharing some personal data by taking part in this survey. If you consent, you will answer a set of questions regarding your experiences, expectations, and perceptions of ADAS and ADS technologies. The results will be compiled in a report (anonymously) and will be included in respective deliverables. Results of this survey will also assist towards ensuring that human-centric considerations are integrated across Cynergy4MIE system architecture, integration, validation, and standardisation efforts.

Data Collection and Processing

As mentioned above, this activity is carried out under the HORIZON JU Research and Innovation Actions project Cynergy4MIE which processes personal data for the purposes of identifying and analysing user and societal acceptance of ADAS and ADS. Again, data processing takes place amidst the above-mentioned activity. The only personal data collected will be that which you voluntarily provide via survey responses. Demographic information (e.g., age, gender identity, ethnic background, disability status) will be collected anonymously and used exclusively in aggregated or pseudonymised form. This data is critical for ensuring inclusivity and fairness in future automotive technologies, allowing the Cynergy4MIE consortium to identify differences in user acceptance, trust, accessibility barriers, and societal impacts across diverse groups. If you prefer not to select from predefined categories, you can use the open-text "prefer to self-identify" option provided in the questionnaire. This effort will be concluded well within the lifetime of Cynergy4MIE, which is running from 01 September 2024 until 31 August 2027.

The data collected by asking participants to provide comments and feedback is to be stored in a highly aggregated and pseudonymised form.

Again, we will not process any of your information if you do not give your consent; as explained in greater detail below, if you change your mind, you can withdraw your consent at any time during or after the activity by reaching out to the responsible research coordinator(s) and/or the Data Protection Officer (contact details are given at the end of this document).

We will only collect and process the minimum amount of information that is required to achieve the purpose of this research activity. We will apply appropriate security measures during all processing and storage of your data (see below). All data collection and processing take place in strict accordance with the EU General Data Protection Regulation 2016/679. You'll be able to exercise all of your rights as a research participant in accordance with the EU General Data Protection Regulation 2016/679, which we fully respect and comply with; these are also described in this sheet.

No automated decision-making or profiling in accordance with Articles 22(1) and (4) of the General Data Protection Regulation 2016/679 is going to take place.

We do not plan to share any personal data with anybody other than the research partners with a legitimate need to know basis (for an overview of the consortium, please consult the project website at https://cynergy4mie.eu) and utilised as explained above.

Will personal data be stored?

Access to the systems is limited to the research coordinator(s) (and their co-workers) in accordance with current security standards.

The data may be stored for the purpose of conducting a possible audit for five more years after the final payment. It will be deleted from all storage media as soon as possible, either in the immediate aftermath of an audit (when it would no longer be needed) or immediately after the end of the above-mentioned five-year period. No further processing will be conducted.

Who may access my information?

We will disclose your information if the European Commission, who is funding this research, requests information for auditing purposes or to evaluate our procedures.

Within the consortium partners, your information will only be accessible on a need-to-know basis.

Your key data protection rights

In accordance with principles of research ethics and the EU data protection framework, you have rights regarding how your personal data is processed. Here are your rights and how we can fulfil them:

- Right to access personal data processed about you, and the right for these data to be in a portable form – If you request access to personal data that we hold about you, we will provide you with these data in an easily accessible format.
- Right to rectify personal data held about you – If you think the personal data that we hold about you is inaccurate or incomplete, you can request us to correct or complete your personal data.
- Right to restrict the processing of your personal data – If you want to restrict the way we process your personal data, you can request that we do so.
- Right to request that your personal data is erased – If you want us to delete your personal data from our systems, you can request that we do so.
- Right to leave the research activity – If you wish to withdraw from participating in this survey, you can do so at any time without negative consequences and your personal data will not be processed.
- Right to be informed about the purpose of the data collection, the use of the data and storage of the provided data.
- Right to request that we transfer your personal data to another organisation.
- Right to complain to a supervisory authority – If you feel we have not adequately dealt with your requests, you can complain to the national data protection authority.
- Right to lodge a complaint to the research coordinator, project coordinator and/or the DPO (contact below).

Requests to exercise these rights will be handled without undue delay. If requests to exercise these rights are excessive, malicious, impossible to fulfil, or require a disproportionate effort, we may reject some requests in accordance with data protection legislation.

What risks will I face by taking part in this study? What will be done to protect me against such risks?

In principle, risk of breach of confidentiality in the handling of your personal data may lead to personal data breaches. Because this study collects information about you, one of the risks of this research is a loss of confidentiality.

Measures to protect against such risks:

- Voluntary participation
- Acknowledgement of the legal and ethical framework by partners
- Accountability and documentation
- Security of retention (appropriate security measures implemented in storing the data)

- Proper explanations of the policy context
- The presence (online or offline) of technical experts that can be consulted

Benefits of participation

Participation will not involve any financial compensation. However, you will contribute valuable insights towards shaping more user-centred and ethical future mobility technologies.

Confidentiality of the research

All data that will be collected and processed will be treated highly confidentially. As explained above, no sharing will take place other than with consortium members that have a need-to-know. Moreover, the data will be stored safely on servers to which only employees of the research partners have access. Appropriate security measures will be implemented to further ensure the confidentiality of data.

Contact Details

- Cynergy4MIE Project Coordination:
  - Katrin AL JEZANY (katrin.aljezany@avl.com)
  - Benjamin WIMMER (benjamin.wimmer@avl.com)
- Data Protection Officer (DPO) for this activity: Christina Vrotsou (christina.vrotsou@convergence.gr)
- Research coordinator for this activity: Panagiota Kokoliou (p.kokoliou@convergence.gr)

Consent Form

By ticking the consent box below, I confirm that I understand the following:

- I have read the information sheet explaining the project and understand how this research activity will collect and process my responses, and my personal data if I choose to provide it.
- I will be asked to provide professional or personal views and that the record of my involvement in the research will be kept confidential.
- I have the right to ask questions about my project participation and receive clear answers before making any decision.
- I may refuse to answer any questions I do not wish to discuss. I am free to end my participation at any time.
- My responses will be incorporated into an aggregated analysis and not kept on file or stored in the form of physical copies.
- If the information I provide is used for the writing of a piece of work to be delivered to the European Commission, or scientific research paper, my name and other

attributable data will be removed from that information so that my identity and experiences remain confidential (unless attribution is required, and I have consented to it).

- I have been made aware of my rights regarding my personal data and how to exercise them.
- Personal data received will be stored in separate files in a secure manner.
- My personal data will not be transferred to third parties.
- I have been given the contact details of the research team and I have been informed that I am free to contact:
    - Cynergy4MIE Project Coordination:
        - Katrin AL JEZANY (katrin.aljezany@avl.com)
        - Benjamin WIMMER (benjamin.wimmer@avl.com)
    - Data Protection Officer (DPO) for this activity: Christina Vrotsou (christina.vrotsou@convergence.gr)
    - Research coordinator for this activity: Panagiota Kokoliou (p.kokoliou@convergence.gr)
- My participation is voluntary. I have not been pressured or coerced in any way to take part in this research activity.
- I hereby consent to participate in the Cynergy4MIE project and to the processing of my personal data associated with this participation for the purposes and procedures as described herein.

Consent Form - Checklist

- By ticking the consent boxes below, I participate in these activities voluntarily. I understand that my participation will involve research of the Cynergy4MIE project.

I have read and understood the information sheet about this study.	☐
I have been informed of the following: • the reason for the study; • the subject matters to be discussed.	☐
I have asked for clarification when information was not clear, and my questions have been answered to my satisfaction. I'm aware that if I have any questions about this study after I sign the document, I can contact the project coordinator, the research coordinator and the DPO for this activity through the information provided.	☐
I consent to voluntarily participate in this study.	☐

I understand that I can refuse to answer questions and that I can withdraw from the survey at any time without having to give a reason.	☐
I understand that the information I provide will be used for the respective Cynergy4MIE research activity and that my personal data will be kept confidential.	☐
I give my consent to the processing of my personal data as described above.	☐
I have been given a copy of the information and consent forms.	☐

Thank you for participating in this survey. As explained in detail in the information sheet, this questionnaire is part of the Cynergy4MIE project and is focused on enhancing user and societal acceptance of mainly Advanced Driver Assistance Systems (ADAS), while also considering emerging Automated Driving Systems (ADS). The questionnaire aims to collect opinions, experiences, and perceptions regarding ADAS and ADS technologies particularly addressing aspects such as trust, transparency, ethics, inclusivity, standardisation, and user acceptance.

This questionnaire is open to everyone interested in or affected by ADAS and ADS technologies, including members of the Cynergy4MIE consortium, automotive industry stakeholders, researchers, policymakers, standardisation bodies, civil society organisations, and the general public/end-users/consumers.

Important note: Since ADS technologies are currently not widely available the general public is advised to answer ADS-related questions based on your expectations or expertise.

Section 1: ADAS and ADS understading and experience

Mini Glossary:

ADAS (Advanced Driver Assistance System): Vehicle-based systems that support the driver with tasks such as steering, braking or acceleration. The driver must always supervise and remain responsible for the driving task. Examples include Lane Keeping Assist (LKA), Adaptive Cruise Control (ACC), and Automatic Emergency Braking (AEB). (SAE J3016 Levels 0–2).

ADS (Automated Driving System): Systems capable of performing the full driving task, including fallback (responding to system failures), under specific conditions without the need for driver input or supervision. The driver may not be required to interevent or even be present. Examples: Traffic Jam Pilot, Highway Pilot (SAE J3016 Levels 3–5).

- **Level 0 (No Automation)**: The driver performs all tasks, and assistance is limited to warnings or momentary interventions.
- **Level 1 (Driver Assistance):** Partial Automation – System assists either steering or acceleration/deceleration tasks (e.g., ACC). The driver remains responsible for all other aspects of driving.
- **Level 2 (Partial Automation):** The system assists with both steering and acceleration/deceleration under specific conditions. Driver must continuously supervise the vehicle. (e.g, Lane Keeping Assist combined with Adaptive Cruise Control)
- **Level 3 (Conditional Automation):** System manages all driving tasks under specific conditions but requires the driver to intervene if this is requested by the system (e.g., Traffic Jam pilot).
- **Level 4 (High Automation):** System performs all driving tasks in specific conditions and will stop the vehicle if those conditions are not met, no driver needed (e.g., automated ride-sharing services in geo-fenced urban areas
- **Level 5 (Full Automation)**: System performs all driving tasks, no driver needed under any conditions.

Question 1. **Have you used any ADAS features in your vehicle?**

- Yes
- No
- Not sure

(If "Yes", display question Q2.)

Question 2. **Which ADAS features have you used? (Select all that apply)**

- Adaptive Cruise Control (ACC)
- Lane Keeping Assist (LKA)
- Automatic Emergency Braking (AEB)
- Blind Spot Monitoring
- Parking Assistance
- Traffic Sign Recognition (TSR)
- Driver Drowsiness/Attention Monitoring
- Rear Cross-Traffic Alert (RCTA)
- Forward Collision Warning (FCW)
- Lane Departure Warning (LDW)
- Other (please specify)

Question 3. **Have you experienced or used any Automated Driving Systems (ADS), capable of autonomous driving (***SAE Level 3–5: this means autonomous driving with limited or no human supervision***)?**

- Yes
- No
- Not sure

(If "Yes," display Q.4)

Question 4. **Briefly describe the context of your ADS experience. (open text)**

Section 2: Trust and Risk Perception

Introduction to the Section

We would like to understand your feelings of trust towards ADAS and ADS and how you perceive potential risks associated with their use.

Question 5. **How much do you trust ADAS features (e.g., lane keeping assist, emergency braking) to operate safely and reliably?**

- 1 — Not at all
- 2 — Slightly
- 3 — Moderately
- 4 — Very
- 5 — Completely

Question 6. **How concerned are you about the possibility of ADAS features malfunctioning during use (e.g., failing to detect obstacles)?**

- 1 — Not concerned
- 2 — Slightly concerned
- 3 — Moderately concerned
- 4 — Very concerned
- 5 — Extremely concerned

Question 7. **To what extent do you feel comfortable relying on ADAS in everyday driving situations (e.g., motorway driving, urban traffic)?**

- 1 — Not comfortable

- 2 — Slightly comfortable
- 3 — Moderately comfortable
- 4 — Very comfortable
- 5 — Extremely comfortable

Question 8. **How often do you feel the need to monitor or override the actions of an ADAS feature?**

- Never
- Rarely
- Sometimes
- Often
- Always

Question 9. **If you experience an unexpected action from an ADAS feature (e.g., sudden braking), how likely are you to reduce your future use of that system?**

- 1 — Not likely at all
- 2 — Slightly likely
- 3 — Moderately likely
- 4 — Very likely
- 5 — Extremely likely

Question 10. **How much would you trust future ADS (Levels 3–5) to safely operate without continuous supervision in specific scenarios (e.g., motorway driving, low-speed traffic jams)?**

- 1 — Not at all
- 2 — Slightly
- 3 — Moderately
- 4 — Very
- 5 — Completely

Question 11. **How concerned are you about relying entirely on ADS technologies (Levels 3–5) in real-world conditions?**

- 1 — Not concerned
- 2 — Slightly concerned
- 3 — Moderately concerned
- 4 — Very concerned
- 5 — Extremely concerned

Section 3: Perceived Usefulness and Ease of Use

Introduction to the Section

We would like to understand how useful and easy you find Advanced Driver Assistance Systems (ADAS) in your driving experience.

Question 12. **Using ADAS features improves my overall driving performance and safety.**

- 1 — Strongly disagree
- 2 — Disagree
- 3 — Neutral
- 4 — Agree
- 5 — Strongly agree

Question 13. **Official certification for safety and reliability by recognised authorities (e.g., ISO, UNECE, national transport agencies) significantly increases my willingness to adopt ADAS features.**

- 1 — Strongly disagree
- 2 — Disagree
- 3 — Neutral
- 4 — Agree
- 5 — Strongly agree

Question 14. **I have easy access to information and support (e.g., tutorials, user manuals, dealership assistance, training/demonstrators) for using ADAS features.**

- 1 — Strongly disagree
- 2 — Disagree
- 3 — Neutral
- 4 — Agree
- 5 — Strongly agree

Section 4: Cost Sensitivity and Willingness to Pay

Introduction to the Section

We would like to understand how cost considerations affect your willingness to adopt Advanced Driver Assistance Systems (ADAS).

Question 15. **How willing would you be to pay extra for a vehicle equipped with advanced ADAS features (e.g., adaptive cruise control, lane keeping assist)?**

- Not willing at all
- Slightly willing
- Moderately willing
- Very willing
- Extremely willing

Question 16. **Would financial incentives (e.g., insurance discounts, government rebates) increase your likelihood of adopting ADAS features?**

- Yes
- No
- Maybe

Section 5: Transparency and Understanding

Introduction to the Section

We would like to understand how important transparency and clear communication are to you when interacting with Advanced Driver Assistance Systems (ADAS).

Question 17. **I feel more confident using ADAS features when I clearly understand how and why the system makes decisions.**

- 1 — Strongly disagree
- 2 — Disagree
- 3 — Neutral
- 4 — Agree
- 5 — Strongly agree

Question 18. **In my opinion, ADAS features should provide real-time explanations (e.g., alerts, messages) about their actions while driving.**

- 1 — Strongly disagree
- 2 — Disagree
- 3 — Neutral
- 4 — Agree
- 5 — Strongly agree

Question 19. **I would trust an ADAS system more if it were certified to meet transparency and explainability standards (e.g., according to ISO/IEC or IEEE guidelines).**

- 1 — Strongly disagree
- 2 — Disagree
- 3 — Neutral
- 4 — Agree
- 5 — Strongly agree

Section 6: Automation Level Preferences

Introduction to the Section

We would like to understand your comfort level with different degrees of vehicle automation.

Question 20. **I prefer ADAS features that assist my driving while I remain fully in control (e.g., lane departure warning, blind spot monitoring).**

- 1 — Strongly disagree
- 2 — Disagree
- 3 — Neutral
- 4 — Agree
- 5 — Strongly agree

Question 21. **I feel comfortable using partially automated features that can control some aspects of driving (e.g., adaptive cruise control with lane keeping) under my supervision.**

- 1 — Strongly disagree
- 2 — Disagree
- 3 — Neutral
- 4 — Agree
- 5 — Strongly agree

Question 22. **If ADS (Levels 3–5) become widely available and certified for use, I would feel comfortable allowing the vehicle to drive itself under certain conditions (e.g., motorway pilot systems) without my constant supervision.**

- 1 — Strongly disagree
- 2 — Disagree
- 3 — Neutral

- 4 — Agree
- 5 — Strongly agree

Question 23. **Hypothetically, (or practically if you have the experience), how do you think your trust in ADS (Levels 3–5) would compare to current ADAS (Levels 1–2)?**

- I trust ADAS much more than ADS
- I somewhat trust ADAS more
- I trust both equally
- I somewhat trust ADS more
- I trust ADS mush more than ADAS

Question 24. **What would increase the acceptance of ADS technologies?**

- Certification by trusted authority (e.g., ISO, UNECE)
- Real-time explanations of ADS actions
- Manual override always available
- Ethical/bias audit of algorithms
- Simulated and real-world testing and validation
- Public consultation and transparency
- Other (please specify): ________

Section 7: Awareness and Attitudes Towards Standardisation

Mini Glossary: *(To assist with the following questions)*

- **ISO**: International Organisation for Standardisation – develops international standards to ensure quality, safety, and efficiency.
- **UNECE**: United Nations Economic Commission for Europe – develops vehicle safety regulations, including for automated driving systems.
- **IEEE**: Institute of Electrical and Electronics Engineers – develops standards for technology, including artificial intelligence and automation.

Introduction to the Section

We would like to understand your awareness and views on the role of international standards and certifications in enhancing the safety, privacy, and ethical operation of ADAS and ADS.

Question 25. **Before today, were you aware that international standards (e.g., ISO, IEEE, UNECE) exist for certifying the safety, reliability, and ethics of ADAS and ADS features?**

- Yes
- No
- Not sure

Question 26. **Knowing that an ADAS and ADS feature is certified by an international standard would increase my trust in using it.**

- 1 — Strongly disagree
- 2 — Disagree
- 3 — Neutral
- 4 — Agree
- 5 — Strongly agree

Question 27. **I believe that safety certification by international standards (e.g., ISO 21448, UNECE WP.29) is essential before using ADAS and ADS features.**

- 1 — Strongly disagree
- 2 — Disagree
- 3 — Neutral
- 4 — Agree
- 5 — Strongly agree

Question 28. **I would be concerned about using ADAS and ADS features that have not been certified for data privacy and ethical use (e.g., GDPR compliance, bias avoidance).**

- 1 — Strongly disagree
- 2 — Disagree
- 3 — Neutral
- 4 — Agree
- 5 — Strongly agree

Question 29. **In your opinion, which aspects should be prioritised in ADAS standardisation? (**Rank from 1 (most important) to 6 (least important))

- Safety and accident prevention

- Data privacy and cybersecurity
- Fairness and non-discrimination
- Environmental sustainability
- Usability and accessibility for all drivers
- Reliability and durability over time

Section 8: Ethical, Privacy, and Societal Concerns

Introduction to the Section

We would like to understand your views on ethical considerations, regarding data privacy, fairness, transparency, and the societal impacts associated with Advanced Driver Assistance Systems (ADAS) and Automated Driving Systems (ADS).

Question 30. **I am concerned about how ADAS and ADS features collect, store and use my personal driving data.**

- 1 — Strongly disagree
- 2 — Disagree
- 3 — Neutral
- 4 — Agree
- 5 — Strongly agree

Question 31. In your opinion/experience, do current ADAS and ADS systems equally accommodate all users, regardless of factors such as age, gender, ethnicity, or disability?

- 1 — Strongly disagree
- 2 — Disagree
- 3 — Neutral
- 4 — Agree
- 5 — Strongly agree

Question 32. **I believe that ADAS and ADS systems should undergo independent audits by external organisations (e.g., governmental agency, certified auditor) to ensure fairness and unbiased treatment of all users, regardless of factors such as age, gender, ethnicity, or disability.**

- 1 — Strongly disagree
- 2 — Disagree
- 3 — Neutral
- 4 — Agree

- 5 — Strongly agree

Question 33. **I would prefer to use ADAS and ADS systems that are designed to contribute to environmental sustainability (e.g., reducing fuel consumption, supporting eco-driving).**

- 1 — Strongly disagree
- 2 — Disagree
- 3 — Neutral
- 4 — Agree
- 5 — Strongly agree

Question 34. I believe clear ethical guidelines should be in place governing how ADAS and ADS systems handle critical driving decisions (e.g., in case of unavoidable accidents)

- 1 — Strongly disagree
- 2 — Disagree
- 3 — Neutral
- 4 — Agree
- 5 — Strongly agree

Question 35. There should be legal clarity regarding who is accountable if an ADAS and ADS system fails or causes an accident.

- 1 — Strongly disagree
- 2 — Disagree
- 3 — Neutral
- 4 — Agree
- 5 — Strongly agree

Section 9: Standardisation, Gaps and Societal/User Acceptance

Introduction to the Section

In this section we seek your insights on current standardisation frameworks and existing gaps related to societal and user acceptance of ADAS and ADS technologies.

Question 36. **Which of the following standards or regulations related to ADAS and ADS does your organisation currently use, implement, or comply with? (**Select all that apply**)"**

- **ISO 26262** (Functional Safety for automotive systems)
- **ISO 21448 (2022)** (Safety of the Intended Functionality – SOTIF)
- **ISO/SAE 21434** (Cybersecurity Engineering for vehicles)
- **UNECE WP.29 Regulations** (e.g., R155 Cybersecurity, R156 Software updates, R157 ALKS)
- **EU General Safety Regulation 2019/2144** (Mandatory ADAS features regulation)
- **ISO 39003 (2023)** (Ethical considerations for automated/autonomous vehicles)
- **IEEE 7000-series** (Ethically Aligned Design series)
- **IEEE 2846-2022** (Safety-related assumptions for ADS)
- **IEEE P2040** (General requirements for fully automated vehicles)
- **IEEE P3474:2024** (Human intentions & AI alignment in autonomous driving)
- **Other (**please specify**): ___________**
- **None**

Question 37. **Which standardisation organisations or initiatives related to ADAS and ADS standardisation are you or your organisation involved in? (**Select all that apply**)"**

- ISO
- IEEE
- SAE International
- UNECE WP.29 Working Groups
- CEN/CENELEC
- Other (please specify): ___________
- None

Question 38. **Current standards sufficiently cover my technical area of contribution.**

- 1 — Strongly disagree
- 2 — Disagree
- 3 — Neutral
- 4 — Agree
- 5 — Strongly agree

Question 39. **Key technology domains lack relevant standards.**

- 1 — Strongly disagree
- 2 — Disagree
- 3 — Neutral
- 4 — Agree

- 5 — Strongly agree

Question 40. **Current standards adequately address ethical AI use, sustainability, and environmental concerns.**

- 1 — Strongly disagree
- 2 — Disagree
- 3 — Neutral
- 4 — Agree
- 5 — Strongly agree

Question 41. **Standardisation efforts sufficiently consider inclusivity, accessibility, and public trust.**

- 1 — Strongly disagree
- 2 — Disagree
- 3 — Neutral
- 4 — Agree
- 5 — Strongly agree

Question 42. **Legal and regulatory frameworks are sufficiently mature for deployment.**

- 1 — Strongly disagree
- 2 — Disagree
- 3 — Neutral
- 4 — Agree
- 5 — Strongly agree

Question 43. **Rate the severity of the following identified gaps for societal acceptance of ADAS and ADS** *(1 = Not severe at all, 5 = Extremely severe).*

Gap	**1**	**2**	**3**	**4**	**5**
Lack of transparency and explainability for end-users	○	○	○	○	○
Insufficient human-machine interface (HMI) standards for user understanding and control handover	○	○	○	○	○
Lack of validation for user trust/driver confidence	○	○	○	○	○
Algorithmic bias considerations and absence of inclusivity requirements	○	○	○	○	○
Lack of ethical decision-making and accountability frameworks for automated driving scenarios	○	○	○	○	○

Inadequate privacy protection and data transparency in ADAS/ADS Artificial Intelligence (AI)/ Machine Learning (ML) reliability and trustworthiness	○ ○ ○ ○ ○

Question 44. **In your view, which societal acceptance themes are least addressed by current standards?** *(Rate the following accordingly: 1 = Not addressed at all, 5 = Sufficiently addressed)*

- Trust and confidence
- Transparency and explainability
- Inclusivity and fairness
- Safety perception (as opposed to technical safety)
- Human-in-the-loop collaboration
- Privacy and data security

Question 45. **Please indicate your level of agreement with each of the following proposed measures to enhance societal and user acceptance of ADAS and ADS.** (1 = Strongly disagree, 5 = Strongly agree). *(Note: Some measures may be more applicable to ADS (Levels 3–5), but your perspective on their importance for future ADAS developments is also valuable.)*

Proposed Measure	**1 2 3 4 5**
Ethical design assurance required for approval (primarily relevant for ADS levels 3–5)	○ ○ ○ ○ ○
Mandatory transparency features (e.g., status displays, intervention explainability)	○ ○ ○ ○ ○
Human-in-the-loop usability testing with non-expert drivers	○ ○ ○ ○ ○
Inclusivity and bias testing for perception and interfaces	○ ○ ○ ○ ○
Post-market monitoring of trust indicators and societal feedback	○ ○ ○ ○ ○
Alignment with AI Act requirements for automotive AI systems	○ ○ ○ ○ ○

Section 11: Open Feedback

Question 46. Are there any additional societal or ethical issues or gaps related to ADAS/ADS systems that this questionnaire has not addressed? If yes, please describe:(Open text field)

Question 47. Do you have any recommendations for additional standardisation measures or improvements that should be considered for ADAS/ADS systems? (Open text field)

Question 48. Do you have any other remarks, suggestions, or priorities regarding societal and user acceptance, ethical considerations, or standardisation needs for ADAS/ADS that you would like to share? (Open text field)

Section 11: Demographic information

Introduction to the Section

This questionnaire aims to understand and analyse the societal and user acceptance aspects and inclusivity of ADAS/ADS systems. As described in detail in the information sheet, demographic information (e.g., age, gender identity, ethnicity, disability) is collected anonymously and in aggregated form solely to ensure inclusivity and to identify differences in user and societal acceptance of ADAS/ADS. All responses will remain anonymous and confidential. These demographic insights are critical towards making recommendations that ensure respective future technologies and advancements are fair, inclusive, and beneficial for all societal groups.

Question 49. **Sector:**

- Research Institute
- University / Academic Institution
- Large Enterprise (OEM, industry partner)
- SME (Technology provider, system integrator)
- Policy maker / Regulatory Authority
- Standardisation Body or Organisation
- Civil Society / NGO/ NPO
- End-user / Consumer
- Other: _____________

For Cynergy4MIE consortium partners only: **Organisation Name:** _______________(drop down list)

1. AVL
2. BELGAN
3. BUT
4. CONV
5. DRIVEU
6. EDI
7. FAU
8. Fraunhofer
9. GIM
10. GRO
11. I&M
12. IFAT

13. IMA
14. INSAR
15. IOTAM
16. ITRI
17. KFU
18. KTH
19. MEDISYS
20. MEV
21. MURATA
22. NXP-NL
23. POLITO
24. PRODRIVE
25. RECHI
26. SAL
27. SAT
28. SSOL
29. ST-I
30. STRIKERSOFT
31. TAAT
32. TG
33. THRO
34. TU/e
35. TUD
36. TUG
37. UNEV
38. VAISTO
39. VER
40. VIF
41. VTT
42. XENOMATIX
43. ZF
44. FUTURE

Question 50. **What is your age group?**

- 18–24
- 25–34
- 35–44
- 45–54
- 55–64

- 65+

Question 51. **What is your gender identity?**

- Man
- Woman
- Non-binary
- Prefer to self-describe...................
-

Question 52. **. In which region do you primarily operate in?**

- EU Member State
- Non-EU European Country
- North America
- South America
- Africa
- Asia
- Oceania
- Other (please specify)

Question 53. Ethic Background (Select all that apply)

- White (e.g., European, North American, Australasian)
- Black (e.g., African, Caribbean, European, North American)
- Asian (e.g., East Asian, South Asian, Southeast Asian)
- Middle Eastern / North African
- Hispanic / Latino/a/x
- Mixed / multiple ethnicities
- Prefer to self-describe: ___________

Question 54. **Do you identify as a person with a disability?**

- Yes
- No
- Prefer to self-describe: ___________

***Follow-up (if 'Yes')*:**

Question 55. **Please specify the nature of your disability:** (Select all that apply)

- Physical

- Sensory
- Cognitive
- Mental health
- Prefer to self-describe: __________

Question 56. **Highest level of education completed.**

- No formal education
- Primary education
- Secondary education
- Vocational / Technical training
- University degree (Bachelor’s)
- Postgraduate degree (Master’s, PhD)
- Other (please specify): __________

Question 57. **How many years of driving experience do you have?**

- Less than 1 year
- 1–5 years
- 6–10 years
- 11–20 years
- More than 20 years

B. Full Survey Questionnaire - Cynergy4MIE Standardisation Analysis of Gap

SC1: Automated Machinery and Transportation

Objective: Gather structured input from all partners contributing to SC1, to support Cynergy4MIE's standardisation mapping, gap identification, and pre-standardisation planning.
To be completed by: All technical and industrial partners to SC1

3.1 Description of the SC and its Scope in Cynergy4MIE

1. Please briefly describe the scope and role of SC1 in Cynergy4MIE.
   (Focus on automated machinery, industrial automation, transportation systems.)

Open text field (200–300 words)

2. What are the main technological domains and use cases your SC1 activities target?

Open text field (200–300 words)

3. Are there specific demonstrators, WP interdependencies, or applications that define your SC?

Open text field (200–300 words)

3.2 Existing Relevant Standards and Regulations

4. Which of the following standards or regulations are directly relevant, referenced, or applied within your SC1 work?
   (Please select and explain their relevance)

☐ ISO 26262 – Functional safety
☐ ISO 13849 – Machinery control systems safety
☐ IEC 61508 – Functional safety of E/E/PE systems
☐ IEC 62061 – Safety of machinery
☐ IEC 60204-1 – Electrical safety in machinery
☐ ISO/PAS 8800 – Road vehicle safety and AI
☐ ISO 13400-2 – DoIP diagnostics
☐ IEEE 2846 – Safety-related assumptions for ADS
☐ 5GAA / AUTOSAR / ASAM frameworks
☐ CSA EXP150.x – Infrastructure and CAV standards
☐ Other: ___________

5. For each selected standard, please briefly indicate:

- How it is used (inspiration, compliance, implementation)
- Whether any testing, validation, or certification is planned

3.3 Technical WP Contributions and Compliance Pathways

6. Are there mechanisms in place for ensuring standard compliance (e.g., testing protocols, checklists, simulation benchmarks)?

4. Gap Analysis

7. Which of the following gaps apply to SC1 domain?
   ☐ No relevant standards exist
   ☐ Standards exist but are outdated
   ☐ Existing standards are not applicable
   ☐ Standards lack coverage of key technology needs

8. Describe the most critical gaps.
   (Examples may include: AI-enabled industrial systems, real-time edge decision loops, adaptive control logic under uncertainty.)

9. What are the key risks or challenges resulting from these standardisation gaps? How is the project currently addressing them?

5. Cynergy4MIE's Value Add to the Standardisation Landscape

10. In your view, what is Cynergy4MIE's potential contribution to the standardisation landscape in this domain?

(e.g., new reference architectures, verification methods, compliance toolchains, open datasets)

10. Are there concrete plans or opportunities for:

- Contributing to ISO / IEEE / CEN / CENELEC working groups?
- Publishing technical white papers or gap-bridging proposals?

11. If you could propose one or two new standardisation directions, what would they be?

SC2: Smart Collaborative Robotics

Objective: Gather structured input from all partners contributing to SC2, to support Cynergy4MIE's standardisation mapping, gap identification, and pre-standardisation planning.
To be completed by: All technical and industrial partners to SC2

3.1 Description of the SC and its Scope in Cynergy4MIE

1. Please briefly describe the scope and role of SC2 in Cynergy4MIE.
   (Focus on collaborative robotics, human–robot interaction, shared workspaces, adaptive robotic control.)
   Open text field (200–300 words)

2. What are the main technological domains and use cases your SC2 activities target?
   (e.g., manufacturing cobots, logistics robotics, robotic perception systems, mobile manipulators)
   Open text field (200–300 words)

3. Are there specific demonstrators, WP interdependencies, or applications that define your SC?
   (e.g., industrial safety use cases, real-time coordination with humans, multi-robot collaboration)
   Open text field (200–300 words)

3.2 Existing Relevant Standards and Regulations

4. Which of the following standards or regulations are directly relevant, referenced, or applied within your SC2 work?
   (Please select and briefly explain their relevance)

☐ ISO/TS 15066 – Collaborative robot safety
☐ ISO 10218-1 – Safety requirements for robot manufacturers
☐ ISO 10218-2 – Safety requirements for robot systems and integration
☐ ISO 13482 – Personal care/service robot safety
☐ ISO/TR 20218-1 – Safety design for robot end-effectors
☐ ISO/TR 20218-2 – Safety for manual load/unload stations
☐ ISO 18646-1 – Performance criteria for wheeled service robots
☐ ISO 8373 – Robotics terminology
☐ IEC 60601-2-77 – Surgical robot safety
☐ ANSI/RIA R15.06 – Industrial robot safety (US version of ISO 10218)
☐ Other: ___________

5. For each selected standard, please briefly indicate:

- How it is used (inspiration, compliance, implementation)
- Whether any testing, validation, or certification is planned

3.3 Technical WP Contributions and Compliance Pathways

6. Are there mechanisms in place for ensuring standard compliance?
   (e.g., safety envelope simulation, compliance-by-design methods, physical

prototyping validation)
Open text field

3.4 Gap Analysis

7. Which of the following gaps apply to SC2 domain?
   ☐ No relevant standards exist
   ☐ Standards exist but are outdated
   ☐ Existing standards are not applicable
   ☐ Standards lack coverage of key technology needs

8. Describe the most critical gaps.
   (Examples may include: dynamic workspace safety, cognitive robotics interfaces, soft robotics compliance, AI–robot fusion safety)
   Open text field

9. What are the key risks or challenges resulting from these standardisation gaps? How is the project currently addressing them?
   Open text field

3.5 Cynergy4MIE's Value Add to the Standardisation Landscape

10. In your view, what is Cynergy4MIE's potential contribution to the standardisation landscape in this domain?
    (e.g., human-in-the-loop safety frameworks, testbeds for dynamic HRI, ethics-aware collaborative systems)

Open text field

11. Are there concrete plans or opportunities for:
    • Contributing to ISO / IEEE / CEN / CENELEC working groups?
    • Publishing technical white papers or gap-bridging proposals?
    Yes/No + brief explanation

12. If you could propose one or two new standardisation directions, what would they be?
    Open text field

SC2

Objective: Gather structured input from all partners contributing to SC3, to support Cynergy4MIE's standardisation mapping, gap identification, and pre-standardisation planning.
To be completed by: All technical and industrial partners to SC3

3.1 Description of the SC and its Scope in Cynergy4MIE

1. Please briefly describe the scope and role of SC3 within Cynergy4MIE.
   (Focus on electric or hybrid powertrains, propulsion systems, drivetrain architectures, and energy efficiency.)
   Open text field (200–300 words)

2. What are the main technological domains and use cases your SC3 activities target?
   (e.g., electric motor control, power electronics, battery integration, energy recovery systems)
   Open text field (200–300 words)

3. Are there specific demonstrators, WP interdependencies, or applications that define your SC?
   (e.g., testbeds for electrified propulsion, multi-energy systems, eAxle simulations, energy harvesting subsystems)
   Open text field (200–300 words)

3.2 Existing Relevant Standards and Regulations

4. Which of the following standards or regulations are directly relevant, referenced, or applied within your SC3 work?
   (Please select and briefly explain their relevance)

☐ ISO 6469-1 to -4 – Electrically propelled road vehicles safety
☐ ISO 26262 – Functional safety for powertrain E/E systems
☐ ISO 21498 – Electrified powertrain architecture
☐ ISO 23273 – Hydrogen vehicle safety
☐ ISO 15118 – Vehicle-to-grid (V2G) communication interface
☐ ISO 21782 – Electric propulsion system efficiency measurement
☐ ISO 12405 – Lithium-ion battery system testing
☐ IEC 61851 – EV conductive charging systems
☐ SAE J1772 / CCS standards – Charging infrastructure interoperability
☐ IEEE 2030.1.1 – Interconnection of electric vehicles
☐ Other: ___________

5. For each selected standard, please briefly indicate:

- How it is used (inspiration, compliance, implementation)
- Whether any testing, validation, or certification is planned

3.3 Technical WP Contributions and Compliance Pathways

6. Are there mechanisms in place for ensuring standard compliance?
   (e.g., testing protocols, thermal management benchmarking, model-based design verification, regulatory audits)
   Open text field

3.4 Gap Analysis

7. Which of the following gaps apply to SC3 domain?
   ☐ No relevant standards exist
   ☐ Standards exist but are outdated
   ☐ Existing standards are not applicable
   ☐ Standards lack coverage of key technology needs
8. Describe the most critical gaps.

   Open text field
9. What are the key risks or challenges resulting from these standardisation gaps? How is the project currently addressing them?
   Open text field

3.5 Cynergy4MIE's Value Add to the Standardisation Landscape

10. In your view, what is Cynergy4MIE's potential contribution to the standardisation landscape in this domain?
    (e.g., system-level modelling approaches, harmonised control interfaces, energy-aware validation methods)
    Open text field
11. Are there concrete plans or opportunities for:
    • Contributing to ISO / IEEE / CEN / CENELEC working groups?
    • Publishing technical white papers or gap-bridging proposals?
    Yes/No + brief explanation
12. If you could propose one or two new standardisation directions, what would they be?
    Open text field

SC4

Objective: Gather structured input from all partners contributing to SC4, to support Cynergy4MIE's standardisation mapping, gap identification, and pre-standardisation planning.
To be completed by: All technical and industrial partners to SC4

3.1 Description of the SC and its Scope in Cynergy4MIE

4. Please briefly describe the scope and role of SC4 within Cynergy4MIE.
   (Focus on automated driving capabilities, sensor-based perception, decision-making logic, and safety-critical functions.)
   Open text field (200–300 words)

5. What are the main technological domains and use cases your SC4 activities target?
   (e.g., mixed traffic simulation, critical scenario detection, V2X-supported manoeuvring, automated road condition mapping)
   Open text field (200–300 words)

6. Are there specific demonstrators, WP interdependencies, or applications that define your SC?
   (e.g., Demo 4.1–4.3, WP1-WP5 interlinkages, V2X integration, road friction mapping, user acceptance surveys)
   Open text field (200–300 words)

3.2 Existing Relevant Standards and Regulations

5. Which of the following standards or regulations are directly relevant, referenced, or applied within your SC4 work?
   (Please select and briefly explain their relevance)

☐ ISO 26262 – Functional safety
☐ ISO 21448 – Safety of the Intended Functionality (SOTIF)
☐ ISO/TS 5083 – Scenario-based safety evaluation
☐ ISO/SAE 21434 – Cybersecurity engineering
☐ ISO 23150 – Sensor–fusion data interfaces
☐ IEEE 2846 – Assumptions for ADS behaviour
☐ IEEE 802.11p – V2X communications
☐ SAE J3016 – Driving automation taxonomy
☐ SAE J2945/1 – DSRC minimum performance
☐ NIST IR 8527 – AV standards and metrics
☐ UNECE WP.29 Regulations (e.g., R157 ALKS)
☐ Other: ___________

6. For each selected standard, please briefly indicate:

- How it is used (inspiration, compliance, implementation)
- Whether any testing, validation, or certification is planned

3.3 Technical WP Contributions and Compliance Pathways

7. Are there mechanisms in place for ensuring standard compliance?
   (e.g., testing protocols, thermal management benchmarking, model-based design verification, regulatory audits)
   Open text field

3.4 Gap Analysis

10. Which of the following gaps apply to SC4 domain?
    ☐ No relevant standards exist
    ☐ Standards exist but are outdated
    ☐ Existing standards are not applicable
    ☐ Standards lack coverage of key technology needs
11. Describe the most critical gaps.
    (Examples may include ethical decision-making in AVs, human–machine interface transparency, multi-modal sensor synchronisation, edge learning in real-time ADS)
    Open text field
12. What are the key risks or challenges resulting from these standardisation gaps? How is the project currently addressing them?
    Open text field

3.5 Cynergy4MIE's Value Add to the Standardisation Landscape

13. In your view, what is Cynergy4MIE's potential contribution to the standardisation landscape in this domain?
    (e.g., data-driven scenario libraries, real-time decision transparency tools, cross-OEM simulation frameworks, trust metrics for AVs)
    Open text field
14. Are there concrete plans or opportunities for:
    • Contributing to ISO / IEEE / CEN / CENELEC / UNECE working groups?
    • Publishing technical white papers or gap-bridging proposals?
    Yes/No + brief explanation
15. If you could propose one or two new standardisation directions, what would they be?
    Open text field

SC5 - Multi-Agent Sensing & Control

Objective: Gather structured input from all partners contributing to SC5 to support standardisation mapping, gap analysis, and potential pre-standardisation contributions.
To be completed by: All technical, system and industrial partners working on multi-agent sensing, control, distributed coordination.

Objective: Gather structured input from all partners contributing to SC4, to support Cynergy4MIE's standardisation mapping, gap identification, and pre-standardisation planning.
To be completed by: All technical and industrial partners to SC4

3.1 Description of the SC and its Scope in Cynergy4MIE

7. Please briefly describe the scope and role of SC5 within Cynergy4MIE.
   (Focus on multi-agent sensor networks, distributed control, collaborative autonomy.)
   Open text field (200–300 words)

8. What are the main technological domains and use cases your SC5 activities target?
   (e.g., distributed warehouse fleets, industrial sensor swarms, UAV coordination, digital twins)
   Open text field (200–300 words)

9. Are there specific demonstrators, WP interdependencies, or applications that define your SC?
   (e.g., Plug-and-produce scenarios, collaborative safety agents, edge–cloud coordination)
   Open text field (200–300 words)

3.2 Existing Relevant Standards and Regulations

6. Which of the following standards or regulations are directly relevant, referenced, or applied within your SC5 work?
   (Please select and briefly explain their relevance)

☐ ISO/IEC 29182-1 – SNRA overview & requirements
☐ ISO/IEC 29182-5 – Sensor network interface definitions
☐ IEC 62443-4-1 – Secure product development lifecycle
☐ IEEE 1872.2 – Autonomous robotics ontology
☐ IEEE P7001 – Transparency of autonomous systems
☐ SAE AS5669A – JAUS transport services
☐ SAE AS5710A – JAUS core service coordination
☐ ISO/IEC/IEEE 12207 – Software lifecycle processes
☐ ISO/IEC 25010 – Software/system quality model

☐ IEEE/IEC 62270 – Control system automation guide

☐ Other: __________

7. For each selected standard, please briefly indicate:

- How it is used (inspiration, compliance, implementation)
- Whether any testing, validation, or certification is planned

3.3 Technical WP Contributions and Compliance Pathways

8. Are there mechanisms in place for ensuring standard compliance?
   (e.g., ontology validation, secure development pipelines, system testing frameworks)
   Open text field

3.4 Gap Analysis

13. Which of the following gaps apply to SC5 domain?
    ☐ No relevant standards exist
    ☐ Standards exist but are outdated
    ☐ Existing standards are not applicable
    ☐ Standards lack coverage of key multi-agent/sensing/control needs

14. Describe the most critical gaps.
    (e.g., emergent behaviour safety, dynamic coalition formation, real-time low-latency consensus, semantic interoperability)
    Open text field

15. What are the key risks or challenges resulting from these standardisation gaps? How is the project currently addressing them?
    Open text field

3.5 Cynergy4MIE's Value Add to the Standardisation Landscape

16. In your view, what is Cynergy4MIE's potential contribution to the standardisation landscape in this domain?
    (e.g., safety-aware multi-agent coordination methods, shared ontology frameworks, metrics for emergent behaviour testing)
    Open text field

17. Are there concrete plans or opportunities for:
    •Contribute to ISO / IEEE / CEN / CENELEC / IEC working groups?
    • Publishing technical white papers or gap-bridging proposals?
    Yes/No + brief explanation

18. If you could propose one or two new standardisation directions, what would they be?
    Open text field

SC6: ECS for Energy Efficiency & Distributed Intelligent Control

Objective: Collect input from SC6 partners to inform standardisation mapping, gap analysis, and pre-standardisation planning.
To be completed by: All technical and industrial contributors to SC6

3.1 Description of the SC and its Scope in Cynergy4MIE

10. Please briefly describe the scope and role of SC6 within Cynergy4MIE.
    (Focus on energy-efficient building/plant control, distributed intelligent EMS, ecosystem-level energy optimization.)
    Open text field (200–300 words)

11. What are the main technological domains and use cases your SC6 activities target?
    (e.g., distributed HVAC control, prosumer microgrids, predictive load management, BACS orchestration)
    Open text field (200–300 words)

12. Are there specific demonstrators, WP interdependencies, or applications that define your SC?
    (e.g., smart campus EMS, demand-response pilots, digital twin building ecosystems)
    Open text field (200–300 words)

3.2 Existing Relevant Standards and Regulations

7. Which of the following standards or regulations are directly relevant, referenced, or applied within your SC6 work?
   (Please select and briefly explain their relevance)

☐ ISO 50001 – Energy management systems
☐ ISO 50006 – Energy performance indicators
☐ ISO 52120-1 – Building energy characteristics and data
☐ ISO 17800 – Facility Smart Grid Information Model
☐ IEC 61850-7-420 – DER/DA logical nodes
☐ IEC 62443-4-1 – Security development lifecycle for control systems
☐ IEC/IEEE 62270-1 – Guide for computer-based automation control

☐ EN 50090-1 – Home & Building Electronic System architecture
☐ ANSI/ASHRAE/IES 90.1 – Building energy efficiency
☐ Other: __________

8. For each selected standard, please briefly indicate:

- How it is used (inspiration, compliance, implementation)
- Whether any testing, validation, or certification is planned

3.3 Technical WP Contributions and Compliance Pathways

9. Are there mechanisms in place for ensuring standard compliance?
   (e.g., energy performance monitoring, cybersecurity risk assessments, digital twin validation)
   Open text field

3.4 Gap Analysis

16. Which of the following gaps apply to SC5 domain?
    ☐ No relevant standards exist
    ☐ Standards exist but are outdated
    ☐ Standards don't apply to emerging EMS architectures
    ☐ Standards lack coverage of distributed energy intelligence use cases
17. Describe the most critical gaps.
    (e.g., real-time predictive load balancing, cybersecurity in edge EMS, prosumer orchestration protocols)
    Open text field
18. What are the key risks or challenges resulting from these standardisation gaps? How is the project currently addressing them?
    Open text field

3.5 Cynergy4MIE's Value Add to the Standardisation Landscape

19. In your view, what is Cynergy4MIE's potential contribution to the standardisation landscape in this domain?
    (e.g., safety-aware multi-agent coordination methods, shared ontology frameworks, metrics for emergent behaviour testing)
    Open text field

20. Are there concrete plans or opportunities for:
    - Participation in ISO / IEC / CEN / IEEE working groups?
    - Publishing technical white papers or gap-bridging proposals?

    Yes/No + brief explanation
21. If you could propose one or two new standardisation directions, what would they be?

    Open text field