ISSN: 3029-0724

Research Article

Journal of Environmental Science and Agricultural Research

Food Defence and Fraudulent Activities in Food Transport: Insights from More than Sixty Transport Hygiene Risk Analyses, 2024–2025

Vladimir Surčinski[1*] and Hans-Dieter Philipowski[2]

[1]ENFIT International Association Supply Chain Safety, Belgrade, Serbia
[2]ENFIT International Association Supply Chain Safety, Hamburg, Germany

[*]Corresponding author
Vladimir Surčinski, ENFIT International Association Supply Chain Safety, Belgrade, Serbia.

Received: May 19, 2026; **Accepted:** May 30, 2026; **Published:** June 05, 2026

ABSTRACT

Background: Food transport is a distributed process with uneven control maturity across routes, assets, and operators. In addition to unintentional contamination hazards, transport networks are exposed to intentional interference (food defence) and economically motivated deception (fraudulent activities). Despite this, transport hygiene risk analyses are still most often discussed through a hygiene lens, with limited synthesis that explicitly combines defence and fraud perspectives.

Methods: We performed a retrospective review of anonymised outputs from more than sixty transport hygiene risk analyses conducted between 2024 and 2025 in bulk food logistics. Each assessment examined cleaning verification and validation evidence, loading and unloading controls, documentation integrity (including cleaning certificates), post-cleaning security, and chain-of-custody governance. Risks were mapped to operational control points (cleaning, sealing, loading, transport, unloading) and screened against credible threat scenarios using Motivation–Opportunity–Capability–Consequence scoring.

Results: The same control gaps repeatedly supported both defence and fraud scenarios. The most frequent weaknesses were: (i) reliance on paper statements and visual checks as release criteria; (ii) limited evidence that cleaning achieves allergen and residue control under operating conditions; (iii) inconsistent competence coverage for seal checks, anomaly reporting, and hold decisions; and (iv) weak control of custody breaks such as overnight stops, public parking, and uncontrolled waiting zones. Digital sealing and digital seal plans were observed in a minority of cases; when combined with geofencing and a defined incident response protocol, they improved detection of unauthorised opening events.

Conclusion: Transport hygiene risk analysis is strengthened when defence and fraud scenarios are built into risk ranking, control design, monitoring, and incident response, rather than treated as parallel topics. Practical recommendations are provided for sealing plans, digital seal governance, cleaning certificate integrity, secure holding zones, and competence-based escalation rules.

List of Abbreviations

FSMS	:	Food safety management system
TACCP	:	Threat assessment critical control points
VACCP	:	Vulnerability assessment critical control points
MOCC	:	Motivation–Opportunity–Capability–Consequence Scoring
THRA	:	Transport hygiene risk analysis

Keywords: Food Defence, Food Fraud, Transport Hygiene, Logistics, Chain of Custody, Digital Seals

Introduction

Food transport is often treated as a prerequisite programme within food safety management systems, yet it behaves as a

Citation: Vladimir Surčinski, Hans-Dieter Philipowski. Food Defence and Fraudulent Activities in Food Transport: Insights from More than Sixty Transport Hygiene Risk Analyses, 2024–2025. J Envi Sci Agri Res. 2026. 4(3): 1-4. DOI: doi.org/10.61440/JESAR.2026.v4.185

moving process line: frequent product changes, geographical transitions, and multiple organizations touching the same asset (vehicle, road tanker, intermediate bulk container, hoses, seals, and documentation). This structure increases variability and dilutes accountability. When acceptance controls rely on short handovers and paper - based proof of cleaning, both accidental failures and intentional manipulation can pass undetected.

Across 2024 - 2025, evaluations repeatedly observed that transport hygiene controls are commonly designed for 'normal' contamination scenarios, while the same control points are attractive for deliberate interference: unauthorized access after cleaning, seal bypass during overnight stops, and falsification of cleaning certificates or previous - cargo declarations. The defence guideline frames this reality as an operational chain of critical infrastructure points - cleaning, sealing, loading, transport, and unloading - and emphasizes structured, standardized, and technology - supported measures (digital seals, sealing plans, secure entry/exit procedures, and real - time control) to reduce opportunity and increase detection likelihood [7].

This manuscript consolidates insights from more than 60 transport hygiene risk analyses carried out during 2024 - 2025 and translates them into a practical improvement model that links food defence and food fraud to day – to - day transport hygiene evidence, with focus on seal governance, certificate integrity, custody breaks, and escalation rules.

Review of Literature

Food defence guidance focuses on credible threats, attacker pathways, and proportionate controls; in logistics the defining feature is that the transport asset spends time outside direct oversight of the food business operator, making custody, tamper evidence and rapid escalation central [1]. Food fraud guidance recognizes economically motivated deception and requires a structured vulnerability assessment and mitigation plan integrated into management systems [3,4]. Codex work to develop prevention and control guidance further confirms the topic's cross-sector relevance [2].

Transport hygiene risk analyses provide a field evidence base that reflects how controls behave in real life: documentation weaknesses, competence gaps, and variability in cleaning verification and validation. Publications describe recurring gaps in cleaning validation, training coverage and documentation depth, and recognize intentional contamination and fraudulent activities as part of the transport risk landscape [5,6]. The defence guideline operationalizes these insights through standardized measures such as sealing plans, digital seals, geofencing logic, and incident response protocols that include hold procedures and role assignment [7].

Materials and Methods

Retrospective observational study using anonymized findings from more than sixty transport hygiene risk analyses conducted from January 2024 to December 2025 across bulk food logistics. Assessments were performed as professional risk evaluations. No company names, routes, locations or commercially sensitive operational details are disclosed.

The transport hygiene risk analysis model reviewed: (i) cleaning evidence (procedures, parameters, verification and validation), (ii) transport unit design and suitability, (iii) loading and unloading control, (iv) documentation integrity and traceability (including cleaning certificates and previous - cargo declarations), and (v) competence and training coverage [5,6].

Table 1: Field - ready indices for certificate quality (CQI) and seal governance maturity (SGM)

Index	Score	Definition	Operational trigger (example)
CQI	0	Statement only; no parameters; no asset linkage	Hold until independent verification; enhanced inspection
CQI	1	Parameters listed but not verifiable	Verify plausibility; request supporting logs; increase sampling
CQI	2	Parameters + traceable link to system record	Standard acceptance + spot checks
CQI	3	Tamper - resistant and independently verifiable record	Standard acceptance; trend review
SGM	0	No defined sealing plan	High vulnerability; implement sealing plan before high - risk cargos
SGM	1	Sealing exists but not standardized	Define seal points and responsibilities; train personnel
SGM	2	Defined sealing plan + responsibilities	Routine seal checks at handover + documented verification
SGM	3	Digital seals + digital seal plan + incident response	Use geofencing alerts; hold on breach; download event log

In line with guidance, vulnerabilities were mapped to critical operational points: cleaning station exit controls, post-cleaning holding zones, sealing points and seal handover, secure entry/exit procedures at loader and receiver/unloader, and transport custody breaks (overnight stops, public parking, route deviation) [7]. Threat evaluation used Motivation–Opportunity–Capability–Consequence scoring. Each element was scored 1–5 and summed to a total risk score; scenarios were categorized as low, medium, or high risk per internal practice.

Findings were coded into standard categories and reported as frequency bands to protect confidentiality. Cleaning evidence strength was graded as none; documentary only; documentary plus on-site verification; or analytical verification (e.g., protein residue swabs, allergen tests, microbiology). A Certificate Quality Index (CQI, 0 - 3) was applied as: 0 = statement only with no parameters; 1 = parameters listed but not verifiable; 2 = parameters plus a traceable link to a system record; 3 = tamper - resistant and independently verifiable record. A Seal Governance Maturity score (SGM, 0 - 3) was applied as: 0 = no defined sealing plan; 1 = sealing exists but not standardized; 2 = defined sealing plan with responsibilities; 3 = digital seals and digital seal plan with centralized logs and defined incident response.

Descriptive statistics were summarized as recurrence bands. Exploratory association screening between CQI/SGM categories and defence vulnerabilities was performed using odds ratios (OR).

$$OR = \frac{a \cdot d}{b \cdot c}$$

Risk ranking (R) followed, where L reflects likelihood/ opportunity indicators (custody breaks, access control, documentation integrity) and I reflect impact (food safety, allergen, regulatory, and brand consequences).
R=L×I

Table 2: Exploratory association screening (odds ratio)

	Vulnerability present	Vulnerability absent
Low CQI / SGM group	a	b
Higher CQI / SGM group	c	d

Results

Across the dataset, four recurring themes aligned strongly with both defence and fraud scenario feasibility.

- Documentation integrity is a primary fraud - enabler. Cleaning certificates and previous - cargo declarations were frequently the decisive acceptance criterion at loading and unloading. In multiple cases the documentation confirmed that cleaning occurred but lacked verifiable parameters such as cleaning method, duration, timestamps, operator identification, and a traceable link to an auditable system record.
- Sealing and post - cleaning security are uneven, especially around custody breaks. Overnight stops, uncontrolled waiting zones, and parked assets after cleaning were common custody - break points. Where seal governance was weak or not standardized, the probability of undetected tampering increased.
- Cleaning validation gaps reduce both hygiene assurance and defence readiness. Where analytical verification was absent, residue carryover (including allergens) remained plausible, and the system had limited post - incident forensic capability.
- Competence coverage is not consistently transport - specific. Even where training exists, it often does not cover seal integrity checks, recognition of tampering indicators, escalation triggers, and hold procedures.

Digital sealing and digital seal plans were present in a minority of cases. When deployed with a defined sealing plan, centralized logs, and geofencing alerts, they enabled rapid detection of missing seals at loading, unauthorized opening events, and route deviations, and supported consistent hold – and - investigate decisions.

Discussion

The dataset indicates that transport systems often fail quietly: routine paperwork and visual acceptance can allow risk accumulation across repeated cycles. The key practical insight is that defence and fraud are not separate topics; they exploit the same structural weaknesses that also drive accidental contamination: weak evidence, variable execution, and diluted accountability.

The defence guideline states that protection of logistics from intentional threats requires structured, standardized, and technology - supported security measures, grounded in practical application and real - time control [7]. In the field dataset, the highest - leverage control upgrades were: (i) standardized sealing plans with defined seal positions and quantities; (ii) digital security seals linked to asset identity and transport documentation; (iii) centralized logging of seal data and event history; (iv) geofencing to detect unauthorized opening or route deviation; and (v) a documented incident response protocol with clear triggers and hold procedures.

Exploratory screening showed low CQI (0 - 1) and low SGM (0 - 1) categories co-present with higher defence vulnerability recurrence (custody breaks without defined response; lack of hold logic; absence of escalation roles). While causality cannot be proven in this observational design, the direction is consistent with fraud mitigation logic: controls must reduce opportunity and increase detection likelihood, not only demonstrate documentation presence [3,4].

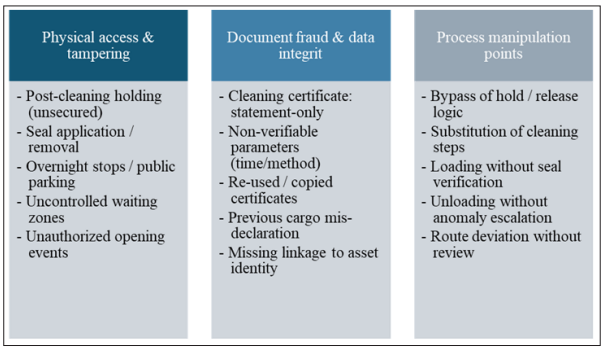

Figure 1: Attack surface map for transport hygiene (defence and fraud)

Use with THRA: map vulnerabilities to control points (cleaning → sealing → loading → transport → unloading) and apply MOCC scoring.

A three-barrier model is recommended for transport systems:

- **Barrier 1:** Evidence - based cleaning control (validated

programmes, parameter - based execution, risk - based analytical verification).
- **Barrier 2:** Tamper - resistant chain – of - custody (secure parking policy, custody - break rules, proportional receipt verification).
- **Barrier 3:** Certificate and seal integrity verification (digital seal plans, plausibility checks, centralized logs, hold – and - investigate triggers).

This model is implementable without over - engineering: it is primarily a governance and competence problem. Technology amplifies performance, but the decisive factor is whether acceptance decisions are evidence - driven and consistently applied.

Conclusion

Transport hygiene risk analysis becomes significantly more effective when it explicitly integrates food defence and food fraud scenarios into risk ranking and evidence requirements. Weak cleaning evidence, low - parameter certificates, weak sealing plans, custody - break gaps, and competence shortfalls create vulnerabilities that can be exploited intentionally or can hide accidental failure. A practical implementation path is to formalize sealing plans and incident response rules, elevate cleaning certificate integrity, and apply digital sealing/ geofencing where risk justifies it.

Limitations

This study is based on real-world professional assessments rather than controlled experiments. The depth of verification evidence varied between cases, and anonymization limited detailed comparisons by product category. Findings are therefore reported in recurrence bands to protect confidentiality, which reduces statistical precision.

Recommendations

1. Define a minimum cleaning certificate and seal data standard: asset identification, cleaning station identification, cleaning method/procedure, duration of exact cleaning procedure, timestamps, operator identification, sealing points, seal serial numbers, and a verification link to an auditable record.
2. Implement standardized sealing plans for each transport unit and assign responsibilities across cleaning, loading, transport, and unloading; require documented seal verification at each handover.
3. Where risk warrants, apply digital security seals and centralized digital seal plans; integrate geofencing alerts into dispatch/control room review.
4. Establish a secure holding zone after cleaning (controlled access, monitoring) and formalize post - cleaning seal application before leaving the cleaning station.
5. Document incident response protocols with hold – and - investigate triggers (seal missing at loading; breach alerts; suspicious objects), escalation roles, and corrective follow - up.
6. Build transport - specific competence profiles and verify through simulation exercises with documented debrief and corrective actions.
7. Perform building of competencies that includes specialized training of those involved in the supply chain with topics of the food defence and potentially fraudulent activities in cleaning and transporting.

Funding

No external funding was received for this study.

Acknowledgments

The author(s) acknowledge ENFIT International Association Supply Chain Safety for enabling anonymized aggregation of transport hygiene risk analysis insights, and thank participating food business operators, logistics providers, and cleaning stations for access to evidence under confidentiality arrangements.

References

1. British Standards Institution. PAS 96:2017. Guide to protecting and defending food and drink from deliberate attack (TACCP). BSI. 2017.
2. Codex Alimentarius Commission. Food fraud work advanced: draft guidelines on prevention and control of food fraud advanced for further development. Rome: FAO/ WHO Codex. 2024.
3. Global Food Safety Initiative. GFSI position on mitigating the public health risk of food fraud. GFSI. 2014.
4. Global Food Safety Initiative. Tackling food fraud through food safety management systems: technical document. GFSI. 2018.
5. Surčinski V. Food on the Move: Managing Hygiene and Safety Risks in Transport. Food Safety Magazine (reprint PDF provided by author). 2025.
6. Surčinski V, Philipowski H-D. Transport hygiene risk assessment results: trend analysis across 50+ evaluated food companies. Abstract. 2nd GHI World Congress: Transformation of Future Food Systems and Emerging Food Industries. 2025.
7. ENFIT International Association Supply Chain Safety. ENFIT-GUIDELINE Food-, Feed- und Chemical Defense. Protection of critical infrastructure in transport and logistic. Document code: 04/2025-1-EN. ENFIT. 2025.