

Secure and Intelligent Autonomy for Agricultural Tractors: An Integrated Framework Combining Swarm Robotics, Telematics, and AI-Based Navigation

Domagoj Zimmer ^{1,*}, Mladen Jurišić ¹, Luka Šumanovac ¹, Anamarija Banaj ¹, Edita Štefanić ² and Pavo Lucić ¹

¹ Department for Agricultural Engineering and Renewable Energy Sources, Faculty of Agrobiotechnical Sciences Osijek, Josip Juraj Strossmayer University of Osijek, 31000 Osijek, Croatia; mjurisic@fazos.hr (M.J.); lsumanov@fazos.hr (L.Š.); abanaj@fazos.hr (A.B.); plucic@fazos.hr (P.L.)

² Department of Plant Medicine, Faculty of Agrobiotechnical Sciences Osijek, Josip Juraj Strossmayer University of Osijek, 31000 Osijek, Croatia; estefanic@fazos.hr

* Correspondence: dzimmer@fazos.hr

Abstract

The next generation of agriculture mechanisation lies in the integration of autonomy, connectivity, and intelligence. This systematic review presents a conceptual, integrated engineering framework for safe and intelligent autonomy in agriculture tractors based on a systematic survey that covers major technical advances between January 2020 and May 2026, including research trends, key authors, conceptual clusters, etc. mapped by AI-assisted tools like Bibliometrix, Litmaps, and Elicit. We have a particular focus on the integration among three key research domains related to swarm robotics, secure telematics, and navigation through artificial intelligence. Important technical trends were identified, including but not limited to decentralised consensus algorithms for multi-vehicle coordination, lightweight telemetry secure protocols (CoAp/Oscore, DTLS), neural networks, and a fuzzy logic hybrid approach that adapts complex data to unstructured field constraints. Through the research reviewed, it was found that safety, decision-making, and collaboration are not designed and evaluated together as part of the overall proposed structure, which inhibits future expandability and safety. Based on current research in both areas and its shortcomings, an integrated concept was created that combines elements of decision-making, in-field telemetry, and safe decision-making from farm to cloud using security as the binding approach. At the end of the paper, three practical engineering guidelines are presented.

Keywords: autonomous agriculture; swarm robotics; secure telematics; AI navigation; functional safety; integrated framework

Academic Editor: Michele Raffaelli

Received: 29 April 2026

Revised: 22 June 2026

Accepted: 29 June 2026

Published: 1 July 2026

Copyright: © 2026 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the [Creative Commons Attribution \(CC BY\)](https://creativecommons.org/licenses/by/4.0/) license.

1. Introduction

Agriculture needs a greater amount of healthy sustenance in a reasonable and safe manner, with less labour, lower risk, and equivalent environmental aims. Technologies developed to improve autonomous cultivating such as unmanned vehicles traversing in tandem across fields or teams of tractors performing field work together have become a research focal point, moving into more accurate agricultural practices. Large-scale employment of autonomous farming in the farming industry would necessitate three separate areas to be developed and integrated so that automation can be executed without harm:

swarm robotics enabling remote/decentralised control of multiple unmanned vehicles across the region, safe telematics ready to confirm the accuracy of messages across low bandwidth with inconsistent wireless connections, and AI-assisted navigation controllers for farming vehicles over difficult/uneven terrain or in rain. While plenty of research has been carried out regarding engineering robotics, cybersecurity, and agriculture, there is only a small quantity of cross-discipline work, and only a few developments integrate security with wisdom and swarm actions as design metrics, rather than individually.

Swarm robotics enables multi-robot decentralized control with distributed control architecture and avoids single points of failure in systems. Recently, potential swarm-based control protocols locally informed with topology switching have been reported for collision-free enclosures or a large tree canopy (e.g., for in situ monitoring with swarms of agricultural robots), using only distance sensing and communication. No consideration for topological graph structures has been shown in any the studies performed [1].

Through experiments with a coordinated robot group operating with only local measurements, Hu et al. [2] demonstrated adaptive formation coordination algorithms capable of tracking dynamic targets exhibiting nonlinear dynamics in the presence of exogenous disturbances, providing proof of principle about practical feasibility in agriculture applications [2].

Using a sample-efficient guided policy search method, has resulted in decentralised policies that rendezvous with a greatly reduced number of training samples, using an alternating process between distributed trajectory optimisations and policy learnings [3]. Several multi-agent path planning approaches have been proposed for agricultural fields to guide swarms within a structured tree-planting environment based upon specific planning constraints [4]. However, multi-tractor transition and coordination remain to be explored completely, including communication integrity and robotic intelligence guidance.

Secure telematics systems rely on small, lightweight cryptography algorithms that provide message integrity, confidentiality, and authenticity with limited computational, storage, and energy budgets found on small, embedded, internet-of-things (IoT) devices. EDHOC and OSCORE protocols result in smaller messages compared to DTLS. More specifically, EDHOC results in a reduction factor of about five in message size compared to DTLS 1.3 with PSK, while preserving security authentication properties and enabling a range of group communication scenarios [5]. Similarly, experiments on constrained devices have demonstrated that OSCORE provides end-to-end CoAP security with similar or better per-message overhead, memory usage, round-trip time, and energy efficiency than TinyDTLS, while still providing stronger end-to-end guarantees, without performance degradation [6]. The literature contains multiple detailed evaluations of OSCORE and EDHOC implementations on microcontrollers quantifying RAM consumption, flash memory occupation, execution speed, and energy consumption, concluding that the use of telematics devices in agriculture is feasible [7]. Moreover, a large-scale experiment of OSCORE on a dedicated testbed shows that OSCORE offers improved performance over CoAP + DTLS in radio environments with bad radio links by avoiding establishment of session, making it suitable for problematic radio environments common in agricultural IoT deployments [8]. The group version of OSCORE was evaluated for secure group communication, demonstrating suitability to secure communications among multiple robots working together for crop harvesting and weed detection tasks [9]. However, lightweight security protocols should be integrated with real-time control loops and coordination algorithms of robot swarms, which poses challenges in agriculture.

AI-based autonomous navigation systems are increasingly able to conquer unpaved, unstructured, and dynamically changing farm environments, where assumptions of geometric path planning usually break. Two main parts of a deep-reinforcement learning agent are trained separately to manage global and local navigation, and the trained local

policy helps avoid the “stuck tendency” of reactive navigating [10]. The unified agent is then used for real-time exploration and mapping in unknown farm environments. Combining advanced A* global path planners with fuzzy Dynamic Window Approach methods is a means for local replanning at a lower rate. In regular DWA-based navigation, turning around 400 times leads to greater average heading error than 25–45 degrees and higher final deviation from the goal route; improvements were made to reduce heading errors to less than 10 degrees [11]. An adaptive neuro-fuzzy inference system (ANFIS) is used to combine goal-guidance controllers and obstacle-avoidance controllers, enabling dynamic collision-free autonomous robot navigation with greater fluidity than standard reactive controllers and lessened computational needs [12]. Domain-specific methods for agriculture, which inject real-time classification results into the navigation cost maps, help navigation by enabling robots to safely ignore green vegetation around them, approaching tasks that an indoor navigation stack would shun, thus increasing the convenience of real field navigation [13]. A position-agnostic approach is proposed based on reinforcement learning and deep learning for autonomous navigation of robots in a vineyard, showing robustness against different start positions, and thus suitability for robotic vineyard exploration [14]. Another local motion planner combining an RGB-D-based algorithm and deep learning techniques has been introduced and tested in a vineyard aisle [15]. A survey gives an extensive review of core technologies in the field of autonomous navigation for field agricultural machinery, including the main breakthroughs recently made and the remaining challenges need to be addressed [16]. However, most AI-based systems do not have intrinsic safety assurance mechanisms and secured communication protocols, and therefore are not ready to for operation in safety-critical scenarios like agriculture.

The safety and regulatory implications of including autonomy, security, and intelligence into agricultural machinery are in need of proactive methods involving risk assessments and the latest standards. Risk assessment methods, availability of information, machine design standards, and applicable regulations for agricultural robots that can run autonomously are still not understood in detail [17]. It is also concluded that a combination of offline model checking and real-time testing is best used as a safety assurance approach to ensure that autonomous agricultural robots are kept out of harm’s way throughout their lifespan [18]. The perception system is dealt with in detail at a systemic scale, with safety-critical automated mobile machines emphasising a safety-by-design approach that prioritises data fusion techniques, as well as map building of the surroundings [19]. These are some discussions of safety considerations, with a particular focus on inculcating system-level integration through decision-making and communication of agricultural robots acting autonomously, rather than seeing them as different individual pieces that function separately [20].

This systematic review addresses this knowledge void by systematically searching, screening, and synthesising research published between January 2020 and May 2026 following PRISMA 2020 guidelines. A total of 369 peer-reviewed papers were identified through structured Boolean searches across SciSpace, Google Scholar, ArXiv, and IEEE Xplore and subjected to quality appraisal prior to thematic synthesis. The purpose of this systematic review is to synthesise and critically assess the current state of secure and intelligent autonomy for agricultural tractors, in order to identify architectural gaps and propose an evidence-based integrated framework for future research and standardisation.

To achieve this purpose, the following research tasks are addressed: (1) review the current state of the art of swarm coordination techniques, cybersecurity measures, and intelligent navigation strategies for autonomous agricultural tractors; (2) develop an integrated framework that incorporates security, safety, and intelligence directly within the core architecture of autonomous agricultural tractors; and (3) identify open challenges and

directions for future research that would support the safe-by-design, interoperable, and real-world implementation of multi-tractor coordination in precision agriculture.

The central hypothesis of this study is that the fragmented treatment of perception, communication, decision-making, security, and actuation as independent modules—as observed across the reviewed literature—represents the primary architectural barrier to the safe and reliable deployment of autonomous agricultural tractor fleets. It is hypothesised that a cross-layer integrated framework, in which these five components are explicitly combined through defined interfaces and feedback mechanisms, would address the identified gaps more effectively than any single-layer solution and would provide a structured basis for future empirical validation and standardisation.

2. Materials and Methods

2.1. Search Strategy and Databases

This systematic review was conducted in accordance with the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA 2020) guidelines [21], and a completed PRISMA 2020 checklist is provided in the Supplementary Materials (Table S1). A comprehensive and systematic literature search was performed across four reputable academic databases: SciSpace, Google Scholar, ArXiv, and IEEE Xplore (the latter being additionally indexed through both SciSpace and Google Scholar). The search was conducted over the period from January 2020 to 31 May 2026.

The search strategy was structured around four overarching thematic domains, each with a dedicated Boolean query string, as follows:

Theme 1—Swarm Robotics and Multi-Tractor Coordination:

("swarm robotics" OR "multi-robot coordination" OR "multi-agent system")

AND ("agricultural robot*" OR "autonomous tractor*" OR "precision agriculture")

AND ("formation control" OR "decentralized algorithm*" OR "distributed consensus")

Theme 2—Secure Telematics and Lightweight Protocols:

("OSCORE" OR "Group OSCORE" OR "DTLS" OR "CoAP security" OR "lightweight cryptograph*")

AND ("IoT security" OR "telematics" OR "constrained device*" OR "agricultural IoT")

Theme 3—AI-Based Navigation in Unstructured Agricultural Environments:

("AI navigation" OR "deep reinforcement learning" OR "neuro-fuzzy" OR "path planning" OR "obstacle avoidance")

AND ("unstructured environment*" OR "agricultural robot*" OR "autonomous navigation")

AND ("vineyard" OR "orchard" OR "field robot*")

Theme 4—Engineering Standards and Regulatory Frameworks:

("ISO 18497" OR "SAE J3211" OR "functional safety" OR "EU AI Act")

AND ("autonomous vehicle*" OR "agricultural machine*" OR "risk assessment" OR "SOTIF")

To further enrich the initial literature corpus and identify interdisciplinary connections, the AI-driven bibliometric tools Bibliometrix (R package, available at: <https://www.bibliometrix.org/>, accessed on 15 April 2026), Litmaps (web application, available at: <https://www.litmaps.com/>, accessed on 15 April 2026), and Elicit (web application, available at: <https://elicit.org/>, accessed on 15 April 2026) were employed as supplementary instruments for citation mapping, cluster identification, and detection of understudied intersections among the three core domains.

2.2. Inclusion and Exclusion Criteria

The selection of publications was governed by the following pre-defined criteria, applied consistently across all four thematic domains:

Inclusion criteria:

- Peer-reviewed research articles, conference papers, and technical reports published in indexed academic venues
- Publications released within the defined search window: January 2020 to May 2026
- Studies addressing autonomous agricultural robots, multi-robot systems in agriculture, IoT communication security for agricultural machinery, or AI-based navigation in outdoor and unstructured environments
- Papers containing empirical data, novel algorithmic contributions, experimental validation results, or systematic analyses of relevant engineering standards
- Works demonstrating direct or transferable applicability to agricultural tractor autonomy, swarm coordination, or field-deployable telematics systems

Exclusion criteria:

- Non-peer-reviewed sources (blog posts, white papers without formal peer review, patents unaccompanied by academic publications)
- Studies focused on indoor robotics or non-agricultural domains without demonstrated transferability
- Purely theoretical approaches without any empirical substantiation
- Duplicate records; where a preprint and journal version both existed, the journal version was retained
- Publications with insufficient methodological detail to allow assessment of validity or reproducibility

ArXiv preprints were included only where a corresponding peer-reviewed published version was identified and verified; in all such cases, the published version was retained and cited. ArXiv records without a verified peer-reviewed counterpart were excluded.

2.3. Screening Workflow and PRISMA Compliance

The literature selection process followed the PRISMA 2020 four-stage workflow, as illustrated in Figure 1.

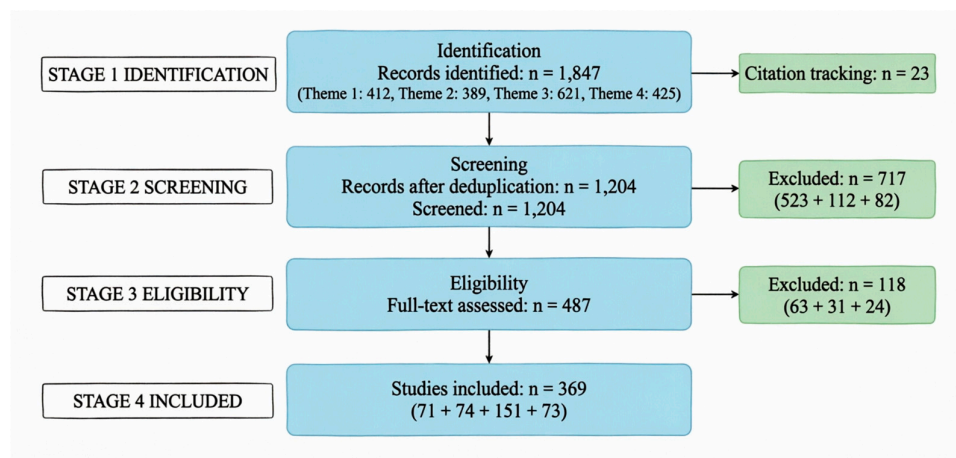


Figure 1. PRISMA 2020 flow diagram illustrating the systematic literature selection process for the review on secure and intelligent autonomy in agricultural tractors (January 2020–May 2026).

Stage 1—Identification: Initial database queries returned a combined total of 1847 records across all four thematic domains (Theme 1: 412; Theme 2: 389; Theme 3: 621;

Theme 4: 425). An additional 23 records were identified through citation tracking of key included papers.

Stage 2—Screening: After deduplication, 1204 unique records remained. Title and abstract screening against inclusion/exclusion criteria retained 487 records for full-text assessment. Excluded records failed due to topical irrelevance ($n = 523$), non-peer-reviewed status ($n = 112$), or publication outside the time window ($n = 82$).

Stage 3—Eligibility: Full-text review of 487 papers excluded those lacking empirical validation ($n = 63$), addressing non-agricultural domains without transferable findings ($n = 31$), or representing superseded duplicate studies ($n = 24$).

Stage 4—Inclusion: The final corpus comprised 369 unique papers: 71 on swarm coordination, 74 on secure telematics, 151 on AI-based navigation, and 73 on engineering standards.

2.4. Quality Assessment

To ensure methodological rigor, a structured quality assessment adapted from the Critical Appraisal Skills Programme (CASP) framework was applied to all 369 papers prior to data extraction, comprising five dimensions:

- Clarity of research objective—Was the research question or engineering objective clearly stated?
- Methodological appropriateness—Was the chosen methodology appropriate for the stated objective?
- Validity of results—Were results supported by adequate empirical evidence or formal verification?
- Reproducibility—Was sufficient methodological detail provided to allow independent replication?
- Relevance to review scope—Did the study contribute directly to one or more thematic domains?

Each dimension was scored 0–2 (fully met/partially met/not met), yielding a maximum score of 10. Papers scoring below 4 were excluded ($n = 12$, reflected in PRISMA Stage 3). Papers scoring 4–6 were included with explicit notation of limitations; papers scoring 7–10 were treated as high-quality evidence in the thematic synthesis.

2.5. Data Extraction and Synthesis

A standard data extraction form was used for each of the 369 papers. They were searched for: (i) type of study and method of validation (simulation/hardware/theory); (ii) main algorithms/architectures/protocols used; (iii) any recorded performance metrics or empirical results; (iv) limitations stated by authors themselves, and; (v) unanswered research questions found, as well as engineering standard/regulatory frameworks, if any were explicitly mentioned in the full text. Data synthesis was performed using a thematic analysis where relevant studies were mapped to primary tech domain/sub-domain categories, as well as underlying trends, methodologies, or unresolved contradictions, if any were found in the large body of work. In cases where the results seem controversial and at an early stage, uncertainty was explicitly included in the synthesis. Some results from automated clustering performed with Elicit and Litmaps are mentioned during the thematic grouping as an appendix to crosscheck the categories. The results are covered starting in Section 3. A gap analysis is presented in Section 4, and finally, an integrating framework is proposed in Section 5. A comprehensive summary of the characteristics, methodologies, and key findings of all 369 included studies, categorized by their primary thematic domain, is provided in the Supplementary Materials (Table S2).

3. Thematic Synthesis

3.1. Swarm Robotics and Decentralised Coordination

3.1.1. Theoretical Foundations

Consensus algorithms enable autonomous agents to reach agreement on average state quantities through communication with limited neighbours. This approach requires neither global coordinate systems nor centralised information, with theoretical foundations rooted in algebraic graph theory and Lyapunov stability analysis [2,22].

Several groups have developed sampled-data consensus algorithms based on the original distributed averaging protocol. These algorithms demonstrate convergence under time-varying and directed network topologies. Notably, Ma et al. [20] established the necessary and sufficient conditions for achieving average consensus under bounded communication delays on directed graphs.

For formation control in multi-agent robotic systems, Hu et al. [22] proposed a leader–follower framework employing game–theoretic leader distribution. In this approach, followers converge to the convex hull of their assigned cluster leaders. Hardware experiments confirmed that this approach is scalable with respect to the number of agents and robust to dynamically changing communication topologies.

To address formation control with non-linear dynamics and external disturbances, Hu et al. [2] developed a Lyapunov stability-based algorithm with proven resilience to unknown disturbances, further validated through experimental implementation. These theoretical and algorithmic foundations collectively underpin the capacity of autonomous tractor fleets to coordinate as a team and maintain precise geometric formations through purely local interactions, without reliance on GPS infrastructure.

The gravitational mass-force (GMF) framework was recently proposed by Starks and Parasuraman [23], which allows for parametric coordination among private, local, and global coordination levels, all the while ensuring network connectivity. Simulation runs and experimental validations suggest a high degree of task-agnostic generalization and connectivity-preserving formation control.

3.1.2. Path Planning and Task Allocation

Agricultural robotics' efficiency relies heavily on field topology and swarm size when it comes to path planning. Four well-known routing algorithms (k-means based on nearest-neighbour approximation, Christofides algorithm, ACO, and BHK), were tested for multiple field topologies by Botteghi et al. [4]. The results indicate that there is no definite winner; instead, different results arise due to different kinds of obstacles in the field or the shapes or number of agricultural robots used, suggesting adaptivity [4,24].

Decentralised approaches using Voronoi partitioning and convex hull path planning were further discussed in the context of large fleets of agribots to ensure less communication. Furthermore, studies by Fayaz et al. [25] compared two communication topologies to coordinate multiple robots in a structured manner. These results confirm the feasibility without ignoring particular trade-offs in communication [23,26].

3.1.3. Byzantine Resilience and Adversarial Robustness

Despite years of research, the critical gap in swarm coordination—specifically Byzantine fault tolerance (handling malfunctioning/malicious robots broadcasting incorrect information)—still poses significant limitations. Established consensus methods like Largest Consensus Protocol (LCP) and Weighted Mean-Subsequence-Reduced (W-MSR) are insufficient to guarantee collision avoidance when robots exhibit untrustworthy behaviour.

A recently proposed rumour-based propagation method, combined with the Expectation-based Extreme Value (EEV) algorithm, has shown promising results in improving collision avoidance and resilience to Byzantine faults in simulations. However, the security and practicality of Byzantine-resilient consensus at massive scale remain open questions. This is particularly relevant for real-world deployments such as large tractor fleets, where lightweight and provably secure consensus protocols have yet to be demonstrated under operational conditions.

3.1.4. Blockchain-Mediated Coordination

Blockchain is also increasingly being recognised not only as a security solution, also as a mechanism for the formation of decentralised coalitions, with its smart contracts that automatically activate and enforce. Smirnov and Teslya [27] proposed an architecture of smart contracts between robots of either one or multiple coalitions for coordination in precision agriculture, with on-chain handling of organisation using a hierarchy-decentralised blockchain. Later, Alsamhi and Lee [28] discussed smart contracting of multiple cooperative (rather than coalitioning in the traditional sense, that is for short-term collaboration) robots during pandemics when working with and handling people through use of master–slave-type blockchain architecture. Blockchain needs communication and processing requirements which may not be present in agricultural robots.

3.1.5. Coordination Summary of Swarm Coordination

There exists a strong body of theoretical work about consensus and formation control of swarms and existing well-tested protocols for communication graphs with directed, time-varying, and delayed communication links. Recent works have investigated coordination using a multi-level adaptive control framework where coordination algorithms can run on a diverse array of vehicles. In agriculture, validation is lacking: there is limited prior work on real farm tractors, as experiments with cooperative swarming have only been performed with two vehicles. Security aspects, including Byzantine faults in swarm systems, have been discussed, and the use of blockchain-assisted solutions for achieving coordination has also been studied, but in the case of embedded systems that are connected to a distributed platform, the resource cost is too high relative to current capabilities. The problems of coordination must be connected with secure communications to guarantee robustness in adverse attack scenarios.

3.2. Secure Telematics and Lightweight Protocols

3.2.1. OSCORE vs. DTLS: Protocol Trade-Offs

There are two different popular methods of implementing secure telecommunications for agricultural IoT that balance encryption level, efficiency of use, and interoperability with the proxy or gateway that translates information for different networks. These two methods consist of DTLS at the transport layer and OSCORE at the application layer. A comparative study conducted in 2021 showed that OSCORE uses more resources than TinyDTLS on the same machine, using around twice as much on one Contiki-NG platform and almost the same as an additional tiny DTLS program on the other platform. OSCORE has lower per-message overhead, and thus less memory usage. However, OSCORE showed 35% less average RTT when running a typical CoAP get request. Most importantly, with DTLS, the gateway must turn the security off, and thus cannot provide true end-to-end security, since it acts as a middleman [6]. In a comparison, Westphall et al. [8] showed that, for an IoT setting, CoAP + DTLS exhibits higher bandwidth usage and a longer handshake duration compared to plain CoAP, but may be better for a longer connection, where the setup time of a session is amortised over a longer time [8]. Therefore, it is commonly argued that OSCORE is a superior option to DTLS for low-power

devices with intermittent communication, and that DTLS would be superior for long, persistent connections or in systems with only trusted middlemen.

3.2.2. Group Communication and Group OSCORE

Agricultural machine groups can be managed by safe multicast group communication sharing broadcast commands and aggregated telematics. Gunnarsson et al. published the implementation and study of group OSCORE on Zolertia Zoul and TI SimpleLink hardware devices. Secured group communication of one to many CoAP messages was implemented. Their study evaluated the usability of group OSCORE for agriculture by considering the computational overheads and protocol overheads in comparison to standard (unsecured) CoAP message transmissions at a representative rate of transmitted agricultural data. Their results demonstrated acceptable incurred costs. A challenge for fleets which frequently change their involved entities is management overhead for the group keys and for their sessions.

3.2.3. Replay Protection and Denial-of-Sleep Attacks

Some vulnerabilities still left in OSCORE are attacks such as defence against replay attacks. The use of a counter-based method in OSCORE cannot mitigate replay attacks over more extended periods or denial-of-sleep attacks. Denial-of-sleep is an attack type where the attackers replay old messages to exhaust devices' energy through the processing of new messages, since in OSCORE messages with new counters would require additional decryption before they can be dropped. To thwart the threat, Krentz and Voigt [29] present OSCORE-NG, which adds timestamps in the nonces in OSCORE, which can assure replay freshness without extra rounds of processing. The results show an improvement in mitigating denial-of-sleep, while OSCORE-NG still requests that loosely synchronised timestamps and drops be delayed past a pre-configured threshold [29].

3.2.4. Scalable Key Management for Dynamic Fleets

When dealing with agricultural fleets, where some of the machinery communicates differently, scalable and light key management still remains an open topic. With the KU-DOS prototype, Höglund et al. [5] aim to find a trade-off that considers the security aspects of the most relevant key update methods applied to OSCORE in relation to the difficulty of implementing these methods [5]. Another interesting approach proposed by Díaz and Almenarez is to establish OSCORE keys at the time of manufacture, combining OSCORE with SRAM-PUF (Physically Unclonable Function) authentication on resource-constrained devices [30]. But because of their need for a device-specific manufacturing process, PUF technologies do not yet represent established standards for agricultural telematics communication, even though they can offer secure storage and establishment for devices.

3.2.5. DTLS Improvements and Alternative Lightweight Protocols

Efforts are under way to improve DTLS for resource-constrained devices; for example, by using a payload-optimised version or a certificate-light approach. For a similar purpose, the Payload Encryption-based Authentication Scheme (PEOS) described by Absata et al. [31] aims to reduce handshake and message size overhead. Work such as the blockchain-based certificate scheme LightCert attempts to shift trust assumptions, but complexity in terms of interoperability and deployment in the Internet of Things are yet to be addressed [32]. Finally, rTLS by Tange et al. [33] presents a secure and efficient TLS session resumption technique to tackle the overhead of reconnecting IoT devices, reducing the latency and overhead associated with new connections.

3.2.6. Application-Layer Optimisations

Lenders et al. [34] demonstrated DNS over CoAP (DoC) with OSCORE, achieving reduced code memory and supporting encrypted en route caching—a valuable feature for distributed agricultural networks with intermittent connectivity.

3.2.7. Synthesis: Open Challenges in Secure Telematics Protocols

The consensus in the literature is that OSCORE is the best choice for telematics applications on telematised vehicles used for constrained farming, due to its properties of enhanced end-to-end security with relatively decreased overhead and effective proxy support. Although OSCORE can be extended to groups for secure multicast communication, key management can become challenging in that case. Further issues of recent interest regard replay protection and denial-of-sleep attack resistance; preliminary results suggest OSCORE-NG as a possible cure for these issues. Meanwhile, substantial gaps remain to be filled in: reliable methods for key provisioning suitable for large, dynamic vehicle fleets; field-based performance appraisals within challenging and realistic networks; and coherent incorporation of enhanced secure telematics protocols in swarm coordination schemes.

3.3. AI-Based Navigation in Unstructured Environments

3.3.1. Hybrid Neuro-Fuzzy Architectures

In environments with uneven terrain, changing obstacles (animals, farmers, machinery), and unpredictable illumination, robots need intelligent systems to navigate effectively. Hybrid neuro-fuzzy systems have emerged as the preferred choice, since they combine the learning capability of neural networks with the interpretability and uncertainty management of fuzzy logic. For multi-robot navigation, Ayub developed a hybrid method based on neural networks, fuzzy logic, and particle swarm optimisation (PSO). Simulation tests found improved path tracking and reduced path length compared to other methods [35]. In 2023, Mohanty [36] applied fuzzy C-means (FCM) clustering with adaptive neuro-fuzzy inference systems (ANFIS/MANFIS) to tackle the reduction of input parameters and the generation of smooth outputs under uncertain conditions. Simulations and real experiments revealed a marked improvement in obstacle avoidance compared to existing approaches [36]. In 2022, Yang [37] designed a self-adaptive version of the dynamic window approach (DWA) coupled with a Mamdani fuzzy controller trained using neural learning. In tests with two simulated robots navigating different environments, his system achieved better obstacle avoidance and reduced total time to reach the goal than a standard DWA with fixed weights [37]. Alzaydi and coauthors expanded this work in 2024 with fuzzy trainers, providing dynamic training datasets, to enable neural network weight updates without needing retraining after deployment. This allowed the system to adapt to its surroundings in real time, while staying within the limitations of computation at the edge [38]. Systems that employ neural networks for obstacle classification into multiple zones and a fuzzy controller for reacting to them have been proven to be effective. Yosif et al. [39] tested a neuro-fuzzy system for the avoidance of dynamic obstacles. Guan [40] investigated similar methods in uncertain environments by building an obstacle classification neural network with intelligent features and then controlling the robot with a fuzzy system.

3.3.2. Deep-Reinforcement Learning and Sampling-Based Planners

DRL combined with rapidly exploring random trees (RRTs) provides the possibility of adapting navigation to dynamic environments in agriculture contexts. The strategy was successfully validated in a simulated olive grove (300 m³) with five different moving obstacles at the same time, with collision-free navigation policies that were constantly updated online according to changes in environment. All pretrained paths are position-agnostic, meaning the policy can be used across different scenarios not requiring precise localisation of robots. This approach was presented at CASE 2022.

3.3.3. Decentralised Multi-Agent Planning with Graph Neural Networks

Furthermore, GNNs also allow for decentralised path planning for teams of tractors, where they learn to communicate and coordinate over local interaction graphs. Coordination of a team of tractors without the presence of a central controller has been explored for purposes of coordination in agriculture: Jo and Son [41] present a decentralised planner based on a GNN that is scalable and depends on local communication. The GNN method is in its early stages and has only been validated in simulated environments; field validation data are not available

3.3.4. Perception-Driven Navigation: Semantic Segmentation and Edge AI

Robust perception is essential for reliable AI navigation. Understanding and classifying different parts of the scene, such as crop rows, lane markings, and obstacles, provides a foundation for structured navigation in diverse and visually complex conditions. The work of Aghi et al. [42] implemented edge-based deep semantic segmentation to navigate vineyards. Their system, running on a low-power embedded computer (NVIDIA Jetson), performed real-time row following, while the generated semantic maps were also used to gauge the health of the crops [43]. Another contribution by Aghi et al. (2020) [15] proposed a real-time motion planner utilising RGB-D cameras, a system of in situ segmentation, and disparity-based control to navigate vineyards. They proved that it was possible to self-label data and extend the capabilities of the model while operating the system on two custom mobile robots, showing how to address variations in environmental diversity, types of crop operations, and visual variations within the row of vines [44].

3.3.5. Hierarchical and Resource-Aware Planning

In order for a planner to maintain long-term farming autonomy, it must be capable of balancing control over momentary variables (e.g., steering, speed) with long-term goals, such as optimising energy use and sequencing tasks efficiently over the entire season. Hierarchical planners which combine an overall mission planning system to handle global navigation, along with simultaneous local obstacle avoidance and a system to react quickly to the agents, have been developed. This was carried out first in simulation and more recently in a semi-field trial. The challenge is that system parameters have to be tuned in the field, and it is not easy to obtain an appropriate set of parameters that work in many real-life situations [45].

3.3.6. Neural and Fuzzy Approaches for Agricultural Manipulator Motion Planning

AI navigation extends beyond ground vehicles to agricultural manipulators. Rodić and Kljajić [46] applied neural network and fuzzy decision-making to motion planning for tree fruit robot pickers, coupling environment models with heuristic gripper path planning among branches.

3.3.7. Summary of AI Navigation

Recently, hybrid neural-fuzzy and deep reinforcement learning (DRL) approaches to autonomous navigation were devised, where the proposed navigation system can avoid different static and moving obstacles whilst plotting optimal paths through a choice of virtual environments (and, to some extent, real-world, controlled experiments) to avoid losing its way. The use of optimised semantic segmentation and on-board edge processing means that the approach is viable for low-cost implantation in agricultural fields such as orchards and vineyards, since the technology does not rely on extensive use of the cloud for processing. Nevertheless, agricultural applications with different crops, terrains, or lighting conditions are yet to be tested on a large-scale; nor has there been much success with sim-to-real transference in any agricultural setting (indeed, this is the biggest issue at hand for the realisation of this technology). In addition, little attention has been given to the issue of improving sensor fusion robustness to temporary obstructions of its view due to vegetation or to its use with large networks of swarm robots.

4. Critical Evaluation and Research Gaps

4.1. Strengths of the Current Research

There are rigorous theoretical foundations under consensus and formation control algorithms, as these use algebraic graph theory and Lyapunov stability to make valid assertions about directed, time-varying, and delayed communication graphs [2,20,21]. OSCORE and group OSCORE have already been implemented and compared on devices that are heavily constrained in their available computational resources, showing an even lower overhead than DTLS and thus offering some practical feasibility for the context of agricultural IoT [6,9]. In addition, the diverse and flexible AI navigation approaches that combine aspects of neuro-fuzzy controllers, deep-reinforcement learning techniques, and sampling-based planners show the ability to handle dynamic obstacles and an unstructured environment, with successful tests in simulation, as well as controlled experiments with a real robot [34,36,40,42]. An increasing awareness of regulatory frameworks is evident in the reviewed literature. ISO 18497 is widely cited as the primary engineering standard for safe autonomous agricultural machinery [17,45]. The EU AI Act (Regulation (EU) 2024/1689), which classifies autonomous systems operating in proximity to humans as high-risk AI applications subject to mandatory conformity assessment, transparency obligations, and post-market monitoring requirements, is beginning to receive attention in the agricultural robotics literature [45,46]. Safety assurance methodologies including HARA, STPA, and SOTIF-equivalent approaches are increasingly discussed as necessary complements to existing standards [17,45,46].

4.2. Identified Research Gaps and Limitations

Most solutions today separate safety, autonomous control, and collaborative algorithms into different layers. This causes issues with the system's resistance against internal faults, makes safety certification harder, and is not ideal for large-scale, multi-robot operations in practice. This review proposes a conceptual integrated framework that incorporates safety by design and cross-layer information sharing within the decision-making and communication subsystems—an architectural hypothesis derived from the convergent gaps identified across the 369 reviewed studies, intended to guide future experimental validation.

Most swarm robot teams or AI-based autonomous driving systems are tested only using small robots or simulations, never using actual, fully-sized, self-driving machines in commercial farming operations. It has only been demonstrated a handful of times that a few tractors can drive autonomously in a farming setting [2,14,21,23,40]. One area of

research in swarm robots concerns malicious robots in the swarm, but experiments so far rely on simulations only. Nobody has demonstrated that tractor fleets can efficiently and securely run a consensus that protects against malicious actors who are Byzantine in nature [24]. In terms of communication security, some solutions are proposed on secure establishment and key updates. Examples of these are PUFs, KUDOS, and blockchains [28,29,31]. However, few of these solutions offer a simple way of standardising this setup for large-scale, dynamic farming fleets, and this problem still has not been tackled. A way that could be used to resist replay attacks is OSCORE-NG, which includes better measures to prevent repeated messages [27], but so far this has not been validated extensively under stressful real-life conditions such as spotty wireless connections or high communication latency [27]. Deep-reinforcement learning and hybrid path planning systems show promising results in simulation but have not been thoroughly validated with regard to how well policies that were learned are transferred into large-scale, real farming fields or across various conditions, like soil types, fields of different terrain, or unpredictable weather patterns [14,40]. Risk evaluation methods like HARA and FMEA cannot be executed reliably if there are no past events recorded, and in the majority of cases this does not happen, since autonomous machinery is still novel and only now becoming widespread [17,47]. ISO 18497 provides foundational safety principles for autonomous agricultural machinery; however, Clauses 4 and 5 prescribe no measurable acceptance thresholds for perception performance—such as maximum false-negative detection rates under reduced-visibility conditions or minimum object-classification confidence levels—nor do they mandate the definition of an agriculture-specific Operational Design Domain (Ag-ODD) [47]. Clause 6, covering validation and verification, specifies neither scenario-based testing protocols nor a requirement for a scenario catalogue systematically covering edge cases such as sensor degradation, animal intrusion, implement occlusion, or variable weather conditions [48]. Furthermore, the standard provides no equivalent to ISO 21448 (SOTIF) for managing functional insufficiency arising from deep-learning-driven perception systems operating outside their design envelope [48]. Runtime verification, formal logic, and other methods to verify AI behaviour at system level remain insufficiently covered by existing standards [18,46].

4.3. Areas of Consensus and Disagreement

4.3.1. Consensus on Best Practices

Several widely accepted principles guide the research into secure agriculture IoT:

OSCORE over DTLS for Constrained Devices: For devices in agricultural settings that are resource-constrained, research indicates that OSCORE is superior to DTLS. It incurs lower computational overhead, requires less memory, and provides end-to-end security without relying on a proxy or gateway for security processing [6,8,9].

Hybrid Approaches for Robot Navigation: A blend of learning-based and model-based techniques has emerged as the preferred method for developing robust agricultural robot navigation systems. Examples include the combination of neuro-fuzzy logic and deep-reinforcement learning (DRL) [36] or the use of RRT-based algorithms coupled with DRL for path planning [40]. Researchers believe these hybrid strategies offer a better balance between adaptability and reliability than end-to-end learning approaches [34].

Need for Layered Assurance: There is a general consensus that adopting security standards alone is not enough to ensure the security and trustworthiness of AI-powered agricultural systems. Security standards are generally considered insufficient on their own, and they need to be complemented with a combination of techniques such as formal verification methods to prove system properties, real-time runtime monitoring to detect anomalies and attacks, and exposure databases to track known vulnerabilities [17,46,48].

4.3.2. Areas of Disagreement and Open Debate

However, significant disagreements and open debates persist within the research community:

Blockchain for Coordination: While some researchers propose using blockchain technology as a decentralised, tamper-resistant ledger to record coordination events and logs [25,26], others argue that the computational overhead and energy consumption of blockchain consensus mechanisms are prohibitively high for many constrained agricultural IoT devices. The practical applicability and benefits of blockchain for this specific domain remain a subject of debate.

Centralised versus Decentralised Key Management: There is no clear consensus on the best approach for managing cryptographic keys in agricultural IoT networks. Proposals include the use of centralised servers (e.g., an EDHOC server) to handle key establishment [28] and fully decentralised schemes that use hardware security modules like Physical Unclonable Functions (PUFs) [29].

Optimal Path Planning Algorithms: While various path-planning algorithms have been proposed for agricultural robots, a recent study by Botteghi et al. [4] demonstrated that the optimal choice of algorithm is dependent on the specific characteristics of the field layout or topology. This research challenges the notion of a single “best” algorithm and suggests that adaptive or hybrid planning approaches might be more suitable in practice.

Sufficiency of ISO 18497: The standard ISO 18497 defines security guidelines for agriculture IoT devices. While some research papers cite this standard as a comprehensive baseline for securing these devices [46], others argue that it is insufficient for addressing the security challenges posed by AI-driven autonomy and requires significant enhancements and additional security measures [17,48].

5. Proposed Integrated Framework: Cross-Layer Fusion and Validation

5.1. Beyond Modular Stacking: The Core Advantage of the Framework

The framework presented in this section constitutes a conceptual proposal synthesized from the patterns, gaps, and convergent findings identified across the 369 papers included in this systematic review. It is not a validated engineering system, and no empirical performance claims are made. Rather, it represents a structured research agenda—an evidence-derived architectural hypothesis intended to guide future experimental work and standardisation efforts. Each of the five layers directly addresses one or more research gaps identified in Section 4, as detailed below.

Unlike traditional architectures that treat perception, communication, and control as isolated silos, the proposed five-layer framework (Perception, Communication, Decision-Making, Security, Actuation) is founded on contract-based design and cross-layer enforcement. The intended advantage of this conceptual framework, if empirically validated, would lie in its deep fusion of safety and intelligence. For instance, a detected anomaly in the Security layer (e.g., a Byzantine fault) does not merely log an error; rather, it is designed to trigger a fallback protocol in the Decision-Making layer and a safe-state transition in the Actuation layer with minimal latency—a property that requires empirical validation in future hardware-in-the-loop testing. This tight coupling is intended to support safe-by-design behaviour even under adversarial or highly unstructured conditions, subject to empirical validation.

5.1.1. Layer 1: Perception

Edge-optimised semantic segmentation and sensor fusion (LiDAR, RGB-D, GNSS) are integrated into the Perception layer [15,42]. Cross layer: In addition to spatial infor-

mation, Perception also outputs a “confidence score” to Decision-Making. When confidence falls below a certain threshold, Perception sends an additional request to the Actuation layer, for higher frame rate scanning and a reduction in the robot’s speed. With this cross-layer confidence-based feedback system, we are filling the gap found in Section 4.2’s survey, which did not combine consideration for uncertainty regarding Perception with speed control at the actuation level.

5.1.2. Layer 2: Communication

It utilises an OSCORE/group OSCORE end-to-end security system [6,9] (cross-layer interaction). The prioritisation is context-aware. Emergency coordination messages with higher CoAP priority levels circumvent standard queueing and thereby enjoy lower latency when the network becomes congested. This priority mechanism is used to fill a gap identified above: that no existing OSCORE deployment accounts for emergency messages in a context-aware manner (Section 4.2).

5.1.3. Layer 3: Decision-Making

Local neuro-fuzzy/DRL path planning (PP) and swarm coordinate behaviour (via distribution consensus [20,21]).

The main interaction that concerns us here is that there is a module which verifies an AI-generated trajectory against “hard boundaries” before execution (runtime RV), so, if violated, this trajectory will be dismissed, and instead a fallback controller will activate [18]. This deals with Section 4.2’s claim of a lack of formal trajectory verification alongside distributed consensus (in this case, as it controls the swarm, which implies a distribution type algorithm or at least that it is locally run in a swarm).

5.1.4. Layer 4: Security

This would comprise intrusion detection-based replay protection and authentication by OSCORE-NG [27], as well as detection of Byzantine nodes [24]. This will continually watch the Security layer. When a node is flagged as being a Byzantine node, the Security layer will immediately revoke its cryptographic keys through the Communication Layer and will remove its influence from the swarm consensus. This converged security layer bridges the gap mentioned in Section 4.2, in which the subject of Byzantine node detection and replay protection has individually been studied but has never been integrated with revoking the key in an effective manner.

5.1.5. Layer 5: Actuation

This layer contains hardware-level fail-operational interlocks. Should the Decision-Making layer fail to deliver a valid “heartbeat” or safety contract within its timeout window and at regular time intervals, then the Actuation layer assumes authority over software-level commands and automatically performs a controlled, safe stop, according to ISO 18497 principles [46]. This heartbeat-triggered cross-layer interaction compensates for the finding reported in Section 4.2 that fail-operational behaviour should be used between the software systems. The Actuation layer translates commands originating directly from the Perception and Decision-Making layers into physical steering and throttle control.

5.2. Definitions with Cross-Layer Interactions

Having introduced each layer’s component technologies and the research gap addressed in Section 5.1, this section formally defines the bidirectional cross-layer interaction contracts—the structured, trigger-based information exchange protocols that distinguish this framework from conventional modular stacking. Table 1 summarises the primary

cross-layer interactions, while Figure 2 provides a visual representation of the complete five-layer integrated framework and its bidirectional information flows.

Table 1. Cross-layer interaction table.

From Layer	To Layer	Trigger Condition	Information Exchanged	Fallback Action
Perception (L1)	Decision-Making (L3)	Confidence score < threshold	Confidence score + spatial data	Request higher-frequency scan; reduce speed via L5
Perception (L1)	Actuation (L5)	Terrain anomaly detected	Wheel slip/torque feedback signal	Reduce speed; alert L3
Communication (L2)	All layers	Emergency message received	Priority CoAP message	Bypass standard queue; immediate delivery
Decision-Making (L3)	Actuation (L5)	AI trajectory generated	Trajectory + heartbeat signal	RV rejection triggers activation of fallback controller
Security (L4)	Communication (L2)	Byzantine node detected	Key revocation command	Isolate node from swarm consensus
Security (L4)	Decision-Making (L3)	Intrusion detected	Security alert	Suspend AI decisions; activate safe mode
Actuation (L5)	Perception (L1)	Unexpected wheel slip	Terrain feedback signal	Increase scan frequency; adapt path

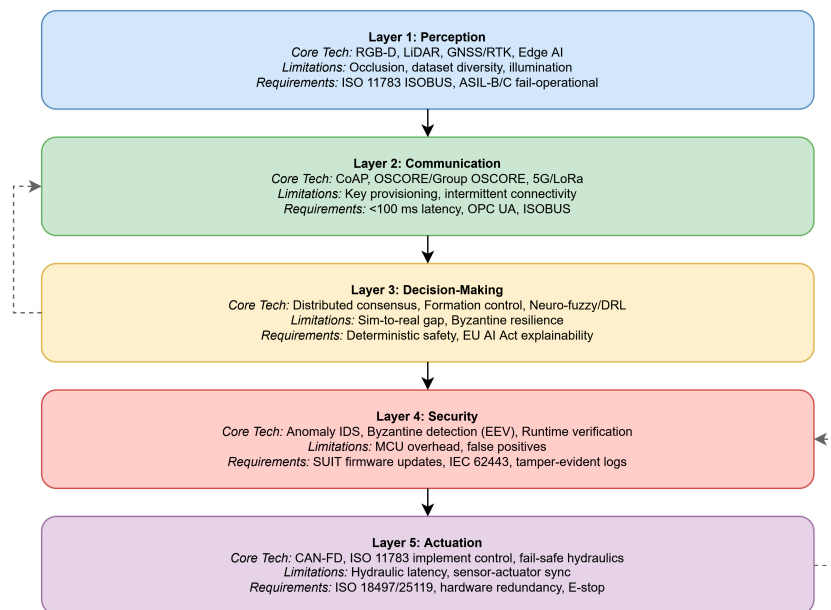


Figure 2. Five-layer integrated engineering framework for autonomous agricultural tractors. Each layer maps core technologies, documented limitations (2020–2025), and interoperability/safety requirements. Solid arrows indicate primary data flow; dashed arrows represent feedback and cross-layer verification loops. Different colors are used to distinguish the five distinct layers of the framework.

The cooperative layer allows tractor-to-tractor communication across all layers of the architecture. In the Perception layer, semantic map and obstacle detection results are exchanged between the tractors as secured (OSCORE protected) messages over CoAP to fuse the sensor information, while the Communication layer makes use of group OSCORE

to communicate the consensus and formation controller messages to its respective group member and subscribe to the secure telemetry messages of the Decision-Making layer, which monitors the AI navigation with runtime verification modules, like speed monitoring against objects in reach, and detects harmful attacks towards the consensus to isolate Byzantine fault behaviour, to name a few. The security components have control over actuators using a secure boot procedure that protects the actuators' firmware via a redundant safe hardware interlock that enforces safety limits no matter what may result from the software state, and so on.

5.3. Interface Definitions and Feedback Mechanisms

To ensure genuine integration, the framework defines strict interfaces and bidirectional feedback loops:

- **Standardised Data Interface:** Inter-layer communication utilises lightweight, structured payloads (e.g., protocol buffers over CoAP). A typical telemetry packet includes {timestamp, node_ID, spatial_data, confidence_score, safety_state, cryptographic_MAC}. This ensures that all layers parse data uniformly and can verify their integrity instantly.
- **Feedback Loop A (Security → Actuation):** Upon detecting a replay attack or consensus divergence, the Security layer sends an immediate CRITICAL_FAULT flag. The Actuation layer receives this out of band, bypassing the standard decision queue to engage mechanical brakes.
- **Feedback Loop B (Actuation → Perception):** If the Actuation layer detects unexpected wheel slip or high torque (indicating unstructured terrain), it sends a feedback signal to the Perception layer to dynamically switch to a more robust sensor fusion model to reassess the environment [44].

5.4. Proposed Validation Strategy

To move beyond theoretical stacking, we propose a rigorous, three-phase validation strategy for this framework:

Phase 1: Model-in-the-Loop (MiL) with Fault Injection. Simulate the full five-layer architecture in a digital twin environment (e.g., ROS 2 + Gazebo). Intentionally inject faults, such as dropping 30% of CoAP packets or simulating a Byzantine node broadcasting false coordinates. Measure the framework's convergence time and safety enforcement latency [49].

Phase 2: Hardware-in-the-Loop (HiL) Testing. Deploy the Communication, Security, and Decision-Making software stacks on actual edge computing hardware (e.g., NVIDIA Jetson) connected to a simulated actuation plant. This validates the real-world computational overhead of OSCORE-NG and runtime verification under resource constraints.

Phase 3: Small-Scale Field Validation (Sim-to-Real). Conduct controlled field trials with two to three autonomous agricultural platforms. Key performance indicators (KPIs) will include (a) successful sim-to-real transfer rate of the neuro-fuzzy navigator, (b) end-to-end latency of secure swarm consensus under real-world RF interference, and (c) the system's ability to safely halt upon simulated sensor failure, adhering to ISO 18497 principles [50].

6. Engineering Guidelines for Safe-by-Design Autonomous Vehicles

6.1. Standards Landscape: ISO 18497 and Beyond

ISO 18497 "Agricultural machinery and tractors—Safety of automated agricultural machines—Principles for design" is now the main engineering standard dealing with the safety of autonomous agricultural machines [46]. The authors of this paper believe that

ISO 18497 is still helpful for promoting the safety of autonomous agricultural machines but is not efficient for addressing the risks of autonomous AI-based systems. It should be enhanced and complemented with ergonomics standards and a range of risk methods, including STPA and other newer risk identification processes.

However, this characterisation of inadequacy requires specification at the clause level to guide meaningful revision. Clauses 4 and 5 of ISO 18497, which establish general requirements for safety functions and risk management, prescribe no measurable acceptance thresholds for perception performance—such as maximum false-negative detection rates under reduced visibility conditions or minimum object-classification confidence levels—nor do they mandate the definition of an agriculture-specific Operational Design Domain (Ag-ODD) that bounds the environmental, temporal, and task-related conditions under which the system may safely operate [47]. This omission becomes critical when a deep-learning-driven perception system must make safety-relevant decisions outside the conditions anticipated during development, a scenario explicitly addressed for road vehicles by ISO 21448 (Safety of the Intended Functionality, SOTIF) but for which ISO 18497 provides no equivalent mechanism to manage functional insufficiency in unstructured agricultural environments [48]. Furthermore, Clause 6 of ISO 18497, covering validation and verification, specifies neither scenario-based testing protocols nor a requirement for a scenario catalogue that would systematically cover edge cases such as sensor degradation, animal intrusion, implement occlusion, or variable weather and lighting conditions [19]. The absence of normative requirements for perception fault management systems—capable of detecting, diagnosing, and mitigating sensor failures or degraded inputs in real time—represents a concrete gap that prevents systematic certification of AI-driven machinery under the current standard.

Similarly, the work by Aby et al. [51] concluded that ISO 18497 offers essential design principles but needs to be supplemented with ergonomics and alternative risk assessment tools (e.g., STPA), because no existing ISO or IEC standard adequately covers risks involving unfamiliar situations arising from novel automation technologies. According to Shutske et al. [17], work based on the SAFER AG workshop highlighted that FMEA and HARA, the primary methods of risk analysis per ISO 12100, rely heavily on historical accident and incident data—something that is scarce for a new generation of automated agricultural equipment. For new machine classes, they recommended building exposure data specific to the new systems. Furthermore, the experts suggested integrating appropriate standards early into the design process, before fully automated functionalities are even deployed. Safety integrity levels, comparable to the Automotive ASIL ratings found in IEC 61508, have been developed and presented for the Functional Safety of Agricultural and Forestry Machinery in ISO 25119, a standard designed to be compatible with automotive functional safety standards like ISO 26262. ISO 11783 is also important, as it enables interoperability between implements and vehicle systems [19,52]. No peer-reviewed publications to date directly analyse the applicability of SAE J3211 to agricultural tractors [52]. This gap is significant because, unlike road vehicles, tractors operate in dynamic coupling with implements that alter vehicle kinematics and sensor field-of-view geometry, necessitating an extension of the SAE J3211 taxonomy to include an implement-coupled autonomy category that accounts for tool-object interactions and implement-induced occlusions. Furthermore, the SAE J3211 framework presupposes a structured traffic environment with defined right-of-way rules and lane markings, whereas agricultural fields, orchards, and pastures possess no equivalent infrastructure, implying the need for dedicated verification and validation (V&V) protocols that combine functional safety methods (per ISO 25119) with SOTIF methodology explicitly adapted for off-highway unstructured operational domains.

Yet this gap is not merely observational; it opens several concrete research directions that must be pursued to enable normative application of SAE J3211 in agricultural contexts. First, unlike road vehicles, tractors operate in dynamic coupling with implements that alter vehicle kinematics, sensor field-of-view geometry, and the set of hazardous scenarios, necessitating an extension of the SAE J3211 taxonomy to include an implement-coupled autonomy category that accounts for tool–object interactions and implement-induced occlusions [52]. Second, the SAE J3211 framework presupposes a structured traffic environment with defined right-of-way rules and lane markings, whereas agricultural fields, orchards, and pastures possess no equivalent infrastructure, implying the need for dedicated verification and validation (V&V) protocols that combine functional safety methods (per ISO 25119) with SOTIF methodology explicitly adapted for off-highway applications and unstructured operational domains [17].

Recent work has begun to address these integration challenges through hybrid safety architectures. Muthusamy [52] proposed a hybrid safety framework that explicitly integrates ISO 18497, ISO 25119, ISO 26262, ISO 21448 (SOTIF), ISO 21434 (cybersecurity), and ISO 8800 (AI safety) with AI-specific measures, including explainable AI, sensor fusion, and fail-safe switching mechanisms, to improve resilience in unstructured agricultural environments. Complementing this systems-level approach, Lee et al. developed a dedicated fault management system for perception systems in highly automated agricultural machines, implementing detection, diagnosis, and mitigation strategies for sensor degradation that are explicitly compliant with ISO 18497 and ISO 25119 [53]. The SAFER AG workshop consensus documented by Shutske et al. confirmed that risk assessment for novel autonomous machine designs is constrained by the absence of historical exposure data and recommended establishing an exposure-based incident database to support risk analyses for new machine classes [19]. Collectively, these developments indicate that the current standards landscape requires AI-specific safety annexes, harmonised exposure data collection frameworks, validated test protocols for scenario-based verification, and explicit SOTIF-equivalent mechanisms to adequately address the safety challenges of fully autonomous, AI-powered agricultural systems.

Under Annex III of the EU AI Act (Regulation (EU) 2024/1689), AI systems intended for the operation of safety-relevant autonomous machinery operating in proximity to humans are classified as high-risk, requiring mandatory conformity assessment, comprehensive technical documentation, and registration in the EU database prior to market placement [45]. Autonomous agricultural tractors operating in proximity to field workers fall within this classification, imposing compliance obligations—including human oversight mechanisms, robustness and accuracy requirements, and transparency towards operators—that the current ISO 18497 framework does not yet explicitly address in its risk management provisions.

6.2. Functional Safety and Verification Strategies

For functional safety to reach the autonomy of the driverless future, a layered system of verification will be necessary. This combines static (offline) verification of control systems and dynamic (runtime) monitoring of the AI, alongside fail-operational design to guarantee safe behaviour during system failures. Adam et al. [18] demonstrated a hybrid approach combining offline and runtime verification for agricultural autonomous systems, applying standard model checkers (UPPAAL/NuSMV) to discrete state-machine-based controllers and runtime verification to continuously check AI component outputs against specified safety boundaries. The efficacy of this approach was validated on an autonomous spraying robot for targeted weed identification, providing evidence toward bridging safety gaps between AI and established engineering approaches.

We recommend leveraging sensor redundancy (different sensors of same/similar type) and fail-operational perception systems (degraded perception capabilities on failure of main components), along with thorough system validation against edge-case failure modes [19].

6.3. Regulatory Compliance: EU AI Act Considerations

Under Regulation (EU) 2024/1689 (EU AI Act), the high-risk classification of AI systems is established by Article 6, which designates as high-risk those AI systems that serve as safety components of products covered by Union harmonisation legislation listed in Annex I or that fall within the categories listed in Annex III [45]. Autonomous agricultural tractors operating in proximity to field workers qualify as high-risk under Annex III, Point 2, and the tractor constitutes machinery covered by Regulation (EU) 2023/1230, also under Article 6(1) read with Annex I.

Systems classified as high-risk must satisfy the following requirements: (a) data governance (Article 10), (b) transparency (Article 13), (c) human oversight (Article 14), and (d) robustness and cybersecurity (Article 15).

Kelly et al. [53] propose a new method for ensuring compliance with the EU AI Act for safety-critical products. It translates high-risk regulatory requirements into several measurable product quality attributes, then transforms them into technical requirements by contract-based design. Their methodology has already been successfully implemented in the automotive and industrial automation industries, and it may also be applied to autonomous agriculture [53].

Based on the EU AI Act, requirements include the following:

****Data governance [10]:** ** Training and validation datasets are required to be representative, without any inherent bias, and to be documented properly. As agriculture operates across varied terrains, crop types, and weather conditions (including illumination), relevant and documented training datasets are essential [53].

****Transparency (Article 13):** ** AI systems must offer explanations of their actions and decisions. One example is hybrid neuro-fuzzy architectures, which have built-in interpretabilities. Alternatively, with end-to-end deep-reinforcement learning (DRL) architectures, explainability methods, such as attention mechanisms and saliency maps, may be applied ex post [14,34].

****Human oversight (Article 14):** ** The human operator should be able to intervene to override an AI decision when it is needed. With telematics interfaces, the system allows for the human to be monitoring and controlling the vehicle operations remotely in real time [6,9].

****Robustness and cybersecurity (Article 15):** ** These systems need to be resistant to adversarial attacks to achieve safety in case of faults. Similar to concepts such as Byzantine-resilient consensus algorithms and robust control, a framework is required for secure and safe telematics applications [24,27]. From a data governance and transparency perspective, Butt et al. proposed a pipeline-native governance framework—termed Governance as Evidence for AI Pipelines (GEAP)—that converts the EU AI Act regulatory clauses directly into machine-enforceable rules with clause-to-artifact traceability and tamper-evident conformity bundles across the full data, training, validation, and operations lifecycle, thereby providing a practical and auditable pathway to satisfying Articles 10 and 13 in high-risk AI deployments [54]. With regard to human oversight and robustness under Articles 14 and 15, Kim et al. [55] introduced EGIS, a hardware-isolated dual-brain controller architecture for physical AI systems—including autonomous vehicles and robots—that enforces safe halt, override, and recovery behaviours in the event of adversarial attacks or system failures, demonstrating through case study analysis that architectural sep-

aration between the operational AI and a guardian module constitutes a viable engineering solution to EU AI Act compliance for autonomous machinery [55]. Finally, Kelly et al. [53] argued that the current risk assessment methods applied to safety-critical AI in machinery are insufficient for EU AI Act conformity assessment under Annex III and proposed systematic, safety case-oriented approaches that enable third-party qualification—a finding directly applicable to autonomous agricultural tractors and field robots, which are classified as high-risk AI systems under Article 6(1) in conjunction with Annex I of Regulation (EU) 2024/1689, by virtue of their function as safety components within machinery covered by Regulation (EU) 2023/1230 [53].

6.4. Practical Recommendations for Deployment Readiness

The reviewed literature offers a fertile ground for actionable research directions, design principles, and policy interventions. We thus present the following recommendations for researchers, system designers, and policymakers.

6.4.1. For Researchers

Focus on Field-Scale Validation: Moving beyond simulations and laboratory studies is crucial. Efforts should be made to validate research findings in operational farm fields using real, full-size tractors across a spectrum of crops, varying terrains, and weather conditions [2,14,21,40].

Develop Operational Exposure Databases: Close collaboration between researchers and industry players is vital to build comprehensive databases containing details about actual incidents, near-misses, and relevant exposure data. Such databases are foundational for building accurate probabilistic risk models [17,48].

Building upon promising rumour-based and EEV algorithms, future research should focus on developing these approaches into formally verified protocols with provable security guarantees against Byzantine adversaries. Subsequent validation with physical tractor fleets is essential to demonstrate their practical efficacy under real-world agricultural operating conditions [24].

Future research efforts will investigate the interactions and dependencies between secure telematics communication and the coupled behaviour of a swarms of tractors, with specific emphasis on failures of communication security and the way that this propagates to swarm coordination. The work will further explore low-latency, end-to-end integrity in messages that is important for the integrity and trustworthiness required to reach consensus. Communication security mechanisms including communication integrity are to be formally evaluated within swarms based on deployments of a group of farming tractors working collaboratively [6,9].

6.4.2. For System Designers

Employ a Layered Assurance Strategy: Reliance on a single standard, such as ISO 18497, is insufficient. A robust safety framework should incorporate formal verification of system behaviour, runtime monitoring for deviations, and compliance with relevant standards as complementary layers of assurance [18,46].

Carry out OSCORE for Agricultural Telematics: For the stringent resource constraints prevalent in agricultural IoT, deploy OSCORE or group OSCORE, along with the OSCORE-NG protocol, for robust replay protection [6,9,27].

Adopt Hybrid AI Architectures: When dealing with the complexities of agricultural environments, hybrid architectures such as neuro-fuzzy systems or methods that combine algorithms like the rapidly exploring random tree (RRT) with deep-reinforcement learning (DRL) are preferable over purely end-to-end learning approaches. These hybrid methods offer better interpretability and robustness [34,36,40].

Design for Fail-Operational Modes: Design safety-critical functions to operate reliably in degraded modes. Incorporate hardware interlocks to ensure that the system fails safely in the event of critical component failure [19].

Anticipate Scalable Key Management: Explore and evaluate key management solutions such as EDHOC, PUF-based approaches, or lightweight Public Key Infrastructure (PKI) methods that are capable of efficiently handling the dynamic enrolment of a large fleet of autonomous tractors [28,29].

6.4.3. For Policymakers and Standards Bodies

Harmonise Agricultural and Automotive Standards: Clarity is needed about the applicability and adaptation of automotive standards such as SAE J3211 and the ISO 26262 functional safety concept to the domain of agricultural autonomy. Development of sector-specific guidelines or annexes to these standards is recommended [17,45].

Mandate Exposure Data Reporting: Policy should require agricultural machine manufacturers to report all operational incidents and near-misses into public, accessible databases. These data are essential for performing rigorous, evidence-based risk assessments [17,48].

Develop Comparative Test Protocols: Standardisation of test protocols for autonomous agricultural machines is needed to cover performance metrics, stability characteristics, and various safety-critical scenarios. Such protocols will be vital for developing certification frameworks [48].

Support EU AI Act Compliance Tools: Policymakers should allocate funding for the development of specific tools and resources, including methodological frameworks, annotated datasets, and explainability mechanisms, tailored to the unique challenges and applications of AI in agriculture. This support will help compliance with the EU AI Act [53].

7. Conclusions

This systematic review addressed the three research tasks defined in Section 1. Regarding task 1, 369 peer-reviewed studies were reviewed, and the theoretical background for swarm robotics (distributed consensus, formation control), secure telematics (OSCORE, group OSCORE), and AI-driven navigation (neuro-fuzzy logic, deep reinforcement learning, sampling-based planners) is fairly mature. Regarding task 2, fragmentation across safety, decision-making, and layer coordination motivated proposing a modular five-layer integrated framework (Perception → Communication → Decision-Making → Security → Actuation) as a conceptual evidence-based architecture for system design. Regarding task 3, there is a lack of full-scale real-world tractor validation, an absence of Byzantine-robust consensus under real-world conditions, and a lack of unified safety standards for autonomous agricultural machinery.

To synthesise and critically assess the progress in secure and intelligent autonomy for agricultural tractors between January 2020 and May 2026, this systematic review critically synthesises the available peer-reviewed literature, with particular focus on swarm robotics, secure telematics, and AI-driven navigation.

We find in the literature a relatively mature theoretical foundation concerning swarm robotics concepts (e.g., distributed consensus, formation control algorithms). Furthermore, there is evidence for the applicability of lightweight and secure transport protocols (OSCORE and group OSCORE) that guarantee a sufficient level of security with less overhead on resource-constrained devices compared with DTLS. Approaches to navigation based on AI (e.g., hybrid neuro-fuzzy logic, deep reinforcement learning, sampling-based path planning algorithms) also show good results, even in unstructured agricultural environments. Nevertheless, there is evidence for architectural fragmentation in systems

that, by nature, would require tight cooperation among safety, decision-making, and coordination layers. Moreover, to the best of our knowledge, empirical evidence on test beds made up of real-size tractors is scarce or else mostly based on simulation, especially concerning Byzantine consensus and robust key management solutions for dynamic fleets. Also, little empirical evidence on the application of safety assurance frameworks in real operational conditions exists. In view of the shortcomings identified, we propose a modular five-layer framework (Perception → Communication → Decision-Making → Security → Actuation) to give designers of secure and intelligent autonomy a structure based on the existing literature and to address requirements for interoperability and safety. Engineering guidelines gathered from the aforementioned ISO standard, methods that could contribute to compliance of the systems under discussion with the EU AI Act, and recommendations found in the academic community are presented, with a strong emphasis on the need for layered assurance, the use of databases covering the entire life cycle of a safety-relevant system, standardised test protocols, and the use of hybrid AI solutions (at least partly), for reasons of interpretability. Until all requirements concerning empirical robustness in real-world tractor tests and concerning the application of common security standards are fulfilled, and until there is regulatory clarification around these aspects, the safe, interoperable, and deployment-ready autonomous agricultural systems that we dream of will not exist.

The main limitations of our systemic review were as follows. (1) We performed our search in four databases (SciSpace, Google Scholar, ArXiv, and IEEE Xplore). Relevant studies in databases other than the consulted databases might be missed. We tried to find some other databases but ended up searching these four, since others are more specific to material science research, such as Nano. Searching Springer university databases was unsuccessful due to login problems. (2) We considered the 2020–2026 time period. Prior works, e.g., 2011 to 2019, were excluded, as they cannot show how COVID affected cyber security-related events. Furthermore, we need recent developments for an applicable system for cyber secure and attack-resilient system for drone infrastructure. (3) We followed quality assessment using a slightly modified CASP assessment tool. Though scoring for methodology quality assessment was straightforward, mapping into themes from 30 papers was mostly related to our best judgment. (4) The proposed architectural framework of a five-layer pyramid has not been tested and is more of a proposal or suggestion. Hardware-in-the-loop and ground testing may still be required to validate the functionality of the layers mentioned above. Finally, future research has to investigate real-world agricultural tractor tests, explore Byzantine-robust cooperation strategies among vehicles, develop fully scalable secure telematics communication systems among vehicles, and evaluate the transfer from simulation environments to real-world deployments systematically. Otherwise, there will be no autonomous farming with secure and intelligent tractor swarms.

Supplementary Materials: The following supporting information can be downloaded at: <https://www.mdpi.com/article/10.3390/agriengineering8070269/s1>, Table S1: PRISMA 2020 Checklist; Table S2: List of 369 Included Studies.

Author Contributions: Conceptualization, D.Z. and M.J.; methodology and systematic search design, L.Š. and D.Z.; writing—original draft preparation, D.Z.; writing—review and editing, P.L.; visualization, A.B. and E.Š.; supervision, D.Z. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by Josip Juraj Strossmayer University of Osijek through the scientific project “Prediction of maize yield potential using machine learning models based on vegetation indices and phenological metrics from Sentinel-2 multispectral satellite images (AgroVeFe)” (Contract No. 581-UNIOS-30), co-funded by the European Union—NextGenerationEU.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The original contributions presented in this study are included in the article/Supplementary Materials.

Acknowledgments: The authors would like to thank the reviewers for their insightful comments.

Conflicts of Interest: The authors declare no conflicts of interest.

References

- De Carolis, G.; Williams, R.K.; Gasparri, A. A swarm-based distributed algorithm for target encirclement with application to monitoring tasks in precision agriculture scenarios. In Proceedings of the IEEE Mediterranean Conference on Control and Automation (MED), Limassol, Cyprus, 26–29 June 2023; pp. 275–280. <https://doi.org/10.1109/med59994.2023.10185862>.
- Hu, J.; Turgut, A.E.; Lennox, B.; Arvin, F. Robust formation coordination of robot swarms with nonlinear dynamics and unknown disturbances: Design and experiments. *IEEE Trans. Circuits Syst. II Express Briefs* **2021**, *69*, 114–118. <https://doi.org/10.1109/tcsii.2021.3074705>.
- Jiang, C.; Guo, Y. Multi-robot guided policy search for learning decentralized swarm control. *IEEE Control Syst. Lett.* **2021**, *5*, 1177–1182. <https://doi.org/10.1109/lcsys.2020.3005441>.
- Botteghi, N.; Sirmacek, S.; Poel, M.; Stramigioli, S. Multi-agent path planning of robotic swarms in agricultural fields. *ISPRS Ann. Photogramm. Remote Sens. Spat. Inf. Sci.* **2020**, *V-1-2020*, 361–368. <https://doi.org/10.5194/isprs-annals-v-1-2020-361-2020>.
- Höglund, R.; Tiloca, M.; Selander, G.; Mattsson, J.P.; Vučinić, M.; Watteyne, T. Secure communication for the IoT: EDHOC and (group) OSCORE protocols. *IEEE Access* **2024**, *12*, 49865–49877. <https://doi.org/10.1109/access.2024.3384095>.
- Gunnarsson, M.; Brorsson, J.; Palombini, F.; Seitz, L.; Tiloca, M. Evaluating the performance of the OSCORE security protocol in constrained IoT environments. *Internet Things* **2021**, *13*, 100333. <https://doi.org/10.1016/j.iot.2020.100333>.
- Hristozov, S.; Huber, M.; Xu, L.; Fietz, J.; Liess, M. The cost of OSCORE and EDHOC for constrained devices. In Proceedings of the ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec), Abu Dhabi, United Arab Emirates, 28 June–2 July 2021; pp. 1–6. <https://doi.org/10.1145/3422337.3447834>.
- Westphall, J.; Westphall, C.; Lins, T. CoAP+DTLS cryptographic performance on an IoT scenario. In Proceedings of the IEEE Sensors Applications Symposium (SAS), Kuala Lumpur, Malaysia, 9–11 March 2020. <https://doi.org/10.1109/sas48726.2020.9220033>.
- Gunnarsson, M.; Brorsson, J.; Seitz, L.; Tiloca, M.; Höglund, R. Performance evaluation of group OSCORE for secure group communication. In Proceedings of the ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec), San Antonio, TX, USA, 16–19 May 2022. <https://doi.org/10.1145/3523064>.
- Kang, J.; Zhang, Z.; Liang, Y.; Chen, X. Autonomous navigation of agricultural robots utilizing path points and deep reinforcement learning. In Proceedings of the International Joint Conference on Neural Networks (IJCNN), Yokohama, Japan, 30 June–5 July 2024. <https://doi.org/10.1109/ijcnn60899.2024.10650416>.
- Wang, Y.; Fu, C.; Huang, R.; Tong, K.; He, Y.; Xu, L. Path planning for mobile robots in greenhouse orchards based on improved A* and fuzzy DWA algorithms. *Comput. Electron. Agric.* **2024**, *227*, 109598. <https://doi.org/10.1016/j.compag.2024.109598>.
- Stavrinidis, S.; Zacharia, P. An ANFIS-based strategy for autonomous robot collision-free navigation in dynamic environments. *Robotics* **2024**, *13*, 124. <https://doi.org/10.3390/robotics13080124>.
- Sani, E.; Sgorbissa, A.; Carpin, S. Improving the ROS 2 navigation stack with real-time local costmap updates for agricultural applications. In Proceedings of the IEEE International Conference on Robotics and Automation (ICRA), Yokohama, Japan, 13–17 May 2024; pp. 17701–17707. <https://doi.org/10.1109/icra57147.2024.10610984>.
- Martini, M.; Cerrato, S.; Salvetti, F.; Angarano, S.; Chiaberge, M. Position-agnostic autonomous navigation in vineyards with deep reinforcement learning. In Proceedings of the IEEE 18th International Conference on Automation Science and Engineering (CASE), Mexico City, Mexico, 20–24 August 2022; pp. 477–484. <https://doi.org/10.1109/case49997.2022.9926582>.

15. Aghi, D.; Mazzia, V.; Chiaberge, M. Local motion planner for autonomous navigation in vineyards with a RGB-D camera-based algorithm and deep learning synergy. *Machines* **2020**, *8*, 27. <https://doi.org/10.3390/machines8020027>.
16. Wu, H.; Wang, X.; Chen, X.; Zhang, Y.; Zhang, Y. Review on key technologies for autonomous navigation in field agricultural machinery. *Agriculture* **2025**, *15*, 1297. <https://doi.org/10.3390/agriculture15121297>.
17. Shutske, J.M.; Issa, S.F.; Johnson, T.; Khorsandi, F.; Pate, M.L.; Gorucu, S.; Walsh, J.; Yoder, A.M.; Dukes, E.; Aby, G.R.; et al. SAFER AG—Risk Assessment, Data, Design Standards, and Regulation: Needs and Recommendations. *J. Agric. Saf. Health* **2025**, *31*, 1–13. <https://doi.org/10.13031/jash.15855>.
18. Adam, M.; Hartmark, E.E.; Andersen, T.; Anisi, D.A.; Cavalcanti, A. Safety assurance of autonomous agricultural robots: From offline model-checking to runtime verification. In Proceedings of the IEEE 20th International Conference on Automation Science and Engineering (CASE), Bari, Italy, 28 August–1 September 2024; pp. 2511–2516. <https://doi.org/10.1109/case59546.2024.10711810>.
19. Lee, C.; Schätzle, S.; Lang, S.A.; Oksanen, T. Design considerations of a perception system in functional safety operated and highly automated mobile machines. *Smart Agric. Technol.* **2023**, *6*, 100346. <https://doi.org/10.1016/j.atech.2023.100346>.
20. Ma, F.; Wang, Y.; Wang, Y.; Ni, Y. Distributed averaging problems of agriculture picking multi-robot systems via sampled control. *Front. Plant Sci.* **2022**, *13*, 898183. <https://doi.org/10.3389/fpls.2022.898183>.
21. Page, M.J.; McKenzie, J.E.; Bossuyt, P.M.; Boutron, I.; Hoffmann, T.C.; Mulrow, C.D.; Shamseer, L.; Tetzlaff, J.M.; Akl, E.A.; Brennan, S.E.; et al. The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. *BMJ* **2021**, *372*, n71.
22. Hu, J.; Bhowmick, P.; Lanzon, A. A decentralized cluster formation containment framework for multirobot systems. *IEEE Trans. Robot.* **2021**, *37*, 1936–1955. <https://doi.org/10.1109/tro.2021.3071615>.
23. Starks, M.R.; Parasuraman, R. GMF: Gravitational mass-force framework for parametric multi-level coordination. In Proceedings of the IEEE International Conference on Robotics and Automation (ICRA), Atlanta, GA, USA, 19–23 May 2025. <https://doi.org/10.1109/icra55743.2025.11128543>.
24. Jayalakshmi, K.P.; Nair, V.G.; Sathish, D. MRSimEx-DSTC: A Dynamic Spanning Tree Coverage Approach for Multi-Robot Exploration and Coverage Path Planning. *IEEE Access* **2025**, *13*, 163085–163102. <https://doi.org/10.1109/access.2025.3610079>.
25. Fayaz, S.; Pawar, S.; Vigneswaran, D.; Karthikeyan, S. Automation in agricultural field using decentralised framework. In Proceedings of the IEEE International Conference on Electronics, Computing and Communication Technologies (CONECCT), Bangalore, India, 9–11 July 2021. <https://doi.org/10.1109/conecct52877.2021.9622347>.
26. Roman, J.B.; Morella, E.; Arslan, O.; de Marina, H.G. Voronoi-Based Area Coverage Algorithms: Turning Real-World Fragility into Strength. In Proceedings of the 2025 IEEE International Symposium on Multi-Robot and Multi-Agent Systems (MRS), Singapore, 4–5 December 2025; pp. 1–7. <https://doi.org/10.1109/mrs66243.2025.11357268>.
27. Smirnov, A.; Teslya, N. Robot coalition coordination in precision agriculture by smart contracts in blockchain. In *Smart Innovation, Systems and Technologies*; Springer: Singapore, 2022; Volume 247, pp. 271–283. https://doi.org/10.1007/978-981-16-3349-2_23.
28. Alsamhi, S.H.; Lee, B. Blockchain-empowered multi-robot collaboration to fight COVID-19 and future pandemics. *IEEE Access* **2021**, *9*, 44173–44197. <https://doi.org/10.1109/access.2020.3032450>.
29. Krentz, K.-F.; Voigt, T. More lightweight yet stronger: Revisiting OSCORE’s replay protection (OSCORE-NG). In Proceedings of the Workshop on Security and Privacy in Standardised IoT (SDIoTSec), San Diego, CA, USA, 14 October 2024. <https://doi.org/10.14722/sdiotsec.2024.23003>.
30. Díaz, J.; Almenarez, F. Integrating an optimised PUF-based authentication scheme in OSCORE. *Ad Hoc Netw.* **2022**, *140*, 103038. <https://doi.org/10.1016/j.adhoc.2022.103038>.
31. Abosata, N.R.A.; Al-Rubaye, S.; Inalhan, G.; Emmanouilidis, C. Lightweight payload encryption-based authentication scheme for advanced metering infrastructure. *Sensors* **2022**, *22*, 534. <https://doi.org/10.3390/s22020534>.
32. Garba, A.; Khoury, D.; Balian, P.; Haddad, S.; Sayah, J.; Chen, Z.; Al-Mutib, K. LightCert4IoTs: Blockchain-based lightweight certificates authentication for IoT applications. *IEEE Access* **2023**, *11*, 28370–28383. <https://doi.org/10.1109/access.2023.3259068>.
33. Tange, K.; De Donno, M.; Fafoutis, X.; Dragoni, N. rTLS: Lightweight TLS Session Resumption for Constrained IoT Devices. In *Information and Communications Security*; Springer: Cham, Switzerland, 2020; pp. 243–258. https://doi.org/10.1007/978-3-030-61078-4_14.
34. Lenders, M.; Gündoğan, C.; Schmidt, T.C.; Wählich, M. Securing name resolution in the IoT: DNS over CoAP. In Proceedings of the ACM Conference on Information-Centric Networking (ICN), Reykjavik, Iceland, 9–11 October 2023. <https://doi.org/10.1145/3609423>.

35. Ayub, S.; Singh, N.; Hussain, M.Z.; Ashraf, M.; Singh, D.K.; Haldorai, A. Hybrid approach to implement multi-robotic navigation system using neural network, fuzzy logic, and bio-inspired optimization methodologies. *Comput. Intell.* **2023**, *39*, 592–606. <https://doi.org/10.1111/coin.12547>.
36. Mohanty, P.K. Path planning of mobile robots under uncertain navigation environments using FCM clustering ANFIS. *Wirel. Pers. Commun.* **2024**, *137*, 1251–1276. <https://doi.org/10.1007/s11277-024-11463-y>.
37. Yang, D.; Li, X.; Yin, J.; Niu, S. Construction of novel self-adaptive dynamic window approach combined with fuzzy neural network in complex dynamic environments. *IEEE Access* **2022**, *10*, 105715–105726. <https://doi.org/10.1109/access.2022.3210251>.
38. Alzaydi, A.; Alshahrani, M.; Alqahtani, A. Advancing autonomous vehicle navigation through hybrid fuzzy-neural network training systems. *Asian J. Res. Comput. Sci.* **2024**, *25*, 309–324. <https://doi.org/10.9734/air/2024/v25i51164>.
39. Yosif, Z.M.; Hasan, M.T.; Abdulkadhim, S.M. Artificial techniques based on neural network and fuzzy logic combination approach for avoiding dynamic obstacles. *J. Eur. Syst. Autom.* **2022**, *55*, 373–380. <https://doi.org/10.18280/jesa.550306>.
40. Guan, L.; Lin, J.; Chen, B.; Guo, Y.; Xie, J. Intelligent obstacle avoidance algorithm for mobile robots in uncertain environment. *J. Sens.* **2022**, *2022*, 8954060. <https://doi.org/10.1155/2022/8954060>.
41. Jo, Y.; Son, H.I. A GNN-based decentralized path planning for agricultural robot team. In Proceedings of the International Conference on Control, Automation and Systems (ICCAS), Jeju, Republic of Korea, 29 October–1 November 2024. <https://doi.org/10.23919/iccas63016.2024.10773055>.
42. Aghi, D.; Mazzia, V.; Chiaberge, M. Deep semantic segmentation at the edge for autonomous navigation in vineyard rows. In Proceedings of the IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS), Prague, Czech Republic, 27 September–1 October 2021. <https://doi.org/10.1109/iros51168.2021.9635969>.
43. Jaquetti, P.; Lopes, H.S. Row Segmentation and Local Path Planning in Fruit Plantations using Lightweight Neural Networks. In Proceedings of the Anais do XVII Congresso Brasileiro de Inteligência Computacional (CBIC 2025), Belo Horizonte, Brazil, 1 December 2025; pp. 1–6. <https://doi.org/10.21528/cbic2025-1190697>.
44. Lobefaro, L.; Sodano, M.; Fusaro, D.; Magistri, F.; Malladi, M.V.R.; Guadagnino, T.; Pretto, A.; Stachniss, C. Spatio-Temporal Consistent Semantic Mapping for Robotics Fruit Growth Monitoring. *IEEE Robot. Autom. Lett.* **2025**, *10*, 9470–9477. <https://doi.org/10.1109/lra.2025.3594985>.
45. Eiffert, S.; Wallace, N.D.; Kong, H.; Pirmarzashti, N.; Sukkarieh, S. Resource and response aware path planning for long-term autonomy of ground robots in agriculture. *Field Robot.* **2022**, *2*, 1–33. <https://doi.org/10.55417/fr.2022001>.
46. Rodić, A.; Kljajić, J. Motion planning of tree fruit robot picker in presence of obstacles using heuristic approach. In Proceedings of the IEEE International Symposium on Applied Computational Intelligence and Informatics (SACI), Timișoara, Romania, 23–26 May 2024. <https://doi.org/10.1109/saci60582.2024.10619767>.
47. Felske, M.; Redenius, J.; Happich, G.; Schöning, J. Towards an Agricultural Operational Design Domain: A Framework. *Smart Agric. Technol.* **2026**, *14*, 102246. <https://doi.org/10.1016/j.atech.2026.102246>.
48. Kumar, A.; Bagalwadi, S. Ensuring Functional Safety and SOTIF for Autonomous Off-Highway Vehicles: Addressing Risks in Complex Systems. In *SAE Technical Paper Series*; SAE International: Warrendale, PA, USA, 2025. <https://doi.org/10.4271/2025-28-0315>.
49. Zhou, R.; Zhang, Z.; Han, H.; Zhang, X.; Chen, Z.; Sun, J.; Shen, Y.; Xu, D. RSFuzz: A Robustness-Guided Swarm Fuzzing Framework Based on Behavioral Constraints. In Proceedings of the 2025 40th IEEE/ACM International Conference on Automated Software Engineering (ASE), Seoul, Republic of Korea, 16–20 November 2025; pp. 495–507. <https://doi.org/10.1109/ase63991.2025.00048>.
50. Katikaridis, D.; Benos, L.; Busato, P.; Kateris, D.; Papageorgiou, E.I.; Karras, G.; Bochtis, D. Experimental Comparative Analysis of Centralized vs. Decentralized Coordination of Aerial–Ground Robotic Teams for Agricultural Operations. *Robotics* **2025**, *14*, 119. <https://doi.org/10.3390/robotics14090119>.
51. Aby, G.R.; Shutske, J.M.; Schwab, J.P. Safety risk assessment of an autonomous agricultural machine. *J. Agric. Saf. Health* **2024**, *30*, 87–104. <https://doi.org/10.13031/jash.15756>.
52. Muthusamy, S. Hybrid Safety Framework for Autonomous Off-Highway Vehicles. In *SAE Technical Paper Series*; SAE International: Warrendale, PA, USA, 2025. <https://doi.org/10.4271/2025-28-0325>.
53. Kelly, J.; Zafar, S.A.; Heidemann, L.; Zacchi, J.-V.; Espinoza, D.; Mata, N. Navigating the EU AI Act: A Methodological Approach to Compliance for Safety-Critical Products. In Proceedings of the 2024 IEEE Conference on Artificial Intelligence (CAI), Singapore, 25–27 June 2024; pp. 979–984. <https://doi.org/10.1109/CAI59869.2024.00179>.
54. Butt, T.A.; Iqbal, M.; Arshad, N. From Policy to Pipeline: A Governance Framework for AI Development and Operations Pipelines. *IEEE Access* **2026**, *14*, 1373–1397. <https://doi.org/10.1109/access.2025.3647479>.

55. Kim, D.; Park, S.W.; Park, J.W. EGIS: A Resilient and Recoverable Dual-Brain Controller Architecture for Physical AI Systems under the EU AI Act. In Proceedings of the 2025 25th International Conference on Control, Automation and Systems (ICCAS), Incheon, Republic of Korea, 4–7 November 2025; pp. 2212–2217. <https://doi.org/10.23919/iccas66577.2025.11301361>.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.