The Cybersecurity and Operational Resiliency Challenges in Agriculture.

Rami Riashy | March 3 2026

North America Automotive Consulting Principal | NCC Group

The Cybersecurity and Operational Resiliency Challenges in Agriculture.

Introduction and Executive Summary:

My name is Rami Riashy, and I have brought over two decades of hands-on experience at the intersection of transportation technology and cybersecurity. My journey began in automotive, where I spent 10 years immersed in systems engineering and validation, working across OEMs and Tier 1 suppliers to bring complex vehicles and their electrical components together. I then shifted gears into the heavy-duty trucking world, leading global homologation efforts and ensuring electrical systems met rigorous standards across international markets. For the next eight years, I dove deep into agriculture, helping a major OEM architect and secure next-generation machine networks, conduct threat analysis and risk assessments (TARAs), and carry out penetration testing on cyber-physical systems critical to the food supply chain. Today, I work as a cybersecurity consultant at NCC Group helping clients “shift left” by building assurance cases, threat models, and test strategies that integrate cybersecurity from the earliest phases of design. This paper reflects the sum of that experience across industries, applied to one of the world’s most essential domains: agriculture.

Modern civilization depends on a stable, resilient, and secure food supply. From rural farms to urban supermarkets, agriculture forms the backbone of human survival and economic stability. Disruptions in planting, harvesting, storage, or distribution can trigger cascading effects, shortages, price spikes, civil unrest, and geopolitical tensions. As the sector digitizes through precision agriculture, cloud-connected equipment, and autonomous machinery, its cyber-physical vulnerabilities have grown exponentially. Securing agriculture is no longer just about safeguarding crops; it’s about defending a global system that feeds billions.

Agriculture is amid a digital transformation. Precision farming, autonomous tractors, and cloud-connected equipment are reshaping how food is grown and delivered. Yet this technological advancement introduces a new risk landscape, Cybersecurity. Unlike traditional enterprise IT systems and the closely correlated automotive industry, agricultural environments are defined by offline operations, legacy machinery, seasonal usage, and multiband ecosystems. These unique conditions demand a tailored cybersecurity approach that balances innovation, safety, and resilience.

This white paper explores the distinct threat model in agriculture, presents representative damage scenarios, highlights ongoing industry efforts to mitigate risk, and outlines the strategic role of various stakeholders. Drawing on insights from leading OEMs, standards bodies, and government discussions, it argues for a unified, forward-thinking security framework to protect the future of food systems.

Acronyms and Abbreviations

Glossary

References

Scope: Agriculture as a Cyber-Physical System

For many outside the agricultural sector, the image of farming may still evoke analog machinery and manual labor. Modern agriculture is one of the most technologically advanced industries on the planet. From autonomous tractors and GPS-guided planters to cloud-based fleet management platforms, precision drone spraying, real-time soil telemetry, AI-driven irrigation optimization, and automated protein production systems, agriculture is now a highly digitized, interconnected ecosystem. The production, storage, distribution, and export of food rely on complex integrations between embedded systems, wireless networks, sensors, edge computing, and cloud infrastructure.

This vast digital transformation supports a full lifecycle, from seed genetics and crop modeling, through planting, growth, and harvesting, to logistics, market pricing, and sustainability tracking. Every link in the chain has become a potential cyber-physical interface and risks a potential point of failure or exploitation.

While backend systems, cloud platforms, dealer networks, and manufacturing infrastructure all play critical roles in modern agriculture, machinery stands apart as the **most immediate point of impact** in the physical world, and the focus of this paper. It is machinery, tractors, combines, sprayers, and autonomous implements that directly interact with soil, seed, and harvest. Machinery operates under unique constraints: offline environments, mixed-brand interoperability, decades-long lifecycles, and real-time safety-critical control. These factors make machinery both **technically challenging and strategically urgent** to secure. As such, while cybersecurity across the agri-tech ecosystem is important, the focus on agricultural machinery is essential, because it is where cyber threats most tangibly become yield losses, safety risks, and food supply disruptions.

Agricultural equipment is part of the broader machinery and off-highway sector and increasingly shares technology with the automotive industry such as CAN-based communication, ECUs, telematics, and OTA update capabilities. As a result, agricultural platforms can benefit from cybersecurity standards and practices developed in automotive, like ISO/SAE 21434 and UNECE R155/R156. However, agriculture presents a **distinct threat landscape**: machines often operate in remote, intermittently connected environments; they are used across multi-brand mixed fleets; they may go decades without updates; and they are tightly coupled to seasonal cycles where failure during a critical window (e.g., planting or harvest) can cause massive financial loss. Moreover, agriculture's centrality to food production introduces risks tied not just to safety or IP theft, but to economic stability and national security. These differences demand a tailored approach to cybersecurity in agriculture.

Agricultural platforms face unique challenges:

Unlike traditional IT systems, agricultural platforms face a set of unique operational and cybersecurity challenges shaped by their physical environments, usage cycles, and interoperability requirements. These machines are often tasked with **safety-critical functions** such as braking, steering, or controlling automated implements like balers and sprayers, where a failure could pose real physical danger to operators, livestock, or bystanders, especially when equipment travels on public roads between farms.

Connectivity is another hurdle: much of the agricultural landscape lies beyond reliable access to cellular, satellite, or Wi-Fi networks, making **real-time patching, cloud-based authentication, and telemetry infeasible** during operation. Many modern applications depend heavily on **precision positioning**, with sub-inch accuracy from RTK-GPS or GNSS systems enabling tasks like autonomous tillage, variable-rate seeding, and targeted spraying; GPS spoofing or jamming could therefore lead to costly agronomic errors or safety incidents. Adding to the complexity is the **multi-brand reality of most farms**, where equipment from different OEMs, such as a John Deere tractor pulling a CNH planter using an AGCO sprayer, must interoperate reliably through standardized protocols, greatly expanding the attack surface.

Compounding these risks is the long lifespan of agricultural equipment: most machines remain in service for **20 to 40 years**, often well beyond support windows, with many never receiving a firmware update. Finally, the **seasonal nature of farming** introduces extreme time pressure; delays during narrow planting or harvest windows (even for a few hours) due to failed updates or security lockouts can lead to significant financial losses. These realities require a cybersecurity approach that prioritizes **resilience, offline functionality, and interoperability** across a fragmented, aging, and safety-critical ecosystem.

- **Safety-Critical Machine Control**
- **Intermittent or No Connectivity**.
- **Precision Positioning Dependency**
- **Multi-Brand, Mixed Fleet Compatibility**
- **Decades-Long Service Lifecycles**
- **Seasonal Time Pressure and Usage Cycles**

Agriculture vs Automotive: Key Differences in Cybersecurity & Tech

While agriculture and automotive industries increasingly share technology platforms, such as CAN-based networks, telematics units, ECUs, and even regulatory frameworks, their **operating environments and risk profiles are fundamentally different**. Automotive systems are designed for mass production, centralized maintenance networks, and daily usage by consumers in connected environments. By contrast, agricultural equipment often operates in **remote, offline conditions**, with machines that may only be used intensively for a few weeks each year yet are expected to remain functional for **20 to 40 years**. This dramatically alters the assumptions around software update cycles, telemetry availability, and secure lifecycle management.

Agricultural machines also face **unique technical and interoperability challenges**. While a car functions as a mostly self-contained system, a modern tractor must work in plug-and-play fashion with implements, such as planters, sprayers, or balers from different manufacturers. This **multi brand ecosystem** requires robust standards for authentication, secure communication, and compatibility across platforms not designed in unison. Moreover, **time-critical operations** like planting and harvest introduce seasonal windows where failure, even for a few days, could result in major economic loss. Whereas automotive cybersecurity often prioritizes safety, privacy, and performance, agricultural cybersecurity must also prioritize **resilience, offline operability, and cross-vendor trust**, characteristics rarely addressed by traditional IT or automotive paradigms.

The table below draws the comparison between Agriculture and Automotive

Category	Agriculture	Automotive
Connectivity	Frequently offline; rural/remote fields often lack reliable cellular or satellite	Assumed always connected; urban LTE/5G access is standard
Lifecycle Length	Equipment stays in use for 20-40 years; legacy systems persist	10-15 years typical; consistent refresh of tech stack
Update Windows	Seasonal; cannot risk updates during planting/harvest windows	Can update overnight or when parked; more flexibility
User Type	Operators are often non-technical; no dedicated IT/security staff on-site	End users are consumers; maintenance via dealership or fleet

Category	Agriculture	Automotive
Mission Criticality	Machine failure can cause **crop loss, injury, or missed harvest**	Failure could be safety-critical (crash) but mostly end-user convenience-driven
Machine Ecosystem	Highly modular; **multi-brand machines** must interoperate in-field (tractor + implement)	Vertically integrated; OEM has full control of system design
Cybersecurity Maturity	Emerging focus; historically limited investment in security	Mature programs due to UNECE R155/R156, ISO 21434, and widespread regulation
Sensor / Tech Stack	GPS/GNSS with **RTK correction**, soil sensors, yield monitors, drone data	LiDAR, radar, ultrasonic, camera fusion for ADAS/AV
OTA Expectations	OTA is desired but difficult due to poor connectivity and long idle periods	OTA is expected for infotainment, diagnostics, and increasing vehicle functions
Market Regulation	Now facing EU CRA and Machinery Regulation, but largely self-regulated until recently	R155/R156 mandatory for UNECE markets since 2022
Threat Actors	Nation-states (food security), ransomware groups, competitors, activists	Nation-states, criminals, insiders, hacktivists
Data Sensitivity	Yield forecasts, planting patterns, soil health, IP (seed genetics), supply chain timing. Fleet position.	Location history, driver behavior, infotainment usage, V2X interactions
Telemetry Usage	Agronomic analysis, fleet management, input optimization	Predictive maintenance, insurance, infotainment personalization

Similar to automotive, these factors necessitate a cybersecurity strategy rooted in resilience, interoperability, and lifecycle-aware design. Agriculture-specific use cases, from offline operations to mixed-fleet environments, demand tailored regulatory approaches that reflect the sector's unique realities

Global and Regional Cybersecurity Regulations Impacting Agriculture and Emerging Standards ("branch off" from Automotive)

Agricultural machinery is increasingly falling under the scope of cybersecurity-related regulations originally developed for other sectors, particularly automotive and industrial equipment. While frameworks like the **EU Cyber Resilience Act (CRA)** and **UNECE R155** were not designed with agriculture in mind, their broad definitions of digital products and connected systems are creating ripple effects throughout the supply chain. As a result, agricultural OEMs must begin aligning with these mandates, despite their unique constraints.

One of the key challenges for agricultural OEMs is the **fragmented and lower-volume supply base**, which lacks the bargaining power and tooling maturity of the automotive sector. Many Tier 1 and Tier 2 suppliers serve both domains but prioritize automotive due to scale and regulatory urgency. CRA poses a disproportionate burden for agricultural manufacturers, who must comply without the economies of scale or cybersecurity staff found in high-volume vehicle production.

To address this gap, a new sector-specific standard is in development: **ISO 24882 – Agricultural machinery, tractors, and earth-moving machinery – Product cybersecurity**. This draft ISO standard is being developed under **ISO/TC 23/SC 19** and aims to define cybersecurity engineering processes for the entire lifecycle of electrical/electronic (E/E) systems in agricultural and off-road machinery. It complements safety standards like **ISO 25119** and draws inspiration from ISO/SAE 21434 but adapts to agriculture's realities, such as offline operation, long service life, and multi brand interoperability.

ISO 24882 will provide structured guidance for threat modeling, secure software and hardware interfaces, lifecycle maintenance, and system decommissioning. It is expected to become the cornerstone for harmonizing regulatory compliance in agriculture and empowering OEMs and suppliers with a common vocabulary and risk management approach. For an industry as critical as food production, the emergence of ISO 24882 signals a timely step toward resilient, secure machinery design.

Cybersecurity in agriculture is increasingly influenced by **regulatory requirements**, especially as agricultural machinery becomes more connected, autonomous, and software driven. While there is **no single global cybersecurity regulation** specific to agriculture yet, the sector is increasingly subject to a **patchwork of applicable frameworks and evolving legislation**. Here's a breakdown of the **most relevant cybersecurity regulatory requirements and standards** that impact agriculture today

ISO 24882 – Cybersecurity for Agricultural and Earth-Moving Machinery (Draft)

- **Applies to**: Agricultural and off-road equipment manufacturers.
- **Relevance**: This emerging standard is purpose-built for agriculture, adapting concepts from ISO 21434 to fit the realities of rural, mixed-brand, and long-lifecycle machines.
- **Scope**: Covers cybersecurity engineering across the full product lifecycle—from concept to decommissioning.
- **Cause**: Recognizes that general vehicle standards do not fully address agriculture's unique operational, environmental, and interoperability needs.
- **Impact**: Provides a common language and structure for OEMs and suppliers to align on cybersecurity expectations, testing, and system design.
- **Timeframe**: **In Draft** (ISO/TC 23/SC 19); **publication anticipated following completion of committee review.**

EU Cyber Resilience Act (CRA) Europe, upcoming enforcement

- **Applies to**: Manufacturers of connected products, including machinery with digital components (most ECU's)
- **Relevance**: Agricultural equipment with connectivity (e.g., telematics, OTA, or IoT) will fall under CRA scope.
- **Key Requirements**:
  - Security-by-design and by-default (HSM, Secure Boot, etc)
  - Vulnerability handling and disclosure
  - Regular security updates for the expected lifecycle
  - Conformity assessments (potentially including CE marking updates)
- **Challenge**: Many agricultural machines are not designed with lifecycle patching or secure development processes, making CRA compliance a paradigm shift.

- **Timeframe**: **Adopted April 2024**, enforcement expected to begin **2027 (36-month transition period)**

UNECE Regulation No. 155 (R155) Global adoption beyond UNECE countries

- **Applies to**: Automotive vehicles (originally), but also relevant to agricultural machinery manufacturers operating in countries that adopt UNECE regulations.
- **Relevance**: Many ag OEMs (e.g., John Deere, CNH, AGCO) use vehicle-derived components; R155 compliance practices are bleeding into off-highway sectors.
- **Key Requirements**:
    - Cybersecurity Management System (CSMS)
    - Threat and Risk Assessment (TARA)
    - Lifecycle risk management
    - Type approval based on cyber readiness
- **Timeframe**: **In force since July 2022** for vehicle type approvals; applicable by extension to Ag OEMs following UNECE alignment

ISO/SAE 21434 – Cybersecurity Engineering (Standard) for Road Vehicles

- **Applies to**: OEMs, Tier 1s, and software suppliers building components for vehicles, including tractors and off-road vehicles.
- **Relevance**: Agriculture shares many systems with automotive (ECUs, CAN, OTA); many Agriculture manufacturers are using ISO 21434 as a foundational engineering process even without legal obligation.
- **Key Standards and Sections**:
    - Security goals and claims
    - Threat modeling (TARA)
    - Cybersecurity assurance levels (CALs)
    - Post-production monitoring
- **Timeframe**: **Published in August 2021**; widely adopted since 2022

EU Machinery Regulation (2023/1230) *Supersedes Machinery Directive*

- **Applies to**: Machinery placed on the EU market, including digital or autonomous machines.
- **Relevance**: Sets functional safety and cybersecurity requirements for intelligent machinery, including agricultural robots and smart implements.
- **Key Requirements**:
  - Cyber threats must not lead to hazardous behavior
  - Safety-related software must be secure against tampering or manipulation
- **Timeframe**: **Adopted in June 2023**; **mandatory from January 20, 2027**

U.S. Executive Orders & NIST Cybersecurity Framework (CSF)

- **Applies to**: Not mandatory for private ag firms but increasingly used by large U.S. agribusinesses and suppliers to guide best practices.
- **Relevance**:
  - U.S. agriculture is designated as part of the **16 critical infrastructure sectors**
  - NIST CSF is often used for internal governance, especially for companies supplying the USDA, Department of Energy, or food logistics sectors.
- **Timeframe**: **Current version 1.1 in use**, **Version 2.0 released in February 2024**

NIS2 Directive (EU 2022/2555) – Revised Network and Information Security Directive

- **Applies to:** Essential and important entities across the EU, including food production, agricultural machinery manufacturing, and agri-tech services.
- **Relevance:** Agriculture is recognized as a critical infrastructure domain under NIS2, particularly in areas related to food supply, smart machinery, and digital platforms. Agri-tech providers and OEMs with EU operations may fall under NIS2 obligations.
- **Key Requirements:**
  - Cyber risk management and governance across IT and OT systems.
  - Mandatory incident reporting within 24 hours of detection for significant incidents.

    - Supply chain risk assessments and third-party security enforcement.
    - Technical and organizational measures, including secure system design and regular vulnerability handling.
- **Challenge:** Many agricultural organizations, especially smaller suppliers or service providers, may lack formal cybersecurity programs or governance structures. NIS2 imposes significant penalties and oversight, pushing ag-sector companies to mature quickly.
- **Timeframe: Effective January 2023; must be implemented in national law by October 2024**

Food and Agriculture Sector-Specific Plan (U.S. DHS & USDA)

- **Applies to**: National-level food production and agricultural systems.
- **Relevance**: Encourages public-private collaboration and cyber preparedness in agricultural infrastructure (including processors, elevators, and major farms).
- **Key Requirements or Themes**:
    - Resilience to cyber and physical threats
    - Secure supply chains
    - Critical data protection
- **Timeframe**: **Updated periodically**; current revision aligned with **DHS 2023 CISA guidance**

Industry & Certification Standards

- **AEF ISOBUS Conformance Testing** (Agricultural Industry Electronics Foundation): Ensures secure interoperability between machines and implements from different OEMs.
- **TIM Certificates and PKI Infrastructure**: Provides secure authentication between tractor and implement pairs.
- **ISO 11783 (ISOBUS):** Defines communication protocols for electronic systems on tractors and implements. While not a cybersecurity standard per se, its secure and deterministic data exchange is foundational for future secure implementations.

- **ISO 25119 (Functional Safety for Ag Machinery):** Sets out safety requirements for control systems on agricultural and forestry machinery. Increasingly intersects with cybersecurity, especially where safety functions are software driven.
- **ISO 24089 (Software Update Engineering for Road Vehicles):** Though automotive-focused, this standard is gaining attention in agriculture for managing OTA updates securely and traceably, critical for field-deployed equipment.
- **ISO 24882 (Draft – Cybersecurity for Agricultural and Forestry Machinery):** A new agriculture-specific cybersecurity standard in development to address the sector's unique threat models, long service life, offline use, and mixed-fleet operations.
- **SAE J1939-91C (Secure Onboard Communication Protocol)**: Adds encryption and message authentication to CAN-based systems, being explored in agriculture to prevent spoofing and tampering of machine messages.
- **SAE J3061**: Cybersecurity guidebook for cyber-physical systems (used in ag as a complement to ISO 21434).

As these regulations evolve, ISO 24882 will likely become the cornerstone standard for harmonizing ag machinery cybersecurity, bridging gaps between automotive-derived regulation and agriculture's real-world operational context.

Threat Landscape in Agriculture

The cybersecurity threat landscape in agriculture extends far beyond the machines operating in fields and must account for the full **cyber-physical ecosystem**. While the cyber-physical vulnerabilities of autonomous tractors, sprayers, and harvesters are pressing, the broader digital ecosystem, spanning cloud infrastructure, dealer networks, manufacturing plants, and diagnostic tools represents an equally critical attack surface.

Distinctive Threat Model

In summary, agricultural vehicles and machines are the most visible cyber-physical targets, but their **true risk profile** can only be understood by viewing them within a **broader ecosystem of cloud, dealer, service, and manufacturing infrastructure**. Attacks can originate from any layer and ripple through the entire supply chain.

A unique dimension of the agricultural cybersecurity threat landscape involves the **intersection of policy, ownership rights, and system security**. The **Right to Repair movement**, which seeks to give farmers and independent technicians access to diagnostic tools, software, and repair capabilities, has sparked considerable controversy. While manufacturers cite cybersecurity, safety, and intellectual property as reasons to limit access, many operators argue that restrictions undermine equipment usability, increase downtime, and infringe on ownership rights. This tension introduces **a new form of risk**: adversarial repair practices, unauthorized firmware modifications, or the use of unofficial service tools that bypass built-in security controls. In this context, **security controls may be perceived as barriers**, leading to unintended behaviors that weaken system integrity. Balancing cybersecurity enforcement with usability and repairability is essential to avoid misalignment between operators, OEMs, and regulators. Agricultural Vehicles & Machines (Edge Assets)

Modern tractors, sprayers, combines, and implements are no longer standalone mechanical tools; they are mobile, cyber-physical platforms loaded with ECUs, GNSS receivers, ISOBUS interfaces, cellular modems, and even vision-based AI systems.

Key threats may include:

- **ECU manipulation** (e.g., spoofing or overriding implement controls)
- **Telematics hijacking** via cellular or Wi-Fi interfaces
- **GNSS spoofing/jamming**, causing navigational or agronomic errors
- **Firmware attacks** on CAN-connected devices (e.g., planter controllers)
- **Denial of service** during critical field windows (planting, harvest)

These machines are also often operated in **offline or low-connectivity environments**, complicating patch management and real-time intrusion detection.

Backend Platforms & Data Infrastructure

These machines often sync with cloud platforms for:

- Yield tracking
- Fleet logistics
- Maintenance schedules
- Agronomic decision support

A compromise in the backend can result in:

- Location and position of machines
- Stolen or manipulated field data

- Cloud-side OTA attacks
- Business disruption (e.g., locked-out fleets or users)

Dealer Networks & Service Tools

Dealerships play a critical role in:

- Right to Repair
- Provisioning and activating equipment
- Applying updates and calibrations
- Diagnosing and maintaining mixed-fleet systems

They often use USB storage devices, service laptops, or web portals with privileged access, all potential cyberattack vectors, especially if physical security is lax or endpoints are poorly hardened.

Operational Technology & Manufacturing

Agricultural OEMs rely on connected assembly lines and embedded software supply chains. A breach here could:

- Delay critical machine production
- Infect ECUs or displays before delivery
- Compromise over-the-air software before deployment

Agricultural cybersecurity machinery must contend with a **distinct threat landscape** shaped by environmental, operational, and business realities unlike those in traditional enterprise or automotive domains. A central challenge for Agricultural machinery is **offline operation**, many machines work in remote fields without consistent connectivity to cellular, Wi-Fi, or satellite networks. This makes real-time patching, over-the-air authentication, and cloud-based monitoring unreliable or not feasible. Security solutions must therefore be designed with **autonomous resilience** in mind, able to detect and respond to threats without relying on a live connection to the cloud. Compounding this is the **long equipment lifecycle** common in agriculture: tractors, sprayers, and implements often remain in use for 20–30 years or more, well beyond the support lifespan of embedded operating systems or cryptographic components. In many cases, these legacy machines will never receive a firmware update, leaving persistent vulnerabilities that attackers could exploit long after they are discovered.

Interoperability adds another layer of risk. Unlike consumer vehicles, agricultural equipment is often used in **multi-brand environments**, where a John Deere tractor might operate alongside a CNH planter or an AGCO sprayer. These machines must communicate securely across **standardized protocols like ISOBUS**, yet differences in implementation, certificate management, or update cadence can introduce mismatched security postures and attack surfaces. All of this unfolds in a **time-critical, safety-sensitive context**: many ag tasks are seasonal and must occur in narrow windows, such as planting before the rains or harvesting before frost. A single point of failure, a lockout from failed authentication, or a misconfiguration caused by a cyber event could delay operations by hours or days, resulting in **severe economic loss** or even **legal liability** if equipment failure causes injury or crop damage. These realities demand a threat model grounded in **resilience, interoperability, and lifecycle-aware design**, not assumptions inherited from always-connected, short-lifecycle IT or automotive platforms.

Threat Actors and Motivations

The agricultural sector is increasingly vulnerable to a diverse range of **threat actors**, each motivated by distinct incentives, but all capable of disrupting critical systems. **Nation-state actors** may seek to infiltrate agricultural networks to gain early insight into crop yields, manipulate global commodity markets, or sabotage food infrastructure as a form of economic or geopolitical leverage. **Cybercriminals**, drawn by the high-value, time-sensitive nature of agriculture, frequently deploy **ransomware** against grain elevators, food processors, and cooperatives, knowing that any disruption during harvest or distribution can force quick payouts (Food and Ag-ISAC reports 84 incidents in Q1 2025 and 212 incidents in 2024; FBI alerts note multiple grain cooperative attacks). **Insiders**, whether disgruntled employees or third-party contractors, pose a persistent risk of **configuration tampering**, **intellectual property theft**, or intentional system sabotage. Meanwhile, **hacktivists** targeting GMOs, industrial farming practices, or environmental concerns may attempt to deface systems, leak sensitive data, or interfere with operations in protest. Lastly, **opportunistic attackers** and hobbyist hackers may exploit vulnerabilities simply to demonstrate their capability or to **resell compromised equipment** on secondary markets. Together, this varied threat landscape makes clear that agricultural cybersecurity must account not just for technical risk, but for the **broad spectrum of human intent** behind cyber intrusions.

Actor Class	**Motivation**
Nation-State	Gain Agriculture intelligence, manipulate markets, or sabotage infrastructure.
Cybercriminals	Ransomware attacks targeting processors, elevators, and co-ops.
Insiders	Unauthorized configuration changes, IP theft, or malicious actions.
Hacktivists	Ideological motives targeting GMOs or industrial farming.
Opportunists	Trophy hacks and resale of stolen equipment.

Agriculture threat actors operate across a **broader surface area**, targeting not just machinery, but also **farm management software**, **cloud agronomy services**, **dealer service portals**, **OEM support systems**, and **food supply chain nodes**. Unlike automotive, where **vehicles and customer safety** are typically the primary focus, agriculture adversaries often aim to disrupt **production, logistics, and economics**, all of which tie directly into **national food security**.

Exploiting Agricultural Data: Economic and Strategic Risks

Agricultural data is not only sensitive, but also economically and geopolitically powerful. Yield estimates, crop models, soil telemetry, and fleet activity are increasingly digitized and stored in cloud platforms. This creates multiple vectors for malicious exploitation:

Market Manipulation via Crop Forecasting

- Early access to regional yield or planting data enables actors to “short” futures markets, speculate on price shifts, or destabilize national reserves.
- Sophisticated actors may monitor field-level data via satellite, drone feeds, or compromised IoT platforms to gain unfair economic advantage.

Competitive Espionage Between Agribusinesses

- Unauthorized access to hybrid seed performance, soil analytics, or application algorithms can give one firm a strategic advantage over another.
- De-anonymization of "public" data through land registries or crop reports is increasingly possible.

Data Poisoning and Yield Manipulation

- Attackers may manipulate agronomic models or telemetry to cause harmful over-fertilization, mistimed irrigation, or poor planting schedules.
- Such attacks are subtle, hard to detect, and may appear as natural variability.

The intelligence value of agricultural data now rivals its economic value. Precision agriculture has created precision targets. Detailed telemetry on yield forecasts, planting patterns, and soil conditions can offer early insight into global food supply trends, information that can be exploited to gain unfair advantage in commodity markets or used to shape geopolitical strategies. For adversaries, this data becomes a lens into a nation's resource security and trade posture. For cybercriminals, it's a high-value asset that can be sold, ransomed, or used to manipulate pricing. And for competitors, unauthorized access to proprietary agronomic models or hybrid seed performance can erode years of R&D investment in a single breach. In this environment, **protecting data** is no longer just a matter of privacy, it is central to safeguarding economic leverage, national resilience, and global food stability

Notable Cybersecurity Incidents in Agriculture

As agriculture becomes increasingly digitized and interconnected, it has also become a more attractive and vulnerable target for cyberattacks. Once considered too low-tech or fragmented to warrant concern, the sector now relies on complex systems spanning cloud-connected machinery, precision data platforms, and time-sensitive logistics networks. This convergence of operational technology (OT) and information technology (IT), often deployed in remote or intermittently connected environments, creates unique challenges for security and incident response. The consequences of cyberattacks in agriculture are not just technical, they are operational, economic, and even geopolitical. In recent years, a few high-profile incidents have demonstrated just how disruptive and far-reaching these attacks can be.

JBS Foods Ransomware Attack (2021)

- **What happened**: JBS, one of the world's largest meat suppliers, suffered a ransomware attack disrupting operations in the U.S., Australia, and Canada.
- **Impact**: JBS paid $11 million in ransom; beef and pork prices spiked due to supply chain interruptions.
- **Takeaway**: Agribusiness is a high-value target for ransomware groups.

John Deere Firmware Vulnerabilities (2022–2023)

- **What happened**: Security researchers revealed vulnerabilities in Deere's firmware and APIs that could allow remote access and data exfiltration.
- **Impact**: Sparked right-to-repair debates and raised awareness of security weaknesses in ag equipment.
- **Takeaway**: OEMs must proactively engage with researchers and invest in secure design.

Ukraine Equipment Disablement (2022)

- **What happened**: John Deere tractors stolen during the Russian invasion were remotely disabled via OEM-controlled software.
- **Impact**: Highlighted the strategic power and ethical questions of remote machine control in conflict zones.
- **Takeaway**: Offline disablement mechanisms must be transparent, ethical, and secure.

Harvest Co-Op Ransomware Attack (2018)

- **What happened**: The New Cooperative grain co-op in Iowa experienced ransomware just before harvest.
- **Impact**: Grain delivery and elevator operations were disrupted during peak harvest window.
- **Takeaway**: Time-sensitive agricultural infrastructure is highly vulnerable to disruption.

The Marks & Spencer Cyberattack (2025)

- **What happened:** Marks & Spencer suffered a highly targeted cyberattack in April 2025 involving ransomware and data exfiltration. Attackers gained access through social engineering and a third-party contractor, encrypting systems and stealing customer and employee data.
- **Impact:** Online ordering for food and other goods was suspended for over 45 days. Contactless payments, inventory, and logistics systems were disrupted, forcing many stores to revert to manual processes. The company estimated losses of £300 million.

- **Takeaway:** Even well-resourced retailers with digital infrastructure are vulnerable to attacks via third-party services and social engineering. The cascading impact on customer trust, operations, and supply chains underscores the critical need for resilient architecture and third-party security governance.

Damage Scenarios and Potential Impacts

Understanding the cybersecurity threat landscape in agriculture requires moving beyond abstract risks and into tangible, real-world scenarios. Unlike many IT systems where data breaches are the primary concern, agricultural cyber incidents can result in **direct physical, operational, and financial harm**. From misconfigured automated tractors or implements to disabled harvesters or corrupted agronomic models, even a single exploit can jeopardize crop yields, worker safety, or supply chain continuity. These systems are not theoretical, they operate in time-sensitive, safety-critical, and often offline environments. The following damage scenarios illustrate how vulnerabilities in connected agricultural platforms could lead to significant disruptions with cascading effects across farms, regions, and markets.

System	Threat	Scenario	Impact
Tractor to Implement Pairing	Certificate spoofing	Fail-to-start or misconfiguration	Crop loss, service delay
Autonomous Implements	Runtime injection	Unintended movement or damage	Safety risk, legal exposure
Cloud Interfaces	Data manipulation	False agronomic analysis	Financial loss, misapplication
High-Value Combines	Remote disablement	Lockout during harvest	Multi-million-dollar impact
Legacy Equipment	No connectivity	Unable to patch or authenticate	Persistent vulnerabilities

Position System	Spoofing or manipulation	Unable to authenticate due to multiple correction services	Guidance system Error, Efficiency loss, Harvest or Plant Sabotage

Ongoing Mitigation Efforts

The risks facing modern agriculture are not hypothetical, they are already present in the field. From spoofed GNSS signals to ransomware attacks against cooperatives and firmware vulnerabilities in smart machinery, the **threat surface is expanding in parallel with innovation**. As automation becomes more advanced and machinery more interconnected, the potential impact of a successful cyber-attack only grows, affecting not just individual farms but entire supply chains, market prices, and even national food security. In response, the industry has begun to invest in proactive cybersecurity measures tailored to agriculture's unique environment. Initiatives like **TIM Command** provide authenticated, certificate-based control between tractors and implements, ensuring only trusted devices can execute machine-critical functions. Cross-OEM interoperability testing, runtime cryptographic validation, and emerging cloud-to-cloud security standards are helping to reinforce trust across brands and platforms. These mitigation efforts represent a crucial step forward, but they also highlight the sector's growing recognition that **cybersecurity is no longer optional, it is foundational to the safe, resilient operation of precision agriculture.**

TIM Certificates and PKI Framework

- Mutual authentication between tractors and implements
- Digital certificates tied to specific functional capabilities
- Offline-capable trust validation

AEF Conformance and Interoperability Testing

- Cross-OEM conformance labs simulating field conditions
- Required protocol testing before deployment

Runtime Security and Cryptographic Controls

- Planned runtime signing and message validation (CoC)
- Need for HSM integration across ECU platforms

Cloud-to-Cloud Data Exchange Standardization (EIN)

- Shared security architecture for cross-brand cloud environments
- Enables farmer-controlled fleet visibility

Securing GNSS Corrections and Positioning Integrity

- Encrypted and authenticated correction services (e.g., RTK over TLS, Galileo OSNMA) are being deployed to protect against GPS spoofing, jamming, and manipulation of autonomous machinery.
- Sensor fusion and multi-constellation receivers improve resilience, but legacy equipment and unsecured base stations still present vulnerabilities in positioning-dependent ag systems.

Stakeholder Responsibilities

Securing the agricultural ecosystem is a shared responsibility. Unlike centralized IT systems, agriculture involves a **decentralized and highly interoperable environment**, with equipment, data, and infrastructure spanning across OEMs, implement manufacturers, farmers, cloud providers, standards bodies, and regulators. Each stakeholder plays a distinct role, not only in protecting their own assets, but in upholding trust and safety across the entire supply chain. As cyber threats grow more sophisticated and the sector becomes increasingly digitized, **clear accountability and coordinated action** among these actors becomes essential. The following matrix outlines the key responsibilities of each stakeholder group in advancing agricultural cybersecurity.

Stakeholder	Role	Security Responsibilities
OEMs	Design tractors and systems	Secure firmware, HSMs, OTA processes
Suppliers	Secure Components	Secure firmware, HSMs,
Implement Manufacturers	Produce balers, planters, sprayers	Certificate compliance, ISOBUS integration
Farmers	End users	Approve updates, operate within trust model

AEF / ISO / VDMA	Standards bodies	Define protocols, PKI structure, testing procedures
Government Regulators	Policy and oversight	Enforce CRA, R155-equivalent regulations
Security Experts	Pen testers, consultants	Threat modeling, audit, design validation
Cloud Platform Providers	Data backend and UX	TLS, access control, telemetry integrity

Key Challenges Ahead

Agricultural cybersecurity faces a unique blend of technical and operational hurdles. **Certificate management remains difficult** due to the lack of secure clocks and update mechanisms in legacy equipment. **Over-the-air (OTA) updates are constrained** by seasonal equipment availability, creating narrow windows for secure deployment. Many systems **lack runtime protection** such as message authentication or encryption on CAN buses, while **long service lifecycles** make it impractical to update or secure older machines. Finally, **shared liability across multi-brand ecosystems** highlights the need for standardized trust frameworks and contractual clarity. Addressing these challenges requires solutions that are resilient, lifecycle-aware, and tailored to agriculture's real-world constraints.

Compounding these technical issues is the reality of the agricultural supply chain: unlike the automotive sector, agriculture operates at **lower production volumes**, limiting OEM buying power and influence over suppliers. This fragmentation makes it significantly harder to enforce cybersecurity standards across ECUs, sensors, and control modules. As a result, broad regulations like the **EU Cyber Resilience Act (CRA)** present a disproportionate burden to agricultural OEMs and Tier 1s who must comply without the economies of scale enjoyed by automotive peers. **Shared liability, legacy constraints, and a fragmented supplier base** all underscore the need for tailored, sector-specific security frameworks in agriculture.

- **Certificate Expiry & Rotation**: Most agricultural machinery lacks a reliable internal clock or secure update process, complicating certificate management and PKI trust models.

- **Data Ownership & Governance**: Disputes around who owns agronomic data (OEM, dealer, or farmer) create ambiguity and legal complexity for securing and sharing sensitive datasets.
- **Right to Repair Conflicts**: Security controls and diagnostics may clash with operator access demands under Right to Repair movements, leading to potential bypasses or tampering.
- **OTA vs Field Availability**: Agricultural updates must be planned around seasonal usage. Downtime or failed updates during planting or harvest windows can have catastrophic financial impacts.
- **Runtime Security Gaps**: Many ECUs still rely on CAN bus networks with no authentication or message integrity, exposing machines to spoofing or unauthorized command injection.
- **GNSS Correction Security**: RTK and GNSS correction signals used for precision farming are vulnerable to spoofing and jamming; secure standards and validation frameworks are urgently needed.
- **Legacy System Integration**: A significant portion of the ag fleet (including implements) will never see a firmware update. Protecting these devices requires network segmentation and compensating controls.
- **Shared Liability & Ecosystem Trust**: Mixed-fleet environments and multi-tier dealer networks require new contractual frameworks for cybersecurity responsibility, incident disclosure, and interoperability testing.

Strategic Recommendations

As we have covered in this article; Agriculture to be a fully digital ecosystem, its cybersecurity strategy must reflect the operational and technological realities of the field, not just the factory floor. First and foremost, agricultural systems must be designed for **offline-aware security**. Unlike connected consumer products or vehicles in urban centers, farm machinery often operates with limited or no connectivity. This demands secure-by-default designs that can authenticate, validate, and operate resiliently in isolation, without relying on real-time cloud checks or update servers.

To support this, the sector should adopt a **federated PKI infrastructure**, one that allows for industry-wide trust models but maintains flexibility by delegating certificate management to individual OEMs. This is especially important in a multi-brand environment where implements and tractors from different manufacturers must interoperate securely in the field.

Coupled with this, **lifecycle-conscious engineering** is critical. Agricultural equipment often remains in use for decades, requiring cybersecurity controls and architectures that anticipate extremely long service lives, with provisions for key rotation, update expiration, and backward compatibility.

In parallel, **harmonized regulation** across jurisdictions is essential. The convergence of ISO 21434, UNECE R155, the EU Cyber Resilience Act (CRA), and the new draft ISO 24882 for agricultural machinery presents an opportunity to align on globally consistent expectations while accommodating agriculture's unique constraints. Importantly, cybersecurity must no longer be siloed, it should be tightly integrated with **functional safety assessments** to create a unified risk picture, especially in safety-critical systems like autonomous tractors or sprayers.

Finally, the industry must invest in **transparent conformance testing**. Publicly available test labs and standardized validation procedures will build confidence across the supply chain, encourage OEM accountability, and reduce vendor lock-in. As new standards and frameworks emerge, the ability to demonstrate secure interoperability will become a cornerstone of trust in modern agricultural ecosystems.

Conclusion: Securing the Future of Food

Cybersecurity in agriculture is not just about protecting machines; it is about safeguarding global food security. From autonomous tractors to cloud-connected planters, agriculture is becoming a cyber-physical domain with high-value targets, safety-critical operations, and massive socio-economic consequences.

The sector must move beyond legacy assumptions and adopt cybersecurity frameworks that reflect its realities: **intermittent connectivity, long equipment lifecycles, and multi-brand mixed fleet field operations**. Through collaboration, standardization, and investment in secure design, the agricultural ecosystem can become resilient, not only to cyber threats but to the evolving risks of a digital world.

NCC Group brings deep expertise in securing cyber-physical systems across agriculture, automotive, and critical infrastructure sectors. We support OEMs, Tier 1s, and Agri-tech firms throughout the entire product lifecycle, from secure system design and threat modeling to **penetration testing, hardware assessments**, and **post-deployment assurance**. Alongside our specialist practices, tool and service capabilities can be refined to be domain focused to enhance functionality and relevance as we span across domains and sectors. Our teams help clients integrate security into development pipelines using **secure SDLC, assurance cases**, and regulatory alignment with ISO 21434, ISO 24882, and the EU Cyber Resilience Act.

Beyond engineering support, NCC offers advanced threat monitoring through **Endpoint Detection and Response (EDR)** and **Managed Extended Detection and Response (MXDR)** services that can also be tailored to fit sector use cases. These capabilities enable 24/7 visibility across endpoints, vehicle gateways, cloud platforms, and field infrastructure, helping detect and respond to attacks in real time. By combining **technical assurance, policy guidance**, and *active threat response*, NCC empowers the agricultural ecosystem to build resilience into machinery, data, and supply chains, today and over the decades-long service lifecycles to come.

To secure agriculture is to secure our futures resilience. And the time to act is now. As agricultural machinery becomes a core vector of innovation and risk, all stakeholders from global OEMs to regional co-ops, must align around a shared vision of security. This includes not just **hardening endpoints and vehicles,** but also ensuring **secure interoperability** across dealer networks, **GNSS correction services**, **software supply chains**, and **cloud-based data platforms**. The path forward requires a coordinated approach to resilience, one that balances performance, safety, regulatory compliance, and the practical constraints of farming cycles. Cybersecurity is no longer a back-office function, it is a frontline requirement for ensuring the **availability, safety, and integrity of modern agriculture.**

Acronyms and Abbreviations

ADAS – Advanced Driver Assistance Systems
AEF – Agricultural Industry Electronics Foundation
AG – Agriculture
AI – Artificial Intelligence
AV – Autonomous Vehicle
CAN – Controller Area Network
CoC – Chain of Custody
CRA – Cyber Resilience Act (European Union)
CSF – Cybersecurity Framework
CSMS – Cybersecurity Management System
DDoS / DoS – Distributed Denial of Service / Denial of Service
ECU – Electronic Control Unit
EDR – Endpoint Detection and Response
E/E – Electrical / Electronic (systems)
EIN – Ecosystem Interoperability Network (as referenced for cloud-to-cloud data exchange)
GNSS – Global Navigation Satellite System
GPS – Global Positioning System
HSM – Hardware Security Module
IP – Intellectual Property
ISOBUS – ISO 11783 tractor–implement communication standard
IT – Information Technology
MXDR – Managed Extended Detection and Response
NIS2 – Network and Information Security Directive (EU 2022/2555)
OEM – Original Equipment Manufacturer
OTA – Over-the-Air (software updates)

OT – Operational Technology

PKI – Public Key Infrastructure

RTK – Real-Time Kinematic

RTK-GPS – Real-Time Kinematic Global Positioning System

SDLC – Software Development Lifecycle

TARA – Threat Analysis and Risk Assessment

TLS – Transport Layer Security

TIM – Tractor Implement Management

UNECE – United Nations Economic Commission for Europe

Glossary

AEF (Agricultural Industry Electronics Foundation)

Industry organization supporting interoperability standards and conformance testing for agricultural electronics, including ISOBUS-related certification and test activities.

Agribusiness

Commercial agriculture organizations spanning production, processing, logistics, and retail, often operating at large scale and reliant on digital platforms.

Agronomic Decision Support

Software-driven analysis that uses field and machine data (e.g., soil telemetry, yield data) to recommend actions such as irrigation timing or input application.

Air-Gapped / Offline Operation

Operation in environments without reliable cellular, Wi-Fi, or satellite connectivity, limiting real-time authentication, monitoring, and patching.

Assurance Case

A structured argument, supported by evidence, that a system's cybersecurity claims are met across its lifecycle.

Attack Surface

The total set of reachable interfaces, systems, tools, and dependencies that could be targeted (machines, cloud, dealer/service tooling, manufacturing, etc.).

Backend Platforms

Cloud and enterprise systems used for fleet management, yield tracking, maintenance, analytics, and user access that integrate with machines in the field.

CAN (Controller Area Network)

A vehicle/machinery communication bus technology used for ECU messaging, common across automotive and agricultural machinery.

Certificate Spoofing

An attack in which an adversary forges or misuses digital credentials to impersonate a trusted machine/implement or service.

Cloud-to-Cloud Data Exchange

Secure exchange of agricultural data between cloud platforms (including cross-brand environments), supporting interoperable fleet visibility and analytics.

CoC (Chain of Custody)
In this paper's context, maintaining trustworthy provenance/traceability of software, messages, or artifacts through signing/validation so changes are detectable.
Conformance Testing
Standardized testing against defined protocols to ensure multi-vendor interoperability and expected behavior in realistic conditions.
Critical Infrastructure
Systems essential to societal stability; agriculture is treated as critical due to its impact on food supply, economic stability, and national security.
CSMS (Cybersecurity Management System)
A governance and process framework required by UNECE R155 to manage cybersecurity risk across the vehicle/product lifecycle.
Cyber-Physical System
A system where digital components (software, networks, sensors) directly control physical behavior (tractors, implements, autonomous machines).
Damage Scenario
A concrete, real-world impact pathway from threat → exploit → outcome (e.g., lockout during harvest, false agronomic analysis, unsafe movement).
Dealer Networks
Dealership ecosystems and their tooling/portals that provision, diagnose, calibrate, and update equipment, often with privileged access.
Denial of Service (DoS)
Disruption that prevents systems from functioning or being used, especially harmful during narrow planting/harvest windows.
Decommissioning
End-of-life lifecycle phase where systems are retired and access, credentials, and data handling must be managed securely.
Diagnostic Tools / Service Tools
OEM or third-party tools (often laptops, USB storage, portals) used to service machines, a prominent attack vector due to privilege and physical exposure.
E/E Systems (Electrical/Electronic Systems)
The integrated electrical and electronic architecture of machines, including ECUs, networks, sensors, and controllers.
ECU (Electronic Control Unit)
Embedded controller responsible for specific machine functions (steering, braking, implement control, etc.), often connected via CAN/ISOBUS.
EDR (Endpoint Detection and Response)
Security capability for monitoring endpoints (devices/systems) for malicious activity and enabling response actions.
EIN (as referenced in paper)

A named effort in your paper describing **cloud-to-cloud data exchange standardization** to support cross-brand security architecture and visibility.

Farm Management Software
Digital systems used by farms to plan, operate, and analyze agricultural operations (often integrating machine and field data).

Federated PKI
A public key infrastructure model where industry-wide trust is enabled while certificate management can remain distributed (e.g., by OEM).

Firmware
Low-level software on embedded devices/ECUs; often difficult to update in long-lifecycle machinery and a common target for exploitation.

Functional Safety
Engineering discipline focused on preventing hazardous behavior from system failures; intersects with cybersecurity where cyber threats can cause unsafe outcomes.

Galileo OSNMA
A referenced satellite-navigation authentication capability intended to strengthen resilience against GNSS spoofing.

GNSS (Global Navigation Satellite System)
Satellite-based positioning (e.g., GPS) used for precision guidance, foundational to autonomy and precision operations.

GPS Spoofing / Jamming
Attacks that falsify or disrupt positioning signals, potentially causing unsafe movement or costly agronomic errors.

HSM (Hardware Security Module)
A hardware component used to protect cryptographic keys and enable secure operations like secure boot and signing.

Homologation
Regulatory compliance and approval activities to ensure systems meet requirements across markets.

Hybrid Seed Performance Data
Sensitive agronomic/IP data related to seed genetics and performance; highlighted as valuable for espionage or competitive advantage.

Incident Reporting (NIS2 context)
The obligation (in relevant EU regimes) to report significant cyber incidents within defined timeframes.

Interoperability
The ability of multi-brand tractors and implements to work together reliably, often via standardized protocols (expands security complexity).

ISOBUS / ISO 11783
A standard defining communication protocols between tractors and implements to enable interoperability, foundational to secure multi-brand operation.

ISO 24089
Software update engineering standard (automotive origin) referenced as relevant for secure and traceable update practices.

ISO 24882 (Draft)
An agriculture/off-road product cybersecurity standard under development, intended to define lifecycle cybersecurity engineering for agricultural and related machinery.

ISO 25119
Functional safety standard for agricultural/forestry machinery control systems; increasingly intersects with cybersecurity.

ISO/SAE 21434
Automotive cybersecurity engineering standard referenced as a foundational model for processes like TARA, security goals, and post-production monitoring.

IT/OT Convergence
Blending of enterprise IT systems (cloud, portals, analytics) with operational technology (machines, controls), increasing systemic risk and blast radius.

Lifecycle-Aware Design
Engineering that accounts for decades-long service life, including update strategy, key/cert rotation, backward compatibility, and decommissioning.

Mixed Fleet / Multi-Brand Ecosystem
Operational reality where equipment from multiple OEMs must interoperate in the same workflow (tractor + implement combinations).

MXDR (Managed Extended Detection and Response)
A managed service providing continuous detection/response across multiple telemetry sources (endpoints, cloud, gateways, etc.).

NIS2 (Directive (EU) 2022/2555)
EU directive imposing cybersecurity governance, risk management, and reporting requirements on essential/important entities (including relevant food/ag domains).

OTA (Over-the-Air) Updates
Remote update capability for software/firmware; valuable but constrained in agriculture by connectivity gaps and seasonal downtime constraints.

Penetration Testing (Pen testing)
Authorized testing that simulates attacker behavior to identify vulnerabilities in machines, platforms, and interfaces.

PKI (Public Key Infrastructure)
System of digital certificates and keys used to authenticate entities and protect communications.

Precision Agriculture
Data-driven agriculture using GNSS, sensors, analytics, and automation to optimize planting, spraying, irrigation, and harvesting.

Provisioning
Enrollment/activation process for equipment and services (often done via dealers/OEM tooling), granting identities and enabling functions.

Right to Repair
Movement advocating farmer/independent access to tools and software for repair; in your paper it also introduces risks via unofficial tools and bypassed controls.

Ransomware
Malware that encrypts systems/data for extortion; highlighted as a major threat to time-sensitive operations like processing and grain elevators.
Resilience / Operational Resiliency
Ability to maintain safe, continuous operations despite disruptions (cyber, physical, environmental), emphasizing offline operability and recovery.
RTK (Real-Time Kinematic) Correction
Technique providing high-accuracy positioning (sub-inch) by using correction signals; important and vulnerable without secure delivery.
Secure Boot
A mechanism ensuring only trusted, signed software can start on a device (often enabled by HSM-backed key protection).
Secure SDLC (Secure Software Development Lifecycle)
Development approach integrating security practices from early design through deployment and maintenance (“shift left”).
Shift Left
Embedding security earlier in the lifecycle (requirements/design), reducing late-stage risk and rework.
Supply Chain Risk
Risk introduced through suppliers, contractors, and third-party tools/services (including software supply chain and dealer/service ecosystems).
TARA (Threat Analysis and Risk Assessment)
A structured method to identify threats, assess risk, and derive security requirements/controls.
Telematics
Connectivity and data exchange capability for machines (fleet management, diagnostics, location, telemetry); a key interface and threat vector.
Telemetry
Operational data collected from machines/sensors (yield, soil, position, performance) used for analytics and decision support, also a sensitive target.
Threat Actor
An individual/group conducting attacks; in your paper includes nation-states, cybercriminals, insiders, hacktivists, opportunists, and competitors.
Threat Model
Structured representation of likely threats, attack paths, and impacts for a system/ecosystem.
Tier 1 / Tier 2 Suppliers
Component and subsystem suppliers in the manufacturing ecosystem; highlighted as fragmented in agriculture vs automotive and central to compliance burden.
TIM (as used in paper)
An industry initiative referenced for authenticated control between tractor and implement using certificates and PKI.

TLS (Transport Layer Security)
Cryptographic protocol referenced for protecting communications (e.g., RTK over TLS) and cloud interfaces.

UNECE R155
Regulation establishing cybersecurity management requirements (CSMS, TARA, lifecycle risk management) for type approval in UNECE markets; noted as influencing off-highway sectors.

UNECE R156
Regulation focused on software update management processes and traceability; referenced as part of automotive-derived practices relevant to ag.

USB Keys / Storage Devices (Service Vector)
Removable media used in service/update workflows; highlighted as a potential compromise path due to privilege and physical handling.

Vulnerability Disclosure / Handling
Processes to receive, triage, remediate, and communicate vulnerabilities; emphasized under regulatory expectations like the EU CRA.

References

ISO. (2021). *ISO/SAE 21434: Road vehicles — Cybersecurity engineering*. International Organization for Standardization.

UNECE. (2021). *UN Regulation No. 155: Cyber security and cyber security management system*. United Nations Economic Commission for Europe.

UNECE. (2021). *UN Regulation No. 156: Software update and software update management system*. United Nations Economic Commission for Europe.

European Union. (2024). *Cyber Resilience Act (CRA)*. Official Journal of the European Union.

European Union. (2023). *Regulation (EU) 2023/1230 on machinery*. Official Journal of the European Union.

European Union. (2022). *Directive (EU) 2022/2555 (NIS2 Directive)*. Official Journal of the European Union.

NIST. (2024). *Cybersecurity Framework (CSF) 2.0*. National Institute of Standards and Technology.

US Department of Homeland Security, & US Department of Agriculture. (2023). *Food and Agriculture Sector-Specific Plan*. U.S. Government.

ISO. (Draft). *ISO 24882: Agricultural machinery, tractors, and earth-moving machinery — Product cybersecurity*. ISO/TC 23/SC 19.

ISO. (2018). *ISO 25119: Tractors and machinery for agriculture and forestry — Safety-related parts of control systems*. International Organization for Standardization.

ISO. (2019). *ISO 11783 (ISOBUS): Tractors and machinery for agriculture and forestry — Serial control and communications data network*. International Organization for Standardization.

ISO. (2023). *ISO 24089: Road vehicles — Software update engineering*. International Organization for Standardization.

SAE International. (2016). *SAE J3061: Cybersecurity Guidebook for Cyber-Physical Vehicle Systems*. SAE International.

SAE International. (2021). *SAE J1939-91C: Secure Onboard Communication*. SAE International.

Agricultural Industry Electronics Foundation. (2023). *ISOBUS Conformance Testing and TIM Certification Framework*. AEF.

CISA. (2023). *Cross-Sector Cybersecurity Performance Goals*. Cybersecurity and Infrastructure Security Agency.

John Deere. (2022–2023). *Security research disclosures and firmware vulnerability discussions*. Public security research reports.

JBS Foods. (2021). *Public disclosures regarding ransomware incident*. Company and media reports.

The New Cooperative. (2018). *Ransomware incident affecting grain operations*. Public reporting.

Marks & Spencer. (2025). *Cybersecurity incident disclosures*. Public financial and regulatory reporting.